UNIVERSIDAD
NACIONAL
DE LOJA

PFC-CIS

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables"

Tesis previa a la obtención del título de Ingeniero en Sistemas.

Autor:

Henry David Quishpe Malla

Director:

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

LOJA-ECUADOR
2016

Certificación del Director

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

DOCENTE DE LA UNIVERSIDAD NACIONAL DE LOJA, DEL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES, DE LA CARRERA DE INGENIERÍA EN SISTEMAS.

CERTIFICO:

Que el proyecto de tesis titulado **ANÁLISIS DE VULNERABILIDADES EN LA RED LAN JERÁRQUICA DE LA UNIVERSIDAD NACIONAL DE LOJA, EN EL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES,** presentado por el estudiante Henry David Quishpe Malla, para optar el título de Ingeniería en Sistemas, ha sido dirigido, orientado y debidamente revisado, por lo que autorizo su presentación y sustentación.

Loja, 27 julio de 2015

Atentamente,

Ing. Carlos Miguel Jaramillo Castro

DIRECTOR DE TESIS

Autoría

Yo **Henry David Quishpe Malla** declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.
Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de la siguiente tesis en el repositorio institucional – Biblioteca Virtual.

Firma:

Cedula: 1104811920
Fecha: 18-08-2016

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **HENRY DAVID QUISHPE MALLA,** declaro ser autor de la tesis titulada: **ANÁLISIS DE VULNERABILIDADES EN LA RED LAN JERÁRQUICA DE LA UNIVERSIDAD NACIONAL DE LOJA, EN EL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES,** como requisito para optar el grado de: **INGENIERO EN SISTEMAS;** autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios puedan consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dieciocho días del mes de agosto de dos mil dieciséis.

Firma:

Autor: Henry David Quishpe Malla

Cedula: 1104811920

Dirección: Loja, (Zamora Huayco, Rio Curaray y Rio Napo)

Correo Electrónico: hdquishpem@unl.edu.ec

Teléfono: (07) 2 139477 **Celular:** 0980092072

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
Ing. Mario Enrique Cueva Hidalgo, Mg. Sc.
Ing. Gastón Rene Chamba Romero Mg. Sc.

Agradecimiento

Agradezco a mi padre Fernando Quishpe por apoyarme incondicionalmente en todos los años de estudio, por sus sabios consejos para superar cualquier obstáculo en la vida y por enseñarme a nunca rendirme.

A mi madre Rosa Malla por brindarme su conocimiento, por estar siempre conmigo, guiándome y enseñándome a dar siempre lo mejor de mí.

A mis hermanos por el apoyo que me brindaron cuando necesité de ellos para la culminación de mis estudios universitarios.

A mi Director y Docentes de la carrera por su ayuda brindada para la culminación de este trabajo de titulación.

A todo el personal de la Unidad de Telecomunicaciones e Información por colaboración en todo lo que estuvo a su alcance.

Y finalmente a mis amigos y compañeros con los cuales compartimos muchos momentos tanto dentro como fuera de las aulas.

Dedicatoria

Dedico especialmente este trabajo de titulación a mis padres que siempre estuvieron apoyándome incondicionalmente y por haberme enseñado los valores de la vida para aplicarlos durante mi fase de estudios.

También a mis hermanos y amigos que siempre estuvieron para darme una mano sin importar el momento.

A mi tutor de tesis y docentes por haberme impartido sus conocimientos en las aulas y por ser parte de mi formación tanto académica como formal.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

a. Título

“Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables”

b. Resumen

El presente trabajo de titulación se enfoca al análisis de vulnerabilidades en la red LAN Jerárquica de la Universidad Nacional de Loja, específicamente en el Área de la Energía, donde se realizan evaluaciones en los equipos críticos de la Red LAN, con el objetivo de identificar vulnerabilidades que los pongan en riesgo.

Se realiza una investigación de las herramientas que son especializadas en el análisis de vulnerabilidades, con el fin de poder realizar un cuadro comparativo y seleccionar las herramientas más idóneas para este proyecto, donde se ve que sean de licencia libre, permita la obtención de reportes, por el tiempo de análisis, por las soluciones que plantean a cada vulnerabilidad encontrada en los equipos y lo más importante la sustentación científica con la que cuentan, el cual es el punto más relevante al momento de elegir la herramienta a utilizar. Se comparan herramientas para realizar el descubrimiento de Red y herramientas para escanear vulnerabilidades.

Además se efectúa un descubrimiento de Red con el objetivo de identificar a todos los equipos conectados a la red, que posteriormente van hacer escaneados para determinar si están siendo vulnerables, además con el descubrimiento de red se realiza un inventario de los equipos encontrados, se presenta un direccionamiento IP y se realiza una topología de la Red LAN del Área de Energía.

Finalmente se utilizan las herramientas Nessus y OpenVas en los equipos considerados críticos en la Red, con el fin de encontrar vulnerabilidades que los puedan poner en riesgo, se realiza una breve descripción de las vulnerabilidades más graves encontradas en los equipos, donde se especifica el impacto que pueden producir cuando un atacante aprovecha una vulnerabilidad y además se indica al puerto que pertenece cada vulnerabilidad hallada. Una vez obtenidos los resultados de ambas herramientas se genera un plan de mitigación de riesgos, en donde se da prioridad a los riesgos más graves. El objetivo del plan de mitigación es recomendar acciones que se pueden realizar en los equipos y en algunos casos indicar el procedimiento que se debe llevar para reducir o eliminar las vulnerabilidades.

Summary

This qualification research paper is focused on analysis of vulnerabilities in the hierarchical LAN network of the National University of Loja, specifically in the area of energy, where different types of scan are performed in some active devices on the LAN, with the aim of identifying vulnerabilities that endanger teams.

A research of the tools that are specialized in the analysis of vulnerabilities, in order to carry out a comparative table and select the most appropriate tools for this project, showing that they are license-free, allows gathering reports, by the time of analysis and solutions posed to each vulnerability found in computers. Tools are compared for the discovery of tools for scanning and network vulnerabilities.

In addition occurs a network discovery with the objective of identifying all the equipment connected to the network, which will later make scanned to determine if they are still vulnerable, with the discovery of network is performed an inventory of found computers, is an IP addressing and is a topology of the LAN network in the Area of energy.

Finally used the tool, Nessus and OpenVas equipment identified on the network, in order to find vulnerabilities that may put at risk the teams, is a brief description of the most serious vulnerabilities were found on computers, which specifies the impact that may occur when an attacker exploits a vulnerability and additionally indicated on the port that belongs to each vulnerability found. Once the results of both tools develops a plan of risk mitigation, where priority is given to the most serious risks. The objective of the mitigation plan is to recommend actions that can be performed on computers and in some cases indicate the procedure that should be to reduce or eliminate vulnerabilities.

c. Introducción

En la actualidad la Red LAN de la Universidad ha ido incrementando su infraestructura tanto física como lógica, con el fin de brindar un mejor acceso a internet a sus usuarios, pero no todo es transparente y seguro, ya que debido al avance de las tecnologías ha incitado a personas mal intencionadas a buscar nuevos métodos o formas más fáciles para explotar vulnerabilidades que finalmente se podrían convertir en riesgos potenciales para la institución.

La falta de medidas de seguridad en las redes es un problema que está creciendo considerablemente, debido a que existen un mayor número de atacantes y también al descuido por parte de sus administradores, por lo cual se pone en peligro la integridad y confidencialidad de la información de la institución, la misma puede quedar expuesta a usuarios no autorizados o a la modificación por parte de un especialista.

Los usuarios de una institución actualmente son considerados el eslabón más débil, debido a que estos navegan por internet, sin saber que pueden ser víctimas de ataques originados por malware, hackers o personas curiosas, subestimando el impacto que puede ocasionar un riesgo de nivel alto.

Los ataques suelen provenir en la mayor parte de la red interna que externa, donde pretenden acceder legítimamente a los sistemas informáticos ya sean para modificar, eliminar o sustraer la información y afectar el funcionamiento de los servicios, es por ello que los administradores deben conocer el comportamiento normal de tráfico de la red, hacer uso de herramientas que los ayuden a la detección de intrusos y posibles ataques para poder tomar las medidas pertinentes.

OBJETIVOS

Objetivo General

Detectar las vulnerabilidades en la Red LAN Jerárquica del AEIRNNR de la Universidad Nacional de Loja mediante el uso de diferentes herramientas de software libre”

Objetivos Específicos

- Analizar las diferentes herramientas de software libre para la detección de vulnerabilidades en una red LAN.
- Implementar las diferentes herramientas tecnologías para la detección de vulnerabilidades en la red LAN Jerárquica de la Universidad Nacional de Loja.
- Elaboración de plan de mitigación para reducir la probabilidad de que un riesgo se materialice.

La estructura del proyecto consta de 3 fases donde;

La primera fase se refiere a la investigación de las diferentes herramientas para realizar un descubrimiento de Red y escaneo de vulnerabilidades en los equipos del Área de Energía de la Universidad Nacional de Loja y además se realizan cuadros de comparación de las herramientas para poder elegir las herramientas más adecuadas, las cuales van a ser utilizadas en los equipos.

La segunda fase abarca varios puntos:

El primer punto se refiere al descubrimiento de la red del Área, donde se hace uso de NMAP para identificar los equipos, para ello se realiza el descubrimiento de equipos de acuerdo a las VLAN existentes.

En el segundo punto se realiza un inventario de los equipos encontrados en cada VLAN, con el fin de tener el conocimiento aproximado de cuantos equipos existen en el área.

En el tercer punto se presenta el direccionamiento IP de las Red LAN del Área de Energía y la topología de la Red.

En el cuarto punto es el más importante de esta fase, ya que se realiza el escaneo de vulnerabilidades en los equipos de la Red LAN del Área de Energía, el escaneo se lo va elaborando de acuerdo al descubrimiento de Red, las VLAN que se escanean son: la que se utiliza para los Switch y Access Point Cisco, para Telefonía, Impresoras y Relojes Biométricos, Cámaras IP y para los Access Point Multimarca. Se presentan los resultados obtenidos de los equipos, donde se describen las vulnerabilidades lógicas encontradas, enfatizando el impacto que pueden llegar a ocasionar y el puerto a la que pertenecen.

En el último punto de esta fase se comparan los resultados obtenidos por las herramientas OpenVas y Nessus en los equipos de cada VLAN, donde se puede comprobar que en algunos resultados concuerdan y en otros se complementan entre sí.

En la fase final (3) se plantea un plan de mitigación de riesgos, aquí se explica el tratamiento que se le debe dar al riesgo, indicando cuales son las acciones que se deben tomar frente a ellos, con el fin reducir el impacto que podrían llegar a ocasionar en caso que se efectúen. Este plan consiste en Recomendaciones y procedimientos que permitan tener una hoja de ruta para la revisión de los riesgos y posterior seguimiento.

d. Revisión de Literatura

1. Seguridad

1.1. Definición

Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

La Seguridad es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. [1]

La Seguridad es el estado de un sistema, el cual indica si está propenso a daños o riesgos.

1.2. Propiedades de la Seguridad

- **Confidencialidad.** Consiste en mantener la información fuera del alcance de usuarios no autorizados.
- **Integridad.** La información solo puede ser modificada por quien está autorizado.
- **Disponibilidad.** Se refiere a la disposición de los servicios a ser usados cuando sea necesario.

1.3. Leyes de Seguridad

- No existen sistemas seguros.
- Para mitigar las vulnerabilidades se tiene que doblar el gasto en seguridad.
- Los intrusos brincan la criptografía, no la rompen.

1.4. Seguridad Física

1.4.1. Definición

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto del mismo; implementados para proteger el hardware y medios de almacenamiento de datos. [2].

Se llama seguridad física a la que tiene que ver con la protección de los elementos físicos de la empresa u organización, como el hardware y el lugar donde se realizan las actividades. [1]

1.4.2. Amenazas a la Seguridad Física

Las principales amenazas que se pronostican en la seguridad física son:

TABLA I

PRINCIPALES AMENAZAS EN LA SEGURIDAD FÍSICA

Amenazas	Descripción
Incendios	Son ocasionados por uso incorrecto de combustibles, fallas de instalaciones eléctricas y un inoportuno almacenamiento y traslado de sustancias peligrosas.
Inundaciones	Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos.
Terremotos	Son fenómenos físicos sísmicos, los cuales pueden ser poco intensos o tan intensos que causan la destrucción de edificios.
Cableado	Los riesgos más comunes para el cableado son el de interferencia, esto se da en cables metálicos. Además el corte de cable impide el flujo de datos y también el daño de cables, que ocasionan que la comunicación no sea tan fiable.
	Las computadoras y servidores son activos valiosos para la empresa y no

Robo	deben estar expuestos. La información importante y confidencial puede ser fácilmente copiada.
Fraude	Millones de dólares son sustraídos de las empresas y en la mayor ocasión las computadoras son utilizadas para dichos fines.
Sabotaje	Puede ser producido por un empleado o persona ajena a la empresa. Las acciones más comunes son la destrucción de hardware e ingreso de datos erróneos.
Acceso físico	El control de acceso no sólo pretende la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas.
Espionaje	Es la acción de la recolección de información de una empresa para ayudar a otra empresa.

1.5. Seguridad Lógica

1.5.1. Definición

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. [2]

Es toda aquella relacionada con la protección del software y de los sistemas operativos, que en definitiva es la protección directa de los datos y de la información. [1]

La seguridad lógica involucra todas aquellas medidas establecidas por la administración-usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. [3]

Los objetivos que la seguridad lógica debe cumplir son los siguientes:

- Restringir el acceso a los programas y archivos
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan
- Asegurar que se estén utilizando los datos, archivos y programas correctos y por el procedimiento correcto
- Que la información transmitida sea recibida solo por el destinario al cual ha sido enviada y no a otro.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la trasmisión de información. [3]

1.5.2. Amenazas en la Seguridad Lógica

Las principales amenazas que se prevén en la seguridad lógica son:

TABLA II

AMENAZAS EN LA SEGURIDAD LÓGICA

Amenazas	Descripción
Virus	Es un segmento de código el cual ralentiza o bloque un ordenador. Además destruye la información en el disco, pudiendo llegar a ser casos vitales para el funcionamiento del sistema.
Gusanos	Se basan en diversos métodos como SMTP, IRC, P2P, entre otros, para propagarse por la red de datos, es decir a otras terminales en red y son capaces de

	llevar esto a cabo sin intervención del usuario.
Malware	Es un tipo de software que tiene como objetivo infiltrarse, dañar una computadora o un sistema de información. [4]- [5]
Sniffing	Es una aplicación utilizada para el monitoreo y análisis del tráfico en la red. Además permite capturar el tráfico y examinarlo.
Denegación de Servicio (DoS)	Es una acción iniciada por un sujeto que busca saturar algún tipo de recurso, ya sea hardware, software o ambos dentro de un determinado sistema. [6]
Man-in-the-middle	Consiste en conseguir la capacidad de leer, insertar y modificar los mensajes o paquetes entre dos víctimas, sin el descubrimiento de que su enlace ha sido interceptado. Denominado también hombre en el medio.
Phishing	Este término hace alusión al intento de hacer que los usuarios muerdan el anzuelo, con el fin de obtener contraseñas o información detallada sobre tarjetas de crédito, mediante el uso de un tipo de ingeniería social.

Ingeniería Social	Es una técnica para la obtención de información confidencial mediante la manipulación de usuarios legítimos. Además de la obtención de información también es utilizado para tener acceso a sistemas de información.
Software Incorrecto	Se refiere a errores cometidos de forma involuntaria por los programadores, a estos errores se los denomina bugs. Son aprovechados por los atacantes para atacar al sistema.
Troyanos	Es un software malicioso que tiene una apariencia inofensiva pero al momento de ejecutarlo le brida un acceso remoto al atacante.
Shoulder Surfing	Consiste en el espió físico a los usuarios para la obtención de claves de acceso al sistema.
Exploits	Son programas que aprovechan una vulnerabilidad del sistema para poder atacar.
Spyware	Son programas espía para la recopilación de información de una persona u organización.
Spam	Recepción de mensajes no solicitados, suelen ser utilizados en los correos electrónicos.

2. Amenazas

2.1. Definición

Es la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. [1]

Es una posibilidad de ocurrencia de un evento que pueden ocasionar daños o alteraciones en los sistemas.

2.2. Tipos de Amenazas

Existen diferentes tipos de amenazas de las que hay que proteger los sistemas como:

2.2.1. De interrupción.

Deshabilitar el acceso a la información, es decir se corta el flujo desde emisor al receptor. Se destruye el elemento del sistema o se hace inaccesible o inútil.

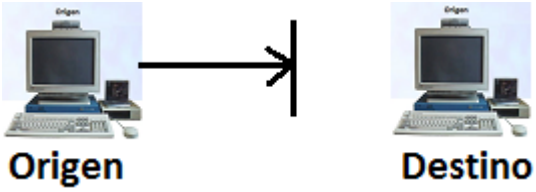


Figura 1. Interrupción.

En este tipo de amenaza se encuentras las siguientes:

- Denegación de Servicio
- Corte de línea de comunicación
- Borrado de programas
- Fallos en el Sistema Operativo.
- Virus
- Troyanos
- Malware

2.2.2. De interceptación

Acceso de Personas, programas o equipos no autorizados a la red.

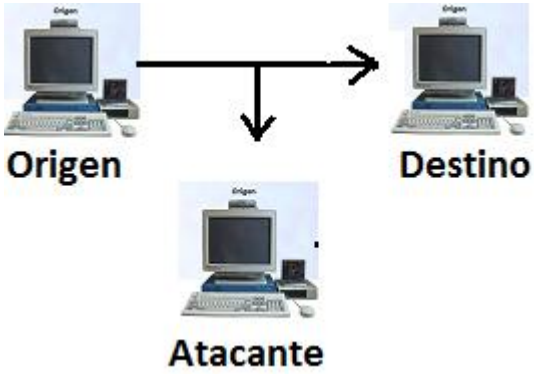


Figura 2. Interceptación

En este tipo de amenaza se encuentras las siguientes:

- Sniffing
- Ingeniería Social
- Virus
- Spyware
- Exploits

2.2.3. De Modificación.

Acceso y alteración de la información por parte de terceras personas no autorizadas.

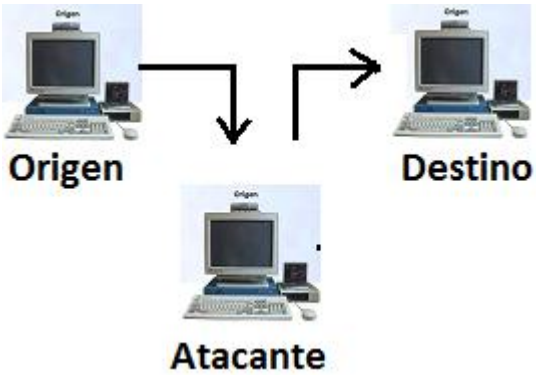


Figura 3. Modificación

En este tipo de amenaza se encuentras las siguientes:

- Exploits
- Virus
- Troyanos
- Man-in-the-middle

2.3. Factor Humano

Se considera a las personas como la principal fuente de amenaza que existen en los sistemas de información y son el tipo de amenaza en el que se intervienen más recursos para controlarlos y mitigarlos.

La mayoría de los robos, sabotaje o accidentes relacionados con los sistemas informáticos son causados por el propio personal de la empresa.

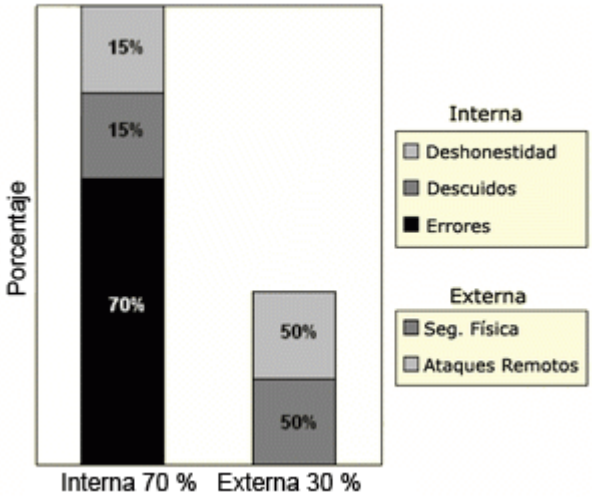


Figura 4. Ataques internos y externos

Fuente: *http://www.cybsec.com*

Es preocupante, ya que cualquier persona que sea encargado de un maquina o un mismo programador conoce perfectamente el sistema, es decir sus puntos fuertes y débiles. El ataque por este tipos de personas es más directo, difícil de detectar y más efectivo que el de un atacante externo.

2.3.1. Personas en la ciberseguridad

La popularidad de las redes sociales y otros sitios muy visitados han dado a los hackers nuevas vías para robar dinero e información.

Cerca de la mitad de las compañías bloquea parcial o completamente el acceso a las redes sociales debido a la preocupación por Cyber-incursiones a través de esos sitios. Esto ocurre a pesar de años de exhortaciones a los usuarios de computadoras, respecto a que, debería mantener su información personal en privado y abstenerse de abrir archivos adjuntos de correos electrónicos provenientes de fuentes no conocidas.

La cuarta parte de los negocios han sido afectados por tácticas como el spam, el phishing o ataques maliciosos a través de twitter u otras redes sociales.

La empresa Sophos descubrió que la cantidad de páginas web con software malicioso se cuadruplico desde principios del 2008, y un 39,6 por ciento de ellas tiene sede en Estados Unidos, que alberga más que cualquier otro país. China es el segundo, con 14,7 por ciento. [8]

Pese a que las empresas de seguridad informática se benefician con un gasto récord en tecnologías para evitar ataques pirata, las personas terminan siendo el eslabón más débil en dichos ataques, según Dmitri Alperovitch, director de tecnología en CrowdStrik, una firma de ciberseguridad en Irvine, California.

“No se apunta a la vulnerabilidad de la computadora –se apunta a la vulnerabilidad de los humanos”, estimó Alperovitch.

2.3.2. Personal atacante

Existen varios motivos que llevan a una persona a cometer delitos informáticos o ataques contra la organización, pero sin importar los que sean o quien los realice, estos se deben prevenir y evitar.

- **Personal Interno.** Las amenazas provienen del propio personal del sistema informático, es por eso que es difícil identificar, ya que no toman en cuenta que el ataque sea producido desde el mismo personal. Generalmente los ataques son accidentales ya sea por desconocimiento o inexistencia de las normas

básicas de seguridad. Pero no siempre son accidentales, a veces pueden ser de tipo intencional.

- **Ex-Empleados.** Este tipo de atacantes burlan la seguridad de la empresa, por inconformidad de su despido o bien porque han renunciado para pasar a trabajar en la competencia. Por lo general se trata de personas descontentas con la empresa, que conocen a la perfección la estructura de los sistemas, es decir los puntos débiles, para así poder atacar y causar daño.
- **Curiosos.** Son considerados los atacantes más frecuentes del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero que no cuentan con los conocimientos ni experiencia básica para ser considerados hackers o crackers. Este tipo de persona en la mayoría son estudiantes que intentan penetrar los servidores de una empresa, sus daños no llegan a ser tan graves pero afectan a la fiabilidad y confiabilidad de un sistema.
- **Terroristas.** Son las personas que atacan al sistema con el objetivo de causar daño de cualquier índole, por lo general lo hacen para modificar la información de la empresa, como sus servidores, base de datos, etc.
- **Intrusos Remunerados.** Son los atacantes más peligrosos, aunque son los menos habituales. Se trata de crackers con grandes conocimientos y experiencia, los cuales son pagados por terceras personas para robar información confidencial como código fuente de programas, base de datos de clientes, diseño de un nuevo producto, etc. Suele darse, solo, en grandes empresas donde la competencia es la principal amenaza.

3. Impacto

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas. [1]

Se habla de un ataque cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Se habla de un impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información.

La metodología MAGERIT estima el impacto de la siguiente manera:

TABLA III

ESCALA CUALITATIVA DEL IMPACTO

Impacto
3: Alto
2: Medio
1: Bajo

4. Probabilidad

Es la posibilidad que existe de que una ocurrencia pase, de acuerdo a un escenario determinado.

Posibilidad de que un hecho se produzca. [UNE-ISO Guía 73:2010]

En la terminología de la gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática [tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado]. [9]

La metodología MAGERIT estima a la probabilidad de la siguiente manera:

TABLA IV

ESCALA CUALITATIVA DE LA PROBABILIDAD

Probabilidad
3: Alta
2: Media
1: Baja

5. Análisis de Riesgos

Es un proceso sistemático, el cual sirve para estimar la magnitud de los riesgos a que está expuesta una Organización.

5.1. Riesgo

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. [9]

EL riesgo revela lo que podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de intereses en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema. [9]

La Metodología MAGERIT estima al riesgo de la siguiente manera:

TABLA V

ESCALA CUALITATIVA DEL RIESGO

Riesgo
6 y 9: Alto
3 y 4: Medio
1 y 2 : Bajo

5.2. Calculo del Riesgo

Para determinar el riesgo que existe en los activos, se debe combinar el impacto que tiene y la probabilidad de ocurrencia de cada amenaza identificada. En el siguiente cuadro se presenta la escala general para la determinación del riesgo dependiendo de la amenaza que se estime:

TABLA VI

MATRIZ DE RIESGOS

Riesgo		**Probabilidad**		
		1	**2**	**3**
Impacto	**3**	3	6	9
	2	2	4	6
	1	1	2	3

5.3. Tratamiento del Riesgo

Es el proceso destinado a modificar el riesgo, es decir reducir las posibilidades de que ocurra.

Hay múltiples formas de tratar a un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización, o, en última instancia, aceptando que pudiera ocurrir y previniendo recursos para actuar cuando sea necesario.

5.4. Salvaguardias

Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal. [9]

5.4.1. Selección de salvaguardas

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica
- Dimensión o dimensiones de seguridad que requieren protección
- Amenazas de las que necesitamos protegernos
- Si existen salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica.** Se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración.
- **No se justifica.** Se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

5.4.2. Efecto de las salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

- **Reduciendo la probabilidad de las amenazas.** Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.
- **Limitando el daño causado.** Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance.

6. Vulnerabilidad

6.1. Definición

Es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo. [5]

Es una debilidad de un sistema informático, el cual es aprovechado por atacantes para violar la seguridad, y así causar daños a la red.

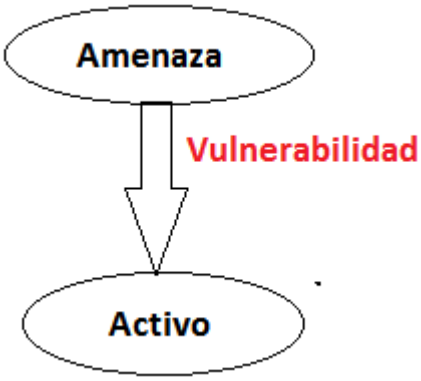


Figura 5. Definición de Vulnerabilidad

6.2. Vulnerabilidad en las redes

Sin importar cuan buenos sean el software, el hardware, procesos y el personal, las vulnerabilidades siempre están presentes en una red de datos, es por ellos que los administradores deben implementar una estrategia, la cual permita eliminar los factores que aumente el riesgo y además incorporar controles para reducir las amenazas.

Para mitigar las vulnerabilidades hay que enfrentarlas con varias mediadas de defensas, lo cual nos proporciona ventajas como:

- La Dificultad en el éxito de ataques, es decir al hacker le resultará más difícil burlar la seguridad y existen más posibilidades de detectar los ataques.
- Ayuda a mitigar el efecto de las nuevas vulnerabilidades en los activos.

6.3. Vulnerabilidades en capas de modelo TCP/IP

En cada capa del modelo TCP/IP pueden existir distintas vulnerabilidades y un atacante puede explotar los protocolos asociados a cada una de ellas. [6]

Cada día se revelan nuevas debilidades en las capas del modelo TCP/IP, las mismas que son descubiertas por organismos internacionales. A continuación se presenta algunas de las vulnerabilidades más comunes en las 4 capas.

6.3.1. Capa de Acceso

Esta capa presenta problemas de control de acceso y de confidencialidad. Son ejemplos de vulnerabilidades a este nivel los ataques a las líneas punto a punto como el desvió de los cables de conexión hacia otros sistemas, interceptación intrusiva de las comunicaciones, escuchar no intrusivas en medios de transmisión sin cables, etc.

6.3.2. Capa de Red

En esta capa se puede realizar cualquier ataque que afecte un datagrama IP. Se incluyen como ataques contra esta capa las técnicas de sniffing, la suplantación de mensajes, la modificación de datos, los retrasos y denegación de servicio.

La suplantación de un mensaje se puede realizar, por ejemplo: En esta capa, la autenticación de los paquetes se realiza a nivel de máquina (por dirección IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el receptor no detectara la suplantación. Para conseguir su objetivo, este tipo de ataques suele utilizar otras técnicas, como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc. [7]

6.3.3. Capa de Transporte

En esta capa se encuentra problemas de autenticación, de integridad y de confidencialidad. Los ataques más conocidos son las denegaciones de servicio (DoS).

6.3.4. Capa de Aplicación

Esta capa presenta varias deficiencias de seguridad asociadas a sus protocolos. Las más conocidas son las siguientes:

Servicio de nombres de dominio (DNS)

Cuando el DNS se ve comprometido, pueden suceder varias cosas. Sin embargo, los servidores DNS comprometidos son a menudo utilizados por los atacantes de una de dos maneras. Lo primero que un atacante puede hacer es redirigir todo el tráfico entrante a un servidor de su elección. Esto les permite lanzar ataques adicionales, o recoger los registros de tráfico que contienen información sensible. La segunda cosa que puede hacer un atacante es capturar todo el correo electrónico. Más importante aún, esta segunda opción también permite al atacante enviar correo en su nombre, con el dominio

de la organización víctima y persiguiendo su propia reputación. Para empeorar las cosas, los atacantes también podrían optar por una tercera opción, que es hacer ambas cosas.

