UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMAS

TÍTULO:

““ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS. “

“TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS”.

AUTORES:

Cesar Augusto Bastidas Moncayo

Mariana Carmen González González

DIRECTOR:

Ing. Hernán Leonardo Torres Carrión Mg. Sc:

Loja – Ecuador
2013

CERTIFICACIÓN

Ing. Hernán Leonardo Torres Carrión Mg. Sc.

DIRECTOR DE TESIS

CERTIFICA:

Que la Tesis Titulada **"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS"**, de autoría de los señores egresados de la carrera de Ingeniería en Sistemas **Cesar Augusto Bastidas Moncayo y Mariana Carmen González González**, ha sido dirigida, revisada y aprobada en su integridad cumpliendo en su totalidad con los lineamiento de forma y fondo necesarios para su presentación y publicación.

Loja, Diciembre de 2012

Ing. Hernán Leonardo Torres Carrión Mg. Sc.

DIRECTOR DE TESIS

AUTORÍA

Nosotros Cesar Augusto Bastidas Moncayo y Mariana Carmen González González, declaramos ser autores del presente trabajo de tesis y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Incondicionalmente aceptamos y autorizamos a la Universidad Nacional de Loja, la publicación de nuestra tesis en el Repositorio Institucional-Biblioteca Virtual.

Autor: Cesar Augusto Bastidas Moncayo

Firma:

Cedula: 1104204795

Fecha: 10 de Mayo de 2013

Autor: Mariana Carmen González González

Firma: 

Cedula: 1104739865

Fecha: 10 de Mayo de 2013

AGRADECIMIENTO

En primer Lugar a Dios y a nuestros padres por habernos acompañado y guiado a lo largo de nuestra carrera, por ser nuestra fortaleza en momentos de debilidad y por brindarnos una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Nuestros más sinceros agradecimientos a la Universidad Nacional de Loja, que nos abrió sus puertas y nos concedió el privilegio de estudiar en esta noble institución de gran prestigio y trayectoria.

A los docentes que conforman la carrera de Ingeniería en Sistemas por compartir con nosotros sus experiencias y conocimientos en cada uno de los módulos hasta alcanzar nuestra meta

A la Unidad de Telecomunicaciones e Información sección Redes, que nos dio total apertura para llevar adelante este trabajo, especialmente al Tecnólogo Daniel Reyes, quien con su infinita paciencia y conocimientos nos supo guiar durante la elaboración del proyecto de fin de carrera.

Al Ingeniero Hernán Torres director de tesis, quien dedicó parte de su valioso tiempo a pesar de sus múltiples ocupaciones para guiarnos durante el desarrollo del proyecto de fin de carrera.

Así mismo agradecemos a todos nuestros amigos y compañeros con quienes compartimos la vida universitaria y fueron un gran apoyo en momentos difíciles, familiares y demás personas que nos supieron dar aliento en toda la etapa de estudiante.

Los Autores

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño.

A ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa.
Con mucho cariño principalmente a mis padres Luis Augusto y Lucia del Cisne, que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, a mí Esposa, Hija, y a todas las personas que con su cariño y aprecio han hecho posible cumplir una meta más en mi vida profesional.

Cesar Augusto

Con el más profundo agradecimiento y amor la presente Tesis la dedico a mis padres Ángel Naún y Aguedita de Jesús, que me apoyaron en todo momento y me ayudaron a cumplir esta gran meta a nivel profesional. Especialmente a ti mamá que estas en el cielo, gracias por tu esfuerzo y sacrificio siempre estarás en mi mente y corazón.

A toda mi familia, por estar siempre unida y brindarme todo su amor, a mis amigos y a todas las personas que con su apoyo incondicional me ayudaron en momentos difíciles y me enseñaron a apreciar la vida, gracias por creer en mí.

Mariana Carmen

CESIÓN DE DERECHOS

Por medio del presente documento Cesar Augusto Bastidas Moncayo y Mariana Carmen González González, autores de este proyecto de Tesis denominado **"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS."**, cedemos los derechos de autoría a la Universidad Nacional de Loja de forma que puedan hacer uso del material entregado como se crea conveniente.

Como autores originales del presente proyecto damos fe que todo lo entregado está de acuerdo al artículo 151 del **REGLAMENTO DE RÉGIMEN ACADÉMICO DE LA UNIVERSIDAD NACIONAL DE LOJA.**

Atentamente,
Los Autores.

A. TÍTULO

"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS. "

B.RESUMEN

En el presente proyecto de tesis se llegó a determinar las siguientes conclusiones y recomendaciones de acuerdo con los objetivos establecidos. Al realizar el análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, se concluyó que en la red de datos existe un solo domino de broadcast que provoca un bajo rendimiento en la red, además que la Sala de Servidores no cuenta principalmente con un Sistema Contra Incendios, UPS y una Planta Generadora de Energía. Por otra parte, se recomienda realizar un estudio para la implementación de VLans que alivie la creciente tormenta de broadcast en la red y adquirir la infraestructura mencionada.

Al determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, se llegó a concluir que la Sala de Servidores necesita principalmente de un segmentador de ancho de banda, UPS, una Planta Generadora de Energía, un Sistema Contra Incendios y se recomienda adquirir todo este equipamiento con las características establecidas en el proyecto.

En el establecimiento de las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores, se concluyó que NMAP es un potente Escáner de puertos y se recomienda actualizar las herramientas usadas para el proyecto como NMAP, NESSUS, NIKTO, CAIN&ABEL, e incrementar nuevas para el diagnóstico efectivo de vulnerabilidades. La principal conclusión a la que se llegó al realizar pruebas a los servidores para determinar las vulnerabilidades en los diferentes servicios que brindan, es que las vulnerabilidades lógicas se producen por el uso de protocolos no seguros para sus comunicaciones como HTTP y FTTP recomendamos usar protocolos seguros como HTTPS, IPSEC, SSH, TLS.

Al Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, se concluyó que las IPTABLES son mecanismos seguros de protección lógica mediante el filtrado de paquetes, recomendamos implementarlas en cada servidor nuevo para estandarizar la seguridad. En la Construcción de un plan de mitigación de riesgos en base a las vulnerabilidades encontradas, se concluyó que dicho plan es una herramienta valiosa para disminuir el impacto de los riesgos en la Sala principal de Servidores y se recomienda analizarlo y restructurarlo cada año.

SUMMARY

In the present thesis project we reached to determine the following conclusions and recommendations in accordance with the established objectives. At the moment to perform the analysis of the physic and logic servers of current situation of the Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, we concluded that there is only one data network domain of broadcast that causes a low performance in the network, besides the mainly server room does not have a fire system protection, UPS and one power generating plant. On the other hand, we recommend making a study for the implementation of the Vlans that alleviate the growing storm of broadcast in the network and obtain the mentioned infrastructure.

To determine the physical securities and the necessary equipment for the servers of the Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, we concluded that the mainly server room needs band width securities, UPS, a power generating plant, a fire system and we recommend to obtain all this equipment with the characteristics established in this project.

In the establishing of the suitable tools for the analysis of the logic vulnerabilities in the servers, we concluded that NMAP is a powerful scanner of ports and we suggest update the tools using for the project as NMAP, NESSUS, NIKTO, CAIN&ABEL and increase new ones for the effective diagnosis the vulnerabilities. The main finding that was reached at the moment to perform a testing to the servers to determine its vulnerabilities in the different services that provide, is that the logics vulnerabilities are produced because it is not used secure protocols for yours communications as HTTP y FTTP we recommend to use secure protocols as HTTPS, IPSEC, SSH, TLS.

To implement the solutions of the logics securities in the servers under the supervision of the Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, we concluded that the IPTABLES are secure logic protection mechanisms through packet filtering, we recommend to implement them in each new server to standardize the security. In the construction of a risk mitigation plan based on the vulnerabilities found, we concluded that the plan is a valuable tool to decrease the risk impact in the main server room and we recommend analyze and restore it each year.

_____

Traductora Lic. Cecilia Moncayo

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

C.INTRODUCCIÓN

La información es la parte fundamental de toda institución para tener un alto nivel de competitividad y posibilidades de desarrollo, por tal motivo la Universidad Nacional de Loja posee gran cantidad de información almacenada en diferentes tipos de servidores tanto internos como externos, los mismos que son susceptibles a ataques malintencionados en la intranet como extranet.

En la Sala de Servidores de la Universidad Nacional de Loja, el análisis de las vulnerabilidades físicas y lógicas de los servidores y la elaboración un plan de mitigación de riesgos es de suma importancia, ya que nunca se ha realizado un estudio de tal magnitud para conocer y solucionar tales vulnerabilidades.

El presente proyecto de fin de carrera detalla el análisis de las vulnerabilidades físicas y la propuesta para que disminuya el impacto de las mismas, también la forma en la que se llegó a determinar las vulnerabilidades lógicas y el proceso para solucionarlas, mejorando notablemente la seguridad lógica en los servidores de la Universidad Nacional de Loja.

Para estructurar el informe se siguieron ciertos lineamientos como: la metodología que nos permitió desarrollar el proyecto investigativo de forma secuencial y ordenada, de tal manera que podamos cumplir con los siguientes objetivos planteados:

- Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
- Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja
- Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores.
- Realizar pruebas a los servidores para determinar las vulnerabilidades en los diferentes servicios que brindan.
- Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

- Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas.

La fundamentación teórica nos ayudó a afianzar conocimientos acerca de procesos y herramientas necesarias en nuestra investigación.

En los resultados damos a conocer a detalle el proceso mediante el cual se llega a plantear soluciones a las diferentes vulnerabilidades físicas y lógicas encontradas durante el análisis realizado.

Parte fundamental del proceso investigativo fue la Evaluación del objeto, etapa en la que se explica cómo se fueron cumpliendo cada uno de los objetivos planteados.

La valoración Técnico-Económico-Ambiental exponemos todos los recursos utilizados para desarrollar nuestro proyecto.

En las conclusiones, damos una valoración del grado de cumplimiento de los objetivos trazados y los resultados alcanzados.

Las recomendaciones nos permiten expresar las consideraciones pertinentes a tomar en cuenta en la institución para salvaguardar los servidores tanto física como lógicamente y para el desarrollo de proyectos similares.

En la bibliografía listamos todas las fuentes consultadas para elaborar el proyecto de fin de carrera, y con los anexos hacemos referencia a toda la documentación clave para sustentar nuestro proyecto.

D. REVISIÓN DE LITERATURA

CONTENIDO

CAPÍTULO I

HACKING ÉTICO

1. HACKING ÉTICO

1.1 CONCEPTO

Desde el Punto de vista de un individuo, un Hacker Ético es un profesional que tiene las habilidades para evaluar la seguridad de un sistema informático de forma integral, llevando a la práctica una serie de pasos secuenciales y teniendo como un criterio trasversal una "Ética Profesional".

Desde el Punto de vista Comercial, el Hacking Ético es un servicio de Auditoria de T.I[1], que ofrecen empresas especializadas, con el fin de evaluar la seguridad de un sistema informático de forma integral.

El concepto de Hacking Ético fue utilizado en el presente proyecto de fin de carrera para buscar una metodología acorde al tema a desarrollar y para conocer detenidamente los lineamientos del hacker desde un punto de vista profesional y comercial.

1.2 TIPOS DE HACKING ÉTICO

Existen 2 tipos de hacking ético: análisis de vulnerabilidades (Vulnerability Assessment) y Test de Penetración (Penetration Test).

TABLA I Tipos de Hacking Ético

ANÁLISIS DE VULNERABILIDADES	TEST DE PENETRACIÓN
Identificación de Puertos Abiertos y Servicios	Tiene un Objetivo definido
Vulnerabilidades Conocidas (Aplicación y S.O)	Se tiene en cuenta el Entorno (IDS, Firewall, IPS)
Clasificación de los Vulnerabilidades	Busca comprometer el sistema objetivo
No hay explotación de vulnerabilidades, ni Intrusión en el Sistema.	Hay explotación de vulnerabilidades e Intrusión en el sistema objetivo

[1] **T.I:** Tecnologías de la información

En la Tabla I realizamos una comparación de las metodologías existentes para realizar proyectos de Hacking Ético, por lo tanto al comparar las dos metodologías se eligió la de Análisis de Vulnerabilidades por no ser intrusiva ni perjudicial para los servidores.

1.2.1 ANÁLISIS DE VULNERABILIDADES (VULNERABILITY ASSESSMENT)

Para la ejecución del presente proyecto de fin de carrera se utilizó la metodología para el Análisis de vulnerabilidades desarrollada por la empresa dsteam y basada en estándares internacionales y la aplicación de buenas prácticas en seguridad de la información, tales como la ISO 27001, ITIL, OWASP, COBIT y OSSTMM. Esta metodología tiene 5 fases.

El Análisis de vulnerabilidades consta de 5 fases claramente definidas que en la Figura 1 se detallan:

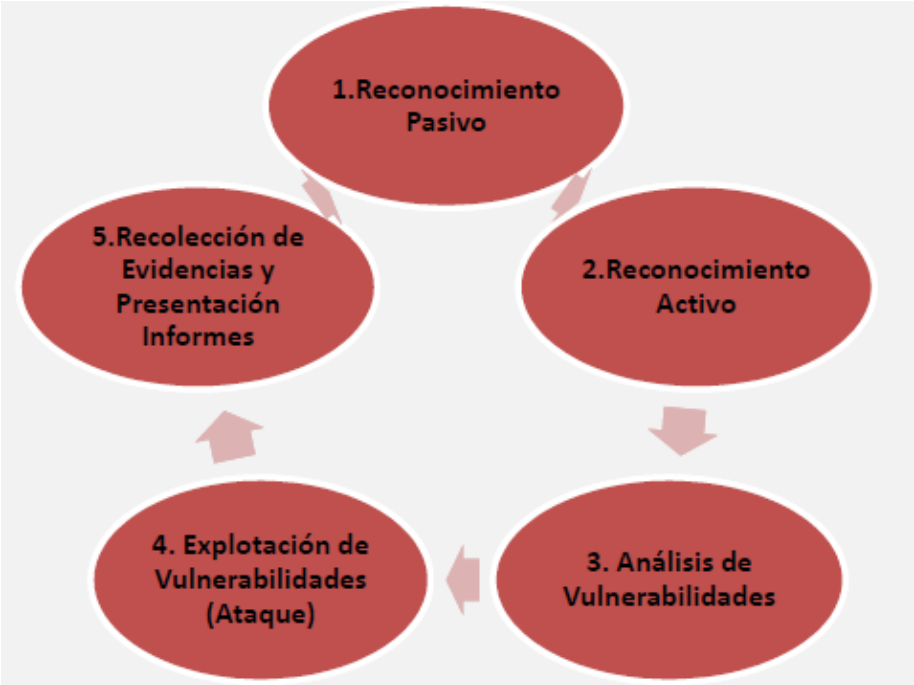


Figura 1. Fases para el Análisis de Vulnerabilidades

1.2.1.1 Reconocimiento Pasivo

En la primera y más importante fase del análisis. El analista trata de recopilar de forma metodológica toda la información al respecto del objetivo".

- No se realiza ningún tipo de escaneo o contacto con la máquina o máquinas objetivo.

- Permite Construir un mapa del Objetivo, sin interactuar con él o los objetivos.
- Existen menos herramientas informáticas que en las otras fases.
- Recolección de Información Pública (Ingeniería Social y Google Hacking).

Esta fase se la utilizó para investigar acerca del direccionamiento de los servidores y se trató de recopilar información acerca de vulnerabilidades que podrían afectar física y lógicamente a los mismos.

1.2.1.2 Reconocimiento Activo

En la segunda fase, y consiste en la identificación activa de objetivos, mediante el Escaneo de puertos y la identificación de servicios y sistemas operativos".

- Identificación y Estado de Puertos.
- Identificar Servicios.
- Identificar Sistemas operativos.
- Hay contacto directo con el Objetivo.
- Enumeración del Objetivo.
- Captura de Banners.

En esta etapa se recolectó información de los servidores y sobre la estructura física de la Sala de Servidores para establecer una lista de vulnerabilidades físicas y se describe el uso de los puertos en cada servidor y sistemas operativos usados.

1.2.1.3 Análisis de Vulnerabilidades

En la tercera fase del análisis, y tiene como objetivo el identificar si un sistema es débil o susceptible de ser afectado o atacado de alguna manera (Hardware, Software, Telecomunicaciones, Humanos)".

- Identificación vulnerabilidades en Versiones de Aplicación y Sistemas Operativos.
- Gestión de Parches (Patch Management).
- Identificar Vulnerabilidades Tecnológicas y Humanas.
- Configuraciones por Defecto.
- Vulnerabilidades Técnicas y Funcionales.

Algunos aspectos importantes que deben de tenerse en cuenta en el análisis de Vulnerabilidades, es el siguiente:

- Las herramientas de análisis de vulnerabilidades se basan en Plugins, por lo tanto es importante mantenerlos actualizados.
- Configurar de forma adecuada el perfil del análisis de vulnerabilidades, según la información recolectada en fases pasadas.
- Experiencia un factor “Relevante”.

Con el Análisis de vulnerabilidades se pudo desglosar cada una de las vulnerabilidades físicas y lógicas encontradas, además de establecer herramientas que se usará en cada fase, así como también se estableció la estructura física necesaria para solucionar las vulnerabilidades físicas.

1.2.1.4 Explotación de Vulnerabilidades

En la cuarta fase del análisis, y una de las más complejas, ya que el evaluador debe buscar aprovecharse de alguna de las vulnerabilidades identificadas, para lograr el ingreso (Intrusión) en el sistema objetivo.

- Escalar Privilegios.
- Explotación de Vulnerabilidades.
- Denegación de Servicios.
- Mantener el Acceso.

La explotación de vulnerabilidades, no necesariamente está ligada a la programación y ejecución de códigos de tipo “Exploit.”.

- Ingeniería Social.
- Claves débiles.
- Configuraciones por defecto.

En la cuarta fase se explotó las vulnerabilidades detectadas en los servidores y se implementó soluciones en la parte lógica en los servidores a los que se tiene acceso.

1.2.1.5 Presentación de Informes

En la quinta fase, que se ve reflejado el análisis del evaluador de seguridad, aquí se plasman todos los hallazgos, las no conformidades, las opciones para mejorar, y las conclusiones y recomendaciones.

- Un buen reporte, un buen análisis.
- Diversidad en reportes (Técnicos, Ejecutivos).
- No generar Alarmas.
- Impactos de Afectación. [1]

En la fase final se construyó un plan de mitigación de riesgos en base a las vulnerabilidades encontradas y se estableció acciones frente a la posibilidad de que cada una de las vulnerabilidades físicas y lógicas se pudiese presentar.

CAPÍTULO II

Identificación de Vulnerabilidades

2. IDENTIFICACIÓN DE VULNERABILIDADES LÓGICAS

2.1 VULNERABILIDAD

‘‘Una vulnerabilidad en seguridad informática hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales.

Las vulnerabilidades en las aplicaciones suelen corregirse con parches, hotfixs[2] o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático.

Las vulnerabilidades se descubren muy seguido en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan intrusos informáticos que quieran aprovecharse de ellas.

El concepto de vulnerabilidad nos permitió conocer de forma clara las debilidades a encontrar en la Sala de Servidores.

2.2 TIPOS DE VULNERABILIDADES

Algunas vulnerabilidades típicas suelen ser:

- ✓ Desbordes de pila y otros buffers.
- ✓ Symlink races[3].
- ✓ Errores en la validación de entradas como: inyección SQL, bug en el formato de cadenas, etc.

[2] **Hotfix:** Es un paquete que puede incluir varios archivos y que sirve para resolver un bug específico dentro de una aplicación informática.
[3] **Symlink races:** Vulnerabilidad de software de seguridad que resulta de un programa de creación de archivos de forma insegura.

- ✓ Secuestro de sesiones.
- ✓ Ejecución de código remoto.
- ✓ XSS[4].

Al conocer los tipos de vulnerabilidades más comunes podemos detectarlas de forma fácil, y en el proyecto de fin de carrera nos fue muy útil conocer este tipo de vulnerabilidades lógicas, ya que se utilizó este conocimiento para clasificar las vulnerabilidades detectadas en los servidores.

2.3 IDENTIFICACIÓN DE VULNERABILIDADES

El escaneo de vulnerabilidades permite identificar debilidades en el sistema evaluado, toma como base los detalles obtenidos durante las fases previas, el objetivo es identificar el método de ataque más efectivo y prever el tipo de información que se obtendrá cuando se explote la vulnerabilidad encontrada. Se debe tomar el mismo enfoque que tomaría un atacante real, ver a la organización como un adversario potencial e intentar causarle el mayor daño posible.

Existen distintos métodos para descubrir vulnerabilidades, así como también existen distintas herramientas automatizadas que pueden ayudar en esta fase. Se mencionan a continuación algunas técnicas que pueden ser utilizadas para descubrir vulnerabilidades:

Verificar la versión de software: Es una de las técnicas más comunes, basta con identificar el número de versión y compararlo con las listas de versiones vulnerables públicas gratuitamente en distintos sitios de seguridad. En este punto, se deben verificar también los parches y upgrades aplicados que podrían eliminar la vulnerabilidad. Aquí podrían ser utilizadas las herramientas libres nmap y amap.

Verificar la versión del protocolo de comunicación: Probablemente la versión de software no contenga vulnerabilidades, pero podría usar algún protocolo de red con problemas de seguridad.

- **Verificar la configuración:** Es necesario analizar los diferentes accesos que se podrían dar, remotos, locales y con distinto tipo de privilegios, no basta solo con analizar si se tiene configuración por default, es necesario revisar si las

[4] **CROSS-SITE SCRIPTING:** Tipo de vulnerabilidad Web, que permite a una tercera parte inyectar en páginas web vistas por el usuario código JavaScript o en otro lenguaje script similar.

configuraciones aplicadas por el administrador bastan para evitar problemas de seguridad.

- **Ejecución de exploits:** Se pueden ejecutar exploits sin conocer las vulnerabilidades presentes, tomando como base el prestigio del exploit y la información obtenida durante las fases previas. Esta técnica puede ser peligrosa ya que podría causar daños al sistema, incluyendo negación de servicio. Sin embargo, es posible representar una técnica muy cercana a lo que pasaría en caso de ser sometidos a ataques reales. Para la ejecución de esta técnica existen herramientas automatizadas. [2]

La forma de identificar las vulnerabilidades nos sirvió para determinar que tipo de identificación de vulnerabilidades se utilizaría en el proyecto de fin de carrera, decidiéndonos por la ejecución de exploits y verificación de la versión de software.

2.4 HERRAMIENTAS PARA LA IDENTIFICACIÓN DE VULNERABILIDADES

2.4.1 NESUSS

Nessus es un analizador de seguridad de red versátil, actualizado y de uso sencillo. Actualmente se encuentra entre los productos más importantes de este tipo en todo el sector de la seguridad y cuenta con el respaldo de organizaciones profesionales de seguridad de la información, tales como SANS[5] Institute. Nessus permite realizar auditorías de forma remota en una red en particular y determinar si alguien accedió de manera ilegal a ella o la usó de alguna forma inadecuada.

Nessus también proporciona la capacidad de auditar de forma local un equipo específico para analizar vulnerabilidades, especificaciones de compatibilidad, violaciones de directivas de contenido y más. A continuación se da conocer las características de NESSUS:

- ✓ **Análisis inteligente:** A diferencia de muchos otros analizadores de seguridad, Nessus no da nada por hecho. Es decir, no supondrá que un servicio dado se ejecuta en un puerto fijo. Esto significa que si se está ejecutado un servidor web en el puerto 1234, Nessus lo detectará y probará su seguridad según corresponda. Cuando sea posible, intentará validar una vulnerabilidad a través de su

[5] **SANS Institute:** SysAdmin Audit, Networking and Security Institute

explotación. En los casos en los que no sea confiable o se pueda afectar de manera negativa el destino, Nessus puede basarse en un banner del servidor para determinar la presencia de la vulnerabilidad. En tales casos, quedará registrado en el informe resultante si se usó este método.

- ✓ **Arquitectura modular:** La arquitectura cliente/servidor proporciona la flexibilidad necesaria para implementar el analizador (servidor) y conectarse con la GUI (cliente) desde cualquier equipo mediante un explorador web, con lo cual se reducen los costos de administración (varios clientes pueden acceder a un único servidor).
- ✓ **Compatible con CVE[6]:** La mayoría de los plugins se enlazan con CVE, para que los administradores obtengan más información sobre las vulnerabilidades publicadas. También incluyen frecuentemente referencias a Bugtraq[7] (BID), OSVDB[8] y las alertas de seguridad de proveedores.
- ✓ **Arquitectura de plugins:** Cada prueba de seguridad está diseñada como plugin externo, y se agrupan en una de 42 familias. De esta forma, se puede añadir fácilmente sus propias pruebas, seleccionar plugins específicos o elegir una familia entera sin tener que leer el código del motor de servidores Nessus, nessusd.
- ✓ **NASL:** El analizador Nessus incluye NASL (Nessus Attack Scripting Language), un lenguaje diseñado específicamente para crear pruebas de seguridad de manera rápida y sencilla.
- ✓ **Base de datos actualizada de vulnerabilidades de seguridad**: Tenable se centra en el desarrollo de comprobaciones de seguridad correspondientes a vulnerabilidades recientemente divulgadas. La base de datos de comprobaciones de seguridad se actualiza diariamente.
- ✓ **Prueba varios hosts de forma simultánea:** Según la configuración del sistema del analizador Nessus, se puede probar una gran cantidad de hosts simultáneamente.
- ✓ **Reconocimiento inteligente de servicios:** Nessus no espera que los hosts de destino respeten los números de puertos asignados por IANA[9]. Esto significa que reconocerá un servidor FTP que se ejecute en un puerto no estándar (por ejemplo, 31337) o un servidor web que se ejecute en el puerto 8080 en lugar del 80.

[6] **CVE:** Common Vulnerabilities and Exposures (Vulnerabilidades y amenazas comunes)
[7] **BUGTRAQ:** Es una lista de correo electrónico para publicacion de vulnerabilidades de software y hardware.
[8] **OSVDB:** Open Source Vulnerability Database
[9] **IANA**: Internet Assigned Numbers Authority

- ✓ **Varios servicios:** Si se emplean dos o más servidores web en un host (por ejemplo, uno en el puerto 80 y el otro en el puerto 8080), Nessus los identificará y los probará todos.
- ✓ **Cooperación de plugins:** Las pruebas de seguridad realizadas por los plugins de Nessus cooperan de manera tal que no se lleven a cabo comprobaciones innecesarias. Si un servidor FTP no ofrece inicios de sesión anónimos, no se realizarán comprobaciones de seguridad relacionadas con estos.
- ✓ **Informes completos:** Nessus no solo le informa qué vulnerabilidades de seguridad existen en su red y el nivel de riesgo de cada una de ellas (bajo, medio, alto y crítico), sino que también notifica sobre cómo mitigarlas, ofreciendo soluciones.
- ✓ **Compatibilidad total con SSL:** Nessus tiene la capacidad para probar los servicios ofrecidos sobre SSL, tales como HTTPS, SMTPS, IMAPS y más.
- ✓ **Plugins inteligentes (opcionales):** Nessus determinará qué plugins deben o no iniciarse en el host remoto. Esta opción se denomina “optimization”.
- ✓ **No destructivo (opcional):** Ciertas comprobaciones pueden ser perjudiciales para servicios de red específicos. Si no desea arriesgarse a provocar un error de servicio en la red, habilite la opción “safe checks” de Nessus, que hará que Nessus se base en los banners en lugar de la explotación de errores reales para determinar si hay alguna vulnerabilidad.

Nessus está basado en una arquitectura de tipo cliente/servidor. El servidor es el encargado de comprobar la seguridad de un equipo y el cliente es el responsable de realizar las peticiones. Podríamos decir que el servidor es el motor y el cliente simplemente el entorno gráfico.

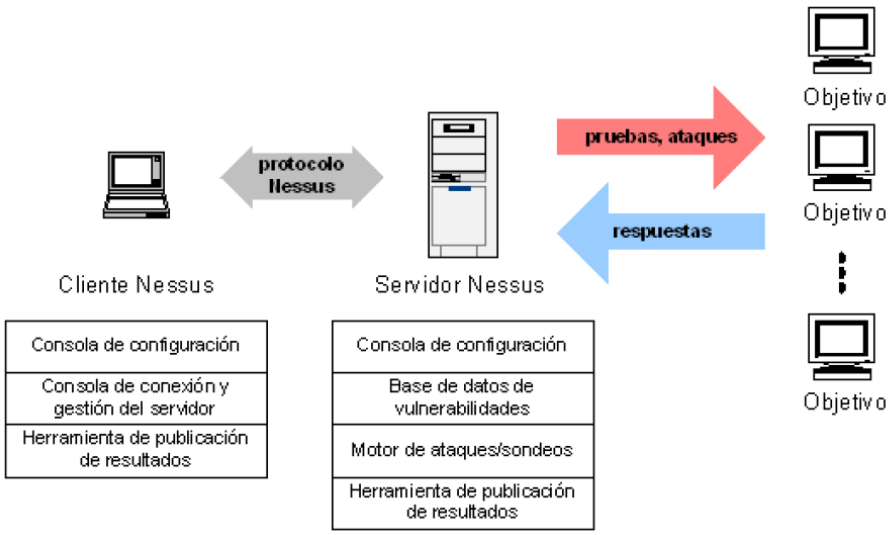


Figura 2. Arquitectura de NESSUS

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

Opcionalmente, los resultados del escaneo pueden ser exportados en reportes en varios formatos, como texto plano, XML, HTML, PDF, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades. [3]

La herramienta para la detección de vulnerabilidades lógicas NESSUS se la utilizó en la fase tres denominada Análisis de Vulnerabilidades.

2.4.2 NMAP

NMAP (Network Mapper o Mapeador de Redes) es una herramienta para scannear puertos abiertos. Se diseñó para explorar grandes redes, aunque funciona a perfecto también para hacer mapeos a equipos individuales. A demás de puertos, también dice que servicio lo utiliza y sus versiones. Otra de las cosas que suele mostrar es que filtros o cortafuegos tiene, y a veces hasta el sistema operativo que tiene el equipo entre otras docenas de cosas.

Figura 3. Ejemplo de uso de NMAP

Nmap es una herramienta que se usa mucho en auditorias de seguridad y además muchos la usan con fines delictivos. Lo primordial es su tabla de puertos con sus estados que son los siguientes:

Closed: Cerrado

Open: Abierto

Filtred: Filtrado

Unfiltred: No Filtrado

Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados.

Existen parámetros en mayúsculas y minúsculas, es muy importante respetarlos ya que varía su función.

Nmap cuenta con una interfaz gráfica denominada Zenmap, válida tanto para Windows como para Ubuntu y otros sistemas (MAC OS, BSD,...), es gratuita y de código abierto.

Proporciona la ventaja de ser más intuitiva para los usuarios que no conocen nmap y sus posibilidades y por otro lado, proporciona más opciones de ejecución a los usuarios más avanzados.

Zenmap permite la creación de perfiles de ejecución y de esa forma hacer más sencilla la repetición de órdenes. También permite guardar los informes obtenidos de la exploración en una base de datos.

Nmap (y Zenmap) permite trabajar con scripts (pestaña Scripting) que amplían la funcionalidad de nmap más allá de la exploración. Con estos scripts nmap puede hacer incluso análisis de vulnerabilidades. Pero hay que recordar que no es esta la finalidad de nmap. Esta funcionalidad está disponible tanto en GNU/Linux (*/usr/share/nmap/scripts*) como en Windows (*Archivos de Programa\Nmap\scripts*).

Los scripts están clasificados por categorías: *safe, intrusive, malware, discovery, vuln, auth, external, default, y all*. La extensión es *.nse*.

El script whois, por ejemplo, permite hacer una consulta a las bases de datos whois para obtener información acerca de una organización, país de origen, nombre de red, etc de los hosts explorados. [4]

El scanner de puertos NMAP se utilizó en la fase de Reconocimiento Activo para identificar el estado de puertos y servicios en los servidores.

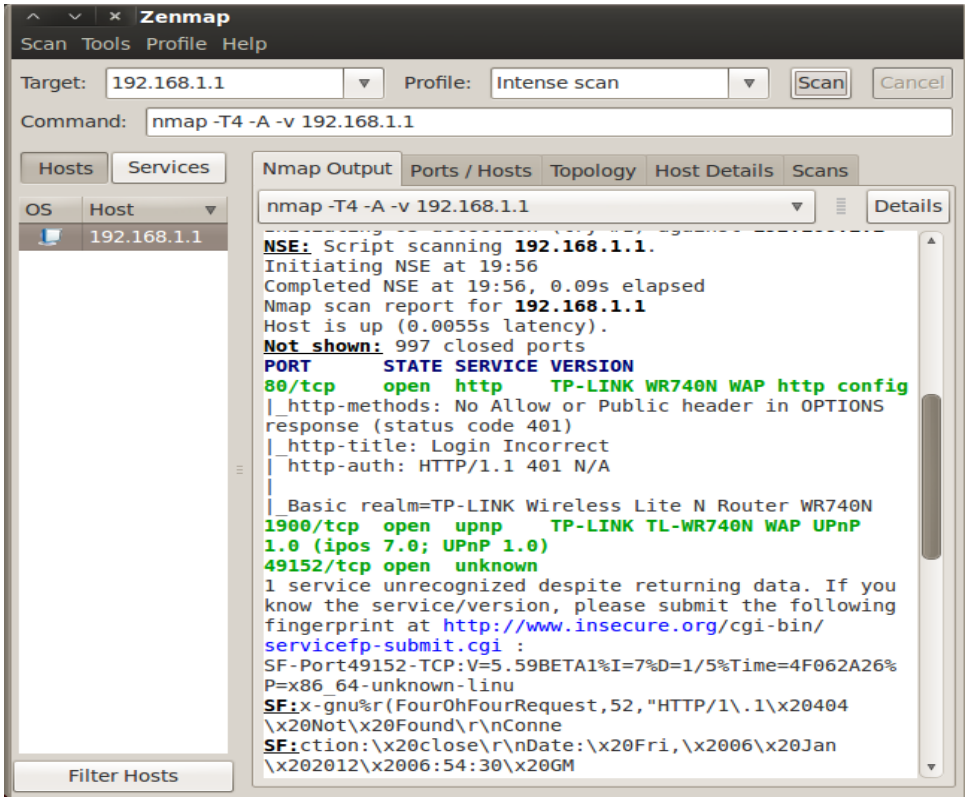


Figura 4. Interfaz gráfica de NMAP

2.4.3 CAIN Y ABEL

Cain & Abel es una poderosa herramienta gratuita que permite comprobar la seguridad de las redes y recuperar contraseñas (usando diccionario, fuerza bruta, sniffing, ataques criptoanálisis, etc), siendo sin duda uno de los referentes mundiales utilizado por administradores de redes, profesores y diferentes profesionales de la seguridad, en la administración, control de redes y recuperación de contraseñas. [5]

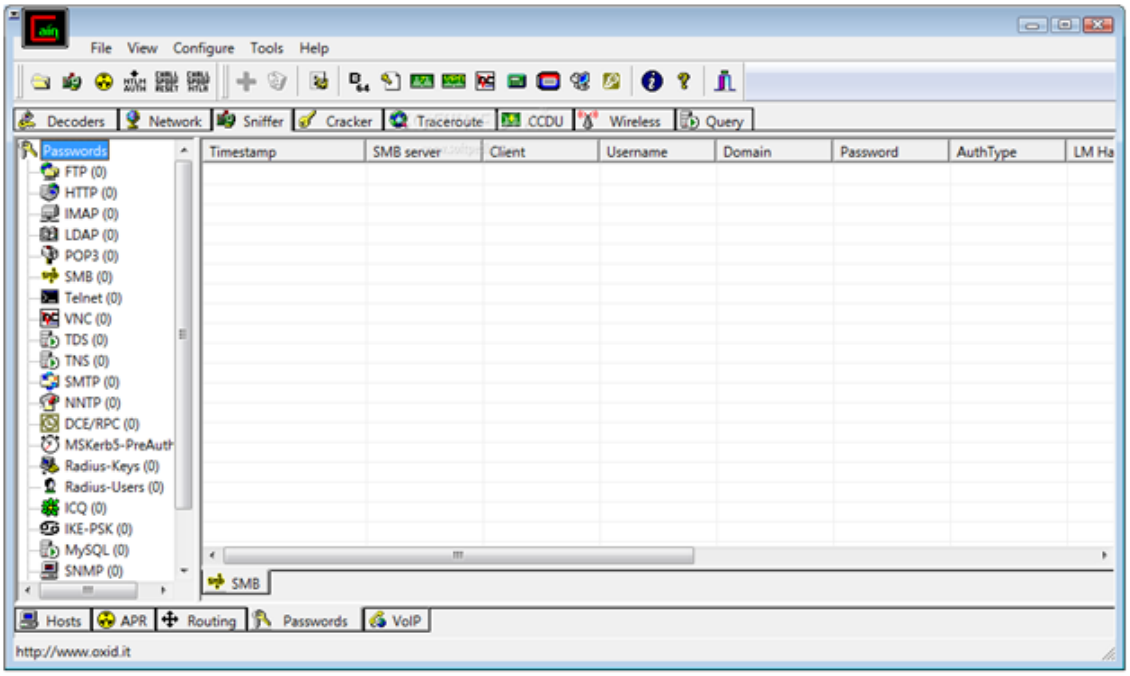


Figura 5. Interfaz de Cain y Abel

La herramienta Cain y Abel fue utilizada en la fase de Explotación y Solución de Vulnerabilidades para demostrar la existencia de las vulnerabilidades encontradas.

2.4.4 NIKTO

Nikto es un scanner de vulnerabilidades de servidores web licenciado bajo la licencia GPL que permite obtener un informe detallado sobre un sitio web para poder evitar posibles ataques.

Una de las ventajas de Nikto es la posibilidad de actualizarlo periódicamente con esto aumentamos la cantidad de ataques más comunes a un sitio web.

Las categorías de búsqueda de fallas que busca nuestro escáner es el siguiente:

- Problemas de configuración. Busca fallos en la configuración del servidor.
- Archivos y scripts por defecto. Detecta problemas en los programas que los servidores implementan por defecto.
- Archivos y scripts inseguros. Analiza el servidor web en busca de funcionalidades inseguras.

- Versiones desactualizadas de software. Permite detectar problemas y nos alerta de si alguna actualización del sistema debe ser instalada para evitar dejar abiertos nuevos agujeros.

Nikto es capaz de trabajar sobre 3200 archivos/CGIs potencialmente peligrosos, 625 versiones de servidores, y 230 problemas específicos de éstos. Los CGI (Common Gateway Interface) son programas o scripts que permiten dar dinamismo a las aplicaciones Web. Ésta es la razón por la cual existen agujeros de seguridad ya sea por un código mal implementado, instalaciones realizadas en forma predeterminada o por versiones posteriores en nuestros programas entre otros.

La utilización de Nikto es muy sencilla. Tan sólo hay que tener instalado un intérprete de Perl en el sistema que entienda las órdenes que se realicen.

Para empezar a utilizar la aplicación se teclea:

nikto [-h destino] [opciones]

Donde –h indica el destino del escaneo y donde opciones es una larga lista en la que se destacan las siguientes:

Parámetros de nikto: [6]

TABLA II Parámetros de Nikto

PARÁMETRO	DESCRIPCIÓN
Cgidirs	Permite indicar qué directorios de cgis se van a escanear, por ejemplo, 'none' indica que ninguno, 'all' todos y un valor concreto como /cgi/ indica que sólo se escaneará dicho directorio.
Evasión	Permite activar la evasión de detección de intrusos de acuerdo a varias opciones extra, como son por ejemplo, la finalización prematura de URL's, tabulador como el espacio requerido en vez del espacio normal, etc… Así

	estamos detectando posibles modos de ocultar la identificación de servidores
Findonly	Utiliza el escaneo de puertos para encontrar puertos válidos de http o https, pero no hace ninguna comprobación contra ellos.
Format	Esta opción se usa conjuntamente con la opción output, y lo que hace es aplicar al archivo de salida (que se crea al usar output) el formato HTML, TXT o CSV
Host	Establece el host o los hosts a los que se les realizan el escaneo. Se pueden utilizar nombres, ficheros o Ip's. Cargar un fichero es muy útil cuando queremos escanear una serie de muchos servidores y así no tenemos que escribirlos a mano.
Id	
Output	Genera un fichero de informe en el formato que la opción –format indique. Si no está especificado con –format, el formato de salida es en TXT.
Port	Permite establecer el puerto que quiere escuchar. Si no se especifica ninguno se utiliza el puerto 80. También puede suministrar una listado de puertos
Ssl	Fuerza a que el modo sea SSL en los puertos que listamos
Timeout	Permite asignar un tiempo de espera personalizado por defecto es 10 segundos.
Useproxy	Utiliza la configuración del Proxy que aparezca en el fichero config.txt para realizar el escaneo.
Dbcheck	Esta opción chequeará la sintaxis de las comprobaciones que se alojan en el

	fichero scan_database.db, lo cual es muy recomendable y útil cuando dichas comprobaciones han sido hechas a mano por el usuario, con la consiguiente personalización que conlleva
Debug	Esta opción proporciona información detallada durante el escaneo. La información suministrada en ocasiones es demasiada y es más recomendable probar con la opción –verbose.
Update	Esta opción se utiliza cuando necesite actualizar la base de datos. Nikto se conecta con Cirt.net y descarga el fichero actualizado de scan_database.db y los plugins nuevos que hayan aparecido.
Verbose	Muestra en pantalla las acciones que realiza Nikto

Nikto fue utilizado en la fase de análisis de vulnerabilidades conjuntamente con NESSUS para contratar resultados obtenidos en los servidores en cuanto a vulnerabilidades lógicas.

CAPÍTULO III

Seguridades físicas y lógicas de Centros de Datos

3. SEGURIDADES FÍSICAS Y LÓGICAS DE CENTROS DE DATOS

3.1 SEGURIDADES FÍSICAS DE CENTROS DE DATOS

Los incidentes de seguridad están aumentando a un ritmo alarmante cada año. A medida que aumenta la complejidad de las amenazas, crece también el número de medidas de seguridad necesarias para proteger las redes.

Es la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Esta parte de seguridades físicas fue útil para conocer los tipos de soluciones en cuanto a la parte física y lógica de los servidores y tener un concepto más amplio del tema.

3.1.1 NORMAS ISO PARA LA SEGURIDAD DE LA INFORMACIÓN

La ISO (International Organization Standardization) es el organismo facultado para promover el progreso de pautas y recomendaciones internacionales de manufactura, comercio y comunicación para todas las ramas industriales a excepción de la electrónica y la eléctrica. Su función principal es la de buscar la estandarización de normas en productos y seguridad para las empresas u organizaciones a nivel internacional.

El conocimiento de las normas ISO nos ayudó en proyecto de fin de carrera para identificar los estándares a seguir para solucionar de manera óptima los problemas de seguridad existentes en la Sala de servidores.

3.1.1.1 ISO 27001

Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI[10] de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. Lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las

[10] **SGSI:** Sistema de Gestión de la Seguridad de la Información

organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles. [7]

Figura 6. Piramide de ISO 27001

Esta norma fue utilizada en el plan de mitigación de riesgos que está basado en este estándar al igual que toda la metodología que se usó para desarrollar el proyecto de fin de carrera.

3.1.2 EIA /TIA 942

La norma TIA-942, está basada en las normas TIA-568 y TIA-569. Asimismo aplica las instrucciones establecidas por la norma TIA-606.

Para el cableado vertical recomienda usar fibra óptica multimodo de 50 um. ya que es efectiva y más económica que la tipo monomodo, para grandes redes por sus altas velocidades en distancias amplias.

Para el cableado vertical siempre recomienda tratar de instalar el medio con mayor capacidad disponible en el mercado para evitar tener que cablear nuevamente ante nuevas necesidades. Por esta razón es que actualmente se recomienda UTP de categoría 6.

Por otro lado se especifica que se deben tener diferentes bastidores y estructuras de ruta por cada tipo de medio de transmisión que se esté usando, tener que cablear nuevamente ante nuevas necesidades. Por otro lado se especifica que se deben tener diferentes bastidores y estructuras de ruta por cada tipo de medio de transmisión que se esté usando.

Niveles de Redundancia

Lo ideal en un centro de datos es que esté disponible siempre, sin embargo a pesar de que el diseño haya sido muy bien detallado, existen fallas en los sistemas que hacen que haya tiempos fuera de servicio. Para evitar esto la norma TIA-942 ha especificado cuatro niveles de redundancia, también llamados tiers; a un mayor nivel se tendrá un centro de datos menos susceptible a interrupciones. Cabe señalar que cada sistema que compone el centro de datos es calificado con un tier, y al final el centro de datos recibirá el menor tier que tiene alguno de sus sistemas. Por ejemplo si el sistema de energía tiene un tier III y el sistema de acceso a telecomunicaciones cuenta con un tier II, entonces el centro de datos tendrá un nivel de redundancia de segundo nivel.

- **Tier I:**

No cuenta con redundancia para ningún sistema. Por ejemplo tiene solo un proveedor de servicios de telecomunicaciones, un solo punto de acceso de energía eléctrica o un solo sistema de HVAC. Cumple las condiciones mínimas para evitar inundaciones, como por ejemplo haber instalado falso piso. Los sistemas de respaldo de energía como los UPS van por la misma instalación eléctrica que la energía principal.

Generalmente se corta el servicio una vez al año por mantenimiento, que junto a las fallas inesperadas suman un aproximado de 29 horas al año fuera de servicio.

- **Tier II:**

Cuenta con un segundo punto de acceso para los servicios de telecomunicaciones, los UPS (se alimentan de un generador diésel) y un segundo sistema de HVAC.

Generalmente se corta el servicio una vez al año por mantenimiento, que junto a las fallas inesperadas suman un aproximado de 22 horas al año fuera de servicio.

- **Tier III:**

Cuenta con redundancia de equipos y rutas redundantes para telecomunicaciones, sistema eléctrico y HVAC. Se puede realizar mantenimiento de los componentes principales sin sufrir un corte de servicios.

El nivel de seguridad es mayor al contar con sistemas de CCTV (Circuito Cerrado de Televisión), blindaje magnético en las paredes, personal durante 24 horas, entre otros.

En el mejor de los casos alcanzará una disponibilidad de 99,98% lo que se traduce en 105 minutos de interrupción al año.

- **Tier IV:**

Cuenta con múltiples componentes y rutas de redundancia, muchas de estas siempre activas.

Soporta en el peor de los casos un incidente no planificado. Todos los equipos tienen redundancia de datos y cableado eléctrico en circuitos separados. Mayor protección para incidentes naturales como terremotos, huracanes o inundaciones.

En el mejor de los casos tendrá una disponibilidad de 99,995%, ya que el tiempo de corte que debería ser por una prueba planeada de la alarma contra incendios o un corte de emergencia de energía, no duraría más de unos cuantos minutos al año. [8]

Con la Norma EIA/TIA 942 se estableció las soluciones en la parte de seguridades físicas de forma técnica y ordenada en el proyecto de fin de carrera.

3.1.3 FACTORES QUE AFECTAN LA SEGURIDAD FÍSICA

Los riesgos ambientales a los que está expuesta la organización son tan diversos como diferentes sean las personas, las situaciones y los entornos. El tipo de medidas de seguridad que se pueden tomar contra factores ambientales dependerá de las modalidades de tecnología considerada y de dónde serán utilizadas.

3.1.3.1 Factores Ambientales

- **Incendios:** Los incendios son causados por fallas en instalaciones eléctricas o almacenamiento de material altamente inflamable.
- **Inundaciones:** Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.
- **Sismos:** Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

- **Humedad:** Se debe proveer de un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y al área de máquinas en forma exclusiva.
- **Hardware:** Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.
- **Suministro de energía:** Las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. También debe procurarse que dichas instalaciones proporcionen los voltajes requeridos para hacer funcionar un dispositivo, pues existen componentes de hardware que necesitan ser energizados a ciertos niveles de voltaje especificados por los fabricantes, de lo contrario se acortará su vida útil.
- **Descuido y mal uso:** Todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor que trae como consecuencia descomposturas prematuras y reducción del tiempo de vida.
- **Red de datos:** Esta amenaza se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta.

3.1.3.2 Factores Humanos

- **Robos:** Las computadoras son posesiones valiosas de las empresas, y están expuestas, de la misma forma que están expuestas las piezas de stock e incluso el dinero. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección de la que dan a una máquina de escribir o a una calculadora, y en general a un activo físico.

- **Actos vandálicos:** En las empresas existen empleados descontentos que pueden tomar represalias contra los equipos y las instalaciones. Actos vandálicos contra el sistema de red. Muchos de estos actos van relacionados con el sabotaje.
- **Fraude:** Cada año millones de dólares son sustraídos de empresas y, en muchas ocasiones las computadoras han sido utilizadas para dichos fines.
- **Sabotaje:** Es el peligro más temido en los centros de cómputo. Empresas que han intentado implementar sistemas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, el saboteador puede ser un empleado o un sujeto ajeno a la empresa.
- **Terrorismo:** Hace unos años, este hubiera sido un caso remoto, pero con la situación bélica que enfrenta el mundo las empresas deben de incrementar sus medidas de seguridad, por que las empresas de mayor nombre en el mundo son un blanco muy llamativo para los terroristas.
- **Ingeniería social:** En el campo de la seguridad informática ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos llevándolos a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social. Los usuarios son el elemento más difícil de controlar en un sistema informático. [9]

Al definir los factores que afectan a la seguridad en un centro de Datos se pudo establecer de forma rápida las vulnerabilidades tanto físicas y lógicas.

3.1.4 TIPOS DE SEGURIDADES FÍSICAS

3.1.4.1 Sistemas Contra Incendios

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas. Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los

elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los Sistemas de supresión con químicos gaseosos (sistemas de agente limpio) se han usado por más de 40 años para proteger equipo eléctrico y otros bienes que son susceptibles a los efectos dañinos de sistemas de protección a base de agua. Los sistemas de Supresión de Incendios con Agente Limpio son superiores al agua y polvos químicos, virtualmente en todos los sentidos:

- Los Agentes limpios no son conductores de electricidad y no dañan equipos electrónicos el agua es conductora de electricidad y arruina la electrónica.
- Agentes limpios son seguros para las personas.
- Agentes limpios no dejan residuos y no requieren de limpieza.
- Agentes limpios reducen la cantidad de humo y daños causado por el fuego, porque actúan rápidamente.
- Agentes limpios proveen una penetración tri-dimensional, extinguiendo incendios que el agua tal vez no puede alcanzar.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo. [10]
- Debe construirse un “piso falso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables. [10]

Conocer los tipos de Sistemas contra Incendios nos ayudó a definir el tipo de sistema contra incendios que recomendamos para la sala de servidores.

3.1.4.2 Impermeabilización

Las inundaciones y goteras son las causas de mayores desastres en centros de cómputos. Además puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas:

- Construir un techo impermeable para evitar el paso de agua desde un nivel superior.

Por la ubicación de la sala de servidores es necesaria conocer acerca de la impermeabilización y se usó para proponer la solución en esta parte.

3.1.4.3 Sistemas Eléctricos

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa. En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Las Compañías de distribución de Energía Eléctrica que brindan el suministro de energía hasta el cuadro de alimentación del CC, no ofrecen protección contra disturbios, porque encarecerían los costos de esta energía regulada. El fabricante de equipos de computación, no incorpora tal protección en sus 9 equipamientos por la misma razón anterior, para poder entregar una energía acorde a las altas exigencias de los CCs de misión crítica se comienza por el suministro de la energía, acondicionamiento y distribución de la misma, logrando así una alta confiabilidad del sistema eléctrico.

Equipamientos por la misma razón anterior, para poder entregar una energía acorde a las altas exigencias de los Centros de Cómputo de misión crítica se comienza por el suministro de la energía, acondicionamiento y distribución de la misma, logrando así una alta confiabilidad del sistema eléctrico.

Los problemas eléctricos son muy comunes en la sala de servidores por esta razón los conceptos que en esta parte presentamos los utilizamos para determinar las soluciones en esta parte.

3.1.4.4 Sistema De Aire Acondicionado

La sala de un CC requiere de un sistema de aire acondicionado capaz de mantener las especificaciones básicas del ambiente. El sistema de aire acondicionado en la sala del CC debe ser dedicado, totalmente independiente de cualquier otro sistema de refrigeración del edificio, no debe tener ambientes compartidos con otras oficinas, laboratorios etc. Debe tener capacidad de filtrar, enfriar, calentar, humidificar y des humidificar el aire, montado de tal forma que sea incapaz de producir vibraciones en el CPD[11]. Especificaciones básicas del ambiente. Estas especificaciones son generales, básicas y de ninguna manera garantizan la durabilidad de un sistema.

- ✓ Temperatura: 18-24 C (21 C Nominal).
- ✓ Variación máxima de temperatura: 3 C/ hora.
- ✓ Humedad relativa: 40 a 60% (50% nominal)
- ✓ Variación máxima de humedad: 6 % / hora.

Todas las especificaciones referentes a la temperatura deben ser reducidas de 1 grado centígrado por cada 1000 m. de altitud. Para que no exista choque térmico, la temperatura, humedad y pureza del aire dentro la sala del CC, deben ser controladas, aunque los sistemas se encuentren apagados.

El sistema de aire acondicionado es necesario para mantener la temperatura adecuada por esta razón, esta parte es importante para conocer especificaciones básicas para enfriamiento en la sala de servidores.

3.1.4.5 Sistemas de Control de Acceso Físico

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos, existen infinidad de mecanismos para el control de acceso:

[11] **CPD:** Centro de Procesamiento de Datos

Llaves	
Tarjeta Inteligente	
Token	
Cerraduras codificadas	
Controles biométricos	

Figura 7. Sistemas de Control de Acceso

La empresa debe contemplar controles adecuadamente razonables para evitar el acceso de individuos e incluso de personal "no autorizado" al CC o a las áreas de manejo de datos o información oficial exclusiva.

Estos sistemas de Seguridad deben contemplar el uso de claves de seguridad a ser ingresadas a través de un componente electrónico ubicado en cada área o por medio del uso de una tarjeta plástica codificada (inteligente). La asignación de claves debe ser modificada periódicamente para evitar cualquier infiltración dentro del archivo maestro de claves o el otorgamiento de las mismas entre usuarios.

La acción más indicada y recomendada para el control de acceso es identificar la profundidad de seguridad y aplicar los mecanismos combinados para el control de acceso.

Al conocer la problemática del control de acceso en la sala de servidores este concepto nos sirvió para determinar el tipo de control para esta vulnerabilidad.

3.2 SEGURIDADES LÓGICAS DE CENTROS DE DATOS

Es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

3.2.1 TIPOS DE SEGURIDADES

3.2.1.1 Control de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardas la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

El control de acceso fue utilizado en el proyecto de fin de carrera para establecer las formas de controlar el acceso lógico a los servidores en la fase de soluciones lógicas.

3.2.1.2 Identificación y Autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina IDENTIFICACIÓN al momento en que el usuario se da a conocer en el sistema; y AUTENTICACIÓN a la verificación que realiza el sistema sobre esta identificación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina “single log-in” o sincronización de passwords.

Este tipo de protección se utilizó en la fase de reconocimiento pasivo para determinar el tipo de identificación y autenticación usadas en los servidores.

3.2.1.3 Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **LECTURA:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **ESCRITURA:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **BORRADO:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Las modalidades de acceso se usan en los servidores para el manejo de archivos por parte de los técnicos y se utilizó en la fase de reconocimiento activo para determinar la modalidad de acceso que tiene cada uno de los técnicos.

3.2.1.4 Control de Acceso Interno

3.2.1.4.1 Palabras Claves (Passwords)

Generalmente se utilizan para realizar a autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

- **SINCRONIZACION DE PASSWORDS:** consiste en permitir que un usuario acceda con el mismo password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario. Sin embargo, estudios hechos muestran que las

personas normalmente suelen manejar una solo password para todos los sitios a los que tenga acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

- **CADUCIDAD Y CONTROL:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstos caduquen. [11]

El uso de passwords fue utilizado en la parte de definición de políticas de seguridad para establecer el uso de contraseñas en los servidores.

3.2.1.5 Puertos (Gateways)

Un Gateway es un server, que proporciona a clientes conectividad hacia el mundo exterior, estén o no dentro de una red.

Este server, puede ser cualquier tipo de máquina, con cualquier sistema operativo que sea capaz de proveer funcionalidades de router y firewall.

Un gateway o puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading, usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

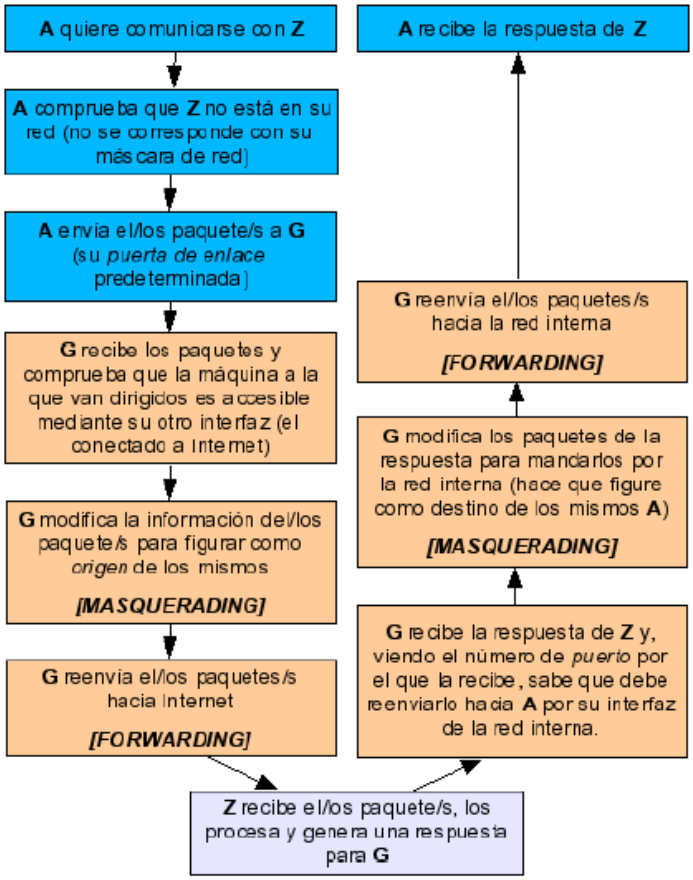


Figura 8. Funcionamiento Gateway

El conocimiento del funcionamiento de un Gateway nos fue útil en la etapa de análisis ya que existen varios servidores de este tipo y es básico conocer su funcionamiento.

3.2.1.6 Cortafuegos (Firewalls)

Se puede definir de una forma simple un sistema firewall, como aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre 2 redes como se muestra en la siguiente figura:

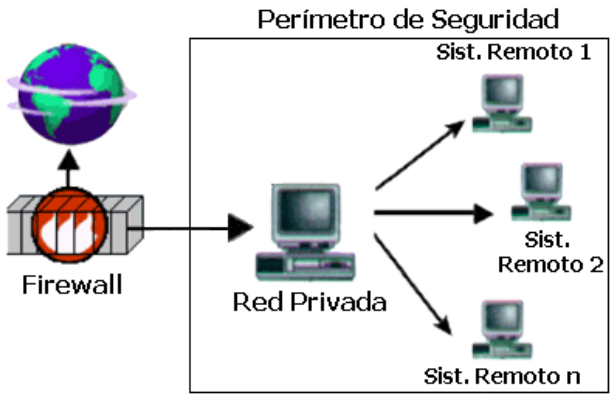


Figura 9. Esquema de funcionamiento de un Firewall

El firewall es un sistema que refuerza las políticas de control de acceso. Estas políticas regulan el tráfico entre una red interna (de confianza) y otra red externa (de dudosa confianza). Normalmente, los firewall se utilizan para proteger a las redes internas del acceso no autorizado vía Internet o mediante otra red externa.

La función del firewall, por tanto, es bloquear el tráfico no autorizado entre un sistema de confianza y un sistema de dudosa confianza.

Un firewall es, a menudo, instalado en el punto donde una red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del firewall, así puede determinar si dicho tráfico es aceptable de acuerdo a sus políticas de seguridad.

Aunque el propósito principal de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes le vuelve muy útil para controlar estadísticas de situaciones como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc. Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- ✓ Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- ✓ Prevenir los ataques
- ✓ Dividir una red en zonas con distintas necesidades de seguridad
- ✓ Auditar el acceso a la red.

Algunos firewall solamente permiten tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otros firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. Generalmente, los firewalls están configurados para proteger contra "logins" sin autorización. Esto ayuda principalmente a prevenir actos de vandalismos en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los usuarios del exterior. Los firewall pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello. [12]

Este concepto fue utilizado en la etapa de soluciones para la propuesta de un firewall a nivel de hardware ya que si se posee un firewall lógico.

3.2.1.7 Iptables

El filtrado de paquetes está incluido en el kernel de Linux. Para poder utilizar iptables, se debe compilar el kernel con la opción CONFIG_NETFILTER activada.

IPtables es un sistema de firewall vinculado al kernel. Un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación, iptables está integrado con el kernel, es parte del sistema operativo. Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas.

Iptables maneja las reglas de filtrado de forma dinámica. Esto significa que cada máquina sea reiniciada, las reglas se borrarán. Por este motivo, se recomienda crear un script que se ejecute al iniciar el sistema para que éstas vuelvan a ser definidas.

Una vez creadas las reglas, pueden ser grabadas por medio de la orden iptablessave y pueden ser recuperadas con iptables-restore.

El núcleo de Linux agrupa las diferentes reglas definidas por el administrador en tres listas denominadas chains: INPUT, OUTPUT y FORWARD. Cuando un paquete es recibido, el sistema utiliza en primer lugar las reglas de la lista INPUT para decidir si la acepta o no. Si las reglas definidas en esta lista indican que el paquete puede ser aceptado, se comprueba dónde debe ser enrutado. Si el destino es una máquina diferente a firewall, se aplican las reglas de la lista FORWARD para reenviarlo a su destino.

La lista OUTPUT se utiliza antes de enviar un paquete por una interfaz de red, para decidir si el tráfico de salida es permitido o no.

Si el paquete no cumple ninguna de las reglas de la lista, puede ser aceptado o rechazado según haya sido configurado el iptables. Para lograr mantener un nivel óptimo de seguridad, se recomienda que sea configurado para que rechace el paquete.

Cuando un paquete cumple con una determinada regla de una lista, se define qué hacer con éste mediante una acción (Target). Las acciones utilizadas en iptables son: ACCEPT, que permite el paso del paquete. DROP, que lo bloquea, QUEUE y RETURN. [13]

El conocimiento de Iptables nos fue útil en la fase de explotación y solución de vulnerabilidades lógicas ya que con este tipo de seguridad se solucionó la mayoría de vulnerabilidades lógicas detectadas.

CAPÍTULO IV

Plan de Mitigación de Riesgos

4. PLAN DE MITIGACIÓN DE RIESGOS

El plan de mitigación de riesgos es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución.

Garantiza la continuidad de las operaciones de los elementos considerados Críticos que componen los Sistemas de Información y definen acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

La siguiente estructura está basada en la Guía Avanzada para la Gestión de Riegos de INTECO empresa española con certificación ISO 27001:2005.

El formato de INTECO fue utilizado en la fase de presentación de informes para elaborar el plan de mitigación de riesgos parte de los objetivos del presente proyecto de fin de carrera.

4.1 RIESGO INFORMÁTICO

La posibilidad que una amenaza se materialice, utilizando una vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños en la actualidad se tiene diferentes medios de ataque que incrementa el riesgo de la pérdida de información.

4.2 PLAN DE MITIGACIÓN DE RIESGOS

Podríamos definir a un plan de mitigación de riesgos como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El un plan de mitigación de riesgos es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

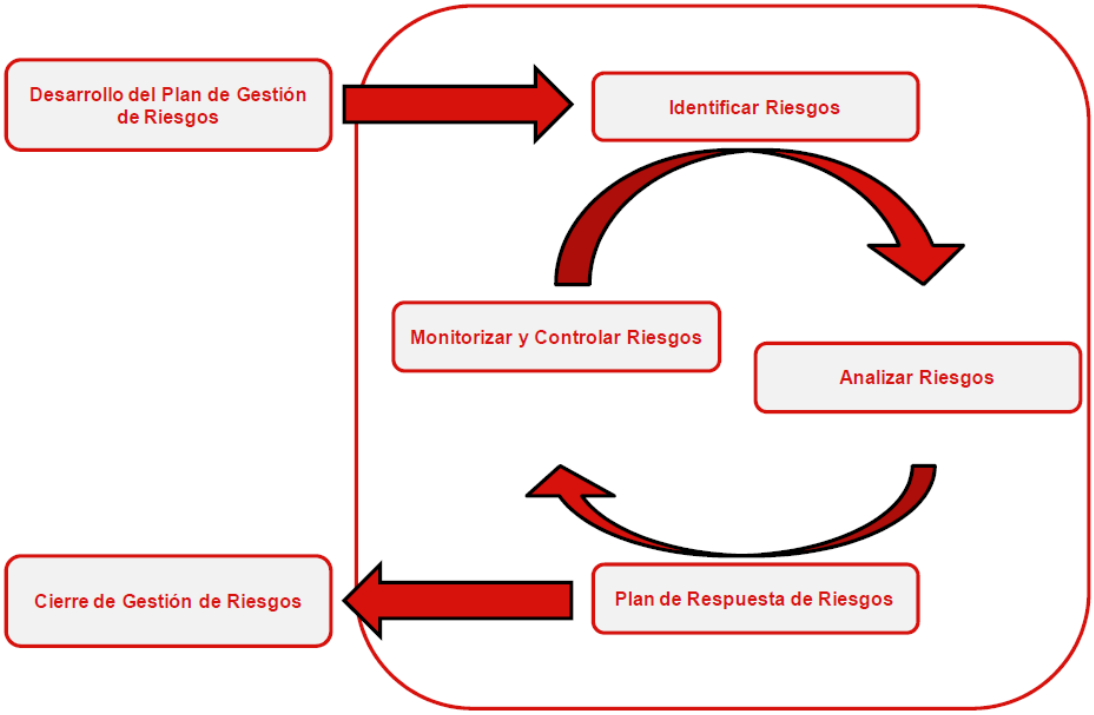


Figura 10. Etapas del Plan de Mitigación de Riesgos

4.2.1 IDENTIFICACIÓN DE RIESGOS

Para la identificación de riesgos se recomienda las siguientes técnicas:

4.2.1.1 Tormenta de ideas

La tormenta de ideas es una herramienta de trabajo grupal que facilita el surgimiento de ideas sobre un tema. La lluvia o tormenta de ideas, habitualmente conocida como "brainstorming", es una técnica de grupo para generar ideas originales en un ambiente relajado. La meta de la tormenta de ideas es obtener una lista completa de los riesgos del centro de cómputo. Se generan ideas acerca de los riesgos del centro de cómputo bajo el liderazgo de un facilitador. Los riesgos luego son identificados y categorizados por tipo y sus definiciones son refinadas.

4.2.1.2 Técnica Delphi

La técnica Delphi es una forma de llegar a un consenso de expertos. Es la búsqueda de consenso entre especialistas (expertos) sobre eventos futuros. Los expertos en riesgos de centros de cómputo participan en esta técnica de forma anónima. Un facilitador emplea un cuestionario con definición clara de objetivos y resultados deseados, para solicitar ideas acerca de los riesgos importantes del centro de

cómputo. Las respuestas son resumidas y luego enviadas nuevamente a los expertos para que realicen comentarios adicionales. En pocas rondas de este proceso se puede lograr el consenso. La técnica Delphi ayuda a reducir sesgos en los datos y evita que cualquier persona ejerza influencias impropias en el resultado.

