ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

ANÁLISIS DE VULNERABILIDADES DEL SERVIDOR E-LEARNING DE LA ESPOCH PARA LA IMPLEMENTACIÓN DE MEJORES PRÁCTICAS DE SEGURIDAD-ACCESO.

Trabajo de titulación presentado para optar al grado académico de**:**

INGENIERO EN ELECTRONICA, TELECOMUNICACIONES Y REDES

AUTORES: AIDA CONCEPCIÓN ALVARADO TAPIA

RICHARD ALFREDO MONTESDEOCA CABRERA

TUTOR: ING. VINICIO RAMOS VALENCIA MSC.

Riobamba – Ecuador

2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRONICA EN TELECOMUNICAIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que la investigación "ANÁLISIS DE VULNERABILIDADES DEL SERVIDOR E-LEARNING DE LA ESPOCH PARA LA IMPLEMENTACIÓN DE MEJORES PRÁCTICAS DE SEGURIDAD-ACCESO", de responsabilidad de la señorita Aida Concepción Alvarado Tapia y el señor Richard Alfredo Montesdeoca Cabrera, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de titulación, quedando autorizada su presentación.

Ing. Washington Luna **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Franklin Moreno **DIRECTOR DE ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Vinicio Ramos MsC. **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Verónica Mora MsC. **MIEMBRO DEL TRIBUNAL**	_____	_____

Nosotros, Aida Concepción Alvarado Tapia, Richard Alfredo Montesdeoca Cabrera, somos responsable de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual del Trabajo de Titulación pertenece a la Escuela Superior Politécnica De Chimborazo

.

Aida Concepción Alvarado Tapia

Richard Alfredo Montesdeoca Cabrera

DEDICATORIA

Quiero dedicar mi título a una persona que decidió tomar una responsabilidad que no le correspondía pero que lo hiso por amor, por un amor de hermandad incondicional, quiero que en este trabajo de titulación quede plasmado tu nombre como símbolo de eterna gratitud por tu sacrificio a ti hermanito JOSE LUIS ALVARADO TAPIA, tú me brindaste esta oportunidad de salir adelante, mi Ingeniería te la dedico y ahora es mi turno de corresponderte, vamos a salir adelante por ti , por mí, por nuestra familia.

Aida.

A mis padres quienes me apoyaron de principio a fin para cumplir éste objetivo, a Dios por la salud y la vida; y por darme cada día nuevas oportunidades y la capacidad de terminar esta carrera, a mis abuelitos que con su constante apoyo me mantuvieron enfocado en la meta, a mi tío que con sus consejos siempre me animaba a no desmayar y a mis hermanos que siempre estuvieron alentándome para culminar ésta meta.

Richard.

AGRADECIMIENTO

Mi DIOS, a ti te agradezco por bendecirme y darme sabiduría para concluir esta etapa en mi vida. A la Escuela Superior Politécnica de Chimborazo por acogerme en sus aulas para lograr ser una profesional. A mi tutor de tesis Mgs. Vinicio Ramos por su paciencia, dedicación y tiempo que me dio para terminar este trabajo de titulación. A todos mis profesores por inculcarme sus enseñanzas y aprendizaje durante toda mi carrera estudiantil, y de una manera muy especial agradezco a mis padres por su apoyo incondicional, por su perseverancia y su amor, gracias por no dejarme caer. A mis hermanos por creer en mí por estar a cada momento apoyándome, aconsejándome y guiándome para salir adelante. A mi esposo por insistir para superarme profesionalmente por no dejarme atrás y darme la mano para salir en cada dificultad que se nos presentó en este largo camino. A mis hijos "Dylan y Luanna" gracias por no haber sido un obstáculo ni la excusa para decaer, que por ustedes logre llegar al final, también agradezco a toda mi familia que directa o indirectamente recibí de su apoyo y sus buenos deseos para cumplir esta meta.

Aida.

Agradezco de todo corazón a mis padres que nunca dejaron de apoyarme aún en los momentos más difíciles, a Dios por toda su bondad, su gracia y favor han sido muy notorias en cada paso que he dado en el tiempo de preparación universitaria, gracias a toda mi familia por su inagotable apoyo, por sus abrazos, besos y sonrisas, a mi querida iglesia que con sus oraciones me mantenían fuerte, gracias a todos mis amigos y conocidos quienes de una u otra forma fueron parte de la culminación de este objetivo.

Richard.

TABLA DE CONTENIDO

Páginas

INDICE DE TABLAS

Páginas

INDICE DE FIGURAS

Página

INDICE DE GRÁFICOS

Página

INDICE DE ANEXOS

RESUMEN

Se realizó un análisis de vulnerabilidades al servidor E-learning de la Escuela Superior Politécnica de Chimborazo para la implementación de mejores prácticas de seguridad y acceso. Se analizó la situación actual del servidor E-learning, para esto se utilizó varios softwares como: Kali Linux, Nessus, Nexpose que encuentran fallas de seguridad por medio del escaneo y ataque con varios plugins y herramientas que incorporan dichos programas. En laboratorio se hizo varias pruebas de escaneo, enumeración de servicios y de ataques al servidor, las pruebas de escaneo se lo realizo con la herramienta de whois.net que nos dio el perfil de usuario del servidor, las pruebas de enumeración de servicios se lo realizo con la herramienta Nmap que realiza un análisis intenso y da todos los servicios que ofrece el servidor, además de las versiones de las mismas. Se eligieron cinco ataques principales: ataque Inyección de SQL que vulnera la base de datos. Ataque CROSS-SITE SCRIPTING que altera el estado actual del servidor cambiando información en base a códigos script. Ataque SNIFFING, espía y captura las contraseñas en un texto plano a través del internet. Ataque DoS, envía miles de paquetes al servidor saturando así las peticiones reales dejando sin servicio a los usuarios. Ataque PHISING, que clona la página real por una alterna con la idea de robar contraseñas. El servidor E-learning fue vulnerable en un 80% con los ataques realizados. Se concluye que el servidor E-learning es un sitio vulnerable a cualquiera de estos ataques en la red, se podría solucionar implementando certificados de encriptación Web, políticas de firewall e implementaciones de DMZ que restringe los privilegios de red al servidor tanto de entrada como de salida, bloqueando el control y acceso a los administradores con rangos privilegio y servicios a los que intentan ingresar desde el internet hacia la red interna. Se recomienda seguir actualizando con nuevas políticas de seguridad ya que un servidor web nunca estará 100% a salvo de algún ataque informático.

Palabras Clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERIA>, <REDES>, <SEGURIDAD DE REDES>, <VULNERABILIDADES> <PRUEBAS D.E HACKING> <IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD>.

SUMMARY

A vulnerability analysis was carried out at the E-learning server of the Polytechnic School of Chimborazo in order to increase security and access practices. We analyzed the current situation of the E-learning server, for this we used several software such as: Kali Linux, Nessus, Nexpose that find security fails through the scan and attack with several plugins and tools that incorporate such programs. In the laboratory there were several tests of scanning, enumeration of services and attacks to the server. The test of scanning was done with the Whois.net tool that gave us the user profile of the server, the enumeration test of service performed with the tool Nmap that performs an intense analysis and gives all the services offered by the server, including the versions of the same. Five main attacks were chosen: SQL Injection attack that violates the database. CROSS-SITE SCRIPTING attack that alters the current state of server by changing information based on script codes. SNIFFING attack, spies and captures the passwords of plain text through the internet. Attack DoS, sends thousands of packets to the server then saturating the real requests and letting users not to use. PHISHING attack, which clones the actual page for an alternate with the idea of stealing passwords. The E-learning server was 80% vulnerable to attacks. It is concluded that the E-learning server is a vulnerable site for these network attacks. They could be solved by implementing Web encryption certificates, firewall policies and DMZ implementations that restricts the network privileges to the server both inbound and outbound, blocking the control and access to the administrators with privileged ranges and services to which they try to enter from the internet towards the internal network. It is recommended to continue updating with new security policies since a web server is never 100% safe from any computer attack.

Keywords: <TECHNOLOGY AND ENGINEERING SCIENCES>, <NETWORKS>, <NETWORKS SECURITY>, <VULNERABILITIES>, <HACKING TEST>, <IMPLEMENTATION OF SECURITY POLICIES>

INTRODUCCIÓN

Desde que se descubrió el internet en Estados Unidos nos ha dado la oportunidad de una comunicación más rápida y efectiva, ahorrándonos tiempo, esfuerzo y dinero; esto ha motivado la utilización del mismo en centros educativos de primaria, secundaria y superior, también es utilizado en centros con fines de lucro públicos y privados dando favorables resultados en el desarrollo de la tecnología y la enseñanza. Los beneficios de la internet han evolucionado mucho a través de los años, uno de ellos es la abundancia de nueva información lo que ha presentado nuevas oportunidades para las universidades y centros educativos especializados, que se hallan abocados en la tarea de "actualización de conocimientos" en forma rápida y global. Ante esta necesidad de comunicación e información en tiempo real, la solución gira en torno a conceptos nuevos como el E-learning o aprendizaje electrónico, un concepto complejo que es presentado como una herramienta formativa desde un punto de vista tecnológico y pedagógico (Moreno, 2009, págs. 18 -19).

La Escuela Superior Politécnica de Chimborazo (ESPOCH) a fin de lograr la excelencia académica, soporta su metodología de enseñanza en el uso de estas nuevas tecnologías; estas tecnologías en su funcionamiento han presentado problemas como: tiempo de funcionamiento, saturación de usuarios, pérdida de información entre otros; lo que justifica esta investigación que busca implementar unas mejores prácticas de seguridad y acceso basándonos en el top 10 de los ataques más críticos de la aplicación web de riesgos de seguridad creado por (OWASP)

Esta investigación consta de tres capítulos, en el primer capítulo se redacta toda la base teórica relacionada y que dará soporte a la investigación; en el segundo capítulo se explica toda la metodología aplicada; en el tercer capítulo damos respuesta a la investigación y se exponen los resultados.

Antecedentes

La incorporación de las nuevas tecnologías en todos los aspectos de la vida y la sociedad misma demanda nuevos modelos de enseñanza y aprendizaje. El modelo de educación centrado en la enseñanza, donde el protagonista es el profesor, está dejando paso a un sistema basado en el aprendizaje, donde el alumno se convierte en el responsable de su propio proceso de aprendizaje y el profesor debe buscar y utilizar la metodología y los medios más adecuados que ayuden al alumno en ese proceso. Es en este entorno de trabajo cooperativo donde las nuevas tecnologías y los entornos de trabajo virtuales –versus semipresenciales- adquieren una gran importancia ya

que, por ejemplo, permiten la comunicación asíncrona en tiempo y lugar entre los agentes implicados y facilitan el acceso a una gran cantidad de recursos e información externa.

Con la inserción de la técnica y la tecnología, las cosas van cambiando, hasta llegar a una emergencia del entorno virtual. En este surgimiento, se implementa la visión digital, que más tarde transforma nuevos ambientes naturales en la educación. (Payares, 2011, pág. 15)

La nueva visión de la educación se fundamenta en procesos innovadores que deben ser dinámicos, creativos y con facilidades para acceder a información de toda índole sobre temas de interés, sin duda en la actualidad todos estos elementos son proporcionados para las TICS, la ayuda de los recursos de información y comunicación, dinamizan los procesos de capacitación e investigación consiguiendo con esto un aprendizaje más completo, donde se desarrolle un pensamiento crítico, creativo, reflexivo y participativo.

La "Escuela Superior Politécnica de Chimborazo" ya viene incorporando al proceso de enseñanza aprendizaje para las diferentes asignaturas muchos años atrás, una serie de recursos informáticos utilizados por los docentes eficientemente resulta ser una inversión con mucho provecho ya que el aula virtual en la plataforma Moodle contiene una gama de alternativas que, al ser diseñadas eficientemente, se podrá alcanzar conocimientos muy significativos en los estudiantes.

Formulación del problema

Como se ha mencionado en apartados anteriores la Escuela Superior Politécnica de Chimborazo implementó la educación virtual como una herramienta en el proceso de educación, buscando mejorar la interacción entre el estudiante-profesor en cuanto a: aprendizaje, tareas, pruebas online, wikis colaborativos, foros de aprendizaje, chats, consultas en vivo, atención al estudiante, entre otros. Todos los objetivos planteados están perdiendo su funcionalidad debido a la vulnerabilidad de la plataforma, lo que ha provocado constantes caídas en su servicio, pérdida de información, modificación de la información por terceros, entre otros. Si la situación descrita persiste en el tiempo afectaría el propósito por el cuál fue implementada la plataforma, poniendo en vulnerabilidad gran parte del soporte del proceso de enseñanza y en última instancia haciendo inútil la inversión económica realizada. Frente a esto, es necesario un análisis del servidor, diagnóstico de su estado en términos de vulnerabilidad y el diseño e implementación de políticas de seguridad, que rijan el normal desarrollo del servidor y eliminen en la medida de lo posible todas las fallas en el servicio.

Sistematización del problema

¿Qué tan seguro es el servidor e-learning de la ESPOCH?
¿Por qué el servidor ha sufrido muchas caídas en el servicio?
¿Se podría analizar e implementar más políticas de seguridad que incrementen la confiabilidad del servicio?
¿Se podría poner más restricciones para el acceso al servicio?
¿Qué parámetros se podría tomar en cuenta utilizando herramientas de vulnerabilidades de redes para que el servidor este en óptimas condiciones de funcionamiento y rendimiento?

Justificación Teórica

En las universidades de la región se han implementado plataformas como: Moodle, Dokeos, Atutor, BlackBoard entre otras, en nuestra localidad y medio de estudio la plataforma usada en la ESPOCH es Moodle de código libre.
En el proceso de implementación de este servidor e-learning se atacó las vulnerabilidades que en aquel tiempo se presentaron, aunque en sus primeras etapas el servidor funcionaba de manera adecuada, año con año sus funcionalidad ha ido mejorando, principalmente se habla de la limitación de hardware, esto es provocado debido a que cada semestre aumenta el número de estudiantes y de materias que se imparten, lo que reduce los recursos de memoria y de disco de almacenamiento, bajando de esta manera la velocidad de procesamiento que es indispensable para el buen funcionamiento del servidor; otro problema muy común es que el servidor deja de funcionar por usuarios que suben archivos pesados, problemas con formatos de los archivos, o personas que hacen ataques a las redes para obtener información del servidor como: nombre de usuarios, información sobre evaluaciones escritas, entre otras.
En una red como e-learning en constante crecimiento, es esencial el análisis de seguridad de redes para preservar la integridad de la información, datos de los usuarios, datos de los profesores; información que por su naturaleza es delicada y que está expuesta para cualquier usuario que tenga acceso a una cuenta de este servidor; lo anterior hace indispensable contar con políticas de seguridad tanto de acceso como de control de la información.

Justificación aplicativa

Conforme va avanzando la tecnología web y aplicaciones en la nube aparecen nuevos impedimentos y problemas para la seguridad de los datos e información para el servidor e-learning.

En la presente investigación se plantea que una de las soluciones para el hospedaje de una plataforma e-learning es ubicarla en una aplicación cloud, es decir contratar un servicio en la nube. Los proveedores de espacio en la nube más comunes son Hostingecuador.com, hostecuador.com, telconet.com, hostmonster.com, que entregan todos los requerimientos tanto de hardware como software para la implementación de la plataforma. El hosting en la nube tiene muchas ventajas con respecto a los servidores físicos, presentan mejores prestaciones de adecuación de las instalaciones, sistemas de refrigeración, seguridad en las instalaciones y provee términos de seguridad de acceso como lo son protección de ataques DoS e inyección SQL. Además, cuenta que ya viene instalado herramientas como PHP y MySql que son herramientas necesarias para la instalación de la interfaz de usuario y las bases de datos, lo que permite guardar toda la información de los usuarios. Otra ventaja es la disponibilidad de tiempo en funcionamiento es decir que va a tener la disponibilidad de servicio de aproximadamente de 99.99% los 365 días del año. (Clavero C, 2013)

Objetivos

Objetivo General

Analizar las vulnerabilidades del servidor e-learning de la ESPOCH para la implementación de mejores prácticas de seguridad – acceso.

Objetivos Específicos

- Analizar el funcionamiento del servidor e-learning de la ESPOCH
- Determinar las vulnerabilidades de hardware y software del servidor e-learning de la ESPOCH.
- Realizar pruebas en los ambientes simulados, con el objetivo de encontrar las fallas de seguridad en el servidor e-leraning de la ESPOCH.
- Implementar una guía de las mejores prácticas para el servidor e-learning de la ESPOCH.
- Evaluar el desempeño del servidor e-learning de la ESPOCH con las mejores prácticas de seguridad acceso

CAPÍTULO I

1. MARCO TEORICO

1.1 Educación Virtual

1.1.1 Concepto

La educación virtual se la conoce como e-learning (educación en línea) o educación a distancia, consiste en el uso de una computadora y del internet donde el estudiante interactúa con el tutor y sus compañeros desde cualquier ubicación (desde la casa o el trabajo), teniendo acceso y facilidad de información para el proceso de aprendizaje acomodándose al tiempo y necesidad del estudiante

1.1.2 Uso el aula virtual

El aula virtual nos permite estudiar a través del internet, ya que por exigencias laborables o situaciones geográficas se hace difícil la asistencia a los diferentes planteles educativos. En este medio de educación se puede interactuar profesor – alumno desde cualquier parte del mundo sin necesidad de contacto físico. La gran mayoría de los usuarios han nacido rodeados de nuevas tecnologías, lo que ha facilitado el manejo y adaptación a las mismas.

1.1.3 Elementos esenciales del aula virtual

Los elementos que componen el aula virtual vienen de una adaptación o evolución del aula física-tradicional a un aula soportada por tecnología computador-internet.

“Un elemento muy importante de estos sistemas es que la librería de documentos une las herramientas asíncronas pero también puede almacenar las síncronas, por ejemplo las discusiones en el chat que pueden ser almacenados para una revisión asíncrona posteriormente. (Magaly, 2007, pág. 2)

Tabla 1-1: Herramientas del Aula Virtual

HERRAMIENTA	CATEGORIA	FUNCIÓN COMÚN
Presentaciones interactivas	Síncrona	Presentación sincronizada
Chat	Síncrona	Comunicaciones en tiempo real basadas en Texto
Broadcast	Síncrona	1-1 ó 1- muchos mensajes directos
E-mail	Asíncrona	Correo electrónico
Foro de discusión	Asíncrona	Discusiones
Librería de documentos	Asíncrona	Colocar y repartir documentos
Pizarrón	Asíncrona	Colocar fechas y eventos importantes

Fuente: Herramientas y sus funciones dentro del aula virtual (Magaly, 2007, pág. 2)
Realizado por: Montesdeoca, R; Alvarado, A. 2017

1.1.4 Características del aula virtual

Las principales características del aula virtual son: 1) facilidad para que el alumno pueda encontrar de forma intuitiva todo la información disponible y actualizada y 2) todas las herramientas y/o aplicaciones para la comunicación.

1.1.1.1 El correo electrónico

Permite la comunicación privada o pública entre profesor y alumno, adjuntar ficheros de texto, imágenes, sonidos, etc. Es el medio más utilizado entre tutor y alumno, es una comunicación asíncrona.

1.1.1.2 Avisos

Se utilizan para mostrar información de obligada lectura antes de acceder al aula virtual, suelen ser personalizados para cada usuario y normalmente son unidireccionales no permiten respuesta.

1.1.1.3 Foros

Se utilizan para facilitar una comunicación activa entre alumnos y profesores pueden ser temáticos, por niveles, por asignaturas, etc. Utilización sencilla por venir implementado en el propio sitio web y no requerir configuración por parte del usuario. La información enviada está accesible para todo el grupo. Quizá sea unas de las herramientas menos utilizadas a no ser por imperativo del tutor, ocurre que muchas veces es difícil seguir una línea conversacional ya que suelen llenarse de aportaciones de escaso interés y repetitivas.

1.1.1.4 Novedades

Permite incluir al profesorado las últimas novedades de interés para el desarrollo de la asignatura y su consulta por los alumnos, son unidireccionales y no permiten respuesta.

1.1.1.5 Chat

Permite la comunicación en línea, en tiempo real y de manera simétrica, se pueden enviar mensaje a todo el grupo o de manera privada a los participantes en la sala de Chat. Este se puede realizar desde un entorno Web o con la utilización de programas adicionales tales como Messenger, etc. Entre los inconvenientes del Chat se surgen cuando en una misma sala concurren varias personas, resultando difícil seguir el hilo de una conversación.

1.1.1.6 Cuenta FTP

Permite consultar, dejar y descargar archivos de todo tipo desde un servidor de FTP. Mediante esta herramienta tanto tutor como alumnos disponen de un espacio en donde colocar cualquier tipo de archivo a la vista de todos los participantes, también es posible hacerlo en zonas restrictivas. (Universidad-Murcia, 2014, pág. 2)

1.1.5 Moodle

Moodle fue diseñado por Martin Dougiamas de Perth, Australia Occidental, quien basó su diseño en las ideas del constructivismo en pedagogía, que afirman que el conocimiento se construye en la mente del estudiante en lugar de ser transmitido sin cambios a partir de libros o enseñanzas y en el aprendizaje colaborativo.

1.1.5.1 Definición de Moodle

Moodle (Modular Object-Oriented Dynamic Learning Environment), es una aplicación que pertenece al grupo de los Gestores de Contenidos Educativos (LMS, Learning Management Systems), también conocidos como Entornos de Aprendizaje Virtuales (VLE, Virtual Learning Managements), un subgrupo de los Gestores de Contenidos (CMS, Content Management Systems).

Moodle es una aplicación para crear y gestionar plataformas educativas, es decir, espacios donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por unos

docentes y organiza el acceso a esos recursos por los estudiantes, y además permite la comunicación entre todos los implicados (alumnado y profesorado).

1.1.5.2 Características de Moodle

- Entorno de aprendizaje modular y dinámico orientado a objetos, sencillo de mantener y actualizar.
- Excepto el proceso de instalación, no necesita prácticamente de "mantenimiento" por parte del administrador.
- Dispone de una interfaz que permite crear y gestionar cursos fácilmente. Los recursos creados en los cursos se pueden reutilizar.
- La inscripción y autenticación de los estudiantes es sencilla y segura. Resulta muy fácil trabajar con él, tanto para el profesorado como el alumnado.
- Detrás de él hay una gran comunidad que lo mejora, documenta y apoya en la resolución de problemas.
- Está basado en los principios pedagógicos constructivistas: el aprendizaje es especialmente efectivo cuando se realiza compartiéndolo con otros.

Moodle se distribuye gratuitamente como Software Libre (Open Source), bajo Licencia pública GNU. Esto significa que Moodle tiene derechos de autor (copyright), pero que tenemos algunas libertades, por ejemplo: podemos copiar, usar y modificar Moodle siempre que aceptemos proporcionar el código fuente a otros, no modificar la licencia original y los derechos de autor, y aplicar esta misma licencia a cualquier trabajo derivado de él.