Los tipos ataques más utilizados para dañar el DNS son:

- **Envenenamiento de caché**. Esto puede suceder después de que un atacante tiene éxito en la inyección de datos DNS maliciosos en los servidores DNS recursivos que son operados por los ISP.
- **DNS autoritarios para un dominio.** El hosting de DNS autoritario es del tipo de servicio que su empresa le proporciona a Twitter. Si un atacante comprometiera un DNS autoritario, el efecto sería global.
- **Registro del dominio.** Este tipo de ataque consisten en comprometer el registro del dominio, para poder acceder y así modificar los servidores DNS asignados al mismo. [12]

Telnet

Se puede utilizar este protocolo para acceder de manera remota aun activo para cambiar su configuración. Los tipos de ataques son:

- **Denegación de servicio.** El atacante explota un defecto del software del servidor Telnet que se ejecuta en el switch, el cual hace que el servicio de Telnet no esté disponible. En general, las vulnerabilidades en el servicio de Telnet que permiten que ocurran los ataques de DoS se enfrentan mediante parches de seguridad incluidos en las revisiones más recientes de IOS de Cisco.
- **Contraseña de fuerza bruta.** Empieza con el uso de contraseñas comunes por parte del atacante y de un programa diseñado para intentar establecer una sesión de Telnet mediante todas las palabras del diccionario.

File Tranfer Protocol (FTP)

Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo. Los ataques más comunes a este protocolo son:

- Ataque de fuerza bruta
- Sniffing

Hypertext Transfer Protocol (HTTP)

Los ataques más comunes al protocolo http son:

- Denegación de servicio
- Cross-site scripting (XSS)
- Ataque por fuerza bruta
- Phishing

6.4. Evaluación de Vulnerabilidades (Vulnerability Assessment)

Se refiere a la búsqueda de vulnerabilidades en distintos tipos de sistemas. Se busca determinar las amenazas, los agentes de amenaza y las vulnerabilidades a los que está expuesto el sistema en su conjunto. Estas debilidades suelen referirse a todas aquellas de carácter técnico que dependen de las cualidades intrínsecas del sistema que se esté evaluando.

Se tomará el concepto de Vulnerability Assessment cuando se refiera a un análisis técnico sobre las debilidades de una infraestructura informática y de telecomunicaciones. Puntualmente, se analizaran vulnerabilidades asociadas a distintos servidores, dispositivos, sistemas operativos, aplicaciones y un largo etcétera vinculando a todas las deficiencias técnicas posibles. Es importante destacar que este tipo de evaluaciones solo identifica potenciales vulnerabilidades, pero no confirma que estas existan, es decir, cuando se detecta una vulnerabilidad en un equipo o sistema, no se trata de explotarla para confirmar su existencia, sino, simplemente, se la reporta.

Por lo general, las diferentes normativas exigen efectuar determinada cantidad de evaluaciones de vulnerabilidades en forma anual. Por ejemplo, PCI-DSS requiere cuatro evaluaciones al año.

Requisitos de las PCI DSS	Procedimientos de prueba	Implemented	No implemented	Fecha objetivo y comentarios
11.2 Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos). ***Nota:*** *no se requiere que se completen cuatro análisis trimestrales aprobados para el cumplimiento inicial de PCI DSS si el asesor verifica que 1) el resultado del último análisis fue un análisis aprobado, 2) la entidad ha documentado políticas y procedimientos que exigen análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En el caso de los años siguientes a la revisión inicial de las PCI DSS, deben obtenerse cuatro análisis aprobados.*	**11.2** Verifique que se realicen análisis de vulnerabilidad externa e interna de la manera siguiente:			
11.2.1 Realice análisis de vulnerabilidad interna trimestralmente.	**11.2.1.a** Revise los informes de los análisis y verifique que se hayan realizado cuatro análisis internos trimestrales durante el período de 12 meses más reciente.			

Figura 6. Extracto del Requerimiento 11 del PCI-DS, donde se pide evaluar vulnerabilidades trimestralmente

7. Activos

7.1. Definición

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa y la consecución de sus objetivos. [1]

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008].

En un sistema de información hay 2 cosas esenciales:

- **La Información** que se maneja y
- **Los Servicios** que se presta.

7.2. Tipos de Activos

Podemos clasificarlos en los siguientes tipos:

- **Datos.** Constituyen el núcleo de toda organización.
- **Software.** Constituido por los sistemas operativos y aplicaciones instaladas en los equipos de un sistema de información.
- **Hardware.** Se trata de los servidores y terminales que contiene las aplicaciones y permiten su funcionamiento. También se incluye los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vías de transmisión de los datos.
- **Redes.** Implica la Red LAN e Internet.
- **Soportes.** Son los lugares donde la información queda registrada y almacenada durante largos tiempos o de forma permanente.
- **Personal.** El conjunto de personas que interactúan con el sistema de información, como administrativos, programadores, usuarios internos y externos y resto del personal de la empresa.
- **Servicios.** Son aquellos que ofrece la institución a sus clientes o usuarios, como productos, sitios web, foros, correo electrónico y otros servicios de comunicaciones, seguridad, etc.

8. Ataques

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. [1]

8.1. Tipos de Ataques

- **Activos.** Consiste en bloquear o saturar los canales de comunicación y modificar la información, causando daños graves.
- **Pasivos.** Cuando existe acceso sin autorización a los datos, son los más difíciles de detectar.

8.2. Métodos comúnmente utilizados por atacantes

Los delitos informáticos siempre tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos. [4]

Los métodos de delitos informáticos reconocidos por Naciones Unidas son:

8.2.1. Ataques al sistema operativo

Los ataques al SO constituyen un punto clásico de la seguridad. Desde esta perspectiva, la búsqueda de fallas se la realiza en lo concerniente al propio sistema base de todo el software de tal modo que, muchas veces, independientemente de lo que se encuentre por encima, se podrá explotar y tomar control del sistema en caso de que sea vulnerable.

En la actualidad se tiene 3 líneas principales: los sistemas de tipo Windows, Linux y MAC OSX, los cuales, si bien están basados en UNIX, a esta altura presentan entidad propia. En el caso de los primeros, desde su origen fueron objeto de ataque dad su masificación y la relativa simplicidad con que se pudo acceder históricamente al núcleo del sistema, incluso, sin contar con su código fuente.

Para el caso de Linux la situación es quizá peor, ya que, al poseer el código fuente, es posible detectar problemas también a nivel de código. Y en cuanto a OSX, los controles de seguridad implementados no son suficientes frente a las amenazas actuales, hacen que el SO de MAC sea un blanco cada vez más buscado por los atacantes. [14]

8.2.2. Ataques por reconocimiento

Se refiere a la fase de preparación, en donde el atacante logra obtener información de su objetivo, antes de lanzar un ataque.

8.2.3. Ataques de acceso

Es cuando el atacante accede a un dispositivo para el cual no tiene o cuenta con una contraseña, esto se logra explotando las vulnerabilidades conocidas del sistema o aplicación atacada con herramientas adecuadas.

8.2.4. Ataques a las aplicaciones

Existen miles y miles de piezas de software y programas de todo tipo y tamaño, disponibles en el mundo. Por supuesto, entre tantos millones de líneas de código, necesariamente se producen errores. Para los ataques a las aplicaciones también se debe tomar en cuenta la masividad de uso.

Las aplicaciones amplían entonces la superficie de ataque de un sistema, por lo que se recomienda siempre evitar la instalación de aquellas que no se requieran, siguiendo el principio de seguridad que sugiere el minimalismo.

8.2.5. Ataques de autenticación

Es cuando el atacante logra dominar un equipo atacado, esto se logra engañando al sistema de la víctima para ingresar al mismo. Generalmente el engaño se realiza tomando las secciones ya establecidas por la víctima y así obteniendo su nombre de usuario y clave.

9. Ethical Hacking

9.1. Introducción

Los primeros hackers surgieron en los años 60's en el Instituto Tecnológico de Massachusetts. El instituto contaba con una microcomputadora PDP-1, la cual atrajo la curiosidad de un grupo de estudiantes que formaban parte del Tech Model Railroad Club, TMRC, ellos podían interactuar directamente con ella mediante códigos de programación.

La microcomputadora tardaba mucho en encender, debido a esto se quedaba encendida toda la noche, permitiendo que los miembros del TMRC tuvieran acceso a la microcomputadora y se pusieron a experimentar, uno de los logros más famosos de estos experimentos fue la creación del videojuego Spacewar. Tiempo después algunos miembros del TMRC se volvieron miembros del Laboratorio de Inteligencia Artificial del MIT y se llevaron con ellos la tradición de jugarse bromas inocentes entre ellos, a las cuales llamaban hacks. Fueron los miembros de este laboratorio los primeros en autonombrarse hackers.

9.2. Hacker

Es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por desafío. [14]

9.3. Tipos de Hacker

Dependiendo de su comportamiento, los hackers pueden clasificarse en diversos tipos:

9.3.1. White Hat Hacking (Hacker Blanco)

Son personas con grandes conocimientos de hacking, que utilizan con fines defensivos. Aprovechan su saber para localizar vulnerabilidades e implementar contramedidas.

Son los llamados buenos muchachos (good guys), y se encuentran del lado de la ley y moral. También se asocia el concepto a los Ethical Hackers. [15]

9.3.2. Grey Hat Hacking (Hacker Gris)

Son personas que trabajan, por momentos, de manera ofensiva, y en otros, defensiva, dependiendo de la circunstancia. Esta categoría plantea una línea divisoria entre hackers y crackers. Un Grey Hat Hacker ocasionalmente traspasa los límites. Una gran cantidad de personas transita durante mucho tiempo en esta vía, para luego encontrar asiento en alguno de los lados puros. [15]

9.3.3. Black Hat Hacking (Hacker Negro)

Están del lado opuesto a la ley y la moral. Son personas con un conocimiento extraordinario que realizan actividades maliciosas o destructivas. También son llamados chicos malos (bad guys). Dentro de esta misma categoría podemos mencionar a los Former Black Hats (ex Hacker Negro), que poseen amplia experiencia de campo, pero escasa credibilidad, dado que existe un oscuro pasado ilegal que no los apoya. [15]

9.4. Ética

El término ética proviene del griego ethikos y su significado es carácter. Tiene como objetos de estudio la moral y la acción humana, y se remonta a los orígenes de la filosofía moral. Una doctrina ética elabora y verifica afirmaciones y juicios en términos de lo bueno y lo malo, lo correcto y lo incorrecto.

Las sentencias éticas son juicios morales que se realizan las personas, teniendo como referencia los principios éticos y lo generalmente aceptado. [15]

9.5. Definición Ethical Hacking

Se refiere a los profesionales de la seguridad de la información que utilizan sus conocimientos de hacking con fines defensivos. Su función es determinar lo que un intruso puede hacer sobre un sistema y la información, y velar por su protección.

10. Pentesting (Penetration Test)

A diferencia de los análisis de vulnerabilidades, estas pruebas no solo identifican las vulnerabilidades potenciales, sino que también tratan de explotarlas y, así, confirmar su existencia y el impacto real que podrían tener en la organización. [14]

La explotación es un punto importante, ya que en muchas ocasiones, una vulnerabilidad reportada como crítica no siempre es crítica en el contexto de una organización en particular.

e. Materiales y Métodos

1. Métodos

1.1. Método Deductivo

La deducción va de lo general a lo particular. El método deductivo es aquél que parte los datos generales aceptados como valederos, para deducir por medio del razonamiento lógico, varias suposiciones, es decir; parte de verdades previamente establecidas como principios generales, para luego aplicarlo a casos individuales y comprobar así su validez.

1.2. Método Deductivo

La inducción va de lo particular a lo general. Empleamos el método inductivo cuando de la observación de los hechos particulares obtenemos proposiciones generales, o sea, es aquél que establece un principio general una vez realizado el estudio y análisis de hechos y fenómenos en particular.

1.3. Metodología para el Análisis de Vulnerabilidades

La metodología utilizada para la elaboración del proyecto es una Metodología Clásica. Esta metodología consta de 3 fases, las cuales fueron adaptadas a las necesidades del proyecto para que sea elaborado de una forma ordenada. Las fases utilizadas en este proyecto fueron las siguientes:

- **Fase 1: Recolección de información del objetivo de evaluación**

Esta fase tiene como objetivo obtener y ampliar información sobre la red objetivo a partir de su nombre de dominio. Principalmente se pretende ampliar el número de equipos que se evaluarán posteriormente. Cabe resaltar que en esta fase no se busca encontrar ninguna vulnerabilidad en absoluto, lo que se pretende es obtener la mayor cantidad posible de equipos que la red objetivo tiene.

En esta fase se hizo uso de la herramienta NMAP, la cual nos permitió la identificación de los equipos en cada VLAN y la recolección de información de cada equipo.

- **Fase 2: Escaneo de puertos y enumeración de servicios**

De la ejecución de la fase anterior se obtiene una lista de todos los equipos que la red objetivo tiene con presencia en internet. En la fase actual se examinarán los puertos y servicios de cada uno de estos equipos y con base en el tipo de servicios que ofrecen, se realizará inferencia sobre el papel que cada uno juega dentro de la red objetivo, así como también la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales). Adicionalmente la información obtenida de la fase anterior también es útil para realizar una evaluación indiscriminada de todos los segmentos de red de una organización objeto de análisis.

La herramienta utilizada fue NMAP la cual además de identificar los equipos de la Red nos permite conocer los puertos abiertos y los servicios que están siendo utilizados por los equipos.

- **Fase 3: Escaneo de Vulnerabilidades**

Los equipos que se encontraron como críticos son los que finalmente se someterán a evaluación en esta última fase, en la que se procede a la utilización de un escáner de vulnerabilidades. Este tiene como objetivo detectar los potenciales riesgos al que están expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red objetivo.

En esta etapa se hizo el uso de dos herramientas, Nessus y OpenVas, se usó dos herramientas con el fin de que se complementen entre si y también para tener menos falsas alarmas al momento de la presentación del informe al departamento de Unidad de Telecomunicaciones e Información de la Institución.

1.4. Metodología MAGERIT

Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Magerit persigue los siguientes objetivos:

Directos

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Para realizar el análisis de riesgos Magerit considera los siguientes elementos:

1. **Activos,** que son los elementos del sistema de información que soportan la misión de la organización.
2. **Amenazas,** que son cosas que les pueden pasar a los activos causando un perjuicio a la organización.
3. **Salvaguardas,** son medidas de protección desplegadas para que aquellas amenazas no causen “tanto” daño.

Con estos elementos se puede estimar:

1. **El impacto:** lo que podría pasar y
2. **El riesgo:** lo que poblanamente pase.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

2. Técnicas

2.1. Investigación de Campo

Se la realiza porque el estudio del problema, es en el lugar donde se están generando los hechos; de esta manera se puede conocer de una mejor manera los inconvenientes que se producen en la Universidad al no realizar la detección de vulnerabilidades. Ventaja que ayuda a proponer posibles soluciones y así cumplir con los objetivos del proyecto.

2.2. Entrevista

Esta técnica es utilizada para obtener la información necesaria y conocer el estado de la red de datos, para poder determinar el riesgo y así proponer un plan para mitigar esos riesgos a los que están expuestos.

2.3. Observación

Nos permite conocer las diferentes amenazas y problemas que ocurren en el AEIRNNR y además identificar los diferentes activos que son irrelevantes para la Universidad.

f. Resultados

1. Analizar las diferentes herramientas de software libre para la detección de vulnerabilidades en una red LAN.

En este apartado se realiza un estudio de las herramientas de software libre y también de software privado que sirven para la detección de vulnerabilidades y para el descubrimiento de los diferentes equipos de la red LAN.

1.1. Herramientas para el descubrimiento de Red

A continuación se analizan algunas herramientas que permiten la recolección de información de una red de datos.

1.1.1. NMAP

Definición

Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales

Características

- Determina qué equipos se encuentran disponibles en una red,
- Qué servicios (nombre y versión de la aplicación) ofrecen,
- Cuáles son los puertos abiertos que tienen,
- Qué sistemas operativos (y sus versiones) ejecutan,
- Qué tipo de filtros de paquetes o cortafuegos se están utilizando.
- Además obtiene algunas características del hardware de red del equipo.
- Brinda información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, los tipos de dispositivo y direcciones MAC.

¿En que se utiliza?

Generalmente se utiliza en auditorías de seguridad, pero muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el

inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

¿Por qué Nmap?

Porque es la herramienta más utilizada y popular, ha estado en tantas películas, existen muchos artículos de noticias, comentarios y libros, que mencionan la utilidad de la herramienta. A continuación se detallan algunos artículos, premios obtenidos y las películas en cuales aparece:

- Nmap ha ganado el premio del editor de Linux Journal Choice a la Mejor Herramienta de seguridad. [17]
- Linux Journal tiene una buena visión general de Nmap en el '01 edición de mayo titulado verificación del trabajo con scanners, Parte I (de II): nmap. En él se describe Nmap como el "Campeón Mundial de Port-escáner" y resume que "en definitiva, Nmap es, con mucho, la más rica en características y versátil puerto-escáner disponibles en la actualidad".
- Nmap gana LinuxQuestions.Org Aplicación de seguridad del año premio. Nmap recibió más votos (56.45%) de todas las demás entradas combinadas. [18]
- Nmap gana 1998 mejor premio de seguridad de la información del producto del mundo (junto con la implementación de IPSEC IETF y de L0phtcrack).
- El Instituto CIO boletín sobre seguridad informática vol. 2. No. 3. avanza la teoría de que los "ataques coordinados multinacionales" en el Pentágono que han estado en las noticias últimamente pueden ser realmente adolescentes aburridos utilizando nmap. [19]
- El Chicago Tribune publicó un artículo sobre Llegar a conocer sus servicios de red. Esta es una buena introducción sobre los conceptos básicos de la exploración de puertos. El artículo recomienda Nmap. [20]
- Nmap ha sido también usado en el film **The Matrix reloaded** por el personaje Trinity para penetrar en el sistema de la central eléctrica, mediante la explotación de vulnerabilidades en el servidor SSH y en el Control de redundancia cíclica, (descubiertas en el 2001). La interfaz gráfica de Nmap en la película suscitó el interés de las discusiones en Internet y fue comentado como una aparición bastante realista de las herramientas de hacking. En esas discusiones, algunos piensan que el personaje Trinity utilizó el ataque Control de redundancia cíclica

(descubierto en 2001) para obtener el acceso, luego de que Nmap revelara la existencia de un servicio SSH. [21]

- En la película **Dredd** contiene varias escenas de Nmap, en donde es usado para el reconocimiento y la exploración de la red. [22]
- En la película **Bourne Ultimatum** usan la herramienta Nmap y su nueva interfaz de usuario Zenmap para piratear el servidor de correo, con el fin de leer un correo electrónico. [23]
- Marcos Wolfgang ha escrito un excelente papel en el descubrimiento de sistemas avanzados usando Nmap. [24]
- En la Tesis **"AUDITORÍA DE LA SEGURIDAD INFORMÁTICA PARA EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA MEDIANTE LA METODOLOGÍA OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL",** se usa la herramienta Nmap para sondear la red de computadoras, incluyendo la detección de equipos y sistemas operativos.
- En la Tesis **"Técnicas y Herramientas de Análisis de Vulnerabilidades de una Red",** elaborada por Javier Ríos Yáguez, menciona que la herramienta más popular para el escaneo de puertos y servicios es Nmap.

1.1.2. NETCAT

Definición

Es una herramienta de depuración y la exploración de la red rica en características, ya que puede crear casi cualquier tipo de conexión que se necesita y tiene varias capacidades incorporadas interesantes. [25]

Características

- Útil para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos.
- Permite la depuración de aplicaciones de red.
- También es utilizada a menudo para abrir puertas traseras en un sistema.
- Las conexiones salientes y entrantes, TCP o UDP, desde o hacia los puertos.
- Destacado modo de túnel que permite también un túnel especial, como UDP a TCP, con la posibilidad de especificar todos los parámetros de red (puerto de origen / interfaz, el puerto de escucha / interfaz, y el host remoto permitido para conectar con el túnel.

- Incorporado en las capacidades de búsqueda de puertos, con distribución al azar.
- Sirve para el escaneo de puertos en los equipos

¿En que se utiliza?

Es un recurso imprescindible tanto para expertos en seguridad de redes como para hackers, los cuales usan esta herramienta para realizar auditorías de red.

¿Por qué Netcat?

- ❖ En el artículo **"Intrusión en el Banco JBR",** se utiliza la herramienta netcat para la detección de puertos TCP/UDP abiertos, versión del sistema y nivel de parche.
- ❖ En la tesis **"Propuesta de soluciones a las vulnerabilidades del protocolo de señalización SIP en VOZ sobre IP",** donde se usa netcat para conocer la información del servidor de comunicaciones.

1.1.3. ETTERCAP

Definición

Ettercap es una aplicación que existe tanto para sistemas WINDOWS como LINUX y su función principal es la de analizar la información que pasa en una red LAN, valiéndonos de conocidas técnicas como lo es el man in the Middle

Características

- Capaz de escanear pasivamente la red: recuperación de información sobre los hosts en la LAN, sus puertos abiertos, las versiones de los servicios disponibles, el tipo de host(puerta de enlace, switch, Access Point, cámara IP, etc) y las distancias estimadas en número de saltos.
- OS fingerprint: es decir, detección del sistema operativo remoto y su adaptador de red.
- Basado en IP: Los paquetes son filtrados basada en IP de origen y destino.
- Compatibilidad con SSH1: puede interceptar usuarios y contraseñas incluso en conexiones "seguras" con SSH.
- Compatibilidad con HTTPS: intercepta conexiones mediante http SSL, incluso si se establecen a través de un proxy.

- Filtrado y sustitución de paquetes.

¿En que se utiliza?

La mayoría de expertos de seguridad utiliza esta herramienta para realizar el ataque man in the Middle y para visualizar el tráfico en la red de datos.

¿Por qué Ettercap?

Ettercap es, junto a Whireshark, el sniffer de red más utilizado por hackers y expertos en seguridad. Su facilidad de uso hace que muchos prefieran éste sobre el Whireshark ya nombrado, aunque la mayoría de los expertos usen los dos indistintamente**.**

- ❖ En un artículo **"Respuesta a incidentes de seguridad de información"**, realizado por **Andrew Rollins**, jefe del departamento de seguridad de la información de la empresa BI Tops, menciona que la herramienta Ettercap es usada para la detección de trazas de incidentes informáticos variedad de sistemas de hardware y software, además para "escuchar" red de área local. [27]
- ❖ En la tesis **"Data Link Layer Security Problems and Solutions",** elaborada por Nasir Siddique, Mustafa Ali y Mubeen Zubair, se usa la Herramienta Ettercap para realizar ataques a los equipos y también se utilizada para la captura de tráfico. [30]

1.1.4. CHEOPS

Definición

Es una herramienta de gestión de red para el mapeo de la red y el control de su red. Tiene la funcionalidad de descubrimiento de sistemas / redes, así como detección de sistema operativo. Se hace un análisis de puertos de cada equipo para decirle qué servicios se están ejecutando. [31]

Características

- Licencia Pública General de GNU versión 2.0 (GPLv2)
- Permite detectar a todos los equipos que se encuentran conectados en la red LAN

- Tiene un escáner de puertos TCP generalizada que permite escanear los puertos de los equipos, pero otros programas son probablemente más adecuado para estas tareas.
- Organizar la red en las páginas adecuadas para que pueda colocar partes pertinentes juntos, y rápidamente se van a un área específica o específica de la red.
- Detección OS: Cheops pueden determinar opcionalmente el sistema operativo de los ordenadores en la red y seleccionar un icono apropiado para ello.
- Encuentra anfitriones: Usted puede encontrar rápidamente un único host entre todos los hosts conocidos en una gran red.
- Asignación: Cheops le puede mostrar las rutas tomadas a las zonas de acceso de la red. (Esta característica está diseñada para redes más grandes, con los routers, subredes, etc.) Este mapeo no sólo hace más clara la jerarquía, pero puede mostrar problemas de enrutamiento inusuales, como este triángulo enrutador inusual.
- Servicios: al hacer clic derecho en un anfitrión rápidamente te muestra una lista de los servicios comunes que presta apoyo, y también le permite rápida y fácilmente el acceso a ellas.
- Visitas múltiple: Para redes grandes, puede ver la red con los iconos más pequeños, o incluso como una simple lista de redes. El diseño puede ser organizado por dominio, el nombre de host, dirección IP, etc., y la búsqueda se apoya en ambos formatos y emblemáticos de la lista.
- Servicio sondeando: Recuperar información de versión de determinados servicios, para estar seguro de cualquier host está al día con la última revisión de sus servicios.
- Altamente configurable: Cheops es altamente configurable, tanto a través de archivos de configuración basados en texto ya través de una gráfica "Opciones".
- Soporte integrado SNMP: Cheops incluye un simple navegador de SNMP integrado, incluyendo la capacidad de escritura, usando la biblioteca UCD SNMP.

¿En que se utiliza?

Generalmente se utiliza en auditorías de seguridad, pero muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el

inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

¿Por qué Cheops?

- En el libro **"HACKING EXPOSED",** escrito por Stuart McClure, le da un reconocimiento a la herramienta Cheops para la exploración de redes.
- El artículo **"La exploración de puertos y Evaluación de vulnerabilidades"** del instituto de Tecnología Georgia, donde hace hincapié que la herramienta Cheops-ng es una de las "mejores" junto con Nmap para administrar y acceder a la red.
- El artículo **"Vulnerability Take Grant (VTG): An efficient approach to analyze network vulnerabilities",** recomienda que se use la herramienta Cheops para la captura de la topología de red. [32]

A continuación se presenta una tabla, donde se comparan las características más significativas de las herramientas analizadas anteriormente:

TABLA VII
COMPARACIÓN DE HERRAMIENTAS PARA EL DESCUBRIMIENTO DE RED Y RECOLECCIÓN DE INFORMACIÓN

Características	NMAP	NETCAT	Ettercap	CHEOPS
Identificación de equipos	SI	NO	SI	SI
Tipo de Licencia	Libre	Libre	Libre	Libre
Permite identificar los puertos abiertos	SI	SI	SI	SI
Permite Determinar los servicios que se están utilizando	SI	SI	NO	SI

Exploración de redes extensas	SI	NO	SI	SI
Identificación del Sistema Operativo	Si	NO	SI	SI
Sustento Científico	Aparece en varias películas, gano algunos premios y ha sido utilizado en algunos artículos.	No se encontró algún artículo donde se hay usado esta herramienta a pesar de ser popular	Existe un artículo, que menciona su uso y existen tesis donde han hecho uso de esta herramienta.	No existen muchos artículos donde se haya usado esta herramienta, es muy buena pero poco conocida.

Una vez analizadas las herramientas y con la ayuda del cuadro de comparación se eligió utilizar la herramienta Nmap, no solo por ser una herramienta popular, por ende muy utilizada, sino por contar con bastante sustento científico, se ha hecho acreedor de varios premios, aparecido en varias películas, la han usado en algunas tesis y artículos para la exploración de la red y para determinar los puertos abiertos y servicios utilizados por los equipos. Cabe recalcar que CHEOPS es una excelente herramienta pero lastimosamente no tiene un buen sustento científico que argumente porque su utilización.

1.2. Herramientas para el escaneo de vulnerabilidades

El objetivo aquí es describir herramientas “open source” para poder analizar la seguridad en redes y sistemas.

1.2.1. Nessus

Definición

Es un programa que escanea vulnerabilidades de diversos Sistemas Operativos (Windows, Linux, Mac, Solaris, etc.), además de encontrar errores de configuraciones y vulnerabilidades, ya sean por falta de actualización del S.O, puertos que pueden llevar a sesiones meterpreter, procesos Web o fallos en softwares instalados (Apache, Mysql, etc).

Características

- Nessus comenzó en el mundo de la seguridad informática con una licencia abierta, convirtiéndose con el paso del tiempo en un producto de pago.
- La licencia de uso que nos otorgan con la descarga de la versión Free es única y exclusivamente para uso doméstico.
- Actualmente existen dos versiones: "Home" y "Work" Esta última de pago y sin restricciones.
- Nessus no solo le informará qué vulnerabilidades de seguridad existen en su red y el nivel de riesgo de cada una de ellas (Info, Low, Medium, High y Critical), sino que también le notificará sobre cómo mitigarlas, ofreciendo soluciones.
- Análisis Nessus 5 tiene cinco niveles de gravedad: ● Informativo ● Riesgo Bajo ● Riesgo Medio ● Riesgo Alto ● Riesgo Crítico.
- Escanear varias redes (Analiza en IPv4, IPv6 y redes híbridas).
- Programación de análisis.
- Tiempo de análisis corto y uso de bajos recursos.
- Notificaciones de correo electrónico dirigidos.
- Tiene una Base de Datos actualizada de vulnerabilidades de seguridad.
- Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando "unsafe test" (pruebas no seguras) antes de escanear.
- Los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX.

¿Por qué Nessus?

Nessus es acreedor de varios premios y certificaciones, los cuales hacen que sea una herramienta confiable al momento de utilizarla.

- En el año 2015, SC Magazine dio a Nessus cinco estrellas y la nombro como una de las mejores compras.
- Obtuvo el premio a la excelencia del producto Elección 2015 NetworkWorld Asia lectores vulnerabilidad de la administración y de supervisión continua.
- En el 2015 SANS dio el Premio a Nessus como el mejor para evaluación de la vulnerabilidad.
- Proveedor de PCI Escaneo Aprobado (ASV)

- Defendible es una Industria de Tarjetas de Pago (PCI) Proveedor Aprobado de Escaneo (ASV). Nessus nube permite a las empresas para validar la adhesión a ciertos requisitos de PCI DSS 3.0 mediante la realización de análisis de vulnerabilidad de los sistemas de revestimiento periódicos de Internet.
- Tenable Network Security utiliza el programa CVE para hacer referencia a cada una de las vulnerabilidades detectadas por Nessus y el explorador de las vulnerabilidades pasivas y presentadas por SecurityCenter.
- En la tesis **"INFORMATICA FORENSE: AUDITORIA DE SEGURIDAD",** se usa la herramienta Nessus para la realización del análisis de vulnerabilidades y utilizando como objetivo las redes extraídas en la fase de Recopilación de la Información. Se tratará de encontrar todas las vulnerabilidades existentes.
- En la tesis **"PROPUESTA DE BEST PRACTICE PARA EL ANALISIS DE VULNERABILIDADES, MÉTODOS DE PREVENCIÓN Y PROTECCIÓN APLICADOS A LA INFRAESTRUCTURA DE RED DEL LABORATORIO DE SISTEMAS",** el autor usa la herramienta Nessus para el análisis de vulnerabilidades en los equipos de la red del laboratorio de sistemas.
- En el artículo **"Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web",** elaborado por Ana Laura Hernández Saucedo, especifica en qué tipo de vulnerabilidades se debe utilizar Nessus.

1.2.2. OpenVas

Definición

Open Vulnerability Assessment System (OpenVAS) ofrece servicios de escaneo y administración de vulnerabilidades. Según su web oficial (www.openvas.org) se actualiza a diario y aglutina ya un total de 47000 test de vulnerabilidad. Se considera a esta aplicación un producto libre cuyos componentes tienen licencia GNU GPL.