Esta técnica está caracterizada por realizar cuestionarios de forma anónima, con un tratamiento estadístico simple y una re evaluación de respuestas para nuevo cuestionario. Los expertos que forman parte de esta técnica han de tener un amplio conocimiento sobre los riesgos.

4.2.1.3 Entrevistas

Entrevistar a participantes experimentados del centro de cómputo, interesados para identificar riesgos. Las entrevistas son una de las principales fuentes de recopilación de datos para la identificación de riesgos.

4.2.2 ANÁLISIS DE RIESGOS

El análisis de riesgos evalúa los riesgos identificados en la fase anterior para determinar la probabilidad de que ocurran, el impacto del riesgo, y la prioridad de cada riesgo.

Las actividades relacionadas con el análisis de riesgos están divididas en tres categorías:

- **Análisis cualitativo de riesgos**: evaluación del impacto y la probabilidad de ocurrencia de los riesgos sobre las salidas del proyecto utilizando métodos cualitativos.
- **Análisis cuantitativo de riesgos:** evaluación matemática de la probabilidad de ocurrencia de cada riesgo y sus consecuencias en las salidas del proyecto.
- **Priorización del análisis**: centralizar el esfuerzo de la gestión de riesgos y ganar el mayor impacto positivo posible sobre el proyecto para dicho esfuerzo.

El análisis de riesgo debería ser revisado y ajustado en función de los cambios que se vayan produciendo sobre los riesgos del centro de cómputo. Mientras se lleva a cabo el análisis de riesgos, es importante permanecer dentro del alcance tal y como se definió en el plan de gestión de riesgos.

Para analizar los riesgos se considera las siguientes técnicas:

4.2.2.1 Delphi

La técnica Delphi es de utilidad cuando se quiere llegar a un consenso entre un número de personas evitando la influencia entre las mismas. La técnica Delphi es utilizada en multitud de situaciones. Un ejemplo de ello es su uso durante la fase de identificación de riesgos. También se suele utilizar durante la fase de análisis cualitativo del proceso de gestión de riesgos.

4.2.2.2 Matriz probabilidad – impacto

La matriz de probabilidad impacto es una técnica comúnmente utilizada para realizar valoraciones cualitativas de riesgos. Se debe elaborar una matriz de análisis de riesgos con los siguientes datos:

TABLA III Matriz de Análisis de Riesgos

CATEGORÍA DEL RIESGO	NIVEL DE IMPACTO	NIVEL DE PROBABILIDAD	NIVEL DE RIESGO
Interrupción eléctrica	Crítico	Moderada	Crítico
Comunicaciones	Insignificante	Poco probable	Bajo
Respaldos	Critico	Poco probable	Crítico

Para establecer los valores de nivel de impacto, nivel de probabilidad y el nivel de riesgo fijarse en los valores descritos en las tablas II y III:

TABLA IV Valores de Niveles de Impacto

NIVELES DE IMPACTO		DESCRIPCIÓN
Crítico	10	El evento provoca una interrupción completa de la Tecnología en Informática y de todas sus operaciones. Los procesos críticos del negocio no tienen acceso a las instalaciones y tampoco a los recursos de información.
Significativo	7	El evento provoca una interrupción entre parcial y completa de la Tecnología en Informática y afecta a todos sus procesos.
Moderado	5	El evento provoca una interrupción en los servicios de TI

		y esto afecta los procesos, pero las actividades críticas no son interrumpidas.
Menor	3	El evento genera un leve impacto en los procesos, pero no ocasiona una interrupción importante en las operaciones. La interrupción de los servicios de TI afecta a menos de un 30% de los usuarios y dura lo suficiente para afectar levemente sus operaciones.
Insignificante	1	El evento no provoca un impacto en los procesos. La interrupción de los servicios de TI afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos.

TABLA V Valores de Niveles de Probabilidad

NIVELES DE IMPACTO		DESCRIPCIÓN
Casi cierta	10	Es muy probable que ocurra un evento de esta naturaleza en un periodo de tres meses.
Probable	7	Es probable que ocurra un evento de esta naturaleza en un periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a un año.
Poco probable	3	Es poco probable que el evento suceda pero podría ocurrir en algún momento de un periodo de un año a dos años.
Muy poco probable	1	Es muy poco probable que el evento se presente en un periodo más de 2 años y no se detectaron vulnerabilidades que aumenten su probabilidad de ocurrencia.

Para cada categoría de riesgo, se deberá especificar el nivel de impacto y el nivel de Probabilidad según las tablas respectivas indicadas anteriormente. Luego de esto, deberá determinar el nivel de riesgo asociado, y para esto deberá, revisar el valor asignado a cada nivel de Impacto y nivel de probabilidad y multiplicar dichos valores.

Para determinar el nivel de riesgo debe comparar los valores resultantes de acuerdo a los rangos de los criterios de calificación de los riesgos.

Para obtener el nivel de riesgo asociado únicamente deberá “cruzar” en la matriz la probabilidad versus el impacto y el color resultante representará el nivel asociado de riesgo.

Para la definición de los criterios de calificación de Riesgos considere la tabla IV y V:

TABLA VI Criterios de Calificación de Riesgos

Riesgo	Rango Inferior	Rango Superior
Muy Alto	70	100
Medio	35	69
Medio	16	34
Medio	6	15
Muy Bajo	1	5

TABLA VII Matriz de Riesgos Operativos

PROBABILIDAD					
	10	30	50	70	100
	7	21	35	49	70
	5	15	25	35	50
	3	9	15	21	30
	1	3	5	7	10
	INSIGN	MENOR	MODER	SIGNIF.	CRITICO
	IMPACTO				

Simbología del riesgo: Bajo | Moderado | Alto | Crítico

4.2.3 PLANIFICAR RESPUESTA A LOS RIESGOS

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal del Centro de Cómputo, personal de Seguridad.

Las actividades a realizar en un Plan de Recuperación de Desastres se clasifican en tres etapas:

- ✓ Actividades Previas al Desastre.
- ✓ Actividades Durante el Desastre.
- ✓ Actividades Después del Desastre.

4.2.4 CONTROLAR Y MONITORIZAR LOS RIESGOS

Las respuestas a los riesgos que están incluidas en el plan de mitigación se ejecutan durante el ciclo de vida del proyecto, pero deben ser supervisadas continuamente para detectar riesgos nuevos o cambiantes.

Controlar y monitorizar riesgos es un proceso que consiste en controlar los riesgos, gestionar los riesgos identificados, realizar seguimientos sobre los riesgos, descubrir nuevos riesgos, ejecutar planes de respuesta de riesgos y evaluar la efectividad de las acciones de respuesta. El proceso de seguimiento y control de riesgos, así como los demás procesos de gestión de riesgos, es un proceso continuo. Un control efectivo y una monitorización adecuada de los riegos proporcionan avisos tempranos de los riesgos y ayudan a ejecutar una toma de decisiones efectivas.

La monitorización de riesgos determina si:

- Los planes de respuesta de los riesgos han sido implementados de la forma adecuada.

- Los planes de respuesta de los riesgos son efectivos o si es necesario el desarrollo de nuevos planes.
- Las suposiciones de los riesgos continúan siendo válidas.
- Un disparador del riesgo ha ocurrido.
- Se han seguido las políticas de la empresa.
- Han aparecido riesgos no identificados.

El control de riesgos normalmente implica elegir nuevas estrategias de respuesta, ejecutar planes de contingencia, tomar acciones correctivas o modificar planes del plan. [14]

E. MATERIALES Y MÉTODOS

El desarrollo del proyecto de fin de carrera requiere seguir los lineamientos de ciertos métodos, así como de técnicas que permitieron la recopilación y análisis de la información necesaria para la presentación del proyecto de tesis, tales como:

MÉTODOS

Los métodos que se utilizaron para seguir un proceso ordenado en nuestra investigación fueron los siguientes:

- **Método Analítico.-** Sirvió para realizar un análisis de la situación actual de la Sala de Servidores, y con este método se pudo hacer un estudio de las vulnerabilidades para determinar sus causas y consecuencias en los servidores.
- **Método Inductivo:** Se lo utilizó para analizar cada una de las vulnerabilidades tanto físicas como lógicas encontradas durante el análisis de la situación actual de la Sala de Servidores.
- **Método Deductivo:** Este método nos sirvió para determinar las herramientas para detectar las vulnerabilidades lógicas y para establecer soluciones de cada una de ellas.
- **Método de Caja Blanca**.- Mediante este método se obtuvo información total acerca de los servidores y pudimos realizar el escáner de los servidores con privilegios dentro de la red, además gracias a este método se realizó un análisis completo y exhaustivo.
- **Metodología para el análisis de vulnerabilidades:** La metodología utilizada para el desarrollo del presente proyecto de fin de carrera es la metodología para el Análisis de vulnerabilidades desarrollada por la empresa dsteam[12] y basada en estándares internacionales y la aplicación de buenas prácticas en seguridad de la información, tales como la ISO 27001, ITIL, OWASP, COBIT y OSSTMM.

  Esta metodología consta de 5 fases claramente definidas que fueron adaptadas a las necesidades del proyecto para desarrollarlo de forma ordenada, y debido a que la primera fase denominada de reconocimiento pasivo es solo para recolección de información teórica se suprimió puesto que dicha recolección se realizó en el marco referencial quedando establecidas 4 fases que se ejecutaron de la siguiente forma:

[12] http://dsteamseguridad.com/

- **Reconocimiento Activo:** En esta fase se realizó entrevistas a los encargados de cada una de las secciones de la UTI para determinar la situación actual del Centro de Cómputo y elaboramos una lista de vulnerabilidades físicas además se identificó los recursos hardware y software con los que cuenta el Centro de Cómputo también mediante el uso de NMAP se pudo identificar los diferentes puertos y servicios de los servidores.
- **Análisis de Vulnerabilidades:** En esta fase se analizó las vulnerabilidades físicas y se propuso soluciones para las mismas según las necesidades del Centro de Cómputo, también se evaluó diferentes herramientas para escanear las vulnerabilidades lógicas y así determinar las adecuadas para el proyecto e identificar el número de vulnerabilidades por cada servidor al que se nos dio acceso.
- **Explotación y Solución de Vulnerabilidades Lógicas:** En esta etapa se realizó la explotación de ciertas vulnerabilidades y se eligió las configuraciones más idóneas para solucionar las vulnerabilidades y se las aplicó a los servidores a cargo de la UTI, y se realizó un nuevo escáner para comprobar que las vulnerabilidades lógicas se solucionaron.
- **Presentación de Informes:** Se elaboró un plan de mitigación de riegos para reducir el impacto de las vulnerabilidades en el Centro de Cómputo y para tener un referente para todos los técnicos, tesistas y pasantes que laboran en esta unidad, se elaboró el plan basándonos en la "Guía Avanzada para la Gestión Avanzada de Riesgos", elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO)[13] empresa española con la certificación ISO 27001 para la Gestión de la Seguridad en Centro de Datos.

TÉCNICAS

Las técnicas que se utilizarán para la recopilación de la información son las siguientes:

- **Lectura comprensiva.-** Con esta técnica se pudo adquirir conocimiento acerca de las vulnerabilidades, sus soluciones y las herramientas necesarias para detectar las vulnerabilidades lógicas.
- **La Entrevista:** Esta técnica ayudó a realizar un análisis preliminar de la UTI, pues permitió obtener la información en forma verbal de estado actual del centro de

[13] http://www.inteco.es/calidad_TIC/descargas/guias/guia_avanzada_de_gestion_de_riesgos

datos, a través de preguntas a los encargados de la Unidad de Telecomunicaciones e Información.

- **La Observación:** Se pudo observar el estado físico de los servidores y las vulnerabilidades físicas determinada previamente.

F. RESULTADOS

1. RECONOCIMIENTO ACTIVO

La fase denominada Reconocimiento Activo comprende el desarrollo del siguiente objetivo:

Objetivo 1: Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

Objetivo 1:

REALIZAR UN ANÁLISIS DE LA SITUACIÓN FÍSICA Y LÓGICA ACTUAL DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA

1.1. SITUACIÓN FÍSICA ACTUAL DE LOS SERVIDORES DE LA U.T.I. DE LA U.N.L.

La Unidad de Telecomunicaciones e Información está compuesto de 3 secciones: Redes, Desarrollo de Software y Mantenimiento. Las mismas que contribuyen a mejorar los servicios informáticos que presta la institución, la UTI[14] cuenta con un cuarto frío en donde se encuentran ubicados varios servidores tanto públicos como privados.

El proveedor de Servicios de internet es la empresa Telconet S.A que garantiza a la institución la conexión con la red de datos para el uso de internet, actualmente la institución cuenta con un ancho de banda de 100Mbps.

1.1.1. IDENTIFICACIÓN DEL HARDWARE DE LOS SERVIDORES

La Sala de Servidores está ubicada en el cuarto piso del Bloque Dos de la Administración Central.

En la tabla VIII se muestra las características hardware de los 27 servidores, que están distribuidos de acuerdo al servicio que prestan como web, OSticket, radio Universitaria, firewall, S.G.A[15], dns, dhcp, M.E.D [16] y proxys de las diferentes áreas, **Ver** Anexo II, en un espacio físico de 9 m^2.

TABLA VIII Hardware de los Servidores de la UTI

TIPO DE SERVIDOR	CARACTERÍSTICAS
FIREWALL (172.16.32.1)	Disco: 80GB Ram: 2 GB Velocidad Procesador: 1.86 GHZ Modelo: Intel(R) Xeon(R) CPU E5320
DNS y DHCP (172.16.32.2)	Disco: 120GB Ram: 2 GB Velocidad Procesador: 3.20 GHZ

[14] **UTI:** Unidad de Telecomunicaciones e Información
[15] **S.G.A:** Sistema de Gestión Académica
[16] **M.E.D:** Modalidad de Estudios a Distancia

	Modelo: Intel(R) Xeon(TM)
PROXY MED (172.16.32.28)	Disco: 320GB Ram: 2 GB Velocidad Procesador: 2.60 GHZ Modelo: Intel(R) Core(TM)2 Duo CPU E4700
PROXY EDUCATIVA (172.16.35.1)	Disco: 180GB Ram: 2 GB Velocidad Procesador: 3.20 GHZ Modelo: Intel(R) Pentium(R) 4
PROXY JURIDICA (172.16.37.1)	Disco: 180GB Ram: 2 GB Velocidad Procesador: 3.20 GHZ Modelo: Intel(R) Pentium(R) 4
PROXY AGROPECUARIA (172.16.40.1)	Disco: 80GB Ram: 2 GB Velocidad Procesador: 3.00 GHZ Modelo: Intel(R) Pentium(R) 4
PROXY ENERGIA (172.16.43.1)	Disco: 180GB Ram: 4GB Velocidad Procesador: 2.33 GHZ Modelo: Intel(R) Xeon(R) CPU 140
PROXY SALUD (172.16.45.2)	Disco: 300GB Ram: 4GB Velocidad Procesador: 2.93 GHZ Modelo: Intel(R) Core(TM)2 Duo CPU E7500
PROXY TRANPARENTE (172.16.32.27)	Disco: 150GB Ram: 1GB Velocidad Procesador: 3.4 GHZ Modelo: Pentium Dual Core
SERVIDOR NOC (172.16.32.3)	Disco: 150GB Ram: 1GB Velocidad Procesador: 3.4 GHZ

	Modelo: Intel Pentium
WEB **(192.188.49.2)**	Disco: 300GB Ram: 4GB Velocidad Procesador: 2.60 GHZ Modelo: Intel(R) Core(TM)2 Duo CPU E4700
WEBMAIL (192.188.49.20)	Disco: 300GB Ram: 2GB Velocidad Procesador: 2.93 GHZ Modelo: Intel(R) Core(TM)2 Duo CPU E7500
EVA **(192.188.49.16)**	Disco1: 160GB Disco2: 1TB Ram: 4G Velocidad Procesador: 2.13 GHZ Modelo: Intel(R) Core(TM)2 Duo
CURSOS **(192.188.49.13)**	Disco: 100GB Ram: 1G Velocidad Procesador: 3.2 GHZ Modelo: Intel Xeon

1.1.2. IDENTIFICACIÓN DE VULNERABILIDADES

Para la identificación de las vulnerabilidades se procedió a realizar una entrevista a los encargados del centro de cómputo, **Ver** Anexo I, y mediante la observación se determinó las siguientes vulnerabilidades físicas que para su mayor comprensión se clasificaron en la tabla IX:

TABLA IX Vulnerabilidades Físicas de los servidores de la UTI

CATEGORÍA	DEFINICIÓN	IMPACTO
Accesos no controlados	Ingreso no autorizado y/o por la fuerza la Sala de Servidores con	Robo o sabotaje de equipos

	intenciones maliciosas	
Filtraciones de Líquidos	Filtración de agua al interior de la Sala de Servidores	Daños en los pisos, el cableado y los equipos causados por goteras en el perímetro de la Sala de Servidores
Incendios	Ocurrencia de fuego no controlada que afecta a los equipos en la Sala de Servidores	Destrucción parcial o total de los equipos informáticos de la Sala de Servidores.
Cortes de luz	Pérdida total de suministro eléctrico.	Perdida del trabajo que se está realizando en la memoria RAM o caché. Perdida de Datos en disco duro
Variaciones de Voltaje	Aumento repentino y sustancial del voltaje.	Daños graves en el hardware y pérdida de datos.
Hardware	Probabilidad que las piezas físicas del sistema fallen ya sea por mal uso, descuido etc.	Disminución del rendimiento de los servicios que presta el servidor posible colapso.
Ubicación	Mala distribución de los equipos al interior de la Sala de Servidores.	Sobrecalentamiento de los equipos por falta de ventilación.

Temperatura de operación.	Temperatura de funcionamiento óptima recomendada por los fabricantes de los equipos.	Recalentamiento, pérdida de información, colapso en el sistema.

1.2. SITUACIÓN LÓGICA ACTUAL DE LOS SERVIDORES DE LA U.T.I. DE LA U.N.L.

Para la identificación de puertos, servicios y software en los servidores se utilizó Nmap con su interfaz gráfica Zenmap para evaluar a cada uno de los servidores.

1.2.1. IDENTIFICACIÓN DE SERVICIOS Y ESTADO DE LOS PUERTOS EN LOS SERVIDORES

Luego de verificar el estado de los puertos con NMAP, utilizando los siguientes comandos:

```
nmap -p 1-65535 T4 -A -v -PE -PS22,25,80,3389 IPServidor
```

4.2.4.1 Dns-Dhcp

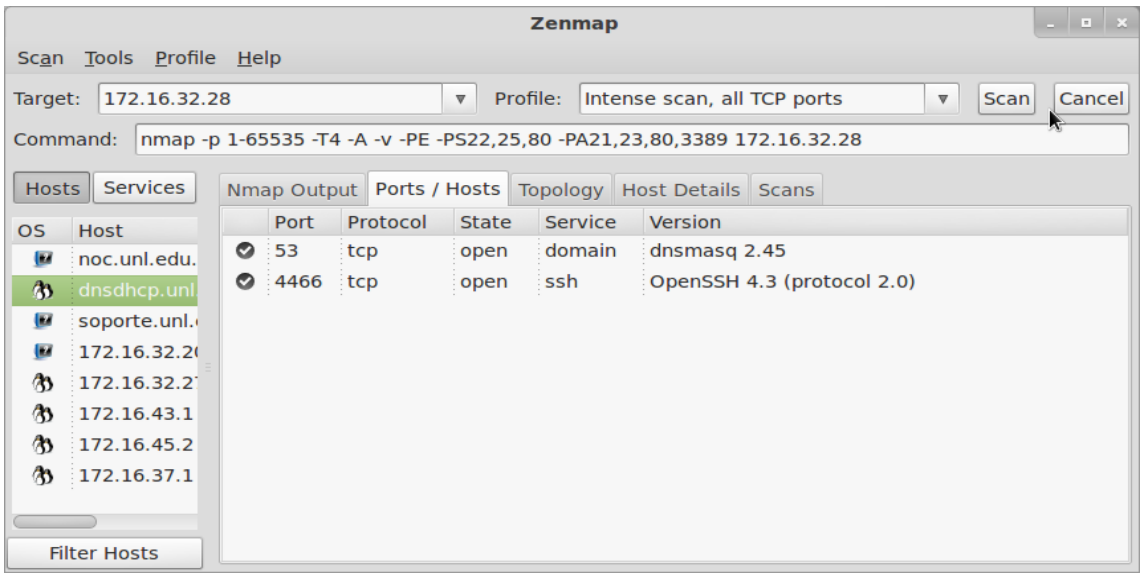


Figura 11. Capturas de ZENMAP servidor DHS-DHCP

4.2.4.2 Web

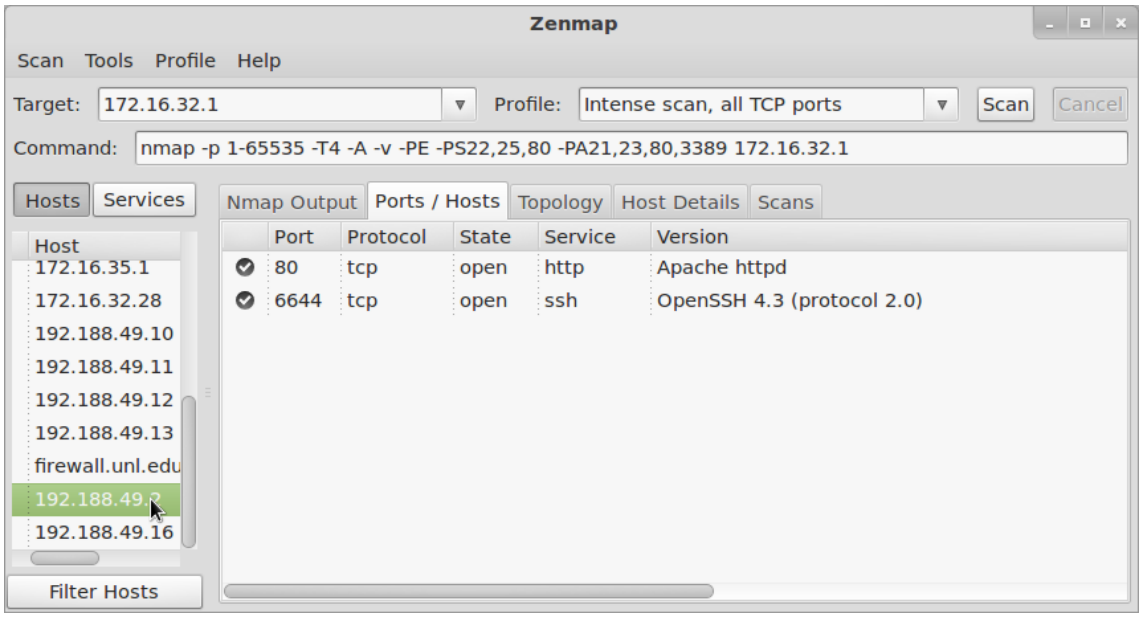


Figura 12. Capturas de ZENMAP servidor Web

4.2.4.3 Proxy Energía

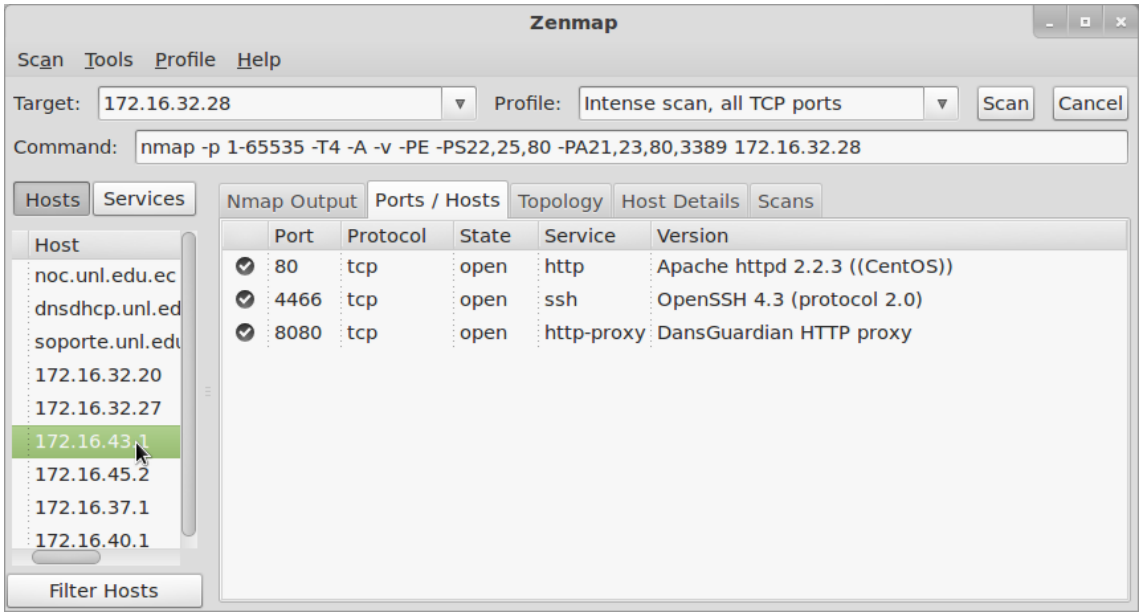


Figura 13. Capturas de ZENMAP servidor Proxy Energía

4.2.4.4 Proxy Salud

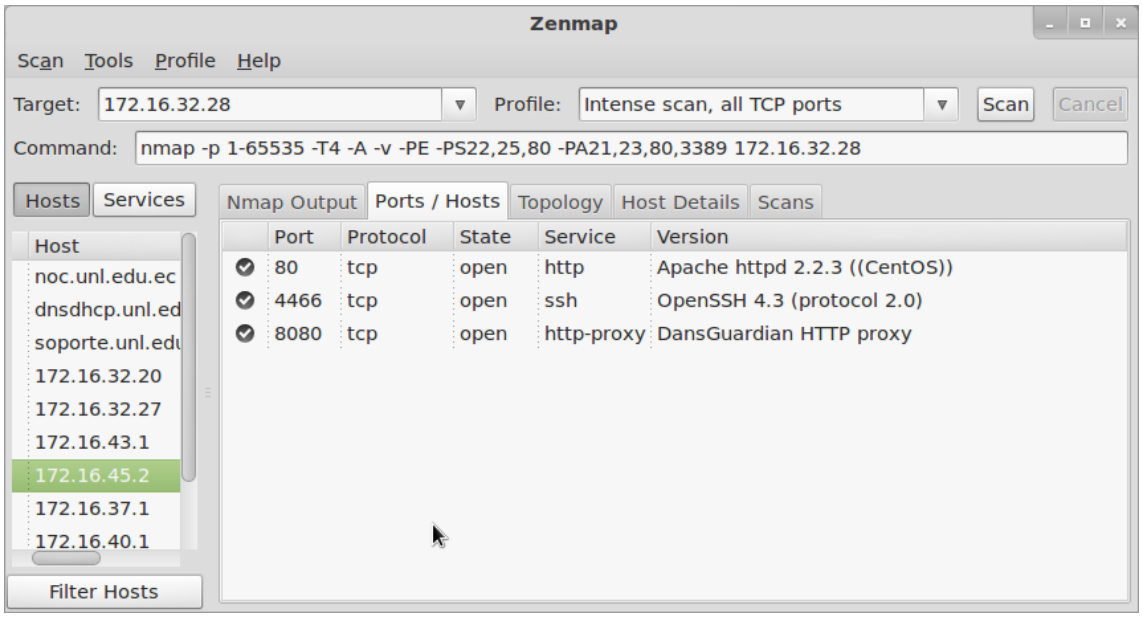


Figura 14. Capturas de ZENMAP servidor Proxy Salud

4.2.4.5 Proxy Jurídica

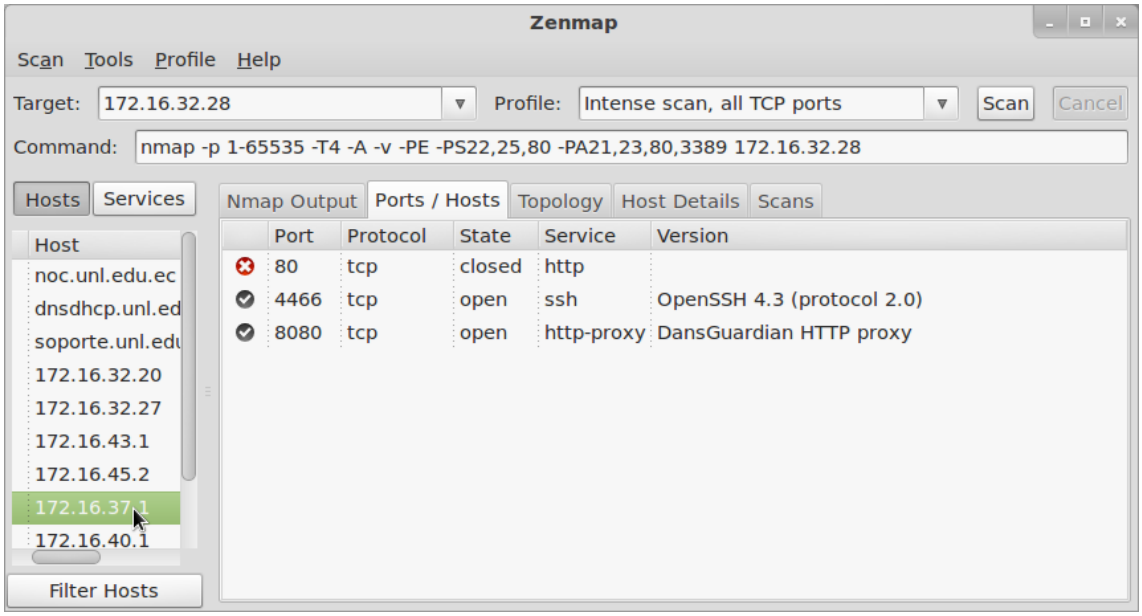


Figura 15. Capturas de ZENMAP servidor Proxy Jurídica

4.2.4.6 Proxy Agropecuaria

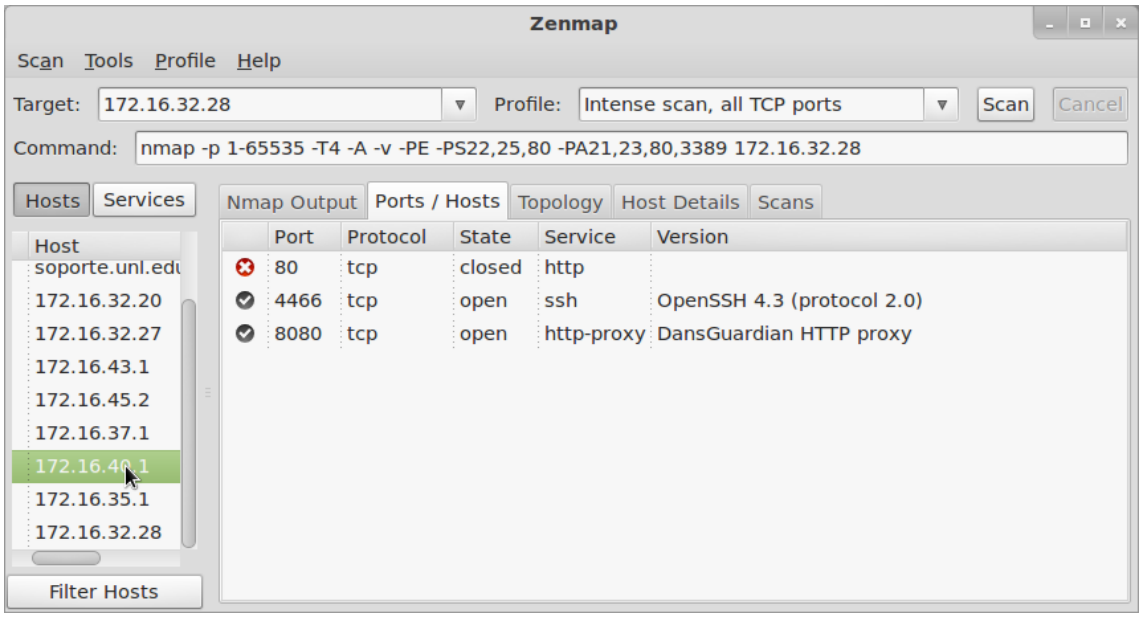


Figura 16. Capturas de ZENMAP servidor Proxy Agropecuaria

4.2.4.7 Proxy Educativa

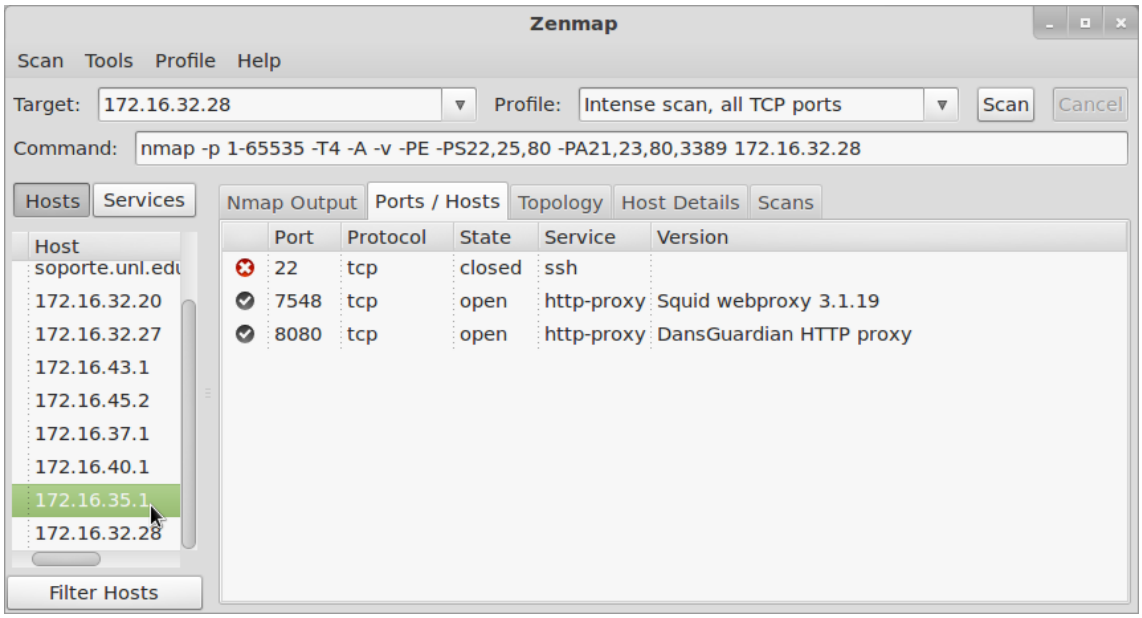


Figura 17. Capturas de ZENMAP servidor Proxy Educativa

4.2.4.8 Proxy Wireless

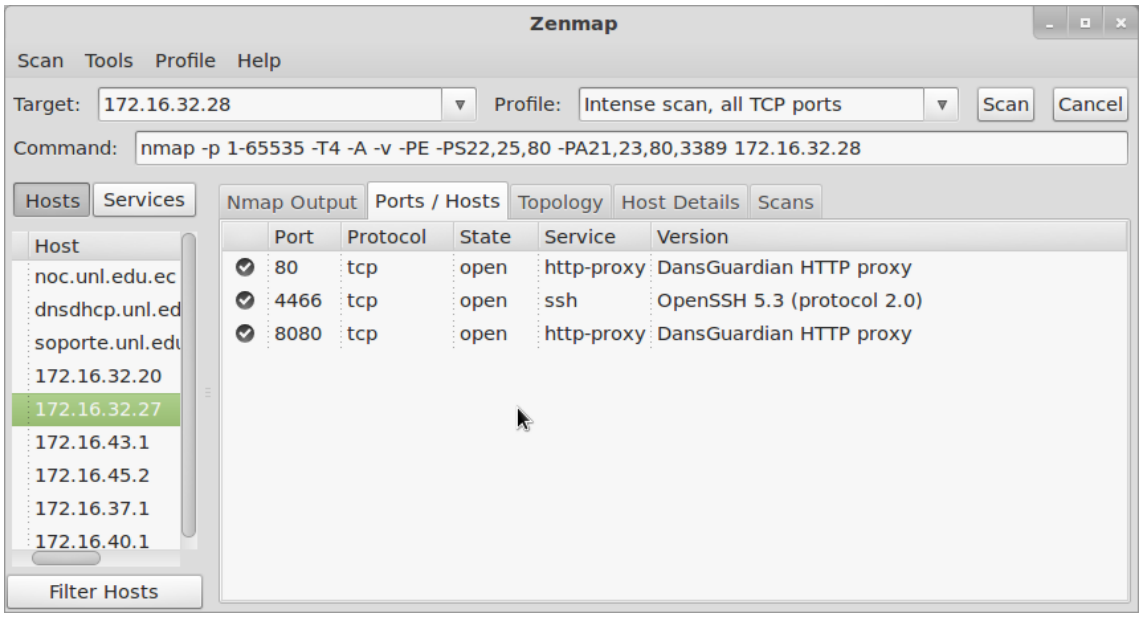


Figura 18. Capturas de ZENMAP servidor Proxy Wireless

4.2.4.9 NOC

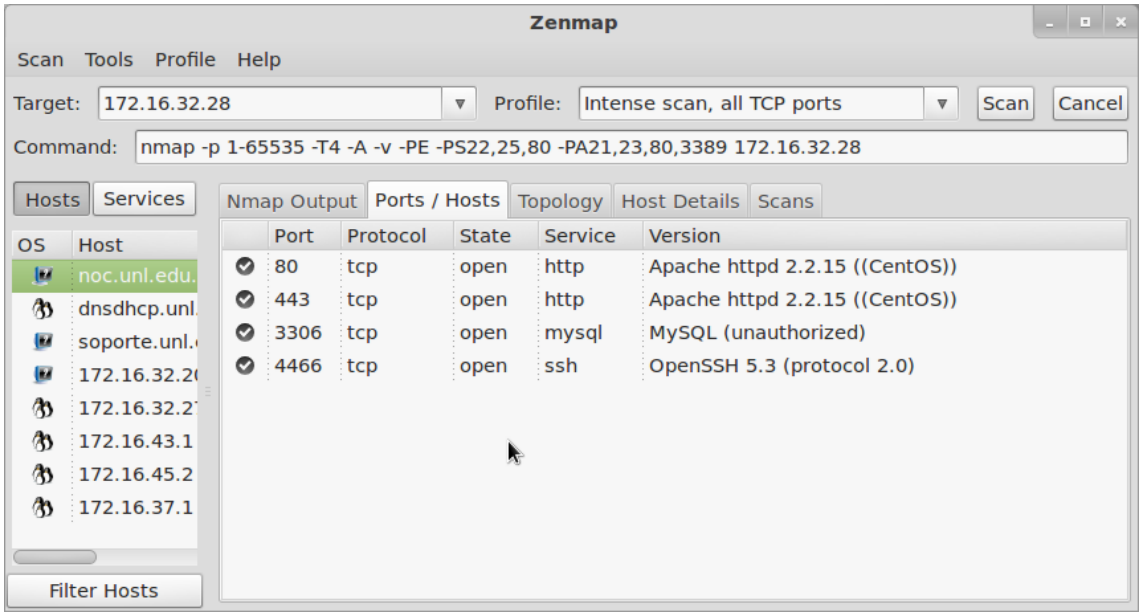


Figura 19. Capturas de ZENMAP servidor NOC

4.2.4.10 EVA

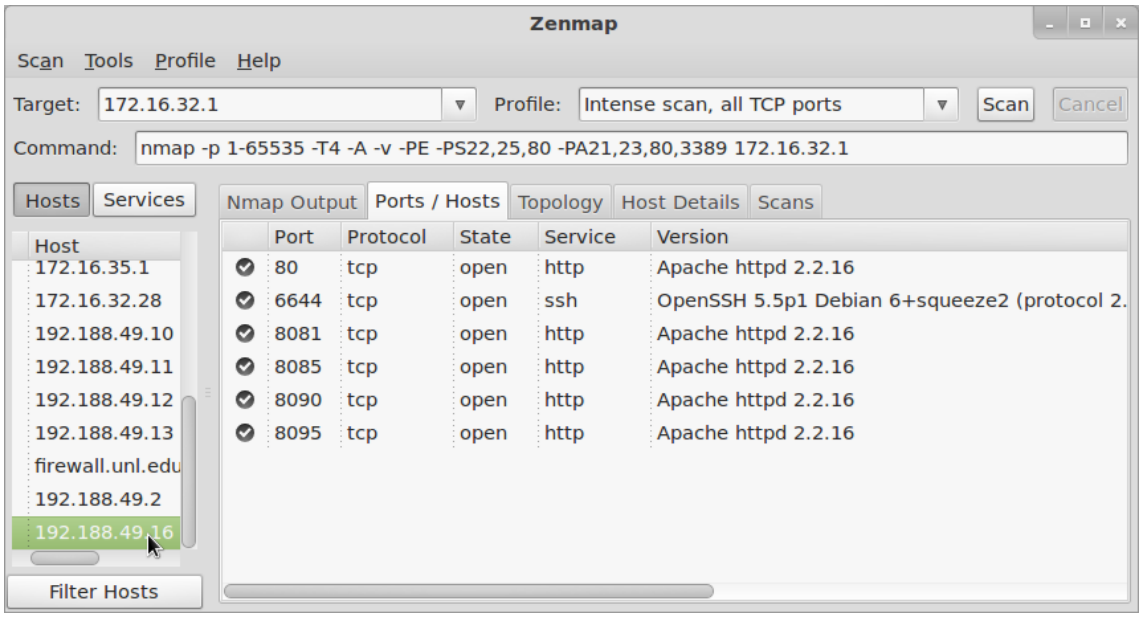


Figura 20. Capturas de ZENMAP servidor EVA

4.2.4.11 Firewall

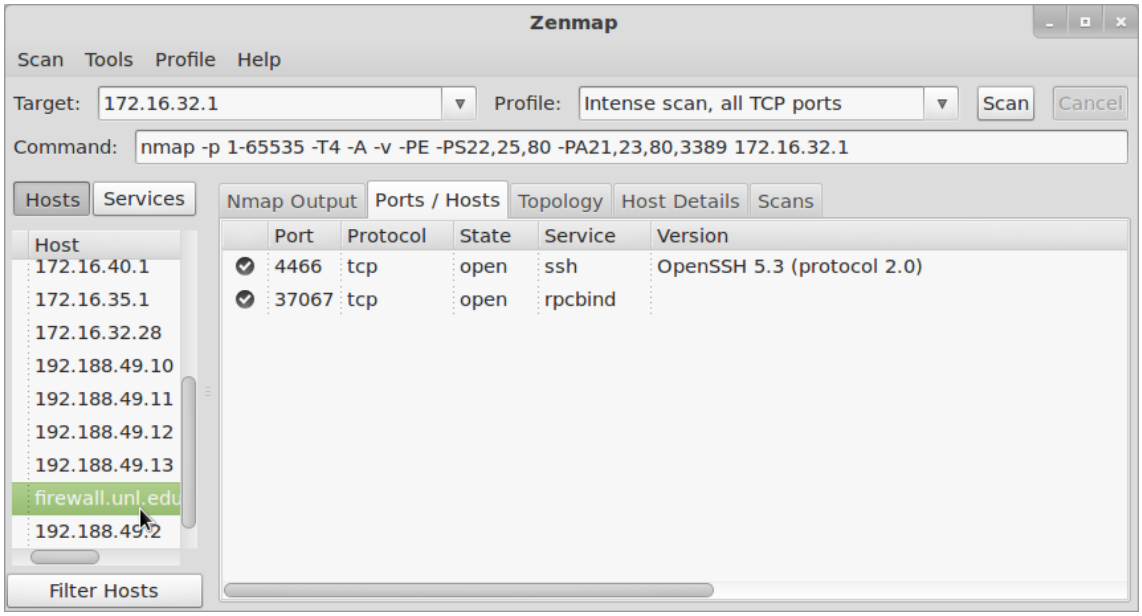


Figura 21. Capturas de ZENMAP servidor Firewall eth0

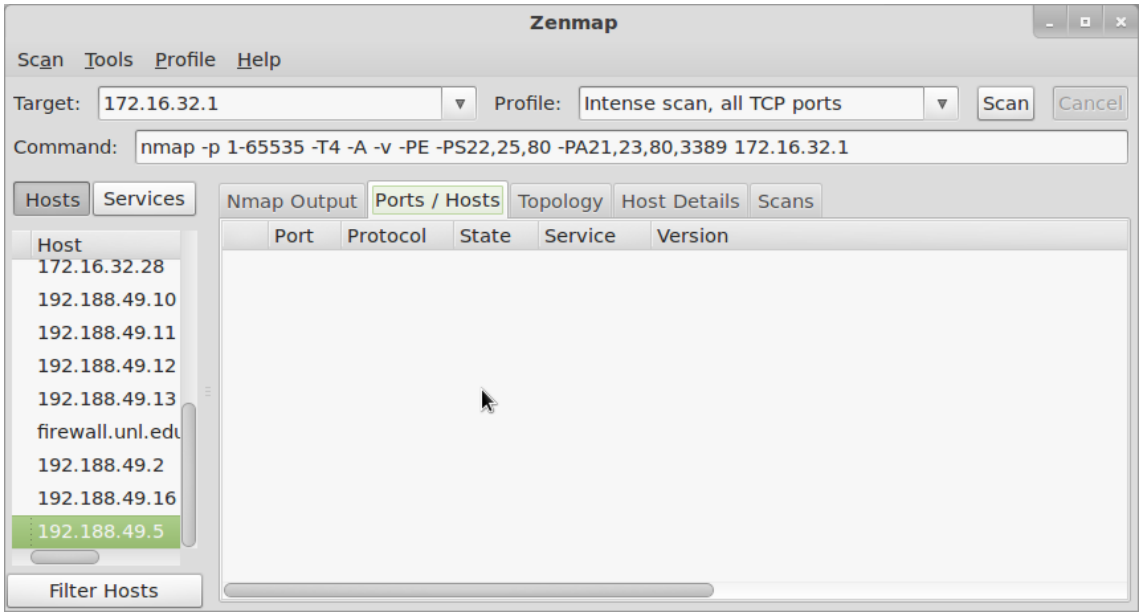


Figura 22. Capturas de ZENMAP servidor Firewall eth1

4.2.4.12 Cursos

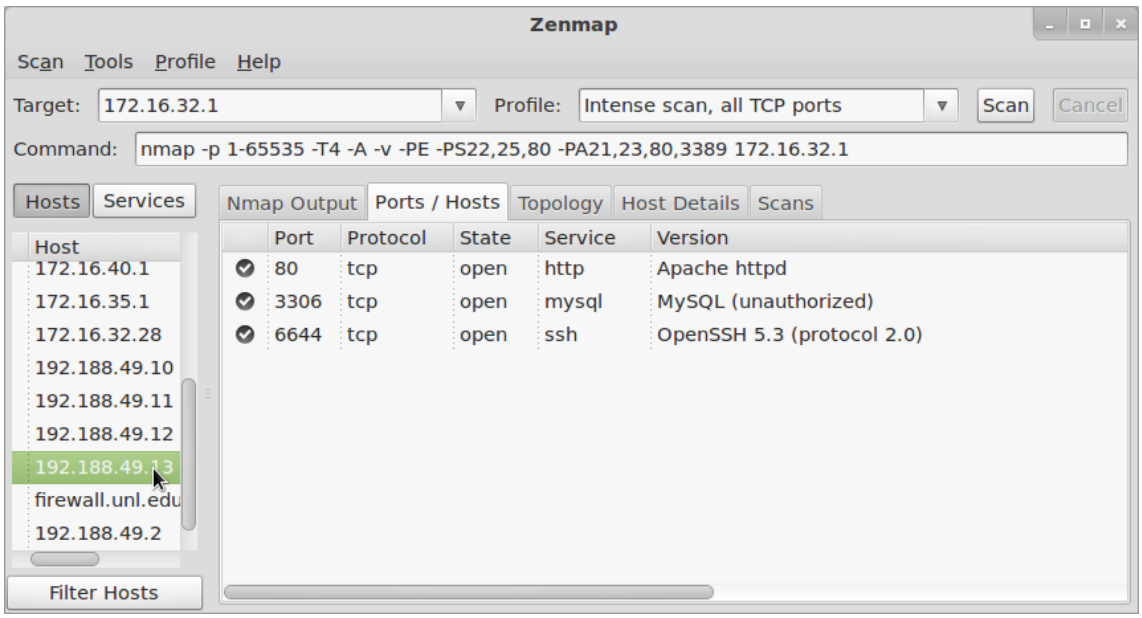


Figura 23. Capturas de ZENMAP servidor Cursos

4.2.4.13 Web Energía

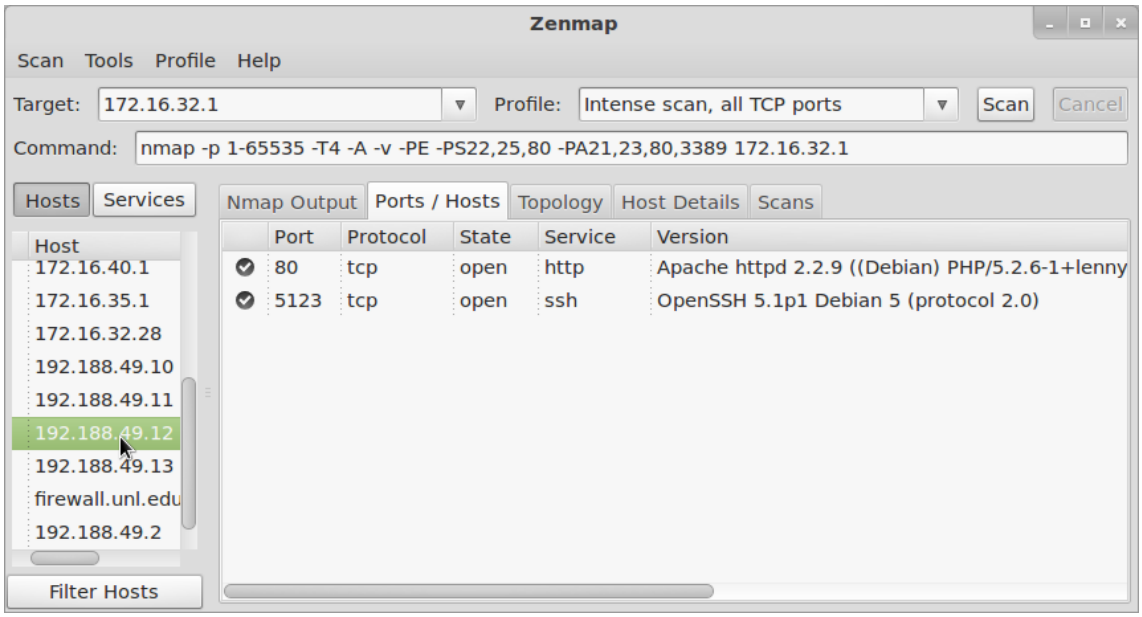


Figura 24. Capturas de ZENMAP servidor Web Energía

4.2.4.14 Radius

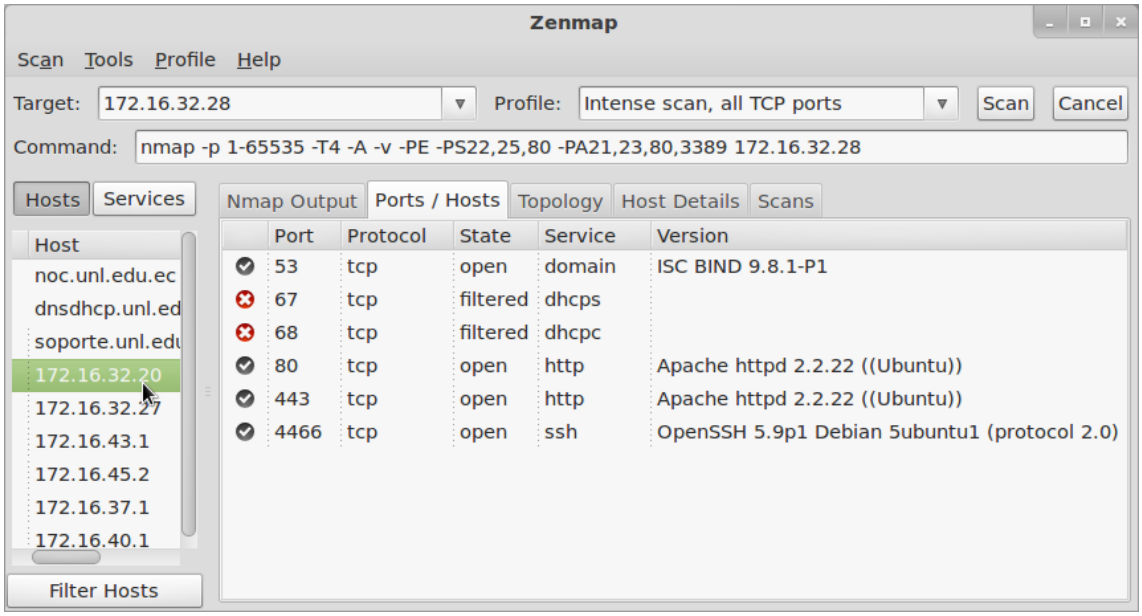


Figura 25. Capturas de ZENMAP servidor Radius

4.2.4.15 Med Virtual

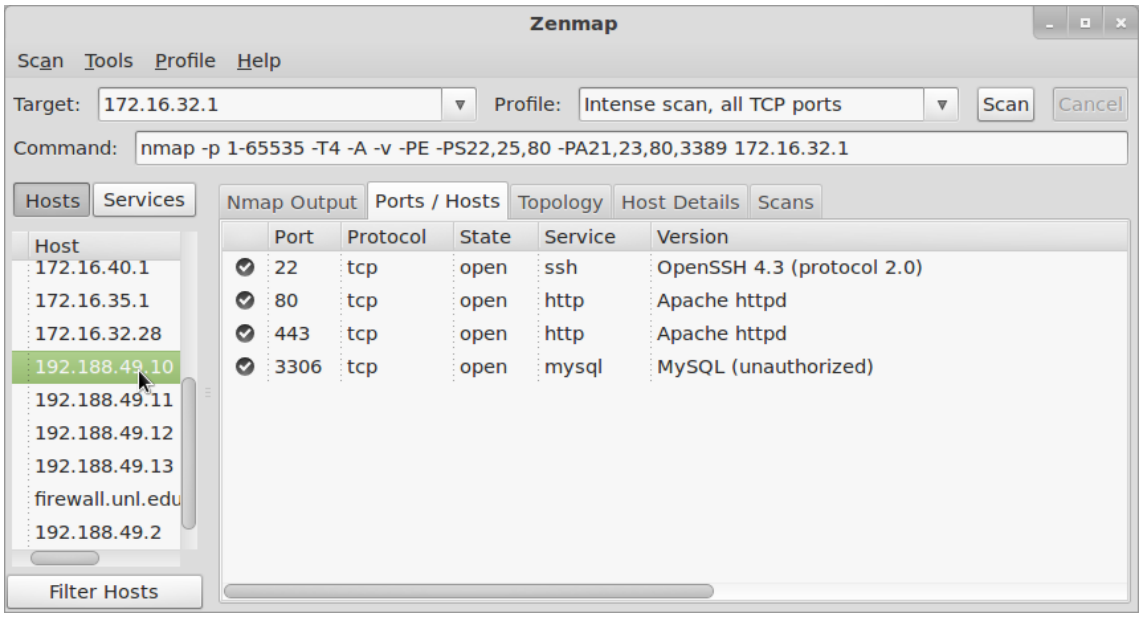


Figura 26. Capturas de ZENMAP servidor Med Virtual

4.2.4.16 Med Cursos

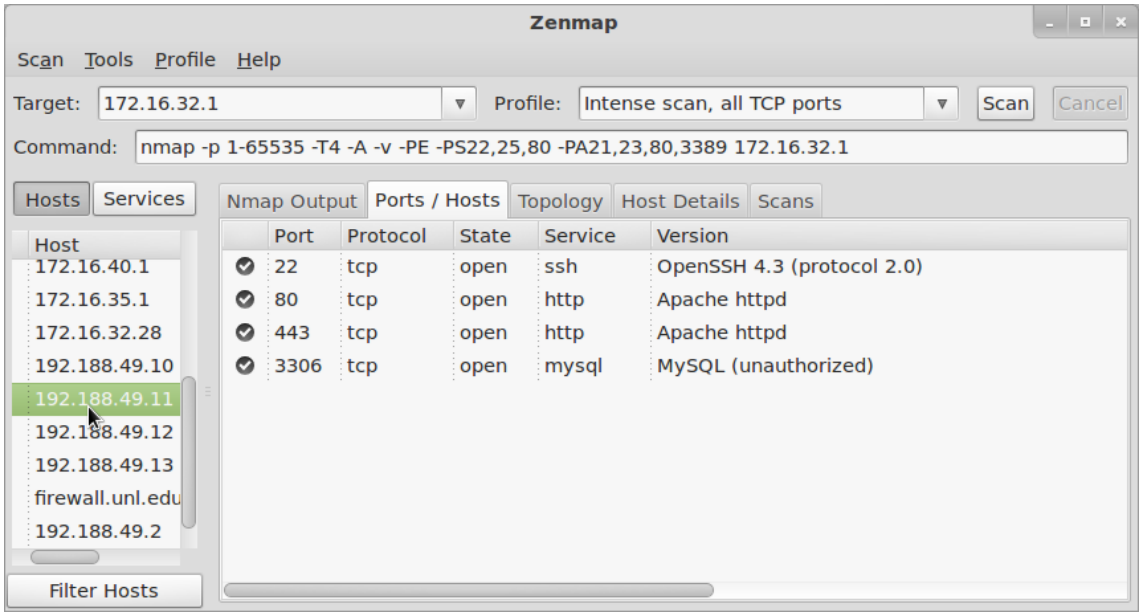


Figura 27. Capturas de ZENMAP servidor Firewall Med Cursos

4.2.4.17 Resumen de puertos y servicios

En la Tabla X, se presenta el estado de los puertos y los respectivos servicios que corren en los mismos:

TABLA X Resumen Estado de Puertos y Servicios de los servidores

NOMBRE	PUERTOS	PROTOCOLO	ESTADO	SERVICIOS
DNS-DHCP	53 4466	tcp tcp	Abierto Abierto	dnsmaq 2.45 OpenSSH 4.3
WEB	80 6644	tcp tcp	Abierto Abierto	Apache httpd OpenSSH 4.3
PROXYS (Energía, Salud, Jurídica, Agropecuaria, Educativa, Administración Central, wireless)	80 4466 8080 22 7548	tcp tcp tcp tcp tcp	Abierto Abierto Abierto Cerrado Abierto	Apache httpd 2.2.3 OpenSSH 4.3 DansGuardian HTTP proxy ssh DansGuardian HTTP proxy
SGA	4466 37067	tcp tcp	Abierto Abierto	OpenSSH 5.3 Rpcbind
NOC	80 443 3306 4466	tcp tcp tcp tcp	Abierto Abierto Abierto Abierto	Apache httpd 2.2.16 Apache httpd 2.2.16 MYSQL OpenSSH 5.3
EVA	80 6644 8081 8085	tcp tcp tcp tcp	Abierto Abierto Abierto Abierto	Apache httpd 2.2.16 OpenSSH 5.5 p1 Apache httpd 2.2.16 Apache httpd

	8090 8095	tcp tcp	Abierto Abierto	2.2.16 Apache httpd 2.2.16 Apache httpd 2.2.16
FIREWALL	4466 37067	tcp tcp	Abierto Abierto	OpenSSH 5.3 rpcbind
CURSOS	80 3306 6644	tcp tcp tcp	Abierto Abierto Abierto	Apache httpd MYSQL OpenSSH 5.3
WEB ENERGÍA	80 5123	tcp tcp	Abierto Abierto	Apache httpd 2.2.9 + PHP 5.2.6-1+lenny Open SSH 5.1p1
RADIUS	53 67 68 80 43 4466	tcp tcp tcp tcp tcp tcp	Abierto Filtrado Filtrado Abierto Abierto Abierto	ISC BIND 9.8.1 dhcps dhcpc Apache httpd 2.2.22 Apache httpd 2.2.22 OpenSSH 5.9
MED VIRTUAL	22 80 443 3306	tcp tcp tcp tcp	Abierto Abierto Abierto Abierto	OpenSSH 4.3 Apache httpd Apache httpd MYSQL
MED CURSOS	22 80 443 3306	tcp tcp tcp tcp	Abierto Abierto Abierto Abierto	OpenSSH 4.3 Apache httpd Apache httpd MYSQL

1.2.2. IDENTIFICACIÓN DE SISTEMAS OPERATIVOS EN LOS SERVIDORES

Los servidores de la UTI cuentan con los siguientes sistemas operativos, **Ver** Tabla XI:

TABLA XI Software de los Servidores

Nombre	Sistema operativo
DNS-DHCP	Centos v. 5.4
WEB	Centos v. 5.4
PROXYS (Energía, Salud, Jurídica, Agropecuaria, Wireless)	Centos v. 5.4
PROXY EDUCATIVA	Centos v.6
SGA	Debian v. 5.0 Debian v. 5.4
OSTICKET	Ubuntu v. 12.04
NOC	Centosv.6.2
EVA	Debianv.4.3.5
FIREWALL	Centosv.5.5
CURSOS	Centosv.6.2
WEB ENERGÍA	Debianv.5
RADIUS	Ubuntu 12.04

1.2.3. ENUMERACIÓN Y DESCRIPCIÓN DE LOS SERVIDORES

La Figura 28 representa la ubicación y la importancia de los servidores públicos y privados en la red de la Universidad Nacional de Loja:

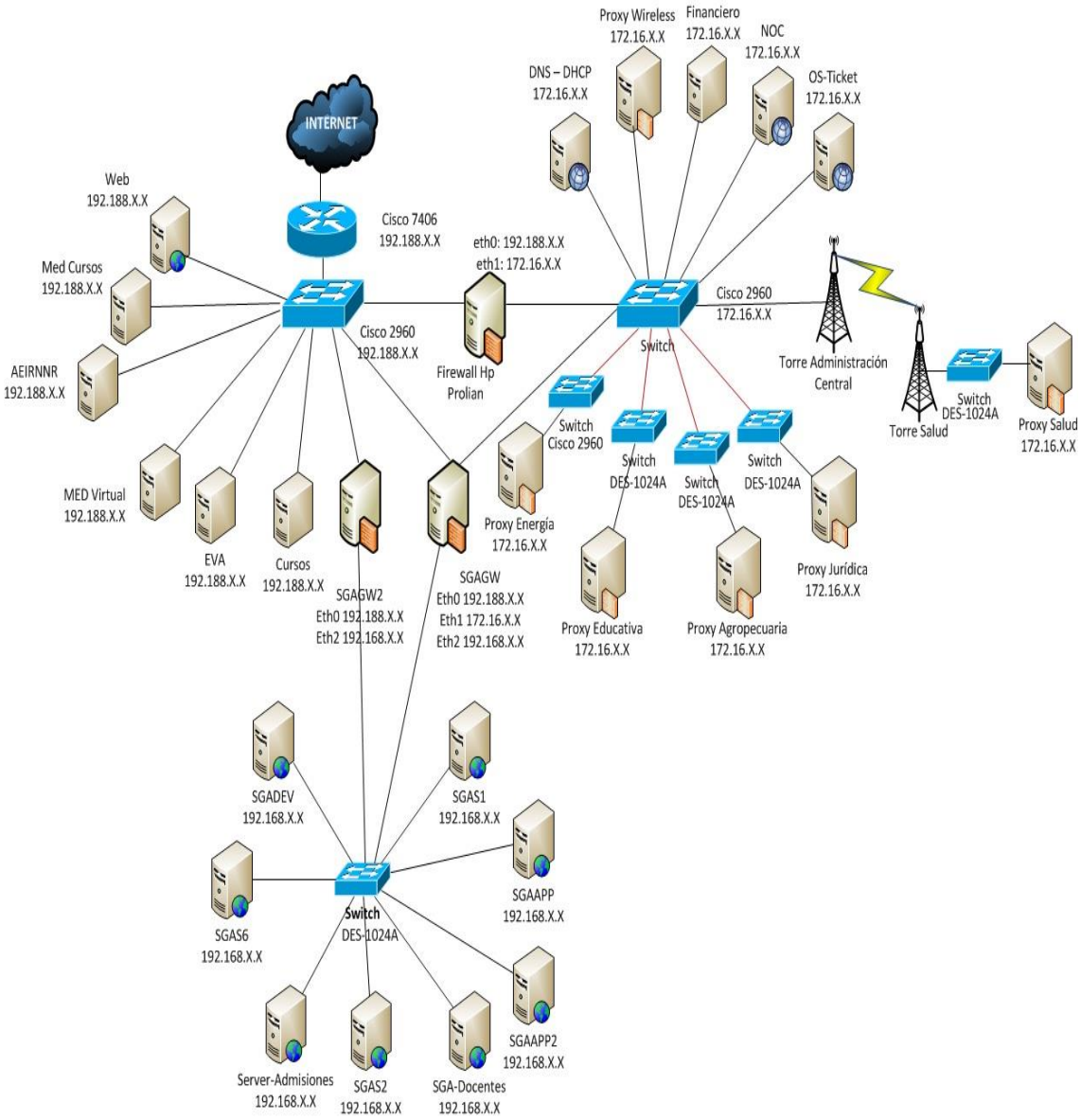


Figura 28. Topología Servidores de la UNL

Simbología

TABLA XII Simbología de la Topología de la Sala de Servidores

DESCRIPCIÓN	SÍMBOLO
Servidor	
Servidor Web mail	

Servidor Web	
Servidor Administración de contenidos	
Servidor Firewall	
Servidor Proxy	
Internet	
Router	
Switch	
Torre de Transmisión	

Al realizar un estudio de la topología de los servidores públicos y privados, **Ver** Figura 28, se ha podido identificar múltiples vulnerabilidades como: La Universidad posee un solo dominio de broadcast, lo que hace que se altere el rendimiento de la red de datos debido a que el paquete debe ser procesado por todos los dispositivos que integren el dominio de broadcast.

Existe un firewall, uno que divide la red pública de la red privada y los servidores públicos están desprotegidos contra posibles ataques. Además la existencia de este firewall permite disminuir el tráfico de la red, cabe recalcar que es administrado por el Departamento de Redes y Equipos Informáticos.

Las áreas carecen de switchs administrables que controlen y monitoreen el tráfico al interior de las áreas.

No existe una DMZ[17] que permita a los equipos (Hosts), prestar algunos servicios a la red externa, como por ejemplo, servicios de correo electrónico y funcionar como un filtro protector para la red interna, protegiéndola de intrusiones maliciosas que puedan comprometer su seguridad. Las DMZ son utilizadas por lo general, para ubicar los equipos que se usarán como servidores, los cuales deben ser accedidos por conexiones externas.

A continuación se da a conocer las funciones de cada uno de los servidores que componen la red de la universidad:

PÚBLICOS

Servidor Web: Permite compartir digitalmente con funcionarios, docentes y estudiantes webs dinámicas, blogs, cursos etc.

Servidor Cursos: Almacena y comparte cursos e información importante de eventos organizados por la Universidad.

Servidores Med Virtual: Estos servidores almacenan la plataforma virtual y los diferentes cursos que se imparten en la Modalidad de Estudios a Distancia (Med).

Servidor Energía: Es un servidor web que permite compartir con los alumnos, docentes y funcionarios del área de la energía información importante como cursos, noticias etc.

Servidor EVA: Contiene el entorno virtual de aprendizaje de la Universidad Nacional de Loja.

[17] **DMZ:** Zona Desmilitarizada

PRIVADOS

Servidor DNS: Permite la resolución directa o inversa de las direcciones de Internet, se encuentra configurado como DNS primario haciendo uso del dominio unl.edu.ec facilitando de esta forma la resolución de nombres a los equipos finales en el campus universitario.