También es importante destacar que, al ser Moodle una aplicación Web, el usuario sólo necesita para acceder al sistema un ordenador con un navegador web instalado (Mozilla Firefox, Internet Explorer, o cualquier otro) y una conexión a Internet. También se necesita conocer la dirección Web (URL) del servidor donde Moodle se encuentre alojado y disponer de una cuenta de usuario registrado en el sistema. (Baños, 2007, pag.9)

Por estar basado en tecnología PHP, la configuración de un servidor con muchos usuarios debe ser cuidadosa para obtener el mejor desempeño. Falta mejorar su interfaz de una manera más sencilla. Hay desventajas asociadas a la seguridad, dependiendo en dónde se esté alojando la instalación de Moodle y cuales sean las políticas de seguridad y la infraestructura tecnológica con la cual se cuente durante la instalación.

1.2 Análisis de Vulnerabilidades

1.2.1 Definición de vulnerabilidad

Una vulnerabilidad es alguna característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza, intencional o accidentalmente. Las vulnerabilidades pueden provenir de muchas fuentes, desde el diseño o implementación de los sistemas, los procedimientos de seguridad, los controles internos, etc. Se trata en general de protecciones inadecuadas o insuficientes, tanto físicas como lógicas, procedimentales o legales de alguno de los recursos informáticos. Las vulnerabilidades al ser explotadas resultan en fisuras en la seguridad con potenciales impactos nocivos para la organización. (Voutssas, 2010, pág. 1)

1.2.1.1 Características de las vulnerabilidades

- Fallas en el diseño o construcción de programas, sobre todo en aquellos que provienen de un mercado masivo; por ejemplo: sistemas operativos, programas de aplicación, el protocolo de comunicaciones TCP/IP, entre otras.
- Uso de computadoras, programas y equipos de red de tipo genérico en aplicaciones críticas.
- Atención insuficiente al potencial error humano durante el diseño, implementación o explotación de sistemas, particularmente debidas a desviaciones u omisiones de buenas prácticas en estas etapas.
- Confianza excesiva en algún único dispositivo u oficina de seguridad.
- Relajamiento de las políticas y procedimientos de seguridad, debidos a falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso.
- Fallas de seguimiento en el monitoreo o indicadores de seguridad.
- Pobre o nula gobernanza de los activos informáticos, debida principalmente a un mal seguimiento de esos activos y sus contextos de seguridad asociados de forma integral.
- Cambio frecuente de elementos de la plataforma informática.
- Falla en la adjudicación o seguimiento de responsabilidades.
- Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas.
- Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.
- Equipos, programas y redes "heredados" de generaciones tecnológicas anteriores.
- Errores inherentes al diseño de microprocesadores y micro códigos que se encuentran en rutinas básicas o "núcleo" de los sistemas, o en el encriptado o virtualización.

- Falta de concientización del personal en general acerca de la importancia de la seguridad y responsabilidades compartidas e integrales. (Voutssas, 2010, pág. 1)

1.2.2 Tipos de vulnerabilidades Informáticas

La identificación de los diferentes tipos de vulnerabilidades, permite conocer la variedad de ataques que podrían ser efectuados y realizados por una persona no autorizada a ver, alterar o modificar el sistema. Se procederá a descripción general de los principales ataques.

1.2.2.1 Ingeniería Social.

Consiste en persuadir a los usuarios para que ejecuten acciones o revelen la información para superar las barreras de seguridad.

1.2.2.2 Negación de servicio (Denial of service, DoS)

Es un tipo de ataque cuya meta fundamental es la de impedir el uso legítimo o negar el acceso a un recurso determinado.

1.2.2.3 Cracking de passwords

Existen dos métodos:

- Diccionario: Consiste en efectuar encriptaciones de palabras (posibles claves) y comparar estas encriptaciones con el original.
- Fuerza Bruta: Consiste en realizar todas las combinaciones posibles de un conjunto de caracteres. En el siguiente cuadro se ve el tiempo de búsqueda de una contraseña de acuerdo a la longitud y tipo de caracteres utilizados. (Cifuentes, 2004, pág. 11)

1.2.2.4 E-mail bombing y spamming

El e-mail bombing consiste en enviar muchas veces el mismo mensaje a una misma dirección. El spamming, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios.

1.2.2.5 Escaneo de puertos

Existen herramientas para verificar los servicios que presta una máquina por medio de la revisión de los puertos abiertos.

1.2.2.6 Buffer Overflows

Es posible corromper la pila de ejecución escribiendo más allá de los límites reservados para un programa en ejecución. La pila es una estructura last-in, first- out (último en entrar, primero en salir) en la que los datos sucesivos se "colocan encima" de los anteriores.

Los errores de programación que causan el desbordamiento son:

- Combinaciones no esperadas: Los programas usualmente son construidos usando muchas capas de código, todas las capas se colocan encima del sistema operativo, Un mal diseño de una capa puede causar que entradas pertenecientes a la capa superior de la aplicación sea mandada directamente al sistema operativo y ejecutado.
- Entradas anormales: La mayoría de los programas manejan parámetros o valores suministrados como entradas válidas. Si un programador no considera un tipo de entrada que el programa no puede manejar, ocasionará el daño de los datos de la aplicación.
- Condiciones de carrera: "Situación en la que dos o más procesos leen o escriben en un área compartida y el resultado final depende de los instantes de ejecución de cada uno. Cuando esto ocurre y acciones que deberían ser particulares no lo son, existe un intervalo de tiempo en el que un atacante puede obtener privilegios y violar la seguridad del sistema" (Cifuentes, 2004, pág. 12)

1.2.2.7 Transmisión en Texto Plano

Servicios como el Telnet, FTP y HTTP no utilizan ningún método de encriptación de la información enviada (recibida) al (del) cliente, dándole la posibilidad a un tercero de interceptar el tráfico y comprender los datos de la transferencia.

1.2.2.8 Programas Dañinos (creados intencionalmente).

Son programas diseñados para atacar al sistema o para conseguir información sensible. Su funcionamiento está basado en el aprovechamiento de errores en los servicios o en partes inseguras del sistema.

1.2.2.9 Sniffers

Los sniffers operan activando una de las interfaces de red del sistema en modo promiscuo. En este modo de configuración, el sniffer almacenará en un log todo el tráfico que circule por la tarjeta de red, ya sea destinado o generado por el propio sistema o desde/hacia cualquiera de los sistemas existentes en el entorno de red compartido. De igual manera, pueden ser instalados tanto en sistemas como en dispositivos de red.

La utilización de un sniffer permite la obtención de una gran cantidad de información sensible enviada sin encriptar, como por ejemplo usuarios, contraseñas, direcciones de correo electrónico, etc. El análisis de la información transmitida permite a su vez extraer relaciones y topologías de las redes y organizaciones.

Aparte de los programas independientes existentes para ésta tarea, los sistemas operativos poseen sniffers en las distribuciones comerciales, típicamente utilizados por el administrador de red para resolver problemas en las comunicaciones. (Cifuentes, 2004, pág. 13)

1.3 Fases de para verificar una vulnerabilidad Informática

1.3.1 Análisis de vulnerabilidades (Vulnerability Assessment)

Este tipo de análisis no es intrusivo, el objetivo es buscar vulnerabilidades en los sistemas evaluados, con el fin de clasificarlas y presentarlas de forma estructurada.

1.3.2 Test de Intrusion (Penetration Testing)

Consiste en realizar varios tipos de pruebas, aprovechando las vulnerabilidades encontradas y de esta manera comprometer los sistemas. Este tipo de auditorías de seguridad es más invasivo que el análisis de vulnerabilidades y puede ser dirigido a un solo objetivo.

1.3.3 Hacking Ético:

La diferencia específica con el test de intrusión, es que es más completa la auditoria en relación con los dispositivos (Servidores de Datos, Firewall, IDS, router) las pruebas que se realizan son más rigurosas, además de la existencia de un pacto previo con el cliente, para poder hacer pruebas de tipo de “denegación de Servicio e Ingeniería social” en horarios planificados que no perjudique el normal funcionamiento laboral de la Institución. (Quirumbay, 2015, pág. 50)

1.4 Seguridad Informática

1.4.1 Definición de seguridad informática

La seguridad en un ambiente de red es la habilidad de prevenir, identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información e equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo se puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización a organización. Independientemente, cualquier compañía con una red debe de tener una política de seguridad que se dirija a conveniencia y coordinación. (Perpiñan, 2011, pág. 6)

1.4.2 Importancia de la seguridad informática

El número de empresas e individuos que utilizan Internet crece cada día. Como el número de usuarios se expande, así mismo aumenta el número potencial de víctimas como objetivos y Crackers. La seguridad debe de incrementarse para proteger a los usuarios de Internet de aquellos que pueden robar información confidencial. Para mantener segura la información que viaja a través de la red esta debe cumplir con tres requisitos:

- **Integridad:** Requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.
- **Confidencialidad:** Se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación
- **Disponibilidad:** Se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella. (González, 2012, pág. 3)

1.4.3 Seguridad en Internet

La magnitud del Internet crea oportunidades para que este sea mal utilizado. Muchas compañías en línea han reportado el robo de número de tarjetas de créditos vía Internet. Los bancos han continuado moviendo la mayoría de sus negocios a Internet. Servicios en línea, denominados como Internet-Banking, tales como información de la cuenta, verificación en línea y pagos directos, hacen que los bancos y sus clientes sean blancos para los crackers. Las Agencias de

Gobierno confían cada vez más en Internet para sincronizar esfuerzos. Agencias tales como NASA, FBI, CIA y NSA están usando Internet para enviar, almacenar y procesar información. La información que ellos poseen (ejemplo medicina, financiera y récords de criminales) son blancos potenciales para los crackers. (Perpiñan, 2011, pág. 8)

1.4.4 Seguridad Física

La seguridad física es un aspecto fácilmente pasado por alto en la seguridad que concierne a Internet. A menudo, la seguridad en Internet es asociada con los cortafuegos, enmascaramiento de IP y otros métodos electrónicos de protección. Aunque todos esos aspectos son importantes en la seguridad de Internet, como también es importante asegurar también los equipos físicamente.
La seguridad física debe de comenzar con una revisión de las facilidades donde un sistema computacional es alojado. Examinar la fuerza de las puertas, cerraduras y ventanas. Estimando la dificultad de entradas forzadas en el edificio y las oportunidades de ser capturados. Están los sistemas de alarma en su lugar.(Perpiñan, 2011, pág. 9)

1.4.5 Seguridad personal

La seguridad en el trabajo comienza en los niveles más básicos, los trabajadores. Cuando se contrata un nuevo empleado, las referencias pueden ser requeridas y verificadas. Es también importante verificar el pasado de los empleados. Después de que la decisión de contratar un empleado es hecha, este debe de ser entrenado e informado de las medidas de seguridad que serán tomadas, incluyendo triturado de toda la información, frecuentemente cambiando y eligiendo la contraseña apropiada y la encriptación de email.

Otra manera de garantizar la seguridad personal es monitorear a los empleados cuidadosamente. El grado de como una compañía debe monitorear un empleado ha sido actualmente traído ante las cortes con personas que demandan por violaciones de a su privacidad. Es importante respetar los derechos de los empleados mientras se les esté monitoreando. (Perpiñan, 2011, pág. 9)

1.4.6 La seguridad como un proceso en curso

La tecnología de Seguridad del Internet avanza constantemente. A medida que más individuos, compañías y organizaciones comienzan a conducir sus negocios en línea, la demanda de seguridad se incrementa. Sin embargo, cada vez que un problema es arreglado, es posible que se haya creado otra vulnerabilidad.

La seguridad siempre será un proceso en curso. La seguridad es parecida a estar en salud, no porque estamos en salud podemos entonces descuidar nuestro comportamiento de dietas, ejercicios, etc. Es importante nunca parar de cuidar nuestra salud y se nos descuidamos lo suficiente la nuestra salud se derrumba. Siempre hay que estar verificando los agujeros de seguridad. Monitoreando sitios como CERT/CC ayudará con este proceso. Ingresar a una lista de servicios con problemas de seguridad y mantenerse actualizado con la tecnología, siempre continuando con su educación.

No hay manera de estar completamente seguro; es solo posible tomar precauciones a través del aprendizaje y atendiendo las vulnerabilidades de su sistema o red y creando políticas de backup para minimizar los efectos de una brecha de seguridad. (Perpiñan, 2011, pág. 10)

1.5 Ataques a la Seguridad Informática

1.5.1 Definición

Un ataque se refiere a las distintas personas que tratan de manera ilegal, la obtención de acceso, datos o información, también, a aquellos que tratan de atacar a una organización con el único fin de la destrucción de la misma, hay atacantes que solo por gusto o curiosidad quieren probar sus habilidades contras ellas, y estos pueden ser: hackers, cracker y otros habitantes del ciberespacio. (Bustamante, 2016, pág. 26). En este apartado se conocerá las diferentes técnicas ataques y herramientas que utilizan para alcanzar entrar a una red informática, y controlar la red, además el robo de información sensible del sistema.

1.5.2 Tipos de ataques en la seguridad

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos los cuales son:

1.5.2.1 Ataques pasivos

Son oidores o monitoreo de las transmisiones. El objetivo de quienes realizan ese tipo de ataque es obtener la información que se está transmitiendo. En este tipo de ataque se pueden encontrar:

- **Divulgación del contenido de un mensaje:** es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida; como por ejemplo escuchar una llamada telefónica, leer un correo electrónico abierto.

- **Análisis de Trafico:** Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que está siendo transmitido aun cuando esté protegido por medio de cifrado. (González, 2012, pág. 4)

1.5.2.2 Ataques activos

Suponen modificaciones de los datos o creación de flujos de datos falsos. Dentro de este tipo de ataques se pueden encontrar:

- **Enmascaramiento:** Es un tipo de ataque activo que tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial.
- **Repetición:** Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- **Modificación de Mensajes:** Se modifican los mensajes para producir efectos no autorizados.
- **Denegación de Servicios:** Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin específico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma. (González, 2012, pág. 5)

1.5.3 Clasificación de los intrusos en las redes

1.5.3.1 Hackers

Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito. (Gómez, 2005, pág. 9)

1.5.3.2 Crackers ("blackhats")

Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivada por intereses económicos, políticos, religiosos, etc.

- **Sniffers:** Los sniffers son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.
- **Phreakers:** Los phreakers son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los phreakers desarrollaron las famosas "cajas azules", que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando éstas todavía eran analógicas.
- **Spammers:** Los spammers son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.
- **Piratas informáticos:** Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual. (Gómez, 2005, pág. 9)

1.5.3.3 Creadores de virus y programas dañinos

Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad. (Gómez, 2005, pág. 9)

1.5.3.4 Lamers ("wannabes"): "Script- kiddies" o "Click-kiddies"

Los "lamers", también conocidos por "script kiddies" o "click kiddies", son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan ni como los hacen. (Gómez, 2005, pág. 10)

1.5.4 Fases de un ataque informático

Los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

- Descubrimiento y exploración del sistema informático.
- Búsqueda de vulnerabilidades en el sistema.
- Explotación de las vulnerabilidades detectadas (para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como "exploits").
- Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas

con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado.

- Eliminación de las pruebas que puedan revelar el ataque y el compromiso del sistema: eliminación o modificación de los registros de actividad del equipo ("logs"); modificación de los programas que se encargan de monitorizar la actividad del sistema. Muchos atacantes llegan incluso a parchear la vulnerabilidad descubierta en el sistema para que no pueda ser utilizada por otros intrusos. (Gómez, 2005, pág. 11)

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido). Estos tres factores constituyen lo que podríamos denominar como el "Triángulo de la Intrusión", concepto que se presenta de forma gráfica en la siguiente figura:

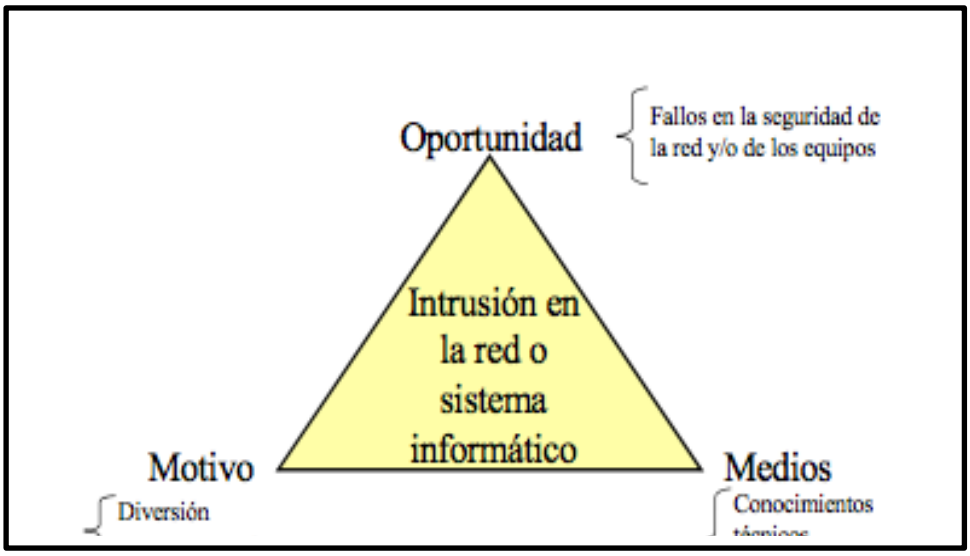


Figura 1-1: El "Triángulo de Intrusión**"**
Fuente: (Gómez, 2005, pág. 11).

1.5.5 Herramientas para realizar ataques informáticos

En cuanto a los medios y herramientas de disponibles en la actualidad para llevar a cabo sus ataques ("Hacking Tools"), podríamos citar las siguientes:

- **Escáneres de puertos:** permiten detectar los servicios instalados en un determinado sistema informático.

- **Sniffers:** dispositivos que capturan los paquetes de datos que circulan por una red. Para ello, también se podría utilizar un equipo conectado a la red con su tarjeta de red (NIC) configurada en "modo promiscuo", para poder procesar todo el tráfico que recibe (aunque vaya dirigido a otros equipos). Por otra parte, existen sniffers especializados en la captura de contraseñas u otros datos sensibles (como los números de cuenta o de tarjetas de crédito).
- **"Exploits":** herramientas que buscan y explotan vulnerabilidades conocidas.
- **"Backdoors kits":** programas que permiten abrir y explotar "puertas traseras" en los sistemas.
- **"Rootkits":** programas utilizados por los atacantes para ocultar "puertas traseras" en los propios ficheros ejecutables y servicios del sistema, que son modificados para facilitar el acceso y posterior control del sistema.
- **"Auto-rooters":** herramientas capaces de automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles vulnerabilidades, explotar una determinada vulnerabilidad y obtener el acceso al sistema comprometido.
- **"Password crackers":** aplicaciones que permiten averiguar las contraseñas de los usuarios del sistema comprometido.
- Generadores de virus y otros programas malignos.
- Herramientas que facilitan la ocultación y la suplantación de direcciones IP (técnicas de "spoofing"), dificultando de este modo la identificación del atacante.
- Herramientas de cifrado y protocolos criptográficos (como PGP, SSH, SSL o IPSec): cada vez es más frecuente que el atacante utilice protocolos criptográficos en sus conexiones con los sistemas y máquinas que ha conseguido comprometer, dificultando de este modo su detección y estudio. (Gómez, 2005, pág. 12)

1.6 Políticas de Seguridad

1.6.1 Definición

Para proteger un sistema, se debe realizar un análisis de las amenazas potenciales que éste puede sufrir, las pérdidas que podrían generar y la probabilidad de su ocurrencia. Este estudio genera las políticas de seguridad que definen las responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se realicen. (Cifuentes, 2004, pág. 20)

1.6.2 Mecanismos de Seguridad

Para implementar estas políticas de seguridad se utiliza lo que se conoce como mecanismos de seguridad. Los mecanismos de seguridad se dividen en tres grupos:

- **Prevención:** Aquellos que aumentan la seguridad de un sistema durante su funcionamiento normal.
- **Detección:** Aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.
- **Recuperación:** Aquellos que se aplican cuando el sistema ha sido atacado. (Cifuentes, 2004, pág. 21)

1.6.3 Elementos de la Seguridad

A continuación, se mostrará los elementos de seguridad más importantes, también se muestra la jerarquía en que esos elementos están organizados. Los niveles serán mostrados comenzando desde los más bajos:

1. Política de Seguridad Corporativa
2. Autenticación del Usuario
3. Encriptación y Control de Acceso
4. Auditoria y Administración

Cada uno de esos elementos opera en conjunto con los otros para asegurar que una Organización puede comunicarse lo más eficientemente posible. Al principio del listado se encuentra las políticas de Seguridad Corporativa, la cual establece la fundación de cualquier sistema de seguridad exitoso. Teniendo una política de seguridad no garantiza que se eliminarán los intrusos o la perdida de la información. Para esos ítems, usted tiene que auditar cuidadosamente su red. Sin embrago, una política de seguridad lo hace proveer un fundamento para todas las acciones subsecuentes. (Perpiñan, 2011, pág. 28)

1.6.3.1 Responsabilidad

Los Administradores implementan y hacen cumplir las políticas de seguridad y auditan la actividad de los usuarios, procurando señalar los problemas de seguridad, los cuales pueden incluir actividad ilícita de un empleado, un sistema con un nivel bajo de parches o un intruso fuera de la red. La administración y los administradores seguridad deben de crear las políticas de seguridad corporativa porque esto provee los fundamentos para todas las actividades de la red.

1.6.3.2 La Política de Seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que la misma debe establecer un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos de operación, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y él porqué de ello, pues cada política de seguridad es una invitación a cada uno de sus empleados a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, la política de seguridad debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos. (Perpiñan, 2011, pág. 29)

1.6.3.3 Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante. Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso. (Perpiñan, 2011, pág. 29)

1.6.3.4 Parámetros para Establecer Políticas de Seguridad

Es importante que, al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas. (Perpiñan, 2011, pág. 30)

1.7 Test de Penetración

Las pruebas de penetración (también llamadas “pen testing”) son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar

El principal objetivo de las pruebas de penetración consiste en determinar las debilidades de seguridad. Una prueba de penetración también puede ser utilizada para probar el cumplimiento de la política de seguridad de una organización, la conciencia de seguridad de sus empleados y la capacidad de la organización para identificar y responder a los incidentes de seguridad. (Rouse Margaret, 2017)

1.7.1 Importancia del Test de penetración

- Determinar la viabilidad de un conjunto particular de vectores de ataque.
- Identificar las vulnerabilidades de alto riesgo que resultan de una combinación de vulnerabilidades de menor riesgo explotados en una secuencia particular.
- Identificar las vulnerabilidades que pueden ser difíciles o imposibles de detectar con los sistemas automatizados de la red o por software de detección de vulnerabilidades.
- Probar la capacidad de las defensas de la red para detectar con éxito y responder a los ataques.

1.7.2 Faces de un test de penetración

Fase de reconocimiento: Esta sea una de las etapas que más tiempo demande. Asimismo, se definen objetivos y se recopila toda la información posible que luego será utilizada a lo largo de las siguientes fases. La información que se busca abarca desde nombres y direcciones de correo de los empleados de la organización, hasta la topología de la red, direcciones IP, entre otros.

Fase de escaneo: Utilizando la información obtenida previamente se buscan posibles vectores de ataque. Esta etapa involucra el escaneo de puertos y servicios. Posteriormente se realiza el escaneo de vulnerabilidades que permitirá definir los vectores de ataque.

Fase de enumeración: El objetivo de esta etapa es la obtención de los datos referente a los usuarios, nombres de equipos, servicios de red, entre otros.

Fase de acceso: En esta etapa finalmente se realiza el acceso al sistema.