Características

- Tiene una base de datos con alrededor de 47000 plugins para las evaluaciones de vulnerabilidades.
- Permite realizar escaneos a una cantidad ilimitada de equipos al mismo tiempo.
- Admite que se escanee una subred, una rango de equipos e incluso equipos individuales.

- Cuenta con una interfaz de usuario.
- Clasifica a las vulnerabilidades en Alto (color rojo), Medio (Color amarillo) y Bajo (color Celeste).
- Recomienda soluciones para mitigar las vulnerabilidades encontradas.
- Los informes se pueden exportar e importar para la comparación con otros informes en los formatos NBE, XML, HTML, LaTeX, ASCII y PDF.
- OpenVAS trae consigo algunas herramientas de seguridad integradas. Estos incluyen nmap (escáner de puertos) Nikto (Examen de los servidores web), Ike-Scan (Examen de servidores IPSec) y AMAP (Se abrirá servicios).
- Se pueden programar las evaluaciones de vulnerabilidades en los equipos.
- El tiempo de análisis es largo, comparado con otras herramientas que arrogan resultados en tiempos más cortos.
- La configuración puede llegar a ser complicada si se instala manualmente, mientras que si se usa desde Kali Linux resulta fácil, ya que viene integrada.

¿Por qué OpenVas?

OpenVas recibe el apoyo y la contribución de muchas personas y organizaciones, añadiendo a la calidad y fiabilidad de la solución: pruebas de penetración, usuarios avanzados, los investigadores de seguridad, los círculos académicos, etc.

- ❖ La Oficina Federal para la Seguridad de la Información (BSI) apoyó diversas características de la estructura de software OpenVas así como diversas pruebas de vulnerabilidad de red.
- ❖ En la tesis **"ESTUDIO DE SEGURIDADES EN UNA RED EXTREMO A EXTREMO, BASADA EN PROTOCOLO IPV6.",** se hace uso de la herramienta OpenVas para identificar las vulnerabilidades en los equipos de la red de estudio.
- ❖ En la tesis **"DISEÑO DE UN MODELO DE ANÁLISIS FORENSE INFORMÁTICO EN EL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA.",** se usa la herramienta OpenVas para la búsqueda de vulnerabilidades en los servidores de la red.
- ❖ En la tesis **"SIMULACIÓN DE ATAQUES A REDES IP EN UN ENTORNO CORPORATIVO REAL",** se usa OpenVas para el escaneo y administración de las vulnerabilidades en los equipos.

1.2.3. OWASP ZAP

Definición

Open Web Application Security Project (OWASP) es un proyecto abierto sin ánimo de lucro destinado a mejorar la seguridad de las diferentes aplicaciones y servicios web con el fin de conseguir un Internet más seguro. Para ello pretende hacer públicos los resultados de diferentes análisis de seguridad para que las organizaciones tengan constancia de ellos y los solucionen lo antes posible para mantener al máximo la seguridad de sus usuarios. [35]

Características

Las principales características de OWASP ZAP son:

- Herramienta totalmente gratuita y de código abierto.
- Herramienta multi-plataforma, compatible incluso con Raspberry Pi.
- Fácil de instalar, dependiendo únicamente de Java 1.7 o superior.
- Posibilidad de asignar un sistema de prioridades.
- Traducida a más de 12 idiomas, entre ellos, el español.
- Excelente manual de ayuda y gran comunidad en la red.
- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Posibilidad de localizar recursos en un servidor.
- Análisis automáticos.
- Análisis pasivos.
- Posibilidad de lanzar varios ataques a la vez.
- Capacidad para utilizar certificados SSL dinámicos.
- Soporte para utilizar tarjetas inteligentes (DNI-e, por ejemplo) y certificados personales.
- Análisis de sistemas de autenticación.
- Posibilidad de actualizar la herramienta automáticamente.

¿Por qué OWASP ZAP?

- Una de las herramientas de OWASP se hace referencia en el premio 2015 Bossie para el mejor trabajo en red y la seguridad del software de código abierto.
- Obtuvo el segundo lugar en las mejores herramientas de seguridad de 2014 según lo votado por los lectores ToolsWatch.org.
- Fue la herramienta de seguridad superior del año 2013 según lo votado por los lectores ToolsWatch.org.
- En la tesis **"GUÍA DE BUENAS PRÁCTICAS DE DESARROLLO DE APLICACIONES WEB SEGURAS APLICADO AL SISTEMA CONTROL DE NUEVOS ASPIRANTES EMPRESA GRUPO LAAR",** se usa OWASP para encontrar vulnerabilidades en aplicaciones web.
- En la tesis **"EFECTIVIDAD DE TÉCNICAS DE OWASP PARA ASEGURAR APLICACIONES WEB CONTRA INYECCIÓN DE SQL",** se usa técnicas de OWASP para resguardar la seguridad de las aplicaciones web contra inyecciones SQL.

1.2.4. Retina

Definición

Es un software comercial de ámbito profesional que permite tanto a los administradores como hackers obtener información muy detallada sobre las vulnerabilidades de un equipo.

Características

- Optimiza el rendimiento de la red y escanea dispositivos de red, sistemas operativos, aplicaciones y bases de datos sin afectar la disponibilidad ni el rendimiento.
- Actualizada permanentemente por el reconocido equipo de investigación de BeyondTrust, esta base de datos le permite estar al día incluso respecto de las amenazas más recientes.
- Se puede implementar Retina como escáner independiente, distribuido en todo un entorno e integrado con Retina CS en implementaciones empresariales.

- Integración con herramientas líderes de ensayo de penetración y soluciones como Core Security, Exploit DB y Metasploit haciendo clic con el botón derecho del mouse.
- Detecta todos los activos de red (local y remota), de web y virtuales de su entorno.
- Evalúa los riesgos y asigne prioridades a las medidas de corrección según los índices de ataque, las normas CVSS y otros factores.
- Presenta informes de avances y resultados a sus colegas que desempeñan funciones gerenciales, de cumplimiento, auditoría, riesgos y otras.
- Intercambie datos con soluciones reconocidas de SIEM, GRC y otras plataformas de administración de la seguridad.
- Incorpora un sistema de generación de formularios que permite realizar informes de seguridad con un alto nivel de detalle.
- Rápida y precisa exploraciones

¿Por qué Retina?

- Cuenta con varios clientes muy conocidos como: Pearson, Capella Education Company, Capital One Bank, etc.
- Tiene la confianza de algunas empresas muy conocidas como: Bank de America, Nasa, NBC y ExxonMobil.
- El artículo **"Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá",** el autor hace uso de la herramienta Retina para el estudio y gestión de las vulnerabilidades informáticas.

A continuación se realiza un cuadro donde se comparan las características más primordiales de las herramientas para la evaluación de vulnerabilidades analizadas anteriormente

:

TABLA VIII
CUADRO COMPARATIVO DE LAS HERRAMIENTAS INVESTIGADAS PARA EL ANÁLISIS DE VULNERABILIDADES

Características	Nessus	OpenVas	OWASP	Retina
Licencia	Libre/Pagada	Libre	Libre	Libre/Pagada
Multiplataforma	Si	Si	Si	Si
Plugins	80355	47000	-----	-------
Tiempo de Análisis	Corto	Largo	Corto	Medio
Clasificación de las vulnerabilidades	Si	Si	Si	Si
Brinda Soluciones a las vulnerabilidades	Si	Si	Si	Si
Configuración	Fácil	Difícil	Fácil	Fácil
Exportación de resultados	HTML, CSV, Nessus y Nessus data.	PDF, HTML, XML, etc.	PDF, HTML, XML, CSV.	PDF, HTML, XML, etc.
Programación de escaneos	Si	Si	Si	Si
Soporte	Única Empresa	Varias Empresas	Varias Empresas	Única Empresa

Consumo de Recursos	Bajo	Medio	Bajo	Medio
Escaneo a cualquier equipos	Si	Si	No, solo para web	Si
Sustento científico	Se ha hecho acreedor a varios premios, es utilizada especialmente para la búsqueda de vulnerabilidades en los equipos de una red.	No cuenta con mucha sustento científico, existen artículos y tesis relacionados su utilización, indicando que es una alternativa de Nessus	Es acreedora de muchos premios en cuento se refiere a la seguridad, hay variedad de artículos donde recomienda s su uso.	Existen algunos artículos donde se usa esta herramienta para la gestión de vulnerabilidad es.

Una vez realizado el análisis de cada herramienta se ha procedido a comparar sus características más principales. Se puedo evidenciar que Nessus es una herramienta muy potente, ganadora de muchos premios, es recomendada en artículos y tesis para la búsqueda de vulnerabilidades en los equipos, tiene una deficiencia que es el tipo de licencia, es verdad que cuenta con una versión gratuita pero solo es para uso doméstico, es por ello que por su tipo de licencia pagada no se iba hacer uso de esta herramienta, aun sabiendo el potencial. Finalmente se decidió utilizar esta herramienta, ya que recientemente en la Unidad de Telecomunicaciones e Información han instalado el servidor Nessus con su respectiva licencia de pago.

Retina tiene la confianza y como clientes a muchas empresas importantes por ejemplo como al banco de América y sin duda a una de las empresas más potentes y conocida como es la NASA, esto es muy importante al momento para seleccionar una herramienta, pero lastimosamente tiene el mismo problema de Nessus en cuanto se refiere al tipo de licencia.

Durante el análisis de la herramienta OWASP se evidencio la popularidad que tiene, la cantidad de premios ganados y algunos artículos y tesis donde se la recomienda, el problema de esta herramienta es que solamente se enfoca a la búsqueda de vulnerabilidades web y en este proyecto se requiere una herramienta que busque vulnerabilidades de todo tipo no solo web, es por eso que no se usa esta gran herramienta pero si la recomiendo usarla en el ambiente web.

Por ultimo nos enfocamos a la otra herramienta usada en este proyecto que es OpenVas, cabe recalcar que no existen muchos artículos donde se mencione que se hace uso de esta herramienta aun siendo una de las más utilizadas a nivel mundial, tiene a su favor el apoyo de la Oficina Federal para la Seguridad de la Información (BSI), es por ello que es la mejor alternativa de las herramientas de licencia libre para la búsqueda de vulnerabilidades, hay que recalcar que OpenVas se derivó de Nessus.

2. Implementar las diferentes herramientas tecnológicas para la detección de vulnerabilidades en la red LAN Jerárquica de la Universidad Nacional de Loja.

Esta fase tiene como objetivo obtener información sobre la red objetivo, donde se pretende descubrir los equipos que se evaluarán posteriormente. Con el uso de la herramienta OpenVas y Nessus se realiza el escaneo de vulnerabilidades en los equipos objetivos de la red LAN.

2.1. Reconocimiento de la Red

Se realiza el descubrimiento de topología de red desde el interior de la red objetivo, donde se obtiene una lista de todos los equipos que la red objetivo tiene. Se examinan los puertos y servicios de cada uno de estos equipos y con base en el tipo de servicios que ofrecen, se realiza inferencia sobre el papel que cada uno juega dentro de la red objetivo, así como también la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales).

Se conoce que la Red LAN utiliza un modelo jerárquico de 3 capas de CISCO. Donde el **SWITCH CORE** se encuentra instalado en el centro de cómputo de la Universidad Nacional de Loja, los **SWITCH DE DISTRIBUCIÓN** se encuentran ubicados en las diferentes áreas de la Universidad (uno por área) y los **SWITCH DE ACCESO** se encuentran distribuidos por los bloques de cada área.

Las subredes utilizadas en el Área de la Energía es la 10.10.0.0/20 – 10.30.0.0/20 y las VLAN son:

- **VLAN 1** para Default
- **VLAN 10** para Administrativos
- **VLAN 20** para Docentes
- **VLAN 30** para Estudiantes
- **VLAN 40** para Telefonía VOIP
- **VLAN 50** para Relojes Biométricos e Impresoras
- **VLAN 60** para Cámaras
- **VLAN 70** para Laboratorios
- **VLAN 120** para Biblioteca

- **VLAN 210** para Wireless

2.1.1. VLAN 1 Default: GESTIÓN EQUIPOS DE RED

Es la VLAN por defecto que se utiliza para los SWITCH DE ACCESO y la subred utilizada es la 10.10.1.0/24, con el uso de la herramienta NAMP se puede determinar los equipos de esta subred, el Sistema Operativo de cada equipo, los puertos abiertos y servicios que brindan.

Se utiliza el comando:

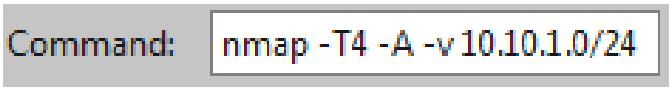


Figura 7. Comando para el descubrimiento de la Red

Donde;

- **-T4** sirve para especificar el tipo de escaneo a efectuarse, en este caso se utiliza un nivel 4 que significa aggressive.
- **-A** sirve para descubrir más a detalle los Sistemas Operativos utilizados en los equipos.
- **-v** sirve para la detección de puertos abiertos para tratar de descubrir servicios y versiones en esos puertos.
- Y por último se especifica el host o la subred que se va a escanear.

Con lo cual se llega a obtener todos los equipos conectados en la subred, su respectivo SO, los puertos abiertos que tiene y los servicios que ofrece.

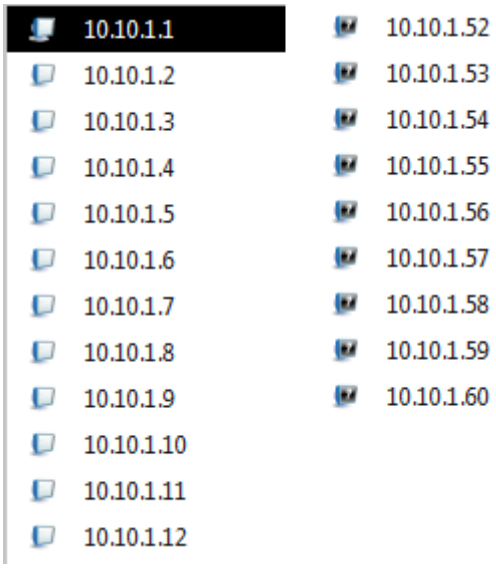


Figura 8. Hosts, puertos y servicios de la VLAN 1

En la figura 8 se puede apreciar los las direcciones IP de los hosts pertenecientes a la VLAN 1, donde se puede contabilizar un total de 21 equipos.

La herramienta también nos permite ver los detalles de cualquier host encontrado en la subred y con ello identificar el Sistema Operativo y deducir el tipo de equipo escaneado.

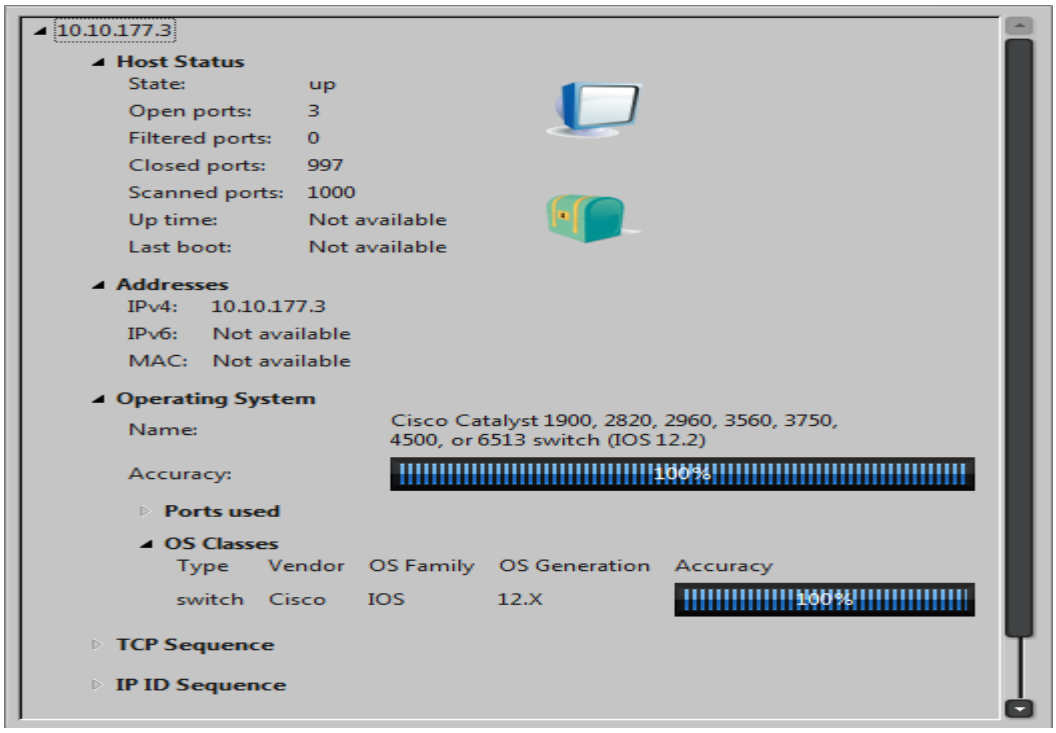


Figura 9. Detalles de un host encontrado

El host escaneado en la figura 9 se puede apreciar que es un SWITCH Cisco y analizando los demás hosts se deduce que los hosts con las direcciones IP 10.10.1.1 – 10.10.1.12 son SWITCH y los hosts con las direcciones IP 10.10.1.52 – 10.10.1.60 son Access Point Cisco.

Cabe recalcar que el SWITCH de DISTRIBUCIÓN también pertenece a esta VLAN y es el primero que aparece en la lista, es decir el que tiene la dirección IP 10.10.1.1.

2.1.2. VLAN 10 para Administrativos

Esta VLAN es utilizada para las personas Administrativas del Área de Energía, como Director del Área, Coordinador de cada carrera, etc. La subred utilizada es la 10.10.2.0/23, donde se encuentran conectadas las computadoras utilizadas por estas personas, estos equipos no son evaluados debido a que son de uso personal y por la cantidad.

2.1.3. VLAN 20 para Docentes

Esta VLAN es utilizada para los Docentes del área de Energía. La subred manejada es la 10.10.3.0/24.

2.1.4. VLAN 30 para Estudiantes

Esta VLAN es utilizada para los estudiantes de área de Energía. La subred manejada es la 10.10.4.0/24.

2.1.5. VLAN 40 para Telefonía

Se utiliza esta VLAN para la telefonía del área de energía. La subred manejada es la 10.10.5.0/24, haciendo uso de la herramienta NMAP se pudieron identificar una variedad de hosts, como se puede observar en la figura 10.

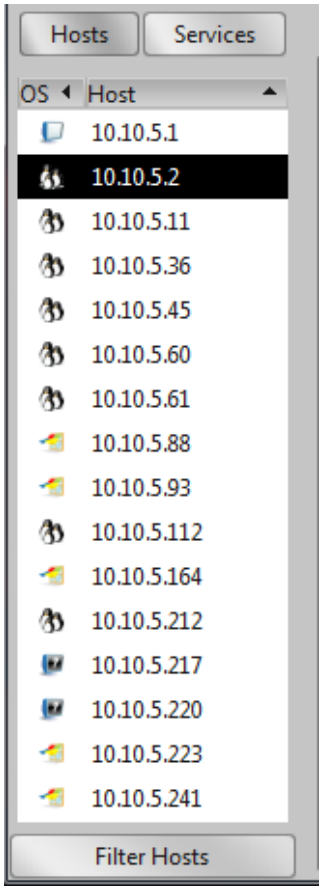


Figura 10. Hosts de la VLAN de Telefonía

Para poder identificar cuál de todos los hosts encontrados son los teléfonos IP, se lo realizado de la siguiente manera: se selecciona un host encontrado y se identifica en la columna versión, que nos muestra la herramienta NMAP, donde se puede determinar que el host es un teléfono IP de marca Grandstream modelo GXP1400, con cual se han encontrado 7 teléfonos IP en el área de energía.

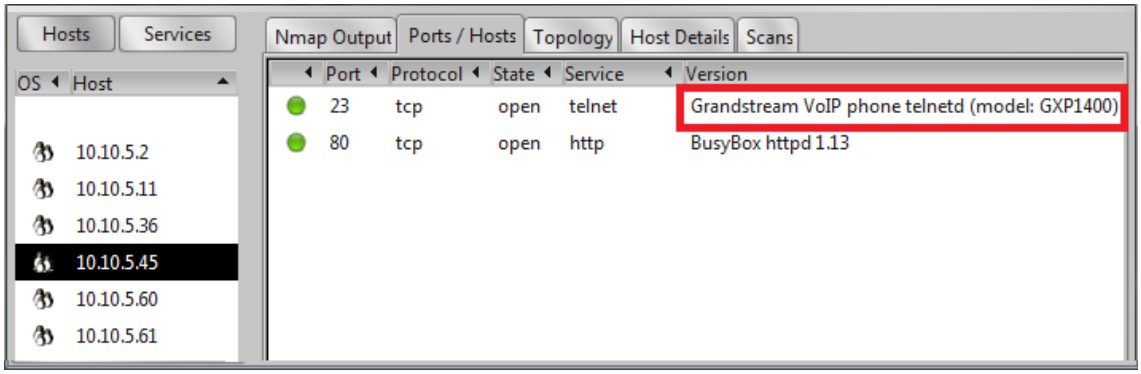


Figura 11. Identificación de un Teléfono IP

De igual forma se puede determinar la existencia de un Servidor, se deduce que es el servidor de comunicaciones, en la figura 12 podemos observar que el host tiene bastantes puertos y servicios abiertos y además podemos identificar en la columna de versión la existencia del SO Centos, lo cual nos indica que existe una mayor probabilidad de que sea el servidor utilizado.

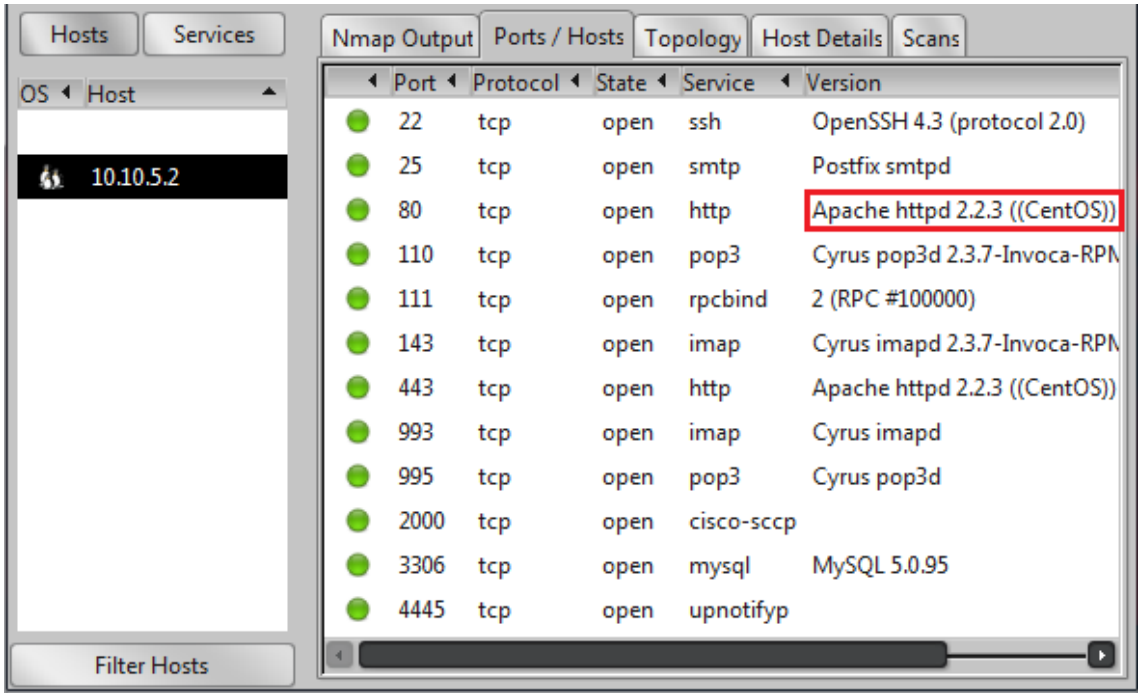


Figura 12. Identificación del Servidor de Comunicaciones

Mientras que en los demás hosts restantes se pudo identificar 5 computados con diferentes sistemas operativos, las mismas que no deben de pertenecer a esta VLAN, pero de una manera se encuentran en ella, esto se puede apreciar en la siguiente imagen.

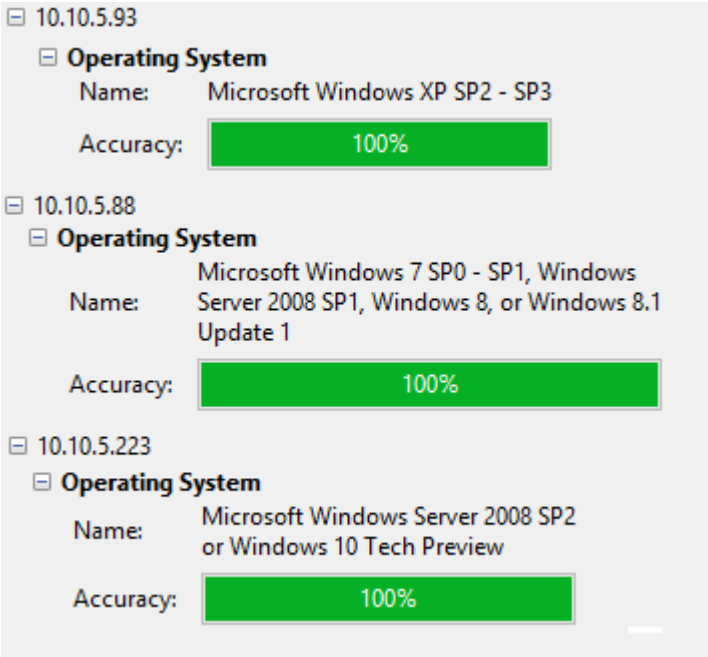


Figura 13. Identificación de computadoras en la VLAN de telefonía

Existen 2 hosts que no se obtiene mucha información, por lo cual no es posible identificar si son computadoras o teléfonos IP.

2.1.6. VLAN 50 para Impresoras y Relojes Biométricos

Se utiliza esta VLAN para los Relojes Biométricos e Impresoras, la subred manejada es la 10.10.6.0/24, con el uso de la herramienta NMAP se encontraron los siguientes equipos.

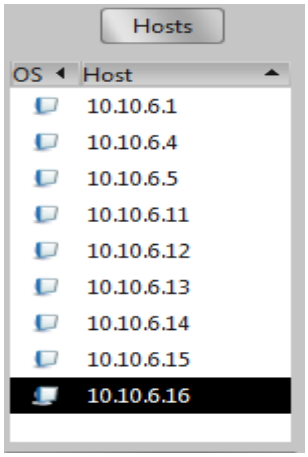


Figura 14. Hosts de la VLAN de Impresoras y Relojes Biométricos

En esta VLAN se pudo identificar la presencia de 2 relojes biométricos, se hizo una consulta en el internet de los sistemas operativos que nos da la herramienta para poder determinar qué tipo de equipo son, es por ello que se dedujo que son relojes biométricos.

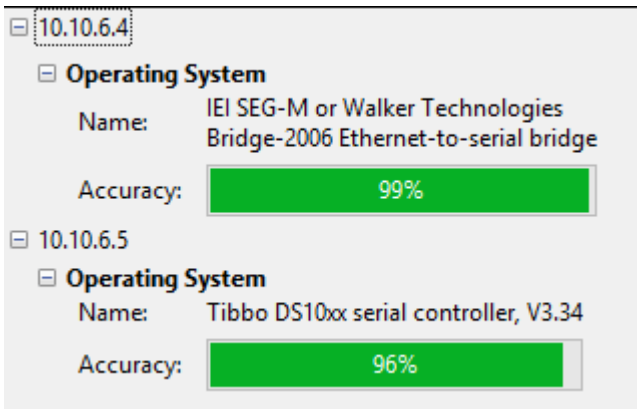


Figura 15. Identificación de los Relojes Biométricos

En cuanto a la identificación de las impresoras fue más fácil por el conocimiento general que se tiene de impresoras, por ejemplo las marcas. Viendo los posibles sistemas operativos que nos presenta la herramienta se puede deducir cual es el correcto y con lo cual determinar si es una impresora. Se identificaron un total de 6 impresoras en el área de energía.

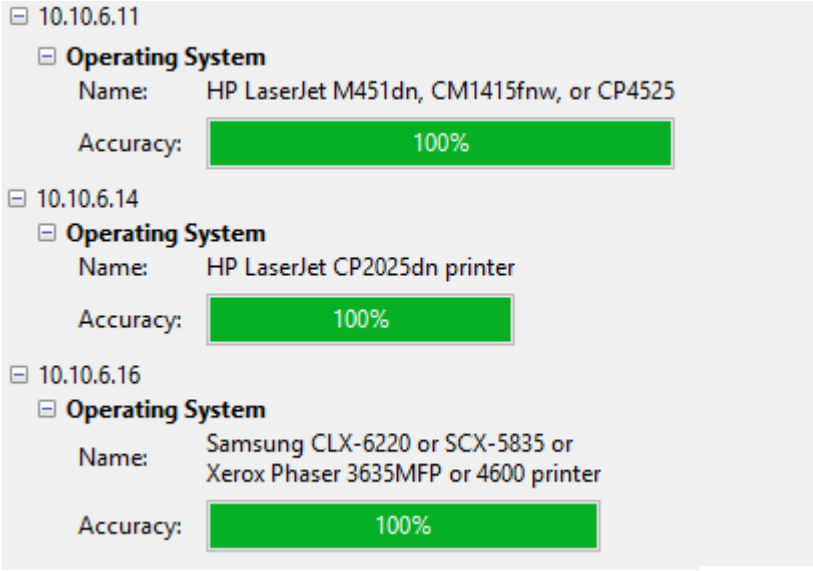


Figura 16. Identificación de las Impresoras IP

2.1.7. VLAN 60 para Cámaras IP

Se utiliza es VLAN para las cámaras, la subred utilizada es la 10.10.7.0/24, solo se encontró un equipo en esta subred del área de energía. En esta VLAN solamente se reportó la existencia de una cámara IP.

2.1.8. VLAN 120 para Bibliotecas

Se utiliza para las bibliotecas, la subred manejada es la 10.10.14.0/24, en esta subred se encuentras las computadoras de la biblioteca del área de energía.