Servidores del Sistema De Gestión Académica (SGA): El SGA cuenta con una granja de servidores que permiten automatizar procesos académicos y brindar servicio a estudiantes y docentes de la UNL.

Servidor DHCP: Permite a los clientes (pcs, impresoras, entre otros) de una red, obtener de forma automática sus parámetros de configuración como son: IP, mascara de subred, puerta de enlace, DNS y dominio.

Servidores Proxy: Es un equipo intermedio que facilita el acceso a los servicios de intranet, servicios públicos e internet a todos los equipos finales de la institución que no cuentan con una conexión directa a internet. En los servidores de este tipo se manejan ciertas políticas de seguridad como es el control de contenido, cada una de las áreas cuenta con un servidor proxy.

Firewall: Controla todas las comunicaciones que pasa de la red externa a la interna y viceversa en función de las reglas establecidas permite o deniega su paso.

Servidor NOC[18]: Este servidor realiza la tarea de monitorizar el rendimiento resto de servidores y elementos de networking de la Universidad Nacional de Loja.

Servidor OsTicket[19]: Sistema que permite almacenar solicitudes de los usuarios y gestionarlos tareas mediante tickets y sirve como medio de soporte para la Unidad de Telecomunicaciones e información.

Servidor Radius[20]: Ayuda a la autenticación de los usuarios de red en el campus universitario.

4.2.4.18 Direccionamiento Ip Servidores Privados

La red interna de datos maneja los siguientes parámetros IPv4, **Ver** Tabla XIII:

[18] **NOC:** Network Operation Center
[19] **OSticket:** Open Source Support Ticket System
[20] **Radius:** Remote Authentication Dial In User Service

TABLA XIII Parámetros Ipv4 de la Red Interna de Datos

DESCRIPCIÓN	ESPECIFICACIÓN
Red clase B	172.16.0.0/19
Dominio	unl.edu.ec
Subred	172.16.32.0
Mascara de subred	255.255.255
Dirección de Brodcast	172.16.63.255
Puerta de enlace	172.16.32.1
DNS	172.16.32.2

Todos los servidores privados están configurados bajo estos parámetros de red.

4.2.4.19 Direccionamiento Ip Servidores Públicos

Para los servidores públicos se utiliza una red tipo C a continuación una pequeña descripción de sus parámetros, **Ver** Tabla XIV:

TABLA XIV Parámetros Ipv4 de la Red Externa de Datos

DESCRIPCIÓN	ESPECIFICACIÓN
Red clase C	192.188.49.0/24
Dominio	unl.edu.ec
Mascara de subred	255.255.255.0
Dirección de Brodcast	192.188.49.255
Puerta de enlace	192.188.49.4
DNS Primario	200.93.221.17
DNS Secundario	200.93.192.148

Fase II

Análisis de Vulnerabilidades

2. ÁNALISIS DE VULNERABILIDADES

La fase 2 denominada Análisis de Vulnerabilidades la comprende los siguientes objetivos:

Objetivo 1: Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Objetivo 2: Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores.

Objetivo 3: Realizar pruebas a los servidores para determinar las vulnerabilidades en los diferentes servicios que brindan.

Objetivo 1:

DETERMINAR LAS SEGURIDADES FÍSICAS Y EL EQUIPAMIENTO NECESARIO PARA LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA

2.1. DETERMINAR LAS SEGURIDADES FÍSICAS Y EL EQUIPAMIENTO NECESARIO PARA LOS SERVIDORES DE LA U.T.I.DE LA U.N.L.

2.1.1. ÁNALISIS DE VULNERABILIDADES FÍSICAS ENCONTRADAS

Accesos no controlados: La Sala de Servidores necesita proteger físicamente sus servidores para evitar robos, daños y alteraciones a los equipos, por parte de personal no capacitado o personas ajenas a la institución.

La Sala de Servidores de la UNL, posee una puerta hecha de aluminio y vidrio, **Ver** Figura 29, la que permanece cerrada bajo llave, pero existen lapsos de tiempo que por verificación o implementación de servicios, se tiende a dejar la Sala de Servidores sin llave lo que es muy riesgoso o con la llave en la puerta de acceso para facilitar a los técnicos que realizan trabajos el ingreso rápido.

Figura 29. Puerta de la Sala de Servidores

La Figura 30 muestra el registro de entrada y salida que se utiliza para controlar el acceso a la Sala de Servidores, este consta de fecha, hora, funcionario, asunto y firma. Este tipo de control de acceso es muy poco fiable porque es fácil de evadir.

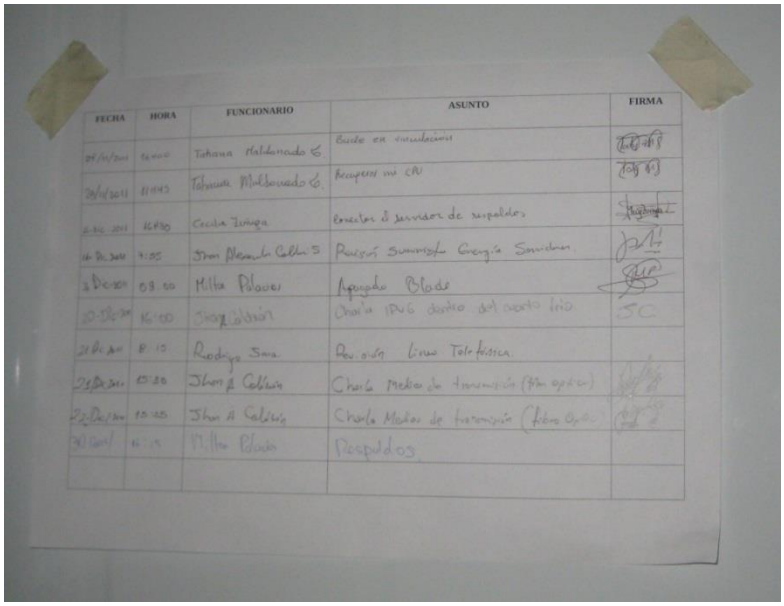


Figura 30. Control de acceso a la Sala de Servidores

Filtraciones de Líquidos: Debido a que la Sala de Servidores de la Universidad Nacional de Loja está ubicado en el cuarto piso de Administración Central, Bloque 2, cuando se producen lluvias existen filtraciones de agua a través de pequeñas fisuras existentes en la losa, **Ver** Figura 31, que pueden producir daños irreversibles en los equipos, cableado y demás dispositivos.

Figura 31. Filtraciones de Líquidos en la Sala de Servidores

Incendios: La Sala de Servidores corre un grave riesgo al no contar con un sistema contra incendios, ya que se almacena muchos equipos, cables de datos y de energía. El riesgo eminente de un cortocircuito provocaría un incendio y sin los medios

necesarios para detectar y controlar el fuego, sería desastroso para todos los equipos que allí se almacenan y para el personal que labora.

Hasta la actualidad no se ha suscitado ningún flagelo en la Sala de Servidores pero el riesgo de ocurrencia es muy alto.

Las causas por las que se puede producir un incendio son:

- Inflamación del aislante del cableado por aumento del calor.
- Negligencia provocada por fumadores o trabajos con fuegos abiertos incontrolados, como puede ser la soldadura.
- Defectos de los componentes eléctricos del equipo, especialmente fuentes de alimentación.
- Cortocircuitos.
- Incendios exteriores a las instalaciones

Consumo Eléctrico: El Proveedor de energía eléctrica es la Empresa Eléctrica Regional del Sur S.A. a través de 2 fases cada una de 110V más un neutro, **Ver** Figura 32, cabe recalcar que la potencia consumida es alrededor de 3146W.

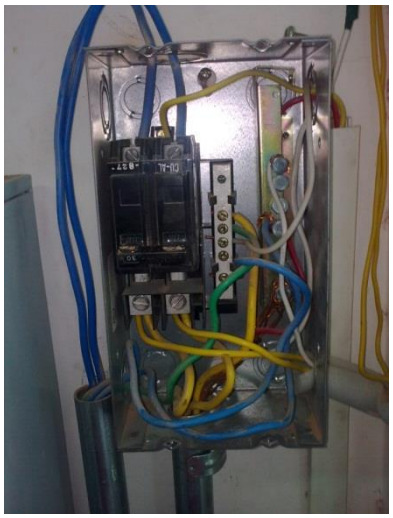


Figura 32. Break del Centro de Cómputo

Se procedió a medir el amperaje de cada una de las fases, llegándose a determinar que la Intensidad de corriente eléctrica en la fase 1 es de 23.1A y en la fase 2 de 5.6A, **Ver** Figura 33 y 34, al realizar la transformación respectiva tenemos que el consumo en la fase 1 es de 2541W y la fase 2 es de 616, evidenciando que la fase 1 está sobrecargada.

Figura 33. Medición Fase 1 **Figura 34. Medición Fase 2**

Cortes de Luz: Los cortes de luz se dan forma inesperada debido a factores externos a la Sala de Servidores como daños en la red eléctrica, caídas de rayos, animales, arboles, accidentes vehiculares etc, internamente los cortes de luz en la Sala de Servidores han producido daños en el disco, fuentes de alimentación, memoria RAM llegando incluso a afectar a la tarjeta Madre y procesador ya que todos los servidores no cuentan con UPS dedicados que nos permitan realizar un apagado correcto de los equipos, **Ver** Figura 35, muchos equipos al apagarse de manera imprevista han sufrido perdida de información y caída de los servicios que están corriendo en los servidores**.**

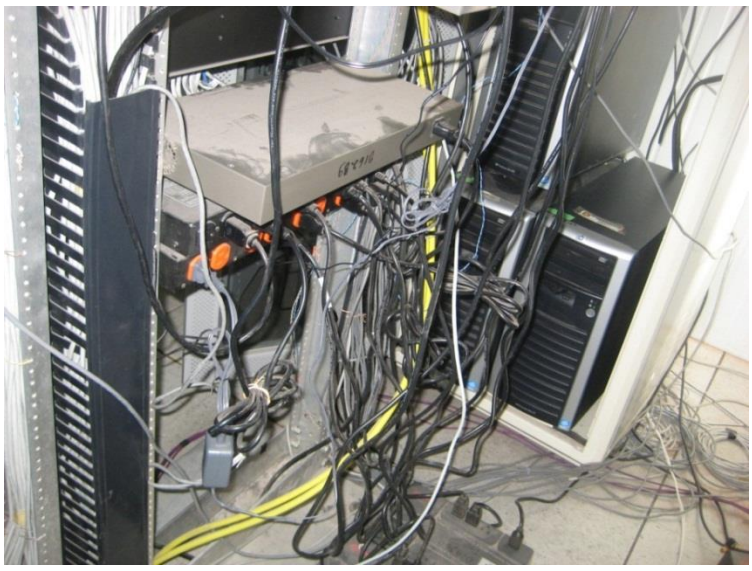


Figura 35. Supresor de Picos en la Sala de Servidores

Variaciones de Voltaje: Al igual que los cortes de luz las variaciones de voltaje afectan a los servidores que no cuentan con UPS, ya que estos dispositivos reducen el impacto de las variaciones de voltaje en los equipos, estas variaciones pueden llegar a quemar las fuentes de poder haciendo que este dispositivo deje de funcionar correctamente.

Hardware: La mayoría de equipos que conforman la Sala de Servidores no tienen características de servidor, lo que hace que el hardware se deteriore rápidamente debido a factores como polvo, humedad, recalentamiento lo que produce un deterioro en el hardware y ocasiona un bajo rendimiento en los equipos y los servicios que se alojan en estos.

Ubicación: Todos los servidores están distribuidos en perchas y algunos en el piso, **Ver** Figura 36, lo que evidencia la mala distribución física de los equipos en la Sala de Servidores de la UTI y dificulta el enfriamiento y el acceso a los servidores.

Figura 36. Perchas de Servidores de la UTI

Temperatura de Operación: En la Sala de Servidores están ubicados 2 aires acondicionados configurados a una temperatura de 20 ºC, **Ver** Figura 37 y 38, los mismos que están ubicados en la parte superior dificultando el enfriamiento de los equipos ubicados en la parte inferior de las perchas, cabe recalcar que este tipo de enfriamiento no es el óptimo para una Sala de Servidores. Además este tipo de Aires Acondicionados son adecuados para hogares y oficinas.

Figura 37. Aire Acondicionado1 de la Sala de Servidores

Figura 38. Aire Acondicionado 2 de la Sala de Servidores

Respaldo de los datos: La Sala de Servidores cuenta con un servidor de respaldos que utiliza Centosv.5.8 y ejecuta un script automáticamente para respaldar los datos de los servidores, está ubicado físicamente en el área de servidores.

2.1.2. SOLUCIONES EN LA PARTE DE SEGURIDADES FÍSICAS

2.1.2.1. Segmentador de Ancho de Banda

La Universidad Nacional de Loja cuenta con un ancho de banda de 100Mbps de los cuales no supera un consumo máximo de 58.77M diariamente y 45.76M semanal, **Ver** Figura 39, el consumo mensual es de 36.23M y anual de 16.52M, **Ver** Figura 40.

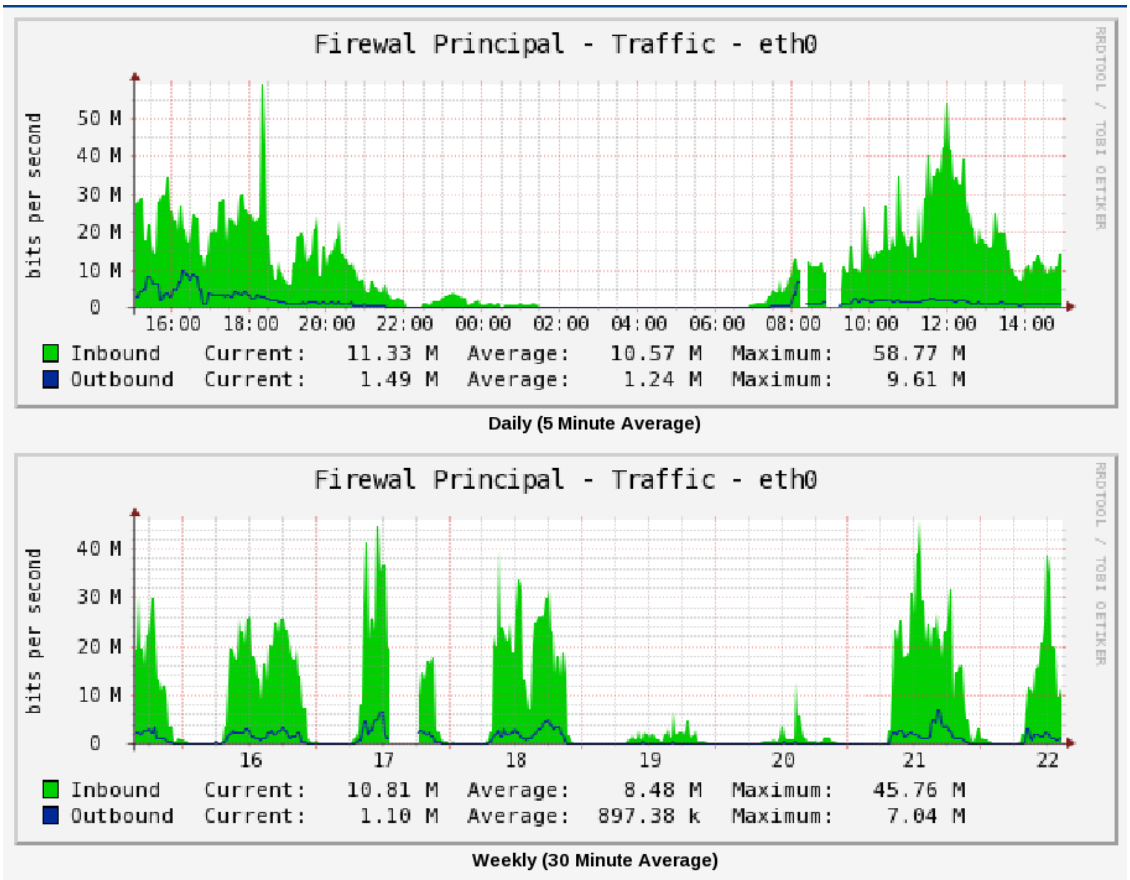


Figura 39. Reportes de consumo de ancho de Banda diario y semanal

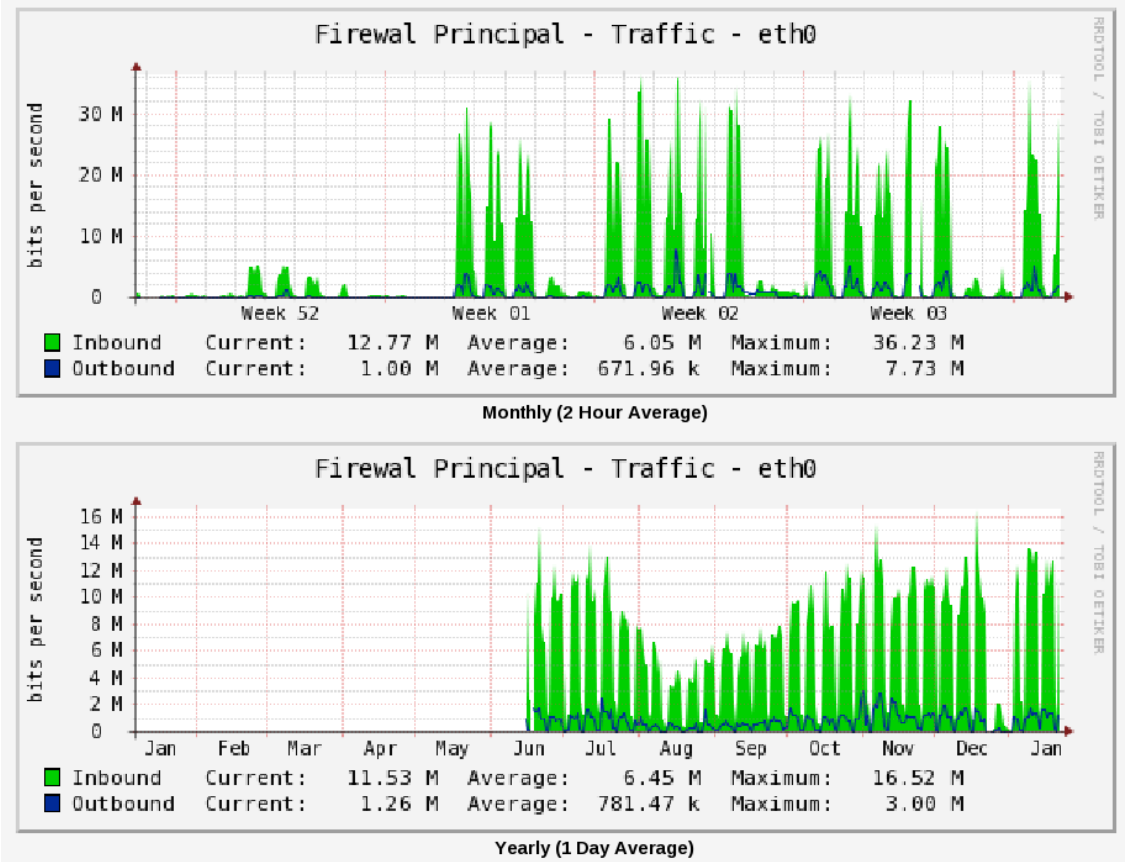


Figura 40. Reporte de consumo de ancho de Banda mensual y anual

Todas estas estadísticas de consumo son bajo el control de contenidos que usa la Unidad de Telecomunicaciones e Información, mediante el uso de servidores proxys implementados con Dansguardian para evitar que se disparen los niveles de consumo de ancho de banda en páginas que no sean académicas.

Para optimizar el uso del ancho de banda que actualmente está desperdiciado en casi la mitad y para eliminar el control de contenidos sin que se dispare el consumo de ancho de banda es necesario contar con un segmentador de ancho de banda que de igual manera nos ayudará a resolver el problema de congestión en la red generado por el único dominio de broadcast que maneja la Universidad. En la Tabla XV se describe las principales tecnologías en segmentadores:

TABLA XV Comparación Segmentadores de ancho de Banda

CARACTERÍSTICAS	7500	10000	10000 ISP***
Marca:	Blue Coat	Blue Coat	Blue Coat
Modelo	PacketShaper 7500	PacketShaper 10000	PacketShaper 10000 ISP
Alimentación	100/240 VAC	100/240 VAC	100/240 VAC
Unidades en bastidor	2Ur	2Ur	2Ur
Dimensiones	Alto: 8.89 cm Ancho: 40.64 cm Largo: 44.07 cm	Alto: 8.89 cm Ancho: 43.97 cm Largo: 51.43 cm	Alto: 8.89 cm Ancho: 43.97 cm Largo: 51.43 cm
Peso	9.29 kg	14.97 kg	n/a
Flujos IP (TCP/IP Otros)	200,000/100,000	300,000/150,000	900,000/360,000
particiones dinámicas	10,000	20,000	20,000
particiones estáticas	512	1,024	5,000
Nº máximo de Reglas	5,120	5,000	12,500
IP Hosts	150,000	200,000	400,000
Monitoreo	Si	Si	Si
Velocidad	10 Mbps 45 Mbps 100 Mbps 200 Mbps	100 Mbps 200 Mbps 310 Mbps 1 Gbps	100 Mbps 200 Mbps 310 Mbps 1 Gbps
Compresión	45 Mbps	155 Mbps	N/A
interfaz de red (entrada y salida)	Copper: 10/100/1000 Mbps	Copper: 10/100/1000 Mbps Fiber: 1000 Mbps	Copper: 10/100/1000 Mbps Fiber: 1000 Mbps
Temperatura	0°C a 40°C	0°C a 40°C	0°C a 40°C
Precio	$ 1,235.56	1,831.50	$ 2,509.23

Para esto se sugiere adquirir el Equipo Gestionador de Ancho de Banda Bluecoat, **Ver** Figura 41, que permitirá administrar el ancho de banda en las diferentes áreas,

acelerar la salida de paquetes y reducir notablemente el tiempo de espera de cada host, a continuación se detalla las características necesarias para este equipo:

Figura 41. Segmentador de ancho de banda Bluecoat

El segmentador de ancho de banda Bluecot ya fue adquirido por la UTI, al igual que los UPS sugeridos, **Ver** Página 114, con el segmentador de ancho de banda se procedió asignar un determinado ancho de banda a un rango de IPs de acuerdo a cada Área, el consumo de ancho de banda se ha estabilizado evidenciándose en la Figura 42.

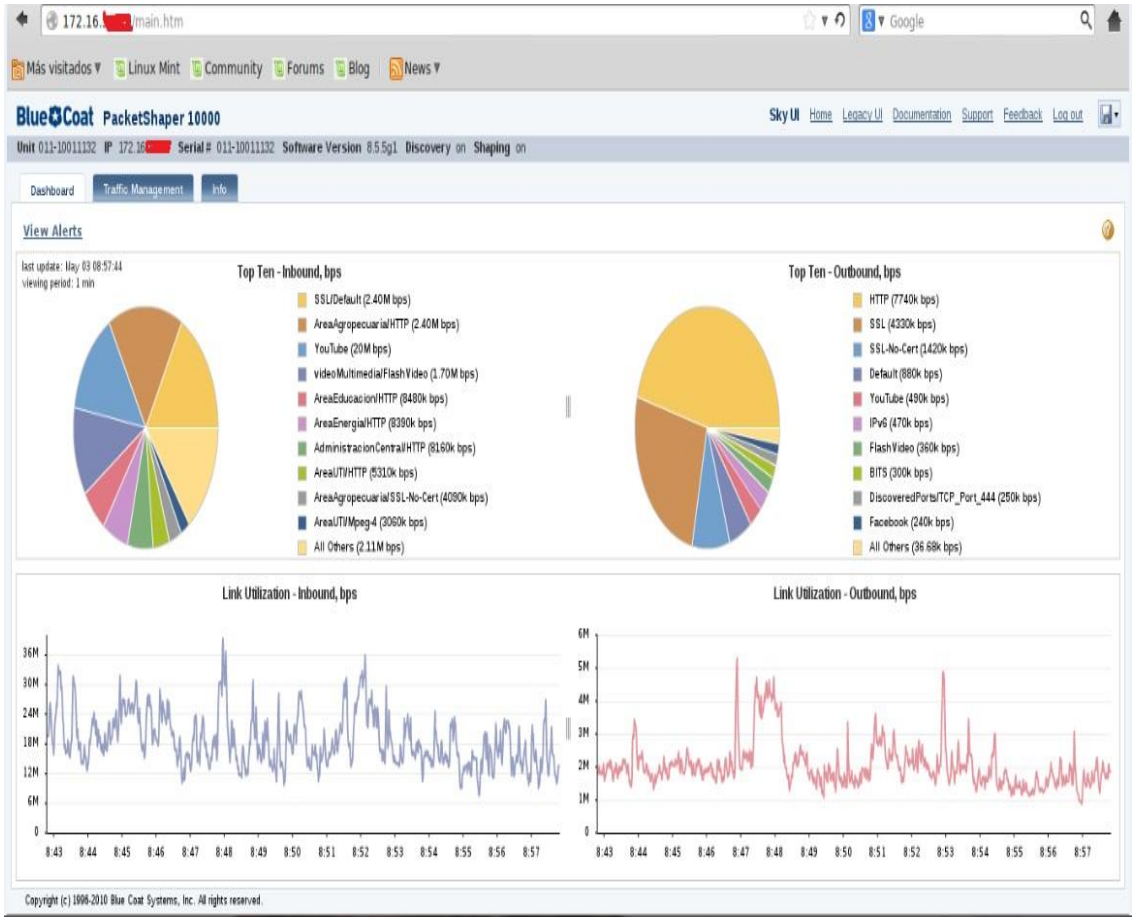


Figura 42 Consumo de ancho de banda utilizando el segmentador de ancho de Banda Bluecot

Existe un estudio realizado previo a la adquisición de este equipo sobre la segmentación del ancho de banda en la que se usa los datos proporcionados por el servidor Cacti de 4 semanas del consumo de subida y bajada de los servidores proxys, el criterio de segmentación tomado en este análisis es el procedimiento de Muestreo y Estimación por Intervalos de confianza[21].

Este método describe el comportamiento de una variable, a base de un conjunto de muestras (de preferencia muestras que abarquen el monitoreo de un periodo de tiempo de corrido sobre un sistema), este método predice comportamientos pasados o predecir comportamientos de la variable en un sistema. El resultado obtenido en el estudio fue, **Ver** Tabla XVI:

[21] Análisis del Requerimiento de un Segmentador de Ancho de Banda para la Red LAN de la Universidad Nacional de Loja e Implementación en el Área de la Energía, las Industrias y los Recursos Naturales No Renovables. Egda Evelin Alvarado. Tesis en Desarrollo. 2013

TABLA XVI Segmentación según estudio de consumo de ancho de banda

DISTRIBUCIÓN DE ANCHO DE BANDA PARA LA UNL	
ÁREA	**ANCHO DE BANDA (Mbps)**
Educativa	7
Jurídica	7
Agropecuaria	3
Salud	4
Energía	12
Med	8
Idiomas	2
Wireless	20
TOTAL	**63**

Como se puede observar el consumo de ancho de banda no supera 12 Mbps y tampoco es menor a 2 Mbps excepto el proxy Wireless en base a estos valores se procedió a establecer como valor mínimo 5 Mbps y 10 Mbps para realizar pruebas debido a que el equipo recientemente se lo está implementando, la segmentación que se realizó queda establecida provisionalmente de la siguiente manera, **Ver** la Tabla XVII:

TABLA XVII Segmentación Actual de Ancho de Banda

DESCRIPCIÓN	SEGMENTO DE RED	MÍNIMO (Mbps)	MÁXIMO (Mbps)
Servidores	172.16.x.x – 172.16.x.x	5	10
Administración Central	172.16.x.x – 172.16.x.x	5	10
Área Jurídica	172.16.x.x – 172.16.x.x	5	10
Área Educación	172.16.x.x – 172.16.x.x	5	10
Área Salud	172.16.x.x – 172.16.x.x	5	10
Área Energía	172.16.x.x – 172.16.x.x	5	10
Área	172.16.x.x – 172.16.x.x	5	10

Agropecuaria			
Área UTI	172.16.63.1 – 172.16.63.255	20	25
Área Wfi	172.16.57.1 – 172.16.60.255	5	15

2.1.2.2. Firewall

Es necesario adquirir un Firewall para gestionar de mejor forma la seguridad de la red es decir proteger las redes internas del acceso no autorizado por usuarios en una red externa, y de esta manera salvaguardar a todos los servidores de la UTI especialmente a los servidores públicos que no cuentan con un firewall y están expuestos a posibles ataques, para este fin se sugiere la adquisición de este equipo, en la Tabla XVIII se realizará la respectiva comparación:

TABLA XVIII Comparación Firewalls

CARACTERÍSTICAS	Cisco ASA 5585	3com X506	HP F1000
Marca:	Cisco	3Com	Hp
Modelo	ASA 5585-X	X506 - US1071	F1000
Alimentación	110/220V	110/220V	110/220V
Unidades en bastidor	2	2	2
Dimensiones	Alto: 8.8 cm Ancho: 48.3 cm Largo: 67.3 cm	Alto: 4.3 cm Ancho:30.5 cm Largo: 29.65cm	Alto: 4.39 cm Ancho: 40.01 cm Largo: 44.2 cm
Memoria	4096 GB	2048	2048
Memoria flash	2048	1024	1024
Procesador	Intel® Xenón® 5600 4Core 2000Mhz	Intel® Xeon® caché L2 de 256K 2Ghz	Intel® Xeon® caché L2 de 512K 2.2 Ghz
Aministración	Web, ssh	Web, ssh	Web, ssh
Interface	2 x gestión Ethernet 10BaseT/100Base	6 x 10BASE-T/100BASE-	12 dual personality ports, auto-sensing

	TX/1000Base-TRJ-45 2 x Hi-Speed USB - 4 PIN USB tipo A 1 x gestión - consola - RJ-45 1 x gestión - auxiliar - RJ-45 8 x red - Ethernet 10Base-T/100Base-TX/1000Base-TRJ45 2x 10 Gigabit	TX /MDI/MDIX 1 x serial (RJ-45)	10/100/1000BASE-T or SFP, 1 RJ-45 serial console port, 2 I/O module slots
Temperatura	0°C a 40°C	0°C a 40°C	0°C a 45°C
Seguridad	Sesiones concurrentes : 10000000 Peers VPN IPSec : 10000 Interfaces virtuales (VLAN) : 1024 Peers VPN SSL : 2 Nodos : ilimitado	IPSec, L2TP/IPSec, PPTP/MPPE	Rich VPN functions, IPSec/GRE/L2TP
Características	Protección firewall, asistencia técnica VPN, equilibrio de carga, soporte VLAN	N/D	Protección de la seguridad integral Alto rendimiento
Precio	$ 8,380.73	5,492.00	$ 7,629.56

Se eligió el Firewall Cisco ASA 5585, **Ver** Figura 43, que es una suite de seguridad empresarial avanzada.

El ASA 5585 es adecuado para las necesidades de seguridad de las organizaciones con las aplicaciones más exigentes, tales como voz, video, datos científicos, sistemas

financieros y de comercio. Este servidor de seguridad ayuda a las empresas a proteger eficazmente sus redes y aplicaciones mediante la incorporación de un sistema de prevención de intrusiones con otras aplicaciones de Cisco.

Figura 43. Cisco ASA 5585

2.1.2.3. Propuesta Alternativa de Topología de Red

En la Figura 44, se muestra la integración del Firewall Cisco ASA 5585 y el Equipo Segmentador de Ancho de Banda Bluecoat en la topología, además de la propuesta de implementación del servidor BLADE.

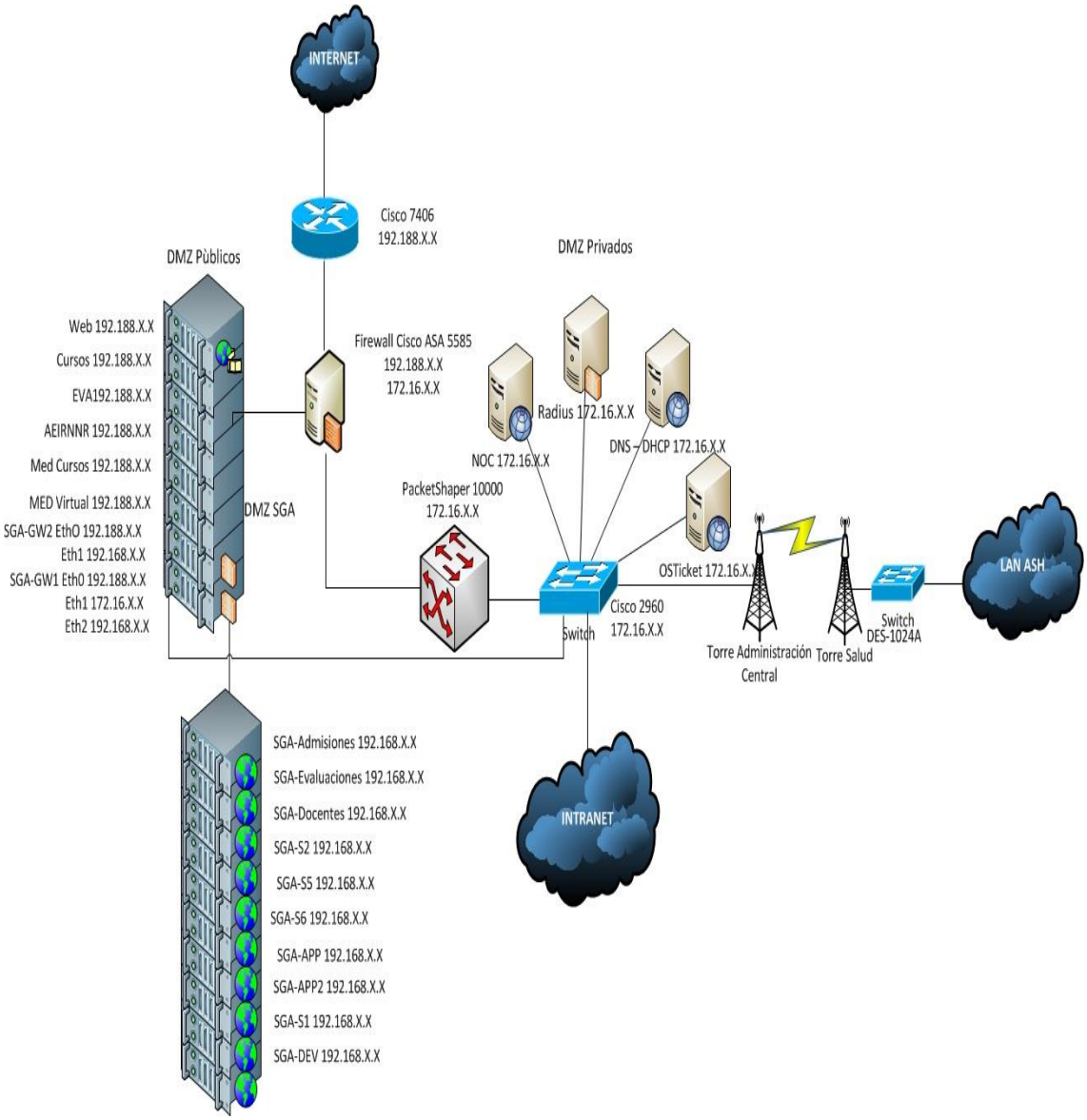


Figura 44. Propuesta de Topología

2.1.2.4. Control de Acceso

Para incrementar el nivel de seguridad se debe regular el acceso del personal y para esto existen muchos sistemas de seguridad como tarjetas inteligentes pero estás pueden extraviarse y caer en manos equivocadas. Las cerraduras codificadas son otra opción pero tienen que cambiar sus códigos periódicamente para evitar que el código sea descifrado o divulgado.

Entonces una opción segura es implementar controles biométricos por medio de la huella digital para asegurar el acceso seguro a los equipos, para dar solución al

problema del acceso no controlado se sugiere adquirir una puerta blindada, con cerradura biométrica, **Ver** Figura 45.

Las Puertas Blindadas comparadas son de las siguientes características, **Ver** Tabla XIX:

TABLA XIX Comparación Puertas

CARACTERÍSTICAS	PUERTA DE SEGURIDAD ENCHAPADA LOOCKS SAFE	PUERTA DE SEGURIDAD CORZA	PUERTA DE SEGURIDAD RINO
Medidas	210 cm x 96 cm x 17 cm	270 cm x 115 cm x 45	190 cm x 115 cm x 25 cm
Materiales	Doble plancha de acero de 1,3 mm,	MDF, pino riadato	Madera lustrada o pintada
Blindaje	3mm con perfiles estructurales de Acero	4mm	Envolvente de lado exterior, acero de 3mm
Cerradura	Multipunto con 6 puntos de cierre. Pestillo auxiliar de Emergencias	Pomo manilla tubular / caja	Chapa acerada de 2,1 mm
Resistencia	patas de cabra, golpes con herramientas contundentes y otras formas comunes de hurto	No especificado	Refuerzo antipalanca en los lados, con planchuelas soldadas de 3mm de espesor.
Marco	Acero	Lenga marca POLI, tipo PROMACEL	No especificado
Bisagras	Tope central para evitar desgaste	Acero bronceado, Marca POLI	Acero

Terminado	Madera contrachapada y con laca catalizada al acido, diseño y color a elegir	MDF pre-pintado – MDF Enchapado	Madera
Aislador Acústico	SI	NO	NO
Mirilla	140º	120º	180º
Precio	$ 1, 680.00	$ 1, 823.89	$ 1, 357.00

Elegimos la Puerta de Seguridad Enchapada Look Safe ya que nos ofrece aislamiento acústico, necesario para la Sala de Servidores, además de tener buen blindaje con acero y reforzamiento superior a las marcas comparadas.

Las características de la puerta escogida se describen a continuación en la Tabla XX:

TABLA XX Características de Puerta Blindada para la Sala de Servidores

MODELO	CARACTERÍSTICAS
PUERTA DE SEGURIDAD ENCHAPADA LOOCKS SAFE	• Puerta de seguridad construida en doble plancha de acero de 1,3mm, teniendo un total de blindaje de 3mm, con perfiles estructurales del mismo material, horizontales y verticales electro soldadas cada 10 centímetros. • Cerradura de procedencia europea multipunto tipo multilok embutida con seis puntos de cierre al frente, tres puntos en la parte posterior, un punto de cierre en el piso y uno en el tumbado. • Pestillo de auxilio adicional para uso de emergencias (solo se ve internamente) • Puerta y marco metálicos diseñados para resistir ataques con patas de cabra, golpes con herramientas contundentes y otras formas comunes de hurto. • Marco metálico construido de acuerdo al ancho de la pared donde va a ser instalado fijado con varillas de

	sujeción introducidas a presión en la pared y electro soldadas. • Instalados con tapa marcos. • Bisagras de seguridad con tope central para evitar desgaste. • Terminado de lujo con madera contrachapada y con laca catalizada al acido, diseño y color a elegir. • Aislador acústico interior. Mirilla de 140grados. • Construida a medida evitando derrocamientos y molestias innecesarias. • Medidas: 210 cm x 96 cm x 17 cm

La puerta de seguridad blindada de ir acompañada por una cerradura biométrica que complemente la seguridad de la sala de servidores, estas son las características de las tecnologías a comparar, **Ver** Tabla XXI:

TABLA XXI Comparación Cerraduras Biométricas

CARACTERÍSTICAS	CERRADURA BIOMETRICA L7000 ZK CVT 76010	CERRADURA DE LA HUELLA DIGITAL (BL-V900-SS)	CERRADURA BIOMETRICA S520
Material	Aleación de zinc	Acero inoxidable, plateado	Aleación de zinc
Pantalla	Oled	Oled	Oled
Sensor	Óptico tipo ZK de 500 dpi	No especificado	No especificado
Nº de Huellas	500	100	180
Nº de Contraseñas	100	100	100
Método de verificación	Huella o contraseña	Huella o contraseña	Huella digital, teclado, huella digital + teclado
Longitud de	6 a 10 dígitos	4 a 8 dígitos	4 dígitos

contraseña			
Temperatura de Operación	0ºc a 45ºc	-20ºc a -50ºc	0ºc a 50ºc
Alimentación	4 baterías 1,5 AA	1,5V	4 baterías 1,5 AA
Dimensiones	185 * 72 * 68.5 mm.	80 x 290 x 40 mm	100 x 90 x 25 mm
Precio	$ 334.88	$500.25	$420.99

La cerradura biométrica elegida es la CERRADURA BIOMETRICA L7000 ZK CVT 76010, esta cerradura biométrica es muy completa ya que posee un menú en pantalla y se puede verificar la identidad de una persona y abrir la puerta mediante una huella y una contraseña.

Además otra de sus ventajas es la administración y el alta de usuarios se puede hacer de una manera muy sencilla directamente en su pantalla. Cuenta con tres niveles de usuario para administrar el sistema: administrador, supervisor y usuario regular. Un administrador es capaz de agregar, borrar o cambiar usuarios en la cerradura.

Provee una interfaz de usuario muy amigable la cual le ayudará a utilizar la cerradura biométrica de una manera muy sencilla una vez que haya leído las instrucciones. Lo más importante su fácil instalación el diseño de esta cerradura puede reemplazar a la cerradura actual sin necesidad de modificar la puerta de acceso.

La privacidad es un factor importante para sugerir este tipo de cerradura las huellas almacenadas en la cerradura permanecen incluso si hay fallos de energía. Las huellas son protegidas con una tecnología muy especial que impide obtener la imagen de la huella desde la cerradura, también está fabricada de una aleación de zinc que provee una firme protección contra impactos.

Cuenta con una alarma de seguridad que se activa cuando es operada de forma indebida por algún intruso y almacena hasta 500 huellas digitales que le permiten registrar a todas las personas que desee darles acceso a sus instalaciones.

La l7000 es alimentada por 4 baterías AA que le brindan hasta 5,000 aperturas. el nivel de la batería es mostrado en su pantalla oled y soporta el uso temporal de una

batería DC externa para verificar su huella o contraseña y poder abrir la puerta conectándole una batería de 9v en la parte inferior de la cerradura.

Figura 45. Modelo cerradura biométrica

Existen muchas marcas y modelos de cerraduras biométricas pero se ha elegido esta opción por las múltiples ventajas ya expuestas que otras cerraduras no ofrecen.

2.1.2.5. Impermeabilización del Cuarto Frio

La Sala de Servidores al estar ubicada en el cuarto piso del Bloque 2 de la Administración Central no cumple con las especificaciones técnicas en cuanto a ubicación, según la norma EIA/TIA 942 esta Sala no debe estar ubicada en los últimos pisos ni en plantas bajas por posibles filtraciones de líquidos, no debe tener ventanas y además se le debería dedicar una planta exclusiva ya que debido a la falta del espacio físico no se puede implementar salidas de emergencia necesarias en caso de presentarse algún riesgo, pero el costo de mover toda la infraestructura para reubicarla en un piso intermedio es elevado. Se necesita la impermeabilización de esta sala para mitigar el impacto de posibles filtraciones de líquidos.

Para realizar la impermeabilización de azoteas se pueden encontrar una gran variedad de opciones ya que existen muchos materiales que se pueden aplicar a la azotea para que tenga a propiedad de ser impermeable. A la hora de escoger el material que se utilizará se debe tener en cuenta una cantidad de aspectos sobre la azotea que se impermeabilizará, así como también que tan expuesta va a estar la misma al contacto

con el agua, para saber si necesita una protección ligera, o una protección más importante.

El Tabla XXII se compara algunos impermeabilizantes populares para elegir el idóneo para la Sala de Servidores:

TABLA XXII Comparación Impermeabilizantes

CARACTERÍSTICAS	SIKAPLAN 12G	PLAVICON MEMBRANA FIBRADA	IMPERMEABILIZANTE ELASTEX TRANSITABLE
Tipo	Membrana	Membrana	Pintura
Componentes	PVC Plastificado, Fibra sintética de poliéster	Poliuretano	100% Elástico
Normas	ASTM 1003, D882, DIN 16734	ISO 9001-2008	No especificado
Usos	Cubiertas Planas o Inclinadas , Rehabilitación de cubiertas o nuevas	Cubiertas Planas o Inclinadas	Exteriores sobre cubiertas planas o inclinadas como techos, terrazas y tinglados, sobre cemento, teja, zinc, galvanizado, chapa, fibrocemento o cerámicos.
Resistencia	Microorganismos, ozono, polución, penetración de raíces, envejecimiento natural, radiaciones ultravioleta, lluvia ácida y granizo	Fricción y transitabilidad	No especificado

Toxicidad	No peligroso ni en aplicación , ni almacenamiento	Uso delicado	Uso delicado
Presentación	Rollo 2m de ancho x 25m de largo	Lata de 5,10, 15, 20 kg	Lata de 1, 4, 10, y 20 litros.
Precio	$ 1,125.20	$ 9,230.70	$ 1,790.33

El impermeabilizante escogido es Sikaplan 12 G que es una membrana a base de PVC plastificado, fabricada mediante calandrado en dos capas y reforzada con una armadura de fibras sintéticas a base de poliéster, que se emplea para la impermeabilización de cubiertas.

Se utilizan para la impermeabilización de cubiertas planas o inclinadas, tanto en obra nueva como en rehabilitación de cubiertas existentes.

Las membranas Sikaplan 12 G proporcionan las siguientes ventajas:

- Elevada durabilidad.
- Estabilidad dimensional
- Elevada resistencia a la tracción.
- Excelente flexibilidad.

Además, las membranas Sikaplan 12 G proporcionan una mayor resistencia a los siguientes parámetros: Microorganismos, ozono, polución, penetración de raíces, envejecimiento natural, radiaciones ultravioleta, lluvia ácida y granizo.

2.1.2.6. Sistema Auxiliar de Energía

Un Sistema Auxiliar de Energía permite obtener un funcionamiento ininterrumpido en la Sala de Servidores necesario para cumplir con la norma EIA/TIA 942.

El total de consumo de la Sala de Servidores es de 3146W y por lo tanto se sugiere adquirir un generador eléctrico que cubra esta necesidad de consumo, en la Tabla XXIII se da a conocer las tecnologías más usadas en generadores eléctricos:

TABLA XXIII Comparación Sistemas Auxiliares de Energía

CARACTERÍSTICAS	PRAMAC P6000S	PORTEN PG6000D	LINCOLN ELECTRIC
Marca:	Pramac	Porten	LincolnElectric
Modelo	P6000S A/C Watts	PG6000D	Ranger 225
Watts de Salida	6000W	4500W	9000 Watts
Watts de Salida Máxima	6500W	6000W	10500 W
A/C Voltaje:	120/240VAC	120V/240V	120V/240V
A/C Frecuencia:	60 Hz	60 Hz	50/60 hz
Cilindrada del Motor:	406cc	418cc	466 cc
Tipo de Motor:	Diésel	Diésel	Diésel
Potencia del Motor:	8.4 HP	9.00 HP	N/D
Aceite Recomendado:	15 W40	15 W40	N/D
Encendido:	Eléctrico Batería Incluida	Eléctrico Batería Incluida	Eléctrico
Indicador Nivel Combustible	Si	Si	Si
Capacidad del Tanque:	5 gl	3.2 gl	12 gl
Horas de Operación	14.9 hrs	9.5 hrs	N/D
Peso:	436.5 lbs / 198 kg	363.76 lbs / 165.00 kg	514 lbs / 233 kg
Medidas:	Alto: 84 cm Ancho:54.72 cm Largo: 91.6 cm	Alto: 56.5 cm Ancho: 77 cm Largo: 95 cm	Alto: 75.9 cm Ancho: 54.6 cm Largo: 107.3 cm
Tablero de trasferencia automática	Si	No	No
Rack de protección	Si	Si	No
Precio	$6,223.86	4,758.02	$ 7200.00

Se eligió el generador PRAMAC P6000S**, Ver** Figura 46, porque es superior en cuanto en características, sobre todo en su tablero de transferencia automática. Este Tablero sirve para poner en funcionamiento el generador en forma automática, cuando hay un corte del suministro de energía eléctrica, además detiene el funcionamiento del generador cuando la electricidad regresa, todo esto sin necesidad de intervención de personas, el tablero asegura que la energía del generador como la de la red pública jamás se encuentren así asegurando las instalaciones.

También otros factores que influyeron para elegir este generador son su bajo consumo de combustible y más horas de operación.

Figura 46. Modelo de generador eléctrico

El generador deber estar ubicado en el primer piso para evitar accidentes o inconvenientes, ya que no es aconsejable que el generador se encuentre ubicado en el mismo piso debido a que el mismo funciona a base de combustible y se podría ocasionar algún daño en los equipos.

2.1.2.7. Fuente de Alimentación Ininterrumpible (Ups)

Basándonos en la norma EIA/TIA 942 una la Sala de Servidores debe contar con UPS para evitar la interrupción de las operaciones por variaciones de voltaje.

Los servidores en la UTI no cuentan con UPS que protejan a los servidores de variaciones de voltaje, por tal motivo se sugiere la adquisición de un UPS, a continuación, **Ver** Tabla XXIV:

TABLA XXIV Comparación UPS

CARACTERÍSTICAS	UPS POWERCOM	UPS Online Titan	Smart-UPS VT
Capacidad	10000VA	10000VA	10000VA
Potencia	7000Watts.	7000Watts.	8000Watts.
Entrada			
Voltaje	220v	220v	220v
Frecuencia	50/ 60Hz. +/-0.5%	50/ 60Hz. +/-0.4%	60 Hz
Factor de potencia	0,99	0.98	N/D
Salida			
Voltaje	110/220V	220V	120/208V
Frecuencia	60 Hz	60 Hz	60 Hz
Factor de potencia	0.7	0.7	N/D
Baterías			
Nª baterías	20 x12V 9ª	20 baterías	2 módulos
Tiempo de autonomía	Tiempo de respaldo 15 minutos a full carga y 7 minutos al 50% de la carga	8 minutos full carga	18 minutos full carga
Tiempo de transferencia	0 ms	0 ms	0 ms
Indicador	LCD: Mide la carga, estado de baterías, 0061larmas, temperatura.	Nivel de carga Nivel de batería Modo de batería Modo AC Modo bay pas Falla	LCD Estatus multifuncional y consola de control
Alarmas audibles	Si	Si	Si
Condiciones Ambientales	0 - 40 °C	0 - 40 °C	0 - 40 °C
Precio	**$ 4.895**	$ 3600	$ 5100

Se eligió el POWERCOM de 10KVA ONLINE, **Ver** Figura 47, que evita los milisegundos sin energía al producirse un corte eléctrico, pues provee alimentación constante desde su batería y no de forma directa, este UPS está controlado por un microprocesador que aumenta la eficiencia y garantiza alta confiabilidad.

Figura 47. UPS POWERCOM de 10KVA ONLINE

En la Figura 48 se muestra el diagrama eléctrico, integrando el UPS POWERCOM y el generador eléctrico:

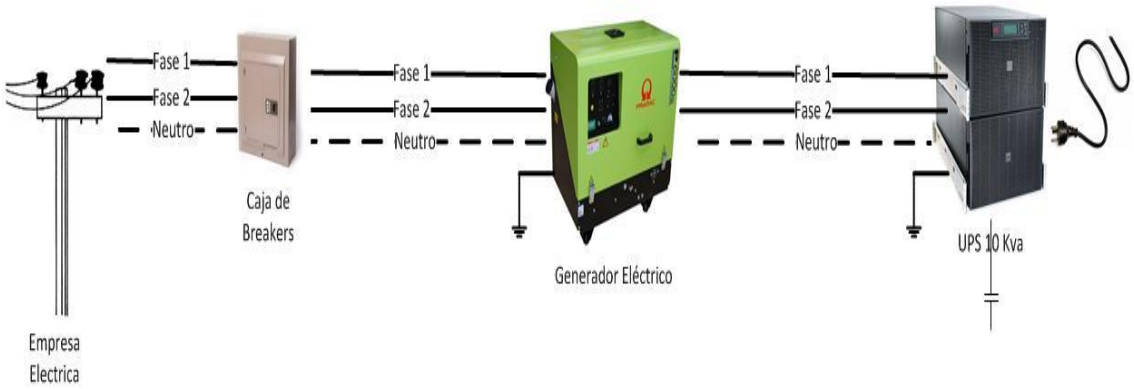


Figura 48. Propuesta Diagrama Eléctrico

2.1.2.8. Sistema contra Incendios

Se sugiere la implementación de un sistema contra incendios, tomando en cuenta que los equipos no deben ser dañados cuando el sistema de supresión de incendios sea disparado, agua o agentes capaces de causar cortos circuitos, pérdidas de aislamientos, choques térmicos o corrosión, no deben ser utilizados.

Hemos elegido algunos de los sistemas más utilizados para elegir el sistema contra incendios idóneo para la Sala de Servidores, **Ver** Tabla XXV:

TABLA XXV Comparación Sistema Contra Incendios

CARACTERÍSTICAS	SISTEMA CONTRA INCENDIOS FM200	SISTEMA CONTRA INCENDIOS PROINERT	SISTEMA CONTRA INCENDIOS ECARO-25
Componentes	1,1,1,2,3,3,3-Heptafluoropropano	IG-55 (combinación con Argón y Nitrógeno)	Agentes Limpios
Normas	ISO 9002 UL, FM, LPCB, ISO 14520, EN 14520, NFPA 2001, US EPA SNAP listed, HAG listed, TPED compliant, DOT compliant	UL, FM, LPCB, ISO 14520, EN 14520, NFPA 2001, US EPA SNAP listed, HAG listed, TPED compliant, DOT compliant	UL, FM, LPCB, ISO 14520, EN 14520, NFPA 2001, US EPA SNAP listed, HAG listed, TPED compliant, DOT compliant
Tóxico	NO	NO	NO
Residuos	NO	NO	NO
Espacio Físico	Mínimo	Mediano	Máximo
Precio	$4,270.23	$5,500.99	$7,400.67

Siguiendo la norma EIA/TIA 942 uno de los sistemas más usados y de alto nivel es el Sistema de Supresión de Incendios, con Agente Limpio basados en FM-200, **Ver** Figura 49, que está diseñado especialmente para equipos electrónicos y eléctricos.

En caso de incendio este gas se mueve por medio de unas tuberías llegando hasta las boquillas donde se descarga en estado gaseoso. Al ser un gas invade todo el espacio llegando a sitios donde otros agentes extintores no pueden llegar. La descarga se realiza en un tiempo máximo de 10 segundos. En sólo ese tiempo el fuego habrá sido sofocado. Este gas lo que hace es romper la reacción en cadena del fuego extinguiendo la energía calorífica de la llama. Apagando los incendios inmediatamente.

Figura 49. Tanques de FM-200

Este tipo de sistema no son conductores de electricidad y no dañan los equipos electrónicos, también son seguros para las personas y no dejan residuos ni requieren de limpieza. El diseño de la Sala de Servidores con el sistema de incendios propuesto quedaría establecido de la siguiente forma, **Ver** Figura 50:

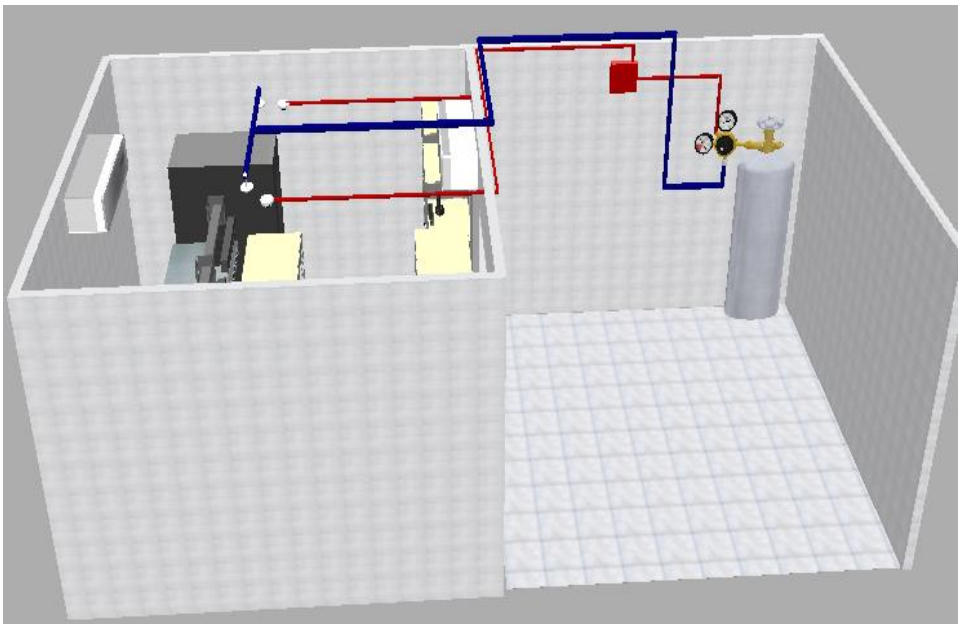


Figura 50. Diseño de Sistema Contra Incendios

Este tipo de sistema contra incendios es diseñado y construido por la empresa HYWOOD, que diseña estos sistemas de acuerdo a las necesidades de cada cliente.

2.1.2.9. Hardware necesario para los Servidores

En vista de que la mayoría de equipos que conforman la Sala de Servidores no tienen características de servidor, y para mejorar los servicios que corren en estos equipos la Universidad Nacional de Loja adquirió un servidor BLADE con varias tarjetas BLADE, para solucionar los problemas de disponibilidad por daños o saturación de los equipos, **Ver** Figura 51.

Además un servidor BLADE permitirá ahorrar considerablemente el espacio que se dispone para los equipos en la Sala de Servidores, debido a que con un solo servidor remplazaríamos físicamente a cerca de 28 servidores almacenados en la Sala de Servidores. También nos permite gran escalabilidad al permitir agregar fácilmente más servidores, simplemente con agregar más tarjetas BLADE ya que cada tarjeta es un servidor auto-contenido, ejecutando su propio sistema operacional y software, está diseñado para activarse y ejecutar sin intervención humana.

Facilita la instalación ya que todo está centralizado, al centralizar los servidores en un solo equipo se podrá reducir notablemente el consumo de energía y distribuir de mejor forma el sistema de enfriamiento.

El fácil mantenimiento es una gran ventaja en estos equipos porque permite intercambio en caliente (Hot-Swap) lo que significa que un BLADE que falla, puede ser remplazado con el equipo energizado (cambio en caliente) sin ningún impacto en los otros BLADE.

A continuación daremos a conocer las características del servidor BLADE adquirido en la tabla XXVI:

TABLA XXVI Características del Servidor Blade UTI

DESCRIPCIÒN	CANTIDAD ADQUIRIDA
HP BL460c G7 X5650 6G 1P Svr **Procesador:** Intel® Xeon® X5650 (2.66GHz/6-core/12MB/95W, DDR3-1333, HT, Turbo 2/2/2/2/3/3), **Memoria** RAM: 6GB; **Puerto de LAN:** NC553i Dual Port FlexFabric 10Gb; **Controlador de**	1

Discos: HP Smart Array P410i Controller (RAID 0/1)	
Procesador Adicional: HP BL460c G7 X5650 FIO Kit	1
Memoria Ram Adicional: HP 4GB 2Rx4 PC3-10600R-9 Kit	4
Almacenamiento Interno: HP 300GB 10K 6G 2.5 SAS DP HDD	2
Conectividad FC al Storage: HP BLc QLogic QMH2562 8Gb FC HBA Opt	1
Contrato de Soporte: HP 3y 4h 24x7 BL4xxc Svr Bld HW Support	1

Figura 51. Servidor Blade UTI

El servidor adquirido por la UNL está ubicado físicamente en la Sala de Servidores pero aún no se han virtualizado los servicios, debido a que no se adquirido el software necesario para realizar esta tarea, el software que se necesita para utilizar de forma eficiente los recursos del BLADE es el VMWARE con licencia privativa.

2.1.2.10. Sistema de Aire Acondicionado

Según la Norma EIA/TIA 942 se debe contar con un sistema de aire acondicionado completo para la Sala de Servidores, en vista que se cuenta con 2 aires acondicionados para oficina y no para Salas de Servidores, por tal motivo se

comparará 3 tecnologías para el enfriamiento de Salas de Servidores para elegir la mejor, **Ver** Tabla XXVII. Para determinar los BTUs[22] necesarios para la Sala de Servidores se utilizó los siguientes parámetros:

$$C = 230xV + (\#PyEx476)$$[23]

En donde:

230 = Factor calculado para América Latina "Temperatura máxima de 40°C" (dado en BTU/hm³)

V = Volumen del ÁREA donde se instalará el equipo, Largo x Alto x Ancho en metros cúbicos m³

 # PyE = # de personas + equipos instalados en el área

476 = Factores de ganancia y perdida aportados por cada persona y/o equipos (en BTU/h)

30% de sobredimensionamiento

$$C = 230x3x3x2{,}80 + (48x476)$$

$$C = 5726 + (22848)$$

$$C = 28574\ BTUs\ x30\%$$

$$C = 37146{,}2\ BTUs$$

Los BTUs son la capacidad de enfriamiento que tiene un Aire Acondicionado en nuestro caso la Sala de Servidores necesita un aire acondicionado mínimo de 28574 BTUs.

[22] **BTU:** Unidad térmica británica/h
[23] Suministro e Instalación de Sistema de Aire Acondicionado, Arq. Manuel Namoc, Universidad Privada Antenor Orrego, Trujillo México, 2011

TABLA XXVII Comparación de Sistemas de Aire Acondicionado

CARACTERÍSTICAS	STULZ CyberAir 2 CWE ASD 1300 CWE/CWU	CelAir OHS	ModulAir MCS
Potencia Frigorífica	Total: 126,4 kW Sensible: 97,9 Kw	Total: 112,2 kW Sensible: 75,4 kW	Total: 95,2 kW Sensible: 57,3 kW
Flujo de Aire	22000 m^3/h	13000 m^3/h	10000 m^3/h
Temperatura del aire de retorno	24 ºC	24 ºC	24 ºC
Humedad del aire de retorno	50% Relativo	45% Relativo	35% Relativo
Temperatura de entrada media	7 ºC	7 ºC	7 ºC
Nº de ventiladores	2	1	1
Consumo de energía de CWU	4,0 KW	NO	NO
Dimensiones	Ancho 2.150 mm Altura 2.495 mm Fondo 890 mm	Ancho 1.150 mm Altura 2.200 mm Fondo 730 mm	Ancho 1.040 mm Altura 2.135 mm Fondo 720 mm
Capacidad máxima de humidificador	15 kg/h	13 kg/h	11 kg/h
Capacidad de enfriamiento.	40000 BTUs	60000 BTUs	50000 BTUs
Precio	$5,723.77	$8,689.56	$7,976.40

STULZ CyberAir 2 CWE ASD 1300 CWE/CWU, **Ver** Figura 52, uno de los sistemas más utilizados a nivel mundial.

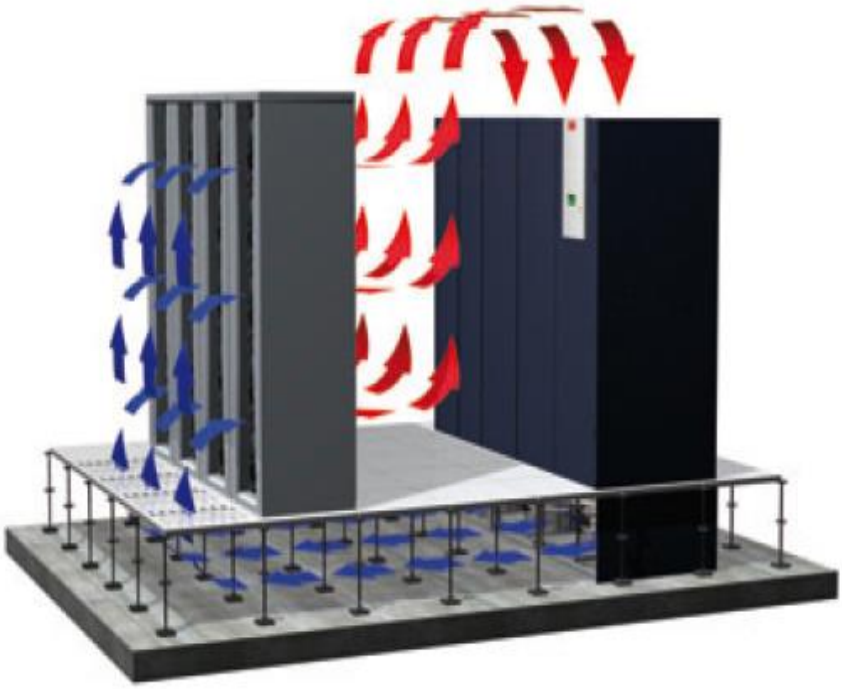


Figura 52. Sistema de Aire Acondicionado STULZ

El sistema de enfriamiento STULZ CyberAir 2 CWE ASD 1300 CWE/CWU ayudará a utilizar la máxima capacidad útil de enfriamiento con una reducción de entrada de energía considerable, además es de instalación flexible según espacio disponible y condiciones del lugar una de las características sobresalientes de este sistema ya que la Sala de Servidores cuenta con un área de $9m^2$.

También cuenta con un Controlador C7000 / gestión de la redundancia y es de fácil mantenimiento, ya que cuenta con un acceso frontal otra ventaja importante es el Intercambiador de calor que optimiza el consumo de energía cuando se presentan altas temperaturas.

2.1.2.11. Respaldos de los servidores

El servidor de respaldo de la Unidad de Telecomunicaciones e Información ejecuta un script para respaldar los archivos de los servidores que han sido modificados durante el día.

El servidor de respaldos está físicamente ubicado en la Sala de Servidores por lo que se recomienda reubicarlo en otro lugar ya que la desventajas de utilizar un medio de respaldo local es que en caso de desastre o robo se verán igual de afectados los

equipos, aun así el respaldo local es una medida muy importante y es la primera línea de defensa para salvaguardar la información, pero no es aconsejable usar este tipo de respaldo.

El respaldo remoto nos ayuda a protegernos contra desastres como incendios e inundaciones, contra robos y otras eventualidades que puedan ocurrir en la Sala de Servidores por eso es aconsejable respaldar la información de esta manera, ubicando el servidor de respaldo en el Área Educativa, Bloque 7 denominado Dirección del Área ya que se cuenta con un espacio disponible y adecuado para ubicar el servidor de respaldos en el segundo piso junto al rack a donde llega la fibra óptica. **Ver** Figura 53.