Fase de mantenimiento de acceso: Luego de haberse obtenido el acceso al sistema, se busca la manera de preservar el sistema comprometido a disposición de quien lo ha atacado. El objetivo es mantener el acceso al mencionado sistema perdurable en el tiempo. (CATOIRA, 2012)

1.7.3 Test de penetración a utilizar

El test de penetración utilizado en este trabajo de titulación esta descrito en el capítulo 2 y está enumerado de la siguiente manera:

1. Recolección de información
2. Escaneo de puertos
3. Explotación de vulnerabilidades
4. Implementación de guía de mejores practicas

Además, la investigación está basada en el Proyecto abierto de seguridad de aplicaciones web Owasp (acrónimo de Open Web Application Security Project), es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

El proyecto abierto de seguridad en aplicaciones Web (OWASP) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que pueden ser confiables. En OWASP se encontrará:

- Herramientas y estándares de seguridad en aplicaciones
- Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro, y revisiones de seguridad en código fuente.
- Controles de seguridad estándar y librerías
- Capítulos locales en todo el mundo
- Investigaciones de vanguardia
- Extensas conferencias alrededor del mundo
- Listas de correo

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada con ninguna compañía de tecnología, aunque apoyamos el uso instruido de tecnologías de seguridad comercial. Al igual que muchos otros proyectos de software de código abierto, OWASP produce muchos tipos de materiales en una manera abierta y colaborativa.

La dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente. No se puede dar el lujo de tolerar problemas de seguridad relativamente sencillos, como los que se presentan en este OWASP Top 10.

El objetivo del proyecto Top 10 es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. El proyecto Top 10 es referenciado por muchos estándares, libros, herramientas, y organizaciones, incluyendo MITRE, PCI DSS, DISA, FCT, etc.

OWASP Top 10 fue lanzado por primera vez en 2003, con actualizaciones menores en 2004 y 2007. La versión 2010 fue renovada para dar prioridad al riesgo, no sólo a la prevalencia. La edición 2013 sigue el mismo enfoque. (Owasp, 2013, Pag 2).

OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP esta lista se publica y actualiza cada tres años por dicha organización.

En la siguiente tabla esta 5 de los ataques encontrados con los softwares Nessus y Nexpose en el servidor E-learning de la ESPOCH que se comparó con esta lista OWASP Top 10, y se escogió para hacer los escaneos y pruebas necesarias para la realización de los objetivos planteados de este trabajo de titulación.

Figura 2-1: Top de los mejores ataques a servidores según Owasp
Fuente: (Owasp, 2013, Pag 4)

1.8 Situación actual del servidor E-learnig de la Espoch

Se ha obtenido la siguiente información del servidor E-learning de la ESPOCH, el mismo que se encuentra ubicado en la provincia de Chimborazo en la ciudad de Riobamba, bajo la administración de la Dirección de tecnologías de la información y comunicación (DTIC), siendo el responsable directo el Ing. Gustavo Hidalgo.

Al realizar una verificación del dominio de la página principal de la ESPOCH a través de la página WHOIS.NET ingresando únicamente el nombre de dominio: espoch.edu.ec, se obtiene datos significativos como correos electrónicos y números telefónicos del personal técnico que labora en el data center, como lo veremos en la Tabla No 2-1.

Tabla 2-1: Recolección de información con Whois.net

Nombre Local	ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO
Dirección del Local	Panamericana Sur Km 1.5 Riobamba, Chimborazo EC060155 EC
Información del Dominio	Created: 15 Jan 1999 Modified: 14 Dec 2016 Expires: 15 Jan 2020
Servidores de DNS	dns.espoch.edu.ec ns2.he.net ns3.he.net ns4.he.net

Contacto Administrativo	Local Name: Byron Vaca Email Address: redes@espoch.edu.ec Phone Number: +00.59332998200
Contacto Técnico	Local Name: David Garces Email Address: dgarces@espoch.edu.ec Phone Number: +00.59332998200

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Fuente: http//www.whois.net/

Como se observa la información es significativa, como la dirección del servidor, 3 correos electrónicos, 3 números telefónicos, y además los nombres de los Ingenieros encargados del mantenimiento de los equipos.

Los servidores de la ESPOCH están siendo administrados por el Departamento de Tecnología de Información y Comunicación (DTIC), que cuenta con una infraestructura para el correcto funcionamiento de los servidores, además cuentan con sistemas de cuartos de enfriamiento automático, sistemas de alimentación regulada y controlada por UPS, generadores diésel en caso que se vaya el fluido eléctrico en la Institución, además está equipada con sistemas de control de acceso restringido en las puertas para usuarios no autorizados, actualmente la ESPOCH fue actualizada en su infraestructura con una nuevos equipos de Core que es el corazón de la red, nuevos switches que se encargan de comunicarse con cada facultad y cada departamento de la Institución, y con la reciente adquisición de nuevas líneas de fibra óptica para cada facultad elevando notoriamente la transmisión de datos en comparación con la infraestructura anterior.

La ESPOCH tiene diversos servidores como: servidores web, servidores de Microsoft IIS, servidores virtuales, servidores de bases de datos, servidores de correo electrónico, servidores FTP, servidores Radius, entre otros. Pero nuestro trabajo de titulación está dirigido al servidor web E-learning de la ESPOCH. En este servidor está enfocado la investigación de trabajo de titulación, poder demostrar que es un servidor vulnerable ante cualquier amenaza y el propósito es poder asegurarlo o proteger ante amenazas ya que es un servidor que está en constante actividad y es necesario para el estudio diario de los estudiantes.

El servidor E-learning de la ESPOCH se encuentra funcionando bajo los técnicos de la DTIC y está bajo la responsabilidad del departamento de desarrollo, los cuales actualizan sus bases de datos, actualizan materias, estudiantes y cursos, bajo su responsabilidad también está la base de datos de contraseñas e información sensible de datos de los estudiantes y profesores.

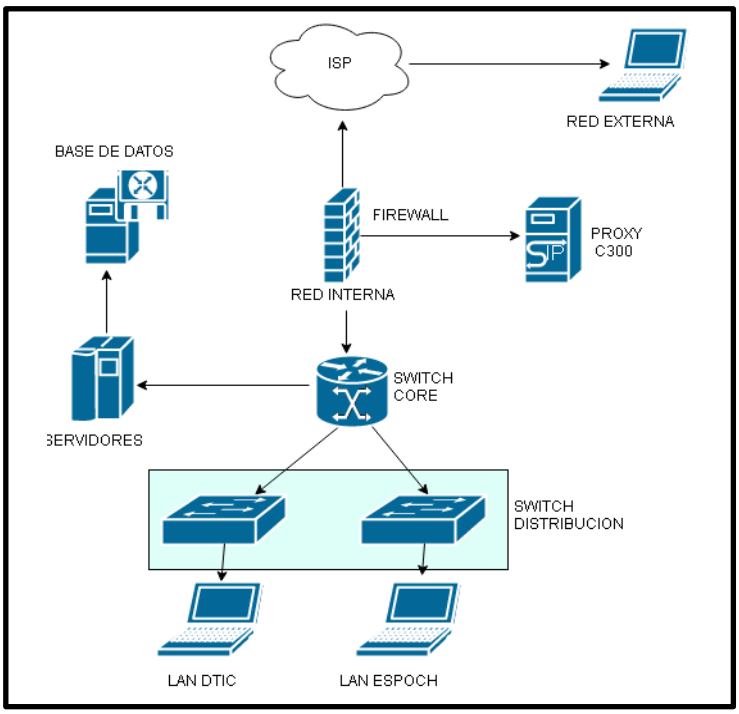


Figura 3-1: Escenario diseño lógico actual del servidor E-learning
Realizado por: Montesdeoca, R, Alvarado, A. 2017

Este escenario demuestra el esquema lógico de cómo está operando la red de servidores en el departamento DTIC y da servicio a todos los estudiantes y docentes de la ESPOCH. Este esquema se divide en dos partes fundamentales para acceder a los servidores, una es dentro de la institución y la otra forma es desde un equipo en internet, un usuario que desea acceder al servidor E-learning desde el internet, primero deberá llegar a un equipo de Firewall, acceder al Switch de Core y le re-direcciona al área del servidor, el servidor hace peticiones a la base de datos para mostrar al usuario la página web con toda la información requerida.

CAPITULO II

2 MARCO METODOLOGICO

2.1 Análisis de vulnerabilidades del Servidor E-learning de la ESPOCH

La metodología que será usada para la elaboración de este trabajo de titulación es una metodología clásica, consta de 4 fases las cuales serán adaptadas para las necesidades en la implementación del trabajo de titulación en los servidores del E-learning de la ESPOCH. Las fases utilizadas en este proyecto serán las siguientes:

2.1.1 Fase 1: Recolección de información del objetivo de evaluación

En esta fase el objetivo es recopilar toda la información necesaria sobre la red objetivo, partiendo de su dominio público, obtener su protocolo de internet público (IP por sus siglas en inglés), e ir obteniendo muchas características de la red como lo haría un atacante informático. En esta fase no se busca ninguna vulnerabilidad, lo que se pretende es obtener la mayor cantidad de datos accesibles que den un panorama general de la red objetivo. Se hará uso de herramientas online y herramientas instaladas en el equipo, para la presente investigación se usará la herramienta NMAP de código libre.

2.1.2 Fase 2: Escaneo de puertos y enumeración de servicios

Del proceso anterior se obtiene una lista de todas las características de la red, además de las características de su funcionamiento. En esta fase se examinarán los puertos y servicios activos en el sistema dando una idea general de los servicios activos del servidor, con esta información un técnico o un espía informático puede tener un panorama claro de la funcionalidad del server, además mirar las versiones de los diferentes softwares, y tener así una enumeración detallada para posteriormente realizar un ataque más específico.

2.1.3 Fase 3: Explotación de vulnerabilidades

En esta fase el servidor E-learning de la ESPOCH será sometido a un proceso de evaluación de vulnerabilidades que consiste en encontrar todas las debilidades críticas del sistema, para lo cual

se utiliza un escáner de vulnerabilidades. El objetivo principal es detectar los potenciales riesgos en la seguridad del servidor y cuales juegan un rol más crítico para la seguridad del mismo.

Se seleccionó algunas herramientas como: Nexpose, Nessus con la finalidad que se complementen entre si y dar un diagnostico seguro, evitando falsas alarmas o falsos resultados al momento de implementar las respectivas correcciones de seguridad y posteriormente la implementación de las mejores prácticas de seguridad y Acceso dentro de la Institución.

2.1.4 Fase 4: Implementación de Mejores Prácticas

Una vez que se han realizado los escaneos respectivos al servidor, se realizara y se implementara una guía paso a paso que demostrar algunas soluciones de seguridad como: SSL, DMZ, Firewal, IPS, AMP, etc. Para mejorar la seguridad del servidor Elearning de la ESPOCH.

2.2 Herramientas para el análisis y escaneo del servidor E-learning de la ESPOCH

Las siguientes herramientas de software descritas a continuación ayudaran a encontrar toda la información, escaneo y vulnerabilidades del servidor E-learning de la ESPOCH. Las mismas que resolverán las fases de análisis 1 y 2 del test de penetración.

2.2.1 Nmap

Se utilizó este software principalmente por que realiza pruebas rutinarias de Redes, auditorias de seguridad y recolecta información para futuros ataques, por lo que este software cumple las necesidades y requerimientos para la utilización en las pruebas de escaneo propuestas en el servidor E-learning para este trabajo de Titulación.

Nmap es un software libre y licencia Open Source, y existe una versión para cada sistema operativo, en nuestro caso será para el sistema operativo Linux. (Luis, 2015, pág. 3). La herramienta Nmap nos da una gran cantidad de datos del servidor en la primera fase 1 de Recolección de Información, esta guía de recolección se encuentra en el ***Anexo A***. La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado.

El estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o

paquetes en ese puerto. Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado.

La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC. (Nmap.org)

2.2.2 Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Realiza el escaneo en el sistema objetivo, y el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Vamos hacer una comparativa con otros tipos software que tienen el mismo objetivo para ver cual nos conviene más para la realización del trabajo de titulación. Estos softwares son los tres principales de una lista de correo de Nmap.

Tabla 1-2: Comparativa entre software de seguridad

Característica	Nessus	Ethereal	Snort:
Software libre	X	X	X
Fácil instalación	X		
Trabaja netamente con Linux	X		
Trabaja con otras plataformas	X	X	X
Genera reportes	X	X	X
Analizador de protocolos		X	
Sistema de detección de instrucciones			X
Herramienta de evaluación de seguridad	X		

Realizado por: Montesdeoca, R; Alvarado, A. 2017
Fuente: http://insecure.org/tools/tools-es.html

Dada la comparativa de los diferentes softwares que muestra en la Tabla 3, se tomó la decisión de trabajar con Nessus debido a que es una herramienta de evaluación de seguridad y por las múltiples características que se analizó, además cuenta con unas características detalladas a continuación:

- Referencia mundial, porque tiene la mayor base instalada y una mejor experiencia en industria, Nessus ofrece a los clientes la, capacidad de identificar sus mayores amenazas y responder rápidamente.
- Tiene paneles de mando detallados para ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas.
- Es rentable porque reduce el tiempo y costo de seguridad en el escaneo y asegura los cumplimientos de seguridad.

2.2.3 Nexpose

Nexpose es una herramienta que permite ejecutar diferentes tipos de escaneos en búsqueda de vulnerabilidades en un host o red, permite la definición de determinadas opciones que nos permiten acceder a un escaneo mucho más preciso con el uso de filtros por puertos. Además, cuenta con una gran base de datos que almacena la información de cada escaneo, también crea informes para poder remediar las vulnerabilidades encontradas y da el resultado a usar en cada vulnerabilidad crítica.

Todos los escáneres en el torneo son sin duda potentísimas herramientas de escaneo, que permiten simplemente a través de indicar una URL detectar un gran número de posibles riesgos en nuestra web, pero impresionan los resultados obtenidos por Nexpose, acercándose al pleno 19.8 sobre 20, solo flaqueando ligeramente en cuanto a los informes de resultados. En un escenario en que las diferentes soluciones debían escanear aplicaciones web especialmente diseñadas para el evento para detectar los riesgos más comunes (inyección SQL, xss...), **Nexpose** ha conseguido una puntuación casi perfecta, 19.8 sobre 20. (HackMiami, 2013)

	Ease of Interface (1 to 5)	Vulnerability Detection (1 to 5)	Reporting (1 to 5)	Overall Value (1 to 5)	Total Score (1 to 20)
Nexpose	**5**	**5**	**4.8**	**5**	**19.8**
Acunetix	**5**	4	4.5	4	17.5
Appscan	3.5	4	**4.8**	3	15.3
BURP	4	4	3.5	**5**	16.5
NTP Spider	4	3	4	3	14

Figura 1-2: Rango de calificación entre diferentes scanner
Fuente: https://cyberseguridad.net/index.php/347-nexpose-considerado-el-mejor-escaner-de-aplicaciones-web-durante-elhackmiami

Principales beneficios de Nexpose

- Obtiene una protección de clase empresarial con análisis de fecha para más de 40000 vulnerabilidades y 110000 controles a través de sus redes físicas y virtuales, sistemas operativos, bases de datos y aplicaciones web.
- Mejora y toma decisiones estratégicas con Rapid7 Real Risk
- Garantiza el cumplimiento de políticas y directrices de auditoria.
- Obtener visibilidad precisa del riesgo actual con el descubrimiento continuo de todos los activos físicos y virtuales.
- Reduce el costo de vulnerabilidades y evaluación de configuraciones.

2.3 Herramientas para la explotación del servidor E-learning de la ESPOCH

Hay miles de programas que hacen este tipo de ataques, pero se escogió a los mejores de acuerdo a su rama y uso, y se demuestra por qué utilizamos cada uno, para el desarrollo de los ataques al servidor E-learning de la Espoch se utilizaron varias herramientas de software, dándonos así un panorama claro para la solución de la fase 3 que es el test de penetración.

2.3.1 Kali Linux

Según la página web techlog360.com da las 10 mejores distribuciones de Linux para fines de hacking de redes son los siguientes:

1. Kali Linux
2. BackBox
3. Parrot Security OS
4. Live Hacking OS
5. DEFT Linux
6. Samurai Web Testing Framework
7. Network Security Toolkit
8. Bugtraq
9. NodeZero
10. Pentoo

Se escogió los dos principales para hacer una comparativa decidir cuál de estos dos utilizaremos. Vamos a utilizar un rango de 1 a 5, para poder concretar qué sistema operativo tiene las características necesarias para el hacking del servidor E-learning de la ESPOCH.

Tabla 2-2: Comparativa de S.O Kali Linux y BackBox

Característica	Kali Linux	BackBox
Conjunto de Capacidades	5	5
Facilidad de uso	5	4
Soporte Comunitario	4	3
Seguridad y probabilidad de ataque superficial	3	3
Tasa de publicación	5	5
Precios y Soporte	4	4
API y extensibilidad	5	5
Integraciones de terceros	5	4
Programa Bounty Bug	5	0
Empresas que lo usan	5	5
Idioma desarrollado	5	5
Curva de aprendizaje	4	3
Total	55	46

Realizado por: Montesdeoca, R; Alvarado, A. 2017
Fuente: https://www.upguard.com/articles/kali-linux-vs-backbox-pen-testing-ethical-hacking-linux-distros

Debido al resultado obtenido se decidió usar el software Kali Linux, ya que este software es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad, y es la mejor opción en cuanto a hacking.

2.3.2 Owasp

Owasp es un nuevo tipo de organización, permite proveer información sobre seguridad de aplicaciones sin riesgos, practica y efectiva, apoya a la investigación innovadora sobre seguridad. El Proyecto de seguridad en aplicaciones Web (OWASP), es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que puedan ser confiables.

Owasp ha sacado un Top 10 de los principales ataques informáticos, el objetivo es crear conciencia de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. (OWASP, 2013)

Tabla 3-2: Selección de Ataques al servidor

Owasp Top10-2013(nuevo)	Ataca	Selecciona
Inyección (Inyection SQL)	Base de datos	Aplica
Perdida de autenticación y gestión de secciones (SNIFFING)	Redirección a una página falsa	Aplica
Secuencia de comandos en Sitios Cruzados(XSS)	Altera el estado actual	Aplica
Referencia directa insegura a objetos	Manipulación de referencias	No aplica
Configuración de seguridad incorrecta (DoS)	Saturación de paquetes	Aplica
Exposición de datos sensibles	Tarjetas de crédito	No aplica
Ausencia de control de Acceso a las Funciones	Interfaz	No aplica
Falsificación de peticiones en Sitios Cruzados (CSRF)	Solicitud HTTP falsificada.	No aplica
Uso de componentes con vulnerabilidades conocidas	Privilegios	No aplica
Redirecciones y Reenvíos no Validos (PHSHING)	Clona la pagina	Aplica

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Se seleccionó del Top 10 los ataques más comunes en servidores web como se muestra en la tabla anterior, estos cinco ataques seleccionados permitirán demostrar de forma clara que el servidor E-lerning de la Espoch es vulnerable, dándole así mejores prácticas de políticas de seguridad para un servidor más seguro.

2.4 Escenario de trabajo

Este escenario consta de una versión clon del servidor E-learning de la Espoch en una máquina virtual, con el objetivo hacer las pruebas y ataques necesarios que requiere este trabajo de titulación y también por no dañar el servidor de producción original ya que debe estar activo todo el tiempo y la mayoría de estudiantes tienen acceso a este servidor E-learning para realizar trabajos, deberes, foros, chat, exámenes en línea etc., y no puede detener sus servicios.

Dado que revelar toda la infraestructura de red de una empresa son datos sensibles y esa información es restringida se hizo uso del siguiente escenario de pruebas como se lo ve en la figura 5, tomando un clon del servidor haciendo uso de una máquina virtual.

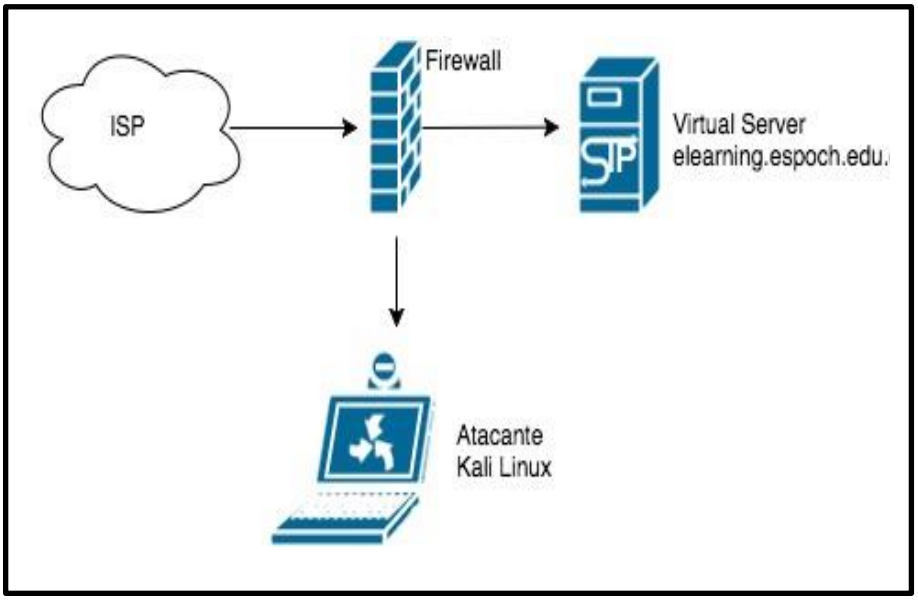


Figura 2-2: Escenario de pruebas para el análisis del servidor E-learning
Realizado por: Montesdeoca, R; Alvarado, A. 2017

Este escenario es una versión clon del servidor E-learning de la ESPOCH, se trabajara en una máquina virtual a través de Kali Linux, se ingresara desde el internet pasando por el Firewal que esta inseguro y dejara pasar directamente al servidor E-learning de la ESPOCH, para de esta manera hacer las pruebas necesarias de escaneo poder implementar la guía de mejores prácticas que servirá para proteger al servidor E-leaning de posibles atacantes y muchas vulnerabilidades a la que está expuesta.

CAPITULO III

3 MARCO DE RESULTADOS Y DISCUSIÓN

En este capítulo se analiza los resultados a los ataques del servidor E-learning que fueron elegidos y basados en la lista de vulnerabilidades propuesta por el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), la cual nos recomienda una lista de 10 ataques comunes basada en 8 conjuntos de datos, 7 firmas especializadas en seguridad de aplicaciones web como SaaS, que abarcan a más de 500.000 vulnerabilidades a través de cientos de organizaciones y miles de aplicaciones. Estas recomendaciones han sido seleccionadas y priorizadas con estimaciones de explotabilidad, detectabilidad e impacto.

Existen cientos de problemas de seguridad de afectan a los servidores o una aplicación web, por lo tanto la seguridad no es una solución sino un proceso que hay que ir actualizando y mejorando constantemente, realizando pruebas y ejecutando parches de seguridad, actualizando software y equipos, ya que cada día más servicios y aplicaciones migran a internet, transferencias de dinero, intercambio de datos personales cada día es más común, por eso muchos atacantes buscan nuevas maneras de acceder a esa información de forma no autorizada.