2.1.9. VLAN 210 para Wireless

Se utiliza para la Wireless, la subred manejada es la 10.30.0.0/20, en esta subred se encontraron los siguientes hosts;

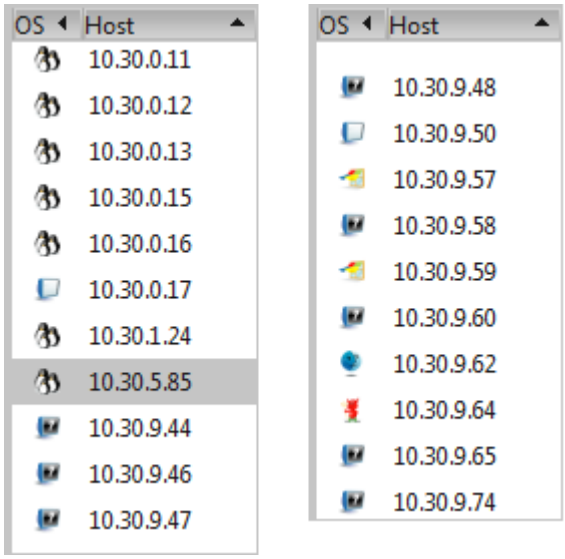


Figura 17. Hosts encontrados en la VLAN de la Wireless

De igual manera como se identificaron los teléfonos IP, se identifican los Access Point (AP), en la columna versión podemos apreciar que nos presenta la marca del AP, en este caso es Linksys.

Se identificaron 7 AP de marca Linksys y 1 de marca D-Link.

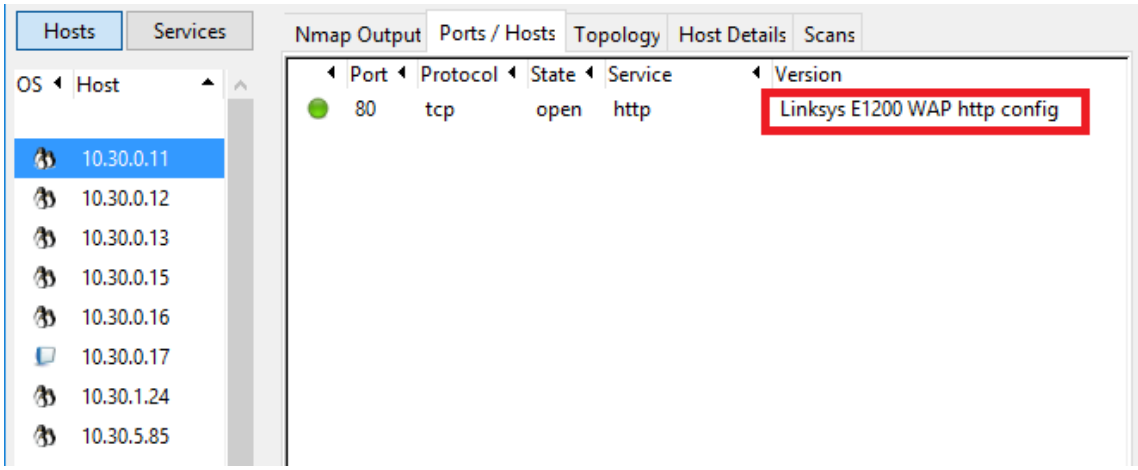


Figura 18. Identificación de los Access Point

Además se identificaron 16 computadoras que al parecer al momento del descubrimiento de red se encontraban conectados a algún AP, es por ello que aparecen en esta VLAN.

Descubrimiento de la Red LAN en el Edificio de Laboratorios del Área de Energía

En cuanto a la topología de red del Edificio de Laboratorios del área de Energía, se considera otra subred, debido a que se utiliza otro SWITCH de DISTRIBUCION, de igual manera se realiza el descubrimiento de red por VLAN.

2.1.10. VLAN 1 Para Default-Edificio de Laboratorios

Es la VLAN por defecto que se utiliza para los SWITCH DE ACCESO y la subred utilizada es la 10.10.177.0/24, con el uso de la herramienta NAMP se puede determinar los equipos de esta subred, el Sistema Operativo de cada equipo, los puertos abiertos y servicios que brindan.

Se encontraron SWITCHES y ACCESS POINT CISCO en esta VLAN, esto se puede apreciar en la siguiente imagen:

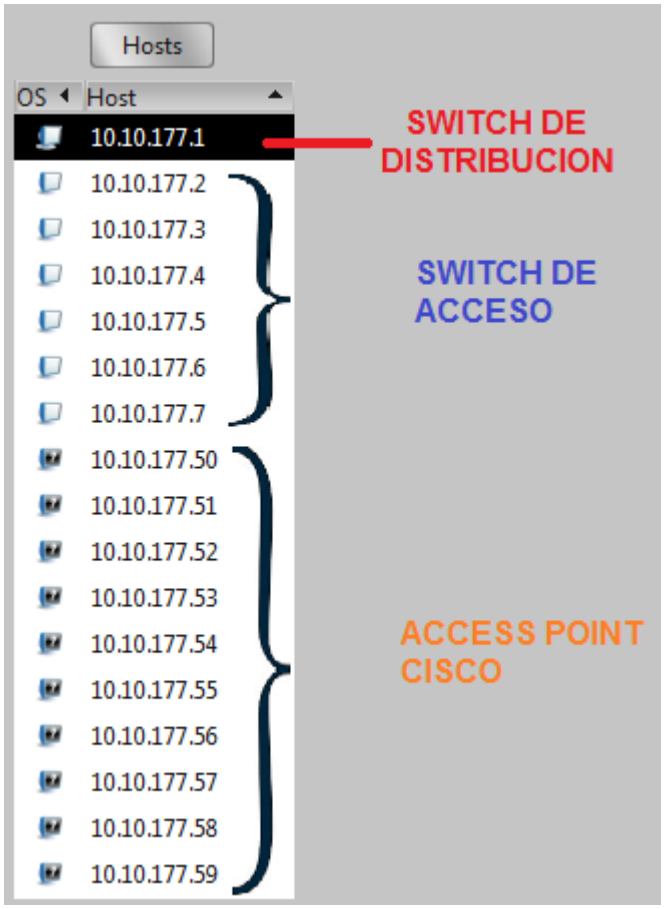


Figura 19. Hosts de la VLAN de Default del Edificio

2.1.11. VLAN 10 para Administrativos-Edificio de Laboratorios

Esta VLAN es utilizada para las personas Administrativas del Área de Energía, como Director del Área, Coordinador de cada carrera, etc. La subred utilizada es la 10.10.178.0/23, donde se encuentran conectadas las computadoras utilizadas por estas personas, estos equipos no son evaluados.

2.1.12. VLAN 20 para Docentes-Edificio de Laboratorios

Esta VLAN es utilizada para los Docentes del área de Energía. La subred manejada es la 10.10.180.0/24.

2.1.13. VLAN 30 para Estudiantes-Edificio de Laboratorios

Esta VLAN es utilizada para los estudiantes de área de Energía. La subred manejada es la 10.10.181.0/24.

2.1.14. VLAN 40 para Telefonía-Edificio de Laboratorios

Se utiliza esta VLAN para la telefonía del área de energía. La subred manejada es la 10.10.182.0/24, haciendo uso de la herramienta NMAP se pudieron identificar los siguientes hosts:

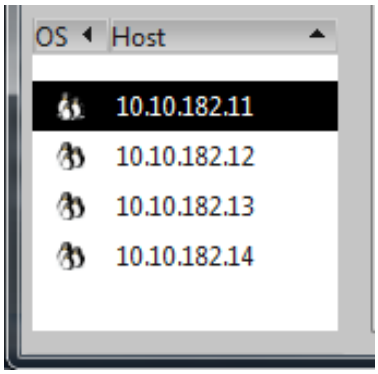


Figura 20. Teléfonos IP encontrados en el Edificio

Se encontraron 4 teléfonos IP de marca GRANDSTREAM modelo GXP1400.

2.1.15. VLAN 50 para Impresoras y Relojes Biométricos-Edificio de Laboratorios

Se utiliza esta VLAN para los Relojes Biométricos e Impresoras, la subred manejada es la 10.10.183.0/24, con el uso de la herramienta NMAP se encontraron 4 relojes, biométricos ZEM560, como se puede observar en la siguiente figura:

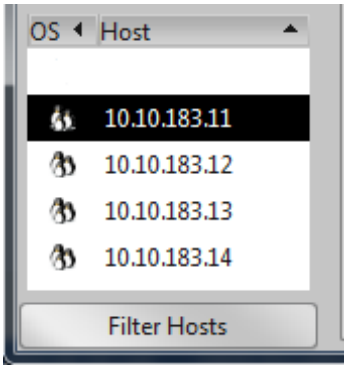


Figura 21. Relojes Biométricos del Edificio

2.1.16. VLAN 60 para Cámaras IP-Edificio de Laboratorios

Se utiliza esta VLAN para las cámaras IP, la subred utilizada es la 10.10.184.0/24, con la herramienta NMAP se encontraron 13 cámaras IP las mismas que son manipulas mediante los servicios HTTP y HTTPS, puerto 80 y 443 respectivamente.

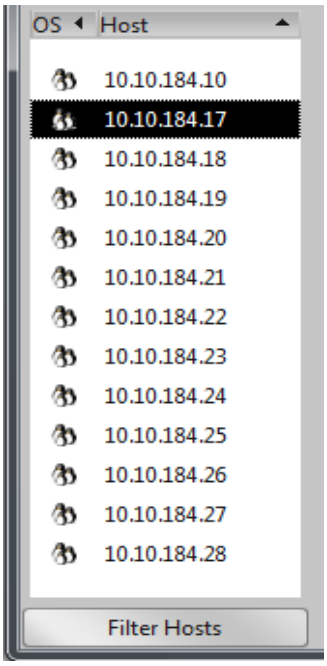


Figura 22. Cámaras IP del Edificio

2.1.17. VLAN 70 para Laboratorios

Se utiliza esta VLAN para los laboratorios, la subred utilizada es la 10.10.185.0/24, con NMAP se encontraron 2 SWITCH Cisco SG 500, los mismos son utilizados para brindar conectividad a las computadoras de los laboratorios.

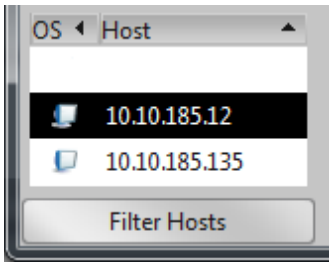


Figura 23. Switch encontrados en la VLAN de Laboratorios

Una vez hecho el descubrimiento de la Red LAN en el edificio del área de energía se ha llegado a la siguiente topología:

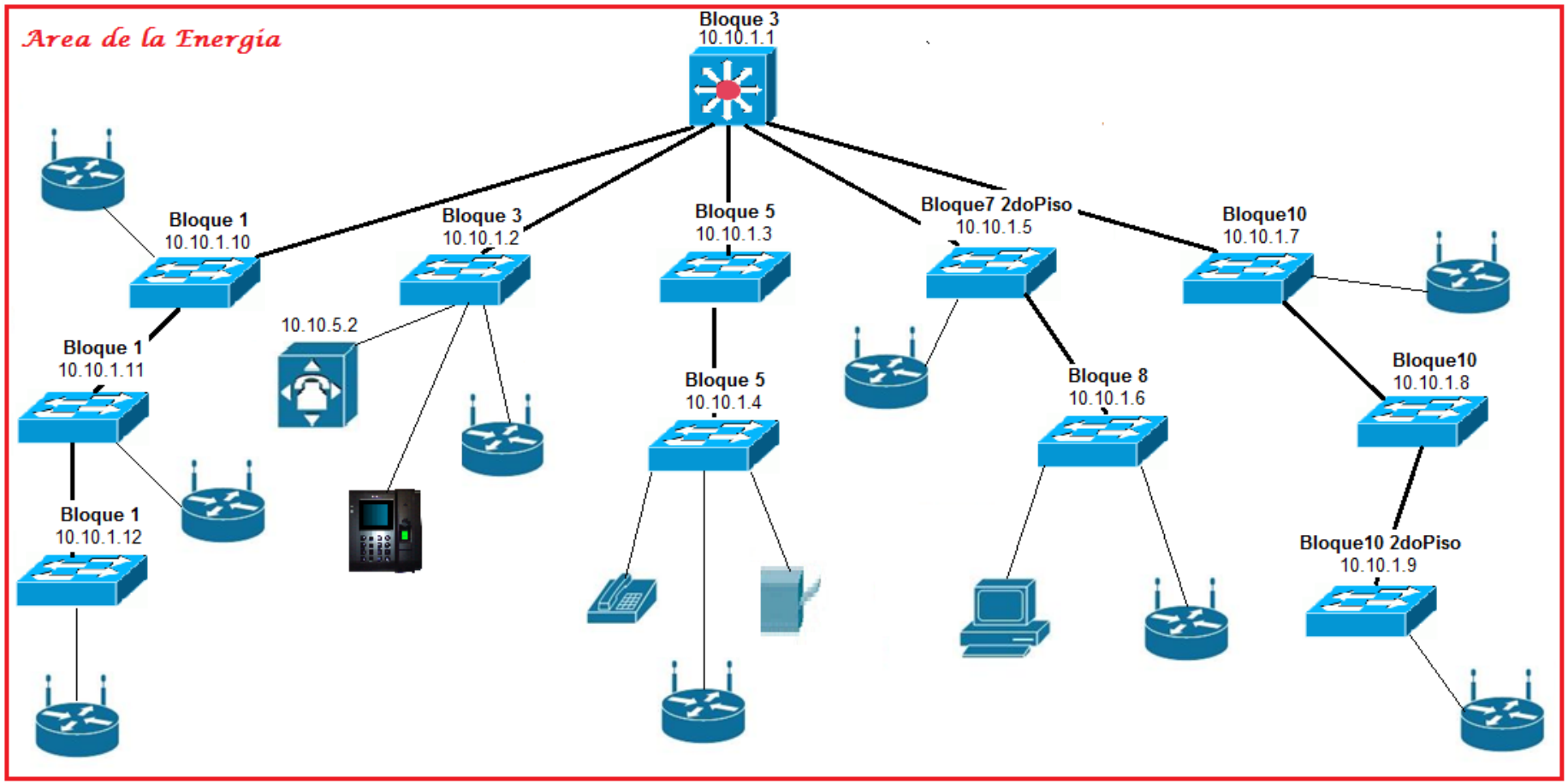


Figura 24. Topología del Área de Energía

A continuación se realiza un cuadro de figuras para un mejor entendimiento del diagrama de red (topología).

TABLA IX
CUADRO DE FIGURAS DE LOS DIAGRAMAS DE RED

Nombre	Símbolo
Switch de Capa 3	
Switch de Capa 2	
Access Point Cisco	
PBX (Servidor de Comunicaciones)	
Teléfono IP	
PC	

Impresora de red	
Reloj Biométrico	

En la tabla X se detalla la ubicación de los switch para una mejor comprensión de la topología de red del Área de Energía, presentada en la figura 24.

TABLA X
DETALLE DE LA UBICACIÓN DE LOS SWITCHES EN EL ÁREA DE ENERGÍA

IP	Bloque	Ubicación	Piso
10.10.1.1	3	EDIFICIO DIRECCIÓN RACK DOCENTES ELECTROMECÁNICA	Primero
10.10.1.2	3	EDIFICIO DIRECCIÓN RACK DOCENTES ELECTROMECÁNICA	Primero
10.10.1.3	5	COORDINACIÓN CARRERA GEOLOGÍA	Primero
10.10.1.4	5	LAB GEOLOGÍA	Primero
10.10.1.5	7	BLOQUES AULAS ELECTRÓNICA (DOCENTES SISTEMAS)	Segundo
10.10.1.6	8	EX SECRETARIA GENERAL (DOCENTES SISTEMAS)	Primero
10.10.1.7	10	BIBLIOTECA	Primero
10.10.1.8	10	BIBLIOTECA	Primero
10.10.1.9	10	SALA DOCENTES ELECTRÓNICA	Segundo
10.10.1.10	1	BIENESTAR UNIVERSITARIO	Primero
10.10.1.11	1	BIENESTAR UNIVERSITARIO	Primero
10.10.1.12	1	BIENESTAR UNIVERSITARIO	Primero

2.1.18. Inventario de los equipos de la Red LAN

De acuerdo al descubrimiento realizado se presenta un inventario de los equipos de red encontrados en la red del Área de Energía.

TABLA XI
INVENTARIO DE LOS EQUIPOS DE RED DEL ÁREA DE ENERGÍA

Equipo de Red	Cantidad
SW-L3-CISCO WS-C3750X-24	1
SW-L3-CISCO WS-C3750X-48PF-S	1
SW Cisco Catalyst 2960	19
Teléfono IP GRANDSTREAM	11
Servidor Elastix	1
Relojes Biométricos	6
Impresoras	6
Cámaras IP	14
AP CISCO	19
AP Linksys	7
AP D-Link	1

2.1.19. Direccionamiento IP de la Red LAN

A continuación se detalla el direccionamiento de la Red LAN del Área de Energía, donde se puede apreciar el direccionamiento IP del Área de Energía y del Edificio de Laboratorios.

TABLA XII
DIRECCIONAMIENTO IP DEL ÁREA DE ENERGÍA

DISPOSITIVO	NOMBRE VLAN	ID VLAN	RED / PREFIJO	MASCARA	GATEWAY/SVI
	SUBREDES: 10.10.0.0/20 – 10.30.0.0/20				
SW-L3-ENERGIA_1.0 CISCO WS-C3750X-24 10.10.1.1	ENLACE	ROUTE	10.10.0.0/30	255.255.255.252	10.10.0.1
	DEFAULT	1	10.10.1.0/24	255.255.255.0	10.10.1.1
	ADMINISTRATIVO	10	10.10.2.0/23	255.255.254.0	10.10.2.1
	DOCENTES	20	10.10.3.0/24	255.255.255.0	10.10.3.1
	ESTUDIANTES	30	10.10.4.0/24	255.255.255.0	10.10.4.1
	TELEFONIA	40	10.10.5.0/24	255.255.255.0	10.10.5.1
	IMPRESORAS-RELOJ	50	10.10.6.0/24	255.255.255.0	10.10.6.1
	CAMARAS	60	10.10.7.0/24	255.255.255.0	10.10.7.1
	LABORATORIOS	70	10.10.8.0/24	255.255.255.0	10.10.8.1
	BIBLIOTECA	120	10.10.14.0/24	255.255.255.0	10.10.14.1
	WIRELESS-NO	200	10.10.12.0/23	255.255.254.0	10.10.12.1
	WIRELESS	210	10.30.0.0/20	255.255.240.0	10.30.0.1

Edificio de Laboratorios					
	SUBREDES: 10.10.176.0/20 – 10.30.176.0/20				
SW-L3-LAB-ENERGIA_1.0 CISCO WS-C3750X-48PF-S 10.10.177.1	ENLACE	ROUTE	10.10.176.0/30	255.255.255.252	10.10.176.1
	DEFAULT	1	10.10.177.0/24	255.255.255.0	10.10.177.1
	ADMINISTRATIVO	10	10.10.178.0/23	255.255.254.0	10.10.178.1
	DOCENTES	20	10.10.180.0/24	255.255.255.0	10.10.180.1
	ESTUDIANTES	30	10.10.181.0/24	255.255.255.0	10.10.181.1
	TELEFONIA	40	10.10.182.0/24	255.255.255.0	10.10.182.1
	IMPRESORAS-RELOJ	50	10.10.183.0/24	255.255.255.0	10.10.183.1
	CAMARAS	60	10.10.184.0/24	255.255.255.0	10.10.184.1
	LABORATORIOS	70	10.10.185.0/24	255.255.255.0	10.10.185.1

2.2. Escaneo de Puertos y Servicios

En esta etapa se realiza el escaneo de todos los puertos abiertos que tienen los equipos, además también se identifican los servicios que utilizan cada uno de ellos, para luego proseguir al escaneo de vulnerabilidades en aquellos que se consideren críticos.

2.2.1. Escaneo de puertos y servicios en los Switches

En los SWITCH se ha logrado identificar los siguientes puertos y servicios:

TABLA XIII.
PUERTOS ABIERTOS Y SERVICIOS EN LOS SWITCH

Puerto	Protocol	Servicio
22	Tcp	SSH
23	Tcp	TELNET
443	Tcp	HTTPS

Se ha identificado que los Switch están utilizando el servicio de telnet, el cual es utilizado para configurar los equipos remotamente, pero no es un protocolo seguro, por lo cual es necesario realizar la búsqueda de vulnerabilidades en estos equipos.

2.2.2. Escaneo de puertos y servicios en los Access Point Cisco

En cuanto se refiere a los AP de marca Cisco, la herramienta NMAP no ha identificado ningún puerto abierto y ningún servicio en estos equipos, por lo cual no hay la necesidad de realizar un escaneo de vulnerabilidades.

2.2.3. Escaneo de puertos y servicios en el servidor de Comunicaciones

En el servidor de comunicaciones se encontraron varios puertos abiertos y la utilización de varios servicios, los mismos que se detallan a continuación:

TABLA XIV
PUERTOS ABIERTOS Y SERVICIOS UTILIZADOS POR EL SERVIDOR DE COMUNICACIONES

Puerto	Protocol	Servicio
22	TCP	SSH
25	TCP	SMTP
80	TCP	HTTP
110	TCP	POP3
111	TCP	RPCBIND
143	TCP	IMAP
443	TCP	HTTPS
993	TCP	IMAP
995	TCP	POP3
2000	TCP	CISCO-SCCP
3306	TCP	MYSQL
4445	TCP	UPNOTIFYP

Como se puede evidenciar en la tabla anterior el servidor de comunicaciones tiene una variedad de puertos abiertos y tiene varios servicios, lo que puede significar que este siendo muy vulnerable, es por ello que es necesario la evaluación de este equipo.

2.2.4. Escaneo de puertos y servicios en los teléfonos IP

En los teléfonos se ha detectado que los puertos 23 y 80 se encuentran abiertos, los servicios utilizados son telnet y http, se usan protocolo que no son seguro, lo que puede representar la existencia de vulnerabilidades en este equipo, es por ello que también se evaluaran estos equipos en la siguiente fase.

2.2.5. Escaneo de puertos y servicios en las Impresoras

En las impresoras en red se ha identificado los siguientes puertos abiertos y servicios:

TABLA XV
PUERTOS ABIERTOS Y SERVICIOS UTILIZADOS POR LAS IMPRESORAS

Puerto	Protocol	Servicio
80	TCP	HTTP
427	TCP	SVRLOC
515	TCP	PRINTER
631	TCP	IPP
5200	TCP	TARGUS-GETDATA
8080	TCP	HTTP-PROXY
9100	TCP	JETDIRECT

En cuanto a las impresoras se han reportado una gran cantidad de puertos abiertos y la utilización de varios servicios, lo que puede significar la existencia de algunas vulnerabilidades de gravedad, es por eso que se consideran como equipos críticos y serán evaluados en la siguiente fase.

2.2.6. Escaneo de puertos y servicios en los Relojes biométricos

En los relojes biométricos se ha identificado el uso del servicio telnet, el cual puede producir la existencia de vulnerabilidades en este equipo, es por ello que se debe realizar la búsqueda de vulnerabilidades.

2.2.7. Escaneo de puertos y servicios en las Cámaras IP

En las cámaras se han identificado varios puertos abiertos y varios servicios los cuales puede generar la existencia de vulnerabilidades, a continuación se detallan los puertos y servicios encontrados:

TABLA XVI
PUERTOS ABIERTOS Y SERVICIOS UTILIZADOS POR LAS CÁMARAS IP

Puerto	Protocol	Servicio
21	TCP	FTP
80	TCP	HTTP
199	TCP	SMUX
443	TCP	HTTPS
554	TCP	RTSP
555	TCP	DSF
1022	TCP	SSH
8080	TCP	HTTPD

Las cámaras IP tienen varios puertos abiertos, por lo cual se los considera críticos para ser evaluados en busca de vulnerabilidades.

2.2.8. Escaneo de puertos y servicios en los Access Point Linksys

En los AP de marca Linksys se identificaron varios puertos abiertos que pueden provocar la existencia de vulnerabilidades que puedan poner en riesgo a los equipos.

TABLA XVII
PUERTOS ABIERTOS Y SERVICIOS UTILIZADOS POR LOS AP LINKSYS

Puerto	Protocol	Servicio
53	TCP	TCPWRAPPED
80	TCP	HTTP
443	TCP	HTTPS
2601	TCP	ZEBRA

Se puede apreciar que se usan protocolos no seguros y que existen puertos innecesariamente abiertos, es por eso que estos equipos se consideran como críticos y es necesario su evaluación.

2.2.9. Escaneo de puertos y servicios en los Access Point D-Link

En el AP de marca D-link se identificaron se encontraron varios puertos abiertos no seguros, los cuales generan la existencia de algunas vulnerabilidades.

TABLA XVIII
PUERTOS ABIERTOS Y SERVICIOS UTILIZADOS EN LOS AP D-LINK

Puerto	Protocol	Servicio
22	TCP	SSH
23	TCP	TELNET
80	TCP	HTTP
443	TCP	HTTPS

Se puede apreciar que se usan protocolos no seguros y que existen puertos innecesariamente abiertos, es por eso que estos equipos se consideran como críticos y es necesario su evaluación.

2.3. Escaneo de vulnerabilidades

La fase anterior proporciona una lista de equipos que se consideran críticos o sensibles para la red objetivo, estos equipos son los que finalmente se someten a evaluación en esta fase, en la que se procede a la utilización de un escáner de vulnerabilidades. Este tiene como objetivo detectar los potenciales riesgos al que están expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red objetivo. Para esta etapa se hace el uso del escáner de vulnerabilidades Nessus y OpenVas, se debe ingresar el equipo o conjunto de equipos o segmento de red a escanear (estos equipos se seleccionan a partir del primer objetivo), posteriormente estas herramientas presentan la opción de generar reportes en los que se indican con amplia descripción cada una de las vulnerabilidades encontradas y se presentan posibles soluciones.

2.3.1. Escaneo de vulnerabilidades lógicas a los equipos de red con Nessus

A continuación se detalla la manera en que la herramienta Nessus clasifica a las vulnerabilidades, es decir el factor de riesgo.

TABLA XIX.
CLASIFICACIÓN DE LAS VULNERABILIDADES SEGÚN NESSUS

Clasificación de Vulnerabilidades				
CRITICA	ALTA	MEDIA	BAJA	INFO
8 – 10	**7 - 7.9**	**4 - 6.9**	**1 - 3.9**	**0**

Las vulnerabilidades de factor de riesgo BAJAS se relacionan con aspectos de la configuración de un sistema, la cual probablemente podría ser utilizada para violar la seguridad del sistema, sin embargo no constituyen por si sola una vulnerabilidad, ya que para ser explotada, requiere de un conjunto de criterios que no necesariamente seria conseguido de forma directa por un atacante.

Las vulnerabilidades de factor de riesgo MEDIAS van asociadas a las funcionalidades disponibles en forma remota en el sistema identificado como objetivo, las cuales normalmente son utilizadas por los atacantes informáticos para explotar otra vulnerabilidad. Es decir que este tipo de vulnerabilidades no son el objetivo final en ningún ataque, sino que dan pie o base a otras vulnerabilidades más críticas, para poder comprometer el sistema, tales como el uso de escalar privilegios.

Las vulnerabilidades de factor de riesgo ALTAS son las que pueden ser usadas para obtener acceso a recursos que deberían estar protegidos en el host remoto. Estas vulnerabilidades como tal comprometen el sistema afectado, ya que si son explotadas por un atacante, este conseguirá el control parcial o total del sistema, además de que podrá ver y cambiar información confidencial y ejecutar comandos y programas en el equipo afectado.

Las vulnerabilidades de factor de riesgo CRÍTICAS son similares a las de factor de riesgo ALTAS, sin embargo estas suelen ser más peligrosas y requieren de la evaluación y corrección por parte de los administradores de informática de forma inmediata.

Las vulnerabilidades de tipo INFORMATIVAS no representan ningún riesgo a los equipos, pero si permiten que un atacante obtenga información del equipo.

Las vulnerabilidades que tengan un factor de riesgo CRÍTICO Y ALTO son a los cuales se les da mayor prioridad al momento de realizar el plan de mitigación, en caso de no existir este tipo de vulnerabilidades, se analizan las de nivel MEDIO.

- **VLAN Default: GESTIÓN EQUIPOS DE RED**

En la figura 25 se puede apreciar 12 hosts que Nessus encontró en la VLAN 1 del área de Energía, los cuales fueron escaneados para comprobar si cuentan con vulnerabilidades.

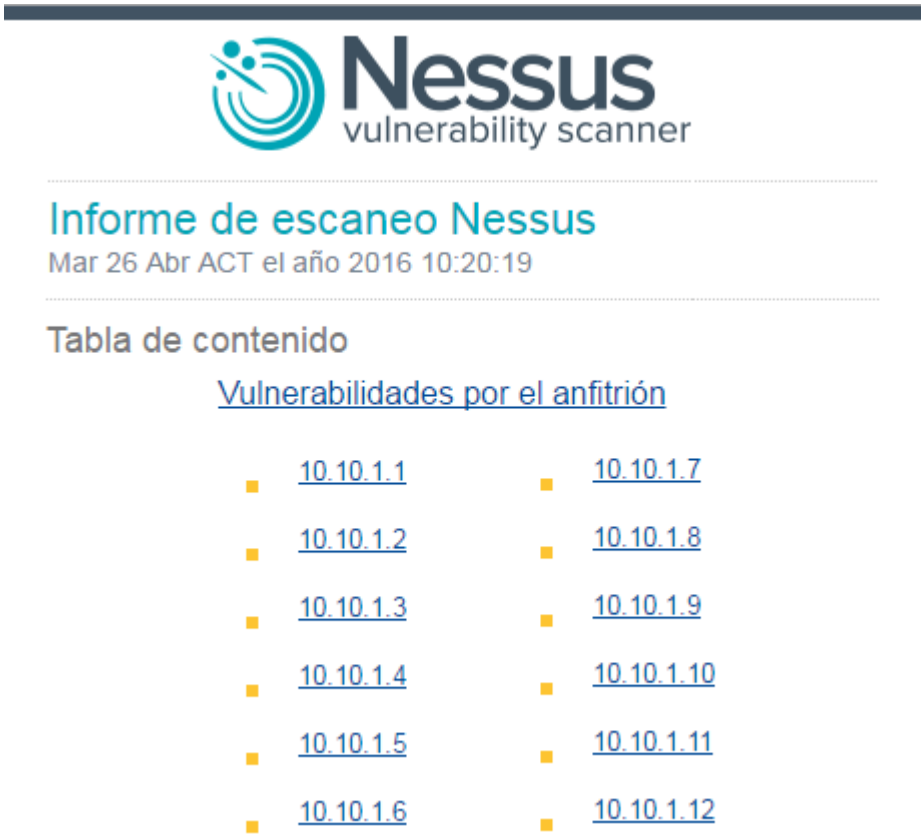


Figura 25. Hosts de la VLAN 1 detectados con Nessus

Solamente con ver el color de la viñeta de cada host, podemos hacernos idea del nivel del riesgo que tiene cada equipo, en la figura 25 podemos ver que los 12 SWITCH no cuentan con vulnerabilidades altas o críticas, solamente medias y/o bajas, esto es debido que el color de la viñeta es amarrillo que representa al factor de riesgo MEDIO.