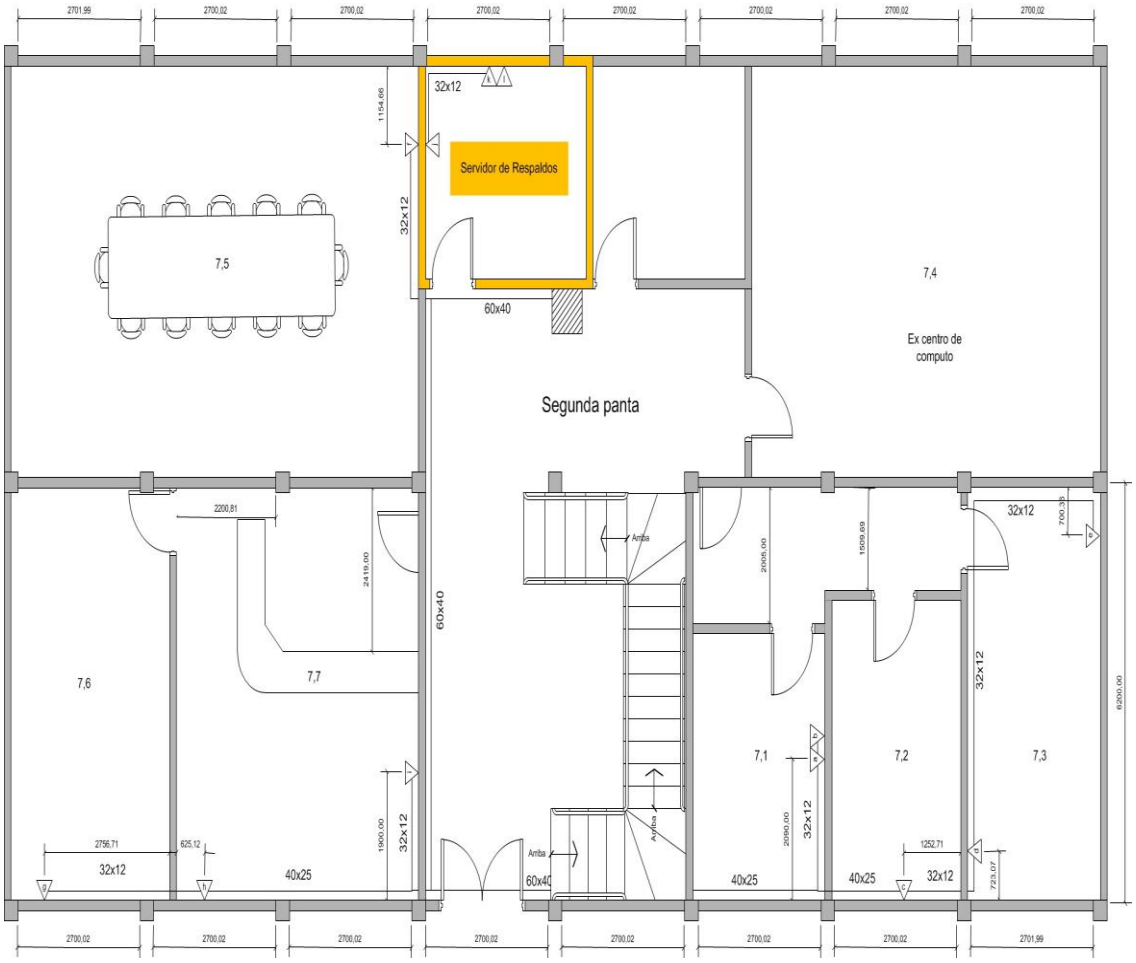


Figura 53 Planos de ubicación Servidor de Respaldos

El diseño final del lugar en el que se ubicará el servidor de respaldos está en la Figura 54:

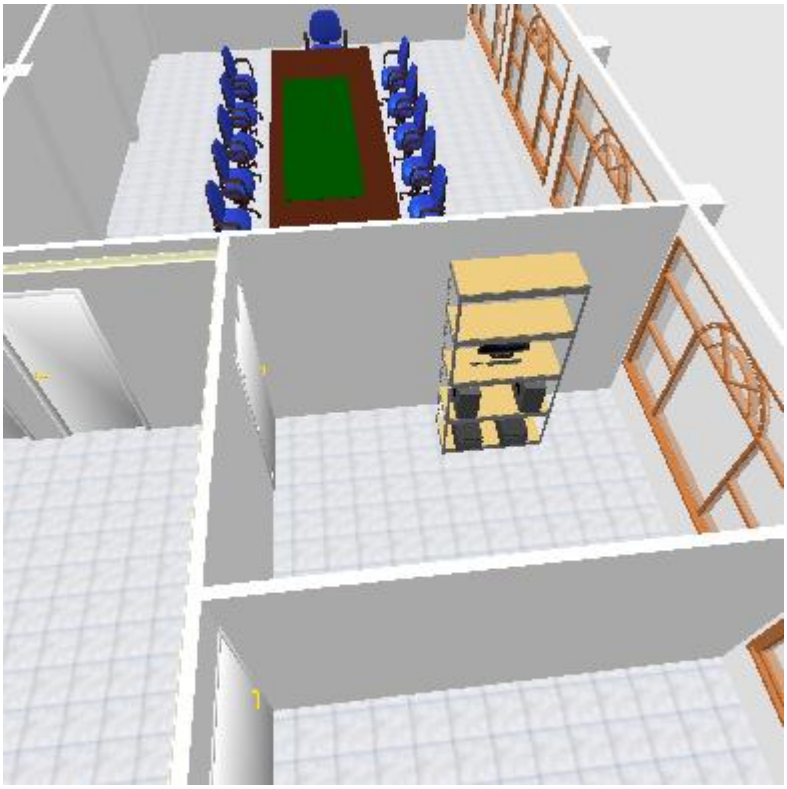


Figura 54 Vista 3D de ubicación del Servidor de Respaldos

2.1.2.12. Diseño de la Sala de Servidores

La propuesta para el diseño final de la Sala de Servidores con todas las adecuaciones según la Norma EIA/TIA 942, queda establecido de la siguiente manera, **Ver f**igura 55 y 56:

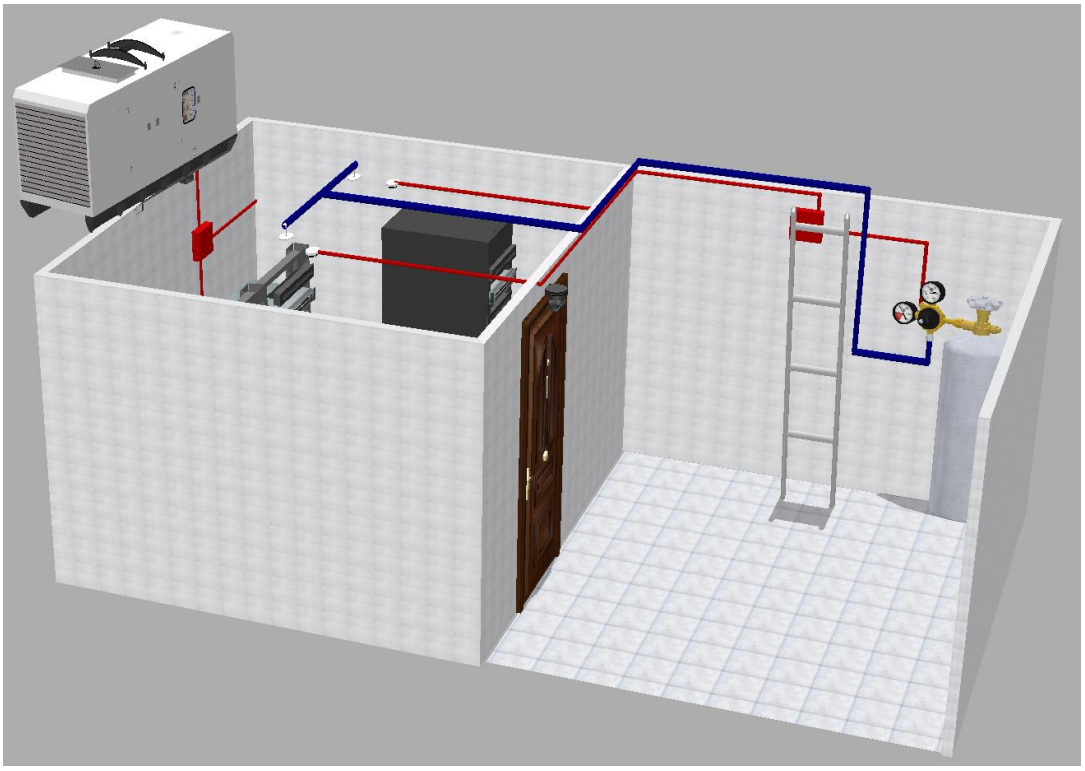


Figura 55: Diseño final de la Sala de Servidores

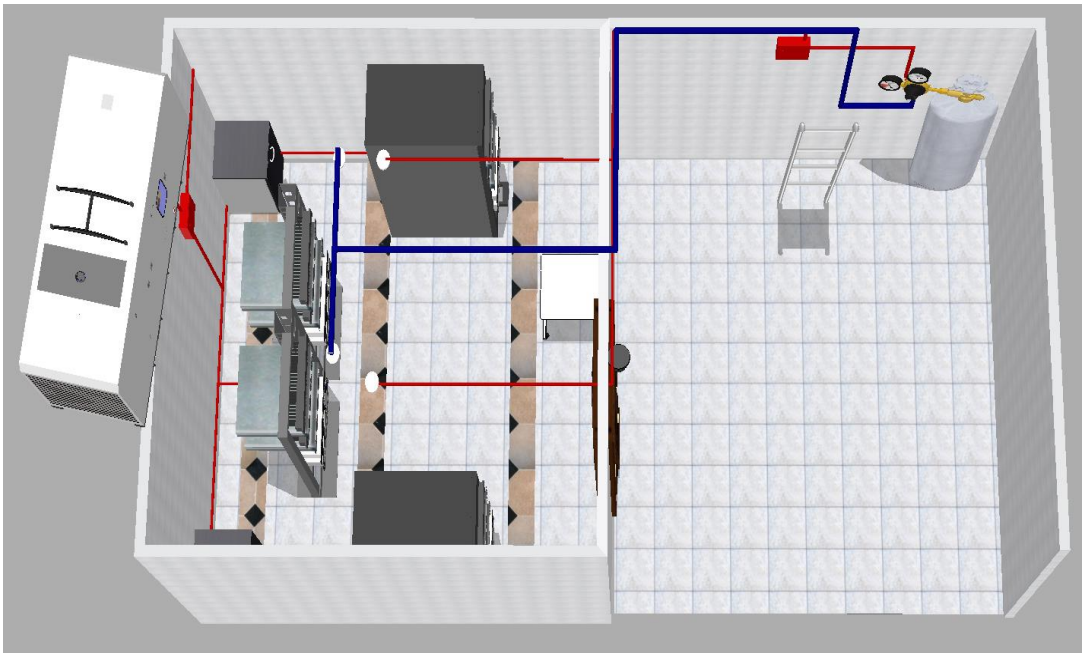


Figura 56. Vista Superior de la Sala de Servidores

2.1.2.13. PRESUPUESTO ESTIMADO PARA LAS SEGURIDADES FÍSICAS

Para implementar las soluciones sugeridas en la parte de seguridades físicas en la Tabla XXVIII se presentará un estimado del presupuesto necesario:

TABLA XXVIII Presupuesto Estimado para Seguridades Físicas

SEGURIDADES FÍSICAS	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
EQUIPO GESTIONADOR DE ANCHO DE BANDA BLUECOAT	1	$1,831.50	$1,831.50
EQUIPO FIREWALL CISCO ASA 5585	1	$8,380.73	$8,380.73
PUERTA DE SEGURIDAD ENCHAPADA LOOCKS SAFE	1	$1,680.00	$1,680.00
CERRADURA BIOMÉTRICA L7000 ZK CVT 76010	1	$334.88	$334.88
IMPERMEABILIZANTE SIKAPLAN 12 G de 20ml	1 rollo de 1,55x20m	$1,125.20	$1,125.20
GENERADOR ELÉCTRICO PRAMAC 6000 WATTS	1	$ 6,653.95	$ 6,653.95
UPS POWERCOM de 10KVA ONLINE	1	$12,300.00	$12,300.00
SISTEMA DE SUPRESIÓN DE INCENDIOS CON AGENTE LIMPIO BASADOS EN FM-200	1	$4,270.23	$4,270.23
BLADE HP BL460c G7 X5650 6G 1P Svr	1	$ 14,906.67	$ 14,906.67
STULZ CyberAir 2 CWE ASD 1300 CWE/CWU	1	$5,723.77	$5,723.77
		TOTAL	$ 57,206.93

Objetivo 2:

ESTABLECER LAS HERRAMIENTAS ADECUADAS PARA EL ANÁLISIS DE LAS VULNERABILIDADES LÓGICAS EN LOS SERVIDORES.

2.2. HERRAMIENTAS PARA EL ANÁLISIS DE LAS VULNERABILIDADES LÓGICAS EN LOS SERVIDORES.

A continuación vamos a revisar las características de los principales scanners de vulnerabilidades, scanners de puertos y herramientas para la explotación de vulnerabilidades que según las páginas sectools.org [24] y insecure.org [25] dedicada a evaluar herramientas de seguridad informática, son las más potentes y usadas.

2.2.1. ELECCIÓN DE LAS HERRAMIENTAS A UTILIZAR

2.2.1.1. Scanners de Puertos

En la fase de Reconocimiento Activo se necesita de un escáner de puertos para identificar los tipos de servicios que están corriendo en cada uno de los servidores, los puertos abiertos o cerrados para tener un amplio conocimiento del estado de los mismos en la Tabla XXIX se realiza una comparativa de los escáner de puertos más completos y utilizados para determinar la herramienta que se ajuste a las necesidades del proyecto.

TABLA XXIX Comparativa de Scanners de Puertos

CARACTERÍSTICAS	NMAP	NETCAT	CHEOPS
Tipo	Scanner de puertos y Fingerprint	Scanner de puertos y snniffer	Scanner de puertos y snniffer
Funcionalidades	- Descubrimiento de servidores - Identifica puertos abiertos en una computadora objetivo. - Determina qué servicios está ejecutando la misma. - Determinar qué	- Corrección de Errores de red - Habilidad de rastrear puertos source-routing - Transmisión/Recepción de datos	- Mapeo/Trazado - Acceso fácil a funciones de gestión (ping, traceroute, ftp , secure shell) - Escaneo de puertos – OS Fingerprinting - Monitoring Support

[24] **Sectools.org:** http://sectools.org/
[25] **Insecure.org:** http://insecure.org/

	sistema operativo y versión - Obtiene algunas características del hardware de red.		
Técnicas de escaneo que usa	TCPSYN TCP connect() FIN Xmas Null Ping Version Detection UDP IP Protocol ACK Window ACK RPC Idle FTP Bounce	ScanningsPorts Random en puertos conocidos, en modo ascendente o descendente, con intervalos de tiempo, utilizando Gateways para evitar mostrar la IP fuente del Scanning	No disponible
Estado de los puertos	Open Filtered Unfiltered Close	Open Close	Open Close Bloked
Exploración de redes extensas	SI	NO	SI
Creación de Perfiles de Ejecución	SI	NO	NO

Después de revisar las características de cada escáner decidimos utilizar la herramienta NMAP, con su interfaz gráfica ZenMap, ya que es un analizador de

puertos muy completo, además de ser una herramienta con licencia libre, y trabajar en puertos UDP y TCP.

Pero la característica principal por la que nos inclinamos por este escáner de puertos es que nos permite crear perfiles de ejecución con parámetros previamente establecidos, ayudándonos a realizar el análisis, con los mismos parámetros y valores a cada uno de los servidores, ahorrándonos valioso tiempo.

Nmap se utilizó para identificar el estado de los puertos y servicios que corren en los servidores en la fase de Reconocimiento Activo.

2.2.1.2. Scanners de Vulnerabilidades

Para la Fase 2 denominada de Análisis de Vulnerabilidades el presente proyecto de tesis se necesita de una herramienta que facilite la detección de Vulnerabilidades, para cumplir esta etapa se compara el software más sobresaliente en scanners de Vulnerabilidades, **Ver** Tabla XXX:

TABLA XXX Comparación scanners de Vulnerabilidades

CARATERÍSTICA	NESSUS	OPENVAS	NIKTO
Fácil instalación	SI	NO	SI
Plugins	48268	25505	58672
Interfaz gráfica amigable	SI	NO	SI
Licencia	LIBRE	LIBRE	LIBRE
Soporte	ÚNICA EMPRESA	VARIAS EMPRESAS	VARIAS EMPRESAS
Configuración	FÁCIL	DIFICIL	FÁCIL
Multiplataforma	SI	SI	SI
Tiempo de análisis	Corto	Largo	Corto
Escaneo con credenciales	SI	NO	NO
Exportación de resultados	PDF, NBE,XML,.nessus, LATEX, HTML	PDF, NBE,XML, HTML	XML, HTML, NBE y CSV
Escaneos programados	SI	SI	NO

Clasificación de vulnerabilidades por nivel de criticidad	SI	SI	SI
Soporte IPV6	SI	NO	SI
Consumo de recursos	BAJO	ALTO	BAJO

NIKTO se lo utilizó para detectar las vulnerabilidades en cada servidor, y contrastar resultados, se lo eligió por su compatibilidad con ipv6, y el bajo consumo de recursos que emplea al realizar un escáner.

Además se eligió NESSUS ya integra funcionalidades muy importantes que no poseen los scanners de vulnerabilidades, NESSUS reduce el tráfico que genera al realizar el escáner de los host remotos si detecta que la red está muy congestionada. **Ver** Figura 57.

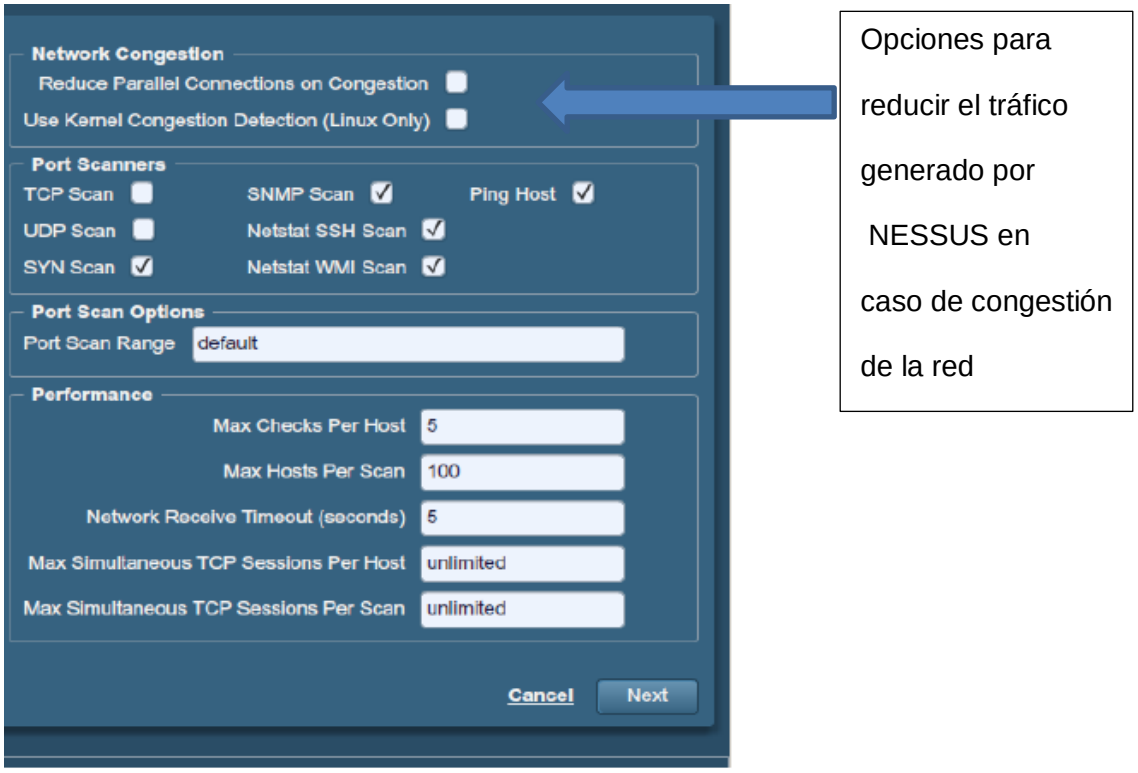


Figura 57. Opciones Nessus para el tráfico de red

Otra funcionalidad importante y que nos ayudó a elegir esta herramienta fue la posibilidad de realizar comprobaciones seguras de los host, mediante una opción llamada *"safe chek"* debido a que ciertas comprobaciones pueden ser perjudiciales para servicios de red específicos, **Ver** Figura 58.

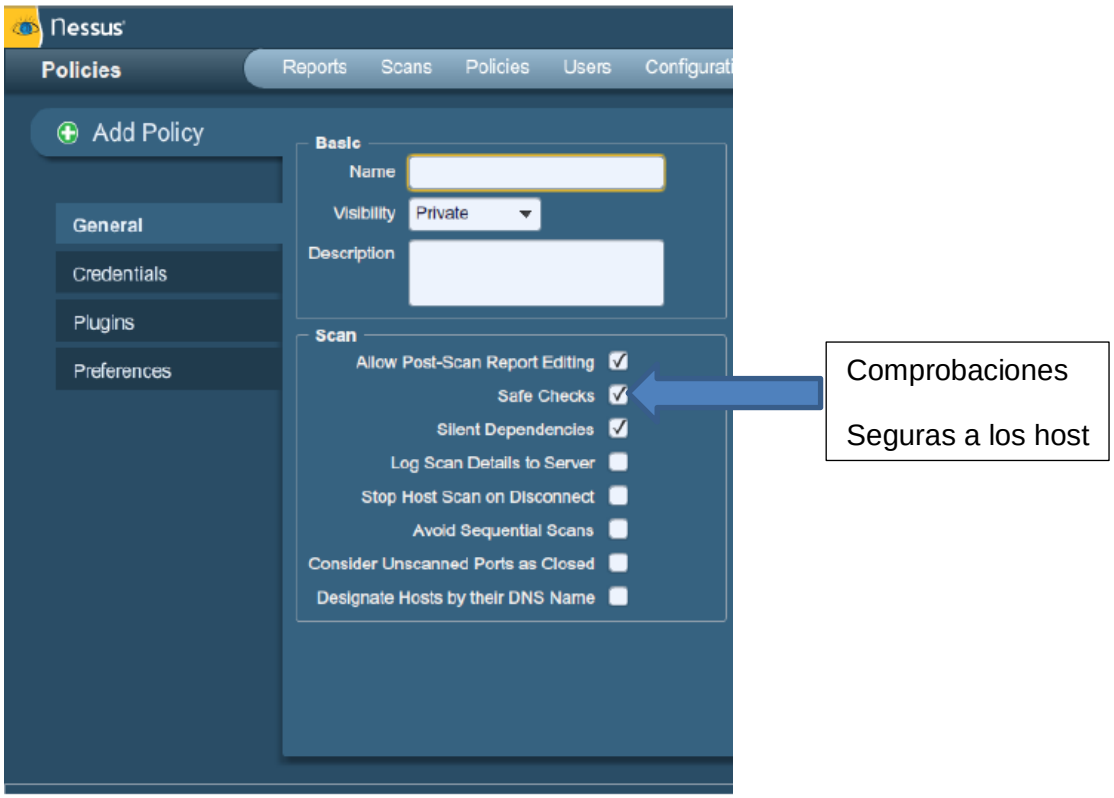


Figura 58. Comprobaciones seguras con NESSUS

Nessus posee a diferencia de los scanners utilizados, es decir que Nessus determinará los plugins que deben ejecutarse en el host remoto. También cuenta con una base de plugins más extensa y actualizada que los demás scanners, **Ver** Figura 59.

Figura 59. Plugins inteligentes de NESSUS

NESSUS además de generar los reportes y exportarlos permite importarlos para compararlos con reportes anteriores, también permite exportar e importar políticas de escaneo. **Ver** Figura 60.

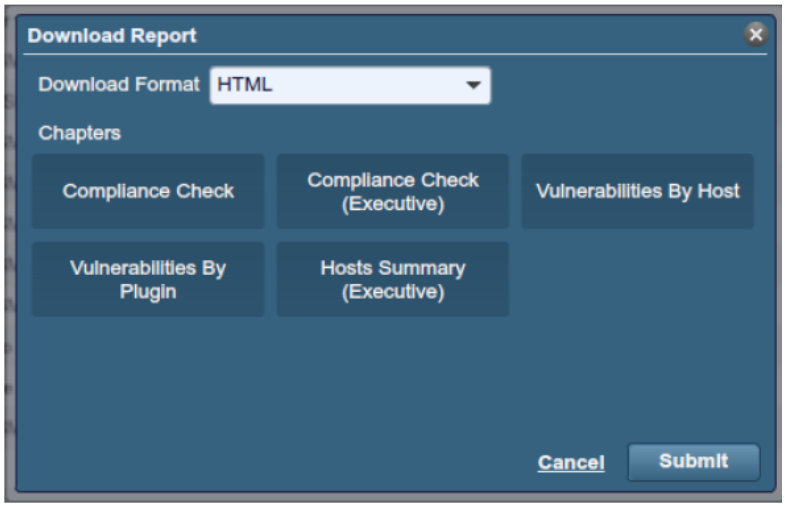


Figura 60. Exportación de Reportes en NESSUS

Una de las ventajas más importantes de NESSUS es su compatibilidad con IPv6 ya que admite análisis de recursos basados en IPv6, haciendo de NESSUS la herramienta más completa.

Por las razones expuestas se ha elegido la herramienta NESSUS, ya que nos proporciona muchas ventajas que nos ayudan en la detección más completa de las vulnerabilidades de cada uno de los servidores.

2.2.1.3. Herramientas para la Explotación de Vulnerabilidades

Para explotar las vulnerabilidades encontradas es necesario contar con una herramienta potente para este fin se contrasta en la Tabla XXXI, las principales herramientas para explotación de vulnerabilidades:

TABLA XXXI Comparación de Herramientas para Explotación de Vulnerabilidades

CARATERÍSTICA	CAIN Y ABEL	SNORT	WIRESHARK
Multiplataforma	SI	SI	SI
Descencriptado de claves	LM, md5, SHA1 y otros	NO	NO
Funcionalidad	Realiza ataques basados en Diccionario, fuerza bruta, sniffing, ataques criptoanálisis, etc	Realiza ataques basados en Backdoor, DDoS, finger, FTP, ataques web, CGI, Nmap...	Captura de tráfico. Trabaja con más de 480 protocolos. Reconstrucción de sesiones TCP
LICENCIA	LIBRE	LIBRE	LIBRE

Al comparar las herramientas para explotar las vulnerabilidades lógicas decidimos elegir Cain y Abel, por las características de descencriptado y captura de paquetes que posee, puesto que las vulnerabilidades que necesitamos explotar son causadas por el uso de protocolos inseguros.

Cain y Abel es una herramienta denominada de fuerza bruta y sirve para descifrar contraseñas y evaluar la seguridad en las redes esta herramienta se la eligió para ser utilizada en la fase de Explotación de Vulnerabilidades Lógicas.

Objetivo 3:

REALIZAR PRUEBAS A LOS SERVIDORES PARA DETERMINAR LAS VULNERABILIDADES EN LOS DIFERENTES SERVICIOS QUE BRINDAN.

2.3. PRUEBAS A LOS SERVIDORES EN BUSCA DE VULNERABILIDADES EN LOS DIFERENTES SERVICIOS QUE BRINDAN.

Los servidores han sido evaluados con el scanner de vulnerabilidades NESSUS y NIKTO, **Ver** Anexo VI, para detectar el mayor número de vulnerabilidades posibles, **Ver** Figura 61. NIKTO que nos ayudó a tener una segunda opinión acerca de las vulnerabilidades existentes, **Ver** Figura 62, y mediante la comparación de resultados se estableció la existencia de varias vulnerabilidades lógicas en los servidores de la UTI, **Ver** Tabla XLVII.

172.16.43.1

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	24	24

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10180	Ping the remote host
Info	10287	Traceroute Information
Info	10335	Nessus TCP scanner
Info	10386	Web Server No 404 Error Code Check
Info	10662	Web mirroring
Info	11032	Web Server Directory Enumeration
Info	11936	OS Identification
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	35716	Ethernet Card Manufacturer Detection
Info	39470	CGI Generic Tests Timeout
Info	39521	Backported Security Patch Detection (WWW)
Info	40984	Browsable Web Directories
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	54615	Device Type

Figura 61. Resultado de Servidor Proxy Energía según Nessus

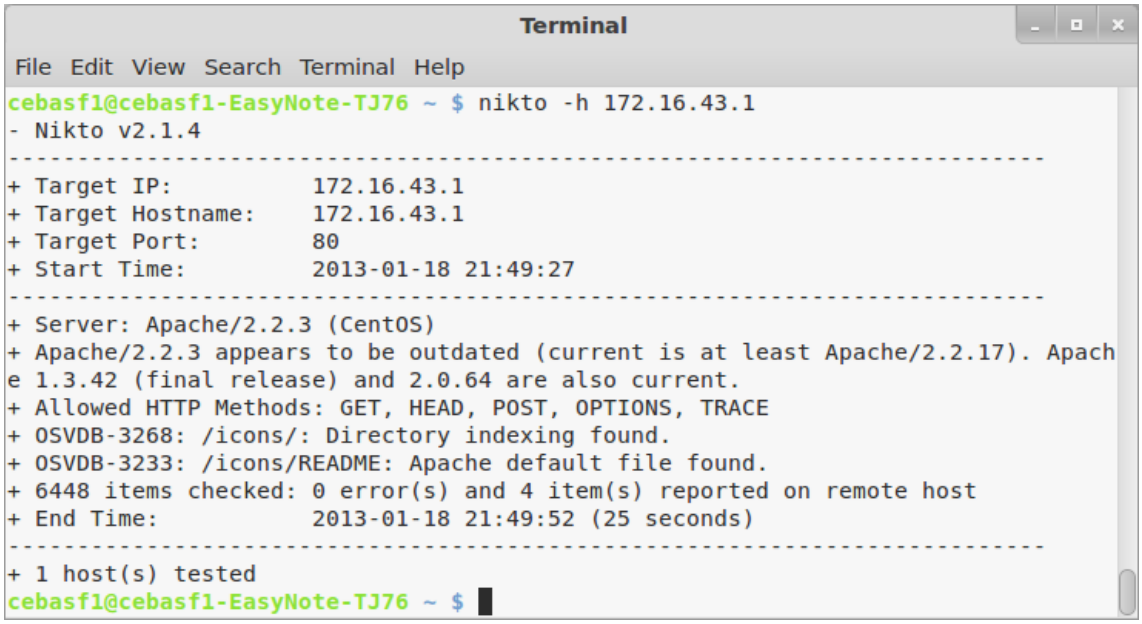


Figura 62. Resultado de servidor Proxy Energía según Nikto

En el caso del servidor Proxy Energía podemos observar que en los 2 resultados hay similitudes en vulnerabilidades.

Al comparar los resultados del servidor Firewall, **Ver** Figura 63 y 64, los 2 scanner no detectaron vulnerabilidades en este servidor.

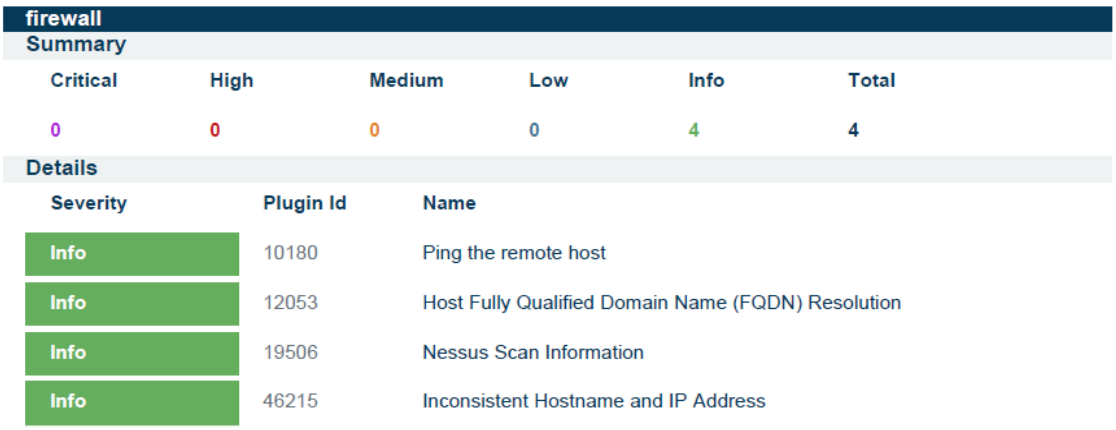


Figura 63. Resultado de servidor Firewall según Nessus

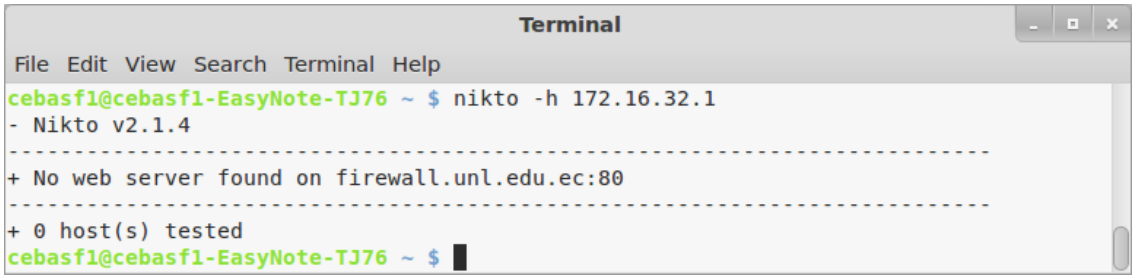


Figura 64. Resultado de servidor Firewall según Nikto

2.3.1. RESULTADOS ACTUALES DE VULNERABILIDADES EN LOS SERVIDORES DE LA UTI

Para la obtención de los siguientes resultados se utilizó las herramientas para análisis de vulnerabilidades denominadas NESSUS y NIKTO, **Ver** Anexo VI.

Las vulnerabilidades lógicas se las clasificó en 5 niveles de criticidad, **Ver** Figura 65, para su mejor comprensión:

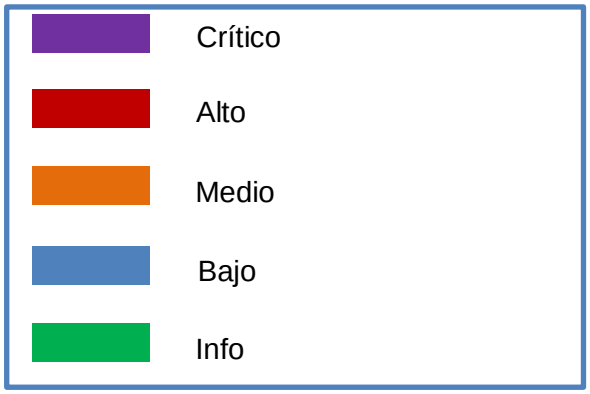


Figura 65 Colores de vulnerabilidades según criticidad

Los resultados actuales de los Servidores de forma general se detallan en Figura 66:

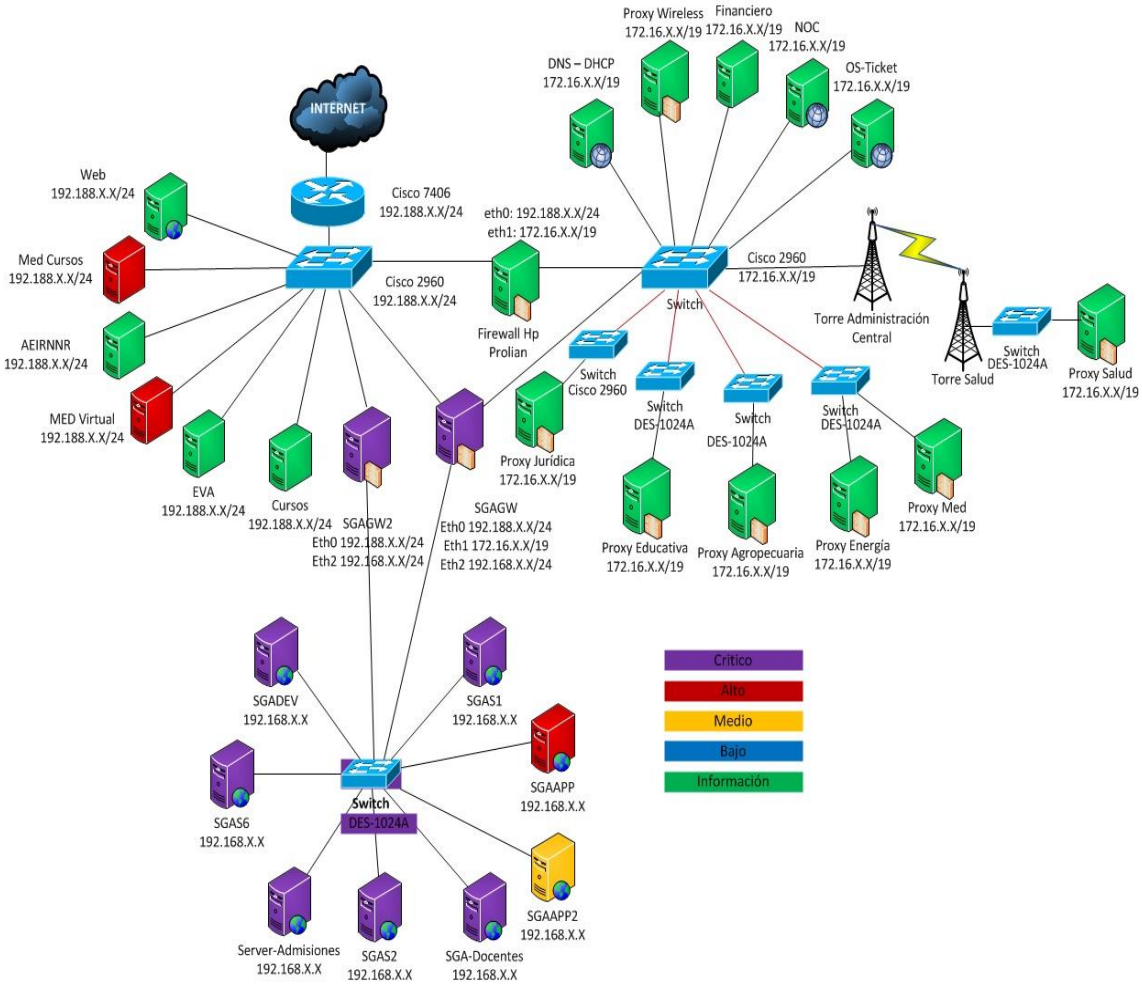


Figura 66 Vista general Servidores

A continuación se resumen los resultados de forma general, divididos en Servidores Privados, Públicos y Servidores del SGA:

2.3.1.1. Servidores Privados

La Figura 67 describe la situación de los servidores luego de solucionadas las vulnerabilidades lógicas, el color verde implica que el scanner realizado solo muestra información básica que no compromete el funcionamiento de los servidores.

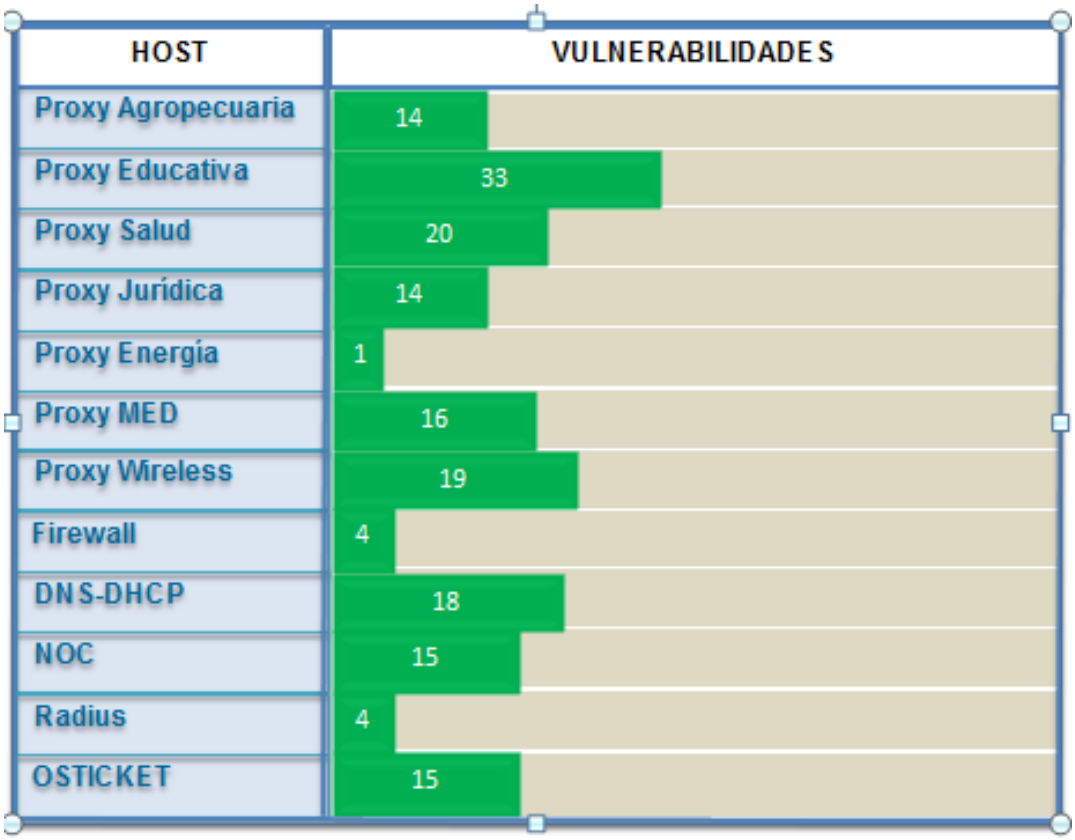


Figura 67 Vista General de Vulnerabilidades Servidores Privados

2.3.1.2. Servidores Públicos

En la Figura 68 se muestra el estado en que quedaron los servidores públicos después de intervenirlos para solucionar sus vulnerabilidades:

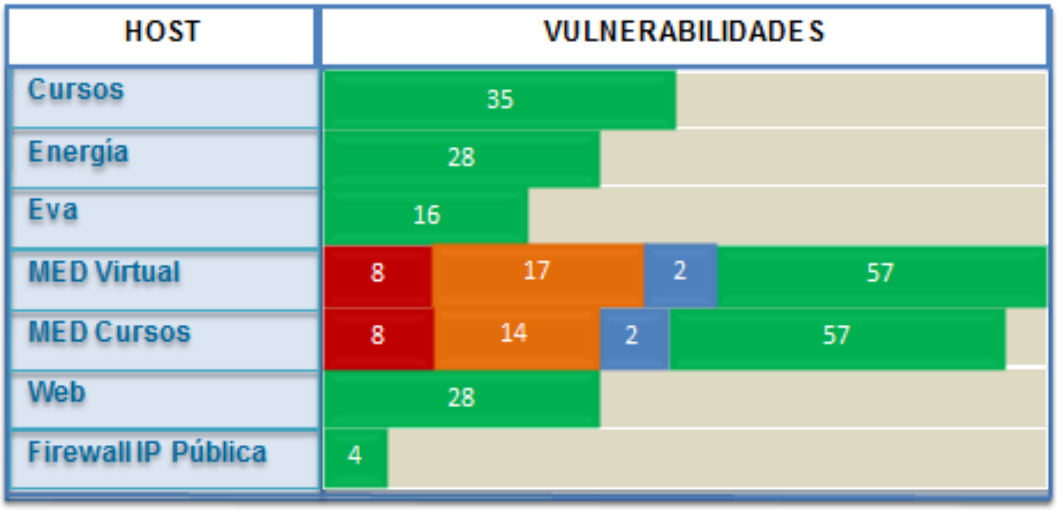


Figura 68 Vista General de Vulnerabilidades Lógicas servidores Públicos

Los Servidores Públicos de Modalidad de Estudios a Distancia (MED) están ubicados físicamente en la Sala de Servidores, pero no están a cargo de ninguna de las secciones de la UTI, al no permitir manipular ningún archivo, se notificó al encargado de dichos servidores mediante un informe, para que proceda a solucionar las vulnerabilidades encontradas si así lo considera pertinente, **Ver** ANEXO VIII.

En las Tabla XXXII y XXXIII, se detallan las vulnerabilidades lógicas de los servidores MED:

Med-Cursos

TABLA XXXII Descripción de Vulnerabilidades Servidor Med-Cursos

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
PHP < 5.2.2 Information Disclosure Versión de PHP detectada en el servidor es 5.1.6	80/tcp	Alto
PHP expose_php Information Disclosure	80/tcp	Alto
PHP < 5.3.9 Multiple Vulnerabilities	80/tcp	Medio
SSL Certificate Cannot Be Trusted	443/tcp	Medio
SSL Self-Signed Certificate	443/tcp	Medio
SSL Certificate with Wrong Hostname	443/tcp	Medio
PHP expose_php Information Disclosure	80/tcp	Medio
HTTP TRACE / TRACK Methods Allowed	80/tcp	Medio
SSL Medium Strength Cipher Suites Supported	443/tcp	Medio
Web Server Uses Plain Text Authentication Forms	80/tcp	Bajo
CGI Generic Injectable Parameter	80/tcp	Bajo

Med-Virtual

TABLA XXXIII Descripción de Vulnerabilidades Servidor Med-Virtual

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
PHP < 5.2.2 Information Disclosure Versión de PHP detectada en el servidor es 5.1.6	80/tcp	Alto
PHP expose_php Information Disclosure	80/tcp	Alto
PHP < 5.3.9 Multiple Vulnerabilities	80/tcp	Medio
SSL Certificate Cannot Be Trusted	443/tcp	Medio
SSL Self-Signed Certificate	443/tcp	Medio
SSL Certificate Expiry	443/tcp	Medio
Adobe Dreamweaver dwsync.xml Remote Information Disclosure	80/tcp	Medio
SSL Certificate with Wrong Hostname	443/tcp	Medio
Web Application Information Disclosure	80/tcp	Medio
PHP expose_php Information Disclosure	80/tcp	Medio
HTTP TRACE / TRACK Methods Allowed	80/tcp	Medio
SSL Medium Strength Cipher Suites Supported	443/tcp	Medio
Web Server Uses Plain Text Authentication Forms	80/tcp	Bajo
CGI Generic Injectable Parameter	80/tcp	Bajo

2.3.1.3. Servidores del Sistema de Gestión Académica

La Figura 69 muestra según el nivel de criticidad los servidores afectados por vulnerabilidades:

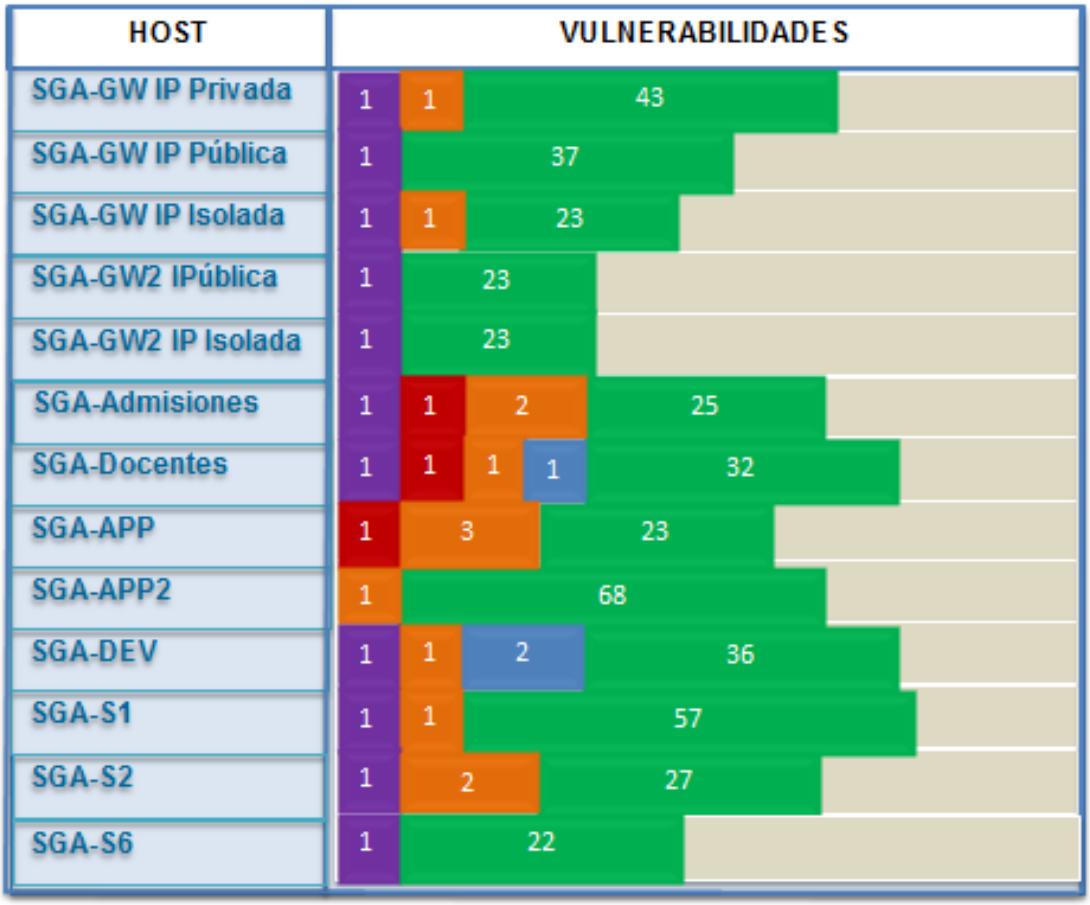


Figura 69 Vista General de Vulnerabilidades de los servidores del SGA

Se detalla a continuación las vulnerabilidades lógicas de los servidores del SGA, y los puertos afectados:

SGA -GW (IP Privada)

TABLA XXXIV Descripción de Vulnerabilidades Servidor SGA-GW (Ip Privada)

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
DHCP Server Detection	67/udp, 80/udp	Media

SGA -GW (IP Pública)

TABLA XXXV Descripción de Vulnerabilidades Servidor SGA-GW (Ip Pública)

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica

SGA -GW (IP Red Isolada)

TABLA XXXVI Descripción de Vulnerabilidades Servidor SGA-GW (Ip Red Isolada)

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
DHCP Server Detection	67/udp, 80/udp	Media

SGA-Gw2 (Ip Pública)

TABLA XXXVII Descripción de Vulnerabilidades Servidor SGA-GW2 (Ip Pública)

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica

SGA-Gw2 (Ip Red Isolada)

TABLA XXXVIII Descripción de Vulnerabilidades Servidor SGA-GW2 (Ip Red Isolada)

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica

SGA -Admisiones

TABLA XXXIX Descripción de Vulnerabilidades Servidor SGA-ADMISIONES

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica

SGA-Docentes

TABLA XL Descripción de Vulnerabilidades Servidor SGA-DOCENTES

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
Secure HyperText Transfer Protocol (S-HTTP) Detection	8080/tcp 8085/tcp	Medio
Web Server Uses Basic Authentication Without HTTPS	83/tcp	Bajo

SGA-APP

TABLA XLI Descripción de Vulnerabilidades Servidor SGA-APP

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Secure HyperText Transfer Protocol (S-HTTP) Detection	8080/tcp 8081/tcp 8082/tcp 8083/tcp 8087/tcp 8090/tcp	Medio

SGA-APP2

TABLA XLII Descripción de Vulnerabilidades Servidor SGA-APP2

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Secure HyperText Transfer Protocol (S-HTTP) Detection	8081/tcp	Medio

SGA-DEV

TABLA XLIII Descripción De Vulnerabilidades Servidor SGA-DEV

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
Secure HyperText Transfer Protocol (S-HTTP) Detection	8000/tcp	Medio
Web Server Uses Plain Text Authentication Forms	80/tcp	Bajo
Web Server Uses Basic Authentication Without HTTPS	80/tcp	Bajo

SGA-S1

TABLA XLIV Descripción de Vulnerabilidades Servidor SGA-S1

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
Secure HyperText Transfer Protocol (S-HTTP) Detection	8086/tcp 8092/tcp	Medio

SGA-S2

TABLA XLV Descripción de Vulnerabilidades Servidor SGA-S2

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica
Secure HyperText Transfer Protocol (S-HTTP) Detection	8081/tcp	Medio

SGA-S6

TABLA XLVI Descripción de Vulnerabilidades Servidor SGA-S6

VULNERABILIDAD	PUERTO	NIVEL DE RIESGO
Unsupported Unix Operating System Debian 5.0		Critica

2.3.1.4. Resumen y descripción de Vulnerabilidades

En todos los servidores se comparó los resultados obtenidos con los scanners NESSUS y NIKTO y se las resumió en la Tabla XLVII con su respectiva descripción e impacto:

TABLA XLVII Descripción de las Vulnerabilidades encontradas en los Servidores

VULNERABILIDAD	DESCRIPCIÓN	IMPACTO
Web Server Uses Plain Text Authentication Forms	El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'password' que transmiten su información a un servidor web remoto en texto no cifrado.	Un atacante que capture el tráfico entre el navegador web y el servidor puede obtener nombres de usuario y contraseñas válidos de usuarios.
Unsupported Unix Operating System	De acuerdo con su versión Debian 5.0, el control remoto del sistema operativo Unix es obsoleto y ya no se mantiene por su vendedor o proveedor.	Lo que implica que no hay nuevos parches de seguridad y que el servidor está expuesto a posibles ataques.
FTP Supports Clear Text Authentication	Las credenciales de autenticación pueden ser interceptadas. El servidor FTP remoto permite que el nombre de usuario y contraseña que se transmitan en texto no cifrado,	Podría ser interceptado por un sniffer de red y robar usuarios y contraseñas del sistema
Web Server Uses Basic Authentication Without HTTPS	El servidor web remoto contiene las páginas web que están protegidos por autenticación 'Básica' a través de texto no cifrado.	Un atacante puede obtener nombres de usuario y contraseñas de los usuarios válidos.
Secure HyperText Transfer Protocol (S-HTTP) Detection	El servidor web remoto cifra el tráfico utilizando un protocolo obsoleto. El servidor web remoto acepta	Robo de Información

	conexiones cifradas mediante Secure Hypertext Transfer Protocol (S-HTTP), una capa de cifrado que fue definido en 1999 por RFC 2660.	
DHCP Server Detection	El script intenta recuperar la información sobre el diseño de la red. Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS[26], o la información de red tal disposición como la lista de los servidores de la red web, y así sucesivamente. No demuestra ninguna vulnerabilidad, pero un atacante local puede utilizar DHCP para estar íntimamente familiarizado con la asociación de la red.	

2.3.2. RESULTADOS HISTÓRICOS DE VULNERABILIDADES EN LOS SERVIDORES DE LA UTI

El resultado general del análisis realizado a los servidores mediante las herramientas nessus y Nikto, **Ver** Figura 70, son los siguientes:

[26] **NIS:** Guarda la información de la base de datos en ficheros llamados *mapas*, que contienen pares clave-valor. Un ejemplo de par clave-valor es el identificativo de un usuario (username) y la forma encriptada de su contraseña.

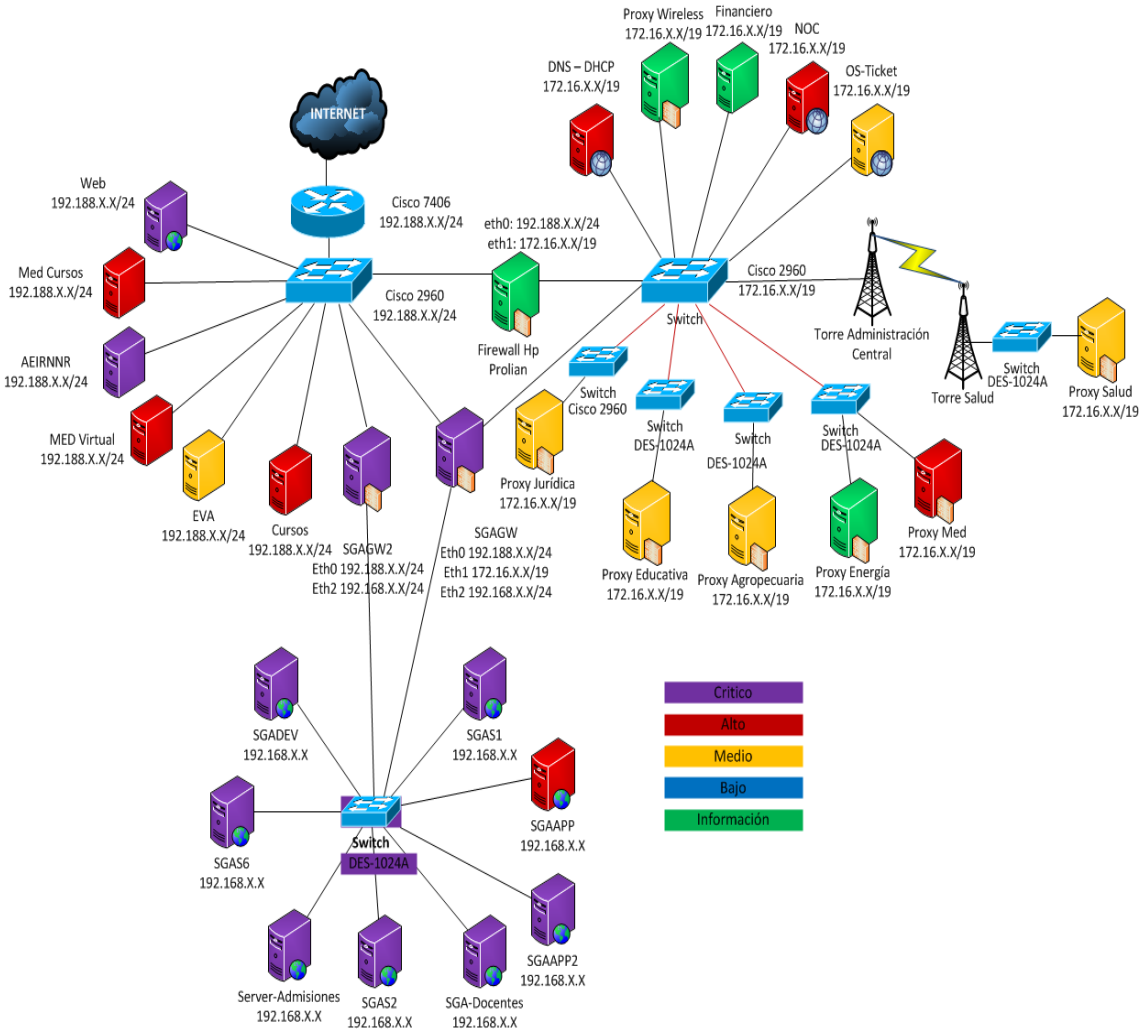


Figura 70 Vista general Servidores Histórica

El estado en el que se encontraron los servidores Privados, Públicos y del SGA al inicio del presente proyecto de tesis es el siguiente:

2.3.2.1. Servidores Privados

La Figura 71 muestra el estado de los servidores públicos al inicio de nuestro análisis:

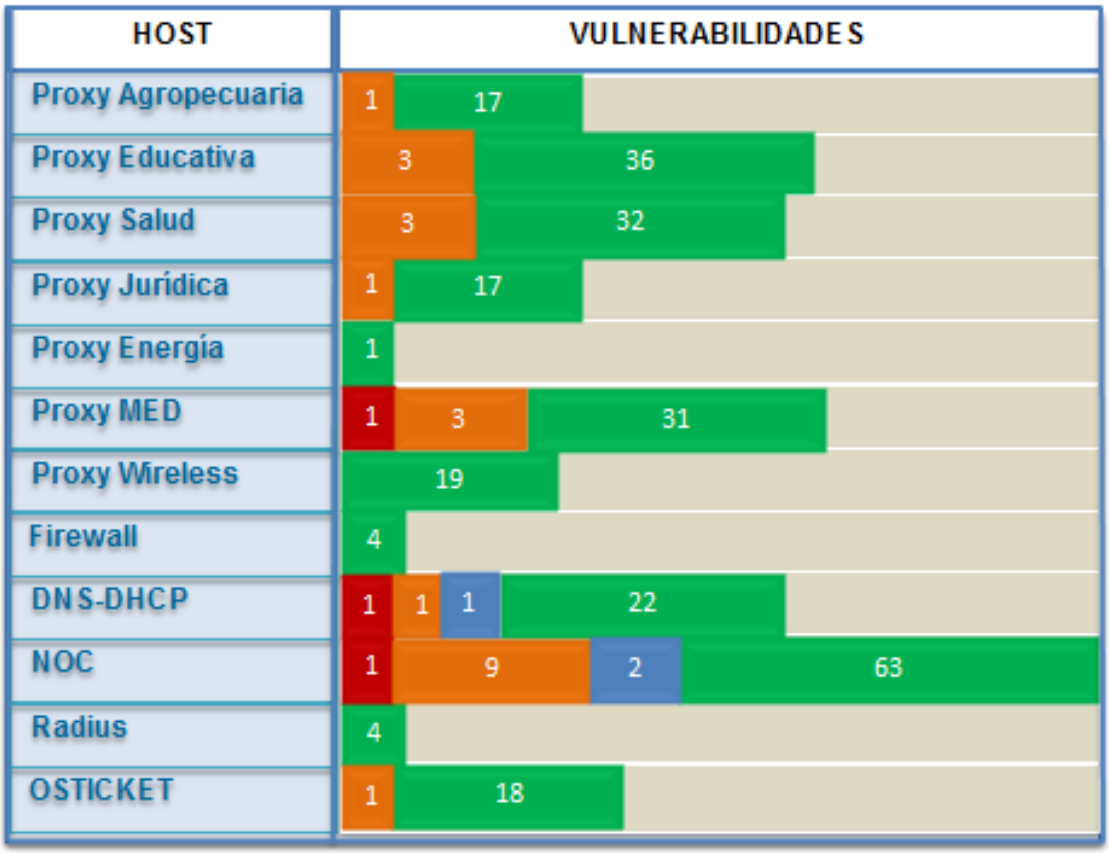


Figura 71 Vista General Vulnerabilidades Servidores Privados Históricos

2.3.2.2. Servidores Públicos

Estos servidores estaban muy afectados por múltiples vulnerabilidades, debido a que no se los actualiza periódicamente los resultados fueron, **Ver** figura 72:

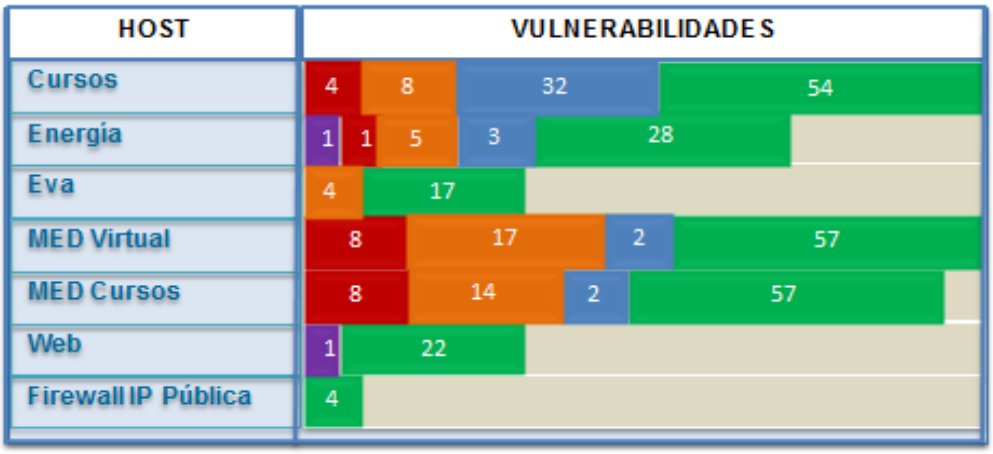


Figura 72 Vista General Vulnerabilidades Servidores Públicos Históricos

2.3.2.3. Servidores del Sistema de Gestión Académica

En la Figura 73 podemos apreciar una panorámica general del estado en que estuvieron estos servidores del Sistema de Gestión Académica:

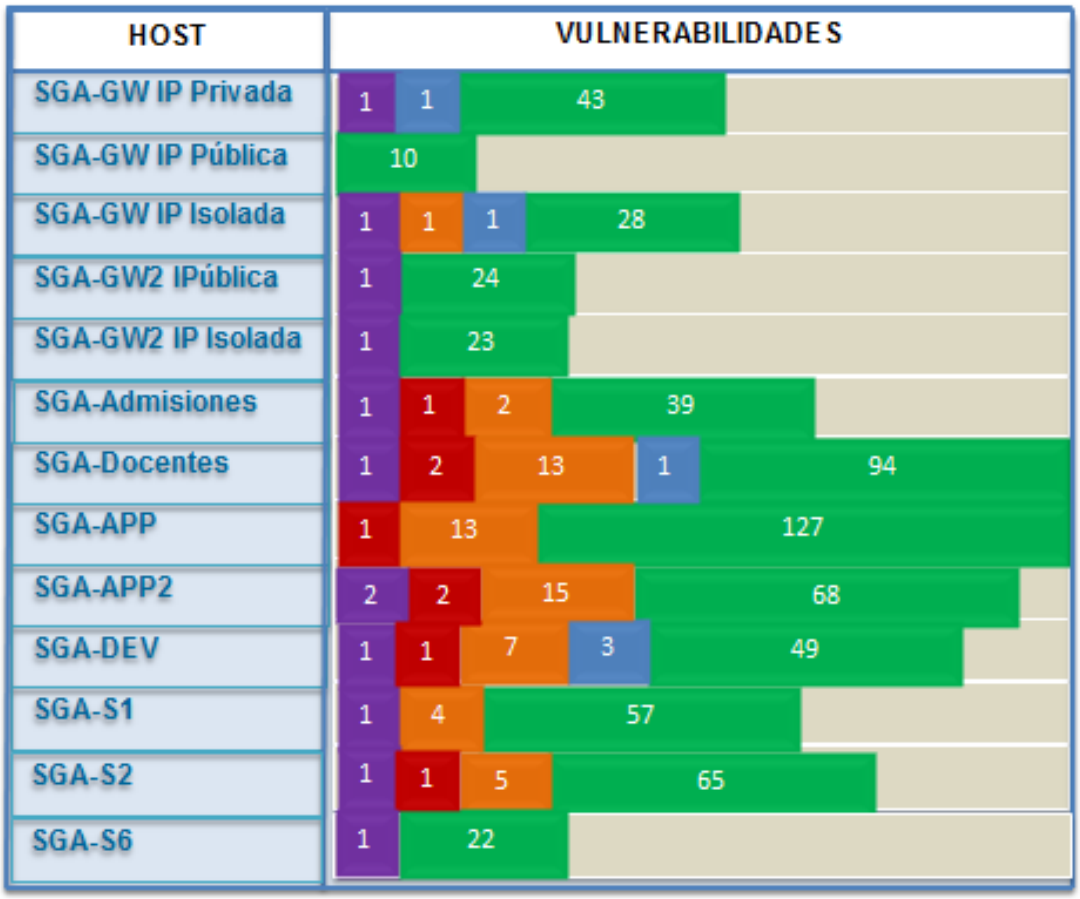


Figura 73 Vista General Vulnerabilidades Servidores del SGA Históricos

Las vulnerabilidades detalladas en la Tabla XLVIII fueron detectadas con la herramienta NESSUS, todas estas vulnerabilidades fueron solucionadas mediante la implementación de IPTABLES, **Ver** Anexo VII, y la actualización de varios servicios en los servidores como Apache, PHP, Moodle y sistemas operativos obsoletos, **Ver** Página 165-189, excepto los servidores que pertenecen a la Sección de Desarrollo de Software por cuestiones de confidencialidad, **Ver** Anexo XI, ya que en esta sección se manejan Datos muy importante de alumnos y docentes.