Las empresas, organizaciones e instituciones están expuestas a un número cada vez más elevado de amenazas que aprovechan cada vulnerabilidad informática para conocer información sensible, datos de usuarios y conocimiento de la red interna, para que personas no autorizadas realicen diversas formas de fraude, espionaje o sabotaje.

Es de vital importancia realizar mediciones periódicas del estado actual de la seguridad de la red, se recomienda realizar un escaneo de la seguridad cada seis meses, en las siguientes páginas de este documento de titulación se demuestra cómo se deberá realizar este análisis y la implementación de las mejores prácticas de seguridad y acceso.

3.2 Resultado del análisis al Servidor E-learnig de la ESPOCH

Los servidores de la ESPOCH están siendo administrados por el DTIC, que cuenta con una infraestructura de red, con sistemas de cuartos de enfriamiento automático, sistemas de alimentación regulada y controlada por UPS, generadores diésel en caso que se vaya el fluido eléctrico, además está equipada con sistemas de control de acceso restringido en las puertas para

usuarios no autorizados, actualmente la ESPOCH fue renovada en su infraestructura de red con nuevos equipos de Switch Core que es el corazón de la red y se encarga de conmutar los paquetes de toda la red a la máxima velocidad, nuevos equipos de Switch de distribución que se encargan de comunicarse con cada facultad y cada departamento de la Institución, uniendo cada enlace con las nuevas líneas de fibra óptica para cada facultad, elevando la velocidad de transmisión de datos en comparación con la infraestructura anterior.

Para la realizar el escaneo de la red, se usó la herramienta Nmap como se lo ve en la figura 3 muestra datos importantes acerca del servidor E-learning como todas las Ips tanto públicas y privadas del servidor, también su proveedor de servicio de internet que es la empresa TELCONET, que da los servicios de internet de fibra óptica y los servidores de nombre de dominio DNS para que se pueda conectar con el mundo a través de la web en internet.

Una información delicada dentro de esta primera fase es conocer el sistema operativo que fue implementado al servidor y cuál es su versión de sistema, dándonos a conocer si el sistema se encuentra actualizado o no. Los sistemas operativos van actualizándose periódicamente es decir cada final de semestre lanzan a los usuarios correcciones de seguridad, parches de puertos, actualizaciones de kernel (núcleo del sistema) y otros servicios que siendo bien configurados proveen una mejor protección ante fallos o ataques a su sistema.

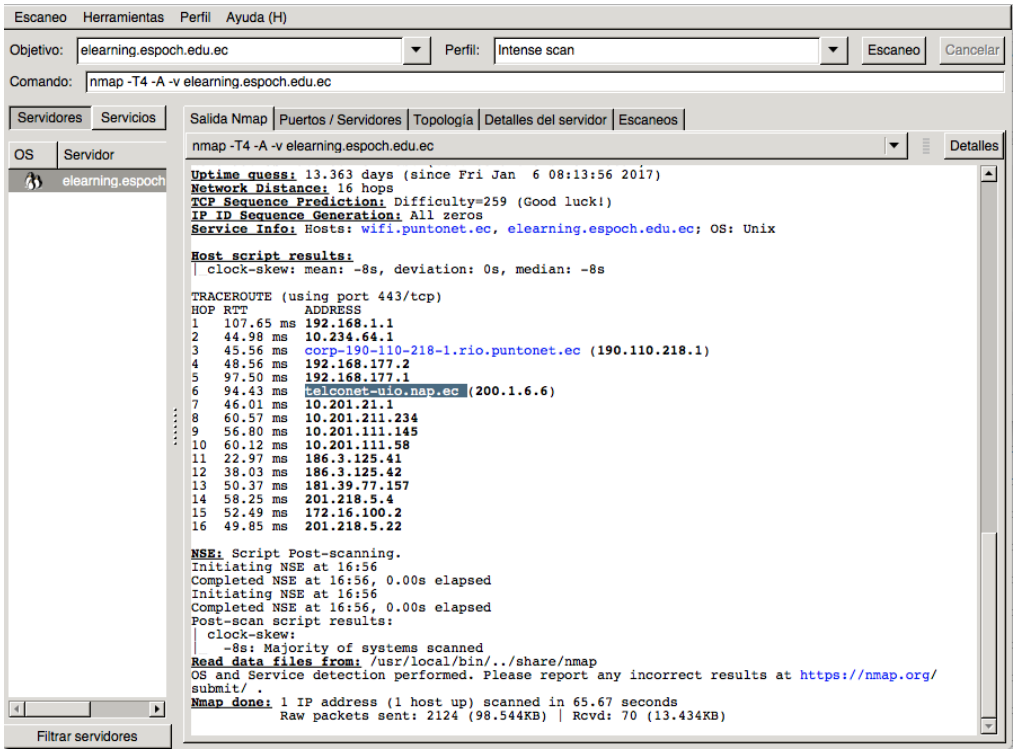


Figura 1-3: Escaneo al Servidor E-learning de la ESPOCH con Nmap
Realizado por: Montesdeoca, R; Alvarado, A. 2017

La topología de red nos ayuda a saber en dónde se encuentra el servidor contando todos los nodos de conexión desde el local host o el equipo que está enviando los paquetes hacia el servidor E-learning. En la figura 6 se observa que el emisor da varios saltos o nodos hasta llegar al receptor, en este caso el servidor, esta fase de reconocimiento permite saber datos sensibles como las IP tanto públicas como privadas, proveedor de servicio y la dirección de red tanto interna como externa.

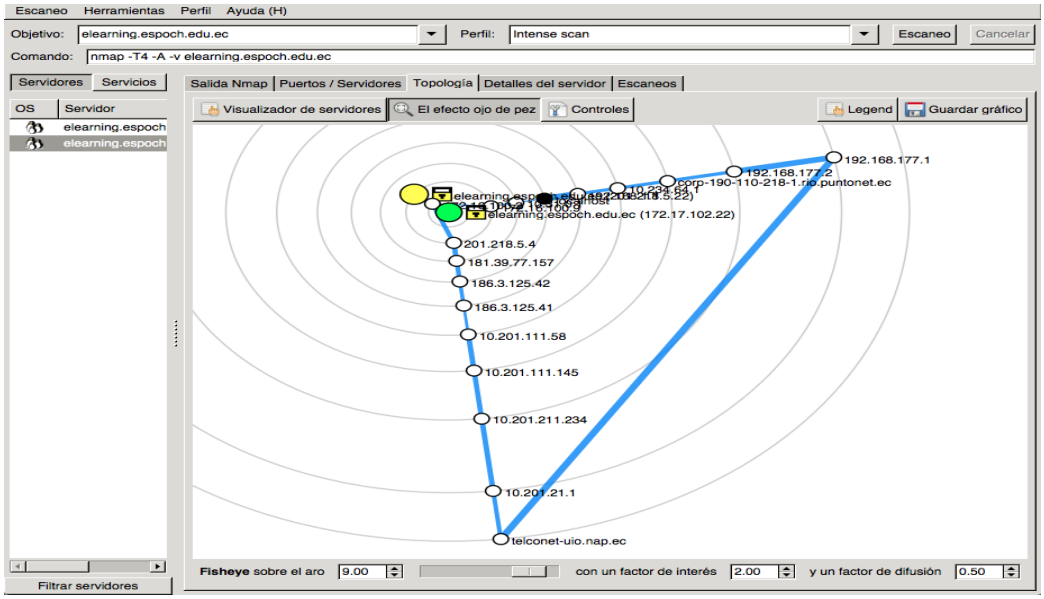


Figura 2-3: Topología de Red del Servidor E-learning de la ESPOCH
Realizado por: Montesdeoca, R; Alvarado, A. 2017

Nmap nos da información de los puertos y los servicios de red, si hay puertos abiertos, los atacantes pueden vulnerarlos y entrar, por eso es indispensable tener la menor cantidad de puertos abiertos dentro del servidor. En la figura 7 podemos observar el resultado del análisis del escaneo de puertos del servidor.

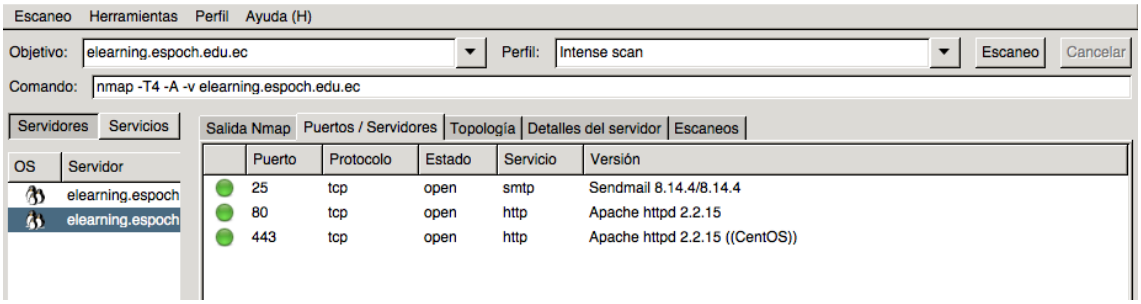


Figura 3-3: Sericios y Puertos Red del Servidor E-learning de la ESPOCH
Realizado por: Montesdeoca, R; Alvarado, A. 2017

En la tabla 1-3 se detallan los principales puertos abiertos encontrados en el servidor y con sus respectivas características:

Tabla 1-3: Puertos abiertos del Servidor E-learning de la Espoch

Puerto	Nombre	Característica
80	Http	Protocolo de transferencia de hipertexto (HTTP) para los servicios del World Wide Web (WWW)
443	Https	Protocolo de transferencia de hipertexto seguro (HTTP)
25	Smtp	Protocolo de correo electrónico

Realizado por: Montesdeoca, Alvarado, 2017
Fuente: Página web: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html

3.3 Resultados de los escaneos del servidor E-learning de la ESPOCH

Nessus es una herramienta para encontrar vulnerabilidades en aplicaciones web, y con ella se realizaron las diferentes búsquedas hasta encontrar las debilidades del sistema. La de implementación y el proceso paso a paso para encontrar las vulnerabilidades se encuentra en la sección de anexos. En la figura 4-3 muestra los resultados del análisis con la herramienta de escaneo Nessus, su implementación y configuración se encuentra en el Anexo A, dando los siguientes datos:

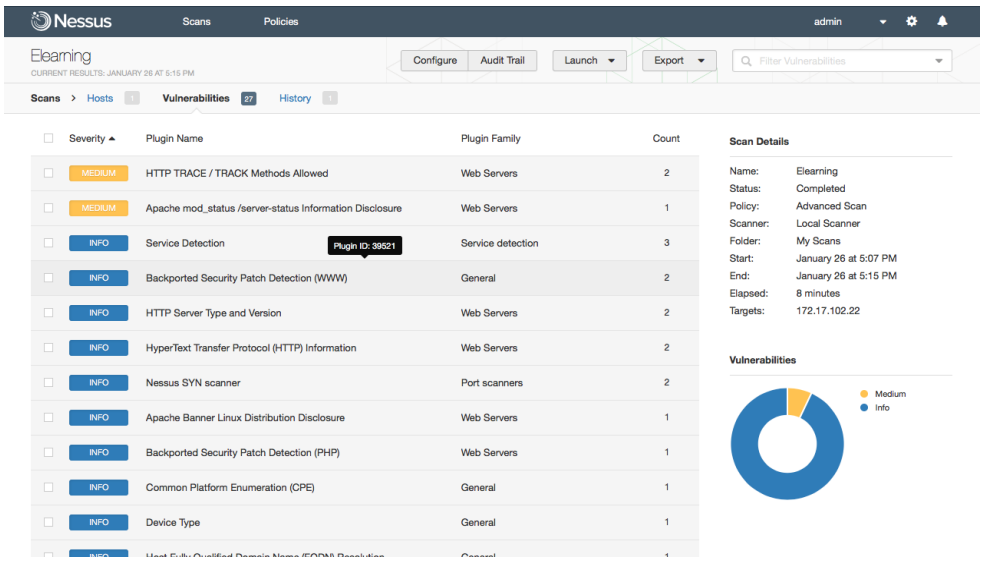


Figura 4-3: Reporte detallado del análisis de vulnerabilidades con Nessus
Realizado por: Montesdeoca, R; Alvarado, A. 2017

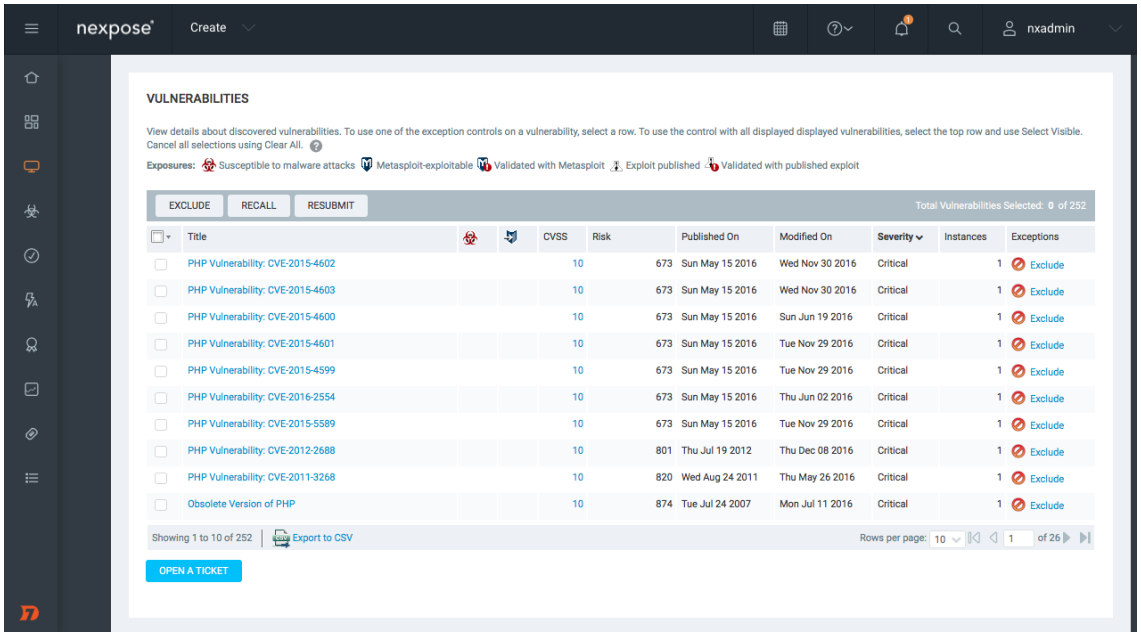


Figura 5-3: Reporte detallado del análisis de vulnerabilidades con Nexpose
Realizado por: Montesdeoca, R; Alvarado, A. 2017

En la figura 5-3 Nessus nos da un reporte con las principales vulnerabilidades encontradas dentro del servidor E-learning, en ella se observa los problemas con las cabeceras http, es decir no existe encriptación de datos, además nos da otra alerta de la versión del apache que esta desactualizada y existe fallas de seguridad de esa versión del apache instalado en la versión en el servidor.

El mismo proceso se lo realizo con el software Nexpose, en el capítulo anterior se analizó el uso de este programa, es un software con licencia y para este proceso se usó la versión de prueba de 30 días gratis, con el propósito de comparar los resultados de Nessus vs Nexpose para llevarlo a la siguiente etapa que es explotar esas vulnerabilidades con Kali Linux.

Uno de los beneficios de Nexpose es que analiza desde que tipo de sistema operativo se encuentra un determinado servidor, examina cada una de las vulnerabilidades además presenta un informe detallado de cada fallo y también presenta la solución a ese problema, como se puede ver en la siguiente figura 6-3.

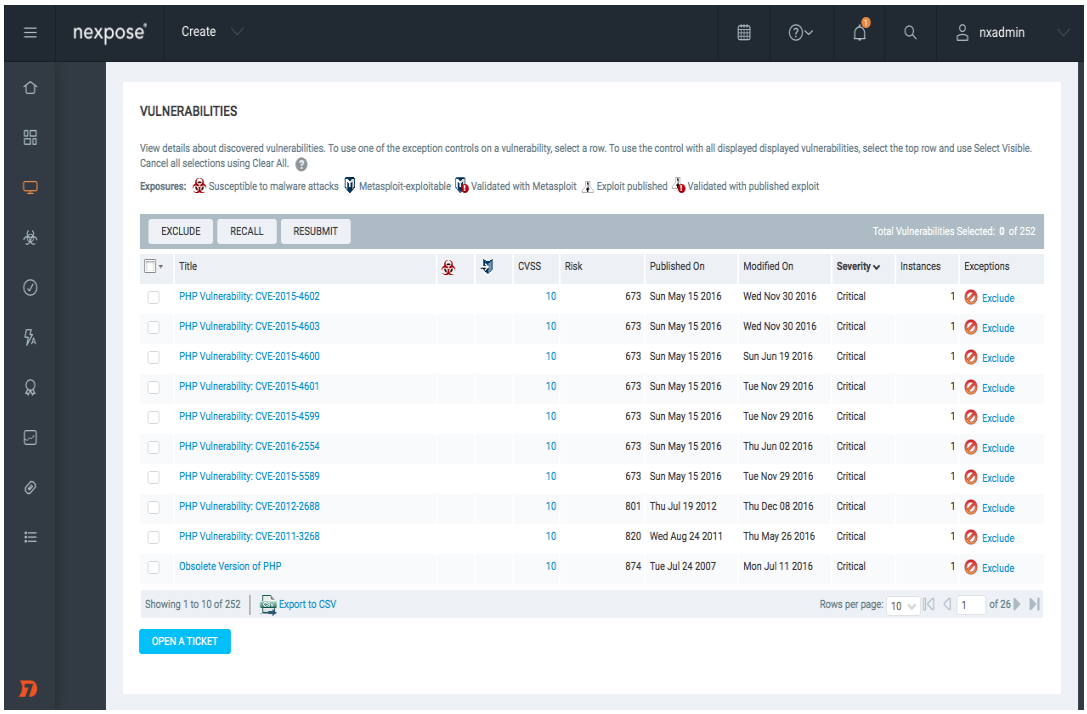


Figura 6-3: Reporte detallado del análisis de vulnerabilidades con Nexpose
Realizado por: Montesdeoca, R; Alvarado, A. 2017

En la siguiente investigación se plantea el uso del software Kali Linux para la realización de los ataques a las vulnerabilidades del servidor E-learning, el ambiente para estas prácticas se usó de 2 escenarios para el análisis, un escenario en la LAN (Red de área Local), y otro escenario en la WAN (Red de área Amplia) dando resultados favorables para este trabajo de titulación.

Tabla 2-3: Resultados del análisis de los Scanners

VULNERABILIDADES ENCONTRADAS CON NESSUS	VULNERABILIDADES ENCONTRADAS CON NEXPOSE
HTTP Trace/ Track Http comprometido a Seguimiento no encriptado	Tráfico sin encriptación HTTP
SSH Weak Algorithms Algoritmos de conexión Segura débiles	Fallas de configuración y versiones de PHP
SSH Server CBC Mode Ciphers Enable Modo CBC Habilitado	Posible ataques de Denial of service (Denegación de servicio)
SSH Weak MAC Algorithms Algoritmos de SSH Débiles	Configuración del servidor web
HTTP Server Type and Version Version del servidor apache	Fallas en la versión del servidor Apache
ICMP Timestamp Request Disclosure Solicitud ICMP descubierta	Posible ataque de Ejecución Remota por XSS
OS identification Identificación del Sistema Operativo	Amenaza de Red Interna

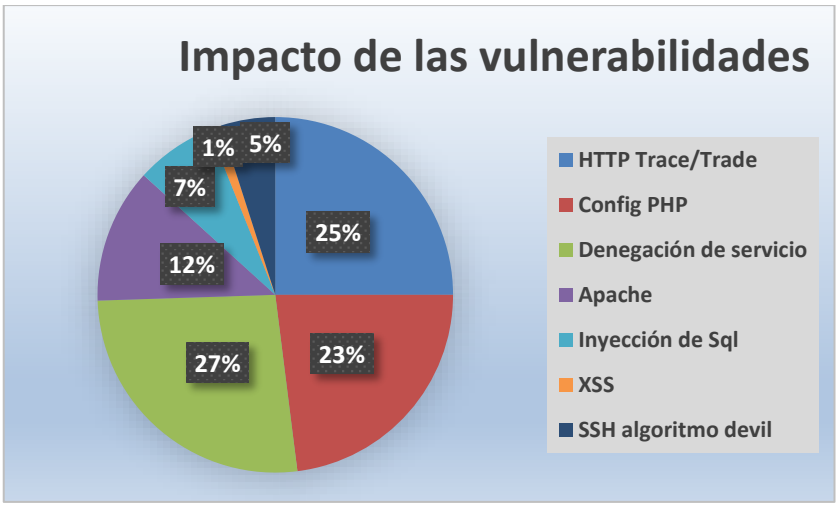


Gráfico 1-3: Tabla de las vulnerabilidades que afectan al servidor
Realizado por: Montesdeoca, R y Alvarado, A. 2017

Del 100% de los resultados obtenidos del escaneo con el software Nessus y Nexpose al servidor E-learning de la ESPOCH que se muestra en la tabla 2-3, se analizó para ver cuál de esas vulnerabilidades está priorizando y cual no al servidor E-learning de la ESPOCH.

La primera advertencia que nos da es la falta de un protocolo seguro para el tráfico de información, necesita un protocolo Https, nos recomienda también correcciones a los archivos de configuración php, y muestra un alto índice a un posible ataque de DoS y XSS con un 18% y 1,8% aproximadamente. El ataque de ejecución Remota es para acceder a las bases de datos, entre otras. Nexpose ejecuta varios paquetes de plugins para atacar las vulnerabilidades, y da todos los posibles ataques a realizarse al servidor en análisis.

3.4 Población y Muestra

Tabla 3-3: Lista de ataques para vulnerar al servidor E-learning de la Espoch

ATAQUES	TIEMPO DE EJECUCION	DURACION DEL ANALISIS	INTENTOS POR ATAQUE
Posible ataque de Ejecución Remota por • XSS • SQL Inyection	Octubre 2016	15 días	4
HTTP Trace/ Track Http comprometido a Seguimiento no encriptado • SNIFFING • PHISHING	Noviembre 2016	15 días	2

Posibles ataques de Denial of service (Denegación de servicio) SSH Server • CBC • DoS	Diciembre 2016	15 días	4

Los resultados obtenidos de los escaneos de vulnerabilidades con los softwares: Nessus y Nexpose, se eligieron estos ataques los cuales serán ejecutados con la siguiente planificación en un lapso de tiempo aproximado de 15 días. Dando así un límite en nuestra investigación.

3.5 Resultados de los ataques a las vulnerabilidades del servidor E-learning

En esta etapa se analizará los ataques realizados al servidor E-learnig de la ESPOCH, esta lista de ataques son seleccionados en base a la Población y muestra definidos del escaneo con los software Nexpose y Nessus, también fueron comparados con el top 10 de la OWASP, que se encuentra en el Anexo F, el cual muestra los principales ataques a servidores web, además estos ataques tienen una guía paso a paso realizada con la herramienta kali Linux, todos los ataques se encuentran en la sección de anexos.