Se coge como ejemplo 2 SWITCH, debido a que todos cuentan con la misma configuración y son de la misma marca.

En la figura 26 se puede observar que el tiempo de escaneo estuvo alrededor de los 8 minutos, además una información general del host y por supuesto los resultados de las vulnerabilidades encontradas.

Nessus ha encontrado un total de 39 vulnerabilidades de las cuales 9 tiene un riesgo medio, 3 son de riesgo bajo y 27 son de información.

10.10.1.1	
scan Información	
Hora de inicio:	Mar Abr 26 de 2016 10:12:23
Hora de finalización:	Mar Abr 26 de 2016 10:20:13
Información de host	
IP:	10.10.1.1
OS:	Cisco IOS, Cisco IOS XE

Resumen de resultados

Crítico	Alto	Medio	Bajo	información	Total
0	0	9	3	27	39

Figura 26. Vulnerabilidades del SWITCH De Distribución

Las vulnerabilidades que tiene un factor de riesgo MEDIO, encontrados en los SWITCH son los siguientes:

TABLA XX
VULNERABILIDADES EN LOS SWITCH

Vulnerabilidad	Descripción	Puerto
Uso del servicio Telnet	El servicio Telnet transmite el trafico sin cifrar, es decir los comando se transfieren en texto plano. Esto permite a un atacante escuchar a escondidas una sesión Telnet para obtener credenciales u otra información sensible y modificar el tráfico entre cliente y el servidor.	23/tcp
Certificado SSL no confiable	El certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host.	443/tcp
Certificado SSL utiliza un algoritmo de hash débil	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hash criptográfica débil (por ejemplo, MD2, MD4, MD5 o SHA1). Estos algoritmos de firma con conocidos por ser vulnerables a los ataques de colisión.	443/tcp
SSL usa conexiones SSL 2.0 y/o SLL 3.0	Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques man-in-the-middle o para descifrar las comunicaciones entre el servicio y los clientes afectados.	443/tcp
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	El host remoto se ve afectado por una vulnerabilidad man-in-the-middle (MitM) la divulgación de información conocido como POODLE. La vulnerabilidad se debe a la forma en la que SSLv3se encarga de bytes de relleno al momento de descifrar mensajes cifrados, usando cifrados de bloque, donde los atacantes puede descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos.	443/tcp

En la figura 27 podemos apreciar los resultados del escaneo de un segundo Switch, donde se puede identificar que los resultados son similares a las del Switch anterior y a las de todos los Switches escaneados.

10.10.1.7					
scan Información					
Hora de inicio:	Mar Abr 26 de 2016 10:12:23				
Hora de finalización:	Mar Abr 26 de 2016 10:19:43				
Información de host					
IP:	10.10.1.7				
OS:	Cisco IOS, Cisco IOS XE				
Resumen de resultados					
Crítico	Alto	Medio	Bajo	información	Total
0	0	9	2	26	37

Figura 27. Resultados del Escaneo de Vulnerabilidades de un SWITCH

El escaneo en la VLAN 1 con la herramienta Nessus detecto 12 Switch, en los cuales se identificaron varias vulnerabilidades, pero ninguna presenta un riesgo alto, sino de riesgo medio y bajo. Nessus no identifico los Access Point Cisco que pertenecen a la misma VLAN.

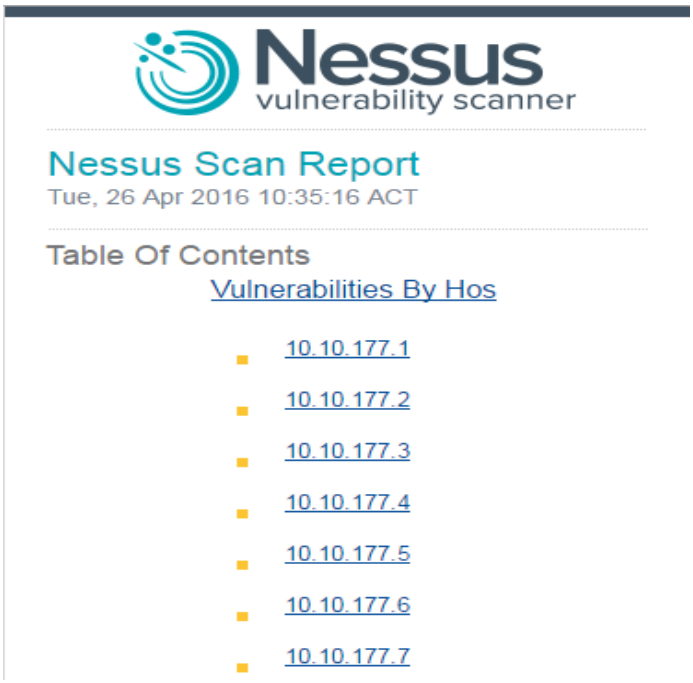


Figura 28. Hosts encontrados en la VLAN 1 del Edificio con Nessus

Nessus reportó que los hosts de la VLAN 1 tienen un total de 36 vulnerabilidades cada uno, de las cuales 8 tienen un factor de riesgo MEDIO y 2 un factor de riesgo BAJO, mientras que las 26 restantes son vulnerabilidades informativas que no afectan de ninguna manera al equipo de red.

Todos los hosts encontrados son SWITCH como se puede apreciar en la figura 29 y 30.

10.10.177.1					
Scan Information					
Start time:	Tue Apr 26 10:30:31 2016				
End time:	Tue Apr 26 10:34:54 2016				
Host Information					
IP:	10.10.177.1				
OS:	CISCO IOS, Cisco IOS XE				
Results Summary					
Critical	High	Medium	Low	Info	Total
0	0	8	2	26	36

Figura 29. Vulnerabilidades en el SWITCH DE DISTRIBUCION Del Edificio

10.10.177.4					
Scan Information					
Start time:	Tue Apr 26 10:30:31 2016				
End time:	Tue Apr 26 10:34:18 2016				
Host Information					
IP:	10.10.177.4				
OS:	CISCO IOS, Cisco IOS XE				
Results Summary					
Critical	High	Medium	Low	Info	Total
0	0	8	2	26	36

Figura 30. Vulnerabilidades en los SWITCH DE ACCESO del Edificio

Nessus encontró las mismas vulnerabilidades de factor de riesgo MEDIO en los SWITCH del Edificio de Laboratorios como en los demás SWITCH del Área de Energía, esto se puede ver en la figura 31.

23/tcp	
	42263 - Unencrypted Telnet Server
	11219 - Nessus SYN scanner
	10335 - Nessus TCP scanner
	22964 - Service Detection
	10281 - Telnet Server Detection
443/tcp	
	51192 - SSL Certificate Cannot Be Trusted
	57582 - SSL Self-Signed Certificate
	35291 - SSL Certificate Signed Using Weak Hashing Algorithm
	20007 - SSL Version 2 and 3 Protocol Detection
	42873 - SSL Medium Strength Cipher Suites Supported
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
	78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Figura 31. Vulnerabilidades de los SWITCH del Edificio de Laboratorios

Es por ello que no es necesario una explicación de las vulnerabilidades encontradas en estos SWITCH, debido a que ya se las realizo anteriormente en la TABLA XX.

De igual manera que el caso anterior la herramienta no identifico los Access Points Cisco encontrados en el descubrimiento de red.

Anteriormente los Access Point no ofrecían un servicio estable, lo cual era una incomodidad para los estudiantes y docentes del Área, el problema radicaba que existía un solo AP por cada edificio, donde cada edificio contaba con más de 4 paralelos de estudiantes, por lo cual un solo AP no abastecía a todos los usuarios, actualmente existe un Access Point por piso, con esto se ha logrado descongestionar el tráfico que manejaba en único AP anteriormente, pero no se ha solucionado el problema en su totalidad debido al consumo de ancho de banda por los estudiantes del Área.

- **VLAN 40 para Telefonía**

La herramienta utilizada encontró una variedad de hosts, los mismos que se someten al escaneo de vulnerabilidades, en la siguiente imagen podemos apreciar todos los hosts encontrados;

Figura 32. Hosts encontrados por Nessus en la VLAN de telefonía

Y en el Edificio de Laboratorios se encontraron los siguientes equipos;

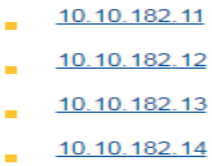


Figura 33. Hosts encontrados por Nessus en la VLAN de telefonía del Edificio de Laboratorios

En el descubrimiento de la Red se identificó la existencia de un servidor en la VLAN de telefonía, el cual tiene asignado la dirección IP 10.10.5.2, la herramienta Nessus también identifico al servidor y se le realizo el respectivo escaneo de vulnerabilidades, obteniendo los siguientes resultados.

10.10.5.2					
Scan Information					
Start time:	Tue Apr 26 11:24:16 2016				
End time:	Tue Apr 26 11:26:18 2016				
Host Information					
IP:	10.10.5.2				
OS:	Linux Kernel 2.6 on CentOS release 5				
Results Summary					
Critical	High	Medium	Low	Info	Total
0	0	11	4	93	108

Figura 34. Escaneo de Vulnerabilidades en Servidor de telefonía

La herramienta nos muestra el Sistema Operativo en el que el servidor corre, el cual es Centos 5, además encontró un total de 108 vulnerabilidades, 11 de factor de riesgo medio, 4 de factor de riesgo bajo y 93 vulnerabilidades informativas.

Las vulnerabilidades informativas nos permiten conocer las características de los equipos escaneados, es por ello que se pudo identificar que el host escaneado es un Servidor de Comunicaciones Elastix, esto gracias a los plugins de Nessus.

4569 / UDP
20834 - Inter-Asterisk Intercambio de detección de Protocolo
Sinopsis
El sistema remoto se está ejecutando un servidor que habla del Inter-Asterisk Exchange Protocol.
Descripción
El protocolo Inter-Asterisk conmutación (IAX2) es utilizado por el servidor de Asterisk PBX y otros clientes de telefonía IP / servidores que permiten la comunicación de voz entre ellos.
Solución
Si es posible, filtrar las conexiones entrantes al puerto de modo que se usa sólo por fuentes de confianza.
Factor de riesgo
Ninguna

Figura 35. Identificación del servidor Elastix

El servidor no cuenta con vulnerabilidades de nivel alto y/o críticas, por lo que no se encuentra tan expuesto, pero tiene 11 vulnerabilidades que pueden afectar en un futuro al servidor. A continuación se describen las vulnerabilidades de mayor puntuación;

TABLA XXI
VULNERABILIDADES ENCONTRADAS POR NESSUS EN EL SERVIDOR DE COMUNICACIONES

Vulnerabilidad	Descripción	Puerto
SSH Algoritmos Débiles	El servidor SSH remoto está configurado para permitir los algoritmos de cifrado débiles.	22/tcp
HTTP/TRACE	El servidor web remoto es compatible con los métodos de trazas y / o la pista. Seguimiento y rastreo son métodos HTTP que se utilizan para las conexiones de servidor de depuración web.	80/tcp
Caducidad del certificado SSL	El certificado SSL del servidor remoto ya ha expirado.	443/tcp
Transport Layer Security (TLS). Vulnerabilidad CRIMEN	El servicio remoto tiene una de las dos configuraciones SSL / TLS que puede hacer que sea vulnerable al ataque del crimen. TLS anuncia el protocolo SPDY anteriores a la versión 4.	443/tcp
Certificado SSL no confiable	Facilita llevar a cabo el ataque MitM	443/tcp
SSL usa conexiones SSL 2.0 y/o SLL 3.0	Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques man-in-the-middle o para descifrar las comunicaciones entre el servicio y los clientes afectados.	443/tcp
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	El host remoto se ve afectado por una vulnerabilidad man-in-the-middle (MitM) la divulgación de información conocido como POODLE. La vulnerabilidad se debe a la forma en la que SSLv3se encarga de bytes de relleno al momento de descifrar mensajes cifrados, usando cifrados de bloque, donde los atacantes puede descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos.	443/tcp

Mediante el descubrimiento de red se pudo identificar los teléfonos IP que existen en el Área de Energía y en el edificio de laboratorios.

A continuación presentamos los resultados del escaneo de vulnerabilidades de un teléfono realizado con Nessus, donde podemos apreciar que solamente cuenta con una vulnerabilidad de factor de riesgo medio y cuenta con 14 vulnerabilidades de tipo informativas, las cuales no representa ningún riesgo para el host.

10.10.5.11

scan Información

Hora de inicio:	Mar Abr 26 de 2016 11:24:16
Hora de finalización:	Mar Abr 26 de 2016 11:26:49

Información de host

IP:	10.10.5.11
OS:	Impresora EPSON Stylus, Linksys Wireless Access Point, Director de Oracle Integrated Lights Out

Resumen de resultados

Crítico	Alto	Medio	Bajo	información	Total
0	0	1	0	14	15

Figura 36. Vulnerabilidades encontradas en un Teléfono IP con Nessus

Como se puede observar en la figura 36, los resultados de la identificación del SO no es precisa, sino que nos presenta una variedad de posibles sistemas operativos.

Tanto los teléfonos IP del Edificio de Laboratorios como los restantes del Área de Energía reportan que solamente cuentan con una vulnerabilidad media, la cual es el uso del servicio TELNET, debido a que este servicio transmite los datos sin cifrar.

TABLA XXII
VULNERABILIDAD ENCONTRADA EN LOS TELÉFONOS IP

Vulnerabilidad	Descripción	Puerto
Uso del servicio Telnet	El host hace uso del servicio telnet a través de un canal no cifrado, lo cual permite que un atacante escuche a escondidas en una sesión telnet, obteniendo información sensible e incluso modificar el tráfico.	23/tcp

Nessus nos muestra que es posible el inicio de una sesión mediante telnet, esto se puede apreciar en la siguiente imagen;