TABLA XLVIII Vulnerabilidades Históricas de los Servidores

VULNERABILIDAD	IMPACTO	PUERTOS
Web Server Generic XSS	Robo de Información	8080/tcp
HTTP TRACE / TRACK Methods Allowed	Robo de Información	80/tcp, 83/tcp
Apache HTTP Server httpOnly Cookie Information Disclosure	Robo de Información y saturación del sistema.	80/tcp, 83/tcp
Apache HTTP Server Byte Range DoS	Saturación del sistema	80/tcp, 83/tcp
SNMP Agent Default Community Name (public)	Robo de Información	161/udp
mDNS Detection	Robo de información	5353/udp
DNS Server Cache Snooping Remote Information Disclosure	Esta vulnerabilidad puede causar la divulgación de información importante sobre la institución.	53/udp
PHP < 5.3.9 Multiple Vulnerabilities	Robo de información y saturación del sistema.	80/udp, 80/tcp, 443/tcp
DHCP Server Detection	El servidor DHCP remoto puede exponer información acerca de la asociación de la red	67/udp, 80/udp
PHP expose_php Information Disclosure	Los Eastern Eggses código oculto que al desencadenarse genera utilidades, juegos, imágenes y demás, que vienen escondidos en el software.	80/udp, 80/tcp, 443/tcp
Web Application Information Disclosure	Robo de información a través de rutas a directorios del servidor.	80/tcp, 83/tcp, 85/tcp, 8085/tcp
Web Server Uses Plain Text	Un atacante que capture el	80/tcp, 443/tcp

Authentication Forms	tráfico entre el navegador web y el servidor puede obtener nombres de usuario y contraseñas válidos de usuarios.	
CGI Generic Injectable Parameter	Intrusos abusan de los programas CGI para modificar páginas Web, robar información de tarjetas de crédito e instalar puertas traseras que les servirán para posteriormente tener acceso a los sistemas comprometidos.	80/tcp, 443/tcp
Unsupported Unix Operating System	Lo que implica que no hay nuevos parches de seguridad y que el servidor está expuesto a posibles ataques.	
IP Forwarding Enabled	Un atacante podría usar este error para utilizar la ruta de paquetes a través de este y potencialmente evitar algunos firewalls / routers / filtrado NAC.	
SSL Certificate Cannot Be Trusted	Un atacante podría robar las credenciales SSL	443/tcp
SSL Self-Signed Certificate	Los certificados auto firmados no puede por naturaleza ser revocado, lo que puede permitir a un atacante que ya ha obtenido acceso a monitorear e inyectar datos en una conexión y suplantar una identidad si una clave privada	443/tcp

	ha sido comprometida.	
SSL Medium Strength Cipher Suites Supported	Robo de información	443/tcp
FTP Supports Clear Text Authentication	Podría ser interceptado por un sniffer de red y robar usuarios y contraseñas del sistema	21/tcp
Apache APR apr_palloc Heap Overflow	Saturación del sistema	80/tcp, 443/tcp
Moodle < 1.9.6 Multiple Vulnerabilities	Robo de Información.	80/tcp, 443/tcp
Apache < 2.2.17 Multiple Vulnerabilities	Robo de información y saturación del sistema.	80/tcp, 443/tcp
YUI charts.swf / swfstore.swf / uploader.swf XSS	Con esta vulnerabilidad se podrían realizar los siguientes ataques: • Direcciones de correo podrían ser cambiadas sin confirmación. • Acceso a perfiles de usuarios borrados. • Potencial inyección SQL en código de eventos. • Potencial XSS no persistente al buscar usuarios pertenecientes a un grupo (solo MSSQL y Oracle). • Inyección SQL en el módulo HotPot	80/tcp, 443/tcp
Multiple Web Server printenv CGI Information Disclosure	Esto da una información atacante como el directorio de instalación,	80/tcp, 443/tcp

	la dirección IP del servidor (lo cual es interesante si se implementa NAT), el administrador del servidor de e-mail, las versiones de servidores y módulos, las variables de entorno de shell	
Apache APR apr_fnmatch DoS	Robo de información y saturación del sistema.	80/tcp, 443/tcp
Apache mod_proxy_ajp DoS	Existe un error en el módulo 'mod_proxy_ajp[27]' que puede permitir peticiones HTTP especialmente diseñada para causar un estado de error en el servidor backend. Esta vulnerabilidad sólo se produce cuando 'mod_proxy_ajp' se utiliza junto con 'mod_proxy_balance[28]'.	80/tcp, 443/tcp
Web Server Uses Basic Authentication Without HTTPS	Un atacante puede obtener nombres de usuario y contraseñas de los usuarios válidos.	83/tcp, 80/tcp, 443/tcp
Backup Files Disclosure	Añadiendo diferentes sufijos (p. ej. ie: .old, .bak, ~, etc...) para los nombres de varios archivos en la máquina remota, parece posible recuperar su contenido, lo que puede dar lugar a la revelación de	80/tcp

[27] **mod_proxy_ajp** : Conector para Apache y Tomcat
[28] **mod_proxy_balance:** Soporte para el balance de carga del proxy en Apache

	información confidencial.	
SSL Certificate with Wrong Hostname	Robo de información	443/tcp
SSL CertificateExpiry	Robo de información	443/tcp
PHP < 5.3.5 String To Double Conversion DoS	Saturación del sistema.	80/tcp
PHP < 5.2.2 Information Disclosure	Robo de Información	80/tcp
Adobe Dreamweaver dwsync.xml Remote Information Disclosure	Esto puede provocar la divulgación de información.	80/tcp
.svn/entries Disclosed via Web Server	Este fallo también puede ser usado para descargar el Código fuente de los scripts (PHP, JSP, etc.) alojada en el servidor remoto.	83/tcp, 85/tcp, 8085/tcp, 81/tcp, 82/tcp, 86/tcp, 8080/tcp, 8081/tcp, 8090/tcp.
Secure HyperText Transfer Protocol (S-HTTP) Detection	Robo de Información	8080/tcp, 8085/tcp, 8081/tcp, 8082/tcp, 8083/tcp, 8087/tcp, 8090/tcp, 8000/tcp, 8086/tcp, 8092/tcp
NFS Exported Share Information Disclosure	Pérdida de confidencialidad, pérdida de la integridad	2049/udp
SQL Dump Files Disclosed via Web Server	Robo de información	80/tcp


Fase III
Explotación y Solución Vulnerabilidades

3. EXPLOTACIÓN Y SOLUCIÓN DE VULNERABILIDADES LÓGICAS

La fase 3 Explotación y solución de vulnerabilidades lógicas abarca el siguiente objetivo:

Objetivo 1: Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Objetivo 1:

IMPLANTAR LAS SOLUCIONES DE LAS SEGURIDADES LÓGICAS EN LOS SERVIDORES BAJO LA SUPERVISIÓN DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA.

3.1. EXPLOTACIÓN DE VULNERABILIDADES LÓGICAS

Se obtuvo vulnerabilidades lógicas realizando pruebas a nivel de interno es decir desde la intranet ya que externamente no se obtuvo ningún resultado lo que prueba que los servidores están bien protegidos de ataques externos gracias al firewall lógico que poseen actualmente.

En esta fase se realizó la explotación de ciertas vulnerabilidades lógicas detectadas previamente como Secure HyperText Transfer Protocol (S-HTTP) Detection, Web Server Uses Basic Authentication Without HTTPS, FTP Supports Clear Text Authentication y Web Server Uses Plain Text Authentication Forms, todas estas vulnerabilidades son causadas porque la información que viaja en la red se transporta mediante el uso protocolos inseguros, para explotar dichas vulnerabilidades utilizamos el Snniffer denominado Cain y Abel.

Un sniffer captura los paquetes que envía nuestra Red (ya sea una computadora en la LAN o nuestro PC), en esos paquetes transporta toda la información que se envía por Internet, así como usuarios y contraseñas de muchos servicios de Internet. Algunos de estos servicios que utilizan usuarios y contraseñas, o datos confidenciales, están encriptados o codificados para que no se puedan leer. Muchos otros como el servicio de FTP (File Transfer Protocol) viajan en texto plano, de manera que cualquiera que intercepte esos paquetes puede llegar a interpretar los datos.

Se realizó un escaneo de la red para determinar los servidores objetivo que serán para este caso un servidor del SGA (192.188.x.x) y el servidor EVA (192.188.x.x), **Ver** Figura 74. Este escaneo nos revela que también los servidores del SGA tienen la Vulnerabilidad de DHCP Server Detection que cualquier atacante podría utilizar para familiarizarse con la red.

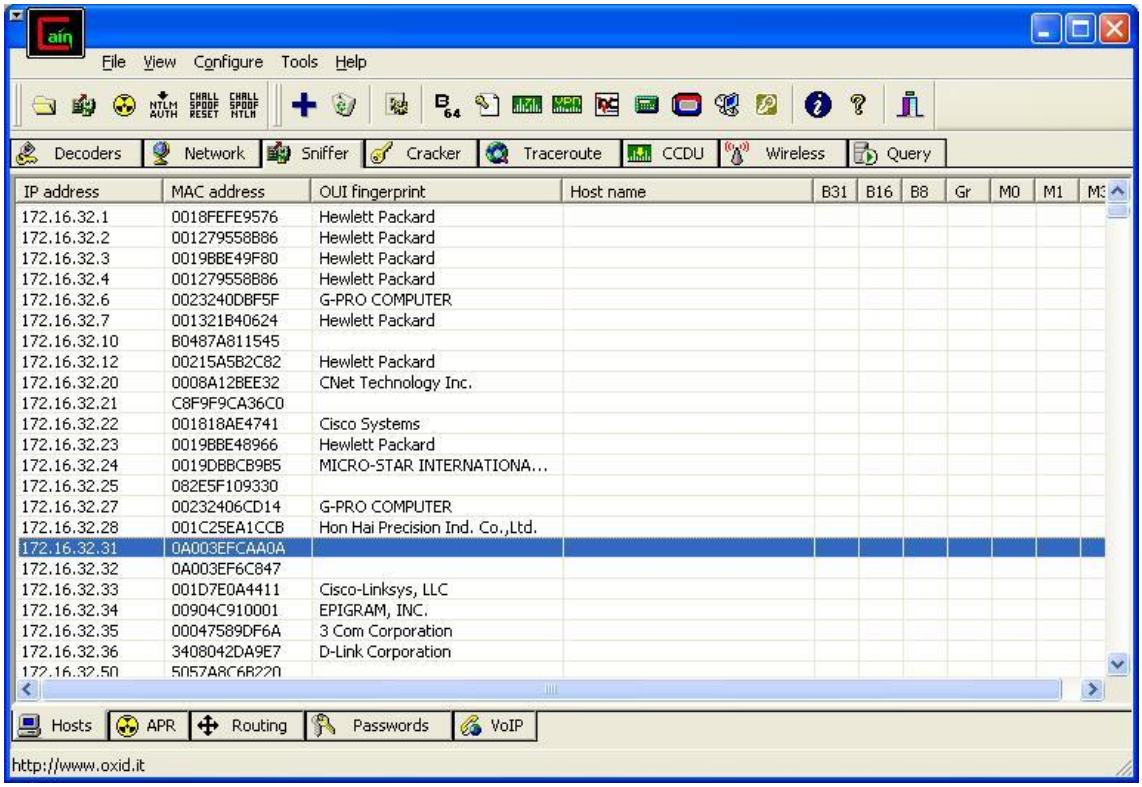
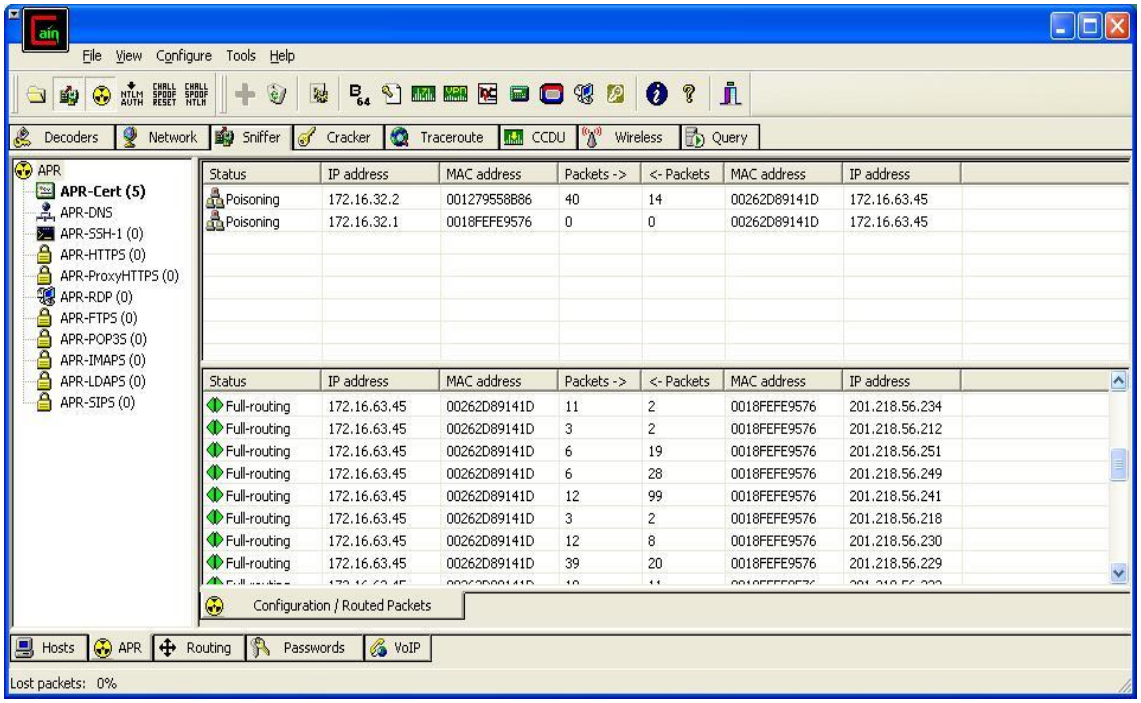


Figura 74. Escaneo del servidor con Cain y Abel

Una vez determinados las máquinas objetivo se procedió a realizar la configuración para capturar las contraseñas en estos servidores y probar las vulnerabilidades antes mencionadas primeramente se debe seleccionar la puerta de enlace y el DNS-DHCP y realizar el respectivo envenenamiento de paquetes (poison), **Ver** Figura 75.



Figuro 75. Configuración de Cain y Abel

Podemos ver en la Figura 75, el aviso de Full-routing, significa que el ataque snniffer ha tenido éxito, y cuando el usuario acceda con algunas credenciales, como HTTP, FTP, quedarán registradas en Cain y Abel, **Ver** Figura 76 y 77.

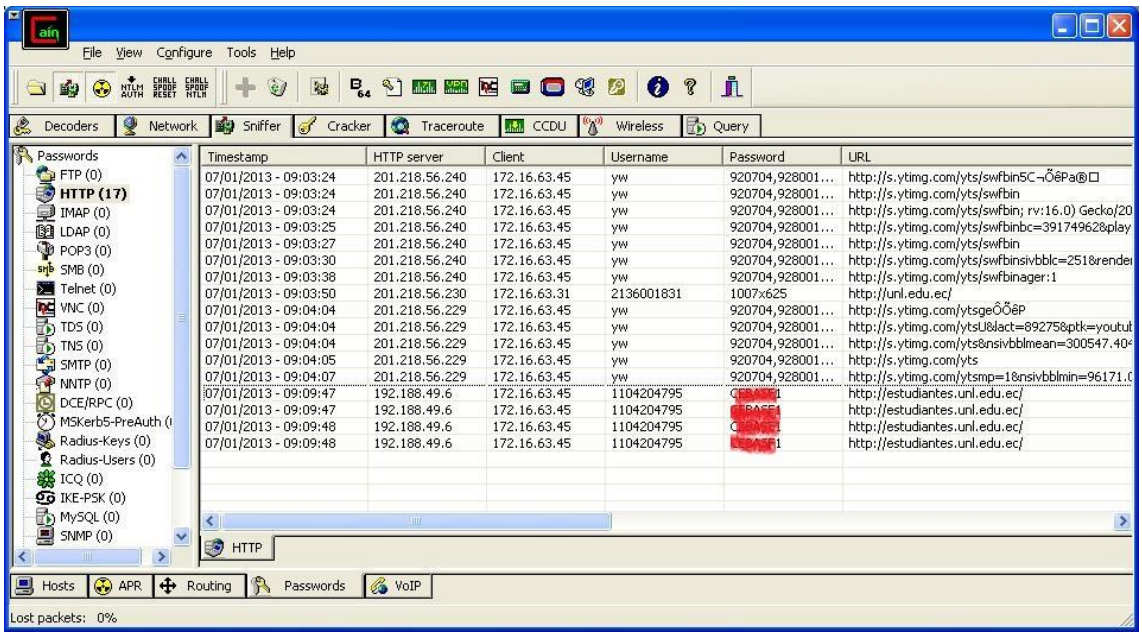


Figura 76. Descifrado de clave con Cain y Abel servidor SGA

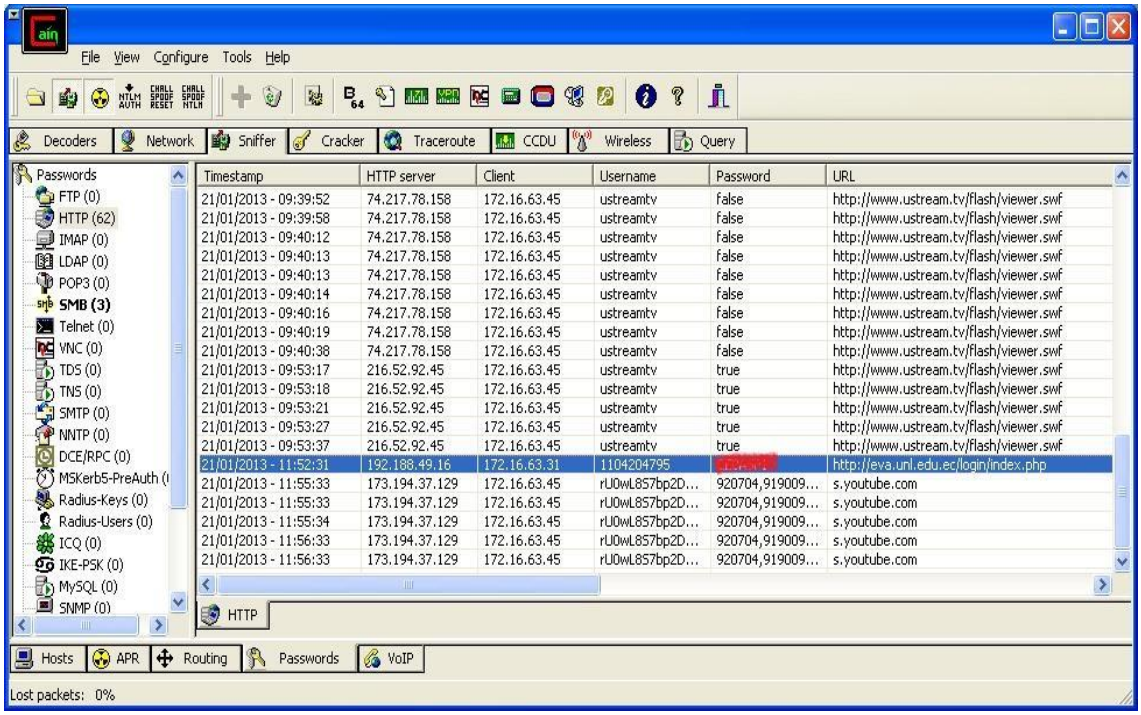


Figura 77. Descifrado de clave con Cain y Abel servidor EVA

3.2. LISTA DE SOLUCIONES A LAS VULNERABILIDADES LÓGICAS DE LOS SERVIDORES

Las siguientes tareas se llevaron a cabo bajo la supervisión de la Unidad de Telecomunicaciones e Información, cabe recalcar que en todos los servidores en los que se solucionaron vulnerabilidades se procedió a actualizar primeramente todos los servicios con los siguientes comandos:

CENTOS	***DEBIAN O UBUNTU***
`yum update`	`apt-get update`
`yum upgrade`	`apt-get upgrade`

A continuación se explica el procedimiento para solucionar las vulnerabilidades lógicas encontradas, **Ver** Tabla XLIX:

TABLA XLIX Soluciones a las Vulnerabilidades Lógicas

VULNERABILIDAD	SOLUCIÓN
Web Server Generic XSS	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado es el 8080 **PROCEDIMIENTO** 1. Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* 2. Habilitamos el Puerto 8080 para permitir navegación de la INTRANET. **Ver** Anexo VII *iptables -A INPUT -s $INTRANET[29] -d $IPORIGEN -i eth0 -p tcp -m tcp --sport 1024: --dport 8080 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN[30] -d $INTRANET -o eth0 -p tcp -m tcp --sport 8080 --dport 1024: -j ACCEPT*
HTTP TRACE / TRACK Methods Allowed	Deshabilitar el método trace/track en http **PROCEDIMIENTO** Para deshabilitar el método trace/track en http, se debe editar el archivo httpd.conf en la siguiente ruta: *sudo vim /etc/httpd/conf/httpd.conf* Copiar el siguiente código al final del archivo: *RewriteEngine on* *RewriteCond %{REQUEST_METHOD} ^TRACE* *RewriteRule .* – [F]*
Apache HTTP Server	Esta vulnerabilidad afecta a versiones inferiores a la

[29] **INTRANET**: 172.16.32.0/19
[30] **IPORIGEN:** Ip del servidor

httpOnly Cookie Information Disclosure	versión 2.2.22. Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
Apache HTTP Server Byte Range DoS	Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.22. Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con:

	yum upgrade (Centos) *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
SNMP Agent Default Community Name (public)	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado que es el 161. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 161. **Ver** Anexo VII *iptables -A INPUT -s $IPDESTINO[31] -d $IPORIGEN -i eth0 -p udp -m udp --sport 1024: --dport 161 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN -d $IPDESTINO* *-o eth0 -p udp -m udp --sport 161 --dport 1024: -j ACCEPT*
mDNS Detection	Este problema se origina porque en Linux viene Avahi instalado por defecto, Avahi permite detectar automáticamente los recursos de una red local y conectarse a ella. Avahi se ocupa de: asignar automáticamente una dirección IP incluso sin presencia de un servidor

[31] **IPDESTINO:** IP del servidor que realiza la petición

	DHCP, hacer la función de DNS (cada máquina es accesible con el nombre nombreMaquina.local), hacer una lista de los servicios y acceder a ellos fácilmente (las máquinas de la red local son informadas de la llegada o salida de un servicio). Esto facilita el uso compartido de archivos, impresoras, etc. Avahi es una implementación del protocolo ZeroConf compatible con Rendezvous, Bonjour de Apple. Por lo tanto es necesario deshabilitarlo en los servidores afectados: **PROCEDIMIENTO** Eliminar los enlaces hacia daemon: *sudo update-rc.d -f avahi-daemon remove* *(Debian o Ubuntu)* */sbin/chkconfig avahi-daemon off* *(Centos)*
DNS Server Cache Snooping Remote Information Disclosure	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado que es el 53 **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 53 para resolución de DNS. **Ver** Anexo VII *iptables -A INPUT -s $DNSINTRANET [32] -d $IPORIGEN -i eth0 -p udp -m udp --sport 53 --dport 1024: -j ACCEPT*

[32] **DNSINTRANET:** 172.16.32.2

	iptables -A OUTPUT -s $IPORIGEN -d $DNSINTRANET -o eth0 -p udp -m udp --sport 1024: --dport 53 -j ACCEPT
PHP < 5.3.9 Multiple Vulnerabilities	Actualizar a PHP 5.3.9 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo la versión de PHP en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de PHP aplicar el siguiente comando: *yum -y update php (Centos)* *apt-get install php5 (Ubuntu o Debian)*
DHCP Server Detection	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 67 y 68. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 67 Y 68 para acceso de

	usuarios. **Ver** Anexo VII *iptables -A INPUT -s $INTRANET -d $IPORIGEN -i eth0 -p udp --sport 67:68 --dport 67:68 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN -d $INTRANET -o eth0 -p udp --sport 67:68 --dport 67:68 -j ACCEPT*
PHP expose_php Information Disclosure	En la configuración de PHP archivo php.ini, establezca el valor de 'expose_php' a 'Off' para desactivar este comportamiento. **PROCEDIMIENTO** Editar el archivo php.ini en la siguiente ruta: *sudo vim/etc/php.ini (Centos)* *sudo vim/etc/php5/apache2/php.ini (Ubuntu o Debian)* Buscar expose_php en el archivo, generalmente viene configurado por defecto en *[On/Off]* y para desactivar este valor cambiar *[Off/On]*: *expose_php = [Off/On]*
Web Application Information Disclosure	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 80 para permitir navegación del proxy. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s*

	$CERO[33] *-d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*
Web Server Uses Plain Text Authentication Forms	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 80 para permitir navegación del proxy. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*
CGI Generic Injectable Parameter	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 80 para permitir navegación del

[33] **CERO:** 0.0.0.0/0

	proxy. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*
Unsupported Unix Operating System Debian 5.0	Actualizar sistema operativo a Debian 6.0. Última versión estable. **PROCEDIMIENTO** 1. Para ello tecleamos en la terminal *sudo vim /etc/apt/sources.list* 2. Esto abre nuestra lista de repositorios lo que haremos será sustituir todos los "lenny" por "squeeze" el resultado debe quedar así: *#REPOSITORIOS OFICIALES* *deb http://ftp.fr.debian.org/debian/ squeeze main* *deb-src http://ftp.fr.debian.org/debian/ squeeze main* *#REPOSITORIOS SEGURIDAD* *deb http://security.debian.org/ squeeze/updates main* *deb-src http://security.debian.org/ squeeze/updates main* *#REPOSITORIOS MULTIMEDIA* *deb http://www.debian-multimedia.org/*

	squeeze main *deb-src http://www.debian-multimedia.org/ squeeze main* 3. Guardar los cambios y aplicar el siguiente comando *aptitude update && aptitude full-upgrade*
IP Forwarding Enabled	Deshabilitar esta opción en el servidor si no es necesaria. **PROCEDIMIENTO** Editar el archivo el sysctl.conf en la siguiente ruta: *sudo vim /etc/sysctl.conf* Añadir o cambiar la siguiente opción: *net.ipv4.ip_forward = 0* Para activar los cambios realizados en el fichero debemos ejecutar: *sysctl -p /etc/sysctl.conf*
SSL Certificate Cannot Be Trusted	No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 443. **Ver** Anexo VII **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s*

	$CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
SSL Self-Signed Certificate	No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 443. **Ver** Anexo VII **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
SSL Medium Strength Cipher Suites Supported	No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 443. **Ver** Anexo VII

	Puerto 443 *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
FTP Supports Clear Text Authentication	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 21 y 22. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el Puerto 21 y 22 para proxy. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 20:21 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 20:21 -j ACCEPT*
Apache APR apr_palloc Heap Overflow	Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.18. Actualizar Apache a la versión 2.2.18 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)*

	2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
Moodle < 1.9.6 Multiple Vulnerabilities	Actualizar Moodle a la versión 1.9.6 o superior. Se recomienda usar la última versión de Moodle disponible y estable que es la versión 2.3.3 **PROCEDIMIENTO** 1. Antes de realizar cualquier cambio en su versión de Moodle revisar los requerimientos para la versión a instalar: Moodle 2.3.3 **Requerimientos:** PHP 5.3.2, MySQL 5.1.33 o Postgres 8.3 o MSSQL 2005 o Oracle 10.2 Moodle 1.9.6 **Requerimientos:** PHP 4.3.0, MySQL 4.1.16 o Postgres 8.0 o MSSQL 9.0 o Oracle 9.0 2. Revisar si se cumple los requisitos o caso contrario actualizar a las versiones especificadas según la versión de Moodle que desea instalar. 3. Al cumplir los requerimientos necesarios para la actualización es necesario hacer una copia de su

	base de datos: */usr/local/pgsql/bin/pg_dump –username=nombre_usuario base_datos >backup.sql* 4. Descargar el archivo de Moodle en .tgz de su página oficial *http://download.moodle.org/*, una vez descargada la versión que se va a utilizar mover todos los archivos ubicados en */var/www/html/moodle* para que no se remplacen: *mv moodle moodle.backup* 5. Descomprimir el archivo descargado en la misma ruta: *tar xvzf moodle-2.3.3.tgz* 6. Para finalizar, copie todo su config.php, los plugins personalizados, y el archivo htaccess. *cp moodle.backup/config.php moodle* *cp -pr moodle.backup/theme/mytheme moodle/theme/mytheme* *cp -pr moodle.backup/mod/mymod moodle/mod/mymod*
Apache < 2.2.17 Multiple Vulnerabilities	Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)*

	2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
YUI charts.swf / swfstore.swf / uploader.swf XSS	Esta vulnerabilidad afecta a versiones de YUI inferiores a la 2.8.3 se necesita actualizar YUI a la versión 2.8.2 o superior. Se recomienda usar la última versión disponible y estable que es la versión 3.7.3 otra opción es la de filtrar los puertos afectados como son el 80 y 443. **PROCEDIMIENTO 1** Actualizar la versión de YUI: */ / Colocar el archivo YUI en su página.* *< script src = "http://yui.yahooapis.com/3.7.3/build/yui/yui-min.js" > </ escritura >* **PROCEDIMIENTO 2** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy. **Ver** Anexo VII **Puerto 80** *iptables -A INPUT -i eth0 -p tcp -s*

	$CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT* **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
Multiple Web Server printenv CGI Information Disclosure	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 80 y 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy. **Ver** Anexo VII **Puerto 80** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*

	Puerto 443 *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
Apache APR apr_fnmatch DoS	Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.18. Actualizar Apache a la versión 2.2.18 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3 **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
Apache mod_proxy_ajp DoS	Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.21. Actualizar Apache a la versión 2.2.21 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

	PROCEDIMIENTO 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando: *yum -y update httpd (Centos)* *apt-get install apache2 (Ubuntu o Debian)*
Web Server Uses Basic Authentication Without HTTPS	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son el 80 y 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy. **Ver** Anexo VII **Puerto 80** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT*

	iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
Backup Files Disclosure	Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 80. **Ver** Anexo VII **Puerto 80** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*
SSL Certificate with Wrong Hostname	No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443.

	PROCEDIMIENTO Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 443. **Ver** Anexo VII **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
SSL Certificate Expiry	No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionar filtrando el tráfico en el puerto 443. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 443. **Ver** Anexo VII **Puerto 443** *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT*
PHP < 5.3.5 String To Double Conversion DoS	Actualizar a PHP 5.3.5 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8

	PROCEDIMIENTO 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo la versión de PHP en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de PHP aplicar el siguiente comando: *yum -y update php (Centos)* *apt-get install php5 (Ubuntu o Debian)*
PHP < 5.2.2 Information Disclosure	Actualizar a PHP 5.2.2 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8. **PROCEDIMIENTO** 1. Actualizar los repositorios con el siguiente comando: *yum update (Centos)* *apt-get update (Ubuntu o Debian)* 2. Luego actualizamos todos los servicios en el servidor con: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)* 3. Si se desea actualizar solo la versión de PHP en

	el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de PHP aplicar el siguiente comando: *yum -y update php (Centos)* *apt-get install php5 (Ubuntu o Debian)*
Adobe Dreamweaver dwsync.xml Remote Information Disclosure	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es el 80. **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos 80. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT*
.svn/entries Disclosed via Web Server	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son 80,81,82,83,85,86,8000,8080,8081,8085,8090. Mediante Iptables utilizando políticas de DROP **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos necesarios en este caso

	utilizaremos el 8081 para peticiones MAHARA[34], como ejemplo. **Ver** Anexo VII *iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p tcp -m tcp --sport 1024: --dport 8081 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p tcp -m tcp --sport 8081 --dport 1024: -j ACCEPT*
Secure HyperText Transfer Protocol (S-HTTP) Detection	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son 8000,8080,8081,8083,8085,8086,8087,8090,8092. Mediante Iptables utilizando políticas de DROP **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos los Puertos necesarios en este caso utilizaremos el 8095 para peticiones TCExam[35] como ejemplo. **Ver** Anexo VII *iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p tcp -m tcp --sport 1024: --dport 8095 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p tcp -m tcp --sport 8095 --dport 1024: -j ACCEPT*

[34] **MAHARA:** Plataforma de eportfolio (portafolio electrónico) basada en un modelo de educación conectivista
[35] **TCExam:** Aplicación diseñada para crear exámenes electrónicos para universidades, colegios y demás instituciones que realicen pruebas de aptitud a sus alumnos, y estén interesadas en realizar éstas a través de ordenadores.

NFS Exported Share Information Disclosure	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es 2049. Mediante Iptables utilizando políticas de DROP **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el puerto 2049 para sistema de archivos de red NFS. **Ver** Anexo VII *iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p udp -m udp --sport 1024: --dport 2049 -j ACCEPT* *iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p udp -m udp --sport 2049 --dport 1024: -j ACCEPT*
SQL Dump Files Disclosed via Web Server	No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es el 80. Mediante Iptables utilizando políticas de DROP **PROCEDIMIENTO** Editar el script en la siguiente ruta: *sudo vim /etc/firewall/iptables* Habilitamos el puerto 80. **Ver** Anexo VII *iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT* *iptables -A OUTPUT -o eth0 -p tcp -s*

	$IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT

Fase IV Presentación de Informes

4. PRESENTACIÓN DE INFORMES

La fase IV denominada presentación de informes comprende el siguiente objetivo:

Objetivo 1: Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas

Objetivo 1:

Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas

4.1. PLAN DE MITIGACIÓN DE RIESGOS

4.1.1. IDENTIFICACIÓN DE RIESGOS

Los riesgos físicos fueron identificados mediante la técnica de la entrevista, a los encargados del centro de cómputo, **Ver** Anexo I, y para identificar los riegos lógicos se utilizó las herramientas descritas en las fases anteriores como NESSUS, NMAP y NIKTO.

4.1.1.1. Riesgos físicos

- Accesos no Controlados
- Filtraciones de Líquidos
- Fallas del Personal
- Incendios
- Interrupción Eléctrica
- Fallas en los Equipos

4.1.1.2. Riesgos lógicos

- Web Server Generic XSS
- HTTP TRACE / TRACK Methods Allowed
- Apache HTTP Server httpOnly Cookie Information Disclosure
- Apache HTTP Server Byte Range DoS
- SNMP Agent Default Community Name (public)
- mDNS Detection
- DNS Server Cache Snooping Remote Information Disclosure
- PHP < 5.3.9 Multiple Vulnerabilities
- DHCP Server Detection
- PHP expose_php Information Disclosure
- Web Application Information Disclosure
- Web Server Uses Plain Text Authentication Forms
- CGI Generic Injectable Parameter
- Unsupported Unix Operating System
- IP Forwarding Enabled
- SSL Certificate Cannot Be Trusted
- SSL Self-Signed Certificate
- SSL Medium Strength Cipher Suites Supported

- FTP Supports Clear Text Authentication
- Apache APR apr_palloc Heap Overflow
- Moodle < 1.9.6 Multiple Vulnerabilities
- Apache < 2.2.17 Multiple Vulnerabilities
- YUI charts.swf / swfstore.swf / uploader.swf XSS
- Multiple Web Server printenv CGI Information Disclosure
- Apache APR apr_fnmatch DoS
- Apache mod_proxy_ajp DoS
- Web Server Uses Basic Authentication Without HTTPS
- Backup Files Disclosure
- SSL Certificate with Wrong Hostname
- SSL Certificate Expiry
- PHP < 5.3.5 String To Double Conversion DoS
- PHP < 5.2.2 Information Disclosure
- Adobe Dreamweaver dwsync.xml Remote Information Disclosure
- .svn/entries Disclosed via Web Server
- Secure HyperText Transfer Protocol (S-HTTP) Detection
- NFS Exported Share Information Disclosure
- SQL Dump Files Disclosed via Web Server

4.1.2. ANÁLISIS DE RIESGOS

Analizaremos el conjunto riesgos encontrados en la Sala de Servidores y los clasificaremos por su nivel de criticidad, **Ver** Tabla L y Tabla LI.

Los valores descritos en la matriz de análisis de riesgos se basan en criterios y experiencias de los técnicos y jefes de sección de la UTI, el nivel de impacto y probabilidad se establecieron en base a la ocurrencia de los eventos según los criterios de dichos expertos.

La escala de valores para el Nivel de Impacto, Nivel de Probabilidad y Nivel de Riesgo están establecidos del 1 al 10 según modelo de Gestión de Riesgos para Centros de Cómputo elaborado por INTECO.

4.1.2.1. Riesgos Físicos

TABLA L Matriz de Análisis de Riesgos Físicos

CATEGORÍA DEL RIESGO	NIVEL DE IMPACTO	NIVEL DE PROBABILIDAD	NIVEL DE RIESGO
Accesos no controlados	Crítico	Casi cierta	Crítico
Filtraciones de Líquidos	Moderado	Moderada	Moderado
Fallas del personal	Moderado	Probable	Alto
Fallas en los Equipos	Significativo	Probable	Alto
Interrupción eléctrica	Crítico	Casi Cierta	Crítico
Incendios	Crítico	Moderado	Alto

4.1.2.2. Riesgos Lógicos

TABLA LI Matriz de Análisis de Riesgos Lógicas

CATEGORÍA DEL RIESGO	NIVEL DE IMPACTO	NIVEL DE PROBABILIDAD	NIVEL DE RIESGO
Web Server Generic XSS	Moderado	Probable	Alto
HTTP TRACE / TRACK Methods Allowed	Moderado	Moderada	Moderado
Apache HTTP Server httpOnly Cookie Information Disclosure	Moderado	Moderada	Moderado
Apache HTTP Server Byte Range DoS	Significativo	Probable	Alto
SNMP Agent Default Community Name (public)	Moderado	Poco probable	Bajo
mDNS Detection	Moderado	Poco Probable	Bajo
DNS Server Cache Snooping Remote Information Disclosure	Moderado	Poco Probable	Bajo

PHP < 5.3.9 Multiple Vulnerabilities	Significativo	Probable	Alto
DHCP Server Detection	Moderado	Moderada	Moderado
PHP expose_php Information Disclosure	Significativo	Moderada	Alto
Web Application Information Disclosure	Significativo	Poco probable	Moderado
Web Server Uses Plain Text Authentication Forms	Significativo	Probable	Alto
CGI Generic Injectable Parameter	Moderado	Poco Probable	Bajo
Unsupported Unix Operating System	Crítico	Casi Cierta	Critico
IP Forwarding Enabled	Menor	Poco Probable	Bajo
SSL Certificate Cannot Be Trusted	Significativo	Moderada	Alto
SSL Self-Signed Certificate	Significativo	Moderada	Alto
SSL Medium Strength Cipher Suites Supported	Significativo	Moderada	Alto
FTP Supports Clear Text Authentication	Significativo	Probable	Alto
Apache APR apr_palloc Heap Overflow	Moderado	Moderada	Moderado
Moodle < 1.9.6 Multiple Vulnerabilities	Menor	Moderada	Bajo
Apache < 2.2.17 Multiple Vulnerabilities	Significativo	Probable	Alto
YUI charts.swf / swfstore.swf / uploader.swf XSS	Moderado	Poco Probable	Bajo
Multiple Web Server printenv CGI Information Disclosure	Menor	Poco Probable	Bajo
Apache APR apr_fnmatch	Moderado	Probable	Alto

DoS			
Apache mod_proxy_ajp DoS	Significativo	Moderada	Alto
Web Server Uses Basic Authentication Without HTTPS	Significativo	Probable	Alto
Backup Files Disclosure	Moderado	Poco Probable	Bajo
SSL Certificate with Wrong Hostname	Significativo	Moderada	Alto
SSL Certificate Expiry	Significativo	Moderada	Alto
PHP < 5.3.5 String To Double Conversion DoS	Menor	Poco Probable	Bajo
PHP < 5.2.2 Information Disclosure	Menor	Moderada	Bajo
Adobe Dreamweaver dwsync.xml Remote Information Disclosure	Menor	Moderada	Bajo
.svn/entries Disclosed via Web Server	Moderado	Moderada	Moderado
Secure HyperText Transfer Protocol (S-HTTP) Detection	Significativo	Moderada	Alto
NFS Exported Share Information Disclosure	Menor	Poco Probable	Bajo
SQL Dump Files Disclosed via Web Server	Significativo	Moderada	Alto

4.1.3. PLANIFICAR RESPUESTAS A LOS RIESGOS

4.1.3.1. Acciones frente a los tipos de riesgos físicos.

- **Clase de Riesgo: Interrupción eléctrica**

Analizar las siguientes situaciones:

a) Los cortes de luz son continuos.

b) Las variaciones de voltaje han dañado equipos constantemente.

c) Si se ha realizado un estudio completo de las instalaciones eléctricas.
d) Existen las debidas protecciones eléctricas.
e) Existe el correcto balanceo de cargas en las fases existentes.

Se recomienda adquirir un sistema de energía eléctrica de emergencia y un UPs para salvaguardar los equipos de cortes de energía eléctrica inesperados y variaciones de voltaje.

- **Clase de Riesgo: Fallas en los equipos.**

Las fallas del sistema de red pueden deberse al mal funcionamiento de los equipos o la pérdida de configuración de los mismos por lo que se deben evaluar las fallas. [2]

Fallas en el disco: Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

a) Ubicar el disco malogrado. Responsable Técnicos de sección afectada
b) Bajar el sistema y apagar el equipo. Responsable Jefe de sección afectada
c) Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo y darle partición. Responsable Técnicos de la sección afectada
d) Revisar el servidor de respaldos y bajar el contenido del servidor dañado. Responsable Técnicos de la sección afectada
e) Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad. Responsable Técnicos de sección afectada
f) Revisar los sistemas que se encuentran en dicho disco y verificar su buen estado. Responsable Técnicos de sección afectada
g) Habilitar el sistema para los usuarios. Responsable Jefe de sección afectada

Daños en la Fuente de poder: Se deben tomar las acciones siguientes:

a) Verificar si la fuente de poder es el origen del problema. Responsable Técnicos de sección afectada
b) Retirar las la fuente de poder dañada y reemplazarla por otra similar. Responsable Técnicos de sección afectada
c) Encender el equipo. Responsable Técnicos de sección afectada
d) Verificar si existen daños en los archivos del servidor. Responsable Técnicos de sección afectada
e) Iniciar operaciones. Responsable Técnicos de sección afectada

Fallas en el software: La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- ✓ Modificación de archivos de forma incorrecta.
- ✓ Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- ✓ Borrar archivos por error.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

a) Verificar el suministro de energía eléctrica. Responsable Técnicos de sección afectada
b) Descargar todos los respaldos disponibles del servidor. Responsable Técnicos de sección afectada
c) Reinstalar los archivos dañados. Responsable Técnicos de sección afectada
d) Probar si se solucionó el problema. Responsable Técnicos de sección afectada
e) Reanudar Operaciones. Responsable Técnicos de sección afectada

Para disminuir el riesgo de fallas en el hardware se de realizar el mantenimiento preventivo de los equipos por lo menos 2 veces al año y realizar limpieza continua en la Sala de Servidores para evitar la acumulación de polvo que pudiese dañar los equipos. [2]

- **Clase de Riesgo: Accesos No Controlados.**

Enfatizar en los temas:

a) Destinar personal de seguridad para vigile y controle el acceso físico al Centro de Cómputo.
b) Mejorar la puerta de acceso, es decir adquirir una puerta blindada con cerradura biométrica.
c) No dejar solo el área de servidores, siempre dejar a alguien encargado.
d) Si se nota alguna actitud sospechosa de alguna persona comunicar inmediatamente a jefe de Unidad.

- **Clase de Riesgo: Fallas del personal.**

a) Capacitar constantemente a los técnicos de las secciones sobre el funcionamiento y uso de los servidores.
b) Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.
c) Asegúrese de que se hacen copias de respaldo regulares de los archivos de los servidores y de que el proceso de restauración es tan organizado y rápido como sea posible.

- **Clase de Riesgo: Incendio.**

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado. El procedimiento de respuesta a esta emergencia es el siguiente:

a) En caso de daño del Edificio, trasladar las operaciones a las Oficinas Alternas.
b) Realizar una reunión con todos los jefes de sección con el fin de hacer un recuento de los daños y determinar una ubicación temporal y el tiempo en que se operaría fuera de las instalaciones.
c) Trasladar los respaldos de datos, programas, manuales, a las oficinas alternas para reiniciar las operaciones. Responsables: Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
d) Restaurar la información de la Base de Datos y programas. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
e) Iniciar las Operaciones.

Cuando el daño ha sido menor:

a) Tramitar la garantía de los equipos dañados en caso de existir o comprar los equipos indispensables para la continuidad de las operaciones. Jefe de Unidad.
b) Instalar el sistema operativo. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
c) Restaurar la información de las bases de datos y programas. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
d) Iniciar las Operaciones.

¿QUE HACER? Antes, Durante y Después de un INCENDIO.

ANTES:

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel, ni fumar en las oficinas o cerca del Centro de Datos.
- Verificar las condiciones de extintores y capacitar al personal para su manejo.
- No almacenar sustancias y productos inflamables.
- No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos y en las instalaciones eléctricas, reportar de inmediato al Jefe de la Unidad.
- Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
- Tener a la mano los números telefónicos de emergencia.

DURANTE

- Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en los servidores, se deberá (si el tiempo lo permite) apagar el (los) servidor(es), y la caja principal de corriente del Centro de Datos.
- Si el fuego está fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.
- Descender por las escaleras pegado a la pared, recordar No gritar, No empujar, No correr y dirigirse a una zona segura.
- Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respirar a través de él.

- Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.
- Si es posible mojar la ropa.
- Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUES

- Retirarse inmediatamente del área incendiada y ubicarse en una zona segura.
- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
- El personal calificado realizará una verificación física del inmueble y definirá si está en condiciones de ser utilizado normalmente.
- Colaborar con las autoridades.

- **Clase de Riesgo: Filtraciones de líquidos.**

a) Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.
b) Cuando el daño ha sido menor se procede:
   - Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Jefe de la Unidad.
   - Recoger los respaldos de datos, programas, manuales y claves. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
   - Instalar el sistema operativo. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
   - Restaurar la información de las bases de datos y programas. Secciones de Redes y Equipos Informáticos y Desarrollo de Software.
c) Realizar un recuento de los daños causados.

4.1.3.2. Acciones frente a los tipos de riesgos lógicos.

- **Clase de Riesgo: Web Server Generic XSS**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado es el 8080

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el Puerto 8080 para permitir navegación de la INTRANET.

```
iptables -A INPUT -s $INTRANET[36] -d $IPORIGEN  -i eth0 -p tcp -m tcp --sport 1024: --dport 8080 -j ACCEPT
```

```
iptables -A OUTPUT -s $IPORIGEN[37] -d $INTRANET -o eth0 -p tcp -m tcp --sport 8080 --dport 1024: -j ACCEPT
```

- **Clase de Riesgo: HTTP TRACE / TRACK Methods Allowed**

Deshabilitar el método trace/track en http

PROCEDIMIENTO

Para deshabilitar el método trace/track en http, se debe editar el archivo httpd.conf en la siguiente ruta:

```
sudo vim /etc/httpd/conf/httpd.conf
```

Copiar el siguiente código al final del archivo:

```
RewriteEngine on

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F]
```

[36] **INTRANET**: 172.16.32.0/19
[37] **IPORIGEN:** Ip del servidor

- **Clase de Riesgo: Apache HTTP Server httpOnly Cookie Information Disclosure**

Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.22. Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

```
yum update (Centos)
```

```
apt-get update (Ubuntu o Debian)
```

Luego actualizamos todos los servicios en el servidor con:

```
yum upgrade (Centos)
```

```
apt-get upgrade (Ubuntu o Debian)
```

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

```
yum -y update httpd (Centos)
```

```
apt-get install apache2 (Ubuntu o Debian)
```

- **Clase de Riesgo: Apache HTTP Server Byte Range DoS**

Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.22. Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

```
yum update (Centos)
```

```
apt-get update (Ubuntu o Debian)
```

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: SNMP Agent Default Community Name (public)**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado que es el 161.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos el Puerto 161.

```
iptables -A INPUT -s $IPDESTINO  -d $IPORIGEN -i eth0 -p udp -m udp --sport        1024: --dport 161 -j ACCEPT

 iptables -A OUTPUT -s $IPORIGEN -d $IPDESTINO -o eth0 -p udp -m udp --sport  161 --dport 1024: -j ACCEPT
```

- **Clase de Riesgo: mDNS Detection**

Este problema se origina porque en Linux viene Avahi instalado por defecto, Avahi permite detectar automáticamente los recursos de una red local y conectarse a ella.

Avahi se ocupa de: asignar automáticamente una dirección IP incluso sin presencia de un servidor DHCP, hacer la función de DNS (cada máquina es accesible con el nombre nombreMaquina.local), hacer una lista de los servicios y acceder a ellos fácilmente (las máquinas de la red local son informadas de la llegada o salida de un servicio).

Esto facilita el uso compartido de archivos, impresoras, etc. Avahi es una implementación del protocolo ZeroConf compatible con Rendezvous, Bonjour de Apple. Por lo tanto es necesario deshabilitarlo en los servidores afectados:

PROCEDIMIENTO

Eliminar los enlaces hacia daemon:

```
sudo update-rc.d -f avahi-daemon remove (Debian o Ubuntu)

/sbin/chkconfig avahi-daemon off (Centos)
```

- **Clase de Riesgo: DNS Server Cache Snooping Remote Information Disclosure**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado que es el 53

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el Puerto 53 para resolución de DNS.

```
iptables -A INPUT -s $DNSINTRANET 38-d $IPORIGEN -i eth0 -p udp
-m udp - sport 53 --dport 1024: -j ACCEPT

iptables -A OUTPUT -s $IPORIGEN -d $DNSINTRANET -o eth0 -p udp -
m udp --sport 1024: --dport 53 -j ACCEPT
```

- **Clase de Riesgo: PHP < 5.3.9 Multiple Vulnerabilities**

Actualizar a PHP 5.3.9 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8

[38] **DNSINTRANET:** 172.16.32.2

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo la versión de PHP en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de PHP aplicar el siguiente comando:

yum -y update php (Centos)

apt-get install php5 (Ubuntu o Debian)

- **Clase de Riesgo: DHCP Server Detection**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 67 y 68.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos los Puertos 67 Y 68 para acceso de usuarios.

iptables -A INPUT -s $INTRANET -d $IPORIGEN -i eth0 -p udp --sport 67:68 – dport 67:68 -j ACCEPT

iptables -A OUTPUT -s $IPORIGEN -d $INTRANET -o eth0 -p udp --sport 67:68 -- dport 67:68 -j ACCEPT

- **Clase de Riesgo: PHP expose_php Information Disclosure**

En la configuración de PHP archivo php.ini, establezca el valor de 'expose_php' a 'Off' para desactivar este comportamiento.

PROCEDIMIENTO

Editar el archivo php.ini en la siguiente ruta:

sudo vim/etc/php.ini (Centos)

sudo vim/etc/php5/apache2/php.ini (Ubuntu o Debian)

Buscar expose_php en el archivo, generalmente viene configurado por defecto en *[On/Off]* y para desactivar este valor cambiar *[Off/On]*:

expose_php = [Off/On]

- **Clase de Riesgo: Web Application Information Disclosure**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos el Puerto 80 para permitir navegación del proxy.

iptables -A INPUT -i eth0 -p tcp -s $CERO[39] *-d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT*

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT

[39] **CERO:** 0.0.0.0/0

- **Clase de Riesgo: Web Server Uses Plain Text Authentication Forms**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el Puerto 80 para permitir navegación del proxy.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --
sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --
sport 1024: --dport 80 -j ACCEPT
```

- **Clase de Riesgo: CGI Generic Injectable Parameter**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el Puerto 80 para permitir navegación del proxy.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --
sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --
sport 1024: --dport 80 -j ACCEPT
```

- **Clase de Riesgo: Unsupported Unix Operating System Debian 5.0**

Actualizar sistema operativo a Debian 6.0. Última versión estable.

PROCEDIMIENTO

Para ello tecleamos en la terminal

```
sudo vim  /etc/apt/sources.list
```

Esto abre nuestra lista de repositorios lo que haremos será sustituir todos los "lenny" por "squeeze" el resultado debe quedar así:

```
#REPOSITORIOS OFICIALES
deb http://ftp.fr.debian.org/debian/ squeeze main
deb-src http://ftp.fr.debian.org/debian/ squeeze main

#REPOSITORIOS SEGURIDAD
deb http://security.debian.org/ squeeze/updates main
deb-src http://security.debian.org/ squeeze/updates main

#REPOSITORIOS MULTIMEDIA
deb http://www.debian-multimedia.org/ squeeze main
deb-src http://www.debian-multimedia.org/ squeeze main
```

Guardar los cambios y aplicar el siguiente comando

```
aptitude update && aptitude full-upgrade
```

- **Clase de Riesgo: IP Forwarding Enabled**

Deshabilitar esta opción en el servidor si no es necesaria.

PROCEDIMIENTO

Editar el archivo el sysctl.conf en la siguiente ruta:

```
sudo vim /etc/sysctl.conf
```

Añadir o cambiar la siguiente opción:

```
net.ipv4.ip_forward = 0
```

Para activar los cambios realizados en el fichero debemos ejecutar:

```
sysctl  -p  /etc/sysctl.conf
```

- **Clase de Riesgo: SSL Certificate Cannot Be Trusted**

No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 443.

Puerto 443

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport
443 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport
1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: SSL Self-Signed Certificate**

No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 443.

Puerto 443

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport
443 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport
1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: SSL Medium Strength Cipher Suites Supported**

No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 443.

Puerto 443

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport
443 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport
1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: FTP Supports Clear Text Authentication**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 21 y 22.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el Puerto 21y 22 para proxy.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport
20:21 --dport 1024: -j ACCEPT
```

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 20:21 -j ACCEPT

- **Clase de Riesgo: Apache APR apr_palloc Heap Overflow**

Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.18. Actualizar Apache a la versión 2.2.18 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: Moodle < 1.9.6 Multiple Vulnerabilities**

Actualizar Moodle a la versión 1.9.6 o superior. Se recomienda usar la última versión de Moodle disponible y estable que es la versión 2.3.3

PROCEDIMIENTO

Antes de realizar cualquier cambio en su versión de Moodle revisar los requerimientos para la versión a instalar:

Moodle 2.3.3

Requerimientos: PHP 5.3.2, MySQL 5.1.33 o

Postgres 8.3 o MSSQL 2005 u Oracle 10.2

Moodle 1.9.6

Requerimientos: PHP 4.3.0, MySQL 4.1.16 o

Postgres 8.0 o MSSQL 9.0 u Oracle 9.0

Revisar si se cumple los requisitos o caso contrario actualizar a las versiones especificadas según la versión de Moodle que desea instalar.

Al cumplir los requerimientos necesarios para la actualización es necesario hacer una copia de su base de datos:

```
/usr/local/pgsql/bin/pg_dump –username=nombre_usuario base_datos
>backup.sql
```

Descargar el archivo de Moodle en .tgz de su página oficial *http://download.moodle.org/*, una vez descargada la versión que se va a utilizar mover todos los archivos ubicados en */var/www/html/moodle* para que no se remplacen:

```
mv moodle moodle.backup
```

Descomprimir el archivo descargado en la misma ruta:

```
tar  xvzf  moodle-2.3.3.tgz
```

Para finalizar, copie todo su config.php, los plugins personalizados, y el archivo htaccess.

```
cp moodle.backup/config.php moodle
```

```
cp -pr moodle.backup/theme/mytheme moodle/theme/mytheme
```

```
cp -pr moodle.backup/mod/mymod moodle/mod/mymod
```

- **Clase de Riesgo: Apache < 2.2.17 Multiple Vulnerabilities**

Actualizar Apache a la versión 2.2.22 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: YUI charts.swf / swfstore.swf / uploader.swf XSS**

Esta vulnerabilidad afecta a versiones de YUI inferiores a la 2.8.3 se necesita actualizar YUI a la versión 2.8.2 o superior. Se recomienda usar la última versión disponible y estable que es la versión 3.7.3 otra opción es la de filtrar los puertos afectados como son el 80 y 443.

PROCEDIMIENTO 1

Actualizar la versión de YUI:

/ / Colocar el archivo YUI en su página.

< script src = "http://yui.yahooapis.com/3.7.3/build/yui/yui-min.js" > </ escritura >

PROCEDIMIENTO 2

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy.

Puerto 80

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT
```

Puerto 443

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: Multiple Web Server printenv CGI Information Disclosure**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. Los puertos afectados por esta vulnerabilidad son el 80 y 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy.

Puerto 80

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT
```

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT

Puerto 443

iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT

- **Clase de Riesgo: Apache APR apr_fnmatch DoS**

Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.18. Actualizar Apache a la versión 2.2.18 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: Apache mod_proxy_ajp DoS**

Esta vulnerabilidad afecta a versiones inferiores a la versión 2.2.21. Actualizar Apache a la versión 2.2.21 o superior. Se recomienda usar la última versión de Apache disponible y estable que es la versión 2.4.3

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: Web Server Uses Basic Authentication Without HTTPS**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son el 80 y 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos los Puertos 80 Y 443 para permitir navegación del proxy.

Puerto 80

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT
```

Puerto 443

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: Backup Files Disclosure**

Filtrar el tráfico del servidor mediante Iptables con políticas de DROP. El puerto afectado por esta vulnerabilidad es el 80.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 80.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT
```

- **Clase de Riesgo: SSL Certificate with Wrong Hostname**

No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 443.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: SSL Certificate Expiry**

No se ha encontrado una solución específica para esta clase de vulnerabilidad pero se ha logrado solucionar filtrando el tráfico en el puerto 443.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos 443.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 443 --dport 1024: -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 443 -j ACCEPT
```

- **Clase de Riesgo: PHP < 5.3.5 String To Double Conversion DoS**

Actualizar a PHP 5.3.5 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo la versión de PHP en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de PHP aplicar el siguiente comando:

yum -y update php (Centos)

apt-get install php5 (Ubuntu o Debian)

- **Clase de Riesgo: PHP < 5.2.2 Information Disclosure**

Actualizar a PHP 5.2.2 o superior. Se recomienda usar la última versión disponible y estable de PHP que es la versión 5.4.8.

PROCEDIMIENTO

Actualizar los repositorios con el siguiente comando:

yum update (Centos)

apt-get update (Ubuntu o Debian)

Luego actualizamos todos los servicios en el servidor con:

yum upgrade (Centos)

apt-get upgrade (Ubuntu o Debian)

Si se desea actualizar solo Apache en el servidor o si después de actualizar todos los servicios no se instaló la versión deseada de Apache aplicar el siguiente comando:

yum -y update httpd (Centos)

apt-get install apache2 (Ubuntu o Debian)

- **Clase de Riesgo: Adobe Dreamweaver dwsync.xml Remote Information Disclosure**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es el 80.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos los Puertos 80.

iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT

- **Clase de Riesgo: .svn/entries Disclosed via Web Server**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son 80,81,82,83,85,86,8000,8080,8081,8085,8090. Mediante Iptables utilizando políticas de DROP

PROCEDIMIENTO

Editar el script en la siguiente ruta:

sudo vim /etc/firewall/iptables

Habilitamos los Puertos necesarios en este caso utilizaremos el 8081 para peticiones MAHARA[40], como ejemplo.

```
iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p tcp -m tcp --sport 1024: --dport 8081 -j ACCEPT
```

```
iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p tcp -m tcp --sport 8081 --dport 1024: -j ACCEPT
```

- **Clase de Riesgo: Secure HyperText Transfer Protocol (S-HTTP) Detection**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en los puertos afectados que son 8000,8080,8081,8083,8085,8086,8087,8090,8092. Mediante Iptables utilizando políticas de DROP

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos los Puertos necesarios en este caso utilizaremos el 8095 para peticiones TCExam[41] como ejemplo.

```
iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p tcp -m tcp --sport 1024: --dport 8095 -j ACCEPT
```

```
iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p tcp -m tcp --sport 8095 --dport 1024: -j ACCEPT
```

[40] **MAHARA:** Plataforma de eportfolio (portafolio electrónico) basada en un modelo de educación conectivista
[41] **TCExam:** Aplicación diseñada para crear exámenes electrónicos para universidades, colegios y demás instituciones que realicen pruebas de aptitud a sus alumnos, y estén interesadas en realizar éstas a través de ordenadores.

- **Clase de Riesgo: NFS Exported Share Information Disclosure**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es 2049. Mediante Iptables utilizando políticas de DROP.

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el puerto 2049 para sistema de archivos de red NFS.

```
iptables -A INPUT -s $CERO -d $IPORIGEN -i eth0 -p udp -m udp --sport 1024: --dport 2049 -j ACCEPT
```

```
iptables -A OUTPUT -s $IPORIGEN -d $CERO -o eth0 -p udp -m udp --sport 2049 --dport 1024: -j ACCEPT
```

- **Clase de Riesgo: SQL Dump Files Disclosed via Web Server**

No se ha encontrado una solución puntual a esta vulnerabilidad pero se ha logrado solucionarla filtrando el tráfico en el puerto afectado que es el 80. Mediante Iptables utilizando políticas de DROP

PROCEDIMIENTO

Editar el script en la siguiente ruta:

```
sudo vim /etc/firewall/iptables
```

Habilitamos el puerto 80.

```
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPORIGEN --sport 80 --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPORIGEN -d $CERO --sport 1024: --dport 80 -j ACCEPT
```

4.1.4. CONTROL Y MONITORIZACIÓN DE RIESGOS

Se realizó simulacros en la parte de Riesgos Físicos y se implementó seguridades en los servidores en el caso de los riesgos lógicos. En los cuales participó el personal de la UTI y se verificó que los planes planteados ante los riegos son efectivos, mediante el control y certificación de los riesgos, **Ver** Anexo XII, se logró capturar algunas observaciones sobre el plan de respuesta propuesto, **Ver** Anexo XIII, que se detallan a continuación:

Riesgos Físicos

- **Accesos no controlados:** En este riesgo la principal observación es que se debe colocar letreros denotando el acceso restringido al área de servidores y que la puerta actual no brinda las seguridades necesarias.
- **Filtraciones de Líquidos:** Se debe tener previamente un local definido en caso de evacuación por daños mayores.
- **Fallas del personal:** Las acciones de respuesta frente a este riesgo son satisfactorias.
- **Fallas del Hardware:** La observación de los participantes es que se debería contar con un stock de repuestos muy variado porque los procesos de compra son muy largos.
- **Interrupciones eléctricas:** Se ha determinado que no se cuentan con las respectivas protecciones eléctricas.
- **Incendios:** Existieron observaciones por parte del personal participante en el simulacro y se determinó que se debe colocar los números de emergencias en un lugar visible.

Riesgos Lógicos

Los pruebas de las acciones frente a los riesgos lógicos han sido satisfactorias ya que su implementación en los servidores han dado buenos resultados. Las vulnerabilidades lógicas utilizadas para las pruebas fueron: Secure HyperText Transfer Protocol (S-HTTP) Detection, Web Server Uses Basic Authentication Without HTTPS, FTP Supports Clear Text Authentication y Web Server Uses Plain Text Authentication Forms

4.2. POLÍTICAS DE SEGURIDAD PARA LA UTI

A los doce días del mes de Enero del presente año en la Sección de Redes de la Unidad de Telecomunicaciones e Información se procedió a realizar conjuntamente con los técnicos de la unidad, las políticas de seguridad para los servidores de la UTI con la presencia del responsable de la unidad Tngo. Daniel Reyes, los técnicos Ing. Jaime Bravo, Tnga. Gabriela Cruz y los tesistas Egdo. Cesar Bastidas y Egda. Mariana González

Luego de debatir cada una de las políticas propuestas por los tesistas se procedió a realizar las observaciones pertinentes quedando plasmadas en el presente documento que se lo ha socializado al interior de la Unidad. **Ver** Anexo XIX.

Las políticas de seguridad se establecieron en base a los resultados del plan de mitigación de riesgos y como una necesidad de la Unidad de Telecomunicaciones de Información para tener un referente para sus empleados.

El presente anexo establece los lineamientos técnicos para la administración de los servidores de la Unidad de Telecomunicaciones de Información con la finalidad de permitir a los responsables de cada sección normativas de seguridad de los servidores.

Se establecen las políticas que norman la infraestructura destinada a brindar la seguridad física y lógica de los servidores de la Unidad de Telecomunicaciones e Información las cuales serán observadas por la Dirección de la Unidad

Es necesario proveer a los servidores mecanismos de cifrado para la transmisión de información a través de la Red Interna para aprovechar la infraestructura, además de la ventaja de que esta configuración es independiente de que exista un acceso adicional a Internet.

Proporcionar a la Dependencia o Entidad los elementos técnicos suficientes para poder detectar alguna intrusión o actividad no autorizada dentro o a través de su servidor, a fin de reportarlo y, en la medida en que sea posible, realizar acciones para contrarrestar la intrusión.

Será necesario sensibilizar a los usuarios y administradores la importancia que tiene la seguridad de la información contenida en los servidores de la UTI

GLOSARIO DE TÉRMINOS

Usuario.- Toda persona, funcionario (empleado, docente, estudiante), que utilice los sistemas de información de la Universidad Nacional de Loja, debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

UTI.- Unidad de Telecomunicaciones e Información

Seguridad.- Mecanismos de control que evita el uso no autorizado de recursos.

Red.- Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Terceras personas.- Toda personas ajenas a la Universidad Nacional de Loja

Servidor.- Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Computador.- Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Centro de cómputo.- Un centro de cómputo, centro de procesamiento de datos, centro de datos o data center es una entidad, oficina o departamento que se encarga del procesamiento de datos e información de forma sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras que están equipadas con el hardware y el software necesarios para cumplir con dicha tarea.

Técnicos.- Persona responsable de, controlar, supervisar, instalar, configurar los sistemas operativos en sus partes, Resolver incidencias que puedan surgir tanto en Linux como en Windows, y garantizar la operatividad y funcionalidad de los sistemas

Responsable de sección.- Persona responsable de administrar, controlar, Supervisar y garantizar la operatividad, funcionalidad de los sistemas a su cargo

Director de la unidad.- Persona responsable de administrar, controlar, Supervisar

Tesista.- Persona que desarrolla su tesis en cualquiera de las secciones dela Unidad de Telecomunicaciones e Información

Pasante.- Persona que realiza sus prácticas pre profesionales en la UTI

Contraseña, clave o password.- Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Puerto.- Los puertos son las vías de comunicación que usan los computadores para conectarse/comunicarse entre sí a través de los cuales los diferentes tipos de datos se pueden enviar y recibir.

Iptables.- Es una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4, IPv6 o mantener registros de log.

Log.- Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

A. SEGURIDADES FÍSICAS

A.1 ACCESO Y PROTECCIÓN FÍSICA

1. Todos los servidores estarán debidamente protegidos con la infraestructura apropiada, **Ver** Página 96, de manera que el usuario no tenga acceso físico directo.
2. Todos los técnicos y jefes de sección deben portar una identificación especial para la Unidad, **Ver** Anexo XIV.
3. El acceso de terceras personas debe ser plenamente identificado, controlado y vigilado por técnicos de la unidad y portando una identificación.
4. Las visitas al interno del Centro de Cómputo se darán siempre y cuando se encuentren acompañadas por el responsable de sección o por cualquiera de los técnicos.
5. Las visitas a las instalaciones físicas del Centro de Cómputo se harán en horas de oficina, cumpliendo con lo estipulado en el artículo 4
6. El Centro de Cómputo debe estar equipado con puertas blindadas o cualquier otra puerta resistente a entradas forzadas. **Ver** Página 105.
7. Los únicos autorizados para mover, cambiar o extraer uno o varios equipos del Centro de Cómputo serán los técnicos de la unidad o el responsable de sección, y notificará al Jefe de la Unidad mediante oficio e informará de los cambios a realizar para la previa autorización.

8. El resguardo de los equipos deberá quedar asignado a la persona que los usa o administra, permitiendo conocer siempre la ubicación física de los equipos.
9. El Centro de Cómputo debe:
    - Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo, según la norma EIA /TIA 942 parte de los técnicos de la unidad.
    - Ser un área restringida, con su respectiva señalización, **Ver** Anexo XV.
    - Recibir mantenimiento preventivo de los servidores por lo menos dos veces al año, según la norma EIA /TIA 942, por parte de los técnicos de la unidad.
    - Contar con instalaciones eléctricas en buen estado.
    - Contar con un sistema de alimentación continuo a base de ups, **Ver** Página 114 y de una planta generadora eléctrica, **Ver** Página 112.
    - Contar con un sistema de enfriamiento adecuado, **Ver** Página 120.
    - Contar con un sistema contra incendios adecuado para el Centro de Cómputo. **Ver** Página 116.
10. Los sistemas puesta a tierra, sistemas de protección e instalaciones eléctricas del Centro de Cómputo deberán recibir mantenimiento periódico y constante con el fin de determinar la efectividad del sistema.
11. Se debe balacear la carga entre los circuitos eléctricos para optimizar el uso de la energía eléctrica.
12. En el Centro de Cómputo, está prohibido fumar, tomar ningún tipo de bebidas o consumir alimento.
13. Los servidores solo pueden ser manipulados física y lógicamente por el director de la unidad, responsables de sección o por los respectivos técnicos bajo la supervisión del responsable.