Anexo C: Ataque de inyección de SQL.
Anexo D: Ataque de Cross Site Script XSS
Anexo E: Ataque de Sniffing
Anexo F: Ataque de DoS
Anexo G: Ataque de Phishing

3.3.1 Análisis y valoración de los resultados de los ataques

La valoración de los resultados es de forma cualitativa (en escala de niveles). Los niveles más significativos dentro de la seguridad en este documento son dos: Homogeneidad es importante poder comparar valores, aunque sean diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño de un entorno o de otro. Relatividad es importante poder relativizar el valor de un activo en comparación con otros activos. Los ambientes de pruebas fueron 2, un ambiente interno dentro de la institución, y un ambiente externo es decir fuera de la institución.

En la siguiente tabla 4 la cuantificación de los indicadores que se utilizó, muestra la importancia de efectuar una solución o criterio para el mejor desempeño de la seguridad en la institución.

Tabla 4-3: Escala cualitativa de cuantificación de indicadores

VALOR		CRITERIO
3	Alto	De mucha importancia para la seguridad
2	Medio	De importancia para la seguridad
1	Bajo	Sin riegos para la seguridad

Fuente: Riesgos de la seguridad Informática (2015 pág. 23).

3.3.2 Estimación de la vulnerabilidad y la muestra

En base a las recomendaciones de la lista de vulnerabilidades de la OWASP están definidas 5 tipos de ataques que se practicara al servidor, de estos ataques se realizaron varios intentos para logar el objetivo planteado y poder ingresar al sistema.

En la Tabla 5-3 se permite estimar el grado de impacto de las vulnerabilidades analizadas, con el fin de priorizar los riesgos que requieren controles rápidos y efectivos para determinar las acciones de seguridad adecuadas y la implementación de controles a fin de brindar protección de dichos controles.

Tabla 5-3: Muestra de los ataques internos realizados al servidor E-learning.

Vulnerabilidad	Amenaza	Consecuencia	Intentos Realizados	Éxito de los ataques	Efectividad del Ataque	Impacto
Sql Inyección	Base de Datos	Datos de usuarios	4	2+ 2-	0,5	50%
XSS Script	Modificar la página Web	Cambiar información sensible	4	0+ 4-	0	0%
Sniffing	Captura y analiza paquetes	Obtener todo el tráfico de red.	2	2+ 0-	1	100%
DoS	Denegación del servicio	Sin servicio a los usuarios	4	3+ 1-	0,75	75%
Phishing	Suplantación de identidad	Robo de contraseñas	2	2+ 0-	1	100%

Realizado por: Montesdeoca, R; Alvarado ,A. 2017

La efectividad del ataque viene dada por los ataques tos realiza con éxito en el servidor, dividido por los intentos realizados.

$$ef = \frac{Ataques\ exitos}{\#\ de\ ataques}$$

3.3.3 Indicador 1: Tabla comparativa de los ataques

La tabla 6-3 muestra el porcentaje de las vulnerabilidades y ataques realizados al servidor E-learning, cabe destacar el escenario de este escaneo fue un escenario interno, dentro de las oficinas del departamento de DTIC mientras se realizaban las practicas pre-profesionales.

Tabla 6-3: Escala cualitativa de los Ataques al servidor, escenario interno.

ATAQUES	IMPACTO	VALORACIÓN	PORCENTAJE
Inyección SQL	Medio	2	50 %
Cross Site Script XSS	Bajo	1	0 %
Sniffing	Alto	3	100 %
Dos	Alto	3	75 %
Phishing	Alto	3	100 %

Realizado por: Montesdeoca, R; Alvarado A. 2017
Fuente: Análisis realizado en Mayo 2016 al servidor E-learning de la Espoch en el DTIC**.**

En la tabla 7-3 se muestra los ataques realizados en un entorno externo, fuera de la red interna de la institución en análisis, se muestra los valores de cómo lo vería un atacante informático, y como tendría una visión general de los servidores de la institución.

Tabla 7-3: Muestra de los ataques externos realizados al servidor E-learning**.**

Vulnerabilidad	Amenaza	Consecuencia	Intentos Realizados	Éxito de los ataques	Efectividad del Ataque	Impacto
Sql Inyección	Base de Datos	Datos de usuarios	4	2+ 2-	0,5	50%
XSS Script	Modificar la página Web	Cambiar información sensible	4	0+ 4-	0	0%

Sniffing	Captura y analiza paquetes Web	Obtener todo el tráfico de red.	2	2+ 0-	1	100%
DoS	Denegación del servicio	Sin servicio a los usuarios	4	2+ 2-	0,5	50%
Phishing	Suplantación de identidad	Robo de contraseñas	2	2+ 0-	1	100%

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Tabla 8-3: Escala cualitativa de los Ataques al servidor, escenario externo

ATAQUES	IMPACTO	VALORACIÓN	PORCENTAJE
Inyección SQL	Medio	2	50 %
Cross Site Script XSS	Bajo	1	0 %
Sniffing	Alto	3	100 %
Dos	Medio	2	50 %
Phishing	Alto	4	100 %

Realizado por: Montesdeoca, R; Alvarado A. 2017

Fuente: Análisis realizado en Junio 2016 al servidor E-learning de la Espoch en el DTIC**.**

En la siguiente Tabla 9-3 es un resumen de los ataques y su impacto al servidor E-learning tanto en los entornos externos como internos de la institución.

Tabla 9-3: Porcentaje del Promedio de los ataques realizados en los 2 escenarios

	INTERNO					EXTERNO				
PI	2	0	4	4	4	1	0	4	2	4
TOTAL	0,2	0	0,4	0,4	0,4	0,1	0	0,4	0,2	0,4
PORCENTAJE	50%	0%	100%	100%	100%	25%	0%	100%	50%	100%

Realizado Por: Montesdeoca, R; Alvarado A. 2017

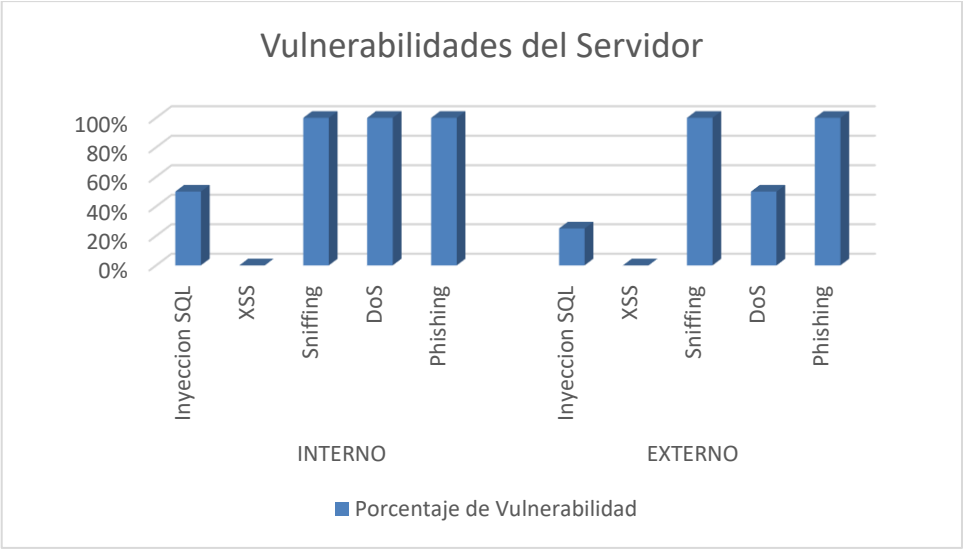


Gráfico 2-3: Gráfico de resultados del análisis de vulnerabilidades del E-learning
Realizado por: Montesdeoca, R; Alvarado, A. 2017

3.3.4 Interpretación de la tabla de resultados

En el Gráfico 2-3 presenta los resultados de la comparativa de ataques realizados en los escenarios internos de la institución y también el escenario desde la internet, esta comparativa muestra el impacto de las vulnerabilidades en el tiempo que fue analizado el servidor, arrojando resultados que requerían atención inmediata de seguridad. El ataque de Inyección Sql muestra una reducción del 25% de un escenario interno a externo, se debe a la acción del antiguo firewall, que ayudaba en parte a reducir este ataque.

La amenaza Cross Site Script (XSS) tuvo un porcentaje del 0% en efectividad en su ataque al servidor en los dos escenarios, porque Moodle y su comunidad de desarrolladores ayuda en cada nueva actualización a mejorar que se mitigue del software los ataques de XSS. Uno de los ataques más preocupantes fue el ataque de Sniffing (husmear la red), con este ataque se consiguió el acceso a varias contraseñas no encriptadas que eran enviadas en texto plano en el tráfico de red.

Con la ayuda del firewall se redujo en un 50% el ataque DoS, dentro de la institución es mucho más efectivo realizar un ataque de DoS, porque el servidor es parte de la red interna y si se realizara el ataque, no hay un equipo quien lo pueda proteger. En el ataque se Phishing da en los dos escenarios una efectividad del 100% del ataque, ya que al no tener certificados de seguridad es fácil para un atacante obtener el robo y captura de los datos de acceso a la página web, mediante una página falsa, los usuarios casi no le prestan mucha importancia a la ip del servidor, sino solamente al Landing Page (Página de llegada) que se cargue bien y enseguida ingresan sus nombres de usuarios y contraseñas.

En el escenario interno se observa que existe mayor riesgo de vulnerabilidad, ya que a tres de estos ataques fue vulnerable en su totalidad al servidor, es decir que el 60% de la integridad de la información estaba afectada si se realizaban con éxito uno de estos ataques dentro de la institución.

En la red externa se observa que tiene una protección adicional en este caso un firewall que le resguarda de ciertos ataques y da la cara al exterior y dando protección a un 40% de los ataques realizados. La herramienta para realizar estos ataques fueron varias proporcionadas por el analizador de ataques de redes Kali Linux.

En la tabla 2-3 se presenta los resultados de los porcentajes de interacción de los 5 ataques realizados, el total representa el valor de 4 esperado con respecto al promedio de las herramientas evaluadas.

3.3 Guía de las mejores prácticas para el servidor e-learning de la ESPOCH.

Esta guía está basada en la seguridad informática de CSIRT (Equipo De Respuesta A Incidentes Y Delitos Informáticos) que tiene un sistema completo de seguridad informática, con referencias y especificaciones del estándar ISO 27002 que es una guía de buenas prácticas que describe cuales deben ser los objetivos de control que se deben aplicar en la seguridad de la información. Se propone que se realice esta implementación a los fallos de seguridad encontrados en el servidor E-learning de la ESPOCH, para luego realizar un análisis con las soluciones propuestas. La guía esta detallada en el ***ANEXO H.***

3.4 Implementación de la guía de las mejores prácticas para el servidor E-learning.

A la par de la implementación de este trabajo de titulación, se fueron desarrollando nuestras prácticas pre-profesionales en el departamento del DTIC con los encargados del área de servidores, esto fue de gran utilidad ya que nos una idea clara de la infraestructura física y lógica de los equipos instalados en la institución, poniendo así en el desarrollo de la fase 4 de la metodología de investigación.

La implementación de varias fases la primera fue la contratación por parte de la Institución la compra de un nuevo firewall capaz de gestionar todo el tráfico de la red con mayores prestaciones y servicios, además incluye un software para analizar el malware que intenta ingresar a la red.

Figura 7-3: Instalación de nuevos equipos en la infraestructura física de la Espoch
Realizado por: Montesdeoca, R; Alvarado A. 2017

El firewall es uno de los componentes fundamentales dentro de cualquier organización que tenga algún servicio de red interna o externa, el firewall que se instaló dentro del área de servidores un firewall ASA Cisco y sus características principales son:

- Funcionalidades de firewall de clase empresarial
- Ofrece capacidades integradas de IPS, VPN y comunicaciones unificadas.
- Ayuda a mejorar su capacidad y mejorar el rendimiento mediante agrupación.
- Proporciona alta disponibilidad para aplicaciones con gran capacidad de recuperación.
- Compatible con los estándares de cifrado de próxima generación, y la integración con Cisco cloud Web Security para brindar protección contra amenazas en la Web. (Cisco, 2015, pág. 1)

Funcionamiento básico de un firewall es ser de un intermediario entre el IPS (Proveedor de Servicios de Internet), y analiza el tráfico que ingresa a la red, y se conecta directamente entre el servidor y el router de red interno.

Figura 8-3: Esquema básico de funcionamiento de un firewall Cisco ASA.
Fuente: https://www.ovh.es/images/options/firewall.jpg

La tecnología Cisco va en constante evolución una de las ventajas en su Interfaz de administración, Cisco permite en su ventana de visualización ver en tiempo real la carga de red, los bloqueos de IP's y bloqueos de ataques, permite fácil administración y salida de reportes Como lo podemos ver en la figura 14:

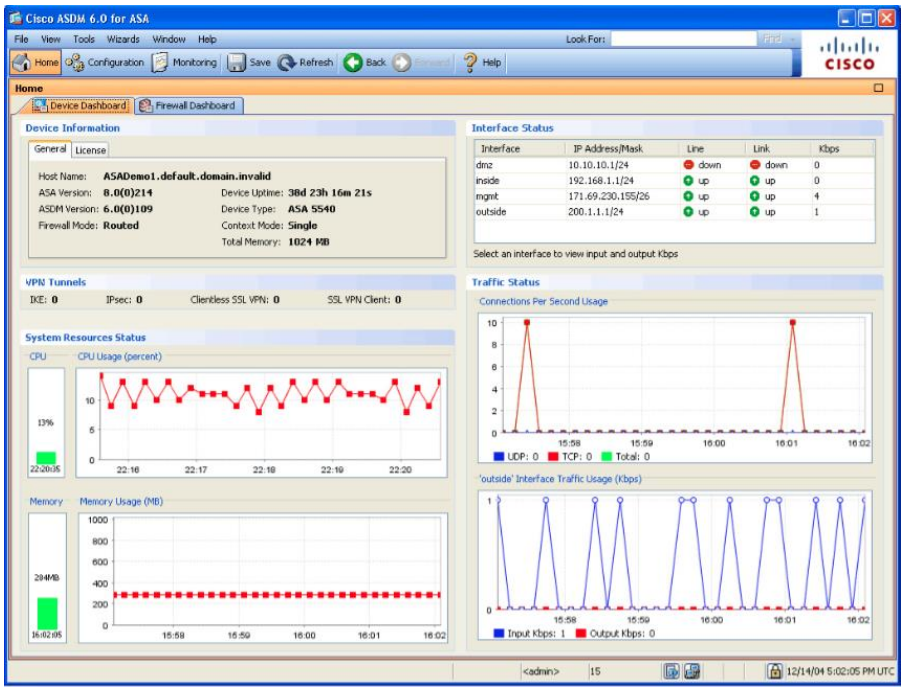


Figura 9-3: Interfaz de administración de un firewall Cisco ASA.
Fuente: https://www.ovh.es/images/options/firewall.jpg

Otra de las implementaciones que se realizaron dentro de la institución fue la instalación de fibra óptica para todas las facultades de la ESPOCH, elevando la velocidad de conexión en la red interna cada facultad, por ende, también a toda la Politécnica.

Los servicios web siempre son escaneados y vulnerados, como en las pruebas de reconocimiento y ataque realizadas al servidor como lo demostramos en el capítulo anterior. Para ello el uso de una zona segura (DMZ) es vital dentro del área de redes y de seguridad, ya que ello proporciona seguridad dentro del área de servidores, así este comprometida la integridad del servidor y en el peor de los casos sea atacado y vulnerado, el atacante no puede entrar dentro de la red ni dentro de la base de datos de la Institución, en el siguiente esquema se puede observar la implementación de un DMZ dentro del área de servidores y como está funcionando actualmente la red de la Espoch.

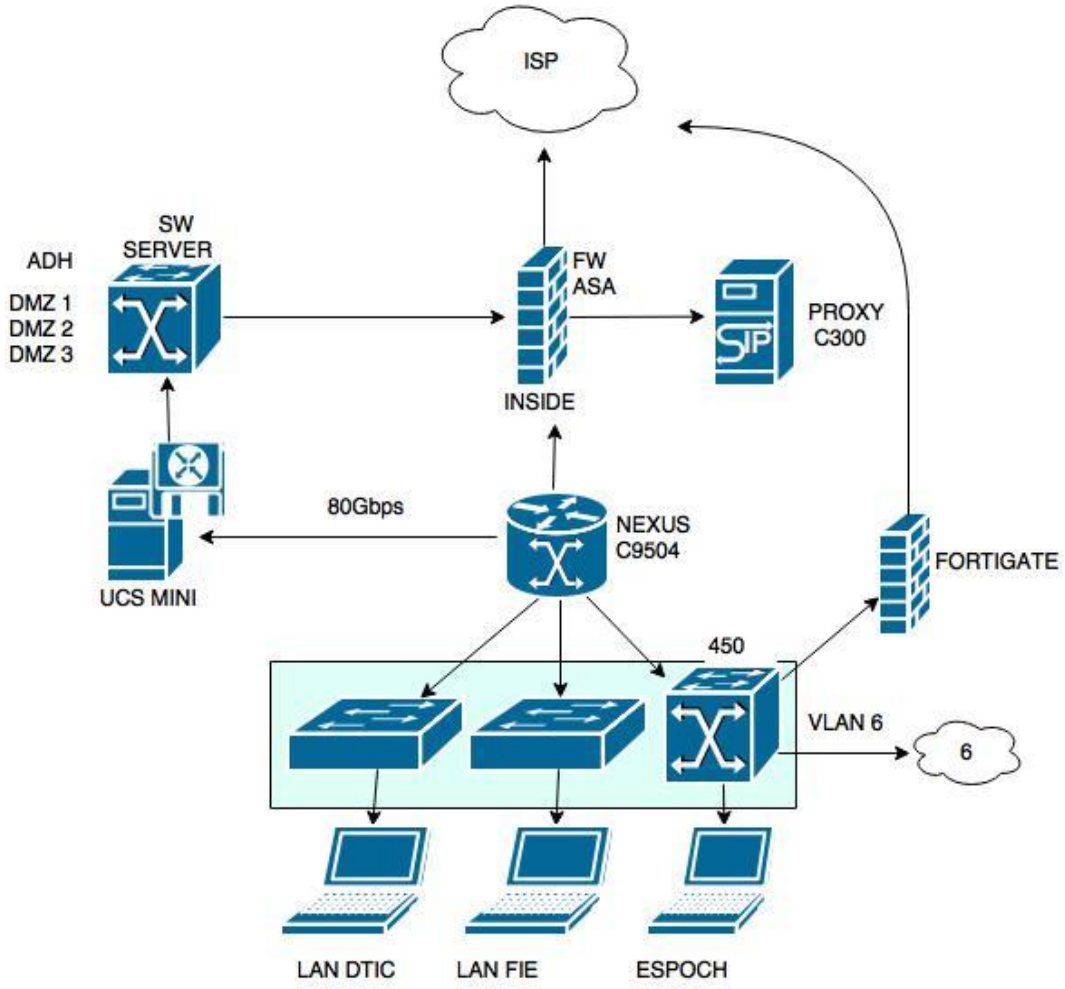


Figura 10-3: Esquema de la implementación de DMZ y Firewall en la Espoch.
Realizado por Montesdeoca, R; Alvarado, A. 2017. Departamento DTIC 2016.

Una vez realizado las diferentes configuraciones del firewall y la DMZ con los servidores funcionando con esos parámetros, la red tiene un nuevo nivel de seguridad, y es capaz de defenderse de varios ataques como DoS, Malware, detección de intrusos, inyección de SQL y otros ataques, pero aún falta la encriptación de la información.

Para la encriptación de la información existe un método que es muy usado por muchos sitios web, siendo ya es un estándar en Internet y son los certificados de encriptación SSL (Capa de Puertos Seguros de transporte), y permite que la información viaje en internet forma segura por métodos de encriptación, que crea un enlace de encriptación entre un cliente y el servidor, con el uso de claves cifradas, SSL utiliza 2 claves cifradas una privada y una pública, que trabajan juntas para obtener una conexión cifrada.

Figura 11-3: Como trabaja el protocolo SSL.
Realizado por: Montesdeoca, R; Alvarado, A. 2017

.

Estas fueron las recomendaciones realizadas al departamento de la DTIC para la implementación de las mejores prácticas de seguridad y acceso, en la siguiente sección se realizará unas pruebas de funcionamiento para comprobar las mejoras.

3.5 Evaluación de la guía de las mejores prácticas para el servidor E-learning.

En esta sección se va a analizar el servidor efectuando todos los ataques anteriormente realizados, pero ahora con las nuevas políticas de seguridad, estas pruebas fueron realizadas con las herramientas y procedimientos descritos anteriormente.

El resultado de la fase de escaneo de puertos nos dio los puertos necesarios para este servicio estos puertos son el puerto 80 que es el http, el puerto 25 smtp para mensajes electrónicos sendmail y el puerto 443 para protocolo de encriptación de datos ssl, eso es indispensable para la seguridad no dejar abiertos puertos innecesarios.

Se actualizo el sistema operativo desde el último análisis, pasando de un Centos 3 a un Centos 4, con la corrección de algunas fallas de seguridad de Centos Linux.

A base de este análisis y la posterior implementación de la guía de mejores prácticas de seguridad, se crearon políticas para el tráfico interno de la red dentro de los firewalls, para que no tenga privilegios la red interna, se restringió el acceso de conexión remota, es decir solo puede ser accedido dentro de la red de los servidores, también se crearon diferentes usuarios con privilegios de acceso diferentes; es decir si es un administrador tiene claves de administrador y puede hacer cambios drásticos y decisivos dentro de cualquier directorio o archivo de configuración; si es un técnico tiene claves de técnico y puede realizar cambio en cuestiones a configuraciones de red, cambios en ciertos archivos pero no puede acceder a directorios principales de los servidores; y si es solo inspector solo puede ver las configuraciones pero no puede hacer cambios dentro de los servidores.

Para la prueba de los ataques al servidor E-learning se realizó con la misma máquina atacante en Kali Linux, como se lo había realizado anteriormente al servidor dando los siguientes resultados ya con la implementación de las mejorar y las nuevas políticas de seguridad:

Tabla 10-3: Escala cualitativa de los Ataques al servidor E-learning de la Espoch

ATAQUES	IMPACTO	VALORACIÓN	PORCENTAJE
Inyección SQL	Bajo	0	0 %
Cross Site Script XSS	Bajo	0	0 %
Sniffing	Bajo	0	0 %
Dos	Medio	1	25 %
Phishing	Medio	1	25 %

Realizado por: Montesdeoca, R; Alvarado, A. 2017
Fuente: Análisis realizado en Febrero 2017 al servidor E-learning de la Espoch en el DTIC.

Interpretación de los resultados de la evaluación del servidor luego de las correcciones de seguridad

Como se demuestra en la tabla 10-3 los ataques realizados al servidor E-learning luego de las implementaciones de mejores prácticas de seguridad y acceso, los diferentes problemas de seguridad fueron corregidos. El ataque inyección SQL que fue solucionado con la ayuda de la encriptación de datos y por la implementación de una DMZ , que restringe a los usuarios de Internet acceder directamente a la base de datos, dejando a este ataque con un 0% de efectividad en comparación al primer análisis realizado en esta investigación, los ataques de Sniffing o captura de datos fue solucionado con un encriptado de datos, que convierte todo el tráfico de la red que está en texto plano y lo codifica en base a 2 llaves una pública y una privada, creando así una línea de comunicación segura, dejando de lado al espionaje de datos con un 0% de efectividad al realizar este ataque.