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
Grandstream GXP1400 Command Shell Copyright 2011
Password:
------------------------------ snip ------------------------------
```

Figura 37. Sesión Telnet para el acceso a un Teléfono IP

Los demás host encontrados son computadoras, las mismas que no deben pertenecer a esta VLAN.

10.10.5.88

Host Information

Netbios Name:	COORDINACIONFIN
IP:	10.10.5.88
MAC Address:	2c:41:38:b5:bd:af
OS:	Microsoft Windows 8 Pro

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	2	0	35	38

Figura 38. Computadora de Coordinación en VLAN de Telefonía

10.10.5.93	
Host Information	
Netbios Name:	BODEGA
IP:	10.10.5.93
MAC Address:	00:16:76:17:6e:bd
OS:	Microsoft Windows XP, Microsoft Windows XP for Embedded Systems

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	22	24

Figura 39. Computadora de Bodega en VLAN de Telefonía

En las figuras 38 y 39 se muestra el reporte de Nessus, donde identifico varias computadoras que pertenecen a la VLAN de Telefonía, cuando estas deben pertenecer a otras VLAN. El problema yace que el punto de internet para el teléfono también es usado para ofrecer conectividad a una computadora y/o se utiliza al teléfono como un Switch para brindar conectividad a un PC.

- **VLAN 50 para Impresoras y Relojes Biométricos**

En la figura 40 se muestran los hosts encontrados por Nessus, donde a simple vista se puede deducir la existencia de vulnerabilidades de alto riesgo.

- 10.10.6.4
- 10.10.6.5
- 10.10.6.11
- 10.10.6.12
- 10.10.6.13
- 10.10.6.14
- 10.10.6.15
- 10.10.6.16

Figura 40. Hosts encontrados por Nessus en las VLAN 50

En el descubrimiento de red se identificó 2 relojes biométricos, los mismos que son escaneados en busca de vulnerabilidades, obteniendo los siguientes resultados:

10.10.6.4

Scan Information

Start time:	Tue Apr 26 09:30:49 2016
End time:	Tue Apr 26 09:32:45 2016

Host Information

IP:	10.10.6.4
MAC Address:	00:20:4a:61:df:9a
OS:	Lantronix Universal Device Server UDS1100

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	0	0	12	13

Figura 41. Reporte de Vulnerabilidades de Nessus de un Reloj Biométrico

Nessus reporto la existencia de una vulnerabilidad con factor de riesgo alto, la cual puede poner en riesgo al Reloj Biométrico. Mientras que en el segundo Reloj Biométrico no se detectaron vulnerabilidades.

En el edifico de laboratorios se encontraron 4 control de acceso, los mismos que fueron escaneados en busca de vulnerabilidades, obteniendo como resultado la existencia de una vulnerabilidad de factor de riesgo medio (ver figura 42).

10.10.183.11

Host Information

IP:	10.10.183.11
OS:	EPSON Stylus Printer, Linksys Wireless Access Point, Oracle Integrated Lights Out Manager

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	9	10

Figura 42. Reporte de Vulnerabilidades de Nessus en los Controles de Acceso del Edificio de Laboratorios

A continuación se describe las vulnerabilidades encontradas en los relojes biométricos del Área de Energía.

TABLA XXIII
VULNERABILIDADES ENCONTRADAS EN LOS RELOJES BIOMÉTRICOS CON NESSUS

Vulnerabilidad	Descripción	Puerto
El nombre de comunidad SNMP puede ser adivinado	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP. Un atacante puede utilizar esta información para obtener más conocimientos sobre el host, o para cambiar la configuración del sistema.	161/udp
Uso de Telnet	El servidor Telnet transmite el tráfico sin cifrar, lo que permite que atacantes puedan obtener credenciales u otra información sensible e incluso modificar el tráfico con un ataque MitM.	23/tcp

En cuanto a las impresoras, el reporte de Nessus nos indica que en 4 impresoras solo existe una vulnerabilidad de factor de riesgo alto, siendo la misma vulnerabilidad en las 4 impresoras. Mientras que en las impresoras restantes se encontraron 6 vulnerabilidades de factor de riesgo medio, 1 de factor de riesgo bajo y una de factor de riesgo alto.

A continuación se describen las vulnerabilidades encontradas en las impresoras que funcionan en el Área de la Energía.

TABLA XXIV
VULNERABILIDADES ENCONTRADAS CON NESSUS, EN LAS IMPRESORAS DE RED

Vulnerabilidad	Descripción	Puerto
El nombre de comunidad SNMP puede ser adivinado	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP. Un atacante puede utilizar esta información para obtener más conocimientos sobre el host, o para cambiar la configuración del sistema.	161/udp
Certificado SSL no confiable	Facilita que se lleve a cabo el ataque MitM	443/tcp
Certificado SSL auto firmado	La cadena de certificados X.509 para este servicio no está firmado por una autoridad reconocida, lo que podría establecer un ataque MitM contra el host.	443/tcp
SSL usa conexiones SSL 2.0 y/o SLL 3.0	Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques man-in-the-middle o para descifrar las comunicaciones entre el servicio y los clientes afectados.	443/tcp

Se puedo evidenciar que no existe un sistema de autenticación para el acceso a la configuración de las impresoras, lo que significa que cualquier persona que conozca la dirección IP de una impresora puede configurarla remotamente sin la necesidad de realizar ningún tipo de ataque de fuerza fruta, esto es muy grave ya que cualquier persona con malas intenciones puede des configurar la impresora.

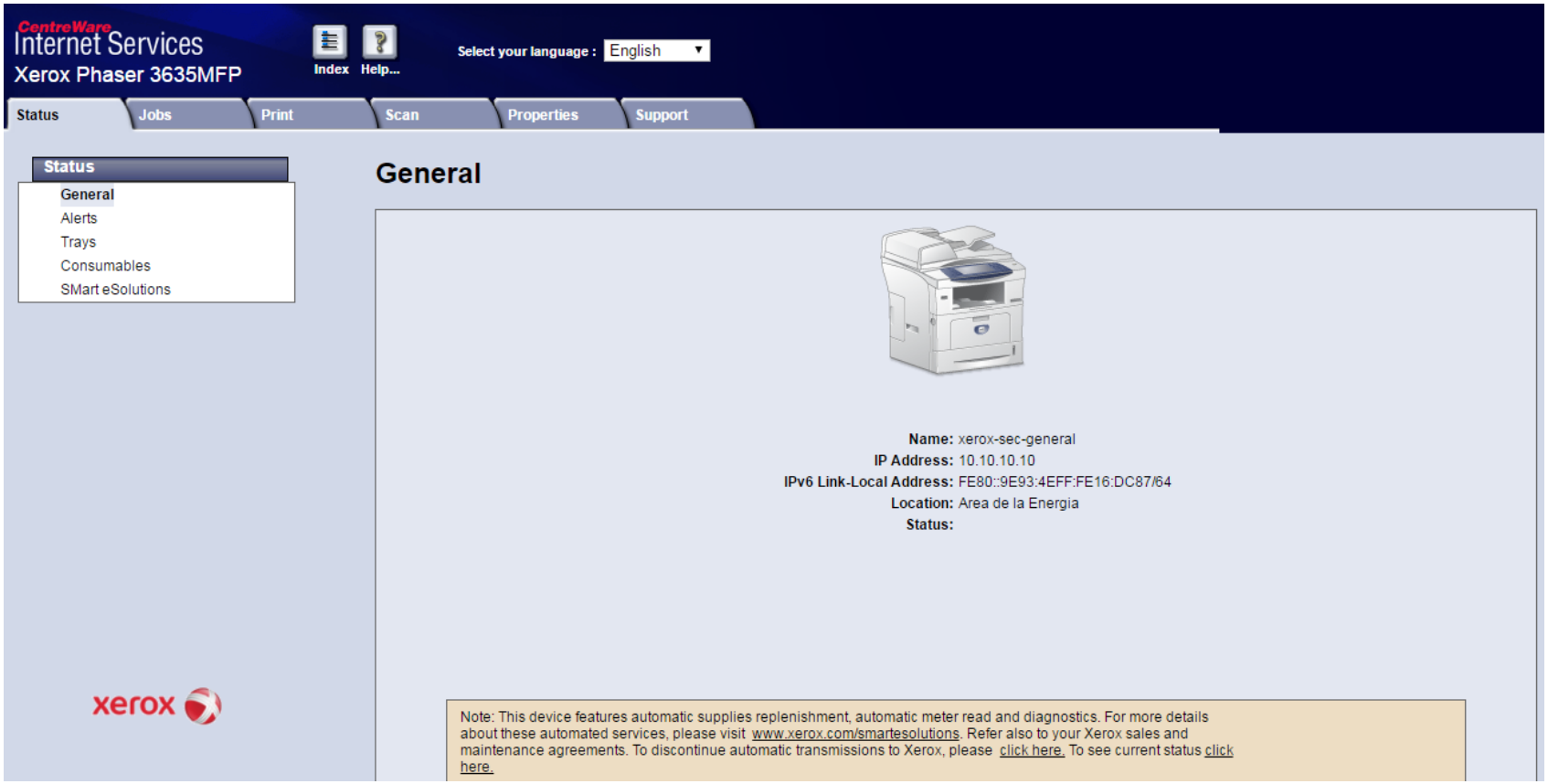


Figura 43. Acceso libre a la configuración de las impresoras

- **VLAN 60 para Cámaras IP**

Nessus identifico 14 cámaras en el Área de Energía, de las cuales 13 están ubicadas en el Edificio de Laboratorios y solamente existe una cámara en las demás departamentos del Área.

Vulnerabilities By Host

- 10.10.7.3
- 10.10.184.10
- 10.10.184.17
- 10.10.184.18
- 10.10.184.19
- 10.10.184.20
- 10.10.184.21
- 10.10.184.22
- 10.10.184.23
- 10.10.184.24
- 10.10.184.25
- 10.10.184.26
- 10.10.184.27
- 10.10.184.28

Figura 44. Cámaras IP encontradas por la herramienta Nessus

En la figura 44 se puede determinar que 2 cámaras que no cuentan con vulnerabilidades que las expongan. Esto se puede evidenciar en la figura 46

10.10.184.10

Host Information

IP:	10.10.184.10
OS:	Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	30	30

Figura 45. Reporte de Vulnerabilidades de una cámara IP, realizado con Nessus

Mientras que las demás cámaras si se encuentran expuestas a diferentes tipos de ataques, esto porque tienen al menos una vulnerabilidad de factor de riesgo alto. Nessus determino la existencia de vulnerabilidades de factor de riesgo alto, medio y bajo, esto se puede apreciar en la figura 46 y 47.

10.10.184.17	
Host Information	
IP:	10.10.184.17
MAC Address:	00:16:6c:82:6e:df
OS:	Dell iDRAC Controller, KYOCERA Printer, Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	1	0	28	30

Figura 46. Reporte de Vulnerabilidades en las cámaras IP

10.10.184.19	
Host Information	
IP:	10.10.184.19
MAC Address:	00:16:6c:7d:82:5d
OS:	Dell iDRAC Controller, KYOCERA Printer, Linux Kernel 2.6

Results Summary

Critical	High	Medium	Low	Info	Total
0	2	1	2	40	45

Figura 47. Reporte de Vulnerabilidades en las cámaras IP del Área de Energía

A continuación se describen las vulnerabilidades encontradas en las cámaras que funcionan en el Área de Energía.

TABLA XXV
VULNERABILIDADES IDENTIFICADAS EN LAS CÁMARAS IP

Vulnerabilidad	Descripción	Puerto
El nombre de comunidad SNMP puede ser adivinado	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP. Un atacante puede utilizar esta información para obtener más conocimientos sobre el host, o para cambiar la configuración del sistema.	161/udp
Dropbear servidor SSH	El host se ve afectado por una vulnerabilidad de ejecución remota de código, el host está ejecutando una versión de Dropbear SSH antes de 2012.55. Como tal, contiene un fallo que podría permitir a un atacante ejecutar código arbitrario en la maquina con privilegios de root.	1022/tcp
Reflexión DDoS SNMP 'GETBULK'	El demonio SNMP responde con una gran cantidad de datos a una solicitud 'GETBULK' con un valor más grande de lo normal para max-repeticiones, con esto un atacante puede utilizar este servidor SNMP para llevar a cabo un ataque distribuido de denegación reflejada del ataque del servicio.	161/udp
Dropbear SSH Server <2013.59 múltiples vulnerabilidades	La versión de Dropbear SSH se ejecuta en este puerto es anterior a 2.013,59. Como tal, es potencialmente afectada por múltiples vulnerabilidades: - Una vulnerabilidad de denegación de servicio causado por la forma en que el 'buf_decompress () "función maneja los archivos comprimidos.	1022/tcp

Cabe recalcar que el protocolo simple de administración de red o SNMP se encuentra vulnerable, es decir están sujetos a la fuerza bruta y ataques de diccionario para adivinar las cadenas de comunidad, cadenas de autentificación, las claves de autentificación, cadenas de cifrado o cables de cifrado.

Nessus mediante las vulnerabilidades informativas reporto que las cámaras están usando el servicio HTTP, es por ello que se ha ingresado la dirección IP de 2 cámaras para conocer si cuentan con algún tipo de seguridad, como una autentificación.

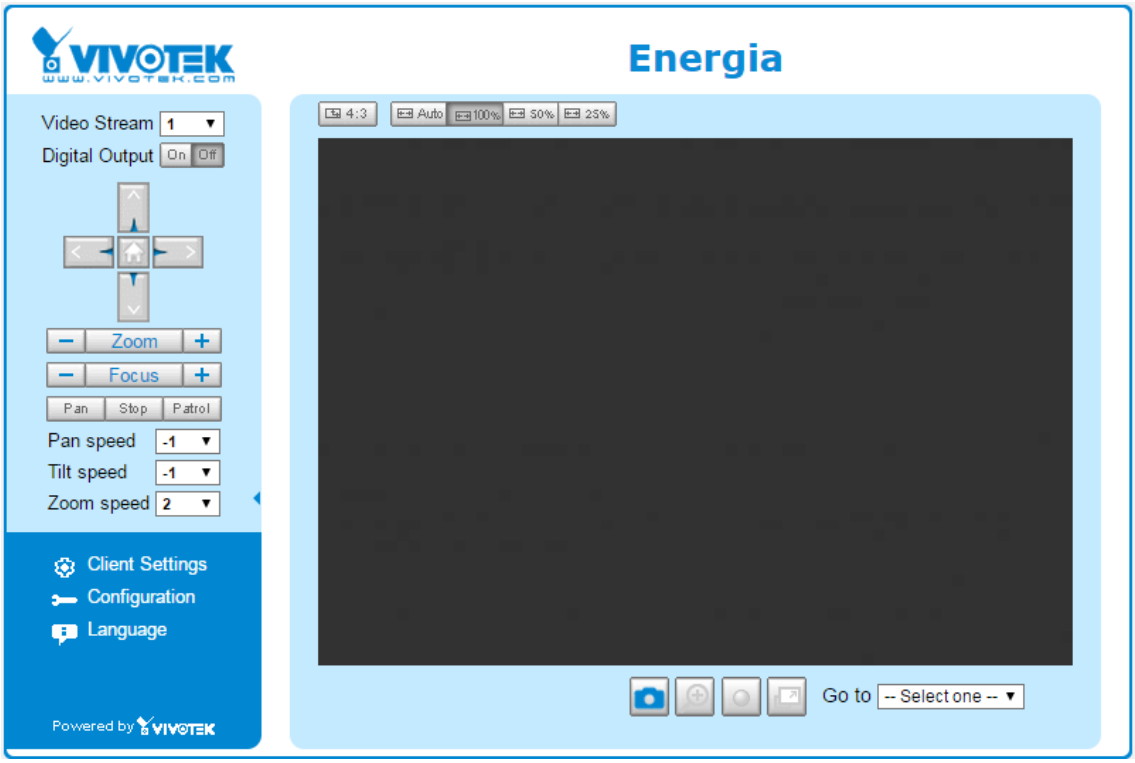


Figura 48. Página web de configuración de una cámara IP

En la figura 48 podemos apreciar la interfaz web de la única cámara existente en el Área de Energía, sin tomar en cuentas las del Edificio de Laboratorios, a la cual se puede acceder solamente poniendo la dirección IP en un navegador, es decir no cuenta con un sistema de autentificación, esto es muy grave, debido a que cualquier persona que conozca la dirección IP tenga acceso a la configuración del host y al manejo de la cámara. En cuanto a las cámaras que se encuentran instaladas en el edifico de laboratorios si cuentan son un sistema de autentificación, pero debido a las vulnerabilidades encontradas están expuestas a un ataque de fuerza bruta.

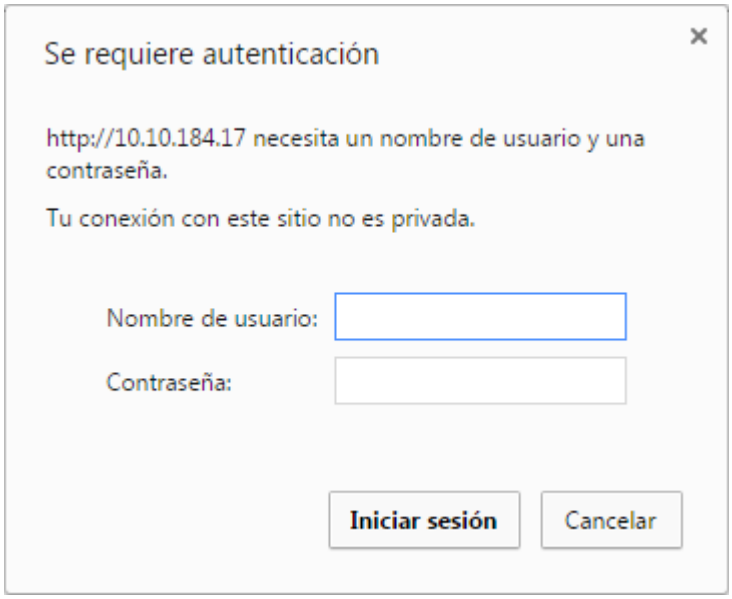


Figura 49. Sistema de Autenticación, para el ingreso a la configuración web de una cámara IP

- **VLAN 200 para la Wireless**

Esta VLAN es utilizada para la Wireless, en el descubrimiento de red se identificaron AP de marca Linksys y D-Link, los mismos que fueron escaneados en busca de vulnerabilidades y en donde se obtuvieron los siguientes resultados:

En los AP de marca Linksys se reportaron la existencia de 7 vulnerabilidad de factor de riesgo medio, las cuales pueden representar en un futuro un riesgo mucho mayor, para lo cual se ha considerado importante su análisis.

10.30.0.15

Host Information

IP:	10.30.0.15
OS:	EPSON Stylus Printer, Linksys Wireless Access Point, Oracle Integrated Lights Out Manager

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	38	45

Figura 50. Reporte de Vulnerabilidades de los AP Linksys

Mientras que en los AP de marca D-Link se reportaron 10 vulnerabilidades de factor de riesgo medio, al igual que en el caso de las vulnerabilidades de los AP Linksys es importante el analisis de estas vulenrabilidades enontradas.

10.30.0.17					
Host Information					
IP:	10.30.0.17				
OS:	D-Link Wireless Access Point				
Results Summary					
Critical	High	Medium	Low	Info	Total
0	0	10	0	28	38

Figura 51. Reporte de Vulnerabilidades del AP Sony WALL (D-LINK)

A continuación de describen las vulnerabilidades que mayor riesgo podrían llegar a significar a los equipos, es por ello que es muy importante su análisis para posteriormente poder dar una posible solución al problema y así evitar catástrofes.

TABLA XXVI
DESCRIPCIÓN DE LAS VULNERABILIDADES DE LOS AP MULTIMARCA

Vulnerabilidad	Descripción	Puerto
SSL Certificate Expiry	El certificado SSL del servidor remoto ya ha expirado	443/tcp
SSL Certificado Autofirmado	La cadena de certificados SSL no está firmado por una autoridad de certificación reconocida. Un atacante podría establecer un ataque main-in-the-middle contra el host.	443/tcp
Detección del protocolo SSLv2 y SSLv3	El servidor remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0, estas versiones se ven afectadas por varias fallas criptográficas.	443/tcp
POODLE SSLv3	El host se ve afectado por una vulnerabilidad man-in-the-middle la divulgación de información conocido como POODLE.	443/tcp
SSL cifrados medios	El host es compatible con el uso de sistemas de cifrado SSL que ofrecen encriptación de fuerza media.	443/tcp

Dropbear SSH múltiples vulnerabilidades	La versión de Dropbear SSH se ejecuta en este puerto es menor a 2.013,59, la cual es potencialmente afectada por múltiples vulnerabilidades.	22/tcp
Uso de Telnet	No es seguro el uso del servicio Telnet, ya que este transmite el tráfico sin cifrar y un atacante mediante un ataque MitM puede obtener y modificar información.	23/tcp
Vulnerabilidad XSS	El servidor web remoto se ve afectado por una vulnerabilidad de cross-site-scripting.	80/tcp
SSL de cifrado RC4	El host es compatible con el uso del sistema de cifrado RC4, el mismo que es deficiente en su generación de un flujo pseudo-aleatoria de bytes.	443/tcp
SSL cifrado débil	El host remoto es compatible con el uso de sistemas de cifrado SSL que ofrecen cifrado débil. El host remoto es compatible con el uso de sistemas de cifrado SSL que ofrecen cifrado débil.	443/tcp

2.3.2. Escaneo de vulnerabilidades lógicas a los equipos de red con OpenVas

A diferencia de Nessus en OpenVas se realiza el escaneo de vulnerabilidades a 2 equipos por VLAN, esto por el inconveniente que tiene OpenVas al momento de presentar los reportes, ya que lo hace de una forma desordenada donde se hace más complejo estar distinguiendo que vulnerabilidades pertenecen a cada equipo. A continuación se detalla la manera en que la herramienta OpenVas clasifica a las vulnerabilidades según su nivel de gravedad:

TABLA XXVII
CLASIFICACIÓN DE VULNERABILIDADES SEGÚN OPENVAS

Clasificación de Vulnerabilidades		
ALTA	MEDIA	BAJA
7 – 10	**4 - 6.9**	**1 - 2.9**

- **VLAN por Default: GESTION EQUIPOS DE RED**

Como ya se explicó anteriormente aquí es donde se encuentran los switches de acceso y los de distribución. En la herramienta OpenVas se ingresó la dirección IP de los switch de distribución tanto del Edificio de Laboratorios como el que se utiliza para el resto del Área de Energía y además 2 switch de acceso, una vez realizado el escaneo, la herramienta arrojo el siguiente reporte que se muestra en la figura 52.

Task	Severity	Scan Results				
		High	Medium	Low	Log	False Pos.
Switch de Acceso 2	6.8 (Medium)	0	4	0	15	0
Switch de Acceso	6.8 (Medium)	0	4	0	17	0
Switch de Acceso-Edificio 2	4.3 (Medium)	0	3	0	15	0
Switch de Acceso-Edificio	4.3 (Medium)	0	3	0	15	0

Figura 52. Resultado del escaneo de vulnerabilidades a los SWITCHES, con OpenVas

En la figura 52 podemos apreciar los equipos escaneados y los resultados, en donde se ha identificado la existencia de vulnerabilidades de gravedad MEDIUM, en los equipos que se encuentran en el Edificio de Laboratorios se han detectado 3 vulnerabilidades de gravedad MEDIUM y 15 log(vulnerabilidades informativas). Mientras que en los equipos que pertenecen al Área se ha identificado 4 vulnerabilidades de gravedad MEDIUM.

A continuación se detallan las vulnerabilidades de mayor riesgo identificadas en los Switch, con la herramienta OpenVas.

TABLA XXVIII
VULNERABILIDADES ENCONTRADAS EN LOS SWITCH POR OPENVAS

Vulnerabilidad	Descripción	Impacto	Puerto
OpenSSL CSS Man in the Middle Security Bypass Vulnerability	OpenSSL es propenso a la vulnerabilidad security-bypass	La obtención de información sensible mediante la realización de un ataque MitM. Esto puede conducir a otros ataques.	443/tcp
Check for SSL Weak Ciphers	El servicio SSL ofrece cifrados débiles.	Captura de información sensible con el ataque MitM	443/tcp
Deprecated SSLv2 and SSLv3 Protocol Deteccion	Se detectó el uso del servicio SSLv2 y/o SSLv3 en este sistema	Un atacante podría ser capaz de utilizar las fallas criptográficas conocidas para escuchar a escondidas la conexión entre los clientes y el servicio para obtener acceso a datos confidenciales transmitidos dentro de la conexión segura.	443/tcp
POODLE SSLv3 Protocol	Este ordenador cuenta con OpenSSL y es propenso a la vulnerabilidad de divulgación de información	Una explotación exitosa permitirá a los atacantes man-in-the-middle acceder al flujo de datos de texto sin formato. Nivel de impacto: Aplicación	443/tcp

- **VLAN 40 para Telefonía**

En esta VLAN se realiza el escaneo de vulnerabilidades al servidor VoIP y a 2 teléfonos IP con la herramienta OpenVas.

En la figura 53 podemos apreciar los resultados obtenidos con la herramienta, donde podemos observar que los teléfonos IP cuenta solamente con una vulnerabilidad de gravedad BAJA, lo cual significa que no se encuentra en riesgo, pero no se puede decir lo mismo del servidor VoIP, ya que la herramienta nos reporta la existencia de 4 vulnerabilidades de gravedad ALTA, 12 de gravedad MEDIA y 2 de gravedad BAJA, lo cual si representa un verdadero peligro para el equipo.

Task	Severity	Scan Results				
		High	Medium	Low	Log	False Pos.
TelefonosIP-Edificio	2.6 (Low)	0	0	1	10	0
Telefono IP	2.6 (Low)	0	0	1	10	0
Servidor Elastix	9.3 (High)	4	12	2	53	0

Figura 53. Reporte de Vulnerabilidades de la VLAN de telefonía

A continuación se detallan las vulnerabilidades que podrían causar mayor peligro al servidor:

TABLA XXIX
VULNERABILIDADES DEL SERVIDOR DE COMUNICACIONES ELASTIX

Vulnerabilidad	Descripción	Impacto	Puerto
MySQL 5.x Unspecified Buffer Overflow Vulnerability	MYSQL es propenso a una vulnerabilidad de desbordamiento de memoria.	Un atacante puede aprovechar este problema para ejecutar código arbitrario en el contexto de la aplicación vulnerable. Fallidos intentos de explotación dará lugar a una condición de denegación de servicio.	3306/tcp
OpenSSH Multiple Vulnerabilities	El host está ejecutando Open SSH y es propenso a múltiples vulnerabilidades.	Una explotación exitosa permitirá a un atacante obtener privilegios, para realizar ataques de suplantación de identidad, para llevar a cabo ataques de fuerza bruta o causar una denegación de servicio. Nivel de impacto: Aplicación	22/tcp
SMTP too long line	Algunos escáneres antivirus mueren cuando procesan un correo electrónico con una cadena demasiado tiempo sin saltos de línea. Dicho mensaje se ha enviado. Si hay un antivirus en su MTA, podría haberse estrellado.		25/tcp

SMTP antivirus scanner DoS	Este script envía el archivo 42.zip recursiva al servidor de correo. Si hay un filtro antivirus, puede empezar a comer enormes cantidades de CPU o la memoria.		25/tcp
Puertos innecesarios abiertos	Se ha detectado que los puertos 110, 143, 993 y 995 en los cuales funcionan los servicios POP3 e IMAP respectivamente, están activados innecesariamente, ya que no se usa en este equipo el servicio de correo electrónico.	Un atacante puede utilizar estos puertos para ingresar al servidor y causas daños graves y obtener información sensible	tcp
OpenSSL CSS Man in the Middle Security Bypass Vulnerability	OpenSSL es propenso a la vulnerabilidad security-bypass	La obtención de información sensible.	443/tcp
Php DoS	Este ordenador está instalado con php y es propenso a múltiples vulnerabilidades de denegación de servicio.	Explotando con éxito este problema permite a atacantes remotos provocar una denegación de servicio (caída de la aplicación). Nivel de impacto: Aplicación	443/tcp
OpenSSH DoS	Este ordenador se ejecuta OpenSSH y es propenso a vulnerabilidad de denegación de servicio.	Explotando con éxito este problema permite a atacantes remotos provocar una denegación de servicio. Nivel de impacto: Aplicación	22/tcp

Check if Mailserver	El servidor de correo en este host da respuestas a VRFY y / o solicitudes EXPN. VRFY y EXPN piden al servidor para obtener información acerca de una dirección. Ellos son inherentemente inutilizable a través de firewalls, gateways, intercambiadores de correo para los anfitriones a tiempo parcial, etc.		25/tcp
SSL Certification Expired	El certificado SSL del servidor remoto ya ha expirado. El certificado SSL en el servicio remoto expiró el 08/23/2014 04:17:28		443/tcp
MySQL multiple Vulnerabilites	MySQL es propenso a una vulnerabilidad security-bypass y de una vulnerabilidad de escalada de privilegios local.	Un atacante puede explotar el tema de la seguridad de la alimentación directa para eludir ciertas restricciones de seguridad y obtener información sensible que puede dar lugar a nuevos ataques. Atacantes locales pueden explotar el tema local privilegio escalada para obtener privilegios elevados en el ordenador afectado.	3306/tcp

OpenSSH Security Bypass Vulnerability	Este ordenador está funcionando OpenSSH y es propenso a la vulnerabilidad de bypass de seguridad.	Una explotación exitosa permitirá a atacantes remotos evitar las restricciones de acceso previstos. Nivel de impacto: Aplicación	22/tcp
Check for SSL Weak Ciphers	El servicio SSL ofrece cifrados débiles.	Captura de información sensible con el ataque MitM	443/tcp
Deprecated SSLv2 and SSLv3 Protocol Detection	Se detectó el uso del servicio SSLv2 y/o SSLv3 en este sistema	Un atacante podría ser capaz de utilizar las fallas criptográficas conocidas para escuchar a escondidas la conexión entre los clientes y el servicio para obtener acceso a datos confidenciales transmitidos dentro de la conexión segura.	443/tcp
POODLE SSLv3	Este ordenador cuenta con OpenSSL y es propenso a la vulnerabilidad de divulgación de información	Una explotación exitosa permitirá a los atacantes man-in-the-middle acceder al flujo de datos de texto sin formato. Nivel de impacto: Aplicación	443/tcp
Oracle MySQL Tables DoS Vulnerability	MySQL es propenso a una vulnerabilidad de denegación de servicio.	Un atacante puede explotar estas cuestiones se bloquee la base de datos, negar el acceso a los usuarios legítimos.	3306/tcp

No se está usando el firewall del servidor, con lo cual se puede conseguir una mejor seguridad en el servidor.

Cabe recalcar que la ubicación del servidor VoIP no es la adecuada, debido a que existe un departamento en la Universidad donde se ubican a los servidores.

Para verificar que el servidor de comunicaciones en realidad se encuentra en riesgo se procede a realizar un ataque MitM, en las vulnerabilidades encontradas nos indicaban que podemos aprovechar ciertas vulnerabilidades para realizar ataques y así obtener información sensible.

A continuación se realiza un ataque man-in-the-middle con el fin de ser un intermediario entre un teléfono IP y el servidor de comunicaciones y así poder escuchar las conversaciones de las llamadas que se realicen en este momento del ataque. Para ello se hace uso de la herramienta Ettercap que nos ayuda a realizar el ataque y la herramienta Wireshark que nos permite capturar el tráfico de la red.

Con la herramienta Ettercap se capturan los teléfonos conectados a la red VoIP, esto se aprecia en la siguiente figura:

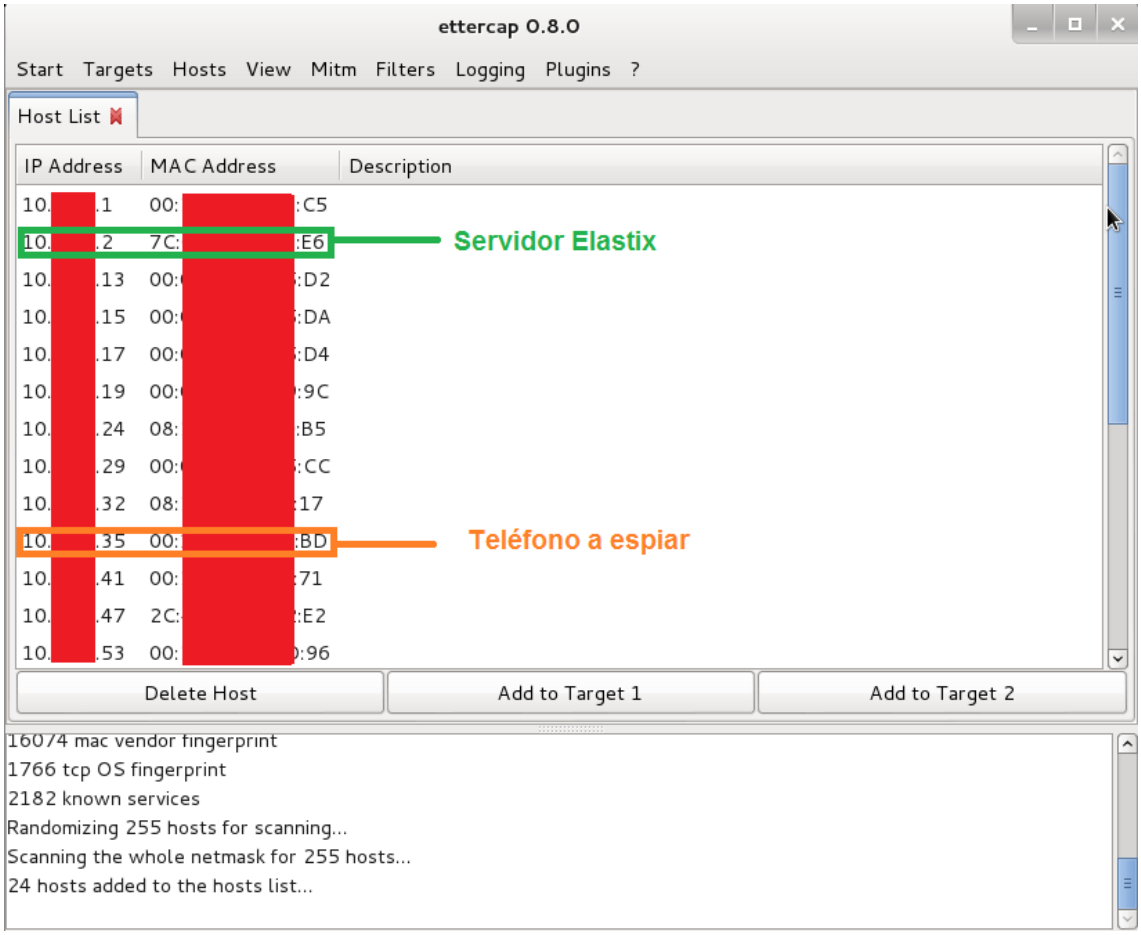


Figura 54. Teléfonos conectados a la Red VoIP

Con el uso de la misma herramienta se debe realizar un ataque MITM, teniendo como victimas al servidor Elastix y cualquier host de la red. Con la herramienta Wireshark se empieza a capturar el tráfico dirigido al servidor desde el teléfono víctima.

Se logra la captura del protocolo SIP, el cual sirve para el inicio de sesiones interactivas de usuarios. En la siguiente imagen se puede observar el origen y destino de los paquetes, el protocolo y una información, en la cual se encuentra la extensión del teléfono de donde se realiza la llamada y además la extensión o número telefónico de destino.

No.	Time	Source	Destination	Protocol	Length	Info
47285	224.933298	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
47286	224.933870	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
47291	224.948728	10.[redacted].45	10.[redacted].2	SIP	491	Status: 200 OK |
47292	224.949267	10.[redacted].45	10.[redacted].2	SIP	491	Status: 200 OK |
59827	284.954712	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
59828	284.955278	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
59833	284.971750	10.[redacted].45	10.[redacted].2	SIP	491	Status: 200 OK | Número Telefónico
59834	284.972307	10.[redacted].45	10.[redacted].2	SIP	491	Status: 200 OK |
60920	290.116419	10.[redacted].45	10.[redacted].2	SIP	533	Request: BYE sip:92582742@10.[redacted].2:5060 |
60921	290.116900	10.[redacted].45	10.[redacted].2	SIP	533	Request: BYE sip:92582742@10.[redacted].2:5060 |
60922	290.117767	10.[redacted].2	10.[redacted].45	SIP	453	Status: 200 OK |
60923	290.118220	10.[redacted].2	10.[redacted].45	SIP	453	Status: 200 OK |
61361	344.977324	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
61362	344.977932	10.[redacted].2	10.[redacted].45	SIP	569	Request: OPTIONS sip:[redacted]5@10.[redacted].45:5060 |
61363	344.990052	10.[redacted].45	10.[redacted].2	SIP	492	Status: 200 OK |
61364	344.990568	10.[redacted].45	10.[redacted].2	SIP	492	Status: 200 OK |
61852	399.505054	10.[redacted].45	10.[redacted].2	SIP/SDP	1057	Request: INVITE sip:92578220@10.[redacted].2 |
61853	399.505683	10.[redacted].45	10.[redacted].2	SIP/SDP	1057	Request: INVITE sip:92578220@10.[redacted].2 |
61854	399.506671	10.[redacted].2	10.[redacted].45	SIP	541	Status: 401 Unauthorized |
61855	399.507156	10.[redacted].2	10.[redacted].45	SIP	541	Status: 401 Unauthorized |
61856	399.518031	10.[redacted].45	10.[redacted].2	SIP	306	Request: ACK sip:92578220@10.[redacted].2 |
61857	399.518570	10.[redacted].45	10.[redacted].2	SIP	306	Request: ACK sip:92578220@10.[redacted].2 |
61858	399.560216	10.[redacted].45	10.[redacted].2	SIP/SDP	1222	Request: INVITE sip:92578220@10.[redacted].2 |
61859	399.560845	10.[redacted].45	10.[redacted].2	SIP/SDP	1222	Request: INVITE sip:92578220@10.[redacted].2 |
61860	399.562371	10.[redacted].2	10.[redacted].45	SIP	485	Status: 100 Trying |
61861	399.562951	10.[redacted].2	10.[redacted].45	SIP	485	Status: 100 Trying |
61905	403.716172	10.[redacted].2	10.[redacted].45	SIP/SDP	784	Status: 200 OK |
61906	403.716891	10.[redacted].2	10.[redacted].45	SIP/SDP	784	Status: 200 OK |
61911	403.753790	10.[redacted].45	10.[redacted].2	SIP	533	Request: ACK sip:92578220@10.[redacted].2:5060 |

Figura 55. Captura del protocolo SIP

También se logra la captura del protocolo RTP, el cual es usado para él envió de paquetes de voz, con lo cual se puede comprobar que no existe una encriptación de los paquetes, contradiciendo lo que se especificó en la entrevista realiza al encargado de la red VoIP (ver anexo 2).

No.	Time	Source	Destination	Protocol	Length	Info
61907	403.725671	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60746, Time=160, Mark
61908	403.726240	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60746, Time=160, Mark
61909	403.745634	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60747, Time=320
61910	403.746168	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60747, Time=320
61913	403.765823	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60748, Time=480
61914	403.766310	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60748, Time=480
61915	403.785947	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60749, Time=640
61916	403.786529	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60749, Time=640
61917	403.805759	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60750, Time=800
61918	403.806374	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60750, Time=800
61919	403.825745	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60751, Time=960
61920	403.826336	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60751, Time=960
61921	403.845944	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60752, Time=1120
61922	403.846475	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60752, Time=1120
61923	403.865826	10.[redacted].2	10.[redacted].45	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x63AB19E7, Seq=60753, Time=1280

Figura 56. Captura del protocolo RTP

Con la misma herramienta se puede visualizar las llamadas realizadas, se debe seleccionar una llamada y darle player para poder escucharla.

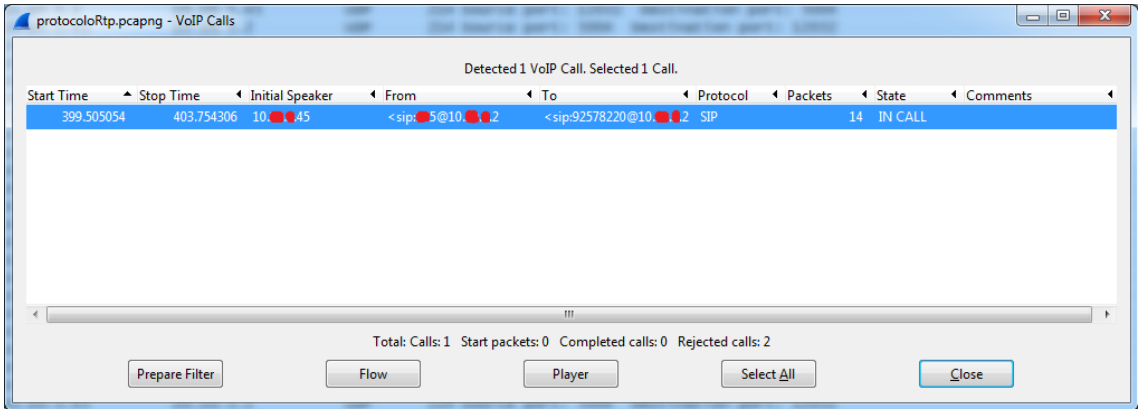


Figura 57. Llamadas realizas por la victima

Para la reproducción de la llamada es necesario seleccionar una o las dos partes que interactuaran:

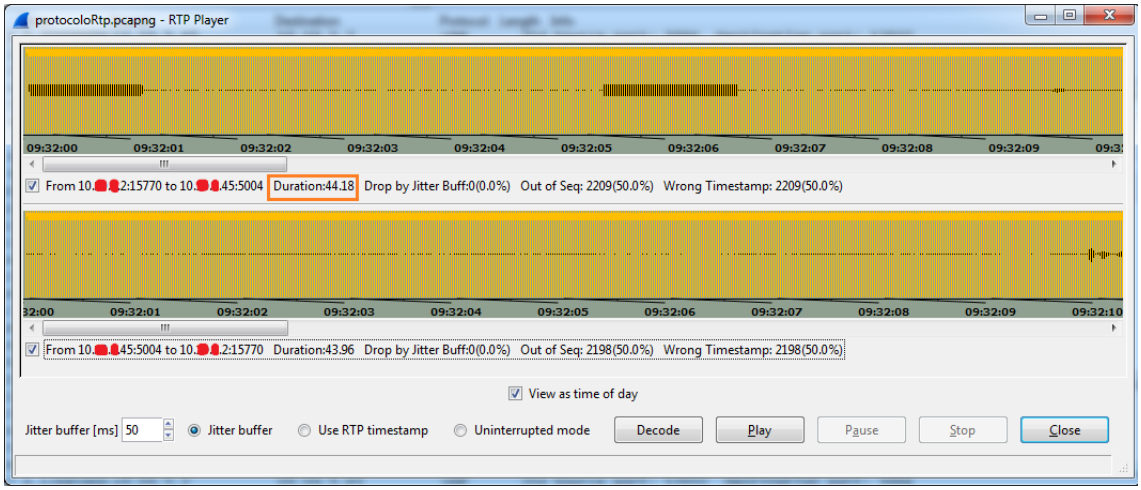


Figura 58. Reproducción de audio

Se comprobó que la vulnerabilidad existe, la cual permite interceptar una llamada y por ende escuchar las conversiones realizadas en las llamadas, esto es muy delicado, debido que en una conversación puede nombrarse claves, número de tarjetas de crédito, etc. Esta información puede ser conocida por un atacante, que no dudara en aprovechar una oportunidad, es por ello que existe un riesgo alto para los usuarios.

Además se comprobó que se puede iniciar sesión Telnet y HTTP, debido a que algunos teléfonos tienen configurado la clave que viene por default en los teléfonos IP, esto se puede apreciar en la figura 59 y 60 respectivamente.