A.2. TESISTAS Y PASANTES

14. Se debe capacitar a Tesistas y Pasantes acerca del uso y manipulación de los equipos de la UTI.
15. Todos los Tesistas y Pasantes serán supervisados por un técnico de la Unidad.

16. El horario labores de los Tesistas y Pasantes será el mismo que el de los técnicos y responsables de la Unidad.
17. Se deberá llevar un control estricto de pasantes especificando nombres completos, fecha, tarea realizada y firma. **Ver** Anexo XVI.

A.3. ESTABLECIMIENTO Y USO DE MANUALES

18. Todos los técnicos de la sección deberán documentar cualquier cambio en los servidores y las razones por las que se modificó dicho servidor. **Ver** Anexo XVII.
19. La implementación de un nuevo servidor debe ser documentada por el técnico que realiza la instalación. **Ver** Anexo XVIII.
20. Los técnicos de la sección deberán realizar respaldos de los archivos de configuración de los servidores a su cargo.

B. SEGURIDADES LÓGICAS

B.1. MANEJO DE CONTRASEÑAS

21. El acceso a los servidores se lo realizará remotamente mediante ssh (Securite SHell)
22. La autenticación en los servidores será mediante criptografía asimétrica con claves públicas y privadas
23. Las claves de los administradores deben seguir el siguiente estándar
    - Más de ocho caracteres.
    - Mezcla de caracteres alfabéticos, como mayúsculas, minúsculas y no alfabéticos.
    - No ser ni derivarse de una palabra del diccionario, jerga o de un dialecto.
    - No derivarse del nombre del usuario o de algún pariente cercano.
    - No derivarse de información personal (del número de teléfono, número de identificación, cedula, fecha de nacimiento, etc...) del usuario o de algún pariente cercano.
    - No contener series de caracteres comunes tales como “123456”

24. Las contraseñas deben crearse de forma que puedan recordarse fácilmente, bien de forma directa o a través de reglas nemotécnicas.
25. No compartir de ninguna forma cuentas y contraseñas. Son estrictamente personales e intransferibles.
26. No revelar ni compartir su contraseña por teléfono, correo electrónico, anotándola o de cualquier otra forma a nadie, incluso aunque le hablen en nombre de la UTI o de un superior suyo en la institución.
27. Todas las contraseñas del sistema deberán cambiarse con una periodicidad de al menos una vez cada seis meses.
28. Ante la sospecha de que una contraseña haya sido comprometida, se cambiará la misma de forma inmediata.
29. El nombre de usuario creado en los servidores deberá ser distinto al nombre
30. Sera opcional la utilización de claves en BIOS y en grub de los servidores

B.2 PUERTOS Y SERVICIOS

31. Se cambiará en medida de lo posible los puertos por defecto de los diferentes servicios de los servidores
32. Será obligatoria el uso de iptables cortafuegos, con políticas de drop en cada uno de los servidores.
33. Solo los servicios que sean necesarios deberán estar activos en el servidor
34. Los archivos al interior del servidor tendrán permisos de lectura escritura y ejecución según su usuario
35. Se deberá actualizar los servidores periódicamente

C. AMBIENTE DE TRABAJO

36. Los técnicos y responsables de la sección tendrán un espacio asignado por la dirección para realizar sus labores diarias.
37. El espacio de trabajo debe contar con una iluminación apropiada de 500 lúmenes según la norma EIA/TIA 942.
38. Cada jefe de unidad, responsables de unidad y técnicos deberán contar con al menos un escritorio, una silla, una computadora sea esta portátil o de escritorio
39. El espacio de trabajo debe contar con al menos un punto de acceso a la red de datos.
40. El espacio de trabajo debe contar con medios de comunicación como teléfono fax, impresora, etc.

41. El espacio de trabajo debe ser tranquilo y libre de ruido

G. DISCUSIÓN

1. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

La Universidad Nacional de Loja, es una institución de educación superior pública que brinda formación académica y profesional de calidad, con sólidas bases científicas y técnicas, que con el paso del tiempo ha evolucionado tanto académica como tecnológicamente.

En calidad de egresados de la carrera de Ingeniería en Sistemas del Área de La Energía, las Industrias y los Recursos Naturales no Renovables, debemos contribuir con la sociedad de forma que apoyemos al desarrollo científico técnico del país haciendo especial énfasis en la seguridad de la información.

Por lo expuesto el trabajo de investigación denominado **"*Análisis de vulnerabilidades físicas y lógicas de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, y construcción de un Plan de Mitigación de Riesgos*",** permitió obtener como resultados la identificación de las vulnerabilidades físicas y lógicas, permitiendo la solución de las vulnerabilidades lógicas y el uso de varias herramientas como NESSUS, NMAP; NIKTO Y CAIN&ABEL, en cada una de las fases, además se proponen soluciones en la parte seguridades físicas .

Todos los objetivos fueron cumplidos paso a paso en el desarrollo del proyecto gracias a la metodología planteada la misma que consta de cuatro fases claramente definidas, la metodología para el Análisis de Vulnerabilidades elaborada por la empresa DSTEAM nos brindó todas las facilidades para cumplir con los objetivos planteados facilidades que no obtuvimos con la metodología de Pentest que se presentaba como una opción más intrusiva y que podía causar problemas en el funcionamiento de los servidores a continuación se detalla como fueron abarcados cada uno de los objetivos en cada una de las fases.

Fase I Reconocimiento Activo: En esta fase se logró cumplir con el primer objetivo y nos permitió obtener un completo conocimiento de la estructura física y lógica actual de la Sala de Servidores de la UTI, en cambio la metodología de Pentest la primera fase se la denomina etapa de Descubrimiento que a diferencia de la primera fase de la

metodología de Análisis de Vulnerabilidades tiene como objetivo detectar mediante pruebas lógicas toda la estructura de la red, sitios web y la identificación de las instalaciones físicas por averiguaciones propias pudiéndose omitir datos importantes en este proceso, mientras que en la fase de Reconocimiento Activo para obtener la información cuentas con la colaboración de todo el personal para obtener un conocimiento más profundo de la situación física y lógica actual, en esta primera fase se obtuvo los siguientes resultados:

- **Objetivo Específico 1:** Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

  Se determinó como está estructurada física y lógicamente la Sala de Servidores de la Universidad y se recolectó la información a través de entrevistas a los encargados de las secciones de Redes y Equipos Informáticos, y Desarrollo de Software que son las secciones que más servidores poseen en la Sala de Servidores. Para la situación lógica se procedió a identificar puertos, servicios y sistemas operativos de cada uno de los servidores de la UTI con ayuda de la herramienta NMAP, mediante la información recolectada y a través de la observación se pudo cumplir este objetivo. **Ver** Anexo I y II.

  Además pudimos establecer una lista de vulnerabilidades físicas detectadas y constatadas pudiéndose determinar correctamente la situación en la que realmente está el centro de cómputo.

Fase II Análisis de Vulnerabilidades: En esta fase se pudo cumplir con tres objetivos claramente definidos, en esta fase se identificó las vulnerabilidades lógicas a través del establecimiento de herramientas y se analizó las vulnerabilidades físicas para proponer las soluciones respectivas, en cambio la metodología de Pentest a esta etapa se la denomina de Exploración y tiene como finalidad identificar blancos para realizar un ataque, detección de sistemas operativos y versiones de servicios pero a diferencia del Análisis de Vulnerabilidades este proceso ya se realizó en la fase de Reconocimiento Activo, y en la presente fase se obtuvo los siguientes resultados:

- **Objetivo Específico 2:** Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

  Se abarcó completamente el objetivo planteado, en base a la información recolectada y analizada, se logró establecer las seguridades físicas básicas necesarias para la Sala de Servidores como controles de acceso, impermeabilización, sistemas auxiliares de energía, sistemas contra incendios y el hardware necesario para optimizar la Sala de Servidores, todas estas recomendaciones en la parte física se basaron en la norma internacional EIA/TIA 942. **Ver** Anexo II, III, IV.

- **Objetivo Específico 3:** Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores.

  Se analizó un conjunto de herramientas y se optó por utilizar las más puntuadas por sectools.org página que analiza las mejores herramientas para el diagnóstico de vulnerabilidades y por sus funcionalidades se instaló NMAP, NESSUS, NIKTO y CAIN&ABEL para utilizarlas bajo la plataforma Centosv5.8 en cada una de las fases de acuerdo a sus características.

- **Objetivo Específico 4:** Realizar pruebas a los servidores para determinar las vulnerabilidades en los diferentes servicios que brindan.

  Mediante la herramienta NESSUS y NIKTO, se procedió a analizar los 21 servidores a cargo de la Unidad de Telecomunicaciones e Información, obteniendo muchas vulnerabilidades por falta de actualización o puertos abiertos innecesariamente y servicios instalados que no hacían falta en el servidor. Ver Anexo V y VI.

Fase III Explotación y Solución de Vulnerabilidades Lógicas: En base a las vulnerabilidades encontradas se procedió a demostrar su existencia a través de su explotación y posterior solución, a diferencia de la metodología de Análisis de Vulnerabilidades a esta fase se la denomina etapa de Evaluación en la metodología de Pentest y se basa en el análisis de las vulnerabilidades encontradas y la clasificación de las mismas, es decir en esta etapa recién se analiza los resultados de las pruebas mientras que con el Análisis de Vulnerabilidades en esta etapa ya se define la forma de explotación y sus soluciones obteniéndose los siguientes resultados.

- **Objetivo Específico 5:** Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
- Para cumplir con el presente objetivo, primeramente se procedió a explotar algunas de las vulnerabilidades lógicas con la ayuda de la herramienta CAIN&ABEL, además para solucionar las vulnerabilidades lógicas se actualizó cada uno de los servidores a los cuales la Unidad de Telecomunicaciones e Información tienen acceso, **Ver** Anexo XI y se procedió a la implementación de Iptables con políticas de DROP en cada uno de los servidores para cerrar puertos no utilizados y minimizar la posibilidad de un ataque. **Ver** Anexo VI y VII.

Fase IV Presentación de Informes: En esta fase se detalla las vulnerabilidades encontradas y las acciones a seguir para mitigar el impacto de las mismas, esta fase es muy importante y decisiva en la metodología de Análisis de Vulnerabilidades en esta fase se trata de corroborar que el trabajo en las anteriores etapas está bien realizado, y en comparación con el Pentest ha esta última etapa se la denomina de Intrusión y se busca obtener el control de todos los servidores mediante un ataque secuencial a los mismos, este tipo de metodología es muy intrusiva y podría causar muchos problemas si no se maneja con cuidado por esta razón y para evitar riesgos innecesarios se decidió utilizar la metodología de Análisis de Vulnerabilidades, y en esta última fase se obtuvo como resultado lo siguiente.

- **Objetivo Específico 6:** Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas.

  Para minimizar el impacto de las vulnerabilidades encontradas se realizó un plan de mitigación de riesgos para minimizar el impacto que pudiesen tener las mismas en la Sala de Servidores y se procedió a probar su el plan mediante simulacro en la parte física e implementación de soluciones en la parte lógica, **Ver** Anexo XIII, tratando de planear actividades antes durante y después del riesgo que pudiese presentarse. Además se planteó políticas de seguridad para la UTI.

2. VALORACIÓN TÉCNICO-ECONÓMICA-AMBIENTAL

2.1 VALORACIÓN TÉCNICA-ECONÓMICA

El presente proyecto de fin de carrera contó con todos los recursos necesarios para desarrollarlo satisfactoriamente, y las herramientas que se utilizó para el análisis de vulnerabilidades y la solución de las mismas cuentan con licencia libre, ayudando a su fácil adquisición, implementación y actualización. Siendo importante mencionar que los recursos económicos fueron asumidos en su totalidad por los tesistas.

Por lo mencionado el desarrollo del proyecto de fin de carrera fue factible ya que se cumplieron totalmente con los objetivos planteados, los recursos utilizados serán detallados a continuación:

Recursos Humanos

TABLA LII Valoración de Recursos Humanos

RECURSOS HUMANOS	CANTIDAD	Nº HORAS	COSTO/HORA	COSTO TOTAL
Asesor Proyecto	1	50	$25.00	$1,250.00
Tesistas *Cesar Bastidas* *Mariana González*	2	1200	$3.00	$7,200.00
			TOTAL	$8,450.00

Recursos Materiales

TABLA LIII Valoración de Recursos Materiales

Materiales	Cantidad	Costo Unitario	Costo Total
Resmas de Hojas A4	8	$4.00	$32.00
Anillado	10	$1.00	$10.00
Materiales de oficina	--	--	$40.00
Borde o Perfil	5	$0.50	$2.50
CD's	4	$0.50	$2.00
Empastados	4	$10.00	$40.00

Copias	1200	$0.02	$24.00
		TOTAL	$150.50

Recursos Técnicos y Tecnológicos

TABLA LIV Valoración de Recursos Técnicos y Tecnológicos

RECURSOS TÉCNICOS / TECNOLÓGICOS	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Computador Portátil Packard Bell Easynote TJ76	1	$600.00	$600.00
Computador Portátil Toshiba Satellite L500-1WH	1	$600.00	$600.00
Impresora	1	$120.00	$120.00
Servidor HP	1	$0.00	$00.00
CentOS 5.4	3	$0.00	$0.00
Nessus	3	$0.00	$00.00
Nmap	2	$0.00	$00.00
Openvas	1	$0.00	$00.00
Metasploit	1	$0.00	$00.00
		TOTAL	$1,320.00

Resumen del Presupuesto

TABLA LV Estimado del Presupuesto del Proyecto

Resumen del Presupuesto	Costo Total
Recursos Humanos	$8,250.00
Recursos Materiales	$150.50
Recursos Técnicos y Tecnológicos	$1,320.65
SUBTOTAL	$9,721.15
Imprevistos 15 %	$1,458.17
TOTAL	**$11,179.32**

2.2 VALORACIÓN AMBIENTAL

Dentro de los aspectos principales considerados para determinar las seguridades físicas en la Sala de Servidores, es que las soluciones planteadas sean ambientalmente amigables, tratando de lograr la eficiencia energética con el uso del servidor BLADE y el sistema de aire acondicionado STULZ CyberAir 2 CWE ASD 1300 CWE/CWU debido a que el ahorro en energía es la principal prioridad hoy en día, por la situación actual de disponibilidad de energía.

Además el sistema contra incendios que se sugiere adquirir para la Sala de Servidores, está basado en agentes de limpios gaseosos como el FM-200, que cuenta con Potencial de Degradación de Ozono (ODP) cero y una baja vida media Atmosférica. Fue clasificado por el EPA (Environment Protection Agency of USA) como "Sin restricción de uso".

H. CONCLUSIONES

- En la red de datos de la Universidad Nacional de Loja existe un solo domino de broadcast que provoca un bajo rendimiento en la red.
- La Sala de Servidores de la Universidad Nacional de Loja no cuenta con una correcta distribución eléctrica de la carga utilizada en cada una de las faces
- Los servidores de la Universidad Nacional de Loja tienen características de escritorio lo que hace que se eleve el riesgo a fallas ya que el hardware no es el adecuado
- Se necesita un sistema de detección de intrusos (IDS) para reducir el riesgo de ataques en los servidores.
- No se ha implementado un sistema de detección de vulnerabilidades que detecte y alerte de las vulnerabilidades a las que están expuestos los servidores.
- La Sala de Servidores de la Universidad Nacional de Loja no cuenta con una planta generadora de energía en caso de que falle el servicio de la Empresa Eléctrica Regional del Sur
- Los equipos de la Universidad Nacional de Loja no posee UPS y reguladores de voltaje que estabilicen y filtren los caídas de tensión en la red eléctrica.
- Existen 2 aires acondicionados en la sala de servidores con características de oficina que no cumple con las especificaciones necesarias para la Sala de Servidores es decir 28574 BTUs de capacidad de enfriamiento.
- La Sala de Servidores no tiene implementado un sistema contra incendios siendo muy vulnerable a la destrucción total de los equipos allí almacenados por posibles incendios.
- El servidor de respaldos está ubicado físicamente en la misma Sala de Servidores lo que es un potencial riesgo debido a que si ocurre un incendio, inundación u otro evento que implique daños severos, destrucción total o parcial de los servidores se perderá toda la información contenida en los mismos.
- La puerta de la Sala de Servidores es frágil y no brinda las seguridades necesarias ante un acceso no controlado por parte de personal ajeno a la UTI.
- Las filtraciones de líquidos son el resultado de la mala ubicación de la Sala de Servidores y de la falta de impermeabilización de la azotea.

- Nmap es un potente escáner de puertos que ayuda a detectar el estado de los puertos y las aplicaciones que corren en ellos.
- El uso de los escáner de vulnerabilidades como Nessus y Nikto, brindan una eficiente detección de vulnerabilidades lógicas y ayudan a tener una panorámica del grado de afectación de cada servidor sin causar daños a los mismos.
- La explotación de vulnerabilidades mediante herramientas como Cain y Abel, permite explotar las vulnerabilidades lógicas provocadas por el uso de protocolos de comunicación no seguros en los servidores.
- Las vulnerabilidades lógicas detectadas en los servidores están en la capa de aplicación del modelo OSI y son causadas en algunos casos por el uso de Sistemas Operativos obsoletos como Centosv5.0 y Debianv5.0 y programas desactualizados como php, apache y moodle.
- Los servidores del SGA utilizan protocolos de red no seguros para sus comunicaciones como HTTP y FTP, siendo fácil la captura de correos o contraseñas.
- Las Iptables son un mecanismo seguro para proteger servidores mediante el filtrado de paquetes.
- La falta de una DMZ expone potencialmente a posibles ataques a todos los servidores de la UTI.
- El plan de mitigación de riesgos se constituye en una herramienta valiosa para disminuir el impacto en el funcionamiento de la Sala de Servidores de posibles riesgos ocasionados por las vulnerabilidades tanto físicas como lógicas encontradas en los servidores.

I. RECOMENDACIONES

- Realizar un estudio para la implementación de VLans que alivie la creciente tormenta de broadcast en la red de la Universidad Nacional de Loja.
- Realizar un análisis exhaustivo de las instalaciones eléctricas de la Sala de Servidores.
- Virtualizar de forma completa el servidor BLADE, de esta forma se ahorrará espacio, se disminuirá el consumo de energía eléctrica y disminuirá la temperatura al interior de la sala de servidores.
- La implementación de un sistema de detección de intrusos que ayude a detectar tempranamente posibles ataques por parte de hackers.
- Realizar análisis de vulnerabilidades de forma periódica para conocer estado de los servidores ante nuevas amenazas.
- La adquisición de una planta generadora eléctrica que subministre energía auxiliar en caso de un apagón inesperado y que cuente con un sistema de transferencia automática para que se active inmediatamente ante cortes de energía inesperados, mínimo de 6000 watts de potencia.
- La implementación de UPS Online que protejan a los servidores de los milisegundos sin energía causada por cortes eléctricos, pues provee alimentación constante desde su batería y no de forma directa, mínimo de 10 KVA.
- Los sistemas de aire acondicionado tipo perimetral permiten optimizar el consumo de energía, ahorrar espacio en la Sala de Servidores y el correcto enfriamiento de los servidores mediante la creación de pasillos fríos y calientes.
- Los Sistemas Contra Incendios basados en agentes limpios son una solución ecológica, económica y menos nociva con las personas, a los riesgos por posibles incendios, además de su efectividad a la hora de extinguir flagelos.
- Adquirir una puerta blindada con cerradura biométrica para controlar y restringir el acceso a la Sala de Servidores de forma idónea.
- Impermeabilizar la azotea de la Sala de Servidores para prevenir filtraciones de líquidos en los equipos, preferiblemente con membranas impermeabilizantes ya que ofrecen mayor durabilidad y protección.
- Se debe ubicar el servidor de respaldos fuera de la Sala de Servidores, preferentemente en el del Área Educativa, Bloque 7 de Dirección en el segundo

piso por espacio físico disponible y además es donde llega los enlaces de fibra para los demás bloques, siendo menor el riesgo de fallas en la red.

- Actualizar periódicamente el Software de los servidores para evitar vulnerabilidades lógicas por desactualización.
- Usar protocolos seguros de comunicación como HTTPS, IPSEC, SSH, TLS en los servidores para disminuir el riesgo de captura de paquetes por hackers.
- La creación de scripts de Iptables en todos los servidores públicos y privados que se implementen a futuro, para mantener la seguridad de los mismos y un estándar en cuanto a protección de los datos.
- Realizar la respectiva actualización de las herramientas NMAP, NIKTO, NESSUS y Cain&Abel usadas para el desarrollo del proyecto de fin de carrera, e incrementar nuevas herramientas para el diagnóstico de vulnerabilidades lógicas.
- Crear 2 DMZ para proteger de mejor manera los servidores públicos y privados debido a que están demasiado expuestos a posibles ataques.
- Analizar y restructurar el plan de mitigación de riesgos cada año de acuerdo a las necesidades de la Unidad de Telecomunicaciones e Información previamente determinadas.
- Crear una comisión para la seguridad de la Sala de Servidores, la misma que evalúe la situación física y lógica de la misma y proponga nuevas alternativas.

J. BIBLIOGRAFÍA

LIBROS:

[12]CHESWICK, William; BELLOWIN, Steven; RUBIN, Aviel. 2003. Firewalls and Internet Security. Editorial Addison Wesley. Segunda Edición

[13]KIRCH, Olaf; DAWSON, Terry. 2000. Guía de Administración de Redes en Linux. Editorial O´Reilly & Associates. Segunda Edición

TESIS:

[7]CHÁVEZ, Alarcón. VLADIMIR Rómulo, Aplicación de la Norma técnica ISO 27001:2005 para la gestión de la seguridad de la información en el IESS. Caso práctico, dirección de desarrollo institucional, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2011. Tesis previa a la obtención del título de Ingeniero en Sistemas de la Información.

[8]DEVOTO, Liliana. Diseño e Infraestructura de Telecomunicaciones para un Data Center EIA/TIA 942. Pontificia Universidad Católica del Perú. Lima 2008. Tesis para optar por el Título de Ingeniera en Telecomunicaciones.

PÁGINAS WEB:

[1]PÁGINA OFICIAL DE DSTEAM. 2010. [En línea]. "Hacking ético vs Ataque en profundidad".ISO27001.[http://www.dsteamseguridad.com/museo/HACKIN%20ETICO_VS_DEFENSA_PROFUNDIDAD_JUANBERRIO.pdf], [Consulta: Enero 2012].

[9]PÁGINA OFICIAL DE LA UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO. 2011. [En línea]. Seguridad Física y Protección en Centros de Cómputo. [http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20III.pdf], [Consulta: Marzo 2012].

[10]PÁGINA OFICIAL DE FIKE. 2010. [En línea]. Agente limpio de supresión de incendios.[http://www.fike.com/documents/firesupp/firessys/hfc/promo/brochures/B9083%20SPA%20Clean%20Agent.pdf], [Consulta: Abril 2012].

[6]PÁGINA OFICIAL DE INFORMATICANOVA. 2012. [En línea]. Nikto escáner de servidores web. [http://www.informaticanova.com/seguridad-informatica/noticias-seguridad/67-nikto]. [Consulta: Marzo 2012].

[14]PÁGINA OFICIAL DE INTECO. 2011. [En Línea]. “Guía Avanzada de Gestión de Riesgos”. ISO 27001. [http://www.inteco.es/calidad_TIC/descargas/guias/guia_avanzada_de_gestion_de_riesgos]. [Consulta: Mayo 2012].

[11]INTERNET-SOLUTIONS. 2011. [En línea]. Seguridad Física y Lógica. [http://www.internet-solutions.com.co/ser_fisica_logica.php], [Consulta: Abril 2011].

[2]COLABORACIÓN DE VARIOS. 2009. [En línea]. [http://www.jbercero.com/index.php?option=com_content&view=article&id=72:hacking-viii-escaneo-de-vulnerabilidades&catid=40:hacking-tecnicas ycontramedidas&Itemid=66], [Consultando: Febrero 2012].

[4]PÁGINA OFICIAL DE NMAP. 2012. [En línea]. Manual para NMAP. e interfaz gráfica [http://nmap.org/zenmap/man.html], [Consulta: Febrero 2012].

[5]PÁGINA OFICIAL DE SOFTZONE. 2012. [En línea]. Comprobar seguridad con Cain y Abel 4.9.43. [http://www.softzone.es/2011/12/04/cain-and-abel-4-9-43-comprueba-la-seguridad-de-redes-y-recupera-contrasenas/]. [Consulta: Marzo 2012].

[3]PÁGINA OFICIAL DE NESUSS. 2012. [En Línea]. Instalación y configuración de Nessus. [http://static.tenable.com/], [Consulta: Febrero 2012].

K. ANEXOS

ANEXO I: Entrevistas a los encargados del Centro de Cómputo

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Entrevista dirigida a los encargados de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, con el fin de Conocer el estado actual de los servidores de la unidad con respecto a la infraestructura y el nivel de seguridades lógicas de los mismos.

Le pedimos de la manera más comedida nos ayude con la resolución de la siguiente entrevista dando respuesta con veracidad del caso que la misma merece ya que dichos resultados irán en beneficio de su institución.

Datos institucionales

Nombre: Daniel Reyes Toro

Cargo (función que desempeña): Jefe de la Unidad de Redes y Equipos Informáticos

Fecha: 08 de Diciembre del 2011

Finalidad: Realizar el diagnóstico de la situación actual del Centro de Cómputo de la Universidad Nacional Loja

Tiempo de servicio: 14 años

Entrevista

1. ¿Tiene usted algún servidor a su cargo?
2. ¿Qué tipo de servidor es?
3. ¿Qué sistema operativo tienen los servidores?
4. ¿Los servidores cuentan con seguridades lógicas? ¿Cuáles son?

5. ¿Los servidores han sido atacados por algún hacker? ¿Qué tipo de ataque fue?
6. ¿Se monitorea el tráfico que reciben los servidores? ¿Con que frecuencia?
7. ¿El acceso a los servidores de la unidad es restringido?
8. ¿Quiénes tienen acceso a los servidores?
9. ¿La ubicación del centro de datos es la correcta? ¿Por qué?
10. ¿La distribución de los servidores dentro de centro de datos es la correcta?
11. ¿El hardware de los servidores es el idóneo?
12. ¿La temperatura del data center es la adecuada?
13. ¿Los servidores cuentan con un sistema de energía auxiliar o de emergencia?
14. ¿Los servidores cuentan con un adecuado sistema de potencia eléctrica?
15. ¿Los servidores cuentan con una adecuada instalación de puesta a tierra en caso de sobrecarga eléctrica?

RESUMEN

En la Unidad de telecomunicaciones e información se manejan servidores públicos y privados, dentro de los públicos tenemos un servidor web, un servidor de una plataforma virtual, dentro de los privados tenemos DHCP, firewall, DNS, servidores proxys de cada una de las áreas, proxy wireless, proxy para administración central, un servidor Asterisk, un servidor Nagios, también están los servidores del SGA pero no están a nuestro cargo solo están ubicados físicamente en el cuarto frío.

Los tipos de seguridades lógicas con las que cuentan nuestros servidores están las iptables, SSH y el firewall. Hemos sufrido ataques externos a nuestro servidor de correo ya que jackearon las cuentas y suplantaron la identidad de algunos usuarios, citando el caso más grave como la suplantación de identidad a través de la IP pública que se realizó al servidor del Área Energía que no se maneja en la UTI. En la actualidad no se realiza monitoreo de trafico de red contantemente.

En cuanto a las vulnerabilidades físicas el acceso al cuarto frío no es totalmente restringido ya que técnicos, pasantes y tesistas ingresan libremente por falta de conocimiento acerca de las restricciones de ingreso al Data Center.

La ubicación del Centro de Datos no es la adecuada pero la fibra del proveedor llega a este piso y edificio por lo que resultaría muy costoso reubicar el Data Center pero hay

ciertas normas en cuanto a la construcción de Data Center que si se siguen se puede hacer un lugar más adecuado.

La distribución de los servidores públicos y privados en el centro de Datos se realiza mediante perchas pero siguiendo normas concernientes a Data Center se puede mejorar la distribución de los equipos.

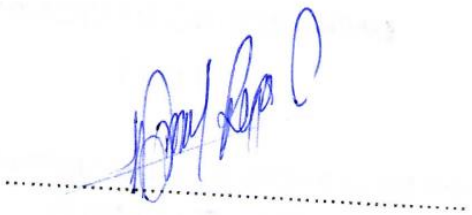
Los servidores están instalados en PCs normales y también en equipos con características para servidores como HP Proliant. Estos servidores no cuentan con un sistema auxiliar de energía, pero en la actualidad se ha realizado un pedido al rector de un UPS de 40 KVA que se espera satisfaga las necesidades de energía en el Centro de Datos.

La energía auxiliar se basa en el uso de UPS, existe un proyecto para la construcción de una planta generación eléctrica, como respaldo de la energía auxiliar, debido a que se tiene pocos cortes de energía eléctrica pero cuando se dan son muy prolongados.

La parte eléctrica no es manejada directamente por la UTI, siempre se ha realizado mediante personas o empresas externas, y para realizar la instalación de todos los servidores se hizo el cálculo del diámetro del conductor, la potencia que soporta para satisfacer las necesidades de ese entonces, dicho estudio se realizó hace 5 años y en la actualidad se han instalado muchos equipos causando problemas eléctricos por sobrecarga en ciertas líneas los mismos que se han solucionado redistribuyendo internamente los equipos para equiparar la carga en ciertas líneas, pero en si no existe un estudio eléctrico del Data Center.

Para salvaguardar los equipos de variaciones eléctricas constantes que han causados daños a los servidores se cuenta con una malla de tierra, que ha ayudado mucho en este tema

En los servidores está instalado software de acuerdo al servicio que presta y software libre como Centos con diferentes versiones, dependiendo del servicio que está corriendo tiene su versión instalada por ejemplo DNS tiene instalado el software Bind, Web tiene software como apache, mysql en servidores proxy se utiliza squid y se hace control de contenido con dansguardian.



Tngo. Daniel Reyes Toro

RESPONSABLE SECCION REDES

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Entrevista dirigida a los encargados de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, con el fin de Conocer el estado actual de los servidores de la unidad con respecto a la infraestructura y el nivel de seguridades lógicas de los mismos.

Le pedimos de la manera más comedida nos ayude con la resolución de la siguiente entrevista dando respuesta con veracidad del caso que la misma merece ya que dichos resultados irán en beneficio de su institución.

Datos institucionales

Nombre: Ing. Patricio Valarezo

Cargo (función que desempeña): Responsable de la Sección de Desarrollo de Software

Fecha: 08 de Diciembre del 2011

Finalidad: Análisis de la situación actual

Tiempo de servicio: 2 años

Entrevista

1. ¿Tiene usted algún servidor a su cargo?
2. ¿Qué tipo de servidor es?
3. ¿Qué sistema operativo tienen los servidores?
4. ¿Los servidores cuentan con seguridades lógicas?¿Cuáles son?
5. ¿Los servidores han sido atacados por algún hacker? ¿Qué tipo de ataque fue?
6. ¿Se monitorea el tráfico que reciben los servidores? ¿Con que frecuencia?
7. ¿El acceso a los servidores de la unidad es restringido?
8. ¿Quiénes tienen acceso a los servidores?
9. ¿La ubicación del centro de datos es la correcta? ¿Por qué?
10. ¿La distribución de los servidores dentro de centro de datos es la correcta?
11. ¿El hardware de los servidores es el idóneo?

12. ¿La temperatura del data center es la adecuada?
13. ¿Los servidores cuentan con un sistema de energía auxiliar o de emergencia?
14. ¿Los servidores cuentan con un adecuado sistema de potencia eléctrica?
15. ¿Los servidores cuentan con una adecuada instalación de puesta a tierra en caso de sobrecarga eléctrica?

RESUMEN

Tengo a cargo uno de los blades de tres o cuatro que se adquirieron por la parte de la universidad, este blade es un equipo robusto cuneta con 16Gb de memoria RAM, dos procesadores, y aparte tengo asignado un espacio en el data center para el almacenamiento de información y de tres procesos del sistema de gestión académico más virtualizaciones de proyectos que se desarrollan en la unidad, aparate de eso tenemos equipos normales que están funcionando como servidores, de esos tememos diez equipos de los cuales dos o tres si tienen características de servidor los demás son equipos de escritorio normales, sin embargo estos servidores forman un clúster para el sistema de gestión académico.

Todos los servidores están trabajando con el sistema operativo Debían en su última versión estable partiendo desde la configuración básica del servidor ninguno tiene ambiente gráfico.

Nuestro departamento no se encarga de la seguridad a nivel de redes porque para eso está el departamento de redes sin embargo nosotros hemos hecho una isolación de la red para poder proteger a los equipos en primera instancia, los equipos que tienen salida directa a internet cuentan con firewall las protecciones básicas que tienen que ver con la lógica de deployment de algún equipo.

Siempre hay intentos por parte de usuarios que tratan de ser hackers, sin embargo sin ningún éxito, nosotros siempre hemos revisado que existen intentos de acceso no autorizado pero nunca se ha cumplido el cometido eso es normal en un equipo que está sometido al internet, incluso por curiosidad la gente externa trata de revisar que tiene, escaneos básico siempre ha habido, sin embargo nosotros guardamos el histórico de lo que está haciendo el servidor en todo momento.

De acuerdo con la estructura que nosotros implementamos el esquema de deployment de los servidores implica que existe solo un servidor afuera este es el único que recibe los request los demás son obviamente internos entonces es tráfico no es necesario monitorear es obvio que el tráfico interno de la red isolada es de esa red el trafico externo en cierta parte no me compete por cuanto a mí me entregan una ip pública y yo trabajo con esa ip pero hay siempre hay alguien más adelante siempre está la empresa telconet y gente así e incluso el departamento de redes que es quien debería estar monitoreando la red nosotros hacemos el software.

Solo yo tengo acceso a los servidores y puedo dar de altas y bajas, de hecho el acceso se lo hace a través de ssh por medio de credencia les ssh A1 y Des, existe un certificado que solo lo tengo yo, con lo que es lo único con lo que se puede acceder

En cuanto al acceso físico yo no soy el dueño el data center, no lo tengo aquí, desde el punto de vista mío como director del departamento siempre necesito que alguien me ayude, por ejemplo moviendo un servidor o de pronto algún servidor se recalentó y toca sacarlo, normalmente eso lo hago con la compañía de alguien, pero por políticas de la unidad no se autoriza el acceso a nadie sin embargo no existe la seguridad absoluta en un sistema, el único servidor protegido en el que está apagado. Con el presupuesto que tenemos creo que está bien el data center en relación a otras universidades que he visto, es en función mucho del presupuesto.

Lo que pasa es que nosotros en un inicio lo que hicimos fue la improvisación, improvisamos la puesta en funcionamiento de todos los servidores para que formen un gran servidor, la otra opción era comprar un gran servidor y eso fue lo que se hizo en primera instancia con el equipo que tenemos en la actualidad el blade pero nosotros no tenemos el control total de ese servidor nosotros tenemos una de las cuatro cuchillas, con lo cual pudiéramos eliminar todos los equipos que tenemos ahí lo que nos haría más eficientes pero esto implica una inversión mayor, la necesidad nos ha obligado a utilizar equipos de baja gama pero que funciona, sin embargo se ha propuesto la necesidad de hacer el cambio sobre todo si se piensa crecer, hemos notificado como departamento que la infraestructura está al límite y que para abordar nuevos retos en el futuro necesitamos migrar a un sistema de servidores ya protegidos que tengan redundancia e incluso redundancia de poder aquí que es lo que pasa, se apaga la luz y se apaga todito y toca volver a empezar y eso es peligroso porque puede llegar a la perdida de datos pero eso ya es más cuestión administrativa que nuestra.

Hay que tomar en cuenta que la temperatura óptima la da el fabricante del producto y también depende mucho del hardware sin embargo pienso que puede ser un gran problema lo de la temperatura pero así como está solucionado está bien.

Bueno hasta que yo se la potencia eléctrica es la que llega de la empresa eléctrica, de lo que yo sé es que existe una fuente de poder única y con sus respectivos protectores de voltaje que nos dan una independencia de diez minutos para que podamos apagar los equipos pero no es una garantía

Habría que analizar la situación de la puesta a tierra puesto que cuando yo llegue a trabajar al data center ya estaba montado, no es mi fuerte ni tampoco es mi responsabilidad.

……

Ing. Patricio Valarezo

RESPONZABLE SECCION

DESARROLLO DE SOFTWARE

ANEXO II: Obtención de las características hardware de los servidores

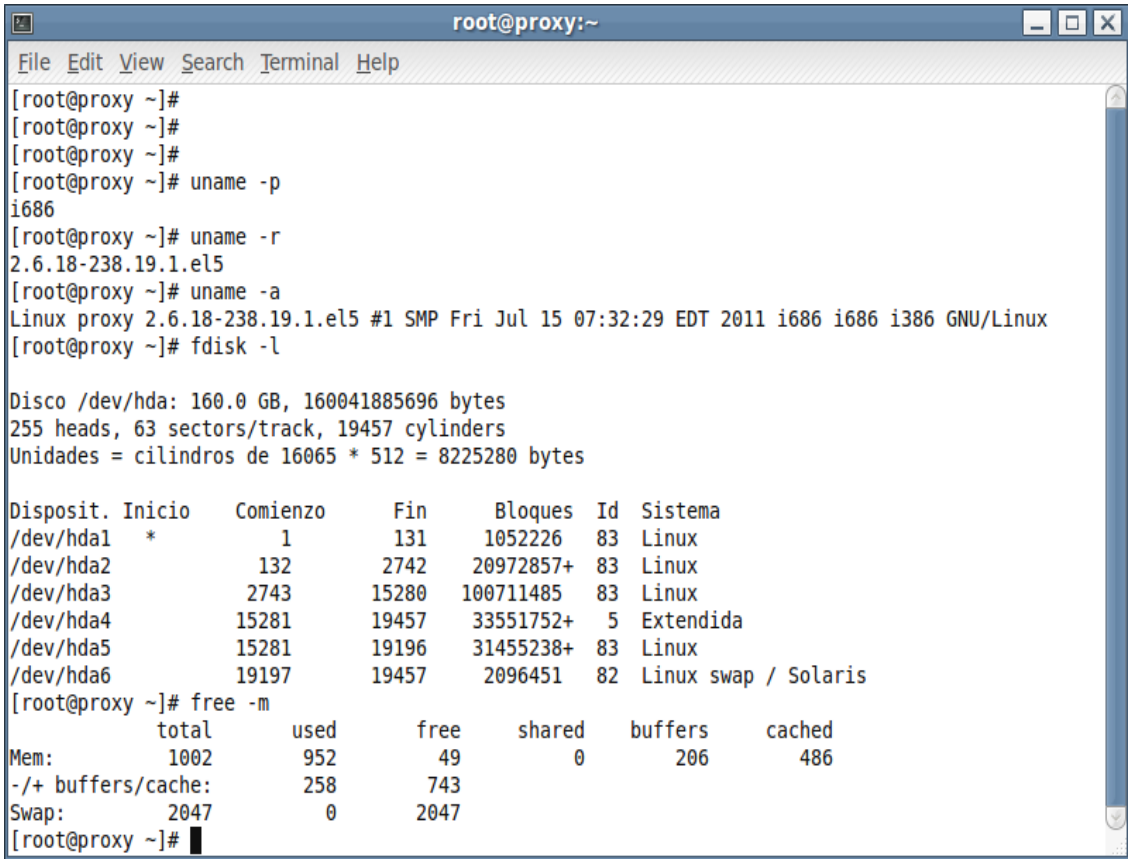


Figura 78. Datos sobre Disco y memoria RAM de los servidores

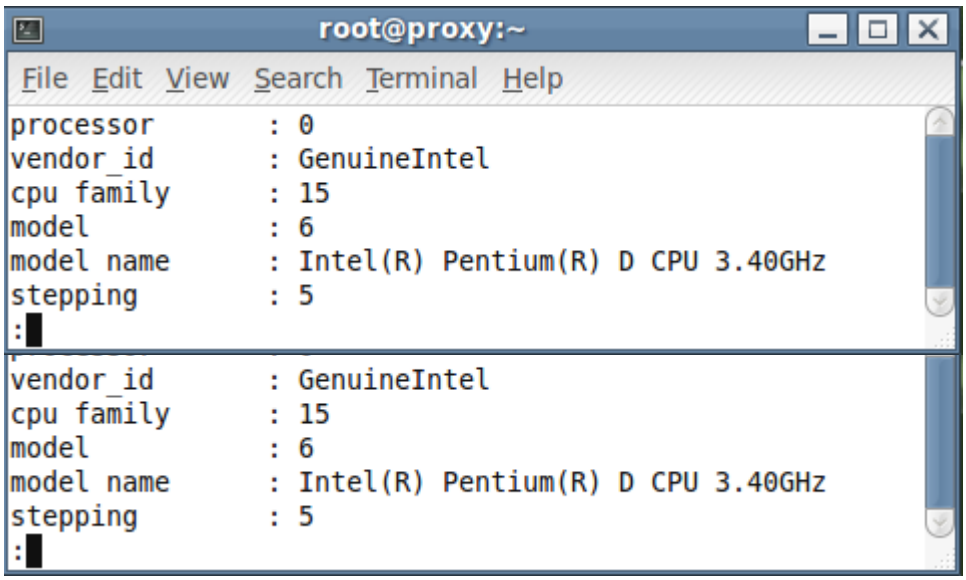


Figura 79. Modelo de procesador de los servidores

ANEXO III: Proforma del Servidor Blade

Cliente: UNIVERSIDAD NACIONAL DE LOJA
Atención: Lcdo. Jamil Ramón
Fecha: jueves, 19 de mayo de 2011
Observación: Proforma Servidor HP BL 460 G7

I	D	Qty.	P. Unitario	P. Total
	Servidor HP BL 460G7			
1	**HP BL460c G7 X5650 6G 1P Svr** **Procesador:** Intel® Xeon® X5650 (2.66GHz/6-core/12MB/95W, DDR3-1333, HT, Turbo 2/2/2/2/3/3), **Memoria RAM:** 6GB; **Puerto de LAN:** NC553i Dual Port FlexFabric 10Gb; **Controlador de Discos:** HP Smart Array P410i Controller (RAID 0/1)	1	$ 5.739,30	**$ 5.739,30**
2	**Procesador Adicional:** HP BL460c G7 X5650 FIO Kit	1	$ 2.331,67	**$ 2.331,67**
3	**Memoria Ram Adicional:** HP 4GB 2Rx4 PC3-10600R-9 Kit	4	$ 401,35	**$ 1.605,40**
4	**Almacenamiento Interno:** HP 300GB 10K 6G 2.5 SAS	2	$ 844,67	**$ 1.689,33**
5	**Conectividad FC al Storage:** HP BLc QLogic QMH2562 8Gb FC HBA Opt	1	$ 1.514,75	**$ 1.514,75**
6	**Contrato de Soporte:** HP 3y 4h 24x7 BL4xxc Svr Bld HW	1	$ 429,08	**$ 429,08**
			Precio Total:	**$ 13.309,53**
			IVA 12%:	**$ 1.597,14**
			TOTAL:	**$ 14.906,67**

Forma de Pago: 60% en adelanto, 40% contra entrega **Tiempo de Entrega:** 45 días a partir de recepción de anticipo **Validez de la oferta:** 15 días
Garantía: 36 meses sobre defectos de Fabricación para servidor

Cordialmente,

Geovanny Pesantez A
Gerente de Cuentas Corporativas
COMPUEQUIP DOS

La información contenida en esta propuesta ha sido preparada por Compuequip DOS en exclusividad para UNIVERSIDAD NACION y no podrá ser difundida ni enviada en forma parcial o completa ni escrita o electrónica sin el consentimiento de Compuequio DOS

ANEXO IV: Proforma Firewall Cisco ASA 5585, Gestionador de Ancho de Banda y UPS 10KVA

Cliente : Universidad Nacional de Loja
Atención: Ing. Milton Palacios
Fecha: jueves, 25 de octubre de 2012
Observación: Presupuesto Firewall Cisco ASA 5585, Gestionador de Ancho de Banda y UPS 10KVA

Item	Descriptio	Qty.	P. Unitario	P. Total
	EQUIPO FIREWALL CISCO ASA 5585			
1	ASA 5585-X Chas with	1	$ 44.394,45	**$ 44.394,45**
2	Active Twinax cable assembly, 10m	1	$ 455,10	**$ 455,10**
3	ASA 5500 5 Security Contexts License	1	$ 4.762,50	**$ 4.762,50**
4	SMARTNET 8X5XNBD ASA 5585-X Chas with	1	$ 8.380,73	**$ 8.380,73**
	EQUIPO GESTIONADOR DE ANCHO DE			
5	PacketShaper 10000, Copper, Up to 200 Mbps of shaping, 2048/5000	1	$ 61.050,00	**$ 61.050,00**
6	BlueTouch Partner, 24x7 L3 Software Only, Packetshaper 10000, Up to	1	$ 7.326,00	**$ 7.326,00**
7	Same Day Ship, Support, Hardware Only, Packetshaper 10000, Up to	1	$ 1.831,50	**$ 1.831,50**
	SERVICIOS PROFESIONALES DOS			
8	Implementación Firewall Cisco ASA5585 24 horas, Capacitación Firewall Cisco ASA5585 20 horas	1	$ 5.000,00	**$ 5.000,00**
9	Implementación BlueCoat PacketShaper 24 horas, Capacitación BlueCoat PacketShaper 20 horas	1	$ 5.000,00	**$ 5.000,00**
	UPS POWERCOM DE 10KVA ONLINE			

	Marca Powercom / Modelo VANGUARD 10000VA (10KVA) / Tecnologia On Line Doble Conversion / ENTRADA AC: Voltaje de entrada 220Voltios, Rango de voltaje de entrada: 180-276V AC sin usar baterías, Frecuencia: 50/60Hz. detencion automatica, Factor de Potencia FP 0,99 / SALIDA AC: Capacidad 10000VA - 7000Watts, Voltaje de salida 110/220Voltios, Frecuencia: 50/ 60Hz. +/-0.5%, Crest Factor 3:1, Factor de Potencia FP 0,7; Transformador de Aislamiento AC, 1 BORNERA AC DE SALIDA DE RESPALDO, Forma de Onda: Sinusoidal Pura, Distorsión Armonica: <3% de T.H.D de carga en línea, Tiempo de transferencia: 0 ms, BATERIAS: Libres de mantenimiento de plomo acido selladas, Voltaje (Vdc): 240V, Tipo de Bateria: 20 x12V9AH, Tiempo de respaldo 7 minutos a full carga y 15 minutos al 50% de la carga, PANEL DIGITAL LCD: Mide la carga, estado de baterías, alarmas, temperatura. CAPACIDAD DE CONTROL Y ADMINISTRACION EN RED: Software de monitoreo, puerto serial RS-232 y Tarjeta SNMP (opcional)	2	$ 6.150,00	**$ 12.300,00**
			Precio Total: **IVA 12%:** **TOTAL:**	**$ 150.500,28** **$ 18.060,03** **$ 168.560,31**

Forma de Pago: 60% en adelanto, 40% contra entrega
Tiempo de Entrega: 60 días a partir de recepción de anticipo
Validez de la oferta: 15 días
Garantía: 12 meses sobre defectos de Fabricación
Cordialmente,

Geovanny Pesantez A.
Gerente de Cuentas Corporativas
COMPUEQUIP DOS

ANEXO V: Informes históricos de Nessus de los servidores

Servidores Privados

proxy

Scan Information

Start time:	Thu Mar 15 09:06:02 2012
End time:	Thu Mar 15 09:15:36 2012

Host Information

DNS Name:	proxy
IP:	172.16.32.13
MAC Address:	00:19:bb:e4:aa:13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	20	20

agropecuaria

Scan Information

Start time:	Thu Mar 15 09:59:08 2012
End time:	Thu Mar 15 10:09:21 2012

Host Information

DNS Name:	agropecuaria
IP:	172.16.40.1
MAC Address:	00:01:02:68:4b:7c
OS:	Cyber Switching ePower PDU

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

educativa

Scan Information

Start time:	Thu Mar 15 09:31:59 2012
End time:	Thu Mar 15 09:42:01 2012

Host Information

DNS Name:	educativa
IP:	172.16.35.1
MAC Address:	d4:85:64:bd:c3:0d
OS:	Linux Kernel 2.6 on CentOS Linux release 6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	36	39

proxy

Scan Information

Start time:	Thu Mar 15 10:08:45 2012
End time:	Thu Mar 15 10:18:20 2012

Host Information

DNS Name:	proxy
IP:	172.16.32.13
MAC Address:	00:19:bb:e4:aa:13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	20	20

juridica

Scan Information

Start time:	Thu Mar 15 09:49:31 2012
End time:	Thu Mar 15 09:59:39 2012

Host Information

DNS Name:	juridica
IP:	172.16.37.1
MAC Address:	00:01:6c:13:e6:62
OS:	Cyber Switching ePower PDU

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

proxymed.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 11:23:00 2012
End time:	Mon Apr 30 11:41:57 2012

Host Information

DNS Name:	proxymed.unl.edu.ec
IP:	172.16.32.28
MAC Address:	00:1c:25:ea:1c:cb
OS:	Linux Kernel 2.6 on CentOS release 5

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	3	0	31	35

proxy

Scan Information

Start time:	Thu Mar 15 10:31:49 2012
End time:	Thu Mar 15 10:41:24 2012

Host Information

DNS Name:	proxy
IP:	172.16.32.13
MAC Address:	00:19:bb:e4:aa:13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	20	20

proxy

Scan Information

Start time:	Thu Mar 15 09:22:22 2012
End time:	Thu Mar 15 09:31:58 2012

Host Information

DNS Name:	proxy
IP:	172.16.32.13
MAC Address:	00:19:bb:e4:aa:13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	19	19

dns

Scan Information

Start time:	Thu Mar 15 09:05:24 2012
End time:	Thu Mar 15 09:11:26 2012

Host Information

DNS Name:	dns
IP:	172.16.32.2
MAC Address:	00:12:79:55:8b:86
OS:	Linux Kernel 2.6.18-194.3.1.el5

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	1	0	31	33

firewall

Scan Information

Start time:	Thu Mar 15 09:04:14 2012
End time:	Thu Mar 15 09:13:52 2012

Host Information

DNS Name:	firewall
IP:	192.188.49.5

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

noc.unl.edu.ec

Scan Information

Start time:	Wed Apr 4 15:19:05 2012
End time:	Wed Apr 4 16:30:56 2012

Host Information

DNS Name:	noc.unl.edu.ec
IP:	172.16.32.3
MAC Address:	00:19:bb:e4:9f:80
OS:	Linux Kernel 2.6.32-131.21.1.el6.i686 (i386)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	9	2	63	75

dhcp

Scan Information

Start time:	Thu Mar 15 09:05:24 2012
End time:	Thu Mar 15 09:11:19 2012

Host Information

DNS Name:	dhcp
IP:	172.16.32.4
MAC Address:	00:12:79:55:8b:86
OS:	Linux Kernel 2.6.18-194.3.1.el5

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	1	1	22	25

soporte.unl.edu.ec

Scan Information

Start time:	Tue May 15 15:56:34 2012

Host Information

DNS Name:	soporte.unl.edu.ec
IP:	172.16.32.24
MAC Address:	00:19:db:bc:b9:b5

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	13	14

Servidores Públicos

radio.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 08:59:32 2012
End time:	Mon Apr 30 09:23:26 2012

Host Information

DNS Name:	radio.unl.edu.ec
IP:	192.188.49.50
OS:	Linux Kernel 2.6 on Ubuntu 11.04 (natty)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	22	23

radius.unl.edu.ec

Scan Information

Start time:	Tue May 22 11:02:30 2012
End time:	Tue May 22 11:13:47 2012

Host Information

DNS Name:	radius.unl.edu.ec
IP:	172.16.32.20
MAC Address:	00:08:a1:2b:ee:32

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

evaluacion.unl.edu.ec

Scan Information

Start time:	Fri Apr 27 08:31:38 2012
End time:	Fri Apr 27 08:41:31 2012

Host Information

DNS Name:	evaluacion.unl.edu.ec
IP:	172.16.32.10
MAC Address:	b0:48:7a:81:15:45
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	1	1	43	46

colegiomcl.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 09:00:43 2012
End time:	Mon Apr 30 09:16:49 2012

Host Information

DNS Name:	colegiomcl.unl.edu.ec
IP:	192.188.49.36
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	16	17

cursos.unl.edu.ec

Scan Information

Start time:	Thu Apr 26 09:47:04 2012

Host Information

DNS Name:	cursos.unl.edu.ec
IP:	192.188.49.13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
4	8	32	6	54	104

aeirnnr.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 08:23:26 2012
End time:	Mon Apr 30 10:34:09 2012

Host Information

DNS Name:	aeirnnr.unl.edu.ec
IP:	192.188.49.12
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	5	3	28	38

tae.unl.edu.ec

Scan Information

Start time:	Thu Apr 26 09:48:03 2012

Host Information

DNS Name:	tae.unl.edu.ec
IP:	192.188.49.16
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	4	0	17	21

mail.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 10:48:49 2012
End time:	Mon Apr 30 11:00:37 2012

Host Information

DNS Name:	mail.unl.edu.ec
IP:	192.188.49.5

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

cursosmed.unl.edu.ec

Scan Information

Start time:	Fri Apr 27 08:35:19 2012

Host Information

DNS Name:	cursosmed.unl.edu.ec
IP:	192.188.49.11
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	8	14	2	53	77

virtual.unl.edu.ec

Scan Information

Start time:	Thu Apr 26 09:51:24 2012
End time:	Thu Apr 26 12:12:07 2012

Host Information

DNS Name:	virtual.unl.edu.ec
IP:	192.188.49.10
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	8	17	2	57	84

admisiones.unl.edu.ec

Scan Information

Start time:	Mon Apr 30 10:52:42 2012
End time:	Mon Apr 30 11:14:08 2012

Host Information

DNS Name:	admisiones.unl.edu.ec
IP:	192.188.49.3
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	1	0	37	39

www.unl.edu.ec

Scan Information

Start time:	Mon Apr 9 10:12:18 2012

Host Information

DNS Name:	www.unl.edu.ec
IP:	192.188.49.2
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	7	2	28	40

Servidores SGA

192.168.112.6

Scan Information

Start time:	Wed Nov 7 10:26:08 2012
End time:	Wed Nov 7 10:36:18 2012

Host Information

IP:	192.168.112.6
MAC Address:	00:1c:25:2c:b6:6a
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	2	0	39	43

192.168.112.20

Scan Information

Start time:	Wed Nov 7 10:46:08 2012
End time:	Wed Nov 7 11:04:16 2012

Host Information

IP:	192.168.112.20
MAC Address:	f4:ce:46:89:fb:00
OS:	Linux Kernel 2.6 on Debian 6.0 (squeeze)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	0	127	141

192.168.112.2

Scan Information

Start time:	Wed Nov 7 03:23:43 2012
End time:	Wed Nov 7 03:49:49 2012

Host Information

IP:	192.168.112.2
MAC Address:	00:00:6c:90:e7:3e
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
2	2	15	0	68	87

192.168.112.3

Scan Information

Start time:	Wed Nov 7 03:24:15 2012
End time:	Wed Nov 7 09:52:11 2012

Host Information

IP:	192.168.112.3
MAC Address:	00:1e:8c:98:64:09
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	7	3	49	61

192.168.112.4

Scan Information

Start time:	Wed Nov 7 10:25:32 2012
End time:	Wed Nov 7 11:08:48 2012

Host Information

IP:	192.168.112.4
MAC Address:	00:1c:25:ea:1b:33
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	2	13	1	94	111

evaluacion.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:05:28 2012
End time:	Tue Nov 6 12:15:29 2012

Host Information

DNS Name:	evaluacion.unl.edu.ec
IP:	172.16.32.10
MAC Address:	b0:48:7a:81:15:45
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	1	31	33

colegiomcl.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:06:29 2012
End time:	Tue Nov 6 12:25:36 2012

Host Information

DNS Name:	colegiomcl.unl.edu.ec
IP:	192.188.49.36
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

192.168.112.1

Scan Information

Start time:	Tue Nov 6 05:39:03 2012
End time:	Tue Nov 6 05:48:05 2012

Host Information

IP:	192.168.112.1
MAC Address:	b0:48:7a:81:15:45
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	1	1	28	31

admisiones.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:06:59 2012
End time:	Tue Nov 6 12:24:23 2012

Host Information

DNS Name:	admisiones.unl.edu.ec
IP:	192.188.49.3
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	24	25

192.168.112.99

Scan Information

Start time:	Tue Nov 6 07:02:42 2012
End time:	Tue Nov 6 07:11:48 2012

Host Information

IP:	192.168.112.99
MAC Address:	00:1c:25:28:15:95
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	23	24

192.168.112.8

Scan Information

Start time:	Wed Nov 7 10:26:48 2012
End time:	Wed Nov 7 10:37:41 2012

Host Information

IP:	192.168.112.8
MAC Address:	00:23:7d:dc:89:7a
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	57	62

192.168.112.9

Scan Information

Start time:	Wed Nov 7 03:26:45 2012
End time:	Wed Nov 7 03:36:59 2012

Host Information

IP:	192.168.112.9
MAC Address:	00:1e:0b:d5:61:28
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	5	0	65	72

192.168.112.13

Scan Information

Start time:	Wed Nov 7 10:57:59 2012
End time:	Wed Nov 7 11:07:35 2012

Host Information

IP:	192.168.112.13
MAC Address:	00:1c:25:28:15:18
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	2	0	30	33

ANEXO VI: Informes de resultados de Nessus y Nikto de los servidores

NESSUS

Servidores Privados

adcentral.unl.edu.ec

Scan Information

Start time:	Tue May 22 10:17:03 2012
End time:	Tue May 22 10:30:28 2012

Host Information

DNS Name:	adcentral.unl.edu.ec
IP:	172.16.32.13
MAC Address:	00:19:bb:e4:aa:13
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	34	34

172.16.40.1

Scan Information

Start time:	Wed May 23 10:25:41 2012
End time:	Wed May 23 10:37:02 2012

Host Information

IP:	172.16.40.1
MAC Address:	00:01:02:68:4b:7c
OS:	Cyber Switching ePower PDU

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	14	14

172.16.35.1

Scan Information

Start time:	Tue May 22 10:38:24 2012
End time:	Tue May 22 10:46:14 2012

Host Information

IP:	172.16.35.1
MAC Address:	08:2e:5f:03:d0:d0
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	33	33

172.16.43.1

Scan Information

Start time:	Tue May 22 10:41:58 2012
End time:	Tue May 22 12:06:37 2012

Host Information

IP:	172.16.43.1
MAC Address:	00:17:a4:f8:16:f2
OS:	Linux Kernel 2.6 on CentOS release 5

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	34	37

172.16.37.1

Scan Information

Start time:	Wed May 23 06:26:17 2012
End time:	Wed May 23 06:37:37 2012

Host Information

IP:	172.16.37.1
MAC Address:	00:01:6c:13:e6:62
OS:	Cyber Switching ePower PDU

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	14	14

proxymed.unl.edu.ec

Scan Information

Start time:	Tue May 29 04:02:56 2012
End time:	Tue May 29 04:14:23 2012

Host Information

DNS Name:	proxymed.unl.edu.ec
IP:	172.16.32.28
MAC Address:	00:1c:25:ea:1c:cb
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	16	16

172.16.45.2

Scan Information

Start time:	Thu Jun 7 05:01:52 2012
End time:	Thu Jun 7 05:18:56 2012

Host Information

IP:	172.16.45.2
MAC Address:	d4:85:64:bc:c5:11
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

proxywifi.unl.edu.ec

Scan Information

Start time:	Tue May 22 10:29:43 2012
End time:	Tue May 22 10:39:48 2012

Host Information

DNS Name:	proxywifi.unl.edu.ec
IP:	172.16.32.27
MAC Address:	00:23:24:06:cd:14
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	13	14

fw.unl.edu.ec

Scan Information

Start time:	Tue May 22 07:25:53 2012
End time:	Tue May 22 07:34:52 2012

Host Information

DNS Name:	fw.unl.edu.ec
IP:	172.16.32.1
MAC Address:	00:18:fe:fe:95:76
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	19	19

noc.unl.edu.ec

Scan Information

Start time:	Thu Jul 5 09:04:20 2012
End time:	Thu Jul 5 09:57:13 2012

Host Information

DNS Name:	noc.unl.edu.ec
IP:	172.16.32.3
MAC Address:	00:19:bb:e4:9f:80
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

dns.unl.edu.ec

Scan Information

Start time:	Wed Jun 6 03:57:41 2012
End time:	Wed Jun 6 04:09:30 2012

Host Information

DNS Name:	dns.unl.edu.ec
IP:	172.16.32.2
MAC Address:	00:12:79:55:8b:86
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

soporte.unl.edu.ec

Scan Information

Start time:	Thu Jul 5 08:54:06 2012
End time:	Thu Jul 5 09:46:57 2012

Host Information

DNS Name:	soporte.unl.edu.ec
IP:	172.16.32.24
MAC Address:	00:19:db:bc:b9:b5
OS:	Linux Kernel 3.0 on Ubuntu 12.04 (precise)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

radius.unl.edu.ec

Scan Information

Start time:	Tue May 22 10:48:39 2012
End time:	Tue May 22 10:58:22 2012

Host Information

DNS Name:	radius.unl.edu.ec
IP:	172.16.32.20
MAC Address:	00:08:a1:2b:ee:32

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

172.16.63.11

Scan Information

Start time:	Thu May 10 16:51:19 2012
End time:	Thu May 10 16:57:25 2012

Host Information

IP:	172.16.63.11
MAC Address:	08:2e:5f:03:d0:d0
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	21	21

cursos.unl.edu.ec

Scan Information

Start time:	Wed Jul 11 08:20:12 2012
End time:	Wed Jul 11 12:04:58 2012

Host Information

DNS Name:	cursos.unl.edu.ec
IP:	192.188.49.13
OS:	Linux Kernel 3.2, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	2	30	35

192.188.45.5

Scan Information

Start time:	Tue May 22 11:01:52 2012
End time:	Tue May 22 11:02:03 2012

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1

radio.unl.edu.ec

Scan Information

Start time:	Tue May 22 11:05:17 2012
End time:	Tue May 22 11:17:46 2012

Host Information

DNS Name:	radio.unl.edu.ec
IP:	192.188.49.50
OS:	Linux Kernel 2.6 on Ubuntu 11.04 (natty)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	20	21

www.unl.edu.ec

Scan Information

Start time:	Thu Sep 27 13:32:53 2012

Host Information

DNS Name:	www.unl.edu.ec
IP:	192.188.49.2
OS:	Linksys Wireless Access Point, Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	2	30	32

Servidores SGA

192.168.112.6

Scan Information

Start time:	Wed Nov 7 10:26:08 2012
End time:	Wed Nov 7 10:36:18 2012

Host Information

IP:	192.168.112.6
MAC Address:	00:1c:25:2c:b6:6a
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	2	0	39	43

192.168.112.20

Scan Information

Start time:	Wed Nov 7 10:46:08 2012
End time:	Wed Nov 7 11:04:16 2012

Host Information

IP:	192.168.112.20
MAC Address:	f4:ce:46:89:fb:00
OS:	Linux Kernel 2.6 on Debian 6.0 (squeeze)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	0	127	141

192.168.112.2

Scan Information

Start time:	Wed Nov 7 03:23:43 2012
End time:	Wed Nov 7 03:49:49 2012

Host Information

IP:	192.168.112.2
MAC Address:	00:00:6c:90:e7:3e
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
2	2	15	0	68	87

192.168.112.3

Scan Information

Start time:	Wed Nov 7 03:24:15 2012
End time:	Wed Nov 7 09:52:11 2012

Host Information

IP:	192.168.112.3
MAC Address:	00:1e:8c:98:64:09
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	7	3	49	61

192.168.112.4

Scan Information

Start time:	Wed Nov 7 10:25:32 2012
End time:	Wed Nov 7 11:08:48 2012

Host Information

IP:	192.168.112.4
MAC Address:	00:1c:25:ea:1b:33
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	2	13	1	94	111

evaluacion.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:05:28 2012
End time:	Tue Nov 6 12:15:29 2012

Host Information

DNS Name:	evaluacion.unl.edu.ec
IP:	172.16.32.10
MAC Address:	b0:48:7a:81:15:45
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	1	31	33

colegiomcl.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:06:29 2012
End time:	Tue Nov 6 12:25:36 2012

Host Information

DNS Name:	colegiomcl.unl.edu.ec
IP:	192.188.49.36
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

192.168.112.1

Scan Information

Start time:	Tue Nov 6 05:39:03 2012
End time:	Tue Nov 6 05:48:05 2012

Host Information

IP:	192.168.112.1
MAC Address:	b0:48:7a:81:15:45
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	1	1	28	31

admisiones.unl.edu.ec

Scan Information

Start time:	Tue Nov 6 12:06:59 2012
End time:	Tue Nov 6 12:24:23 2012

Host Information

DNS Name:	admisiones.unl.edu.ec
IP:	192.188.49.3
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	24	25

192.168.112.99

Scan Information

Start time:	Tue Nov 6 07:02:42 2012
End time:	Tue Nov 6 07:11:48 2012

Host Information

IP:	192.168.112.99
MAC Address:	00:1c:25:28:15:95
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	0	0	23	24

192.168.112.8

Scan Information

Start time:	Wed Nov 7 10:26:48 2012
End time:	Wed Nov 7 10:37:41 2012

Host Information

IP:	192.168.112.8
MAC Address:	00:23:7d:dc:89:7a
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	57	62

192.168.112.9

Scan Information

Start time:	Wed Nov 7 03:26:45 2012
End time:	Wed Nov 7 03:36:59 2012

Host Information

IP:	192.168.112.9
MAC Address:	00:1e:0b:d5:61:28
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	5	0	65	72

192.168.112.13

Scan Information

Start time:	Wed Nov 7 10:57:59 2012
End time:	Wed Nov 7 11:07:35 2012

Host Information

IP:	192.168.112.13
MAC Address:	00:1c:25:28:15:18
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