Los siguientes ataques el DoS Denegación de servicio y el phishing fueron en gran parte solucionados por la DMZ zona segura y las políticas del Firewall (Cortafuegos), gracias al software de Cisco ASA permite la rápida detección de ataques como DoS y bloqueando las conexiones y eliminando el tráfico de las que no es conocido por la red, también se encuentra instalado un IPS que ayuda a detectar a intrusos dando mayor seguridad a la red por parte de la solución para equipos Cisco.

3.6 Cuadro comparativo del análisis del servidor antes y después de la implementación

En el siguiente cuadro comparativo del servidor E-learning desde que se inició el análisis, tenía instalada un sistema de seguridad básico, con un cortafuego con varios años de servicio, siempre daba problemas de funcionamiento porque ya había superado su capacidad de carga y tiempo de vida útil, con la nueva implementación aumento sus prestaciones, dando mejor desempeño en rendimiento, mayor capacidad en procesamiento de tráfico de red, y además cuenta con una interfaz aplicativa de operación.

Varios equipos fueron reemplazados en el área de servidores del DTIC, esto favoreció a la implementación de nuevos sistemas, uno de ellos fue el sistema de virtualización WMWare, que usa un servidor físico y utiliza todos sus recursos de mejor manera y puede virtualizar más servidores dentro de uno solo, compartiendo recursos de memoria, procesador y disco duro.

Toda la infraestructura tanto física como lógica la ESPOCH ha invertido una suma considerable de recursos en las mejoras de la calidad de los servicios en redes, además de constantes capacitaciones al personal técnico para tener toda la infraestructura correctamente funcional. La siguiente tabla 11-3 muestra los resultados finales y la implementación de las mejoras tanto de hardware como de las políticas de seguridad dentro del servidor de la ESPOCH.

Tabla 11-3: Porcentaje del Promedio de los ataques realizados antes y después.

	SIN MEDIDAS DE SEGURIDAD					**CON SOLUCIONES DE SEGURIDAD**				
PI	2	0	4	4	4	0	0	0	1	1
TOTAL	0,2	0	0,4	0,4	0,4	0	0	0	0,1	0,1
PORCENTAJE	50%	0%	100%	100%	100%	0%	0%	0%	25%	25%

Realizado Por: Montesdeoca, R; Alvarado, A. 2017

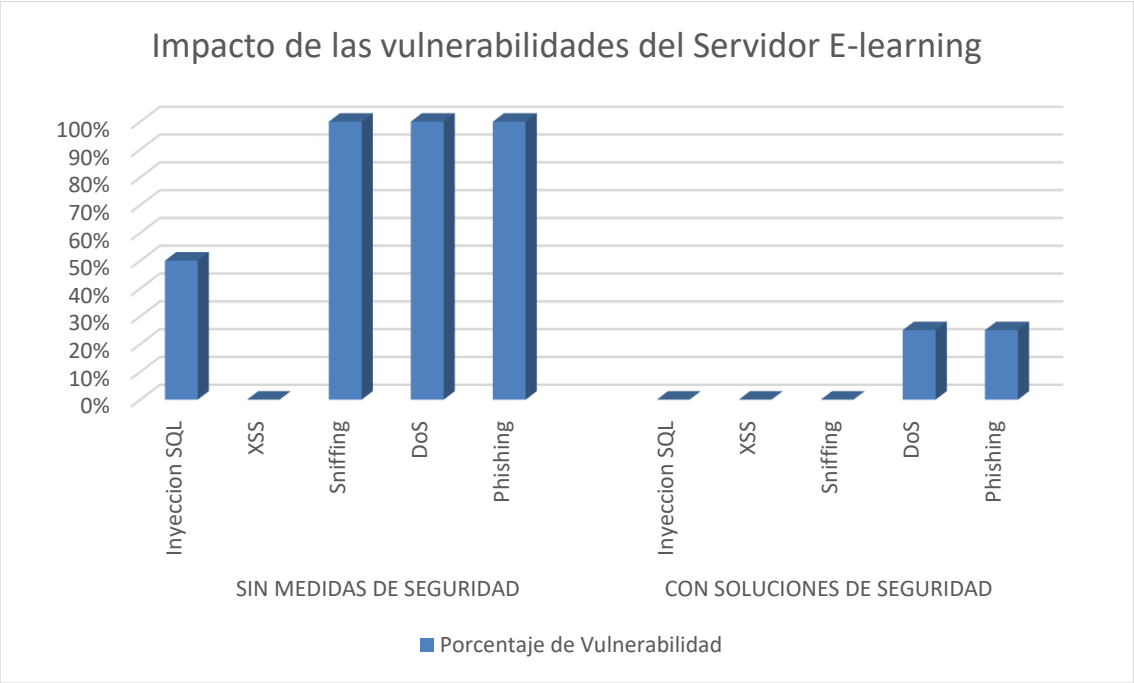


Gráfico 3-3: Comparación del análisis de vulnerabilidades del E-learning
Realizado por: Montesdeoca, R; Alvarado, A. 2017

Interpretación del gráfico de Impacto de las vulnerabilidades antes y después de la implementación de las mejores prácticas de seguridad del servidor E-learning.

En el gráfico 3-3 muestra las mejoras al implementar las medidas y las políticas de seguridad, en la parte izquierda del gráfico se observa que existía un gran número de fallas vulnerables y atacables, donde un atacante podía hacer un escaneo hacer uso de esas fallas y dañar el sistema, o modificar la información sensible, dejando sin servicio a la institución y alrededor de 10000 estudiantes que hacen uso de la plataforma.

El ataque Inyección de SQL quedo con 0% de efectividad, al tener instalado un DMZ, aislando las bases de datos de los servidores de producción, con esta solución así sufran ataques los servidores web, las bases de datos se encuentran en otra sección no accesible para los atacantes. El ataque de XSS viene desde el principio de este análisis sin tener ningún tipo de efectividad, ya que Moodle y el firewall ASA ayudan a que no se pueda ingresar código malicioso.

Los ataques de Sniffing tenían efectividad cuando la información pasaba por la red sin ningún tipo de encriptación, gracias a los certificados de seguridad ahora tienen un 0% de alcance de este ataque.

En la parte derecha del gráfico 3-3 se ve claramente en base a las pruebas realizadas un bajo nivel de impacto de las vulnerabilidades que afectan al servidor, porque aún no se elimina el ataque de

DoS o el Phishing, aunque el servidor ahora cuenta con medidas para contrarrestar esos ataques, esto no quiere decir que no se vaya a hacer estos tipos de ataques, ya cuando el sistema de protección detecta los ataques, los cortafuegos o los IPS actúan y eliminan el ataque, dejando otra vez en el funcionamiento normal al servidor.

En base a las mejoras realizadas, ahora el servidor web es menos propenso a sufrir este tipo de vulnerabilidades, se ha cerrado las puertas a muchos ataques, ahora es más confiable y consta de equipos especializados en ayudar a mejorar su seguridad tanto interna como externa.

CONCLUSIONES

- El servidor E-learning presentaba problemas como: caídas de servicio, no contaba con seguridad en su autenticación, huecos de seguridad y falta de recursos de Hardware, tráfico de red en texto plano, puertos abiertos y sin restricción de usuarios.

- Luego del análisis se encontró vulnerabilidades en el software que requerían una pronta atención y solución por ejemplo el tráfico de red en texto plano, puertos abiertos, restricción de usuarios (DMZ), certificados de seguridad y protección ante Malware. En el caso de hardware se encontró equipos muy usados y con pocos recursos para la red.

- Después de realizar las pruebas en los ambientes simulados se llegó a la conclusión que 4 de 5 ataques al servidor E-learning de la ESPOCH fueron realizadas con éxito, es decir que en un 80% el servidor fue vulnerable.

- Al finalizar el proceso de escaneo y pruebas de penetración al servidor se realizó una guía de mejores prácticas de seguridad que propone solucionar en un 70% de vulnerabilidades encontradas en el servidor E-learning de la ESPOCH, por medio de un DMZ, un firewall ASA, con IPS y cisco AMP.

- Con la implementación de las nuevas políticas de seguridad y acceso a los servidores en el firewall ASA, más la integración de DMZ y los sistemas IPS & AMP, permite una protección contra una gran cantidad de ataques informáticos. Con esta solución el servidor tiene mayor seguridad evitando el 60% de los ataques realizados y dando mejor calidad de servicio a los usuarios.

RECOMENDACIONES

- Se recomienda que para las pruebas de seguridad hacerlas en entorno simuladas con el fin de proteger al servidor de producción.

- Para realizar los ataques de un servidor de una determinada organización es necesario tener los permisos o la autorización respectiva y que los administradores estén al tanto para que no haya conflictos ni malos entendidos con el personal técnico y los investigadores.

- Si utilizamos un servidor propio, se sugiere sistemas de seguridad y acceso tanto físico como privilegios de usuario, es decir, restringir el acceso solo a personal autorizado.

- Actualizar constantemente el software ya que en las actualizaciones se corrigen los problemas de seguridad y errores encontrados en versiones anteriores, tanto en bases de datos, archivos de configuración de PHP y el sistema operativo del servidor.

- En el hardware debido a que no estamos completamente seguros en cuanto catástrofes naturales o accidentes sin intención, se recomendaría tener un respaldo de los servidores en la nube “cloud”, hay muchas empresas que prestan este servicio y a precios muy cómodos.

GLOSARIO

E-LEARNING	Aula virtual que intercambia información
DTIC	Departamento de Tecnología de Información y Comunicación
MOODLE	Software diseñado para ayudar en la educación en línea
PHP	Hypertext Preprocessor
MySQL	Sistema de gestión de bases de datos
FTP	File Transfer Protocol
TCP/IP	Protocolo de comunicaciones
Sniffers	Es un ataque que captura datos sin permisos
UPS	Unidad de control de energía
IP	Protocolo de internet publico
NMAP	Evalúa la seguridad de sistemas informáticos
WHOIS.NET	Página web
NESSUS	Escáner de vulnerabilidades de código abierto
NEXPOSE	Software para el análisis de vulnerabilidades
RAPID7	Empresa que crea software para seguridad de aplicaciones
INYECCION SQL	Ataque informático a las bases de datos
VEGA	Software de búsqueda de fallas de seguridad

KALI LINUX	Distribución de Linux para la penetración y auditorias de seguridad
CROSS-SITE SCRIPTING	Ataque informático que altera el estado actual de y original del servidor
XXS	Ross-site scripting
SNIFFING	Ataque informático que copia las contraseñas
ETTERCAP	Software intermediario para abrir un puerto
DoS	Ataque informático que paraliza o deja sin servicio el servidor
LAN	Red de área local
PHISING	Ataque informático que clona la página real por una página alterna
OWASP	Open Web Application Security Project

BIBLIOGRAFÍA

BAÑOS , JESUS. *Manual de consulta para el profesorado (versión 1.8).*[en linea]. Madrid-Getafe. 2007. p. 9. Disponible en: http://www.fvet.uba.ar/postgrado/Moodle18_Manual_Prof_1.pdf

BUSTAMANTE SANCHEZ, Ruben . *Seguridad en Redes*.[en linea].(Monografia) (Ingenieria). Universidad Autonoma del estado de Hidalgo.Instituto de Ciencias Basicas e Ingenieria. Escuela de Electronica y telecomunicaciones.Estado de Hidalgo.(2016) . p. 26. [citado en Noviembre del 2016].. Disponible en. https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

CABAÑAS VALDIVIESO, Julia Emilia & OJEDA FERNANDEZ, Yessenia Magaly. *Aulas Virtuales como herramientas de apoyo en la educacion en la universidadNacional Mayor de San Marcos*.[en linea].(tesis).(Ingenieria).Universidad Nacional Mayor de San Marcos. Ingenieria en sistemas e Informatica. Ingenieria en Sistemas. (Lima -Peru).2013.pp. 15-25.[citado en Febrero del 2017].Disponible en: http://cybertesis.unmsm.edu.pe/bitstream /cybertesis/2534/1/cabanas _vj.pdf

CATORIA, FERNANDO. *Penetration Test, ¿en qué consiste?* [En Línea]. Latinoamérica. (2012). p. 2. [citado en Abril del 2017].Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

CISCO. *Protección frente a malware avanzado para la red*. [En Linea]. España. (2015) [citado el 11 de Noviembre del 2016].Disponile en: http://www.cisco.com/c/es_es/products/security/amp-appliances/index.html

CIFUENTES, Henry Jesus & NARVAEZ, Cesar Augusto. *Manual de detección de vulnerabilidades de sistemas operativos linux y unix en redes tcp/ip*. [En linea]. (tesis).(Ingenieria). Santiego de Cali. Facultad de Ingenieria. Ingenieria Electrica y Electronica (Colombia). (2004). pp. 13-15. [citado en Noviembre del 2016]. Dispo. en: https://es.scribd.com/doc/41637606/manual-de-detecciOn-de-vulnerabilidades-de-sistemas-operativos-linux-y-unix-en-redes-tcp-ip

CISCO. *Firewall y plataforma de seguridad de la red de eficiencia comprobada.* [En linea]. España. (2015) [citado en Enero del 2016].Disponible en:

http://www.cisco.com/web/LA/productos/security/asa_ software.html.

CLAVERO, CARLOS. *Ventajas y Desventajas del hosting gratuito*. [En linea]. Malaga. 2013.[citado en Enero del 2016]. Disponible en: http://www.mlgdiseno.es/ventajas-y-desventajas-del-hosting-gratuito/

GÓMEZ, ALVARO. *Patencia Tipos de Ataques y de Intrusos en las redes informáticas*. [En linea]. Galicia. (2005). [citado en Diciembre del 2016]. p. 9. Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

GONZÁLEZ, Jaime & VANEGAS Alberto. "La seguridad en las redes de comunicaciones".*Revista Vinculos*. (2012). Colombia. pp. 3-5 [citado en Octubre del 2016]..Disponible en: http://revistavinculos.udistrital.edu.co/files/2012/12/LA-SEGURIDAD-EN-LAS-REDES-DE-COMUNICACIONES-ED5.pdf

HACKMIAMI. *Nexpose considerado el mejor escaner de aplicaciones web durante el HackMiami*. [En linea]. Miami .HackMiami (2013). [citado en Octubre del 2016].Disponible en: https://cyberseguridad.net/index.php/347-nexpose-considerado-el-mejor-escaner-de-aplicaciones-web-durante-el-hackmiami

INFORMATICAHOY. *Que es una DMZ.* [En Línea]. (2016). [citado el 26 de abril del 2017]. Disponible en: . http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-DMZ.php

INTEROUTE. *Sistemas de prevención de Intrusiones.* [En línea]. España. 2017. [citado el 26 de abril del 2017]. Disponible en: España.http://www.interoute.es/hosting/servicios-gestionados/seguridad-gestionada/prevencion-de-intrusiones

MIERES, JORGE. "Security Incident Response Team". *Guía para la implementación de mejores prácticas de seguridad informática*. [En Línea]. Latinoamérica. CSIRT. (2010). pp. 5-6. Disponible en: http://csirtchihuahua.uach.mx/pdf/Mejores_practicas_de_seguridad.pdf

MORENO, EDUARDO. *El campus virtual como medio de educación alternativo en el Ecuador*.[En linea].(tesis). (Maestria). Instituto de Altos Estudios Nacionales. Ecuador (Quito). (2009). pp. 56-70. [citado en Febrero del 2017]. Disponible en: http://repositorio .iaen.edu.ec/bitstream/24000/191/1/IAEN-011-2009.pdf

NMAP. *Guía de referencia Nmap.* [en Linea]. NMAP.ORG. [citado en Febrero del 2017]. Disponible en: https://nmap.org/man/es/index.html

OWASP. "The Open Web Application Security Project" *Owasp: The ten most critical web apllication security risks*. [En Linea]. Sevilla. Eventbrite. (2013). [citado en Febrero del 2017]. Disponible en: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf

OWASP. "The Open Web Application Security Project"*Los Diez riesgos mas criticos en aplicaciones Web.* [En Linea]. Sevilla. Eventbrite (2013). [citado en Abril del 2017]. Disponible en: https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

PINILLA LUIS . *Que es y como usar nmap*.[En Linea]. SlideShare (2015). [citado en Octubre del 2016]. Disponible en: https://es.slideshare.net/luispinilla96/que-es-y-como-usar-nmap

PAPAYARES, DIANA. *Historia de la educacion Virtual.* [Blog]. Colombia (Bolibar). Viernes 15 de Abril del 2011. (2011). [citado en Febrero del 2017]. Disponible en: http://jodiia.blogspot.com/2011/04/historia-de-la-educacion-virtual.html

PERPIÑAN, LUIS. *Seguridad de sistemas gnu/linux*. [En Linea]. Fundacion Codigo Libre Dominicano. Santo Domingo. (Republica Dominicana). (2011). p 6. [citado en Febrero del 2017]. Disponible en: https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/Libro-Seguridad-GNU-Linux-Antonio-Perpinan-2011.pdf

QUIRUMBAY YAGUAL, Daniel Ivan. *Desarrollo del esquema de seguridad, plan de recuperación ante desastres informáticos y solución para el nivel de exposición de amenazas y vulnerabilidades aplicada a los servidores y equipos de comunicación del centro de datos de la municipalidad de la ciudad del este*. (tesis). (maestria). Escuela

Superior Politecnica Del Litoral. Facultad de Ingenieria Electronica y Computacion. Ecuador (Guayaquil). (2015) pp. 49-53. [citado en Enero del 2017]. Disponible en: https://www.dspace.espol.edu.ec/retrieve/88647/D-84693.pdf

ROUSE, MARGARET. *Prueba de penetración (pen test).*[En Lineaa]. TechTarget. 2017. [citado en Enero del 2017]. Disponible en: http://search datacenter.techtarget.com/es/definicion/Prueba-de-penetracion-pen-test

SYMANTEC. *Guía para principiantes sobre los certificados SSL*. [En línea]. Madrid España. 2013. [citado 23 de abril del 2017]. Disponible en: https://www.symantec.com/content/es/es/enterprise/ white_papers/b-beginners-guide-to-ssl-certificates_WP.pdf

TP-LINK-IPS. *Que es una DMZ.* [En linea]. España. (2016**).** [citado en Octubre del 2016]. Disponible en: http://www.tp-link.es/FAQ-28.html

UNIVERSIDAD-MURCIA. *Caracteristicas Comunes de las Aulas Virtuales.* [En linea]. España. (2014). [citado en Octubre del 2016]. Disponible en: http://www.conocimientosweb.net/portal/article2309. .html

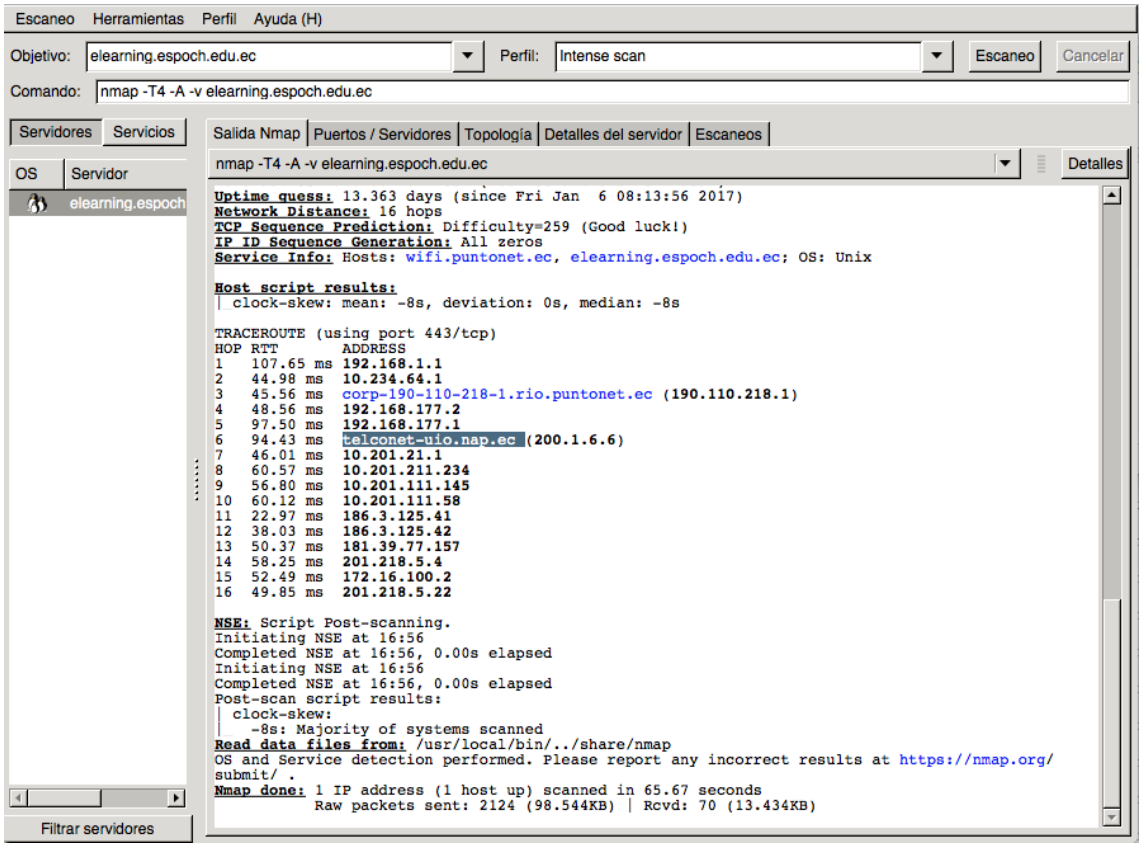
VOUTSSAS, JUAN. *Preservación documental digital y seguridad informática.* [en linea] . Mexico. (2010).[citado en Octubre del 2016]. Disponible en: http://132.248.242.3/~publica/archivos/50/ibi002305007.pdf

WIKIHOW. *Cómo instalar un certificado SSL*. [en línea]. 2017. [citado el 25 de abril del 2017]. Disponible en: http://es.wikihow.com/instalar-un-certificado-SSL

ANEXOS

Anexo A: Pasos para verificar el estado actual del servidor E-learning de la ESPOCH

1.- Recolección de Información: Haciendo uso de la herramienta instalada en el equipo NMAP se obtuvo la siguiente información del servidor E-learning, presentado en la siguiente figura



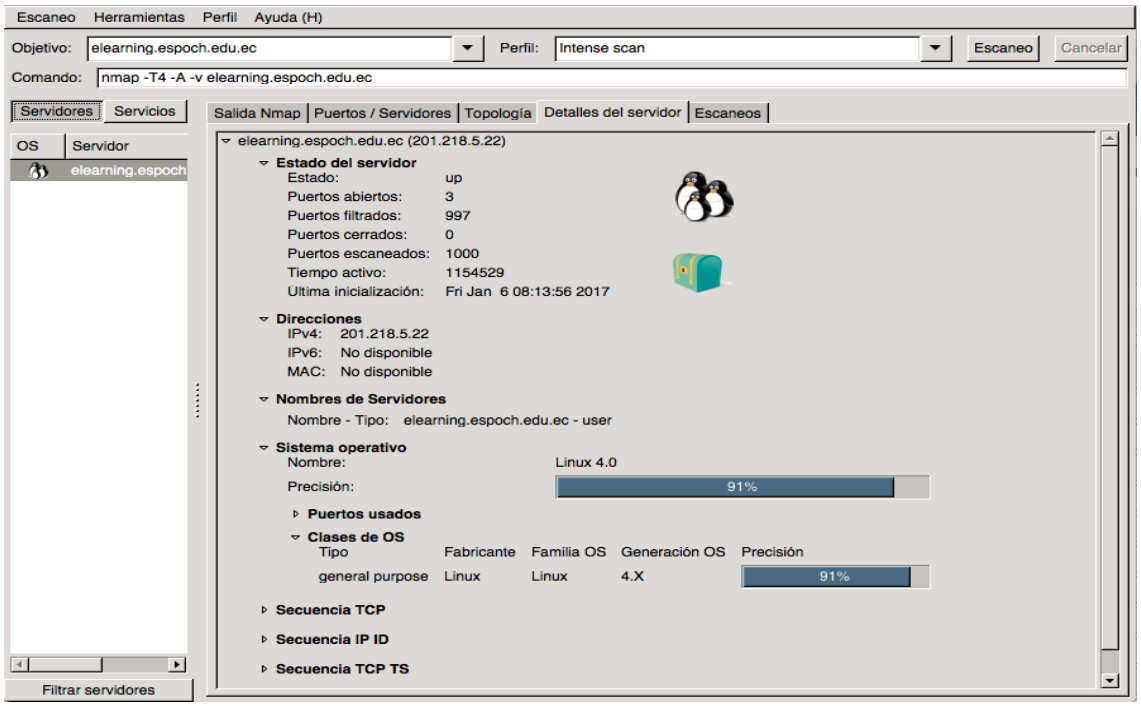
Escaneo al Servidor E-learning de la ESPOCH

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

En la figura muestra datos importantes acerca del servidor E-learning uno de ellos es su proveedor de servicio de internet, en lo que se refiere al proveedor de internet para la universidad es la empresa TELCONET, que da los servicios de internet de fibra óptica y los servidores de nombre de dominio DNS para que se pueda conectar con el mundo a través de la web en internet.