```
root@Henry:~# telnet 10.[redacted].[redacted].23
Trying 10.[redacted].[redacted].23...
Connected to 10.[redacted].[redacted].23.
Escape character is '^]'.
Grandstream GXP1400 Command Shell Copyright 2011
Password:  Clave por defecto (admin)
GXP1400> help
Supported commands:
    config        -- Configure the device
    status        -- Show device status
    ps_status     -- Show ps command output
    phone_status    -- Show current phone basic status
    upgrade       -- Upgrade the device
    reboot        -- Reboot the device
    reset         -- Factory reset
    format mode   -- Format user data partition
         mode 0   -- Reset user data
    link          -- Show Ethernet link status
    help          -- Show this help text
    exit          -- Exit this command shell
```

Figura 59. Inicio de una sesión Telnet en un teléfono IP

Con el uso de la contraseña por defecto se tiene acceso vía telnet, lo que no debería ser permitido por que un atacante puede realizar cambios en el host e incluso cambiar la configuración. De igual manera se tuvo acceso vía HTTP ya que la contraseña es la misma.

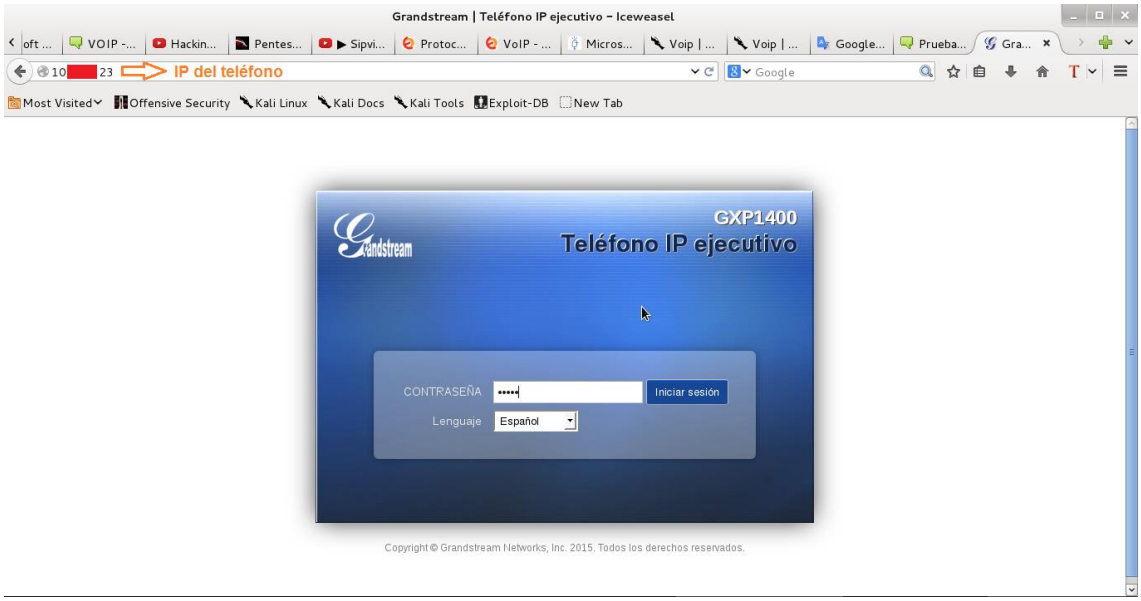


Figura 60. Inicio de una sesión vía Web (HTTP) de un teléfono IP

Significa un riesgo alto que un atacante pueda acceder mediante HTTP a un teléfono, ya que desde esta vía puede modificar la configuración y por ende dañar la configuración.

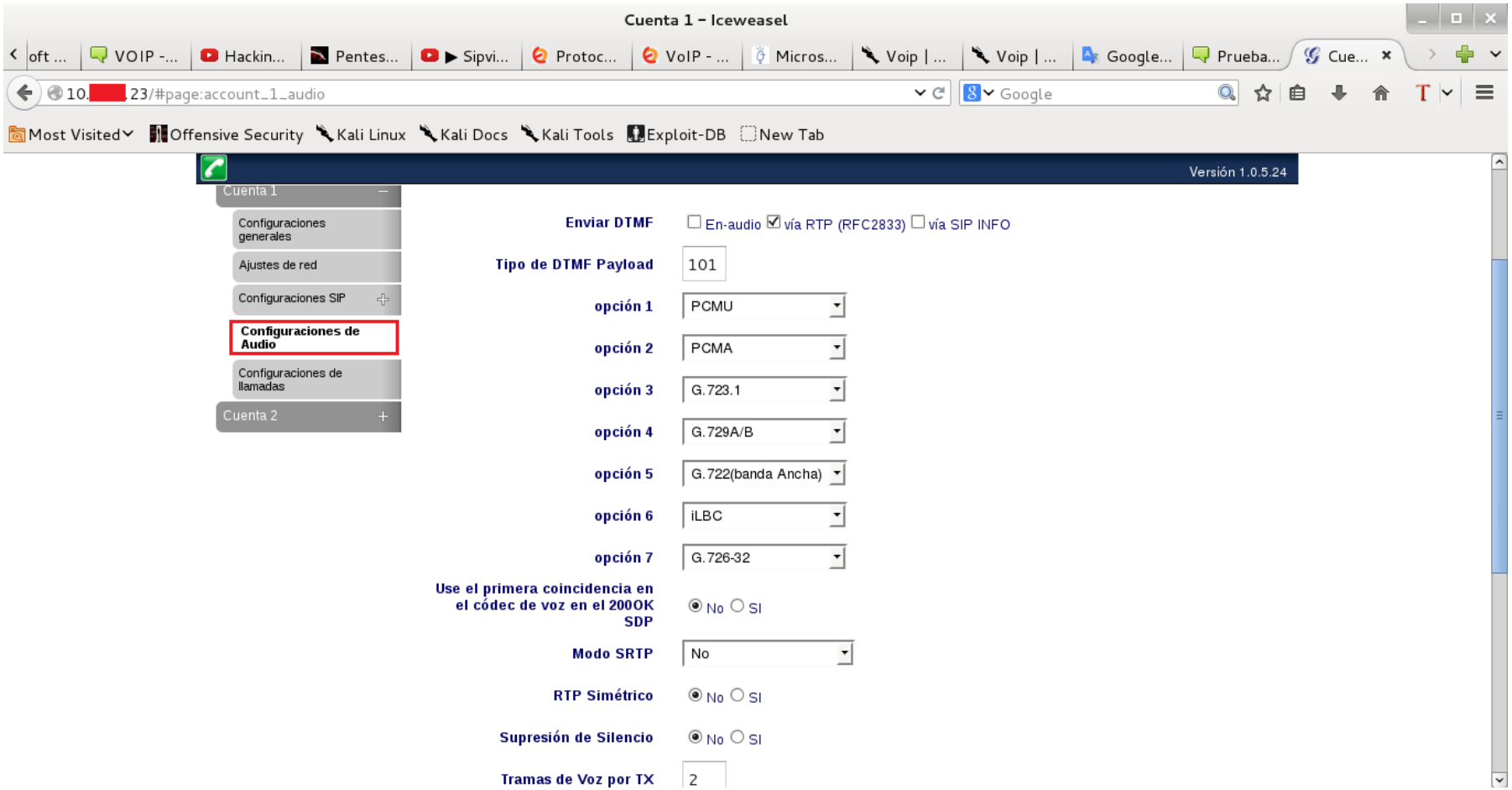


Figura 61. Página Web para la configuración de un teléfono IP

- **VLAN 50 para Impresoras y Relojes Biométricos**

La herramienta OpenVas no reportó ninguna vulnerabilidad en las impresoras que funcionan en el área de la energía, mientras que en los relojes biométricos reporto la existencia de una vulnerabilidad de gravedad ALTA en un solo reloj biométrico del área.

Task	Severity	Scan Results				
		High	Medium	Low	Log	False Pos.
Impresora 3	0.0 (Log)	0	0	0	1	0
Reloj Biometrico 2	0.0 (Log)	0	0	0	3	0
Impresora	0.0 (Log)	0	0	0	1	0
Impresora 2	0.0 (Log)	0	0	0	1	0
Reloj Biometrico	7.5 (High)	1	0	0	5	0

Figura 62. Reporte de Vulnerabilidades encontradas en la VLAN de relojes e impresoras

A continuación se describe la vulnerabilidad encontrada en el reloj biométrico:

Vulnerabilidad

Report default community names of the SNMP Agent

Resumen

Simple Network Management Protocol (SNMP) es un protocolo que puede ser utilizado por los administradores para administrar de forma remota un ordenador o dispositivo de red. En general, existen 2 modos de monitorización SNMP remoto. Estos modos son más o menos "leer" y "escribir" (o públicas y privadas).

Agente SNMP respondió como se esperaba con el nombre de comunidad: privado

Impacto

Si un atacante es capaz de adivinar una cadena pública de la comunidad, que sería capaz de leer datos SNMP desde el dispositivo remoto. Esta información puede incluir la hora del sistema, las direcciones IP, las interfaces, procesos en ejecución, etc.

Si un atacante es capaz de adivinar una cadena de comunidad PRIVADO (escritura o de 'writeall'), ellos tienen la capacidad de cambiar la información en la máquina remota. Esto podría ser un enorme agujero de seguridad, lo que permite a atacantes remotos causar estragos completos, como el tráfico de red de enrutamiento, procesos de iniciación, etc. En esencia, 'writeall' dará acceso al atacante a distancia los derechos administrativos sobre la máquina remota.

Tenga en cuenta que esta prueba sólo se recopila información y no intenta escribir en el dispositivo remoto. Así, no es posible determinar de forma automática si la comunidad reportado es público o privado.

- **VLAN 60 para Cámaras IP**

La herramienta OpenVas solamente reportó una vulnerabilidad de gravedad BAJA en la cámara IP utilizada en el área de energía, la cual no representa un riesgo para el equipo, al igual que Nessus no detectó el problema de falta de un sistema de autenticación para el ingreso a la página web de configuración de la cámara IP.

Mientras que en las cámaras IP que se encuentran en el edificio de laboratorios si se reportaron vulnerabilidades que pueden significar un riesgo a los equipos, esto se puede apreciar en la figura 63.

Task	Severity	Scan Results				
		High	Medium	Low	Log	False Pos.
CAMARA IP-EDIFICIO 1	7.5 (High)	2	1	1	19	0
CAMARA IP-EDIFICIO 2	5.0 (Medium)	0	1	1	17	0
CAMARA IP	2.6 (Low)	0	0	1	16	0

Figura 63. Reporte de Vulnerabilidades encontradas en la VLAN de cámara

TABLA XXX
DESCRIPCIÓN DE LAS VULNERABILIDADES DE LAS CÁMARAS IP

Vulnerabilidad	Descripción	Impacto	Puerto
Report default community names of the SNMP Agent	Agente SNMP respondió como se esperaba con el nombre de comunidad: público	• Capaz de leer datos SNMP • Cambiar la información en la máquina remota • Permite a atacantes remotos causar estragos completos, como el tráfico de red de enrutamiento, procesos de iniciación, etc.	161/udp
Dropbear SSH Server Use-after-free Vulnerability	Este ordenador se instala con Dropbear servidor SSH y es propenso a una vulnerabilidad del uso después de liberación.	Esta falla permite a usuarios remotos autenticados ejecutar código y de mando de derivación restricciones arbitrarias a través de múltiples solicitudes de comandos diseñados, relacionadas con los canales de concurrencia.	22/tcp
Dropbear SSH Server Multiple Security Vulnerabilities	Este ordenador se instala con Dropbear servidor SSH y es propenso a múltiples vulnerabilidades.	Los defectos permiten a atacantes remotos provocar una denegación de servicio o para descubrir los nombres de usuario válidos.	22/tcp

SNMP GETBULK Reflected DRDOS	El demonio SNMP permite a distancia (DRDOS) ataques de amplificación reflexión y distribuido	Con éxito la explotación de esta vulnerabilidad permite a los atacantes para provocar condiciones de denegación de servicio contra ordenadores remotos	161/udp

- **VLAN 210 para Wireless**

La herramienta OpenVas reportó que un Access Point Linksys cuenta con 9 vulnerabilidades de gravedad Medium y con 9 vulnerabilidades de gravedad Low, las cuales podrían llegar afectar a los equipos, en la figura x se puede observar los resultados del escaneo de vulnerabilidades del host.

Task	Severity	Scan Results				
		High	Medium	Low	Log	False Pos.
AP Multimarca	6.8 (Medium)	0	9	9	76	0

Figura 64. Reporte de Vulnerabilidades de la VLAN de Wireless

A continuación se describen las vulnerabilidades que pueden significar más peligro a los Access Point:

TABLA XXXI
DESCRIPCIÓN DE LAS VULNERABILIDADES DE LOS AP LINKSYS

Vulnerabilidad	Descripción	Impacto	Puerto
OpenSSL CSS Man in the Middle Security Bypass Vulnerability	OpenSSL es propenso a la vulnerabilidad security-bypass	La obtención de información sensible.	443/tcp
Dropbear SSH	Este ordenador se instala con Dropbear servidor SSH y es propenso a múltiples vulnerabilidades.	Los defectos permiten a atacantes remotos provocar una denegación de servicio o para descubrir los nombres de usuario válidos.	22/tcp
SSL Certification Expired	El certificado SSL del servidor remoto ya ha expirado. El certificado SSL en el servicio remoto expiró el 08/23/2014 04:17:28		443/tcp
Check for SSL Weak Ciphers	El servicio SSL ofrece cifrados débiles.	Captura de información sensible con el ataque MitM	443/tcp

Deprecated SSLv2 and SSLv3	Se detectó el uso del servicio SSLv2 y/o SSLv3 en este sistema	Escuchar a escondidas la conexión entre los clientes y el servicio para obtener acceso a datos confidenciales transmitidos dentro de la conexión segura.	443/tcp
POODLE	Este ordenador cuenta con OpenSSL y es propenso a la vulnerabilidad de divulgación de información	Una explotación exitosa permitirá a los atacantes man-in-the-middle acceder al flujo de datos de texto sin formato. Nivel de impacto: Aplicación	443/tcp

2.3.3. Identificación de vulnerabilidades físicas en la red

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.

A continuación se realiza el cálculo de los riegos, esto se lo hace de acuerdo a lo que nos indica la metodología MAGERIT, en donde el nivel de riesgo depende del nivel del impacto que genere por la probabilidad de que una amenaza pueda efectuarse exitosamente.

TABLA XXXII
CÁLCULO DEL RIESGO DE LAS AMENAZAS EXISTENTES

Amenazas	Impacto	Probabilidad	Riesgo
Incendio	3	1	3
Inundaciones	3	1	3
Terremotos	2	1	2
Robo de equipos	3	2	6
Incinerado de equipos	3	1	3
Fraude	3	1	3
Sabotaje	3	1	3

A continuación se presenta las vulnerabilidades que permiten que las amenazas puedan perjudicar a ciertos equipos en el área de energía:

- **Acceso No Controlados**

Se pudo evidenciar que algunos racks que se encuentran en el Área de la Energía no cuentan con una buena seguridad. Hay algunos racks que se encuentran en cuartos donde solo personal autorizado tiene acceso, pero actualmente los funcionarios de la Unidad de Telecomunicaciones e Información como los pasantes de la misma no

cuentan con credenciales, es decir que cualquier persona puede filtrarse como pasante con el fin de desconectar los cables de los equipos e incluso sustraer esos equipos de los rack, existen algunos rack que están alcance de todas las personas y sin vigilancia alguna, lo que ocasiona que sean vulnerables. Los seguros del rack, son fáciles de vulnerar, es decir, es fácil abrir un rack o romper un vidrio para desconectar los cables o sustraer los equipos. Los rack no cuentan con sensores o alarmas que alerten al personal encargado de los equipos de red. Hay que recalcar que los funcionarios del departamento de la UTI llevan un monitoreo de los equipos, lo que les permite saber en tiempo real el estado de conectividad de los equipos.

Figura 65. Rack utilizado en el Área de Energía

Hay que mencionar que usan reguladores de voltaje para prevenir que los equipos llegan a quemarse por un fallo eléctrico y además existe un UPS en el rack donde se encuentra el switch de distribución que además también funciona como regulador de voltaje, esto se puede corroborar en el anexo 6.

- **No existe Seguridad para los Access Point Cisco**

Los AP del Área de la Energía son vulnerables a la desconexión del cableado, debido que se encuentran al alcance de terceras personas e incluso están expuestos a un robo, ya que no cuenta con un tipo de rejilla que los proteja de ser sustraídos.

Figura 66. Access Point Cisco sin Seguridad

En la figura 66 se puede observar que no existe ningún tipo de seguridad para los AP, por lo cual es posibles desconectar el cable sin problema y dejar el equipo son conectividad e incluso se puede apreciar que se puede sustraer fácilmente el equipo.

Figura 67. Access Point sin vigilancia

- **Ubicación de los equipos**

En la fase de recolección de información se identificó la existencia de un servidor en la VLAN de telefonía, se establece primeramente que este equipo no debe pertenecer a esa VLAN y que ubicación física no es la correcta.

También se detectó que el Access Point Cisco para exteriores no está ubicado en el lugar correcto, esto causa que no se tenga una buena cobertura, la potencia no sea buena por su alejamiento.

En la figura 68 podemos apreciar el AP que es utilizado en el área para brindar conectividad a internet a los estudiantes y docentes.

Figura 68 Access Point Cisco Para Exteriores

Mientras que en la figura 69 podemos observar la ubicación del AP y lo distanciado que esta de los bloques.

Figura 69. Ubicación del Access Point Cisco para Exteriores

2.4. Comparación de los resultados de las herramientas

En este apartado se comparan los resultados de las herramientas empleadas en busca de vulnerabilidades, se lo realiza de acuerdo a los equipos escaneados.

En el artículo **"Nessus/ OpenVas Comparison test",** realizado por el Laboratorio de Systems and Signals, declara a la herramienta Nessus como la herramienta más completa, en cuanto se refiere a la búsqueda de vulnerabilidades en una red, además recalca que OpenVas no queda tan mal parada en esta comparación, llegando a la conclusión de que en caso de que no se tenga la licencia de Nessus, OpenVas viene a ser la mejor alternativa para la evaluación de vulnerabilidades.

2.4.1. Comparación de vulnerabilidades encontradas en los SWITCH

Los SWITCH fueron los primeros equipos escaneados en busca de vulnerabilidades, tanto la herramienta Nessus como OpenVas no detectaron vulnerabilidades de factor de riesgo CRITICO o de gravedad ALTA, solamente encontraron vulnerabilidades de gravedad MEDIA y BAJA.

TABLA XXXIII
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LOS SWI TCH

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
SWITCH	0	0	9	2	0	4	0	• Uso de encriptaciones débiles SSL • Uso del protocolo SSLv2 y SSLv3 • POODLE SSLv3
SWITCH Edificio de Laboratorios	0	0	8	2	0	3	0	

Conclusión: Nessus encontró más vulnerabilidades de gravedad MEDIO que OpenVas, pero ninguna herramienta encontró alguna vulnerabilidad de gravedad ALTO que puede poner en riesgo a los equipos. Ambas herramientas obtuvieron resultados similares y confirman la no existencia de vulnerabilidades de gravedad en los SWITCH del Área de Energía.

2.4.2. Comparación de vulnerabilidades encontradas en los AP CISCO

Los Access Point de marca Cisco fueron los segundos equipos en ser escaneados, estos equipos no fueron detectados por Nessus, por ello se procedió a ingresar las direcciones IP de los equipos en la herramienta.

TABLA XXXIV
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LOS AP CISCO

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
AP CISCO	0	0	0	0	0	0	0	
AP CISCO Edificio de Laboratorios	0	0	0	0	0	0	0	

Conclusión: Ninguna de las herramientas empleadas identificó ningún tipo de vulnerabilidades en los AP CISCO del Área de Energía.

2.4.3. Comparación de vulnerabilidades encontradas en los teléfonos IP

Los teléfonos IP fueron los siguientes en ser escaneados, en ellos no se encontraron vulnerabilidades que signifiquen un riesgo a los equipos.

TABLA XXXV
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LOS TELÉFONOS IP

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
Teléfonos IP	0	0	1	0	0	0	1	Ninguna
Teléfonos IP Edificio de Laboratorios	0	0	1	0	0	0	1	

Conclusión: La herramienta Nessus identifico una vulnerabilidad de factor de riesgo MEDIO, mientras que la herramienta OpenVas identifico la presencia de una vulnerabilidad de gravedad BAJO, ambas herramientas tuvieron resultados similares.

2.4.4. Comparación de vulnerabilidades encontradas en el Servidor de Comunicaciones

En la VLAN de telefonía se encuentra el servidor de comunicaciones, el cual fue escaneado con las herramientas, las mismas reportaron la existencia de varias vulnerabilidades.

TABLA XXXVI
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN EL SERVIDOR ELASTIX

Equipo	Reporte Nessus				Reporte OpenVas		
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo
Servidor Elastix	0	0	11	4	4	12	2

Conclusión: En esta ocasión los resultados de ambas herramientas no son muy similares, Nessus no reporta ninguna vulnerabilidad de factor de riesgo ALTO y/o CRITICO en el servidor, mientras que la herramienta OpenVas reportó 4 vulnerabilidades de gravedad ALTO, esto es un resulto muy variable. En cuanto a las vulnerabilidades de factor de riesgo MEDIO y BAJO si obtiene resultados similares.

2.4.5. Comparación de vulnerabilidades encontradas en los Relojes Biométricos

También se realiza un escaneo de vulnerabilidades en los relojes biométricos del área de energía, los mismos que son utilizados para el control de acceso y control de entrada y salida de los empleados de la Universidad.

TABLA XXXVII
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LOS RELOJES BIOMÉTRICOS

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
Relojes Biométricos	0	1	0	0	1	0	0	• Agente SNMP defecto Nombre de comunidad (público)
Relojes Biométricos de Laboratorios	0	0	1	0	0	0	0	

Conclusión: Los resultados de las herramientas son muy similares, ya que ambas encuentran una vulnerabilidad de gravedad ALTO en un Reloj Biométrico del Área de Energía.

2.4.6. Comparación de vulnerabilidades encontradas en las Impresoras IP

Las impresoras IP también son escaneadas en busca de vulnerabilidades, donde las herramientas reportaron vulnerabilidades que pueden poner en riesgo a los equipos.

TABLA XXXVIII
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LAS IMPRESORAS IP

Equipo	Reporte Nessus				Reporte OpenVas		
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo
Impresoras IP	0	1	6	1	0	0	0

Conclusión: En este caso las herramientas no coinciden para nada, Nessus reportó varias vulnerabilidades en las impresoras, mientras que OpenVas no reportó ninguna, esto puede ser por la falta de plugins de OpenVas.

2.4.7. Comparación de vulnerabilidades encontradas en las Cámaras IP

No podía faltar el escaneo a las cámaras IP que funcionan en el Área, las herramientas empleadas encontraron vulnerabilidades que podrían poner en riesgo a los equipos.

TABLA XXXIX
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LAS CÁMARAS IP

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
Cámaras IP	0	0	0	0	0	0	1	• Agente SNMP defecto Nombre de comunidad (público) • Dropbear SSH Server Use-after-free • Dropbear SSH Server Multiple Vulnerabilities
Cámaras IP Edificio de Laboratorios	0	2	1	2	2	1	1	

Conclusión: En las cámaras IP es donde las herramientas tienen un reporte de vulnerabilidades casi idéntico, es decir coinciden en las vulnerabilidades encontradas y en la puntuación y gravedad de las vulnerabilidades.

2.4.8. Comparación de vulnerabilidades encontradas en los Access Point Linksys y D-Link

Y por último se realiza el escaneo de vulnerabilidades en la VLAN para Wireless, en donde se encontraron Access Point de diferentes marcas, en los cuales no se identificó vulnerabilidades de mayor riesgo.

TABLA XL
COMPARACIÓN DE RESULTADOS DE LAS HERRAMIENTAS EN LOS ACCESS POINT MULTIMARCA

Equipo	Reporte Nessus				Reporte OpenVas			Vulnerabilidades Semejantes
	Critico	Alto	Medio	Bajo	Alto	Medio	Bajo	
Access Point Linksys	0	0	7	3	0	9	9	• Cifrados SSL débiles • Detection SSLv2 y SSLv3 • POODLE SSLv3 • Dropbear SSH Server multiples vulnerabilidades. • Caducidad del certificado SSL
Access Point Sony WALL (D-Link)	0	0	10	0	0	9	0	

Conclusión: En esta ocasión los reportes de ambas herramientas también tienen una gran similitud.

3. Elaboración de un Plan de Mitigación para reducir la probabilidad de que un riesgo se materialice.

Con la utilización de las herramientas Nessus y OpenVas, se han identificado la existencia de varias vulnerabilidades que ponen en riesgo a los equipos, es por ello que se plantea una solución para mitigar las vulnerabilidades encontradas, para ello se ha tomado en cuenta las soluciones que nos brindan las herramientas de escaneo.

3.1. Plan de Mitigación de Riesgos

Una vez identificadas varias vulnerabilidades en los diferentes equipos utilizados en el Área de la Energía, se propone un plan de mitigación, con el fin de amenorar las vulnerabilidades y así reducir la probabilidad del éxito de un ataque a los equipos utilizados por los usuarios.

Una vez realizado el análisis de vulnerabilidades en los diferentes equipos de red se presentan las acciones que se deben tomar frente a ellos. Se hace una recomendación para cada vulnerabilidad o también puede ser de forma general que abarquen varias vulnerabilidades.

Se les da prioridad a las vulnerabilidades que representan un mayor riesgo a los equipos, luego se proceden a las que no representan un verdadero riesgo, pero que si se deben tratar para no tener problemas a futuro con los equipos.

Una vez que se realizó el plan de mitigación se procedió solicitar un día a los funcionarios de la Unidad de Telecomunicaciones e Información para presentar los resultados obtenidos, es decir las vulnerabilidades encontradas en los equipos, donde también se socializo el plan de mitigación con el fin de revisar conjunto con los funcionarios las recomendaciones planteadas, las cuales van a ser utilizadas como base para empezar a mitigar las vulnerabilidades más graves. (Ver anexo 4 y 5).

3.1.1. Plan para Mitigar las Vulnerabilidades en los SWITCH

A continuación se dan unas recomendaciones para mitigar las vulnerabilidades encontradas en los SWITCH, debido a la no existencia de vulnerabilidades de factor de riesgo ALTAS, se ha procedido a seleccionar las vulnerabilidades de gravedad MEDIA que pueden significar un peligro en estos equipos.

TABLA XLI
PLAN DE MITIGACIÓN PARA LOS SWITCH

Vulnerabilidad	*Recomendación*
Uso del servicio HTTP	Desactivar este servicio y en su lugar usar solo el servicio HTTPS

OpenSSL CSS Man in the Middle Security Bypass Vulnerability	Actualizar la versión más reciente de OpenSSL, cabe recalcar que tanto el cliente como el servidor tiene que ser vulnerables para que el ataque sea exitoso.
	
	Procedimiento
	
	Actualizar OpenSSL a su última versión que es 1.0.2
	
	`$ sudo apt-get update`
	`$ sudo apt-get upgrade`
	
	Para comprobar que OpenSSL se ha actualizado correctamente ejecutamos el siguiente comando:
	
	`$ sudo openssl version -a`

Uso del servicio Telnet	Se recomienda desactivar el servicio **telnet** y utilizar en su lugar **SSH**.
	
	Procedimiento
	
	Editamos los puertos de acceso telnet (vty) para que sólo se permita el acceso por SSH y deshabilitar el acceso inseguro (telnet), configuramos los 16 puertos disponibles (0 al 15):
	
	`switch(config)#line vty 0 15`
	`switch(config-line)#transport input ssh`
	`switch(config-line)#login local`

SSL usa conexiones SSL 2.0 y/o SLL 3.0	Se recomienda desactivar el SSLv2 en desuso y / o SSLv3 y usar el protocolo TLSv1 o una versión superior.
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Lo mejor que podemos hacer es deshabilitarlo de inmediato. Y de paso deshabilitar también la versión 2.0 que es más antigua todavía y no es necesario utilizarla.

Se recomienda solo el uso del servicio SSH para la configuración de estos equipos, es por eso que se recomienda que se desactive el servicio HTTPS, si no se está utilizando, con lo cual se eliminarían la mayoría de vulnerabilidades encontradas en estos equipos.

3.1.2. Plan para Mitigar las Vulnerabilidades en los Access Point

Se ha concluido que un Access Point Cisco para exteriores se encuentra mal ubicado, los encargados de Redes y Telecomunicaciones de la Universidad supieron manifestar que actualmente ya cuentan con un plan para mover a una mejor ubicación al AP de exteriores. (Ver anexo 6)

En este caso se ha realizado una recomendación de las reglas básicas para la colocación AP que contribuyen a la exactitud de la ubicación:

- Proporcione la cobertura del perímetro AP.
- Asegure la suficiente densidad AP.
- Escalone los AP, determinado adentro de largo y las áreas de cobertura estrechas.
- Verifique el despliegue inalámbrico con un estudio sobre el sitio.

3.1.3. Plan para Mitigar las Vulnerabilidades en el servidor de comunicaciones

En el servidor de comunicaciones es donde más vulnerabilidades se encontraron, las mismas que ponen en riesgo al equipo, es por ello que es importante un plan para reducir las vulnerabilidades y así proteger al equipo de posibles ataques.

TABLA XLII
PLAN DE MITIGACIÓN DE VULNERABILIDADES EN EL SERVIDOR DE COMUNICACIONES

Vulnerabilidad	Recomendación
MySQL 5.x Unspecified Buffer Overflow Vulnerability	Actualizar MySQL a una versión mayor a 5.2, debido que las anteriores es vulnerables a este tipo de ataque. Cerrar el Puerto 3306/tcp para no permitir conexiones a otros equipos, y aplicar iptables. **Procedimiento** Para actualizar MySQL ingresamos el siguiente comando en el servidor: yum -y update mysql*
OpenSSH Multiple Vulnerabilities	Actualizar a OpenSSH 7.0 o posterior
Firewall Desactivado	Activar el firewall del servidor, para la creación de IPTABLES en los servicios SSH y HTTPS, con el fin de prevenir ataques de fuerza bruta.
SMTP too long line	Deshabilitar estos servicios en aquellas maquinas que no son servidores de correos.
SMTP antivirus scanner DoS	
	Cambiar las contraseñas de acceso para los protocolos TELNET y HTTP. **Procedimiento:** 1. Abra un navegador Web en su ordenador 2. Introduzca la dirección IP del teléfono en la barra de direcciones del navegador

Uso de contraseñas por default	3. Introduzca el nombre de usuario y la contraseña del administrador para acceder al menú de configuración Web. (El nombre de usuario predeterminado del administrador es "admin". La contraseña de administrador por defecto es "admin") 4. Ir a la opción de Mantenimiento y seleccionar acceso web 5. Cambiar la contraseña tanto de usuario y del administrador. 6. Al cambiar cualquier configuración, siempre guarde los cambios pulsando el botón "Guardar y Aplicar".
Puertos innecesarios abiertos	Se recomienda desactivar los servicios de POP3 e IMAP, los cuales funcionan en los puertos 110, 995, 143 y 993 respectivamente.
No hay encriptación de las comunicaciones (SIP)	Para la interceptación de llamadas y/o ataques man in the Middle se recomienda el uso de TLS, el cual proporciona privacidad y la integridad de los datos entre dos aplicaciones que se comunican.
No hay encriptación de las datos multimedia	Se recomienda no usar el protocolo RTP para transportar los datos multimedia, en su lugar utilizar el Secure Real Time Protocol (SRTP), el cual provee confidencialidad, integridad y autenticación de los datos (voz, video, mensajería, entre otros).
Puerto 80 abierto (HTTP)	Se recomienda desactivar este servicio y solo usar HTTPS
Uso del Protocolo Telnet	Se recomienda no usar este protocolo, el modelo del teléfono IP no soporta el protocolo SSH.
Ubicación del Servidor	Se recomienda que se reubique al servidor a la sala de servidores y también colocar en la VLAN correspondiente.

Php DoS	Actualizar a Php 5.5.30 o 5.6.14 o una versión posterior. **Procedimiento** Para actualizar Php ingresamos el siguiente comando dependiendo del SO: *yum upgrade (Centos)* *apt-get upgrade (Ubuntu o Debian)*

OpenSSH DoS	Actualizar a OpenSSH versión 7.1p2 o posterior
	
	Procedimiento
	
	Para actualizar OpenSSH a una versión posterior primero es necesario desinstalar el paquete proveniente de los repositorios. Para ello ejecutar:
	
	`rpm -e openssh-clients`
	`rpm -e openssh-server`
	`rpm -e openssh-askpas`
	`rpm -e openssh`
	
	Luego descargamos la nueva versión de OpenSSH y la instalamos.

3.1.4. Plan para Mitigar las Vulnerabilidades en los Relojes Biométricos

A continuación se dan unas recomendaciones para reducir la probabilidad de un ataque a los relojes biométricos y con ello se consiga proteger a los equipos e información almacenados en estos.

TABLA XLIII
PLAN PARA REDUCIR LAS VULNERABILIDADES EN LOS RELOJES BIOMÉTRICOS

Vulnerabilidad	Recomendación

El nombre de comunidad SNMP puede ser adivinado	• En caso de no utilizar SNMP deshabilitarlo
	• Y en caso de usar SNMP, se recomienda filtrar el tráfico a este servicio mediante iptables con políticas de DROP.
	• Validar y verificar los nombres de comunidad mediante snmpwalk
	
	Procedimiento
	
	Crear un iptables en el firewall habilitando 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`

3.1.5. Plan para Mitigar las Vulnerabilidades en las Impresoras de Red

A continuación se realiza el plan para mitigar las vulnerabilidades encontradas en las impresoras de red del Área de Energía, las vulnerabilidades encontradas en las impresoras son las que se encuentra presenten en otros equipos, es por ello que se recomienda realizar las mismas acciones para tratar de reducirlas y así proteger los equipos.