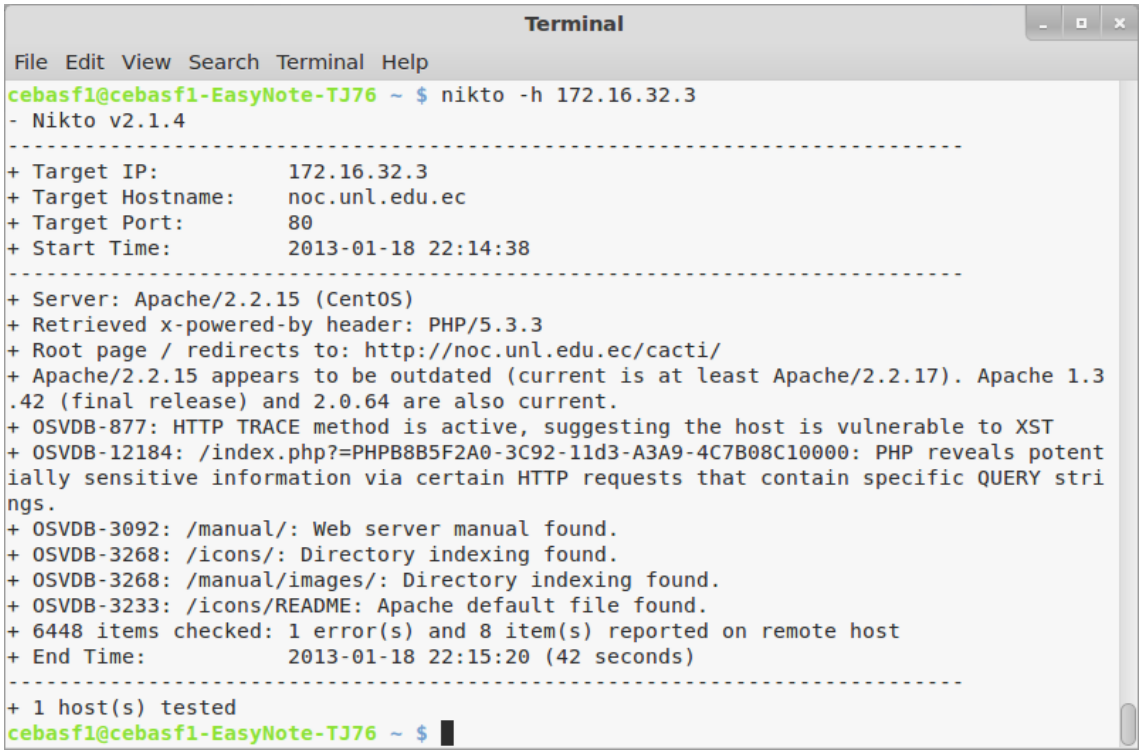
Results Summary

Critical	High	Medium	Low	Info	Total
1	0	2	0	30	33

NIKTO

```
Terminal
File  Edit  View  Search  Terminal  Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.1
- Nikto v2.1.4
---------------------------------------------------------------------------
+ No web server found on firewall.unl.edu.ec:80
---------------------------------------------------------------------------
+ 0 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $
```

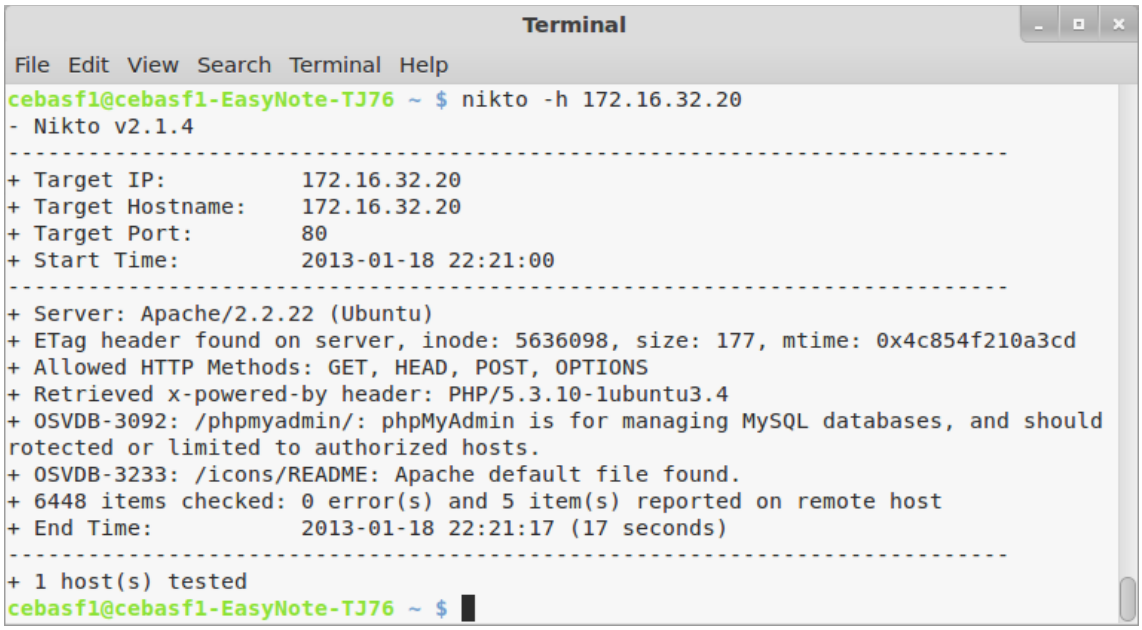
```
Terminal
File  Edit  View  Search  Terminal  Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.2
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          172.16.32.2
+ Target Hostname:    dnsdhcp.unl.edu.ec
+ Target Port:        80
+ Start Time:         2013-01-18 21:43:38
---------------------------------------------------------------------------
+ Server: Apache/2.2.20 (Ubuntu)
+ ETag header found on server, inode: 6040786, size: 177, mtime: 0x4ce910fcb1959
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out approp
riate line in httpd.conf or restrict access to allowed hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2013-01-18 21:44:15 (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $
```


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.3
- Nikto v2.1.4

+ Target IP: 172.16.32.3
+ Target Hostname: noc.unl.edu.ec
+ Target Port: 80
+ Start Time: 2013-01-18 22:14:38

+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.3.3
+ Root page / redirects to: http://noc.unl.edu.ec/cacti/
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3
.42 (final release) and 2.0.64 are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potent
ially sensitive information via certain HTTP requests that contain specific QUERY stri
ngs.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 8 item(s) reported on remote host
+ End Time: 2013-01-18 22:15:20 (42 seconds)

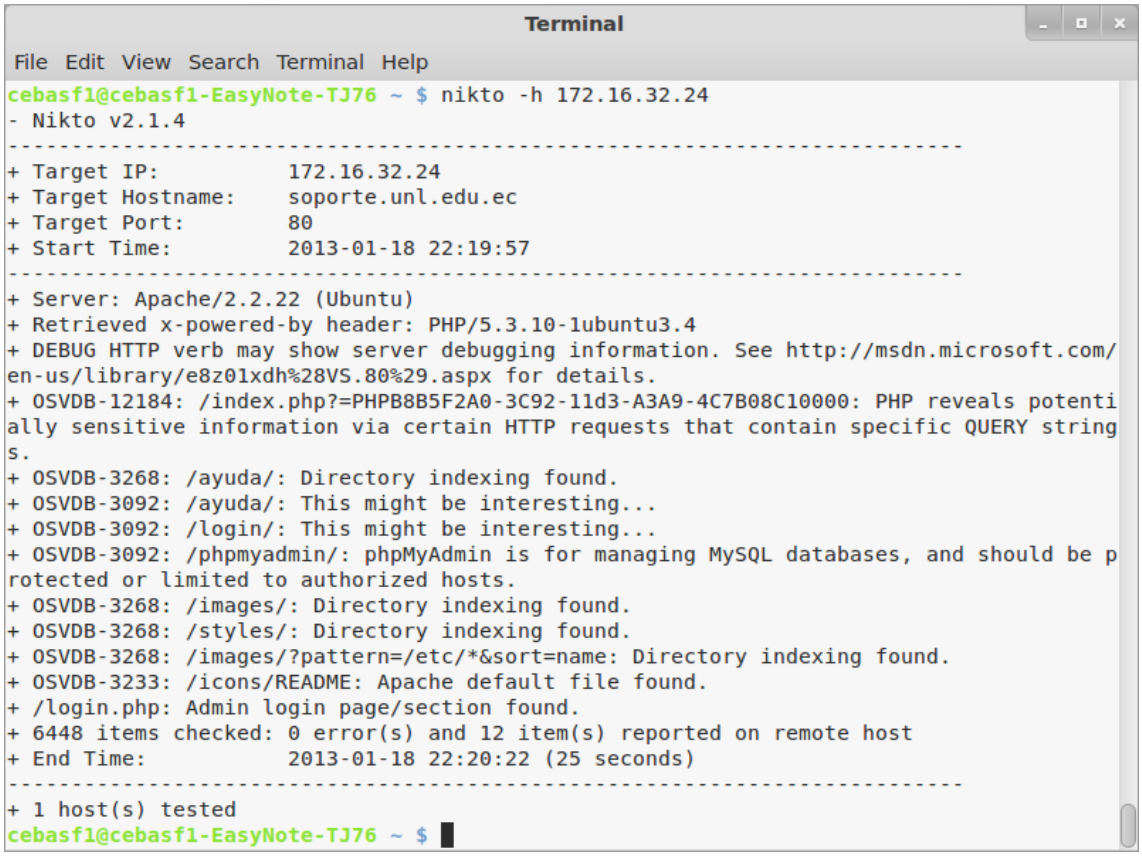
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.20
- Nikto v2.1.4

+ Target IP: 172.16.32.20
+ Target Hostname: 172.16.32.20
+ Target Port: 80
+ Start Time: 2013-01-18 22:21:00

+ Server: Apache/2.2.22 (Ubuntu)
+ ETag header found on server, inode: 5636098, size: 177, mtime: 0x4c854f210a3cd
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.4
+ OSVDB-3092: /phpmyadmin/: phpMyAdmin is for managing MySQL databases, and should
rotected or limited to authorized hosts.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2013-01-18 22:21:17 (17 seconds)

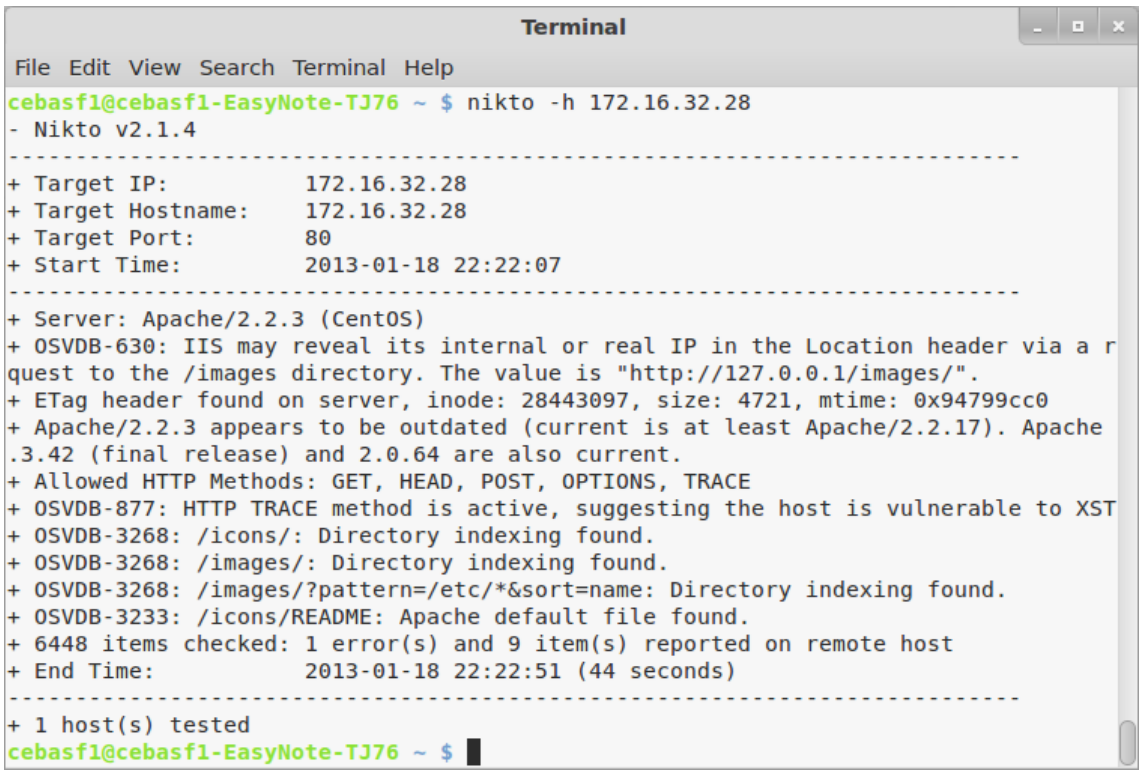
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.24
- Nikto v2.1.4

+ Target IP: 172.16.32.24
+ Target Hostname: soporte.unl.edu.ec
+ Target Port: 80
+ Start Time: 2013-01-18 22:19:57

+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.4
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /ayuda/: Directory indexing found.
+ OSVDB-3092: /ayuda/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /styles/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6448 items checked: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2013-01-18 22:20:22 (25 seconds)

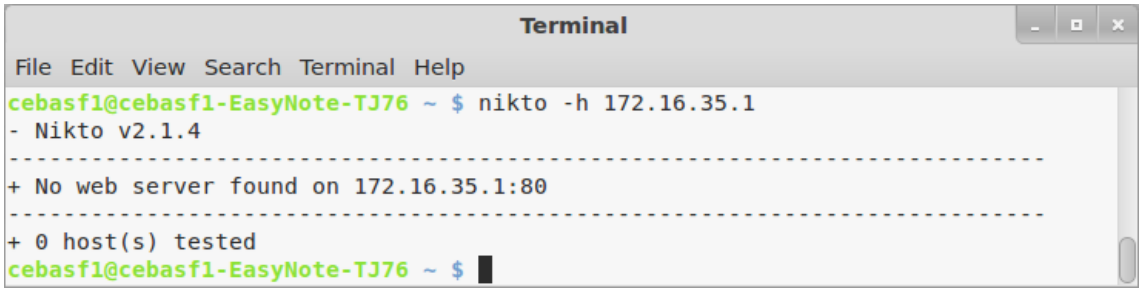
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.32.28
- Nikto v2.1.4

+ Target IP: 172.16.32.28
+ Target Hostname: 172.16.32.28
+ Target Port: 80
+ Start Time: 2013-01-18 22:22:07

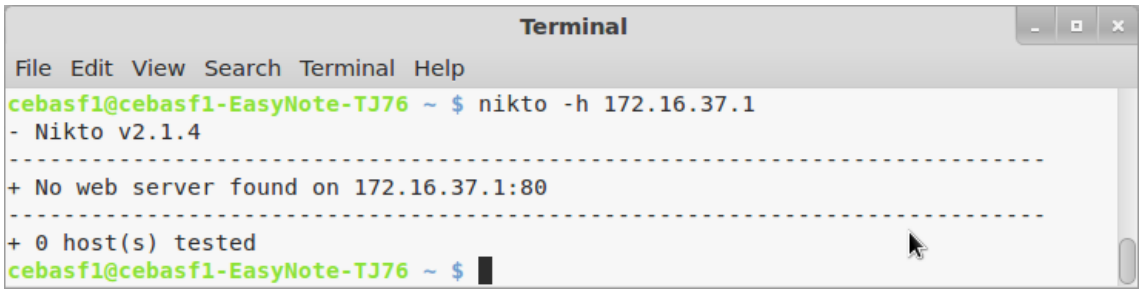
+ Server: Apache/2.2.3 (CentOS)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://127.0.0.1/images/".
+ ETag header found on server, inode: 28443097, size: 4721, mtime: 0x94799cc0
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.17). Apache.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 9 item(s) reported on remote host
+ End Time: 2013-01-18 22:22:51 (44 seconds)

+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.35.1
- Nikto v2.1.4

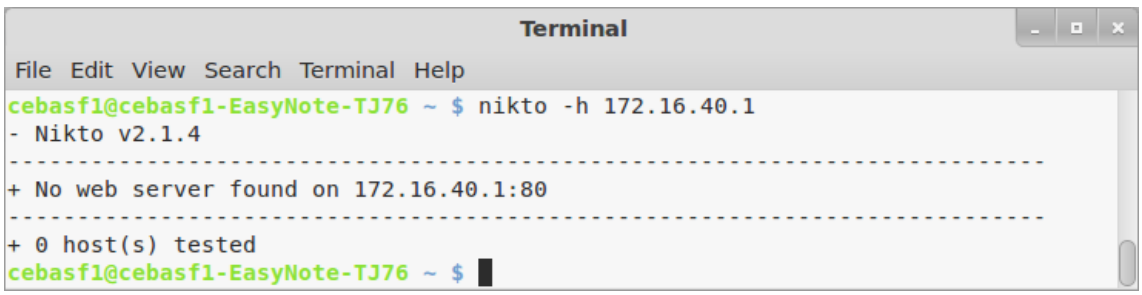
+ No web server found on 172.16.35.1:80

+ 0 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.37.1
- Nikto v2.1.4

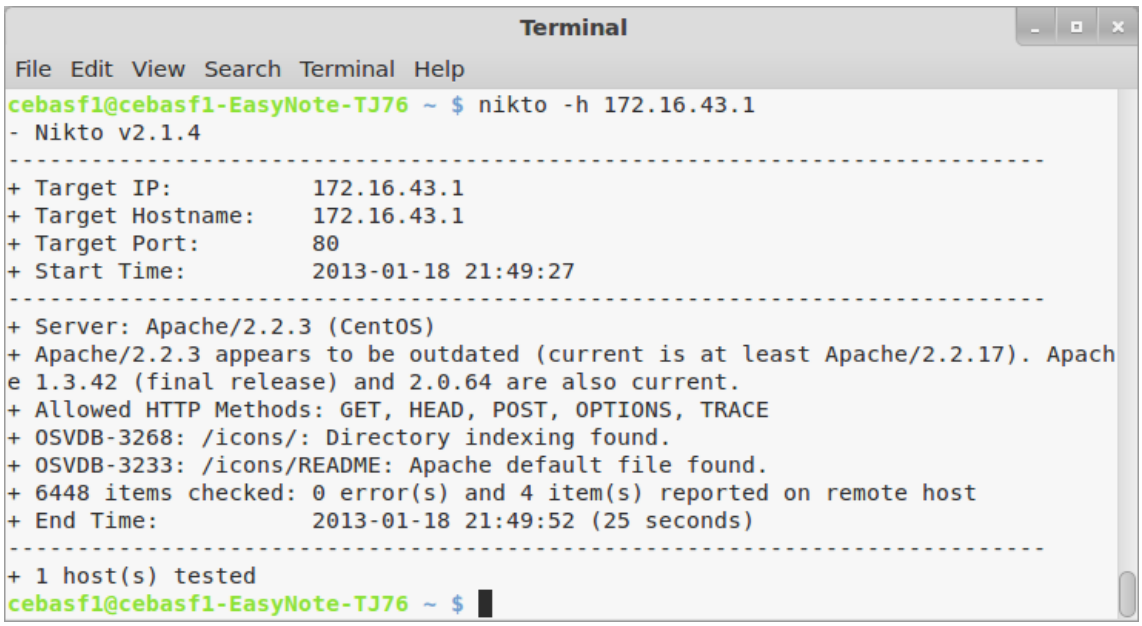
+ No web server found on 172.16.37.1:80

+ 0 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.40.1
- Nikto v2.1.4

+ No web server found on 172.16.40.1:80

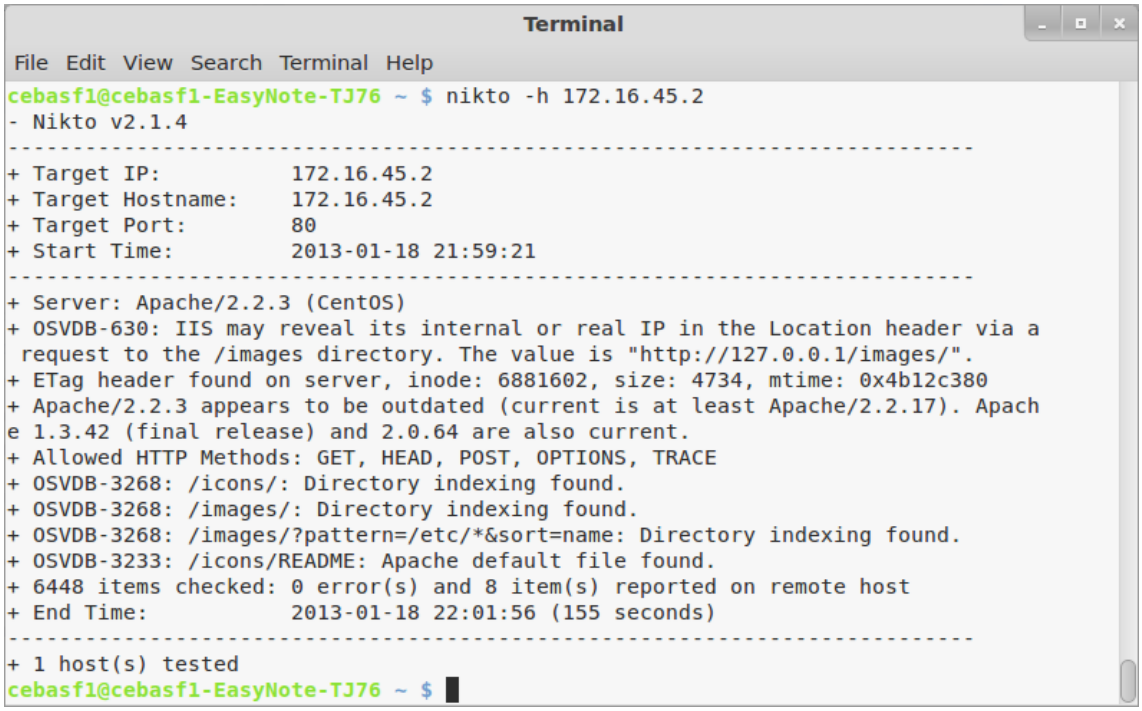
+ 0 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.43.1
- Nikto v2.1.4

+ Target IP: 172.16.43.1
+ Target Hostname: 172.16.43.1
+ Target Port: 80
+ Start Time: 2013-01-18 21:49:27

+ Server: Apache/2.2.3 (CentOS)
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.17). Apach
e 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2013-01-18 21:49:52 (25 seconds)

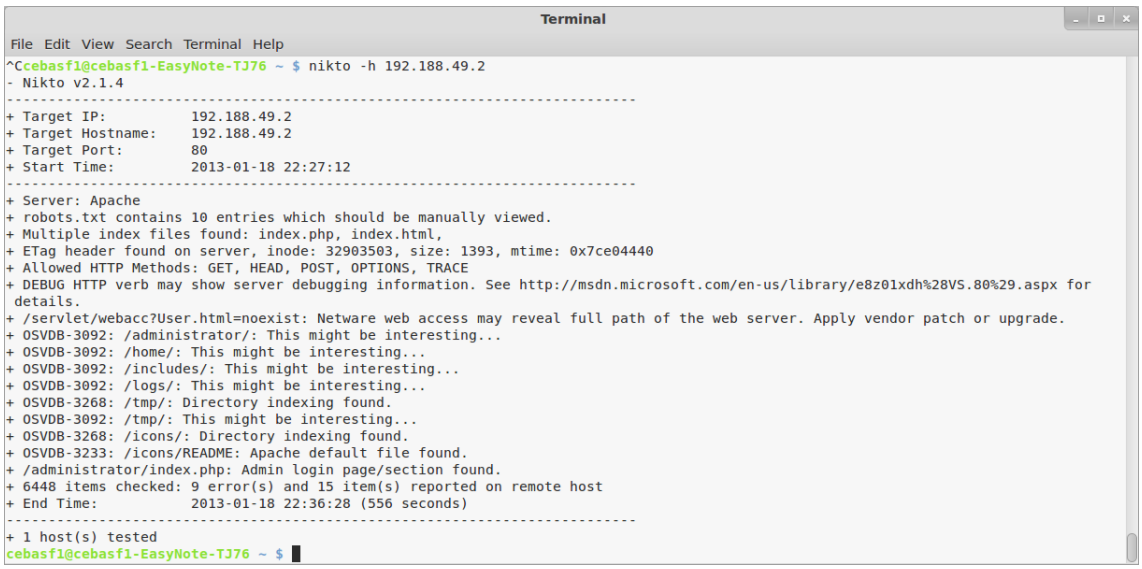
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 172.16.45.2
- Nikto v2.1.4

+ Target IP: 172.16.45.2
+ Target Hostname: 172.16.45.2
+ Target Port: 80
+ Start Time: 2013-01-18 21:59:21

+ Server: Apache/2.2.3 (CentOS)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://127.0.0.1/images/".
+ ETag header found on server, inode: 6881602, size: 4734, mtime: 0x4b12c380
+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2013-01-18 22:01:56 (155 seconds)

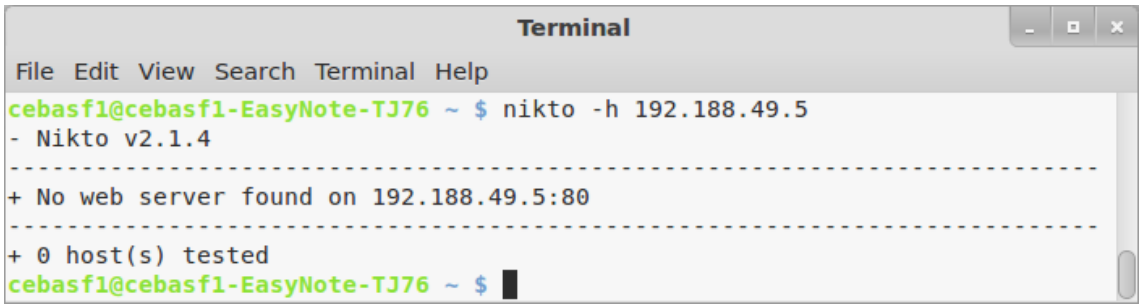
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
^Ccebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.2
- Nikto v2.1.4

+ Target IP: 192.188.49.2
+ Target Hostname: 192.188.49.2
+ Target Port: 80
+ Start Time: 2013-01-18 22:27:12

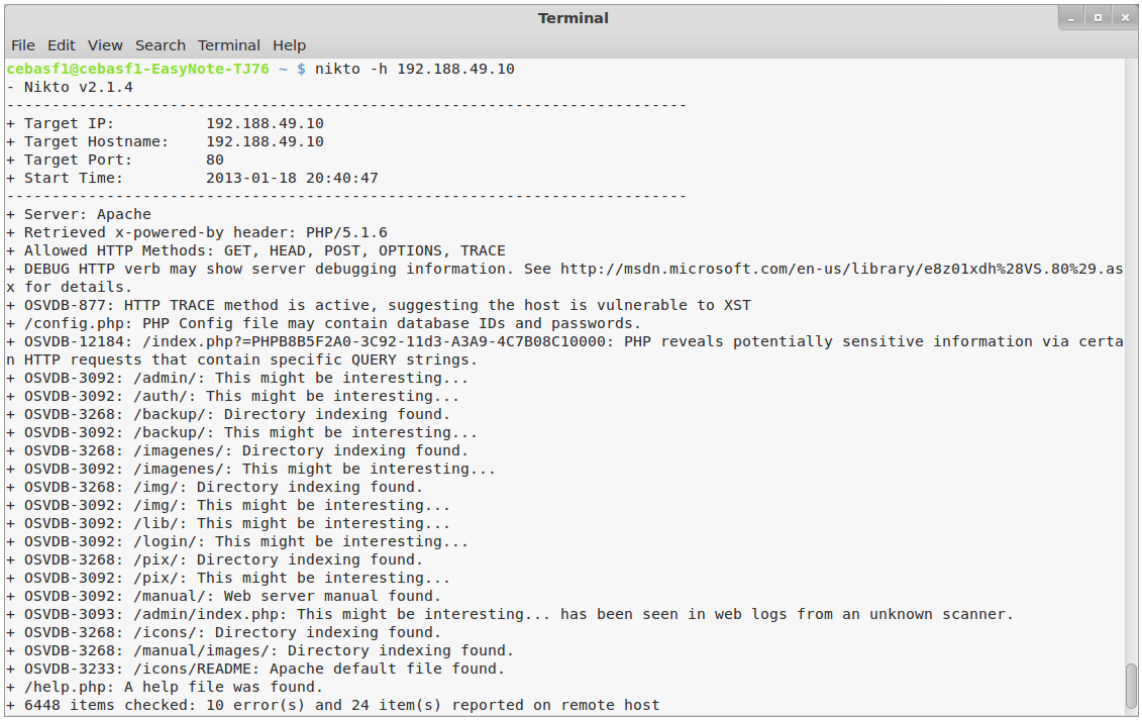
+ Server: Apache
+ robots.txt contains 10 entries which should be manually viewed.
+ Multiple index files found: index.php, index.html,
+ ETag header found on server, inode: 32903503, size: 1393, mtime: 0x7ce04440
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /servlet/webacc?User.html=noexist: Netware web access may reveal full path of the web server. Apply vendor patch or upgrade.
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /home/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /logs/: This might be interesting...
+ OSVDB-3268: /tmp/: Directory indexing found.
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /administrator/index.php: Admin login page/section found.
+ 6448 items checked: 9 error(s) and 15 item(s) reported on remote host
+ End Time: 2013-01-18 22:36:28 (556 seconds)

+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.5
- Nikto v2.1.4

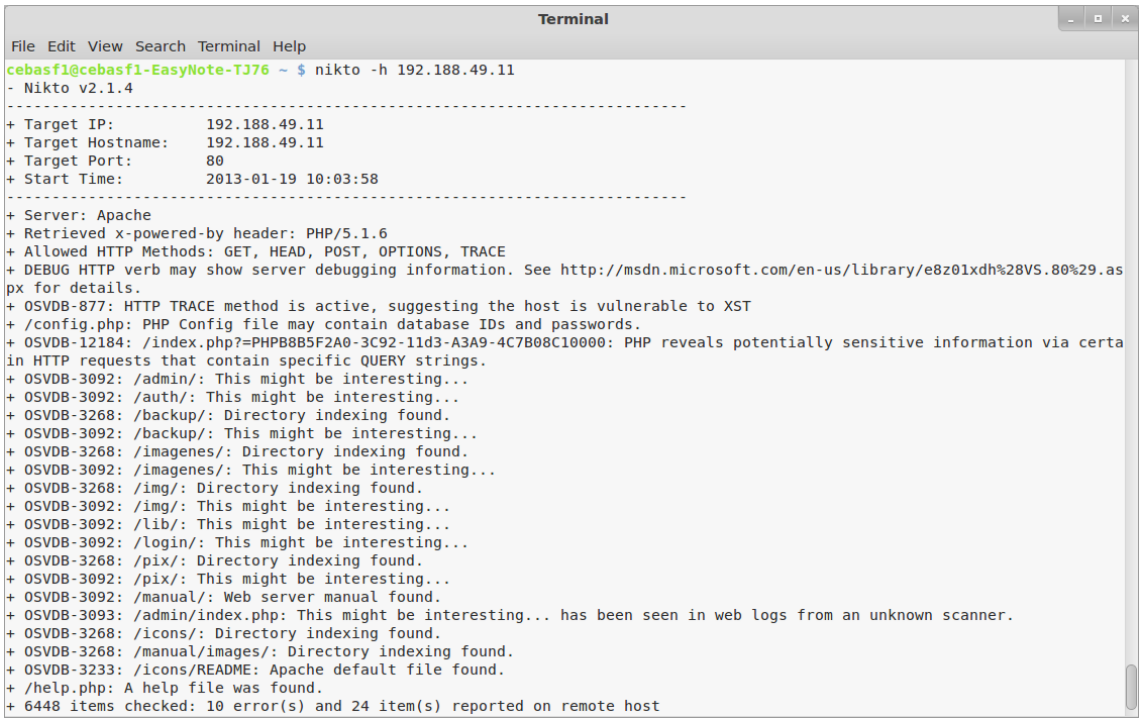
+ No web server found on 192.188.49.5:80

+ 0 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.10
- Nikto v2.1.4

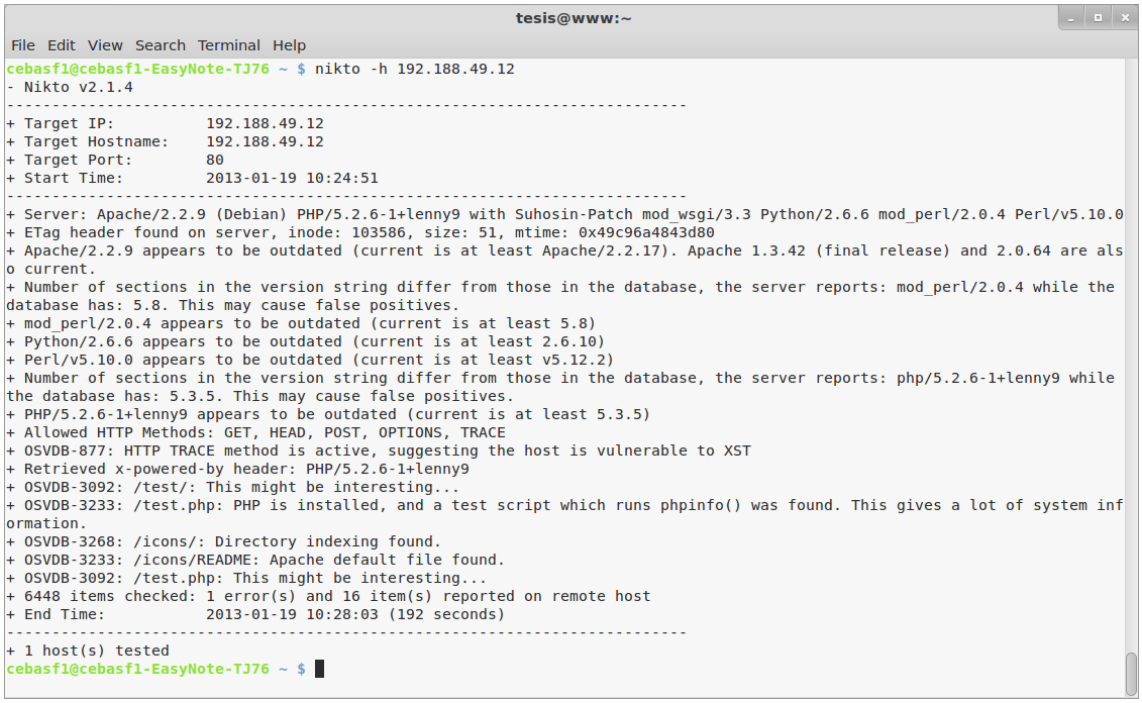
+ Target IP: 192.188.49.10
+ Target Hostname: 192.188.49.10
+ Target Port: 80
+ Start Time: 2013-01-18 20:40:47

+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.1.6
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.as
x for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certa
n HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /auth/: This might be interesting...
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3268: /imagenes/: Directory indexing found.
+ OSVDB-3092: /imagenes/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3268: /pix/: Directory indexing found.
+ OSVDB-3092: /pix/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /help.php: A help file was found.
+ 6448 items checked: 10 error(s) and 24 item(s) reported on remote host


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.11
- Nikto v2.1.4

+ Target IP: 192.188.49.11
+ Target Hostname: 192.188.49.11
+ Target Port: 80
+ Start Time: 2013-01-19 10:03:58

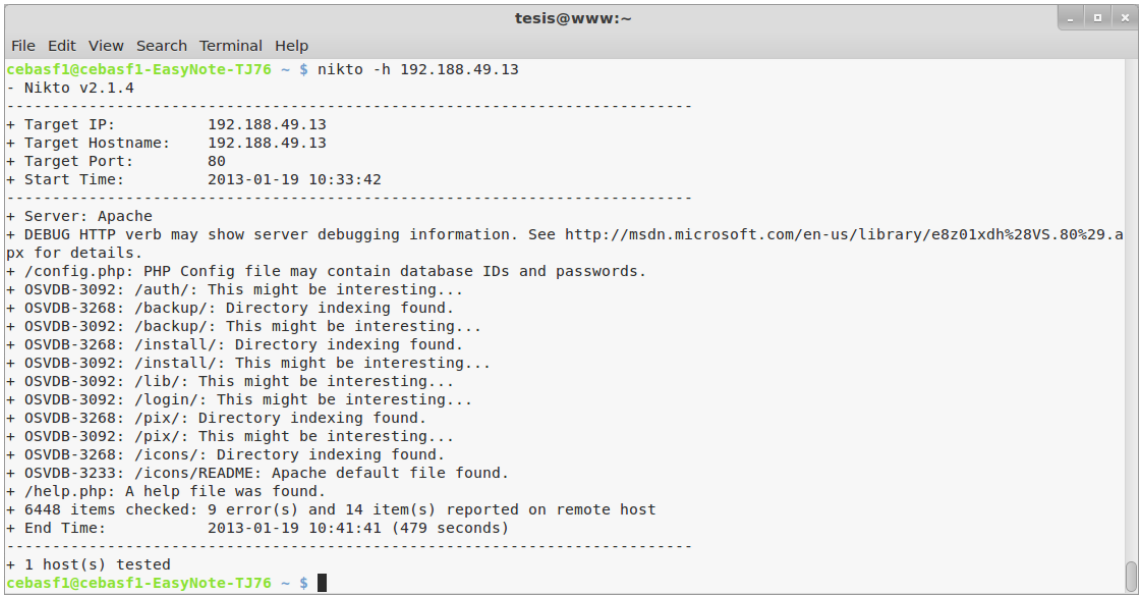
+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.1.6
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.as
px for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certa
in HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /auth/: This might be interesting...
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3268: /imagenes/: Directory indexing found.
+ OSVDB-3092: /imagenes/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3268: /pix/: Directory indexing found.
+ OSVDB-3092: /pix/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /help.php: A help file was found.
+ 6448 items checked: 10 error(s) and 24 item(s) reported on remote host


tesis@www:~
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.12
- Nikto v2.1.4

+ Target IP: 192.188.49.12
+ Target Hostname: 192.188.49.12
+ Target Port: 80
+ Start Time: 2013-01-19 10:24:51

+ Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch mod_wsgi/3.3 Python/2.6.6 mod_perl/2.0.4 Perl/v5.10.0
+ ETag header found on server, inode: 103586, size: 51, mtime: 0x49c96a4843d80
+ Apache/2.2.9 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are als
o current.
+ Number of sections in the version string differ from those in the database, the server reports: mod_perl/2.0.4 while the
database has: 5.8. This may cause false positives.
+ mod_perl/2.0.4 appears to be outdated (current is at least 5.8)
+ Python/2.6.6 appears to be outdated (current is at least 2.6.10)
+ Perl/v5.10.0 appears to be outdated (current is at least v5.12.2)
+ Number of sections in the version string differ from those in the database, the server reports: php/5.2.6-1+lenny9 while
the database has: 5.3.5. This may cause false positives.
+ PHP/5.2.6-1+lenny9 appears to be outdated (current is at least 5.3.5)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.2.6-1+lenny9
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /test.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system inf
ormation.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6448 items checked: 1 error(s) and 16 item(s) reported on remote host
+ End Time: 2013-01-19 10:28:03 (192 seconds)

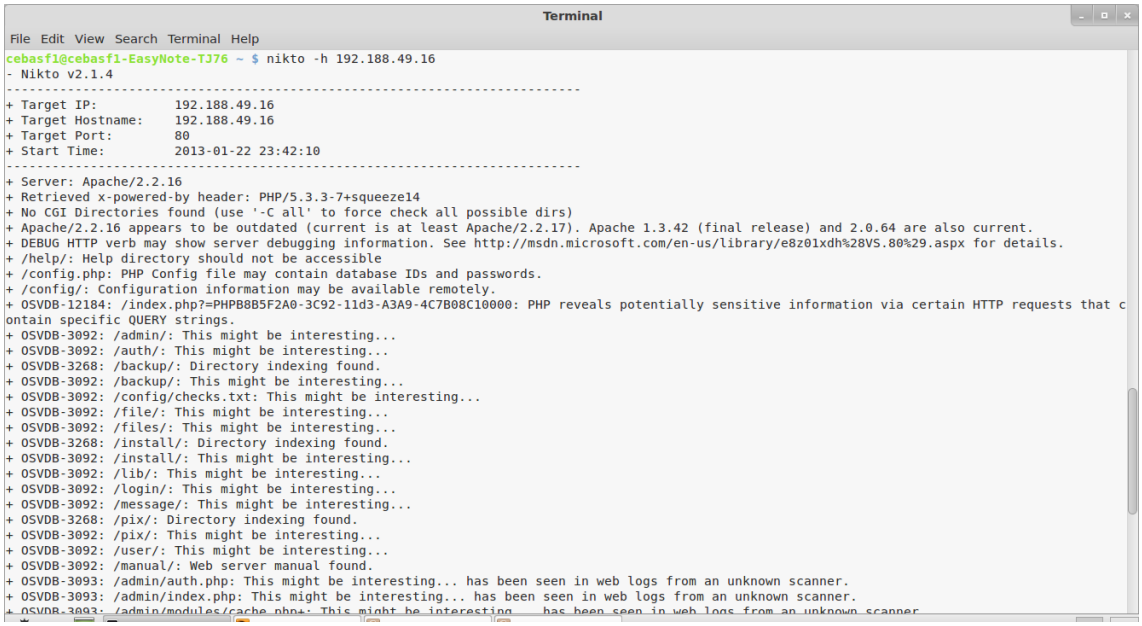
+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


tesis@www:~
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.13
- Nikto v2.1.4

+ Target IP: 192.188.49.13
+ Target Hostname: 192.188.49.13
+ Target Port: 80
+ Start Time: 2013-01-19 10:33:42

+ Server: Apache
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.a
px for details.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3092: /auth/: This might be interesting...
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3268: /install/: Directory indexing found.
+ OSVDB-3092: /install/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3268: /pix/: Directory indexing found.
+ OSVDB-3092: /pix/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /help.php: A help file was found.
+ 6448 items checked: 9 error(s) and 14 item(s) reported on remote host
+ End Time: 2013-01-19 10:41:41 (479 seconds)

+ 1 host(s) tested
cebasf1@cebasf1-EasyNote-TJ76 ~ $


Terminal
File Edit View Search Terminal Help
cebasf1@cebasf1-EasyNote-TJ76 ~ $ nikto -h 192.188.49.16
- Nikto v2.1.4

+ Target IP: 192.188.49.16
+ Target Hostname: 192.188.49.16
+ Target Port: 80
+ Start Time: 2013-01-22 23:42:10

+ Server: Apache/2.2.16
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeeze14
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /help/: Help directory should not be accessible
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that c
ontain specific QUERY strings.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3092: /auth/: This might be interesting...
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3092: /config/checks.txt: This might be interesting...
+ OSVDB-3092: /file/: This might be interesting...
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3268: /install/: Directory indexing found.
+ OSVDB-3092: /install/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /message/: This might be interesting...
+ OSVDB-3268: /pix/: Directory indexing found.
+ OSVDB-3092: /pix/: This might be interesting...
+ OSVDB-3092: /user/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3093: /admin/auth.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.

ANEXO VII: Iptables de los servidores

Servidores Proxy

```
#! /bin/bash

echo "Iniciando Script | Aplicando reglas del Proxy
Administracion Central Universidad Nacional de Loja"

#       iptables:               Creador Script | Proxy
Administracion Central | Universidad Nacional de Loja
#       autor:                  SecciÃ³n Redes y Equipos
InformÃ¡ticos
#       fecha:                  20 / 04 / 2011
#       instituciÃ³n:            Universidad Nacional de Loja |
Ecuador

# Interfaces eth0 "172.16.x.x"

IPPROXY=172.16.x.x
INTRANET=172.16.32.0/19
DNSINTRANET=172.16.x.x
IPNOC=172.16.x.x
CERO=0.0.0.0/0

# Limpiando todo "filter" - "nat"
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

# Estableciendo polÃtica por default "DROP"
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

### Estableciendo reglas en las cadenas "INPUT" y "OUTPUT" ###

# Aceptar todas las acciones en localhost "127.0.0.1"
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Acciones sobre ICMP todos "type" 0 - 8
iptables -A INPUT -i eth0 -p icmp -s $INTRANET -d $IPPROXY -j
ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p icmp -s $IPPROXY -d $INTRANET -j
ACCEPT
iptables -A INPUT -i eth0 -p icmp --icmp-type 0 -s $CERO -d
$IPPROXY -j ACCEPT
iptables -A OUTPUT -o eth0 -p icmp --icmp-type 8 -s $IPPROXY -d
$CERO -j ACCEPT

### Acceso "ssh" port "4466" Proxy Educativa ###
#Daniel Reyes
iptables -A INPUT -i eth0 -p tcp -m iprange --src-range
172.16.x.x-172.16.x.x -d $IPPROXY --sport 1024: --dport 4466 -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -m iprange --dst-
range 172.16.x.x-172.16.x.x --sport 4466 --dport 1024: -j ACCEPT
# Cecilia ZuÃ±iga "cexy" - SHH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT

# Tatiana Maldonado "tatius" - SSH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT
iptables -A INPUT -i eth0 -p tcp -s 172.16.63.21 -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT

# Hernan Torres "hernan" - SSH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT

# Abrir 4466 para permitir scp des proxy al server de respaldos
iptables -A INPUT -s 172.16.x.x -d $IPPROXY -i eth0 -p tcp -m
tcp --sport 4466 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d 172.16.x.x -o eth0 -p tcp -m
tcp --sport 1024: --dport 4466 -j ACCEPT

# Jhon Alexander CalderÃ³n SanmartÃn "dxlnx" - SSH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPPROXY --
sport 1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT
## Acceso "http-proxy" port "8080"
```

```
iptables -A INPUT -s $INTRANET -d $IPPROXY -i eth0 -p tcp --
sport 1024: --dport 8080 -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d $INTRANET -o eth0 -p tcp --
sport 8080 --dport 1024: -j ACCEPT

# Acceso SNMP Server NOC
iptables -A INPUT -s $IPNOC -d $IPPROXY -i eth0 -p udp -m udp --
sport 1024: --dport 161 -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d $IPNOC -o eth0 -p udp -m udp -
-sport 161 --dport 1024: -j ACCEPT
iptables -A INPUT -s $IPNOC -d $IPPROXY -i eth0 -p udp -m udp --
sport 1024: --dport 23 -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d $IPNOC -o eth0 -p udp -m udp -
-sport 23 --dport 1024: -j ACCEPT

## Acceso port 80 para logs de navegacion"
iptables -A INPUT -s $INTRANET -d $IPPROXY -i eth0 -p tcp --
sport 1024: --dport 80 -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d $INTRANET -o eth0 -p tcp --
sport 80 --dport 1024: -j ACCEPT

## ResoluciÃ³n "DNS"
iptables -A INPUT -s $DNSINTRANET -d $IPPROXY -i eth0 -p udp --
sport 53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -d $DNSINTRANET -o eth0 -p udp --
sport 1024: --dport 53 -j ACCEPT

## Abrir http para permitir navegacion del proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport 80
--dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 80 -j ACCEPT

## Abrir https para permitir navegacion del proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
443 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 443 -j ACCEPT
iptables -A INPUT -d $IPPROXY -i eth0 -p tcp -m tcp --sport 563
--dport 1024:65535 -j ACCEPT
iptables -A OUTPUT -s $IPPROXY -o eth0 -p tcp -m tcp --sport
1024:65535 --dport 563 -j ACCEPT

## Abrir ftp port 20 y 21 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
20:21 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 20:21 -j ACCEPT

# Abrir ftp port 23 para proxy Descargas
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
23: --dport 1024: -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 23: -j ACCEPT

## Abrir 8080 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
8080 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 8080 -j ACCEPT

## Abrir 8001 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
8001 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 8001 -j ACCEPT

## Abrir 8081 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
8081 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 8081 -j ACCEPT

## Abrir 8082 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
8082 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 8082 -j ACCEPT

## Abrir 8900 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
8900 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 8900 -j ACCEPT

## Abrir 9009 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
9009 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 9009 -j ACCEPT

## Abrir 7777 para proxy
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPPROXY --sport
7777 --dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPPROXY -d $CERO --sport
1024: --dport 7777 -j ACCEPT
```

```
#! /bin/bash

echo "Iniciando Script | Aplicando reglas del Dns-Dhcp de la
Universidad Nacional de Loja"

#       iptables:               Creador Script | Dns-Dhcp |
Universidad Nacional de Loja
#       autor:                  SecciÃ³n Redes y Equipos
InformÃ¡ticos
#       fecha:                  04 / 06 / 2012
#       instituciÃ³n:            Universidad Nacional de Loja |
Ecuador

# Interfaces eth0 "172.16.x.x"

IPDNS=172.16.x.x
IPDHCP=172.16.x.x
INTRANET=172.16.32.0/19
DNSEXTERNO=200.93.x.x
DNSGOOGLE=8.8.8.8
IPNOC=172.16.x.x
CERO=0.0.0.0/0

# Limpiando todo "filter" - "nat"
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

# Estableciendo polÃtica por default "DROP"
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

### Estableciendo reglas en las cadenas "INPUT" y "OUTPUT" ###

# Aceptar todas las acciones en localhost "127.0.0.1"
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Acciones sobre ICMP todos "type" 0 - 8
iptables -A INPUT -i eth0 -p icmp -s $INTRANET -d $IPDNS -j
ACCEPT
iptables -A OUTPUT -o eth0 -p icmp -s $IPDNS -d $INTRANET -j
ACCEPT
```

```
iptables -A INPUT -i eth0 -p icmp --icmp-type 0 -s $CERO -d
$IPDNS -j ACCEPT
iptables -A OUTPUT -o eth0 -p icmp --icmp-type 8 -s $IPDNS -d
$CERO -j ACCEPT

### Acceso "ssh" port "4466" DNS-DHCP ###
#Daniel Reyes
iptables -A INPUT -i eth0 -p tcp -m iprange --src-range
172.16.x.x-172.16.x.x -d $IPDNS --sport 1024: --dport 4466 -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPDNS -m iprange --dst-
range 172.16.x.x-172.16.x.x --sport 4466 --dport 1024: -j ACCEPT
# Tesistas "tesis" - SSH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPDNS --sport
1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPDNS -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT
# Jhon Alexander CalderÃ³n SanmartÃn "dxlnx" - SSH
iptables -A INPUT -i eth0 -p tcp -s 172.16.x.x -d $IPDNS --sport
1024: --dport 4466 -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPDNS -d 172.16.x.x --
sport 4466 --dport 1024: -j ACCEPT

# Abrir 4466 para permitir scp des proxy al server de respaldos
iptables -A INPUT -s 172.16.x.x -d $IPDNS -i eth0 -p tcp -m tcp
--sport 4466 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d 172.16.x.x -o eth0 -p tcp -m tcp
--sport 1024: --dport 4466 -j ACCEPT

# Acceso SNMP Server noc.unl.edu.ec
iptables -A INPUT -s $IPNOC -d $IPDNS -i eth0 -p udp -m udp --
sport 1024: --dport 161 -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $IPNOC -o eth0 -p udp -m udp --
sport 161 --dport 1024: -j ACCEPT

# Acceso de usuarios Dns interno UDP
iptables -A INPUT -s $INTRANET -d $IPDNS -i eth0 -p udp --sport
1024: --dport 53 -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $INTRANET -o eth0 -p udp --sport
53 --dport 1024: -j ACCEPT

# Acceso de usuarios Dns interno TCP
iptables -A INPUT -s $INTRANET -d $IPDNS -i eth0 -p tcp --sport
1024: --dport 53 -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $INTRANET -o eth0 -p tcp --sport
53 --dport 1024: -j ACCEPT

# Acceso de usuarios Dns externo UDP
iptables -A INPUT -s $DNSEXTERNO -d $IPDNS -i eth0 -p udp --
sport 53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $DNSEXTERNO -o eth0 -p udp --
sport 1024: --dport 53 -j ACCEPT
```

```
iptables -A INPUT -s $DNSGOOGLE -d $IPDNS -i eth0 -p udp --sport
53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $DNSGOOGLE -o eth0 -p udp --
sport 1024: --dport 53 -j ACCEPT

# Acceso de usuarios Dns externo TCP
iptables -A INPUT -s $DNSEXTERNO -d $IPDNS -i eth0 -p tcp --
sport 53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $DNSEXTERNO -o eth0 -p tcp --
sport 1024: --dport 53 -j ACCEPT
iptables -A INPUT -s $DNSGOOGLE -d $IPDNS -i eth0 -p tcp --sport
53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPDNS -d $DNSGOOGLE -o eth0 -p tcp --
sport 1024: --dport 53 -j ACCEPT

# Acceso de usuarios Dhcp
iptables -A INPUT -s $INTRANET -d $IPDHCP -i eth0 -p udp --sport
67:68 --dport 67:68 -j ACCEPT
iptables -A OUTPUT -s $IPDHCP -d $INTRANET -o eth0 -p udp --
sport 67:68 --dport 67:68 -j ACCEPT

iptables -A INPUT -s $INTRANET -d $IPDHCP -i eth0 -p tcp --sport
67:68 --dport 67:68 -j ACCEPT
iptables -A OUTPUT -s $IPDHCP -d $INTRANET -o eth0 -p tcp --
sport 67:68 --dport 67:68 -j ACCEPT

## Abrir http para permitir navegacion
iptables -A INPUT -i eth0 -p tcp -s $CERO -d $IPDNS --sport 80 -
-dport 1024: -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -s $IPDNS -d $CERO --sport
1024: --dport 80 -j ACCEPT


echo "Se aplicÃ³ iptables en servidor DNS-DHCP"
```

Servidores Públicos ipv4

```
#! /bin/bash

echo "Iniciando Script | Aplicando reglas del servidor WEB
Universidad Nacional de Loja"

#       Iptables:               Creador Script | WEB |
Universidad Nacional de Loja
#       Autor:                  SecciÃ³n Redes y Equipos
InformÃ¡ticos
#       Fecha:                  26 / 11 / 2010
#       InstituciÃ³n:            Universidad Nacional de Loja |
Ecuador

# Interface eth0 "192.188.x.x"

IPFIREWALL=192.188.x.x
IPWEB=192.188.x.x
IPVINCULACION=192.188.x.x
CERO=0.0.0.0/0
DNS1=200.93.x.x
DNS2=200.93.x.x

# Limpiando todo "filter" - "nat"
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z

# Estableciendo polÃtica por default "DROP"
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

### Estableciendo reglas en las cadenas "INPUT" y "OUTPUT" ###

# Aceptar todas las acciones en localhost "127.0.0.1"
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Acciones sobre ICMP todos
iptables -A INPUT -i eth0 -p icmp -s $CERO -d $IPWEB -j ACCEPT
iptables -A OUTPUT -o eth0 -p icmp -s $IPWEB -d $CERO -j ACCEPT

#Habilitar ssh
iptables -A INPUT -s $CERO -d $IPWEB -i eth0 -p tcp -m tcp --
sport 1024: --dport 6644 -j ACCEPT
```

```
iptables -A OUTPUT -s $IPWEB -d $CERO -o eth0 -p tcp -m tcp --
sport 6644 --dport 1024: -j ACCEPT

#ResoluciÃ³n DNS
iptables -A INPUT -s $DNS1 -d $IPWEB -i eth0 -p udp -m udp --
sport 53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPWEB -d $DNS1 -o eth0 -p udp -m udp --
sport 1024: --dport 53 -j ACCEPT
iptables -A INPUT -s $DNS2 -d $IPWEB -i eth0 -p udp -m udp --
sport 53 --dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPWEB -d $DNS2 -o eth0 -p udp -m udp --
sport 1024: --dport 53 -j ACCEPT

#NavegaciÃ³n http
iptables -A INPUT -d $IPWEB -i eth0 -p tcp -m tcp --sport 80 --
dport 1024: -j ACCEPT
iptables -A OUTPUT -s $IPWEB -o eth0 -p tcp -m tcp --sport 1024:
--dport 80 -j ACCEPT

#Recibir Peticiones http - Web
iptables -A INPUT -s $CERO -d $IPWEB -i eth0 -p tcp -m tcp --
sport 1024: --dport 80 -j ACCEPT
iptables -A OUTPUT -s $IPWEB -d $CERO -o eth0 -p tcp -m tcp --
sport 80 --dport 1024: -j ACCEPT

# Acceso SNMP Server NOC
iptables -A INPUT -s $IPFIREWALL -d $IPWEB -i eth0 -p udp -m udp
--sport 1024: --dport 161 -j ACCEPT
iptables -A OUTPUT -s $IPWEB -d $IPFIREWALL -o eth0 -p udp -m
udp --sport 161 --dport 1024: -j ACCEPT
iptables -A INPUT -s $IPFIREWALL -d $IPWEB -i eth0 -p udp -m udp
--sport 1024: --dport 23 -j ACCEPT
iptables -A OUTPUT -s $IPWEB -d $IPFIREWALL -o eth0 -p udp -m
udp --sport 23 --dport 1024: -j ACCEPT


#Recibir Peticiones http - Vinculacion
iptables -A INPUT -s $CERO -d $IPVINCULACION -i eth0 -p tcp -m
tcp --sport 1024: --dport 80 -j ACCEPT
iptables -A OUTPUT -s $IPVINCULACION -d $CERO -o eth0 -p tcp -m
tcp --sport 80 --dport 1024: -j ACCEPT

echo "Reglas WEB-SERVER | Universidad Nacional de Loja
aplicadas"
```

Servidores Públicos ipv6

```
#! /bin/bash

echo "Iniciando Script | Aplicando reglas del servidor WEB
Universidad Nacional de Loja | IPv6"

#       Iptables:               Creador Script | WEB |
Universidad Nacional de Loja
#       Autor:                  Jhon Alexander CalderÃ³n
SanmartÃn y Rubi Rafale Cabrera Erreyes
#       Fecha:                  13 / 06 / 2011
#       InstituciÃ³n:            Universidad Nacional de Loja |
Ecuador

# Interface eth0 "2800:68:7:49::2"
ALLIPv6=2000::/3
WEBIPv6=2800:68:7:49::2/64
FWIPv6=2800:68:7:49::5/64
DIPv6=2800:68:7:32:63::17
JIPv6=2800:68:7:32:63::7
TIPv6=2800:68:7:32:63::20
CIPv6=2800:68:7:32:63::30


# Limpiando todo tabla "filter"
ip6tables -t filter -F
ip6tables -t filter -Z
ip6tables -t filter -X

# Estableciendo polÃtica por default "DROP"
ip6tables -t filter -P INPUT DROP
ip6tables -t filter -P OUTPUT DROP
ip6tables -t filter -P FORWARD DROP

# Estableciendo polÃtica por default "DROP"
ip6tables -t filter -A INPUT -i lo -j ACCEPT
ip6tables -t filter -A OUTPUT -o lo -j ACCEPT

# Icmpv6 - todos los types
ip6tables -t filter -A INPUT -i eth0 -p ipv6-icmp -j ACCEPT
ip6tables -t filter -A OUTPUT -o eth0 -p ipv6-icmp -j ACCEPT

# Habilitar Acceso Remnoto
ip6tables -A INPUT -i eth0 -p tcp -s $DIPv6 -d $WEBIPv6 --sport
1024: --dport 6644 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s $WEBIPv6 -d $DIPv6 --sport
6644 --dport 1024: -j ACCEPT
ip6tables -A INPUT -i eth0 -p tcp -s $JIPv6 -d $WEBIPv6 --sport
1024: --dport 6644 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s $WEBIPv6 -d $JIPv6 --sport
6644 --dport 1024: -j ACCEPT
```

```
ip6tables -A INPUT -i eth0 -p tcp -s $TIPv6 -d $WEBIPv6 --sport
1024: --dport 6644 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s $WEBIPv6 -d $TIPv6 --sport
6644 --dport 1024: -j ACCEPT
ip6tables -A INPUT -i eth0 -p tcp -s $CIPv6 -d $WEBIPv6 --sport
1024: --dport 6644 -j ACCEPT
ip6tables -A OUTPUT -o eth0 -p tcp -s $WEBIPv6 -d $CIPv6 --sport
6644 --dport 1024: -j ACCEPT

# Escuchar puerto 80 todo Internet IPv6
ip6tables -t filter -A INPUT -i eth0 -p tcp -s $ALLIPv6 -d
$WEBIPv6 --sport 1024: --dport 80 -j ACCEPT
ip6tables -t filter -A OUTPUT -o eth0 -p tcp -s $WEBIPv6 -d
$ALLIPv6 --sport 80 --dport 1024: -j ACCEPT

echo "Reglas Aplicadas Exito Web-Server | Universidad Nacional
de Loja | IPv6"
```

ANEXO VIII: Informe de vulnerabilidades de los servidores de la MED

Loja, 2 de julio de 2012

Ing.

Milton Palacios M.

COORDINADOR TECNOLÓGICO DE LA MED

Ciudad.

De nuestra consideración:

MARIANA CARMEN GONZÁLEZ GONZÁLEZ Y CÉSAR AUGUSTO BASTIDAS MONCAYO, tesistas del Proyecto **"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS"**, en el desarrollo de nuestra investigación se ha detectado que los Servidores MED-VIRTUAL y MED-CURSOS poseen múltiples vulnerabilidades, además incluimos las sugerencias y soluciones, de acuerdo al informe que se adjunta.

Particular que comunicamos para los fines pertinentes.

Atentamente,

Mariana González G.

César Bastidas M.

INFORME DE VULNERABILIDADES SERVIDORES DE LA MED

SERVIDOR MED-CURSOS

Tabla de vulnerabilidades

Ip del servidor	192.188.49.11		
Vulnerabilidad	Alta	**Puerto**	80/tcp
Descripción.- Según la versión de PHP 5 instalada en el servidor, esta es inferior a la versión 5.2.1 Estas versiones pueden verse afectadas por varios asuntos, incluyendo desbordamientos de búfer, las vulnerabilidades de formato de cadena, la ejecución de código arbitrario.			
Solución.- Actualizar a la versión de PHP a su versión mas reciente			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	80/tcp, 443/tcp
Descripción.- El servidor web remoto es compatible TRACE and/or TRACK que son métodos HTTP que se utilizan para depurar las conexiones del servidor web.			
Solución.- Desactivar estos métodos.			

Ip del servidor	192.188.49.11		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.- El host remoto compatible con el uso de sistemas de cifrado SSL que ofrecen cifrado de tipo medio, que actualmente consideramos como aquellos con longitudes de clave de al menos 56 bits y bits de menos de 112. Nota: Esto es mucho más fácil de explotar, si el atacante está en la misma red física.			
Solución.- Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.			

Ip del servidor	192.188.49.11		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.-El CommonName (CN) del certificado SSL se presenta en este puerto es para una máquina diferente.			
Solución.- Compre o generar un certificado adecuado para este servicio.			

Ip del servidor	192.188.49.11		
Vulnerabilidad	Media	**Puerto**	80/tcp
Descripción.-La instalación de PHP en el servidor remoto se configura de una manera que permite la divulgación de información potencialmente sensible a un atacante a través de una URL especial.			
Solución.- En la configuración del archivo PHP, php.ini, establezca el valor de 'expose_php' a 'Off' para desactivar este comportamiento. Reinicie el demonio de servidor web para poner en vigor este cambio.			

Ip del servidor	192.188.49.11		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.-La cadena de certificados X.509 para este servicio no está firmado por una autoridad certificadora reconocida. Si el host remoto es un anfitrión del público en la producción, esto anula el uso de SSL como cualquiera podría establecer un medio del ataque contra el sistema remoto. Tenga en cuenta que este plugin no comprueba cadenas de certificados que terminan en un certificado que no es auto-firmado, pero está firmado por una autoridad de certificación reconocida.			
Solución.- Compre o generar un certificado adecuado para este servicio.			

Ip del servidor	192.188.49.11		
Vulnerabilidad	Baja	**Puerto**	80/tcp
Descripción.-El servidor web remoto contiene varios campos de formulario HTML que contiene una entrada de tipo 'password' que transmiten su información a un servidor web remoto en texto plano. Un atacante escucha el tráfico entre el navegador y el servidor puede obtener usuarios y contraseñas de los usuarios válidos.			
Solución.- Asegúrese de que todas las formas sensibles transmite el contenido a través de HTTPS.			

Servidor MED-VIRTUAL

Tabla de Vulnerabilidades

Ip del servidor	192.188.49.10		
Vulnerabilidad	Alta	**Puerto**	80/tcp
Descripción.- Según la versión de PHP 5 instalada en el servidor, esta es inferior a la versión 5.2.2. Estas versiones pueden verse afectadas por varios asuntos, incluyendo desbordamientos de búfer, la ejecución de código arbitrario, 'safe_mode' y 'open_basedir'.			
Solución.- Actualizar a la versión de PHP a su versión mas reciente			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	80/tcp, 443/tcp
Descripción.- El servidor web remoto es compatible TRACE and/or TRACK que son métodos HTTP que se utilizan para depurar las conexiones del servidor web.			
Solución.- Desactivar estos métodos.			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	80/tcp, 443/tcp
Descripción.- Al menos una aplicación web alojada en el servidor web remoto conoce la ruta de acceso física a sus directorios, cuando la solicitud se envía con formato incorrecto de la misma. Fugas en este tipo de información puede ayudar a un atacante afinar los ataques contra la aplicación y su back-end.			
Solución.- Filtrar los mensajes de error que contienen información de la ruta.			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.- Este script comprueba las fechas de caducidad de los certificados SSL asociados con los servicios habilitados en el objetivo y los informes si alguno ya ha caducado.			
Solución.- Generar un nuevo certificado SSL para remplazar el existente.			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	80/tcp
Descripción.- Dreamweaver de Adobe es conocida por producir archivos dwsync.xml. Estos contienen la información de sincronización, que puede incluir la lista de archivos y directorios sincronizados. Esto puede conducir a la divulgación de información.			
Solución.- Desactivar la opción 'mantener la sincronización de la información' de la categoría Datos remotos de la vista avanzada del cuadro de diálogo Definición del sitio. Además, eliminar los archivos involucrados, si ya creados por el sistema			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.-El CommonName (CN) del certificado SSL se presenta en este puerto es para una máquina diferente.			
Solución.- Compre o genere un certificado adecuado para este servicio.			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Media	**Puerto**	443/tcp
Descripción.- El host remoto es compatible con el uso de sistemas de cifrado SSL que ofrecen cifrado de tipo medio, que actualmente consideramos que aquellos con longitudes de clave de al menos 56 bits y 112 Nota: Esto es mucho más fácil de explotar, si el atacante está en la misma red física.			
Solución.- Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.			

Ip del servidor	192.188.49.10		
Vulnerabilidad	Baja	**Puerto**	80/tcp
Descripción.- El servidor web remoto contiene varios campos de formulario HTML que contiene una entrada de tipo 'password' que transmiten su información a un servidor web remoto en texto plano. Un atacante escucha el tráfico entre el navegador y el servidor puede obtener usuarios y contraseñas de los usuarios válidos.			
Solución.- Asegúrese de que todas las formas sensibles transmite el contenido a través de HTTPS			

ANEXO IX: Anteproyecto

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, DE LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS. "

Autores:

Cesar Bastidas Moncayo

Mariana González González

2012-2013

1. TEMA

“Análisis de vulnerabilidades físicas y lógicas de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, y construcción de un plan de mitigación de riesgos. “

2. PROBLEMÁTICA

2.1. Situación Problemática

La Universidad Nacional de Loja es una institución de educación superior pública que brinda formación académica y profesional de calidad, con sólidas bases científicas y técnicas, que con el paso del tiempo ha evolucionado tanto académica como tecnológicamente.

La información es la parte fundamental de toda empresa para tener un alto nivel de competitividad y posibilidades de desarrollo, por tal motivo la Universidad Nacional de Loja posee una gran cantidad de información almacenada en diferentes tipos de servidores tanto internos como externos, los mismos que son susceptibles a ataques malintencionados en la intranet como extranet.

La Unidad de Telecomunicaciones e Información tiene a su haber alrededor 22 servidores los mismos que están distribuidos de acuerdo al servicio que prestan como web, webmail, radio Universitaria, firewall, S.G.A, dns, dhcp, asterisk, M.E.D y proxys de las diferentes áreas.

Los servidores se encuentran en el Data Center ubicado en el cuarto piso del bloque dos de Administración Central, al cual tiene acceso solo personal autorizado por la Unidad de Telecomunicaciones e Información pero el sitio donde funciona no posee las seguridades físicas adecuadas, además no existe el espacio y la correcta distribución de los equipos que forman este centro de datos, los equipos están ubicados en escritorios que no brindan las características técnicas de funcionamiento. Los servidores cuentan con ups conectados en serie y carecen de un sistema de suministro eléctrico adecuado y de emergencia, además los equipos que manejan no poseen características de servidores ya que utilizan PCs de escritorio.

Internamente los servidores poseen configuraciones básicas de acuerdo al servicio que prestan, en servicios similares como proxy la configuración es la misma. La mayoría de los servidores de la Unidad de Telecomunicaciones e Información trabajan bajo la plataforma Centos.