Una información muy importante dentro de esta primera fase es conocer el sistema operativo que fue implementado al servidor y cuál es su versión de sistema, dándonos a conocer si el sistema se encuentra actualizado o no. Los sistemas operativos van actualizándose periódicamente es decir cada final de semestre lanzan a los usuarios correcciones de seguridad, parches de puertos, actualizaciones de kernel (núcleo del sistema) y otros servicios que siendo bien configurados proveen una mejor protección ante fallos o ataques a su sistema.

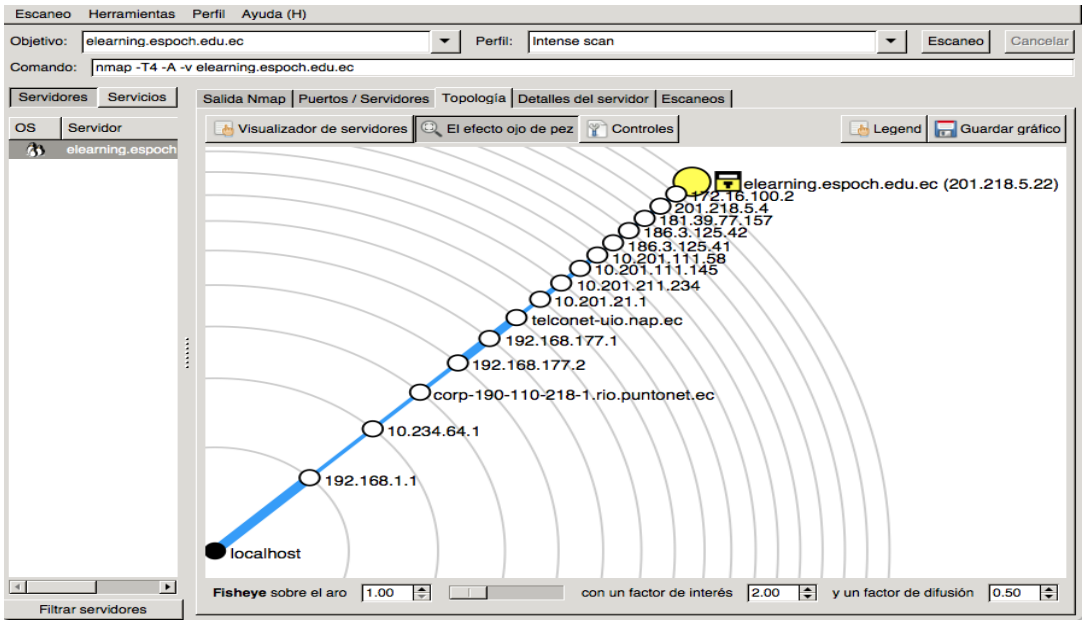
En la figura siguiente se muestra el sistema operativo del servidor E-learning y su versión.



Detalles del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

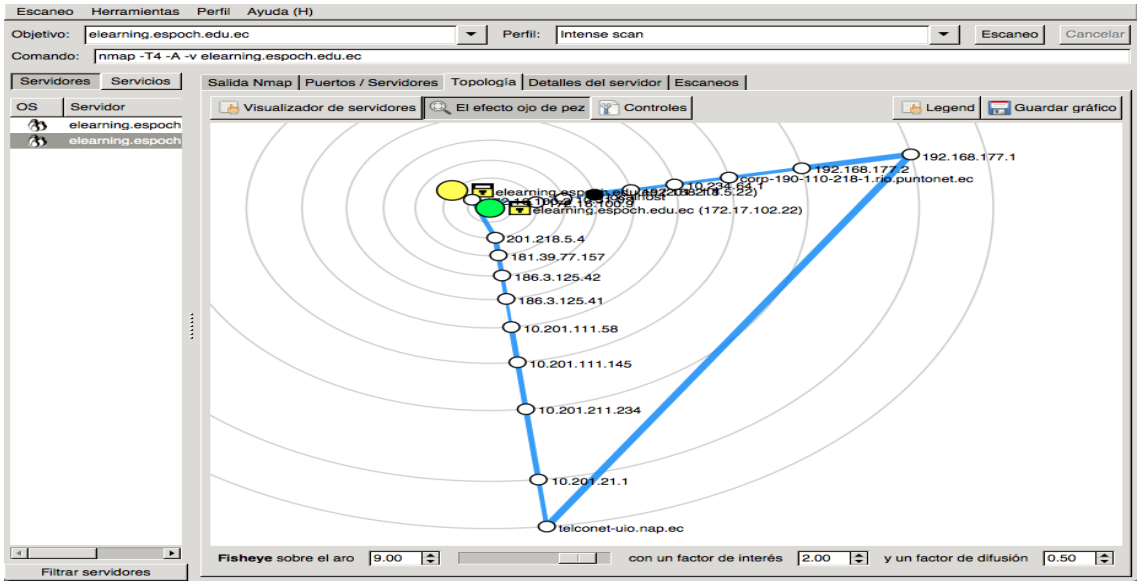
La topología de red nos ayuda a saber en dónde se encuentra el servidor contando todos los nodos de conexión desde el local host o el equipo que está enviando los paquetes hacia el servidor E-learning. En la figura se observa los que el emisor da 16 saltos o nodos hasta llegar al receptor en este caso el servidor, esta fase de reconocimiento permite saber datos sensibles como las IP tanto públicas como privadas, proveedor de servicio y la dirección de red tanto interna como externa.



Topología Externa de red del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

En el escaneo interno es decir en la red interna de la ESPOCH se revela la topología interna de la red, las IP de enlace interno hacia la red de datos y la IP del servidor Elearning.

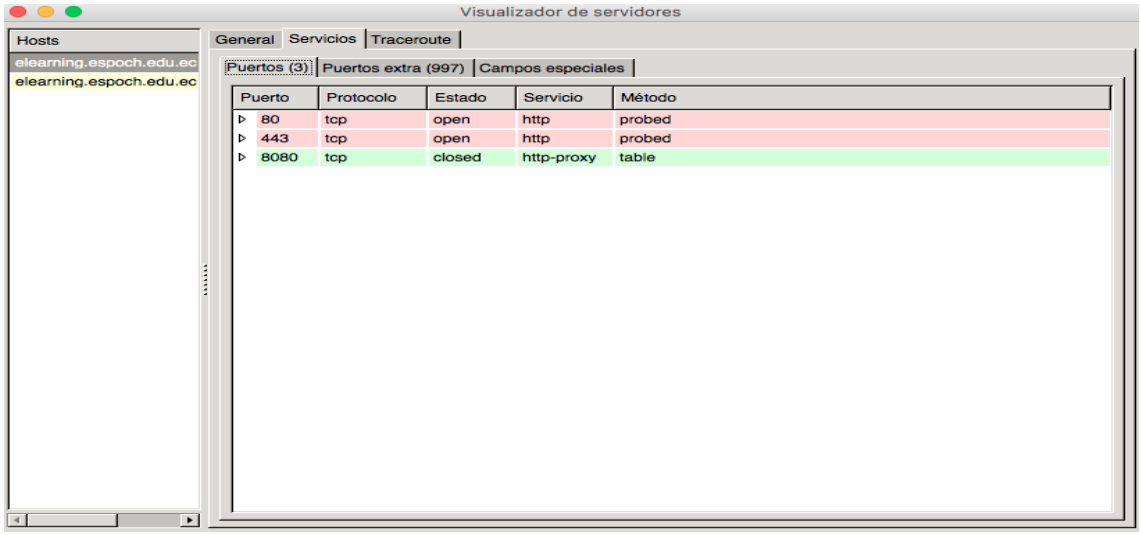


Topología Interna de Red del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

2. Escaneo de puertos: Los puertos abiertos dentro de un servidor determinan exclusivamente el tipo de servicio que ofrece, por ejemplo, en un servidor web el puerto debe estar abierto a 80 http que es servicio de navegación web o servidor web, aunque este servicio es altamente usado por atacantes para encontrar nuevas entradas por él.

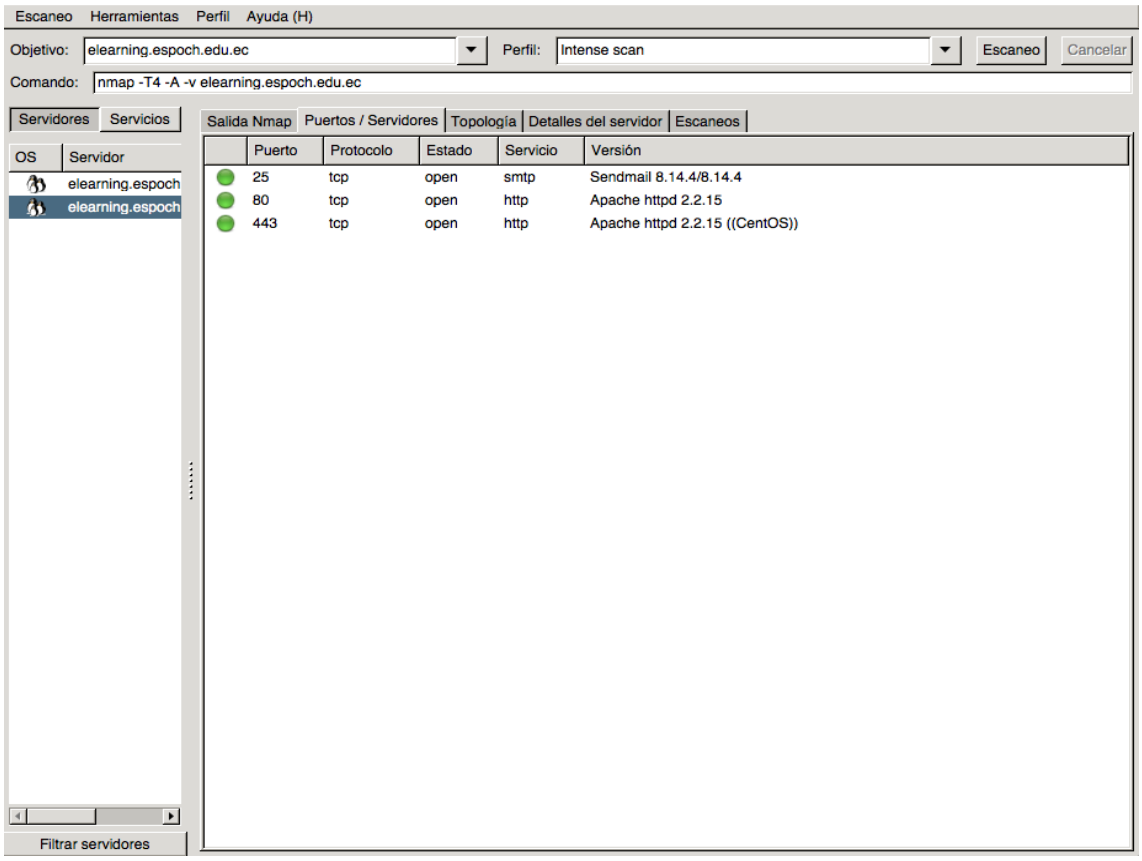
En la figura podemos observar los diferentes puertos y servicios del servidor E-learning, dentro del cual observamos que es un servidor web, con 2 puertos principales abiertos.



Puertos Red encontrados del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Para un análisis más profundo se debe tomar en cuenta la versión de cada servicio la herramienta NMAP nos da la siguiente información.



Servicios y Puertos Red del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

A continuación en la tabla se detallan los principales puertos abiertos encontrados en el servidor y sus características.

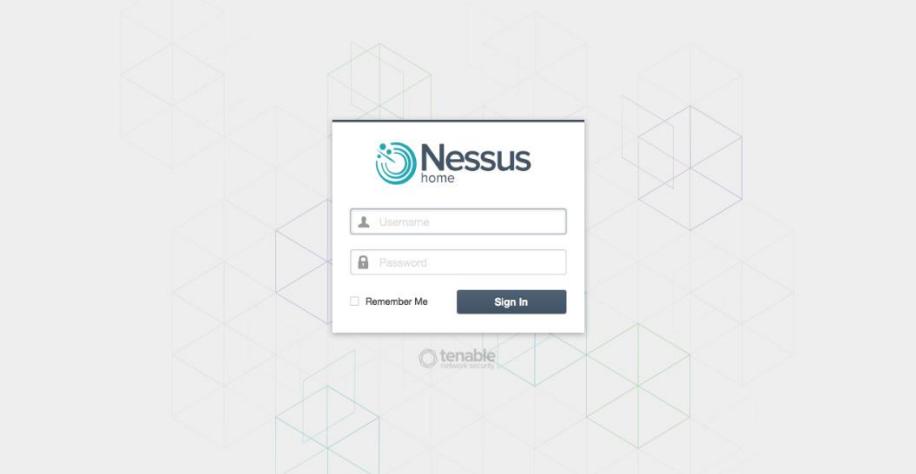
Puertos abiertos del Servidor E-learning de la Espoch

Puerto	Nombre	Característica
80	Http	Protocolo de transferencia de hipertexto (HTTP) para los servicios del World Wide Web (WWW)
443	Https	Protocolo de transferencia de hipertexto seguro (HTTP)

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Fuente: Página web: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html

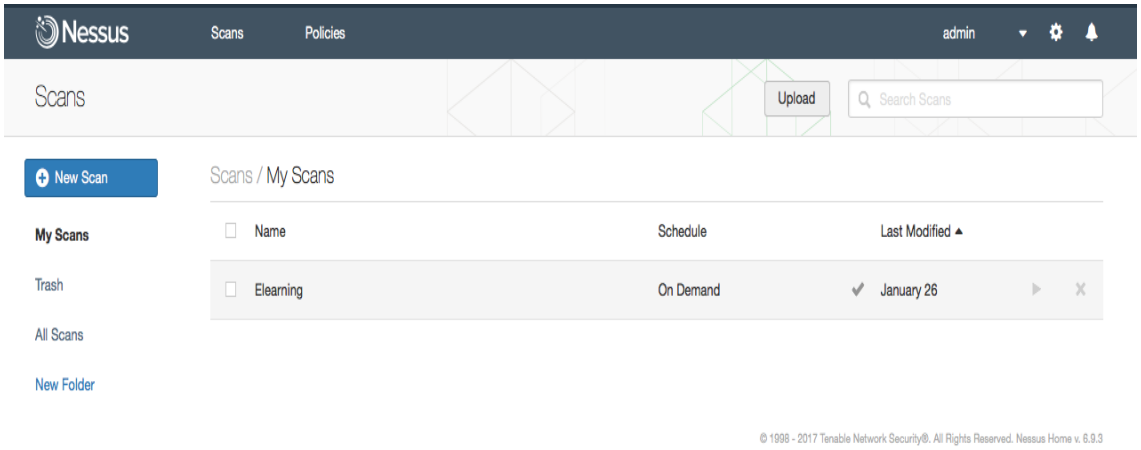
NESSUS: Este software fue descargado de la página oficial: https://www.tenable.com/products/nessus/select-your-operating-system/ Cuando finaliza la descarga, se instala y se crea un usuario, de esta manera se ingresa a la pantalla de inicio:



Pantalla de inicio para abrir el software Nessus

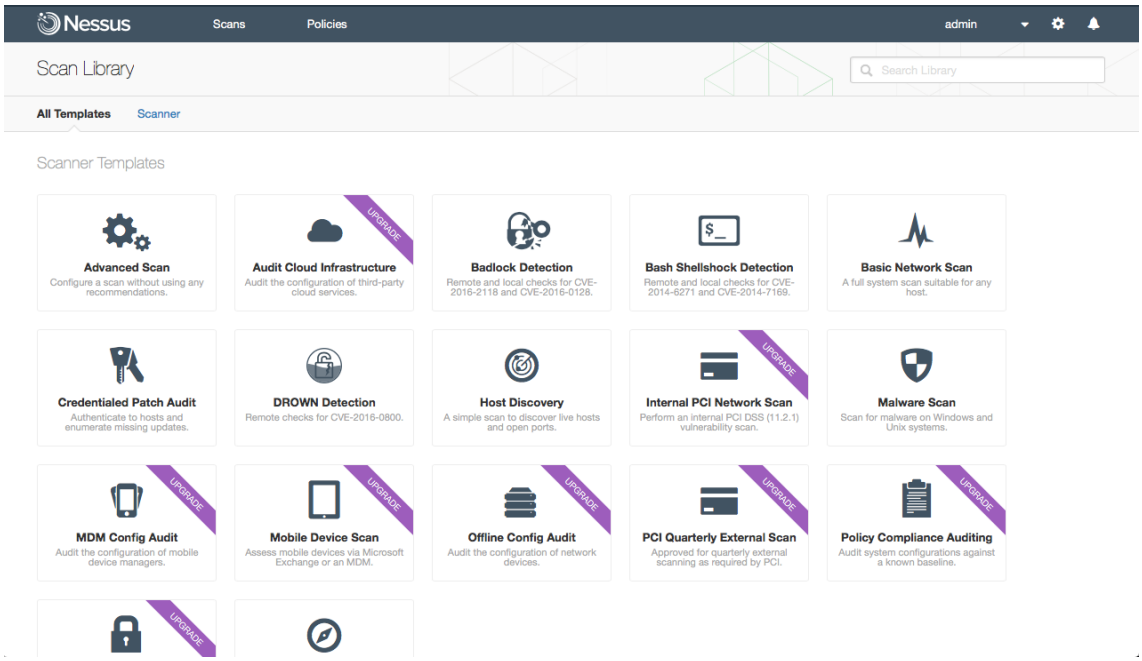
Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Una vez dentro del programa ingresado el usuario y el password hacer el escaneo es relativamente fácil gracias a la interfaz de Nessus que permite que cualquier persona así no sea un experto informático realice un escaneó de la red. Lo primero que se va a hacer es hacer click en New Scan, escoger la opción Advanced Scan.



Escaneo de vulnerabilidades con Nessus

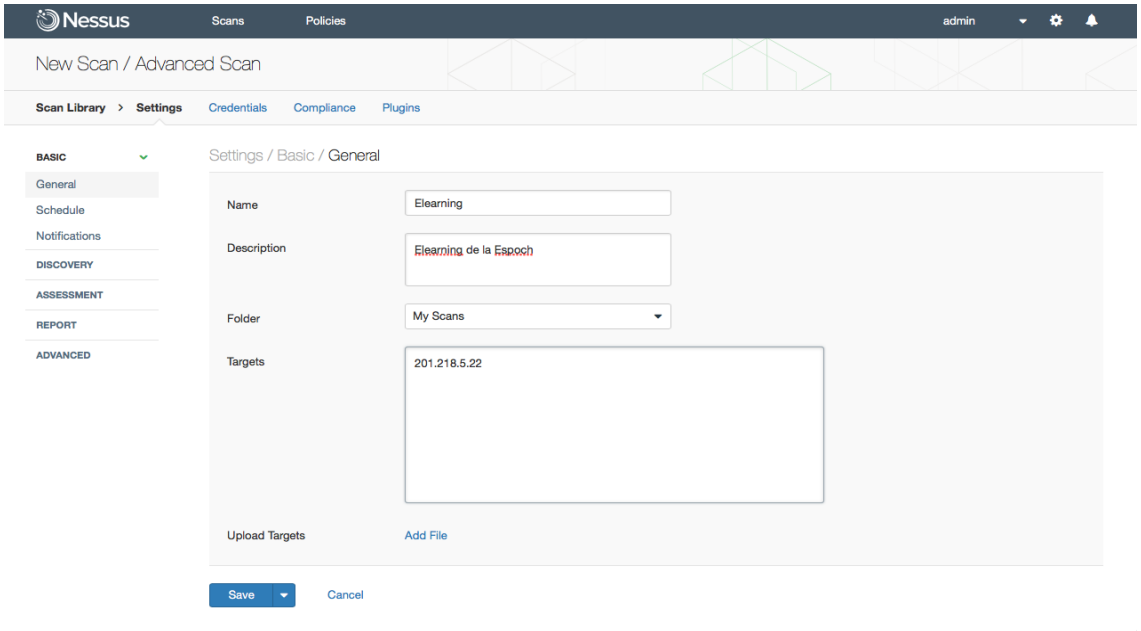
Realizado por: Montesdeoca, R; Alvarado, A. 2017



Tipos de escaneos que se realizan con Nessus

Realizado por: Montesdeoca, R; Alvarado, A. 2017

En la pantalla siguiente de completa los datos y se ingresa la IP a donde queremos atacar, si desconocemos la IP de un servidor a cuál queremos atacar es muy sencillo haciéndole un ping a su nombre de dominio.