TABLA XLIV
PLAN PARA MITIGAR LAS VULNERABILIDADES EN LAS IMPRESORAS

Vulnerabilidad	Recomendación
El nombre de comunidad SNMP puede ser adivinado	En caso de no utilizar SNMP deshabilitarlo
Acceso libre a la configuración web	Utilizar un sistema de autenticación, que permita controlar el acceso a la configuración web de las impresoras

3.1.6. Plan para Mitigar las Vulnerabilidades en las Cámaras IP

A continuación se realiza el plan para mitigar las vulnerabilidades encontradas en las cámaras IP, donde se pudo identificar la presencia de vulnerabilidades de factor de riesgo ALTA, que pueden poner seriamente en peligro a los equipos, existen vulnerabilidades donde ya se presenciaron en otros equipos de la red del área de energía y por ende se recomienda el mismo proceso para reducirlas.

TABLA XLV
PLAN PARA MITIGAR LAS VULNERABILIDADES DE LAS CÁMARAS IP

Vulnerabilidad	Recomendación
El nombre de comunidad SNMP puede ser adivinado	• En caso de no utilizar el protocolo SNMP deshabilitarlo • Crear una política para que los nombres no sean adivinados • Validar y verificar los nombres de comunidades con snmpwalk

Dropbear servidor SSH	Actualizar a la SSH Dropbear 2012.55 o posterior.
Acceso libre a la configuración de la camara	Se recomienda la utilización de un sistema de autenticación para el acceso a la página web de configuración de la cámara vulnerable.
Reflexión DDoS SNMP 'GETBULK'	Se recomienda restringir y controlar el acceso a este servicio
Dropbear SSH Server <2013.59 múltiples vulnerabilidades	Actualizar a la SSH Dropbear 2013.59 o posterior.

3.1.7. Plan para Mitigar las Vulnerabilidades en los Access Point Multimarca

Los últimos equipos evaluados fueron los Access Point de marca Linksys y D-Link, en los cuales no se detectaron la presencia de vulnerabilidades que pongan en riesgo a los equipos, pero si se encontraron vulnerabilidades de gravedad MEDIA las cuales pueden llegar a significar un riesgo a los equipos, es por ello que se realiza un plan para mitigar las vulnerabilidades que pueden poner en riesgo a los AP.

TABLA XLVI
PLAN PARA MITIGAR LAS VULNERABILIDADES EN LOS ACCESS POINT MULTIMARCA

Vulnerabilidad	Marca del AP	Recomendación
Caducidad del Certificado SSL	Linksys	Adquirir o generar un nuevo certificado SSL para reemplazar el existente.

Certificado SSL no confiable	Linksys y D-link	El certificado SSL se utiliza un certificado gratuito que funciona correctamente pero que no es reconocido por Nessus, por lo tanto esta vulnerabilidad no afecta o pone en riesgo al equipo.
Detección del Protocolo SSL 2.0 y SSL 3.0	Linksys y D-link	Desactivar los protocolos encontrados y usar TLS versión 1.1 o superiores
Uso de Telnet	D-link	Desactivar el servicio de Telnet y utilizar en su lugar SSH
Uso de HTTP	Linksys y D-link	Desactivar el servicio y solo usar HTTPS

3.1.8. Plan para mitigar las vulnerabilidades físicas encontradas en la red LAN.

En la red del Área de energía se reportaron la existencia de 2 vulnerabilidades muy graves, a las cuales se brinda su respectiva recomendación para tratar de mitigar.

TABLA XLVII
PLAN PARA MITIGAR LAS VULNERABILIDADES FÍSICAS EN LA RED

Vulnerabilidad	Recomendación
Accesos No Controlados	Se recomienda usar credenciales para los funcionarios y pasantes de la UTI y además la instalación de alarmas o sensores que permita la identificación del abierto de puertas a la fuerza, esto con el fin de evitar que cualquier persona intencionada desconecte a los usuarios de la red o para evitar la sustracción de algún equipo.
Falta de seguridad para los AP CISCO	Se recomienda la implementación de rejillas para proteger a los Access Point Cisco de ser desconectados o sustraídos por terceras personas.

g. Discusión

Para realizar el presente proyecto, el cual trata sobre temas de seguridad, es necesario entender y conocer el funcionamiento de la red LAN y claro lo que es más relevante para la institución, con el fin de protegerlo de terceras personas. Una institución en la mayor parte del tiempo esta arriesgada a un ataque interno que a un externo, eso según los reportes presentados por Cybsec.

Aplicando las herramientas Nessus y OpenVas se pudo comprobar la existencia de vulnerabilidades en los equipos de red, esto significa que los equipos están expuestos a una variedad de ataques, los cuales pueden llegar tener daños irreversibles como económicos.

Desarrollo de la propuesta alternativo

En el primer objetivo se realiza un análisis de aquellas herramientas que se dedican a la exploración de una red de datos, es decir la identificación de los equipos existentes en la red, además que determinen los estados de los puertos y los servicios que están siendo usados para con ello decretar los equipos más críticos, que serán evaluados en la siguiente fase. Se analizan cuatro herramientas de las cuales se utilizará solo una, para ello se investiga las características de cada una en libros, artículos científicos, revistas, páginas web y repositorios. Lo más importante de la investigación radica en el sustento científico de cada herramienta, este es uno de los factores más importantes a considerar para la elección de la herramienta. Se hace de igual manera para seleccionar la herramienta más apropiada para la búsqueda de vulnerabilidades en los equipos.

En el Segundo objetivo lo primero que se realiza es el descubrimiento de todos los equipos existentes en la red, esto se lo realiza con la herramienta Nmap, la cual fue elegida en el objetivo 1, una vez obtenidos todos los equipos se empieza a escanear los puertos abiertos y servicios que utilizan los equipos para determinar a cuáles son necesarios el escaneo. Una vez explorada la red se efectúa una topología con su respectivo direccionamiento y diagrama de figuras.

Descubiertos los equipos en cada VLAN se procede al escaneo de vulnerabilidades, para ello se hace uso de la herramienta NESSUS, que es una de las más completas para este tipo de análisis, la desventaja es que su licencia es privada, es decir de pago. También se hace uso de la herramienta OPENVAS la cual posee una licencia libre que

permite su uso y configuración a gusto del cliente. Ambas herramientas son empleadas en los equipos en busca de vulnerabilidades, finalmente se realiza una comparación de resultados obtenidos por las herramientas con el fin de confirmar la presencia de cierta vulnerabilidad en los equipos y para complementar a la otra herramienta.

Las vulnerabilidades de gravedad ALTA son a los que se les debe dar una pronta atención, pero eso no quiere decir que a los riesgos bajos y medios no se los debe tomar en cuenta, ya que en un futuro pueden llegar a ser peligrosos incluso más que los riesgos altos.

En el último objetivo se elabora un plan de mitigación para las vulnerabilidades encontradas en el proceso de escaneo, se toma en cuenta las posibles soluciones que nos brinda las diferentes herramientas, luego se presenta los funcionarios del Departamento de Unidad de Telecomunicaciones e Información, con el fin de que se apruebe y corrija las recomendaciones.

h. Conclusiones

A continuación se muestran las conclusiones con respecto al trabajo realizado:

- El análisis de las herramientas basado en artículos, revistas, tesis y trabajos comprobados fueron fundamentales para la elección tanto de las herramientas para la exploración de red y evaluación de vulnerabilidades a utilizar en este proyecto.

- El uso de la herramienta NMAP fue esencial en este proyecto, ya que con esta se consiguió localizar a todos los equipos existentes en la red LAN e identificar a que familia pertenecen junto con su sistema operativo. A parte reveló los estados de los puertos y averiguar los servicios utilizados en cada equipo.

- Utilizar las herramientas OpenVas y Nessus para la búsqueda de vulnerabilidades lógicas en los equipos fue muy valioso, ya que se logró una complementación entre ambas y con ello un eficiente resultado.

- Aplicar la Metodología Clásica para el Análisis de Vulnerabilidades en la red del Área de Energía fue trascendental, porque sintetiza el análisis en solamente tres fases con lo que se consigue realizar el proyecto en un tiempo corto y de forma organizada.

- Al utilizar la metodología MAGERIT se consiguió determinar el nivel de riesgo (bajo, medio o alto) de las amenazas que ponen en peligro la protección de los elementos físicos del Área, como el hardware y su ubicación, para luego revelar las vulnerabilidades físicas que existen en la red del Área de Energía.

- La elaboración del Plan de Mitigación de Riesgos constituye una parte valiosa dentro del proyecto, ya que se brindan recomendaciones para disminuir el impacto de posibles riesgos en los equipos que pueden ser ocasionados por las vulnerabilidades encontradas.

i. Recomendaciones

- Utilizar al menos dos herramientas para la evaluación de vulnerabilidades en una red de datos, para lograr que ambas herramientas se complementen entre sí y hallar la mayor cantidad de debilidades existentes en los equipos, con esto se llega a obtener un resultado muy eficiente para determinar el nivel de seguridad de cada equipo.

- Realizar ataques informáticos como Denegación de Servicio, Fuerza Bruta, Man in the Middle, Inyección SQL, etc., a los equipos conectados a la red, con el fin de determinar si las vulnerabilidades encontradas están verdaderamente permitiendo que algún ataque se pueda realizar exitosamente y además para encontrar nuevas fallas en los sistemas.

- Ejecutar un análisis interno y externo de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red, tales como cambio de topología de red modificaciones en las normas de firewall, actualizaciones de protocolos.

- Al momento de realizar un plan de mitigación se debe tener muy en cuenta las versiones del software de los equipos, debido a que se puede recomendar el uso de protocolos o programas que no son soportados por ciertos equipos, lo que ocasiona que ese plan de mitigación se vuelva obsoleto e inservible para la institución.

- Elaborar el plan de mitigación en conjunto con los encargados de la seguridad informática de la institución para obtener una buena elaboración y que sea utilizado como base para mitigar las vulnerabilidades encontradas en los equipos de la institución.

j. Bibliografía

[1] P. Aguilera, Seguridad Informática, 1 ed., Editex, 2010, p. 240.

[2] O. O. Avidán y V. L. Rene Arturo, Seguridad de la Información, Primera ed., S. Alonzo y M. García, Edits., Gautemala, 2014.

[3] A. Villalón Huerta, «Seguridad en Unix y Redes,» vol. 2.1, p. 503, Julio 2006.

[4] M. Robert, «TechNet,» Microsof , 1 Octubre 2003. [En línea]. Available: https://technet.microsoft.com/en-us/library/dd632948.aspx. [Último acceso: 05 Junio 2015].

[5] E. Skoundis y L. Zeltser, Malware: Fighting Malicious Code, New Jersy: Pearson Education, 2004.

[6] Hacking Desde Cero, vol. I, Buenos Aires: Primera, 2011.

[7] D. Bartz, «Las personas son el eslabón debil en la ciberseguridad,» *Reuters,* 22 Julio 2009.

[8] M. A. Amutio Gómez, J. Candau y J. A. Mañas, MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, vol. III, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[9] F. J. López Moliner, Informáticos Generalitat Valenciana, Valencia: Mad S.L, 2005.

[10] X. Perramón Tornil, Aspectos Avanzados de Seguridad en Redes, Barcelona, 2004.

[11] M. F. García Guerra, «Análisis del comportamiento normal e intrusivo del tráfico en un Red TCP/IP,» Quito, 2011.

[12] Cio Perú, «Tres tipos de ataques DNS y cómo tratar con ellos,» CIO, 23 Octubre 2013. [En línea]. Available: http://cioperu.pe/articulo/14359/tres-tipos-de-ataques-dns-y-como-tratar-con-ellos/. [Último acceso: 23 Abril 2015].

[13] S. Bortnik, «Seguridad de la Información,» 16 junio 2013. [En línea]. Available: http://revista.seguridad.unam.mx/numero-18/pruebas-de-penetraci%C3%B3n-para-principiantes-5-herramientas-para-empezar. [Último acceso: 26 abril 2015].

[14] H. Jara y F. G. Pacheco, Ethical Hacking, Primera ed., Buenos Aires, 2012.

[15] S. Bruce, Ther Hacker Crackdown, Virginia: Bantam Books, 1993.

[16] Debish, «DebianHackers,» FeedBurner, 8 Octubre 2012. [En línea]. Available: https://debianhackers.net/nmap-escaner-de-puertos/. [Último acceso: 12 Abril 2016].

[17] L. J. Choice, System Administration, 2001.

[18] «LinuxQuestion,» 2003. [En línea]. Available: http://www.linuxquestions.org/questions/showthread.php?s=&threadid=116374.

[19] CIO, «CIO Instituto Boletín sobre seguridad informática,» vol. 2, nº 3, 1999.

[20] V. Navratilova, «Llegar a conocer sus servicios de red,» Chicago Tribune, Chicago, 2000.

[21] W. Bros, Dirección, *The Matrix Reloaded.* [Película]. EEUU: Village Roadshow Pictures, 2003.

[22] P. Travis, Dirección, *Dredd.* [Película]. EEUU: DNA Films, 2012.

[23] P. Greengrass, Dirección, *The Bourne Ultimatum.* [Película]. EEUU: Universal, 2007.

[24] M. Wolfgang, « Host Discovery with nmap,» 2002.

[25] G. Giacobbi, «The GNU Netcap,» 1 Noviembre 2006. [En línea]. Available: http://netcat.sourceforge.net/.

[26] A. Ornaghi, «Ettercap,» Tick Tock Computers, LLC. [En línea].

[27] Socuros, «Ettercap: analizador de tráfico universales,» vol. 1, nº 1, 2010.

[28] F. G. Benito, *Laboratorio Virtualizado de Seguridad Informática con Kali Linux,* Valladolid.

[29] A. Rollis, «Respuesta a Incidentes de Seguridad de la Información,» 2005.

[30] M. A. M. Z. Nasir Siddique, *Data Link Layer Security Problems and Solutions*, Halmstad: Halmstad University, 2015.

[31] «cheops-ng,» sourceforge.net, 2005. [En línea]. Available: http://cheops-ng.sourceforge.net/.

[32] R. J. Hamid Reza Shahriari, «Vulnerability Take Grant (VTG): An efficient approach,» *Elservier*, p. 12, 2006.

[33] D. G. Gómez, «Sistemas de Detección de Intrusiones,» vol. 1, nº 01, Junio 2003.

[34] J. R. Yáguez, «Técnicas y herramientas de análisis de vulnerabilidades de».

[35] OWASP, « OWASP la comunidad libre y abierta sobre seguridad en aplicaciones,» [En línea].

[36] G. Lyon, Nmap Network Scanning, California: Nmap.org , 2011.

[37] G. Lyon, «Nmap Security Scanner,» Nmap.org, [En línea]. Available: http://nmap.org/. [Último acceso: 20 abril 2015].

[38] M. Carey, P. Criscuolo y M. Petruzzi, Nessus Network Auditing, vol. II, Boston: Syngress, 2008.

[39] H. Kumar, Learning Nessus for Penetration Testing, 2014.

[40] «Teneble Network Security,» 2015. [En línea]. Available: http://www.tenable.com/products/nessus-vulnerability-scanner.

[41] Dragon, «Manual de Metasploit Framework en Español,» 20 Marzo 2010. [En línea]. Available: http://www.dragonjar.org/manual-de-metasploit-framework-en-espanol.xhtml.

[42] D. Kennedy, J. Gorman, D. Kearns y M. Aharoni, Metasploit The Penetration Tester's Guide, H. Moore, Ed., Boston, 2011.

[43] A. E. Quezada Caballero, Hacking con Kali Linux, O. Security, Ed., 2015.

[44] OpenVas, «Open Vulnerability Assessment System,» 02 Abril 2015. [En línea]. Available: http://www.openvas.org/index.html.

[45] M. Á. Mendoza, «WeliveSecutiry,» ESET, 18 Noviembre 2014. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/. [Último acceso: 2015 Abril 21].

[46] E. Geier, «Cio Peru,» CIO, 09 Mayo 2014. [En línea]. Available: http://cioperu.pe/articulo/15863/6-escaneres-de-vulnerabilidades-de-red-gratuitos/. [Último acceso: 21 Abril 2015].

[47] G. Díaz, F. Mur, S. Elio, M. Alonso Castro y J. Piere, Seguridad en las comunicaciones y en la información, Madrid, 2012.

[48] C. Laura y C. Gerald, «Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide,» Chappell University, 2012.

[49] J. Vásquez Pérez, «Manual de uso wireshark En Español.,» Servicio Nacional De Aprendizaje Sena, Medillin, 2013.

[50] Vv.Aa, SEGURIDAD INFORMATICA: CONOCER EL ATAQUE PARA MEJOR DEFENSA(ETHICAL HACKING), Barcelona: ENI, 2013.

[51] Watkis, Kevin; McAfee Labs, «Las vulnerabilidades de VoIP,» 2009.

[52] S. Guaci, «ENABLE SECURITY,» 2012. [En línea]. Available: http://www.enablesecurity.com/. [Último acceso: 23 Junio 2015].

[53] A. Avaya, «Introducing VoIPaudit,» VoIP Shield Systems, Inc, 2015. [En línea]. Available: http://www.voipshield.com/#!voipaudit/c1739. [Último acceso: 25 Junio 2015].

[54] C. Hadnagy, Ingenieria Social: El Arte del hacking Personal, Anaya Multimedia, 2011.

[55] OWASP, «XSS (Cross Site Scripting) Prevención Cheat Sheet,» OWASP, 25 Junio 2015. [En línea]. Available: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet.

[56] OWASP, «Categoría: Proyecto OWASP ModSecurity Core conjunto de reglas,» 22 Abril 2015. [En línea]. Available: https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project.

k. Anexos

1. Anexo 1

Entrevista sobre la situación actual de la Red LAN de la Universidad Nacional de Loja, Área de la Energía.

UNIVERSIDAD NACIONAL DE LOJA

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Estimada Subdirectora:
Actualmente me encuentro realizando el proyecto final de modulo, el cual consiste sobre el Análisis de vulnerabilidades en la Red LAN de esta institución. Para lo cual considero que sus opiniones serán importantes para tener un mejor conocimiento de la Red.
Le pido contestar las siguientes preguntas:

1. **¿En la actualidad la institución cuenta con políticas o normas para la seguridad de la red?**

Si cuenta, aunque aún no están validadas. Para el acceso a los servidores se lo hace de una manera local y mediante SSH.

Para el acceso al servidor de comunicaciones se lo realiza mediante SSH y HTTP. Para los switches mediante TELNET, SSH y localmente.

2. **¿Cómo se encuentra actualmente estructurada la red, su topología, cuenta con VLAN's, cuantos servidores tiene, esta segmentada?**

Actualmente la red tiene una topología en estrella, el modelo de referencia utilizado es el OSI cuenta con el modelo jerárquico de 3 capas de cisco, además cuenta con VLAN's

3. **¿Describa los equipos de gestión de seguridad o Software con los que actualmente cuenta la institución?**

Firewall.- Tiene configurado una zona DMZ y un conjunto de politicasm se utiliza el NATEO y reglas de seguridad. Ademas se cuenta con ACL's para una mayor seguridad.

VPN.- Se utiliza equipos mikrotik, pero al momento de levantarlo se sufre ataques, cuenta con 3 cuenta de usuarios.

Nessus.- Este servidor es utilizado para el análisis de vulnerabilidades en la red, pero actualmente no está en funcionamiento debido a los cambios que se realizaron en la misma.

---	---
Henry David Quishpe	**Nohelia Bustamante**
Responsable	Subdirectora del Departamento de Redes

2. Anexo 2

Entrevista sobre la situación actual de la Red VoIP

UNIVERSIDAD NACIONAL DE LOJA

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Estimada Subdirectora:

Actualmente me encuentro realizando el proyecto final de modulo, el cual consiste sobre el Análisis de vulnerabilidades en la Red LAN, en el AEIRNNR de esta institución. Para lo cual considero que sus opiniones serán importantes para tener un mejor conocimiento de la estructura de la red de comunicaciones.

Le pido contestar las siguientes preguntas:

1. ¿Qué software es utilizado para el servidor de comunicaciones?

Centos 5 consola y Elastix

2. ¿Qué protocolo de señalización es utilizado para la red de VoIP?

SIP

3. ¿Qué códec de voz es utilizado para la red de VoIP?

G729

4. ¿Qué tipo de teléfonos IP (Hardware) se utilizan para la comunicación?

Grandstream

5. ¿Qué protocolo se utiliza para el transporte de voz?

RTP

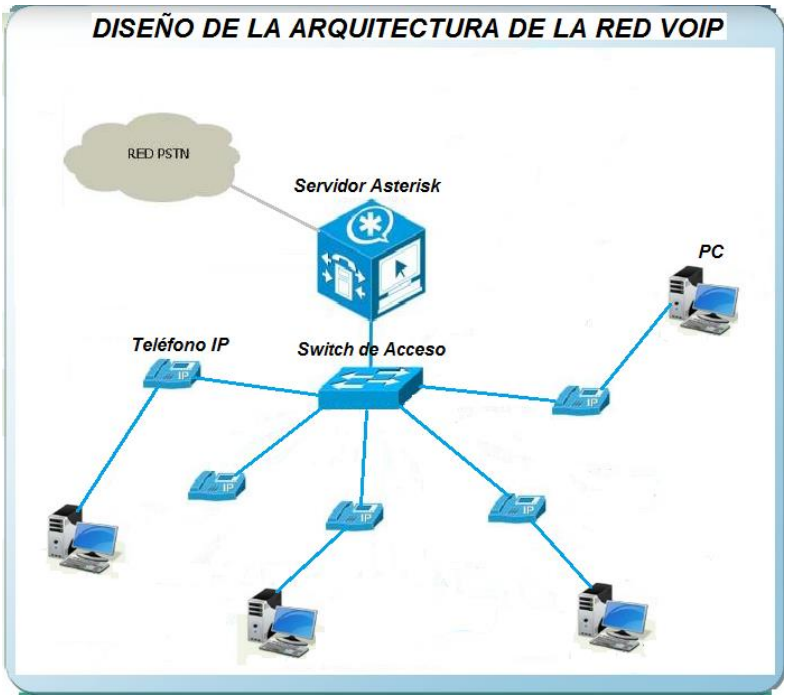
6. ¿La información que viaja por la red es cifrada?

No tengo conocimiento debido a que no existe documentación acerca de la configuración, pero según mis conocimientos si está cifrada.

7. ¿Tiene conocimiento de algún ataque que se haya realizado al servidor de comunicaciones?

No hemos detectado ningún ataque hasta el momento

8. ¿Cuál es el esquema manejado para la red VoIP?



……...

Henry David Quishpe
Responsable

……

Nohelia Bustamante
Subdirectora del Departamento de Redes

3. Anexo 3

Entrevista sobre la situación actual de la Red inalámbrica.

UNIVERSIDAD NACIONAL DE LOJA

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Estimada Subdirectora:
Actualmente me encuentro realizando el proyecto final de modulo, el cual consiste sobre el Análisis de vulnerabilidades en la Red LAN, en el AEIRNNR de esta institución. Para lo cual considero que sus opiniones serán importantes para tener un mejor conocimiento de la Red inalámbrica.
Le pido contestar las siguientes preguntas:

1. **¿Qué tipos de mecanismos de seguridad posee la red inalámbrica de la institución?**

Actualmente no se cuenta con mecanismos, la red es abierta, se planea la implementación de active directory pero solo a nivel administrativo.

2. **¿Cree que han existido robos de contraseñas a docentes en la red inalámbrica?**

No se ha detectado, por lo que hacen uso del protocolo HTTPS

3. **¿Han existido ataque a la red inalámbrica? En caso de haber existido que se ha realizado para sobrellevarlas.**

Si, los más conocidos son los botnets y para sobrellevar estos ataques se bloquea los botnets en el firewall.

4. **¿Con que frecuencia existen caídas de la señal de la red inalámbrica en el Área de la Energía?**

Cuando existe falta de energia, se vuelve lento cuando llega al límite de usuarios que es de 50 por AP con un ancho de banda de 1 MB.

5. **¿Qué estándar usa la red inalámbrica de la institución?**

Para los docentes y administrativos se hace uso de WPA y WPA2

6. **¿De qué manera se lleva el control al acceso de la red inalámbrica?**

No existe un control para los usuarios, la red es totalmente abierta

7. **¿Ha existido la conexión de usuarios no autorizados a redes privadas?**

No se han detectado hasta la actualidad, se hace uso de contraseñas seguras.

8. **¿Con que frecuencia cambia el nombre y contraseña de los Puntos de Acceso?**

Cada 6 meses

9. **¿Existe alguna norma para el uso de la red inalámbrica?**

No se restringe nada

10. **¿La información que viaja por la red es cifrada?**

Si lo es.

…….	…….
Henry David Quishpe	**Nohelia Bustamante**
Responsable	Subdirectora del Departamento de Redes

4. Anexo 4: Solicitud Para Socialización de Resultados

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Loja, 7 de julio de 2016

A los funcionarios de la Unidad de Telecomunicaciones e Información, se los convoca a una reunión el día Viernes 8 de Julio del presente año, a las 08h00 a.m., en la sala de reuniones de la Unidad de Telecomunicaciones e Información, con el fin de realizar la sustentación de los resultados del proyecto de titulación denominado: **ANÁLISIS DE VULNERABILIDADES EN LA RED LAN JERÁRQUICA DE LA UNIVERSIDAD NACIONAL DE LOJA, EN EL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES.**

Esperando contar con la presencia de todos, desde ya les antelo mis más sinceros agradecimientos.

UNIVERSIDAD NACIONAL DE LOJA

SUBDIRECTOR DE INFORMACIÓN

Ing. Jhon Calderón

SUBDIRECTOR DE REDES

Ing. Juan Pablo Ramón

FUNCIONARIO UTI

Ing. Rodrigo Japón

FUNCIONARIO UTI

Ing. Bolivar Feijo

FUNCIONARIO UTI

Ing. Carlos Heredia

FUNCIONARIO UTI

Atentamente: Henry Quishpe

TESISTA

5. Anexo 5: Certificado de Socialización de Resultados

Acta de Reunión No. 016-2016

Asunto:	Exposición de resultados del proyecto: Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables		
Inicio:	08:00	**Duración:**	09:00
Convocado por:	Henry Quishpe	**Fecha:**	08/07/2016

AGENDA

- Sustentación de los resultados del Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables.

COMPROMISOS

- Por parte del estudiante Henry Quishpe se realiza la entrega formal del reporte Análisis de Vulnerabilidades en la Red LAN del Área de la Energía, Industrias y los Recursos Naturales No Renovables.
- Los resultados expuestos fueron revisados a detalle y serán considerados por la Subdirección de Redes y Equipos Informáticos para mitigar las vulnerabilidades encontradas en el Área de la Energía, así mismo se replicarán procesos similares en el resto de dispositivos de red y servidores de la institución.

ASISTENTES:

Ing. Jhon Calderón **SUBDIRECTOR DE REDES**	Ing. Juan Pablo Ramón **FUNCIONARIO UTI**	Ing. Bolívar Feijo **FUNCIONARIO UTI**
Ing. Carlos Heredia **FUNCIONARIO UTI**	Ing. Rodrigo Japón **FUNCIONARIO UTI**	Henry Quishpe **TESISTA**

6. Anexo 6: Entrevista sobre Vulnerabilidades Físicas

UNIVERSIDAD NACIONAL DE LOJA

Entrevista dirigida a la Unidad de Telecomunicaciones e Información

Fecha: 27 de Julio de 2016

Estimado Subdirector de Redes y Equipos Informáticos:

Actualmente me encuentro realizando el proyecto final de módulo, el cual consiste sobre el Análisis de vulnerabilidades en la Red LAN, en el AEIRNNR de esta institución. Para lo cual considero que sus opiniones serán importantes para poder corroborar la existencia de algunas vulnerabilidades físicas en la red LAN del Área de Energía.

Le pido contestar las siguientes preguntas:

Accesos no Controlados

1. ¿Se utilizan credenciales para los funcionarios y pasantes de la Unidad de Telecomunicaciones e Información al momento de ingresar a las oficinas para realizar cualquier actividad en los racks?

Se ha otorgado únicamente credenciales a los estudiantes practicantes de la Subdirección de Redes y Equipos Informáticos que se encuentran realizando el levantamiento de información del Plan de Inventario.

2. ¿Alguna vez se ha detectado el forzamiento al acceso físico a un rack, es decir ha existido el rompimiento del seguro o vidrio de la puerta del rack?

No hemos conocido que se haya realizado un acceso físico no autorizado en ninguna parte del campus universitario.

3. ¿Los Access Point Cisco, ubicados en los diferentes bloques del área cuentan con una seguridad para que no puedan ser sustraídos por terceras personas?

No cuentan con seguridad física, pero cabe indicar que se encuentran en una altura que no es de fácil acceso.

4. ¿Se lleva un monitoreo de los equipos del Área como Switch y Access Point para conocer cuando son desconectados, sustraídos o cuando falta suministración de energía?

Actualmente se ha implementado una herramienta de monitoreo para todos los equipos de red y servidores de la institución.

5. ¿Los AP de marca Linksys y D-Link ubicados en los diferentes cubículos de docentes u oficinas de administrativos tiene algún encargado bajo su cuidado?

No en todos los casos, actualmente los responsables de Bodega conjuntamente con personal de la Subdirección de Redes y Equipos Informáticos están realizando la constatación física para elaborar las actas de traspaso.

Energía Eléctrica

6. ¿En todos los rack existe al menos un supresor de picos o regulador de voltaje que ayude a que los equipos no se quemen en caso de algún corte de luz inesperado?

En los sitios donde se encuentran los switch de distribución L3 existe un UPS como regulador y respaldo de energía.

Ubicación de los equipos

7. ¿Cree que el Access Point Cisco para exteriores se encuentra bien ubicado, se tiene algún plan para su movilización a un lugar más idóneo?

Correcto, existen alrededor de 5 APs outdoor que van a ser reubicados, previo a la presentación de un informe técnico y autorización del Director de la UTI.

Henry David Quishpe

Tesista

Ing. Jhon Alexander Calderón

Subdirector de Redes y Equipos Informáticos