Los servidores de esta unidad no han sido sometidos a un análisis de vulnerabilidades tanto físicas como lógicas que reflejen el grado de integridad, confidencialidad y autenticidad de la información.

Es por eso que el proyecto que se presenta pretende solucionar algunos de los problemas descritos.

2.2. Problema General de Investigación

Falta de seguridades físicas y lógicas de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, y falta de un plan de mitigación de riesgos.

2.3. Delimitación

2.3.1. Problemas específicos de investigación

Luego de conocer la situación problemática de los servidores de la Unidad de Telecomunicaciones e Información, hemos podido determinar los siguientes problemas:

1. Falta de un análisis de vulnerabilidades a los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
2. Carencia de un sistema de energía adecuado para los servidores de la unidad de telecomunicaciones e información de la Universidad Nacional de Loja.
3. Necesidad de una adecuada distribución de espacios de los servidores de la unidad de telecomunicaciones e información de la Universidad Nacional de Loja
4. Falta de un plan de mitigación de riesgos.

2.3.2. Espacio

El presente proyecto de investigación tiene como escenario la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

2.3.3. Tiempo

El presente proyecto de investigación, tiene una planificación de acuerdo a los parámetros a realizarse que se encuentran detallados en el cronograma de actividades con duración de 12 meses a partir de la fecha de aprobación del presente proyecto.

2.3.4. Unidades de Observación

La unidad de observación para la realización de este proyecto serán los servidores de la Universidad Nacional de Loja, administrados por la Unidad de Telecomunicaciones e Información.

3. JUSTIFICACION

3.1. Justificación

La Universidad Nacional de Loja como centro de educación superior, con una notable importancia en la Región Sur del País, brinda a sus egresados y profesionales la oportunidad de aportar, los conocimientos adquiridos durante el transcurso de la carrera, involucrando consigo a la sociedad.

Justificación Académica

Este proyecto se justifica académicamente en la necesidad que tenemos, como egresados de la carrera de Ingeniería en Sistemas, de poner en práctica todos los conocimientos adquiridos durante nuestra formación profesional, además el proyecto se enmarca dentro de las líneas de investigación de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja.

Justificación Económica

Económicamente de justifica este proyecto porque contamos con los medios económicos necesarios que nos permitirán solventar los gastos que requieran el desarrollo del mismo.

Justificación Técnica

Para la realización del presente proyecto contamos con todos los medios técnicos (computadoras, impresora, etc.) y herramientas (software libre, etc.) necesarias, que usaremos a lo largo de su desarrollo. Además es factible de realizar porque podemos acceder a diversos medios de consultas bibliográficas como libros, recursos de internet, etc. con la finalidad de obtener la información necesaria que me permita sustentar este proyecto. Además del apoyo y capacitación que nos pueden brindar el personal de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

3.2. Viabilidad

Este proyecto de investigación es viable, debido a que contamos con los medios técnicos, tecnológicos y económicos, que se requieren para su realización; además de contar con la asesoría de los docentes de la Carrera de Ingeniería en Sistemas y del personal de la Unidad de Telecomunicaciones e Información, la misma que nos servirá para poner en marcha este proyecto que contribuirá en el mejoramiento de la seguridad de la información de los servidores de la Universidad Nacional de Loja.

4. OBJETIVOS

4.1. General

1. Realizar el análisis de las vulnerabilidades tanto físicas como lógicas de los servidores de la unidad de telecomunicaciones e información de la Universidad Nacional de Loja.

4.2. Específicos

- Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

- Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

- Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores.

- Realizar pruebas a los servidores para determinar las vulnerabilidades en los diferentes servicios que brindan

- Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

- Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas.

5. MARCO TEORICO

Esquema

5.1. Seguridades físicas

5.1.1. Revisión de perímetro
5.1.2. Revisión de monitoreo
5.1.3. Evaluación de controles de acceso.
5.1.4. Revisión de respuestas de alarmas.
5.1.5. Revisión de ubicación
5.1.6. Revisión de entorno
5.1.7. Requisitos hardware para un servidor
5.1.7.1. Requisitos de almacenamiento de un clúster
5.1.7.2. Requisitos de CPU
5.1.7.3. Requisitos de memoria de acceso aleatorio (RAM)

5.2. Tipos de métodos para analizar vulnerabilidades de servidores
5.2.1. Modelo de seguridad informática PDCA
5.2.1.1. Análisis de cada nivel

5.3. Seguridad Informática

5.3.1. Propiedades de un sistema seguro

5.3.2. Tipos de ataques

5.4. Escaneo de puertos.
5.4.1. Tipos de Exploración soportados
5.4.1.1. Escaneo TCP connect()
5.4.1.2. Escaneo TCP SYN
5.4.1.3. Escaneo ping:
5.4.1.4. Escaneo Udp

5.5. Analizador de protocolos.
5.6. Ingeniería social.
5.7. Seguridades lógicas
5.7.1. Sondeo de Red
5.7.2. Identificación de los Servicios de Sistemas
5.7.3. Testeo de Sistema de Detección de Intrusos

5.7.4. Testeo de Medidas de Contingencia
5.7.5. Descifrado de Contraseñas
5.7.6. Testeo de Denegación de Servicios
5.7.7. Evaluación de Políticas de Seguridad
5.8. Documentación e informes

5.1. Seguridades físicas

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos.

5.1.1. Revisión de perímetro

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico

1. Trazar mapa del perímetro físico
2. Trazar mapa de las medidas de protección físicas (cercas, puertas, luces, etc.)
3. Trazar mapa de las rutas de acceso y/o métodos físicos
4. Trazar mapa de las áreas no monitoreadas

5.1.2. Revisión de monitoreo

Este es un método para descubrir puntos de acceso monitoreados, a una organización y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico

1. Enumerar los dispositivos de monitoreo
2. Trazar mapa de sitios protegidos y rutas recorridas
3. Trazar mapa de áreas monitoreadas y no monitoreadas
4. Examinar los dispositivos de monitoreo en búsqueda de limitaciones y vulnerabilidades

5. Examinar posibles ataques de denegación de servicio sobre los dispositivos de monitoreo

5.1.3. Evaluación de controles de acceso.

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos

1. Enumerar áreas de control de acceso
2. Examinar dispositivos y tipos de control de acceso
3. Examinar tipos de alarmas
4. Determinar el nivel de complejidad en un dispositivo de control de acceso
5. Determinar el nivel de privacidad en un dispositivo de control de acceso
6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades
7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

5.1.4. Revisión de respuestas de alarmas.

Este es un método para descubrir procedimientos y equipos de alarmas en una organización por medio del descubrimiento de custodia y monitoreo electrónico

1. Enumerar los dispositivos de alarmas
2. Trazar mapa de procedimientos de detonación de alarmas
3. Trazar mapa de precauciones de seguridad activados por alarmas
4. Descubrir las personas involucradas en un procedimiento de alarma
5. Evaluar el incremento de alarma
6. Examinar la activación y desactivación de alarmas
7. Examinar los dispositivos de alarmas en búsqueda de limitaciones y puntos débiles
8. Examinar posibles ataques de denegación de servicio sobre los dispositivos de alarma
9. Examinar posibles ataques de denegación de servicio sobre los procedimientos de alarma

5.1.5. Revisión de ubicación

Este es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos

1. Enumerar las áreas de la organización que son visibles (Línea de visión)
2. Enumerar las áreas dentro de la organización que son audibles (Escuchas electrónicas, con láser y otros dispositivos)
3. Examinar las áreas de la ubicación referentes a las entradas por abastecimiento en búsqueda de puntos débiles y vulnerabilidades
4. Listar las empresas y empleados de abastecimiento
5. Listar las empresas y empleados de limpieza
6. Listar días y horarios de los ciclos de entregas
7. Listar días y horarios de los ciclos de visitantes

5.1.6. Revisión de entorno

Este es un método para ganar acceso o dañar a una organización o sus bienes, a través de puntos débiles en su entorno

1. Examinar las condiciones de la región respecto de los desastres naturales
2. Examinar las condiciones del entorno político
3. Examinar los procedimientos de resguardo y recuperación
4. Identificar puntos débiles y vulnerabilidades en los procedimientos de resguardo y recuperación
5. Identificar posibles ataques de denegación de servicio en los procedimientos de resguardo y recuperación
6. Examinar impedimentos físicos y electrónicos frente a distintas condiciones climáticas
7. Comparar procedimientos operacionales con las leyes, costumbres y ética regional

5.1.7. Requisitos hardware para un servidor

5.1.7.1. Requisitos de almacenamiento de un clúster

Cada nodo de un clúster debe disponer de suficiente capacidad de almacenamiento permanente para almacenar copias permanentes de todas las aplicaciones y otros

recursos necesarios para ejecutar todos los grupos. Realice este cálculo para cada nodo como si todos estos recursos del clúster se estuviesen ejecutando en ese nodo, aunque algunos o todos los grupos se ejecuten en otros nodos la mayor parte del tiempo. Organice estos permisos de espacio de disco de forma que cualquier nodo pueda ejecutar eficazmente todos los recursos durante una conmutación por error.

5.1.7.2. Requisitos de CPU

La conmutación por error puede forzar la capacidad de procesamiento de la CPU de un nodo cuando toma el control de los recursos desde un nodo en el que se ha producido un error. Sin un plan adecuado, es posible que durante la conmutación por error se exceda la capacidad práctica de la CPU del nodo activo, lo que reduciría el tiempo de respuesta para los usuarios. Planee la capacidad de la CPU de cada nodo, de forma que se puedan ejecutar nuevos recursos y la CPU siga respondiendo eficazmente.

5.1.7.3. Requisitos de memoria de acceso aleatorio (RAM)

Cuando planee la capacidad, asegúrese de que cada nodo del clúster tiene suficiente memoria RAM para ejecutar todas las aplicaciones que podrían ejecutarse en cualquier nodo. Además, asegúrese de que los archivos de paginación están configurados correctamente para la memoria RAM de cada nodo.
Para obtener más información acerca de los archivos de paginación, vea Optimizar el tamaño y la ubicación del archivo de paginación y Cambiar el tamaño del archivo de paginación de memoria virtual.

5.2. Tipos de métodos para analizar vulnerabilidades de servidores

La sociedad de la información y las nuevas tecnologías de comunicaciones plantean la necesidad de mantener la confidencialidad de la información que soportan los sistemas de las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas. El núcleo del negocio no debe parar, es la capacitación especializada la que conforma profesionales especializados en seguridad

informática para que implementen y gestionen de manera eficaz sus sistemas de información en forma segura.

5.2.1. Modelo de seguridad informática PDCA

Dada la complejidad del problema de la seguridad cuando se trata como un todo dentro de la organización, surge de forma natural la necesidad de la gestión de la seguridad por lo que las organizaciones deben plantearse un sistema de gestión de la seguridad de la información SGSI. El objetivo primordial de los SGSI es salvaguardar la información, para empezar se debe identificar que "activos de información" deben ser protegidos y en qué grado, luego debe aplicarse el plan PDCA "PLAN – DO – CHECK – ACT", es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

La seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización: En consecuencia la organización debe entender la seguridad como un proceso que nunca termina pues Los riesgos nunca se eliminan en cambio se gestionan. De los riesgos se desprende que los problemas de seguridad no son únicamente de índole tecnológica por ello nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que inician por Planificar y termina en Actuar, reciclando en mejoras continuas:

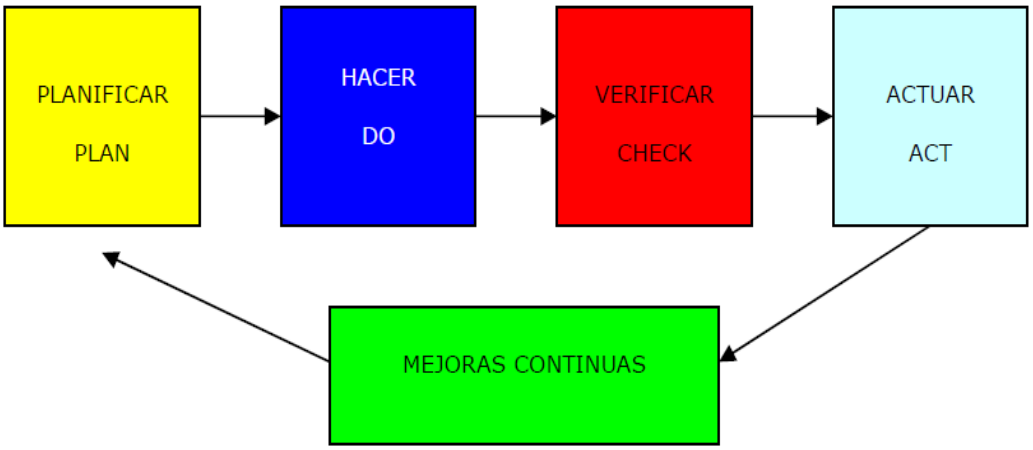


Fig 1. Modelo PDCa

5.2.1.1. Análisis de cada nivel

PLANIFICAR (Plan): Establecer el contexto

- En este nivel se crean las Políticas de seguridad
- Se describe el alcance del SGSI
- Se hace análisis de riesgos
- Selección de controles
- Estado de aplicabilidad

HACER (Do): Implementar el sistema

- Implementar el sistema de gestión de seguridad de la información
- Implementar el plan de riesgos
- Implementar los controles

VERIFICAR (Check): Monitorea y revisa

- Monitorea las actividades
- Revisa
- Hace auditorías internas

ACTUAR (Act): Mantenimiento y mejora

- Implementa mejoras
- Acciones preventivas
- Acciones correctivas

5.3. Seguridad Informática

Un sistema de información se considera seguro si se encuentra libre de todo riesgo y daño Es imposible garantizar la seguridad o la inviolabilidad absoluta de un sistema informático, por ello es preferible utilizar el término fiabilidad

La seguridad informática es una idea subjetiva, mientras la inseguridad informática es una idea objetiva, es por ello que no es fácil tener control absoluto sobre la seguridad

informática, porque lo subjetivo es incierto, esto no ocurre con la inseguridad informática, que sabemos a ciencia cierta, que nos va a ocurrir si continuamos conviviendo irresponsablemente con las vulnerabilidades y los riesgos inherentes de nuestros sistemas informáticos.

5.3.1. Propiedades de un sistema seguro

Hay 3 variables o parámetros que determinan el estado de un sistema informático, estos son:

- **Confidencialidad:** Los recursos del sistema solo pueden ser accedidos por los elementos autorizados

- **Integridad:** Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados

- **Disponibilidad:** Los recursos del sistema deben permanecer accesibles a los elementos autorizados

5.3.2. Tipos de ataques

- **Modificación:** También llamados webdefacement buscan comprometer la confidencialidad y la integridad del sistema, por ejemplo cuando un atacante modifica la página web de una organización sin previa autorización

- **Fabricación:** comprometen la integridad del sistema por ejemplo al insertar un nuevo usuario en el sistema operativo

- **Interceptación:** Busca comprometer la confidencialidad del sistema, un ejemplo son los key loggers o spyware y los Sniffers

- **Interrupción:** Comprometen la propiedad Disponibilidad un ejemplo serían los ataques de denegación de servicios o DoS.

5.4. Escaneo de puertos.

La exploración de puertos es una de las primeras etapas que el atacante elabora dentro del plan de ataque para investigar o enumerar cuales servicios tienen la victima activados.

Existen muchas herramientas para hacer exploración de puertos pero en este documento solo se abordara la más utilizada y conocida en el entorno académico: nmap.

Nmap ha sido diseñado para permitir a administradores de sistemas y gente curiosa en general el escaneo de grandes redes para determinar que servidores se encuentran activos y que servicios ofrecen.

NMAP es compatible con un gran número de técnicas de escaneo como: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, and Null scan.

NMAP proporciona también características avanzadas como la detección remota del sistema operativo por medio de huellas TCP/IP, escaneo tipo stealth (oculto), retraso dinámico y cálculos de retransmisión, escaneo paralelo, detección de servidores inactivos por medio de ping paralelos, escaneo con señuelos, detección de filtrado de puertos, escaneo por fragmentación y especificación flexible de destino y puerto.

Se han hecho grandes esfuerzos encaminados a proporcionar un rendimiento decente para usuarios normales, por desgracia, muchas de las interfaces críticas del kernel (tales como los raw sockets) requieren privilegios de administrador. Entonces para efectos prácticos se debería ejecutarse nmap como el usuario root en sistemas Linux/unix siempre que sea posible.

5.4.1. Tipos de Exploración soportados

5.4.1.1. Escaneo TCP connect()

Es la forma más básica de escaneo TCP. La llamada de sistema connect() proporcionada por nuestro sistema operativo se usa para establecer una conexión con todos los puertos interesantes de la máquina.

Si el puerto está a la escucha, connect() tendrá éxito, de otro modo, el puerto resulta inalcanzable. Una ventaja importante de esta técnica es que no resulta necesario tener privilegios especiales. Cualquier usuario en la mayoría de los sistemas UNIX tiene permiso para usar esta llamada.

Este tipo de escaneo resulta fácilmente detectable dado que los registros del servidor de destino muestran un montón de conexiones y mensajes de error para aquellos servicios que accept() (aceptan) la conexión para luego cerrarla inmediatamente.

5.4.1.2. Escaneo TCP SYN

A menudo se denomina a esta técnica escaneo "half open" (medio abierto), porque no se abre una conexión TCP completa. Se envía un paquete SYN, como si se fuese a abrir una conexión real y se espera que llegue una respuesta.

Un SYN|ACK indica que el puerto está a la escucha. Un RST es indicativo de que el puerto no está a la escucha. Si se recibe un SYN|ACK, se envía un RST inmediatamente para cortar la conexión (en realidad es el kernel de nuestro sistema operativo el que hace esto por nosotros).

La ventaja principal de esta técnica de escaneo es que será registrada por muchos menos servidores que la anterior. Por desgracia se necesitan privilegios de root para construir estos paquetes SYN modificados.

5.4.1.3. Escaneo ping:

A veces únicamente se necesita saber que servidores en una red se encuentran activos. Nmap puede hacer esto enviando peticiones de respuesta ICMP a cada dirección IP de la red que se especifica. Aquellos servidores que responden se encuentran activos. Desafortunadamente, algunos sitios web como microsoft.com bloquean este tipo de paquetes. Nmap puede enviar también un paquete TCP ack al puerto 80 (por defecto), si se obtiene por respuesta un RST, esa máquina está activa. Una tercera técnica implica el envió de un paquete SYN y la espera de un RST o un SYN/ACK. Para usuarios no root se usa un método connect(). Por defecto (para usuarios no root), nmap usa las técnicas ICMP y ACK en paralelo. Se puede cambiar la opción -p descrita más adelante. Nótese que el envió de ping se realiza por defecto de todas maneras y que solamente se escanean aquellos servidores de los que se obtiene respuesta. Esta opción solamente en el caso de que desee un ping sweep (barrido ping) sin hacer ningún tipo de escaneo de puertos.

5.4.1.4. Escaneo Udp

Este método se usa para saber que puertos UDP (Protocolo de Datagrama de Usuario, RFC 768) están abiertos en un servidor. La técnica consiste en enviar paquetes UCP de 0 bytes a cada puerto de la maquina objetivo. Si se recibe un mensaje ICMP de puerto no alcanzable, entonces el puerto está cerrado. De lo contrario, asumimos que está abierto.

Alguna gente piensa que el escaneo UDP no tiene sentido. Se recuerda el reciente agujero en Solaris rpcbind. Puede encontrarse a rpcbind escondido en un puerto UDP no documentado en algún lugar por encima del puerto 32770.

Por lo tanto, no importa que el puerto 111 este bloqueado por el firewall. Pero, quien puede decir en cuál de los más de 30000 puertos altos se encuentra a la escucha el programa Con un escáner UDP se podría

Por desgracia, el escaneo UDP resulta a veces tremendamente lento debido a que la mayoría de los servidores implementan una sugerencia recogida en el RFC 1812 acerca de la limitación de la frecuencia de mensajes de error ICMP.

5.5. Analizador de protocolos.

Un analizador de protocolos es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite al ordenador capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red que se está analizando. Esto último es muy importante para un programador que esté desarrollando un protocolo, o cualquier programa que transmita y reciba datos en una red, ya que le permite comprobar lo que realmente hace el programa.

Además de para los programadores, estos analizadores son muy útiles a todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red, si bien su estudio puede resultar poco ameno, sobre todo si se limita a la estructura y funcionalidad de las unidades de datos que intercambian. También, gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos, para así, comprender mejor su funcionamiento.

Los analizadores de protocolos se usan en diversas arquitecturas de red, tales como Redes LAN (10/100/1000 Ethernet; Token Ring; FDDI (Fibra óptica)), Redes Wireless LAN, Redes Gigabit, Redes WAN...

5.6. Ingeniería social.

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema está solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (pesca). Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores. En realidad, los administradores de sistemas informáticos raramente (o nunca) necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas. Sin embargo incluso este tipo de ataque podría no ser necesario — en una encuesta realizada por la empresa Boixnet, el 90% de los empleados de oficina de la estación Waterloo de Londres reveló sus contraseñas a cambio de un bolígrafo barato.

5.7. Seguridades lógicas

5.7.1. Sondeo de Red

El sondeo de red es simplemente una forma de empezar un test; otra forma sería recibir el rango de direcciones IP a comprobar. En este módulo, no se realiza ningún tipo de intrusión directamente en los sistemas, excepto en los sitios considerados un dominio cuasi-público. En términos legales, un dominio cuasi-público es una tienda que invita a realizar compras. La tienda puede controlar el acceso y puede denegar la entrada a ciertos individuos, aunque la mayor parte de la tienda esté abierta al público

en general (incluso en aquellos casos en que se monitoree a los usuarios). Este es el paralelismo al e-business o a un sitio web. A pesar de no ser realmente un módulo en la metodología, el sondeo de red es un punto de partida. Muy a menudo se detectan más hosts durante el test. Hay que tener en cuenta que los hosts descubiertos posteriormente pueden ser añadidos en las pruebas como un subconjunto de los sistemas definidos y a menudo solamente con el permiso o colaboración del equipo de seguridad interna de la organización a analizar

5.7.2. Identificación de los Servicios de Sistemas

En este módulo se deben enumerar los servicios de Internet activos o accesibles así como traspasar el cortafuego con el objetivo de encontrar más máquinas activas. La pequeña cantidad de protocolos empleados aquí tiene el objetivo de resultar en una definición clara de los objetivos. Es por esto que algunos de los protocolos no aparecen.

El testeo de diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los sistemas. En la sección Referencias de Testeo aparece una lista más completa de protocolos. Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP posibles (incluido el Puerto 0). En cualquier caso, no siempre es necesario comprobar todos estos puertos en cada sistema. Esto se deja a la libre elección del equipo que realiza los tests.

Los puertos que son importantes para el testeo según el servicio que ofrecen se listan con las tareas del módulo.

Una vez los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. En algunos casos, más de una aplicación puede encontrarse detrás de un servicio donde una aplicación es la que realmente escucha en dicho puerto y las otras se consideran componentes de la aplicación que escucha.

5.7.3. Búsqueda y Verificación de Vulnerabilidades

La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red. La investigación concerniente a la búsqueda de vulnerabilidades es necesaria hasta prácticamente el momento de la entrega del informe.

Esta investigación incluye la búsqueda en bases de datos online y listas de correo relativas a los sistemas y redes que se están auditando. No se debe limitar la búsqueda a la web, también se debe considerar la utilización del IRC, grupos de noticias, y sitios FTP underground. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Aunque muchos escáneres automáticos están actualmente tanto en el mercado como en el mundo underground, es importante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen actualmente en el mundo underground.

No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida de la red. La búsqueda manual de vulnerabilidades hace referencia a las personas que delante del ordenador utilizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo

5.7.4. Testeo de Aplicaciones de Internet

Un test de Aplicaciones de Internet emplea diferentes Técnicas de testeo de Software para encontrar “fallos de seguridad” en aplicaciones cliente/servidor de un sistema desde Internet. En este módulo, nos referimos a aplicaciones cliente/servidor que sean desarrolladas por los administradores de sistema con propósitos de la empresa y programadas con cualquier tecnología y lenguaje de programación. E.j. Aplicaciones web para transacciones entre empresas es un objetivo en este módulo. Tests como "Caja Negra" y/o "Caja Blanca" pueden ser utilizados en este módulo

5.7.5. Enrutamiento

Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado. La protección también debe estar diseñada para restringir el flujo de salida de ciertos tipos de tráfico. Los Router están siendo cada vez más complejos y algunos tienen propiedades desconocidas para el auditor y a veces para la organización auditada. El papel del auditor es en parte determinar la función del router dentro de la DMZ

5.8. Detección de vulnerabilidades

5.8.1. Revisión de Privacidad

La revisión de privacidad se centra en cómo se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a empleados y clientes. La utilización de estos datos supone una gran preocupación para muchas personas y es por esto que la legislación está definiendo reglas específicas con relación a la privacidad. Aunque muchas de estas leyes son locales, todas son aplicables a Internet y por tanto afectan de forma internacional a todos los auditores de seguridad.

5.8.2. Testeo de Sistema de Detección de Intrusos

Este test está enfocado al rendimiento y susceptibilidad de un IDS. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunos de estos tests están relacionados con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estos tests.

Repasar los registros del servidor es necesario para verificar que los tests realizados en presencia en Internet, especialmente en los casos donde el resultado de éstos no es inmediatamente evidente para el auditor .Algunos que son desconocidos son destinados para el analista, quien no ha revisado los registros y alertas

5.8.3. Testeo de Medidas de Contingencia

Las medidas de contingencia dictan el manejo de lo traspasable, programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados. Debe ser necesario responder primero a una nueva cuenta de correo electrónico de pruebas o al sistema de escritorio donde el administrador pueda monitorizar

5.8.4. Descifrado de Contraseñas

Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizadas, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos.

Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que explote los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos

(p.ej. Usuario: SystemContraseña: Test) o fácilmente predecible por parte del error de un usuario (p.ej. Usuario: joe Contraseña: joe).Este puede ser un sistema para obtener acceso a un sistema inicialmente, quizá sea siempre con acceso de administrador o root, pero solo con fines educativos.

Una vez entrado con privilegios de root o administrador en un sistema, el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales (gracias a los usuarios cuyas contraseñas sean coincidentes en múltiples sistemas) y es una técnica válida que puede ser usada por influencia del sistema a través de un test de seguridad. Descifrados de contraseñas minuciosos pueden ser realizados como un ejercicio de simple y debe ser subrayada la necesidad de algoritmos criptográficos fuertes para contraseñas de almacenamiento de sistemas de llave, también subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática, o módulos del tipo PAM

5.8.5. Testeo de Denegación de Servicios

La Denegación de Servicios (DoS) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos. Es muy importante que los tests de DoS reciban ayuda adicional de la organización y sea monitorizada a nivel privado. Inundación y ataques DoS Distribuidos (DDoS) están específicamente no comprobados y prohibidos por este manual. Los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo.

5.8.6. Evaluación de Políticas de Seguridad

Esta tareas exigen que el testeo y verificación de vulnerabilidades sea hecho en su totalidad y que todas las otras revisiones técnicas hayan sido llevadas a cabo. A menos que esto sea realizado, no es posible compararlos resultados con los lineamientos a lograr especificados por las políticas de seguridad, traducidos en medidas de protección del entorno operativo.

5.9. Documentación e informes

Como finalización del análisis de vulnerabilidades se debe presentar un informe donde se detalle cada uno de los tests realizados y los resultados.

En este informe se debe especificar:

- Diseño de un sistema de seguridad.
- Soluciones de seguridad.
- Lista de vulnerabilidades probadas.
- Lista de vulnerabilidades detectadas.
- Lista de servicios y dispositivos vulnerables.

6. METODOLOGIA

6.1. MATRIZ DE CONSISTENCIA GENERAL

PROBLEMA DE INVESTIGACIÓN: Falta seguridades físicas y lógicas de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, y falta de un plan de mitigación de riesgos.			
TEMA	**OBJETO DE INVESTIGACIÓN**	**OBJETIVO DE INVESTIGACIÓN**	**HIPÓTESIS DE INVESTIGACIÓN**
Análisis de vulnerabilidades físicas y lógicas de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, y construcción de un plan de mitigación de riesgos.	Los servidores internos y externos de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Construir un plan de mitigación de riesgos para minimizar el impacto de los posibles ataques a los servidores de la UNL	Un plan de mitigación de riesgos permitirá reducir notablemente el riesgo de ataques mal intencionados a los servidores de la UNL y contribuirá a resguardar correctamente la información de los mismos.

Tabla N° 1: Matriz de Consistencia General

6.2. Materiales, métodos y técnicas de trabajo

6.2.1. Métodos

El desarrollo del proyecto de investigación requiere seguir los lineamientos de ciertos métodos, así como de técnicas e instrumentos que permitan la recopilación y análisis de la información necesaria para la presentación del proyecto de tesis, tales como:

- **Método Inductivo.-** Va de lo particular a lo general. Se lo utilizó para determinar el problema general de investigación.

- **Método Deductivo.-** De lo general a lo particular. Este método nos sirve para encontrar las soluciones adecuadas para los problemas específicos planteados en el presente trabajo investigativo.

- **Método Analítico.-** Sirve para realizar un análisis del objeto en estudio. Se utiliza para realizar un minucioso estudio de los problemas, causas y consecuencias que se está respecto al problema general de investigación.

- **Método de Caja Blanca**.- Se tiene una visión total de la red a analizar, así como acceso a todos los equipos como súper usuario. Este tipo de análisis tiene la ventaja de ser más completo y exhaustivo para detectar las vulnerabilidades de los servidores.

6.2.2. Técnicas e instrumentos.

Los métodos e instrumentos que se utilizarán para la recopilación de la información son los siguientes:

- **Test de Penetración.-** Durante el test de penetración se simula ser un atacante. Desde esta posición, se realizan varios intentos de ataques a la red, buscando debilidades y vulnerabilidades. El resultado del test de penetración mostrará una idea general del estado de la seguridad de los sistemas frente a los ataques. Si se encontraran una o más vulnerabilidades, no se realiza su explotación.

- **Lectura comprensiva.-** Consiste en obtener un conocimiento ordenado y sistemático de un aspecto de la realidad o de los acontecimientos hecho o ideas relacionadas con el tema específico.

- **La Entrevista:** Esta técnica es muy importante para el realizar un análisis preliminar, pues permite obtener la información en forma verbal, a través de preguntas a los encargados del Departamento de Telecomunicaciones e Información.

- **La Observación:** Esta técnica permite apreciar los problemas encontrados respecto a la falta de seguridad en los servidores de la Universidad Nacional de Loja

- **La Encuesta:** Son entrevistas con un gran número de personas utilizando un cuestionario prediseñado. Según el mencionado autor, el método de encuesta incluye un cuestionario estructurado que se da a los encuestados y que está diseñado para obtener información específica.

7. CRONOGRAMA

8. PRESUPUESTO Y FINANCIAMIENTO

Los materiales que vamos a utilizar para desarrollar este proyecto, son los siguientes:

Descripción	Cantidad	Horas	Valor/unit	Valor/Total
Recursos Humanos				
Aspirantes	2	1200	$0.00	$0.00.
Coordinador	1	300	$0.00	$0.00
Asesor Proyecto	1	100	$0.00	$0.00
Recursos Técnicos y Tecnológicos				
Hardware				
Computador Portátil Packard Bell Easynote TJ76	1	200	$ 0.70	$ 140.00
Computador Portátil Dell Inspiron 1420	1	200	$ 0.70	$ 140.00
Impresora	300	s/v	$ 0.10	$ 30.00
Software				
CentOS 5.3	1	n/a	$ 0.00	$ 0.00
Linux Backtrack 2.0 o superior	1	n/a	$ 0.00	$ 0.00

Nessus	1	n/a	$ 0.00	$ 0.00
Nmap	1	n/a	$ 0.00	$ 0.00
Recursos Materiales				
Hojas A4	300		$ 0.03	$ 9.00
Anillado	3		$ 1.80	$ 5.40
Materiales de oficina	Varios		varios	$ 35.00
Borde o Perfil	5		$ 0.50	$ 2.50
CD's	5		$ 0.35	$ 1.75

Tabla N° 2 Presupuesto

Resumen del Presupuesto

Resumen del Presupuesto	Costo Total
Recursos Humanos	$0.00
Recursos Técnicos y Tecnológicos	$330.00
Recursos Materiales	$53.65
SUBTOTAL	$383.65
Imprevistos 15 %	$57.54
TOTAL	**$441.19**

Tabla N° 3 Resumen de Presupuesto

9. BIBLIOGRAFIA

LIBROS:

- CARVAJAL, Armando. 2007. Técnicas globales para la seguridad de la información. Medellín, Colombia. GlobaltekSecurity. Pág. 140.
- MORON LERMA, Esther. 2002. Internet y derecho penal: Hacking y otras conductas ilícitas en la red. Madrid- España. Editorial Aranzadi S.A. Pág. 155.
- SCHNEIER BRUCE, Beyond Fear. 2003. Thinking Sensibly about security in an uncertain world. Toronto, Canada. Copernicus Books. Pág 126.
- TORI, Carlos. 2008. Ingeniería Social: Hacking Ético. Buenos Aires, Argentina. Mastroianni Impresiones. Pág.86-92.

PÁGINAS WEB:

- COLABORACIÓN DE VARIOS. Servidores y sus servicios. 2010. [En línea]. [http://es.scribd.com/doc/56130026/35/Identificacion-de-los-Servicios-de-Sistemas]. [Consulta: 19 Septiembre 2011].

- COLABORACIÓN DE VARIOS. Hardware para servidores. 2009. [En línea]. [http://technet.microsoft.com/es-es/library/cc740023%28WS.10%29.aspx]. [Consulta: 01 Septiembre 2011].

- COLABORACIÓN DE VARIOS. Seguridades informáticas. 2006. [En línea]. [http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29]. [Consulta: 11 agosto 2011].

Anexos

10. Matriz de consistencia específica.

PROBLEMA ESPECÍFICO: Desconocimiento de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Data center de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Revisión de perímetro Revisión de monitoreo Evaluación de controles de acceso. Revisión de respuestas de alarmas. Revisión de ubicación Revisión de entorno Seguridad informática

Tabla N° 4 Matriz de consistencia específica 1

PROBLEMA ESPECÍFICO: No tener identificadas las vulnerabilidades físicas que se necesitan en el Data Center de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Data center de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Protección del hardware Protección de los datos.

Tabla N° 5 Matriz de consistencia específica 2

PROBLEMA ESPECÍFICO: Variedad de herramientas para detectar las vulnerabilidades en los servidores.		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores	Los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Tipos de métodos para analizar vulnerabilidades de servidores Seguridad Informática Escaneo de puertos. Analizador de protocolos. Ingeniería social.

Tabla N° 6 Matriz de consistencia específica 3

PROBLEMA ESPECÍFICO: Falta de conocimiento de los puntos vulnerables en cada uno de los servicios que brindan los servidores		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Realizar pruebas a los servidores en busca de vulnerabilidades en los diferentes servicios que brindan.	Los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Sondeo de Red Identificación de los Servicios de Sistemas Búsqueda y Verificación de Vulnerabilidades Testeo de Aplicaciones de Internet Enrutamiento Verificación de Redes Inalámbricas.

Tabla N° 7. Matriz de consistencia específica 4

PROBLEMA ESPECÍFICO: No tener implantado seguridades lógicas necesarias para resguardar los servidores de posibles ataques.		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.	Los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Vulnerabilidades de implementación. Vulnerabilidades de configuración. Vulnerabilidades de dispositivo. Vulnerabilidades de protocolo. Vulnerabilidades de aplicación Revisión de Privacidad Testeo de Aplicaciones de Internet. Testeo de Sistema de Detección de Intrusos Testeo de Medidas de Contingencia Descifrado de Contraseñas Testeo de Denegación de Servicios Evaluación de Políticas de Seguridad

Tabla N° 8. Matriz de consistencia específica 5

PROBLEMA ESPECÍFICO: Ausencia de un plan de mitigación de riesgos que ayude a minimizar un posible ataque a los servidores.		
OBJETIVO ESPECÍFICO	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas.	Los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja	Documentación e informe.

Tabla N° 9. Matriz de consistencia específica 6

10.2. Matriz de operatividad de objetivos específicos

- **OBJETIVO ESPECÍFICO:** Realizar un análisis de la situación física y lógica actual de los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Determinar el personal a ser entrevistado	Entrevista	03/10/2011	03/10/2011	Investigadores	2	Constatar el estado físico del Data Center en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja
Elaborar la entrevista para cada uno del personal involucrado	Entrevista	04/10/2011	07/10/2011	Investigadores	2	
Imprimir las entrevistas	Entrevista	10/10/2011	10/10/2011	Investigadores	10	
Aplicar entrevistas	Entrevista	11/10/2011	11/10/2011	Investigadores	2	

Analizar los resultados	Entrevista	12/10/2011	13/10/2011	Investigadores	5	
Constatación las seguridades físicas de los servidores	Observación	14/10/2011	18/10/2011	Investigadores	10	
Elaborar una lista con las principales vulnerabilidades físicas	Deductivo	19/10/2011	26/10/2011	Investigadores	20	

Tabla N° 10 Matriz de operatividad de objetivos específicos 1

- **OBJETIVO ESPECÍFICO :** Determinar las seguridades físicas y el equipamiento necesario para los servidores de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Examinar cada una de las vulnerabilidades de la lista preestablecida.	Deductivo	02/01/2012	04/01/2012	Investigadores	25	
Escoger las soluciones más viables en la parte de las seguridades físicas.	Analítico	05/01/2012	10/01/2012	Investigadores	20	
Obtener la lista de las características hardware de cada uno de los servidores.	Deductivo	11/01/2012	12/01/2012	Investigadores	10	
Investigar el tipo de hardware necesario para	Deductivo	13/01/2012	16/01/2012	Investigadores	20	

los servidores de acuerdo al servicio que brinda.	Inductivo	17/01/2012	19/01/2012	Investigadores	40	
Elaborar una lista con las características hardware para cada uno de los servidores.	Inductivo	20/01/2012	25/01/2012	Investigadores	20	
Realizar una lista con las vulnerabilidades	Analítico	26/01/2012	31/01/2012	Investigadores	30	
Clasificar las vulnerabilidades lógicas.	Analítico	01/02/2012	06/02/2012	Investigadores	15	Identificar claramente cuáles son las principales vulnerabilidades a nivel físico de los servidores y sus requerimientos hardware
Clasificar las vulnerabilidades por un nivel de riesgo.						
Investigar acerca de parches para servidores Linux.	Inductivo	07/02/2012	14/02/2012	Investigadores	30	
Realizar una lista de	Deductivo	15/02/2012	17/02/2012	Investigadores	15	

configuraciones posibles.						

Tabla N° 11 Matriz de operatividad de objetivos específicos 2

- **OBJETIVO ESPECÍFICO**: Establecer las herramientas adecuadas para el análisis de las vulnerabilidades lógicas en los servidores.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Investigación en libros, revistas e internet.	Inductivo	27/10/2011	31/10/2011	Investigadores	35	Encontrar las herramientas adecuadas para detectar las vulnerabilidades de los servidores.
Analizar ventajas y desventajas de cada herramienta	Analítico	01/11/2011	11/11/2011	Investigadores	15	
Determinar el grupo de herramientas adecuado para realizar las pruebas	Deductivo	14/11/2011	25/11/2011	Investigadores	5	

Tabla N° 12 Matriz de operatividad de objetivos específicos 3

- **OBJETIVO ESPECÍFICO:** Realizar pruebas a los servidores en busca de vulnerabilidades en los diferentes servicios que brindan.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Elaboración de entrevista para los encargados de los servidores.	Entrevista	01/12/2011	09/12/2011	Investigadores	5	
Realizar entrevista a los encargados de los servidores.	Entrevista	12/12/2011	16/12/2011	Investigadores	10	
Analizar los resultados de la	Analítico	19/12/2011	19/12/2011	Investigadores	5	

entrevista. Fase de reconocimiento de los servidores (Servicios que brinda). Análisis de servicios disponibles. Estudio de debilidades.	Método de caja blanca Método de caja blanca Método de caja blanca	20/12/2011 21/12/2011 22/12/2011	20/12/2011 21/12/2011 23/12/2011	Investigadores Investigadores Investigadores	10 5 2	Encontrar las vulnerabilidades en los diferentes servicios que brindan los servidores

Tabla N° 13 Matriz de operatividad de objetivos específicos 4

- **OBJETIVO ESPECÍFICO:** Implantar las soluciones de las seguridades lógicas en los servidores bajo la supervisión de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Elegir las configuraciones más idóneas para los servidores.	Inductivo	20/02/2012	27/02/2012	Investigadores	20	Identificar claramente las vulnerabilidades tanto físicas como lógicas e determinar el nivel de riesgo que representa.
Implementar las configuraciones bajo la supervisión de la UTI	Inductivo	28/02/2012	20/03/2012	Investigadores	5	
Comprobar que las vulnerabilidades han sido solucionadas.	Analítico	21/03/2012	09/04/2012	Investigadores	6	

Tabla N° 14 Matriz de operatividad de objetivos específicos 5

- **OBJETIVO ESPECÍFICO:** Construir un plan de mitigación de riesgos en base a las vulnerabilidades encontradas.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLES	PRESUPUESTO	RESULTADOS ESPERADOS
		INICIO	FINAL			
Realizar una lista de vulnerabilidades probadas	Inductivo	10/04/2012	13/04/2012	Investigadores	25	
Elaborar una Lista de vulnerabilidades detectadas.	Inductivo	16/04/2012	18/04/2012	Investigadores	20	
Hacer una Lista de servicios y dispositivos vulnerables.	Inductivo	19/04/2012	23/04/2012	Investigadores	35	

Realizar el nivel de riesgo que involucra cada vulnerabilidad encontrada en cada servicio y dispositivo.	Inductivo	24/04/2012	27/04/2012	Investigadores	15	
Añadir conclusiones y recomendaciones al informe.	Deductivo	30/04/2012	02/05/2012	Investigadores	10	Elaborar el plan de mitigación de riesgos.
Imprimir el plan de mitigación de riesgos.						
Entregar el plan de mitigación de riesgos a los encargados de los servidores.		03/05/2012	03/05/2012	Investigadores	70	

Tabla N° 15 Matriz de operatividad de objetivos específicos 6

10.3 Matriz de control de resultados

N°	RESULTADOS	FECHA		FIRMA DEL DOCENTE
		INICIO	FIN	
1	Determinar el personal a ser entrevistado	03/10/2011	03/10/2011	
2	Elaborar la entrevista para cada uno del personal involucrado	04/10/2011	07/10/2011	
3	Imprimir las entrevistas	10/10/2011	10/10/2011	
4	Aplicar entrevistas	11/10/2011	11/10/2011	
5	Analizar los resultados	12/10/2011	13/10/2011	

6	Constatación las seguridades físicas de los servidores	14/10/2011	18/10/2011	
7	Elaborar una lista con las principales vulnerabilidades físicas	19/10/2011	26/10/2011	
8	Examinar cada una de las vulnerabilidades de la lista preestablecida.	02/01/2012	04/01/2012	
9	Escoger las soluciones más viables en la parte de las seguridades físicas.	05/01/2012	10/01/2012	

10	Obtener la lista de las características hardware de cada uno de los servidores.	11/01/2012	12/01/2012	
11	Investigar el tipo de hardware necesario para los servidores de acuerdo al servicio que brinda.	13/01/2012	16/01/2012	
12	Elaborar una lista con las características hardware para cada uno de los servidores.	17/01/2012	19/01/2012	
13	Realizar una lista con las vulnerabilidades	20/01/2012	25/01/2012	
14	Clasificar las vulnerabilidades	26/01/2012	31/01/2012	

	lógicas.			
15	Clasificar las vulnerabilidades por un nivel de riesgo.	01/02/2012	06/02/2012	
16	Investigar acerca de parches para servidores Linux.	07/02/2012	14/02/2012	
17	Realizar una lista de configuraciones posibles.	15/02/2012	17/02/2012	
18	Investigación en libros, revistas e internet.	27/10/2011	31/10/2011	
19	Analizar ventajas y desventajas de cada herramienta	01/11/2011	11/11/2011	

20	Determinar el grupo de herramientas adecuado para realizar las pruebas	14/11/2011	25/11/2011	
21	Elaboración de entrevista para los encargados de los servidores.	01/12/2011	09/12/2011	
22	Realizar entrevista a los encargados de los servidores.	12/12/2011	16/12/2011	
23	Analizar los resultados de la entrevista.	19/12/2011	19/12/2011	
24	Fase de reconocimiento de los servidores (Servicios que brinda).	20/12/2011	20/12/2011	

25	Análisis de servicios disponibles.	21/12/2011	21/12/2011	
26	Estudio de debilidades.	22/12/2011	23/12/2011	
27	Elegir las configuraciones más idóneas para los servidores.	20/02/2012	27/02/2012	
28	Implementar las configuraciones bajo la supervisión de la UTI	28/02/2012	20/03/2012	
29	Comprobar que las vulnerabilidades han sido solucionadas .	21/03/2012	09/04/2012	
30	Añadir conclusiones y recomendaciones al informe.	30/04/2012	02/05/2012	

31	Imprimir el plan de mitigación de riesgos.	03/05/2012	03/05/2012	
32	Entregar el plan de mitigación de riesgos a los encargados de los servidores.	04/05/2012	04/05/2012	

Tabla N° 16 Matriz de control de resultados

ANEXO X: Certificado UTI

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD TELECOMUNICACIONES E INFORMACIÓN

ING. MILTON PALACIOS

C E R T I F I C A:

Que se ha implementado en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja un servidor de análisis de las vulnerabilidades de la red, el mismo que es parte para dar cumplimiento con un objetivo del proyecto de investigación que titula **"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS"** de los egresados Mariana Carmen González González y Cesar Augusto Bastidas Moncayo, aspirantes a obtener el Título de Ingeniero en Sistemas. Este proyecto fue desarrollado en los términos que fue planteado en la propuesta, y actualmente se encuentra prestando el servicio de monitoreo de las vulnerabilidades mediante la herramienta Nessus en la Unidad antes mencionada.

Es cuanto puedo certificar en honor a la verdad.

Loja, 26 de septiembre de 2012

Lo certifica,

Ing. Milton Palacios M.
DIRECTOR TELECOMUNICACIONES E INFORMACIÓN

Tngo. Daniel Reyes T.
RESPONSABLE SECCIÓN REDES

ANEXO XI: Certificado SGA

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD DE TELECOMUNICACIONES E NFORMACIÓN

Ing. Milton Palacios
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

CERTIFICA:

Los tesistas **Mariana Carmen González González** y **Cesar Augusto Bastidas Moncayo** no han podido solucionar las vulnerabilidades detectadas en los servidores que conforman el sistema de Gestión Académica en su proyecto de fin de Carrera que titula **"ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS."** Ya que estos servidores se encuentran en producción y no es posible la manipulación de ningún archivo que podría comprometer el funcionamiento de los mismos.

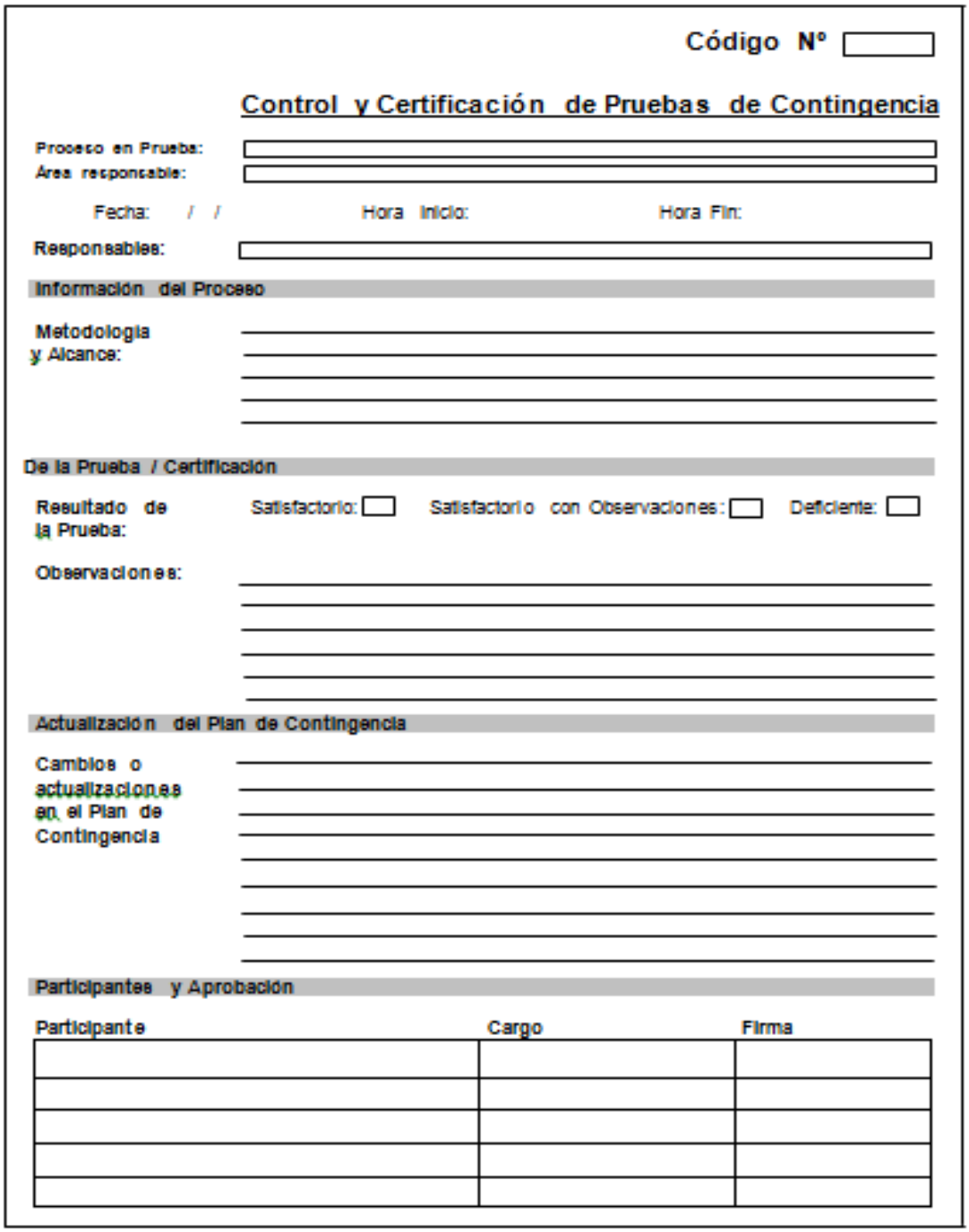
Es cuanto puedo certificar en honor a la verdad.

Loja, 20 de Febrero del 2013.

Ing. Milton Palacios
DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

ANEXO XII: Modelo de Control y certificación del Plan de Mitigación de Riesgos

Riesgos Físicos



Código Nº

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba:
Área responsable:

Fecha: / / Hora Inicio: Hora Fin:

Responsables:

Información del Proceso

Metodología y Alcance:

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: Satisfactorio con Observaciones: Deficiente:

Observaciones:

Actualización del Plan de Contingencia

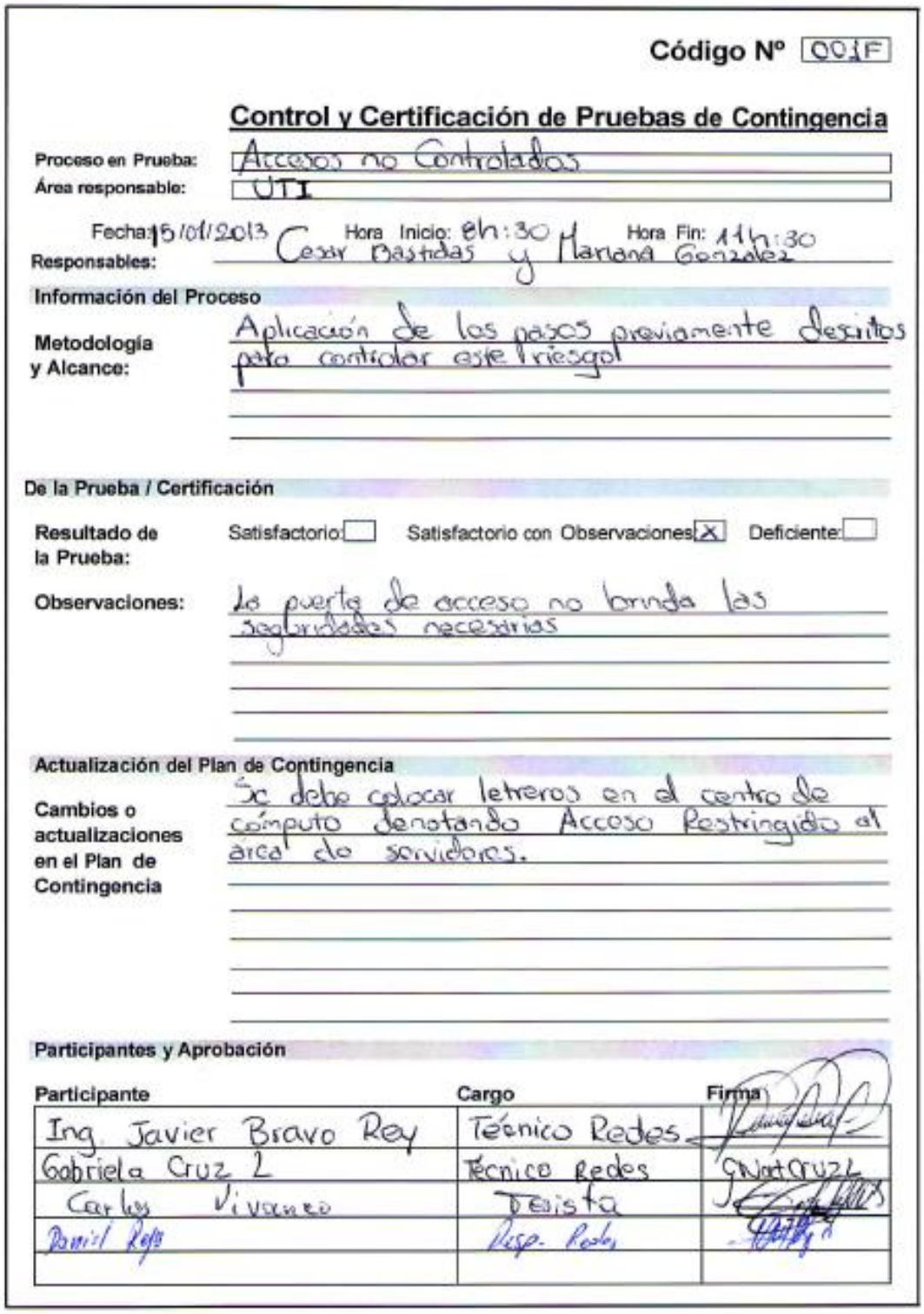
Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma

ANEXO XIII: Certificados del Plan de Contingencia

Físicos



Código Nº 001F

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Accesos no Controlados

Área responsable: UTI

Fecha: 15/01/2013 Hora Inicio: 8h:30 Hora Fin: 11h:30

Responsables: Cesar Bastidas y Mariana Gonzalez

Información del Proceso

Metodología y Alcance: Aplicación de los pasos previamente descritos para controlar este riesgo!

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio ☐ Satisfactorio con Observaciones ☒ Deficiente ☐

Observaciones: La puerta de acceso no brinda las seguridades necesarias

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia: Se debe colocar letreros en el centro de cómputo denotando Acceso Restringido al área de servidores.

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L.	Técnico Redes	
Carlos Vivanco	Teísta	
Daniel Rojo	Resp. Redes	

Código Nº 002F

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Filtraciones de líquidos

Área responsable: UTI

Fecha: 16/04/2013 Hora Inicio: 9h:30 Hora Fin: 18h:00

Responsables: Cesar Bastidas y Mariana Gonzalez

Información del Proceso

Metodología y Alcance: Cumplir con los pasos descritos en este riesgo cuando el daño del edificio ha sido mayor y menor.

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfactorio con Observaciones: ☒ Deficiente: ☐

Observaciones: Tener previamente definido el nuevo local en donde funcionará el centro de cómputo de forma provisional en caso de daños mayores al local.

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GCruzL
Carlos Vivanco	Tesis	
	Resp Redes	

Código Nº 003 F

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Fallas del personal

Área responsable: UTI

Fecha: 17/01/2013 Hora Inicio: 8h:30 Hora Fin: 18h:30

Responsables: Cesar Bautidas y Mariana Gonzales

Información del Proceso

Metodología y Alcance: Controlar el riesgo Fallas del personal cumpliendo los pasos descritos en la planificacion de respuestas a los riesgos del plan de contingencia

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: [X] Satisfactorio con Observaciones: [ ] Deficiente: [ ]

Observaciones:

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	
Carlos Vivanco	Teista	
Daniel Rojas	Resp Redes	

Código Nº 004F

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Fallas del Hardware

Área responsable: UTI

Fecha: 18/01/2013 Hora Inicio: 8h.30 Hora Fin: 17h:30

Responsables: César Bastidas y Mariana Gonzales

Información del Proceso

Metodología y Alcance: Realizar el control del riesgo Fallas del Hardware utilizando los pasos para controlar este riesgo planteados en el plan de mitigación de Riesgos

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfactorio con Observaciones: X Deficiente: ☐

Observaciones: Adquirir un stock de repuestos y equipos necesarios para reemplazar los componentes dañados ya que los procesos de compra son tardados.

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Jaime Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GNatCruz2
Carlos Vivanco	Docente	

Código Nº 0057

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Interrupción Eléctrica

Área responsable: UTI

Fecha: 19/01/2013 Hora Inicio: 8h:30 Hora Fin: 16h:30

Responsables: Cesar Bastidas y Mariana Gonzalez

Información del Proceso

Metodología y Alcance: Analizar las situaciones planteadas para este riesgo

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfactorio con Observaciones: ☒ Deficiente: ☐

Observaciones: No existen las debidas protecciones eléctricas

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GNatCruzL
Carlos Vivanco	Tesista	
Daniel Rojo	Resp Redes	

Código Nº 006F

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Incendios

Área responsable: UTI

Fecha: 20/01/2013 **Hora Inicio:** 8h:30 **Hora Fin:** 12h:00

Responsables: Cesar Bastidas y Mariana Gonzalez

Información del Proceso

Metodología y Alcance: Verificar los pasos para planificar las respuestas a los riesgos para el caso de incendio

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☐ Satisfactorio con Observaciones: ☒ Deficiente: ☐

Observaciones: Se debe colocar en una parte visible los teléfonos de emergencias

No hay extintores ni sistemas contra incendios

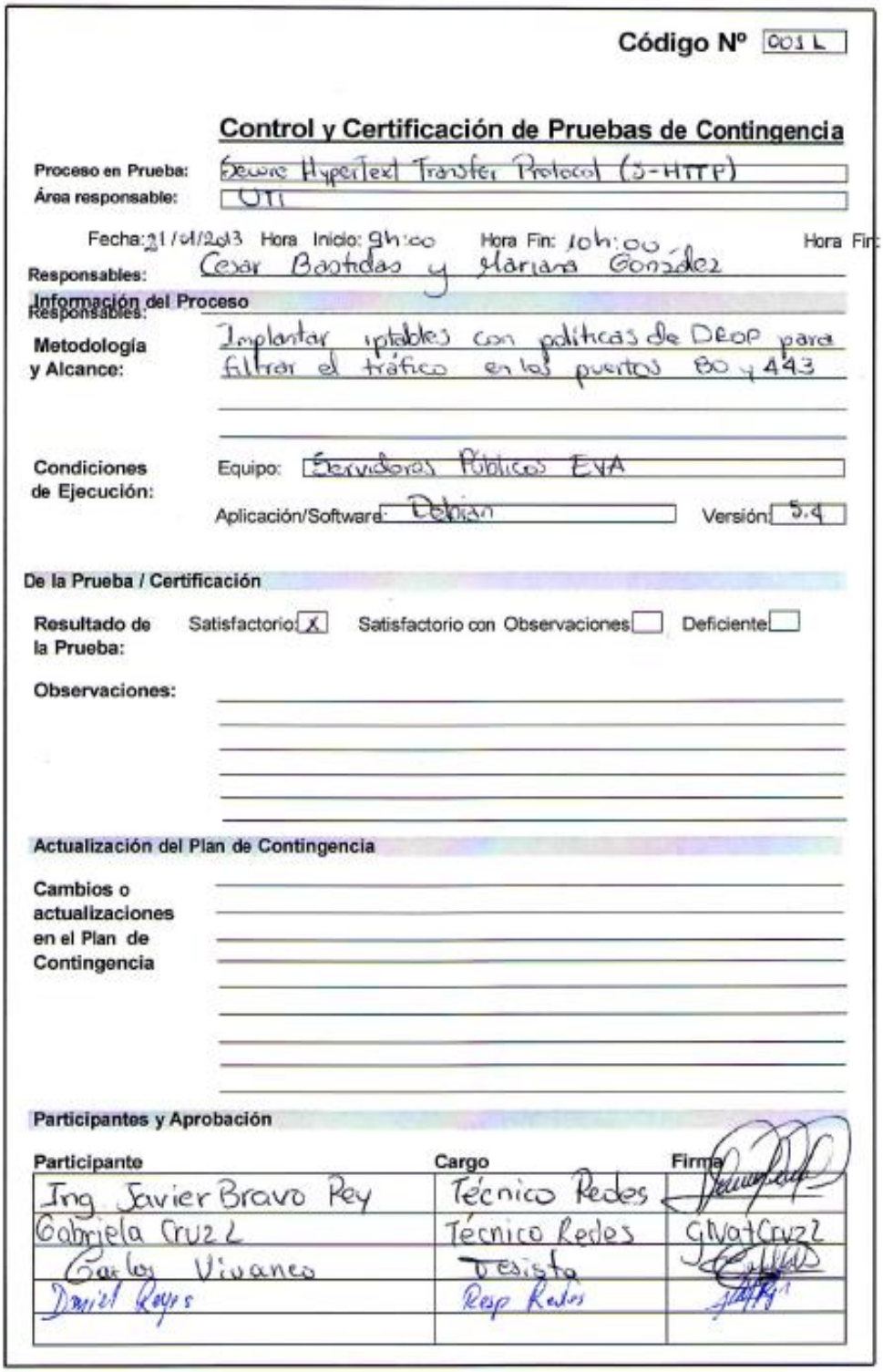
Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Roy	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GNatCruzz
Carlos Vivanco	Tecnico	
Danil [illegible]	Resp Redes	

Lógicas



Código Nº 001 L

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Secure HyperText Transfer Protocol (S-HTTP)

Área responsable: UTI

Fecha: 21/01/2013 Hora Inicio: 9h:00 Hora Fin: 10h:00 Hora Fin:

Responsables: Cesar Bastidas y Mariana González

Información del Proceso

Responsables:

Metodología y Alcance: Implantar iptables con políticas de Drop para filtrar el tráfico en los puertos 80 y 443

Condiciones de Ejecución: Equipo: Servidores Públicos EVA

Aplicación/Software: Debian Versión: 5.4

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: X Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones:

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GCruzL
Carlos Vivanco	Tesista	
Daniel Reyes	Resp Redes	

Código Nº 002

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Web Server Basic Authentication Without HTTPS

Área responsable: UTI

Fecha: 22/04/2013 Hora Inicio: 10h:00 Hora Fin: 11h:30 Hora Fin:

Responsables: Cesar Bastidas y Mariana González

Información del Proceso

Metodología y Alcance: Utilizar políticas de Drop en las iptables e implementarlas en el servidor filtrando los puertos afectados.

Condiciones de Ejecución:

Equipo: Servidores DGA

Aplicación/Software: Debian Versión: 5.0

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio: ☑ Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones:

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	GVatCruzL
Carlos Vivanco	Tesista	
Daniel Reyes	Resp Redes	

Código Nº 003L

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: FTP Supports ClearText Authentication

Área responsable: GTI

Fecha: 23/01/2013 Hora Inicio: 9h:30 Hora Fin: 10h:30 Hora Fin:

Responsables: Cesar Bastidas y Mariana Gonzáles

Información del Proceso

Metodología y Alcance: Filtrar el tráfico en los puertos 21 y 22

Condiciones de Ejecución:

Equipo: Servidor Cursos

Aplicación/Software: Centos Versión: 5.0

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio [X] Satisfactorio con Observaciones [ ] Deficiente [ ]

Observaciones:

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz L	Técnico Redes	
Carlos Vivanco	Tesista	
Javier Rey	Resp Redes	

Código Nº 0042

Control y Certificación de Pruebas de Contingencia

Proceso en Prueba: Web Server Uses Plain Text Authentication Forms

Área responsable: UTI

Fecha: 24/01/2013 Hora Inicio: 09h:00 Hora Fin: 11h:00 Hora Fin:

Responsables: Cesar Bastidas y Mariana Gonzalez

Información del Proceso

Metodología y Alcance: Filtrar Puertos 80 y 443 en el servidor afectado

Condiciones de Ejecución:

Equipo: Servidor Cursos y Energía

Aplicación/Software: Centos Versión: 5.9

De la Prueba / Certificación

Resultado de la Prueba: Satisfactorio [x] Satisfactorio con Observaciones [ ] Deficiente [ ]

Observaciones:

Actualización del Plan de Contingencia

Cambios o actualizaciones en el Plan de Contingencia

Participantes y Aprobación

Participante	Cargo	Firma
Ing. Javier Bravo Rey	Técnico Redes	
Gabriela Cruz 2	Técnico Redes	GCruz2
Carlos Vivanco	Tesista	
David Reyes	Resp Redes	

ANEXO XIV: Modelo de Identificación para la UTI

ANEXO XV: Modelo de Señales para el Centro de Cómputo

Figura 80.Personal Autorizado

Figura 81. Prohibido Alimentos

Figura 82. No Fumar

ANEXO XVI: Control de Pasantes

NOMBRES COMPLETOS	FECHA	TAREA REALIZADA	FIRMA

ANEXO XVII: Formulario para Registrar cambios en los servidores

Registro de Modificaciones para los servidores

Responsable:_____ **IP:**_____

Fecha:_ ……...

Procedimiento

1. _____
2. _____
3. _____
4. _____

Paquetes modificados

_____
_____
_____
_____
_____

Observaciones

_____
_____
_____

Motivo(s) para las modificaciones

_____
_____

_____
Firma del Responsable

ANEXO XVIII: Formulario para la Implementación de un servidor

Registro para la Instalación de servidores

Responsable:_____ **IP:**_____

Fecha:_ ……..

Procedimiento

1. _____
2. _____
3. _____
4. _____

Paquetes Instalados

_____
_____
_____
_____
_____

Observaciones

_____
_____
_____

Requerimientos adicionales

_____
_____

_____
Firma del Responsable

ANEXO XIX: Acta Políticas de Seguridad

Loja, 12 de enero de 2013

A los doce días del mes de Enero del presente año en la Sección de Redes de la Unidad de Telecomunicaciones e Información se procedió a realizar conjuntamente con los técnicos de la unidad, las políticas de seguridad para los servidores de la UTI con la presencia del responsable de la unidad Tngo. Daniel Reyes, los técnicos Ing. Jaime Bravo, Tngo. Gabriela Cruz y los tesistas Egdo. Cesar Bastidas y Egda. Mariana González

Luego de debatir cada una de las políticas propuestas por los tesistas se procedió a realizar las observaciones pertinentes quedando plasmadas en un documento que se lo ha socializado al interior de la unidad

Para constancia del acta firman los participantes.

Tngo. Daniel Reyes

Ing. Jaime Bravo

Tngo. Gabriela Cruz

Egdo. Cesar Bastidas

Egda. Mariana González