Creando un reporte de vulnerabilidades con Nessus

Realizado por: Montesdeoca, R; Alvarado, A. 2017

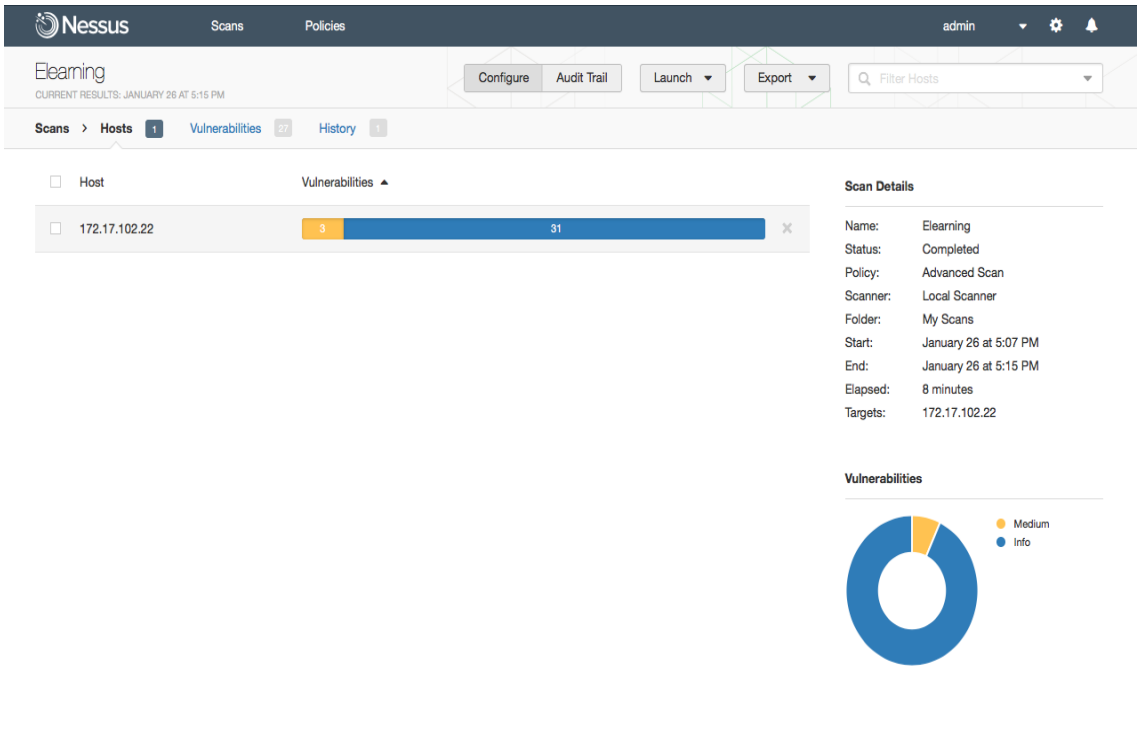
Se obtiene la IP de un servidor simplemente haciéndole un ping al nombre de dominio ejemplo:

```
Last login: Sun Jan 29 22:45:20 on console
MacBook-Pro:~ richardmontesdeoca$ ping elearning.espoch.edu.ec
PING elearning.espoch.edu.ec (201.218.5.22): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
^C
--- elearning.espoch.edu.ec ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
MacBook-Pro:~ richardmontesdeoca$
```

Obteniendo la Ip Pública del Servidor E-learning de la ESPOCH

Realizado por: Montesdeoca, R; Alvarado, A. 2017

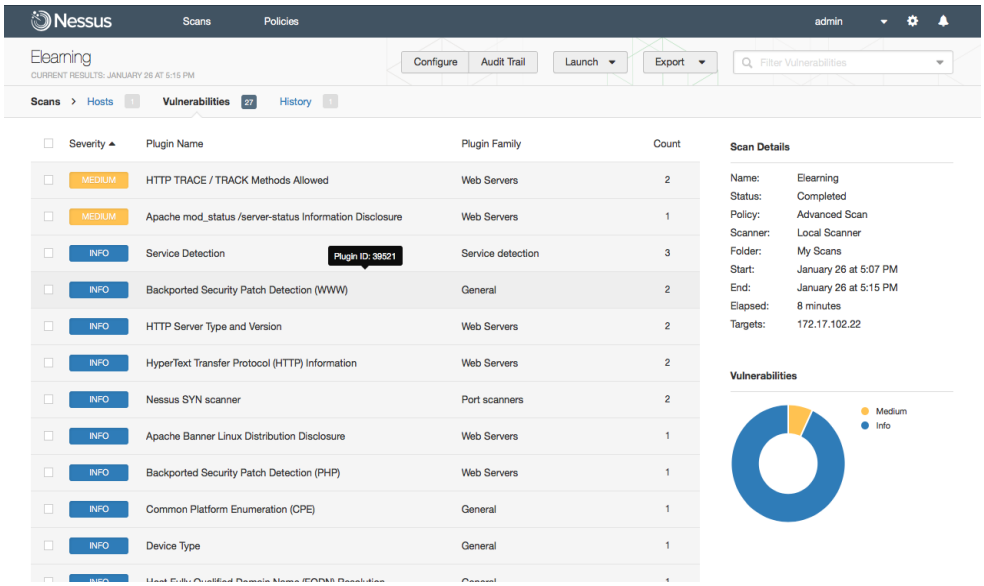
Una vez ya con toda la información necesaria para realizar el escaneo se procede a capturar todas las vulnerabilidades con el software Nessus, una vez que se ejecute el software tomará alrededor de 30 min a 1 hora en llevar todo el proceso de escaneo y dará los resultados de las vulnerabilidades encontradas por el programa.



Resultado del reporte de vulnerabilidades con Nessus

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

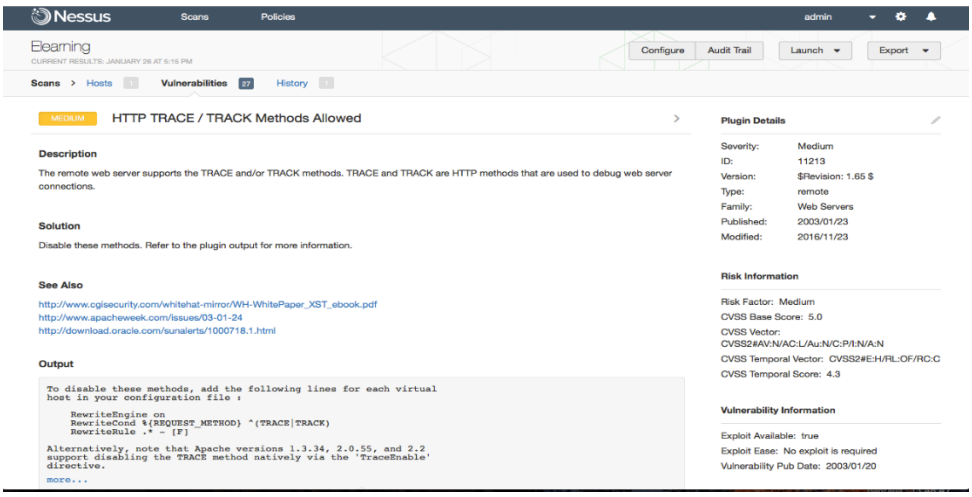
La pestaña de vulnerabilidades permite ver cada una de las vulnerabilidades existentes dentro del Servidor E-learning.



Reporte detallado del análisis de vulnerabilidades con Nessus

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Cada una de las vulnerabilidades encontradas Nessus da una sugerencia de cómo podríamos resolver ese error, para ver los detalles de cada falla basta con darle un click en cada una de las opciones de la lista allí encontrada.



Reporte detallado y sugerencias de Nessus

Realizado por: Montesdeoca, R; Alvarado, A. 2017

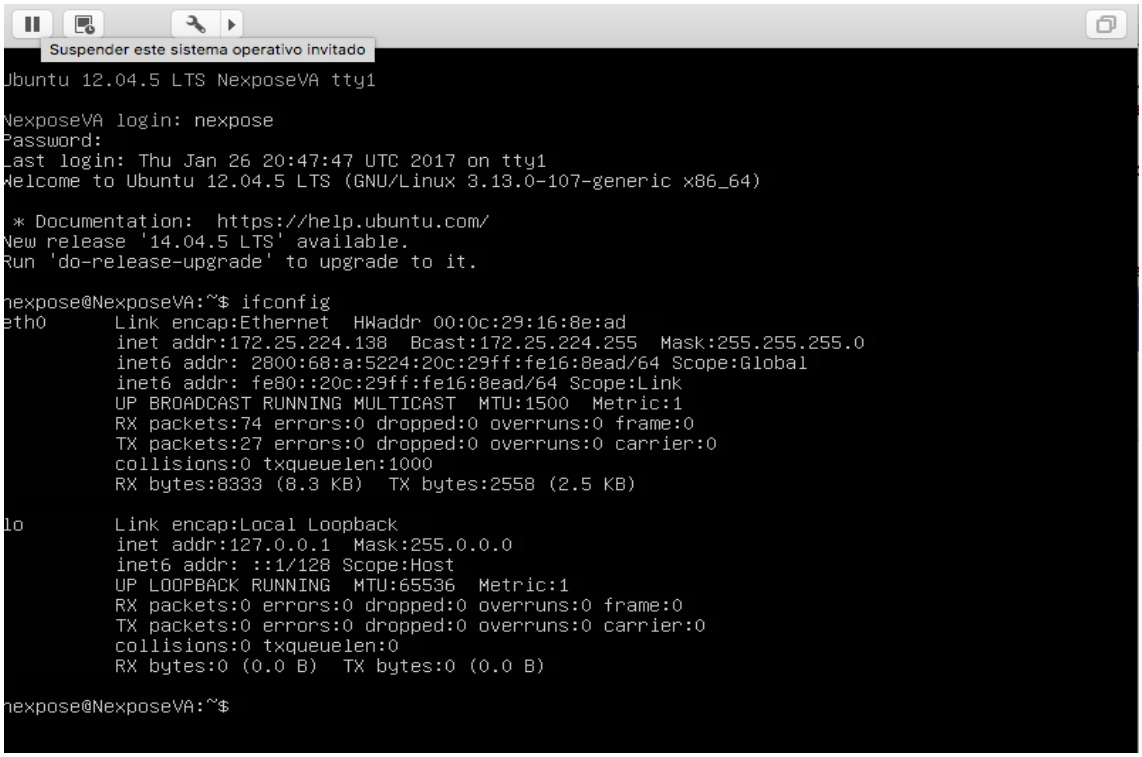
Nexpose: Nexpose es un software creado por la empresa Rapid7 para el análisis de vulnerabilidades de redes. Para poder instalar Nexpose hay que registrarse en la página web oficial de Rapid7 https://www.rapid7.com/products/nexpose/download/ descargar el producto, existen 2 formas posibles una community edition y otra Enterprise Edition, la community se puede usar

gratuitamente por 30 días y permite un escaneo por barrido de Ips de 32, esta versión será la utilizada para hacer el análisis de los servidores de la ESPOCH.

Una vez descargado el software e instalado, se procede a activarlo, cuando se registra en la página de Radid7 envían al correo electrónico del solicitante una clave para validarlo, solo funciona por 30 días que para propósitos de este escaneo se usará ya que este software es altamente reconocido por muchas empresas de seguridad como unos de los mejores programas para el análisis de vulnerabilidades no solo para redes, sino también para encontrar fallos en sistemas operativos, bases de datos, aplicaciones y archivos, y detecta programas maliciosos o peligrosos, respecto a seguridad informática.

Rapid7 entrega un archivo ova que es un formato de archivo de una máquina virtual, y se activará en VMware player que es una versión gratuita del simulador de máquinas virtuales. Realizado el montaje de la máquina virtual se procede a la ejecución que es relativamente sencilla ya que está configurada para que funcione sin ningún problema.

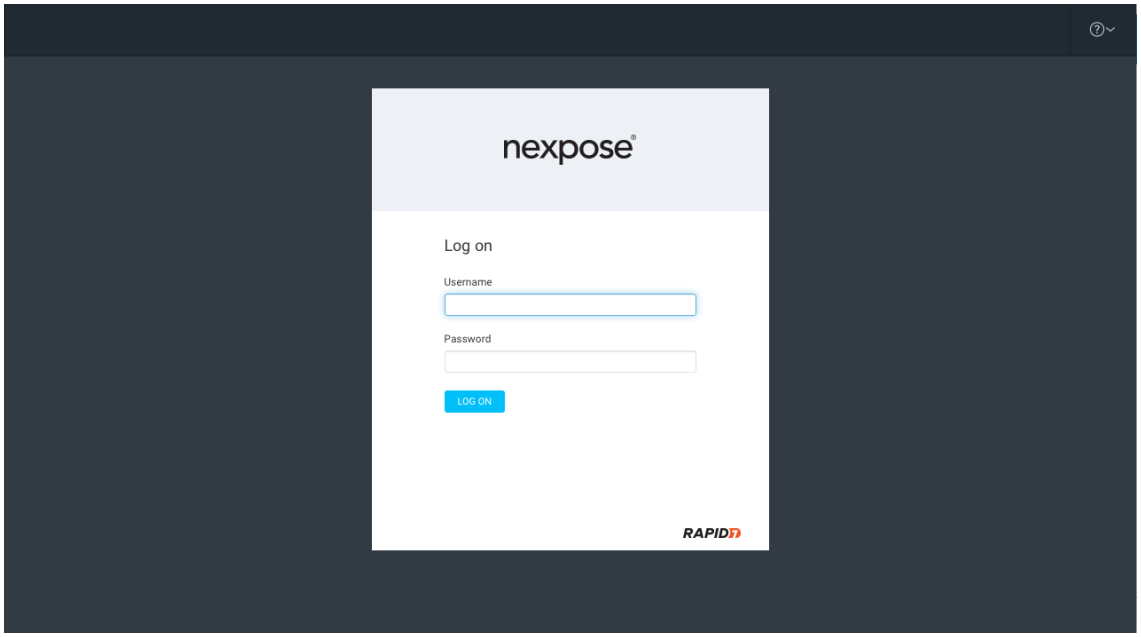
Para acceder a la máquina virtual es necesario autenticar con Nexpose login: nexpose y el password: nexpose, para conectarse en el navegador, es necesario saber la IP de la máquina virtual nexpose y para saberlo es con un solo comando en el terminal: ifconfig



Máquina Virtual con Nexpose

Realizado por: Montesdeoca, R; Alvarado, A. 2017

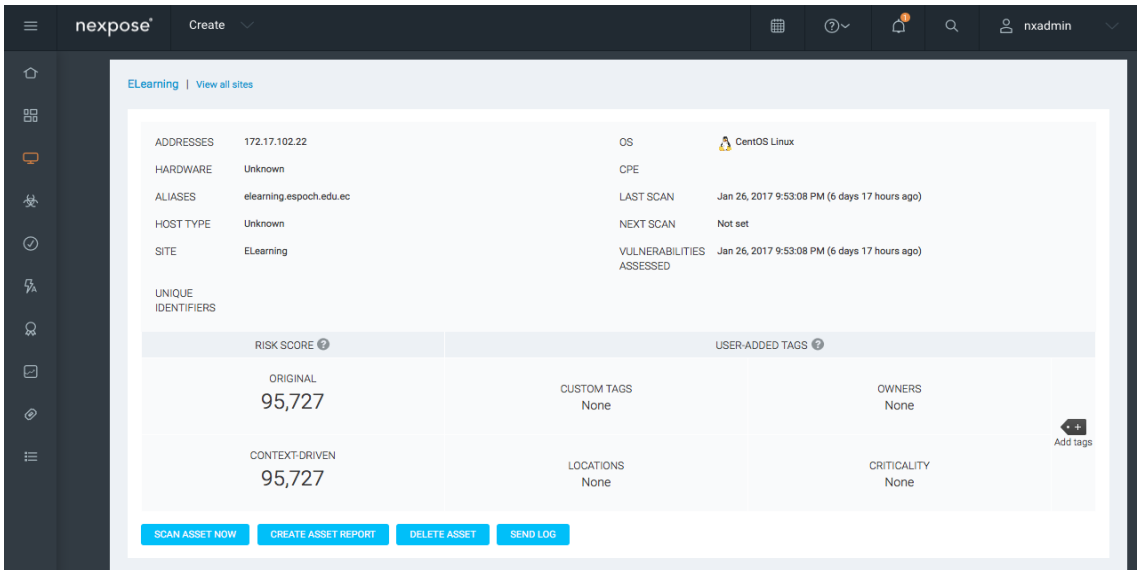
En el explorador independiente de la empresa puede ser de Microsoft, Chrome, Firefox o Safari, en la barra de búsquedas escribimos la siguiente dirección: https://192.168.1.139:3780/ el puerto 3780 es el que usa Nexpose para arrancar la interfaz web.



Página de Inicio de Nexpose en un navegador

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Para ingresar se usan las contraseñas por defecto que son Username: nxadmin y Password: nxpassword que vienen descritas cuando nos dan la guía de instalación cuando nos registramos en la página oficial de Rapid7.

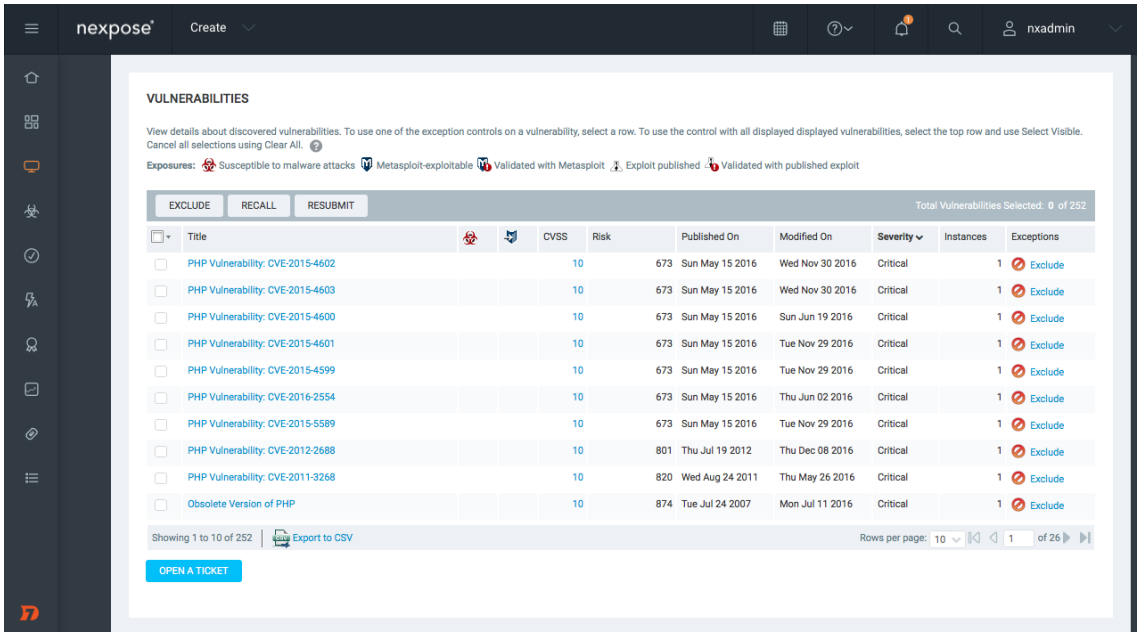


Escaneo de vulnerabilidades con Nexpose

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Para crear un nuevo análisis se debe seguir los mismos pasos como se lo realizó en el software anterior, crear un nuevo sitio, añadir la IP de destino o el rango de IP, luego definir la intensidad del escaneo si se requiere un escaneo intenso o un escaneo ligero, para este análisis se escoge el análisis intenso que dura aproximadamente unos 60 min.

Uno de los beneficios de Nexpose es que analiza desde que tipo de sistema operativo se encuentra un determinado servidor, examina cada una de las vulnerabilidades además presenta un informe detallado de cada fallo y también presenta la solución a ese problema, como se puede ver en la siguiente figura



Reporte del análisis de vulnerabilidades con Nexpose

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Anexo B: Recomendaciones de la OWASP de los 10 principales ataques a servidores

Prefacio

El software inseguro está debilitando las finanzas, salud, defensa, energía, y otras infraestructuras críticas. A medida que la infraestructura digital se hace cada vez más compleja e interconectada, la dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente. No se puede dar el lujo de tolerar problemas de seguridad relativamente sencillos, como los que se presentan en este OWASP Top 10.

El objetivo del proyecto Top 10 es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. El proyecto Top 10 es referenciado por muchos estándares, libros, herramientas, y organizaciones, incluyendo MITRE, PCI DSS, DISA, FCT, y muchos más . Esta versión de OWASP Top 10 marca el aniversario número diez de este proyecto, de concientización sobre la importancia de los riesgos de seguridad en aplicaciones. OWASP Top 10 fue lanzado por primera vez en 2003, con actualizaciones menores en 2004 y 2007. La versión 2010 fue renovada para dar prioridad al riesgo, no sólo a la prevalencia. La edición 2013 sigue el mismo enfoque.

Lo invitamos a que utilice el Top 10 para hacer que su organización se inicie en la temática sobre seguridad en aplicaciones. Los desarrolladores pueden aprender de los errores de otras organizaciones. Los ejecutivos deben comenzar a pensar como gestionar el riesgo que las aplicaciones de software crean en sus empresas.

A largo plazo, le recomendamos que cree un programa de seguridad en aplicaciones que sea compatible con su cultura y su tecnología. Estos programas vienen en todas las formas y tamaños, y debe evitar tratar de hacer todo lo prescrito por algún modelo de procesos. En cambio, debe de aprovechar las fortalezas existentes en su organización para hacer y medir lo que le funcione a usted. Esperamos que OWASP Top 10 sea útil para sus esfuerzos de seguridad en aplicaciones. Por favor no dude en ponerse en contacto con OWASP para sus dudas, comentarios, e ideas, ya sea públicamente a owasp-tooten@lists.owasp.org o en privado a dave.wichers@owasp.org.

Acerca de OWASP

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que pueden ser confiables. En OWASP encontrará gratuitas y abiertas ...

- Herramientas y estándares de seguridad en aplicaciones
- Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro, y revisiones de seguridad en código fuente
- Controles de seguridad estándar y librerías
- Capítulos locales en todo el mundo
- Investigaciones de vanguardia
- Extensas conferencias alrededor del mundo
- Listas de correo

Aprenda más en: https://www.owasp.org

Todas las herramientas de OWASP, documentos, foros, y capítulos son gratuitas y abiertas a cualquiera interesado en mejorar la seguridad en aplicaciones. Abogamos por resolver la seguridad en aplicaciones como un problema de personas, procesos y tecnología, ya que los enfoques más efectivos para la seguridad en aplicaciones requieren mejoras en todas estas áreas.

OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada con ninguna compañía de tecnología, aunque apoyamos el uso instruido de tecnologías de seguridad comercial. Al igual que muchos otros proyectos de software de código abierto, OWASP produce muchos tipos de materiales en una manera abierta y colaborativa.

La fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto. Casi todos los asociados con OWASP son voluntarios, incluyendo la junta directiva de OWASP, comités globales, líderes de capítulos, los líderes y miembros de proyectos. Apoyamos la investigación innovadora sobre seguridad a través de becas e infraestructura.

¡Únase a nosotros!

Historia de la empresa Owasp

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

OWASP Top 10 – 2010 (Previo)	OWASP Top 10 – 2013 (Nuevo)
A1 – Inyección	A1 – Inyección
A3 – Pérdida de Autenticación y Gestión de Sesiones	A2 – Pérdida de Autenticación y Gestión de Sesiones
A2 – Secuencia de Comandos en Sitios Cruzados (XSS)	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)
A4 – Referencia Directa Insegura a Objetos	A4 – Referencia Directa Insegura a Objetos
A6 – Defectuosa Configuración de Seguridad	A5 – Configuración de Seguridad Incorrecta
A7 – Almacenamiento Criptográfico Inseguro – Fusionada A9→	A6 – Exposición de Datos Sensibles
A8 – Falla de Restricción de Acceso a URL – Ampliada en →	A7 – Ausencia de Control de Acceso a las Funciones
A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)
<dentro de A6: – Defectuosa Configuración de Seguridad>	A9 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	A10 – Redirecciones y reenvíos no validados
A9 – Protección Insuficiente en la Capa de Transporte	Fusionada con 2010-A7 en la nueva 2013-A6

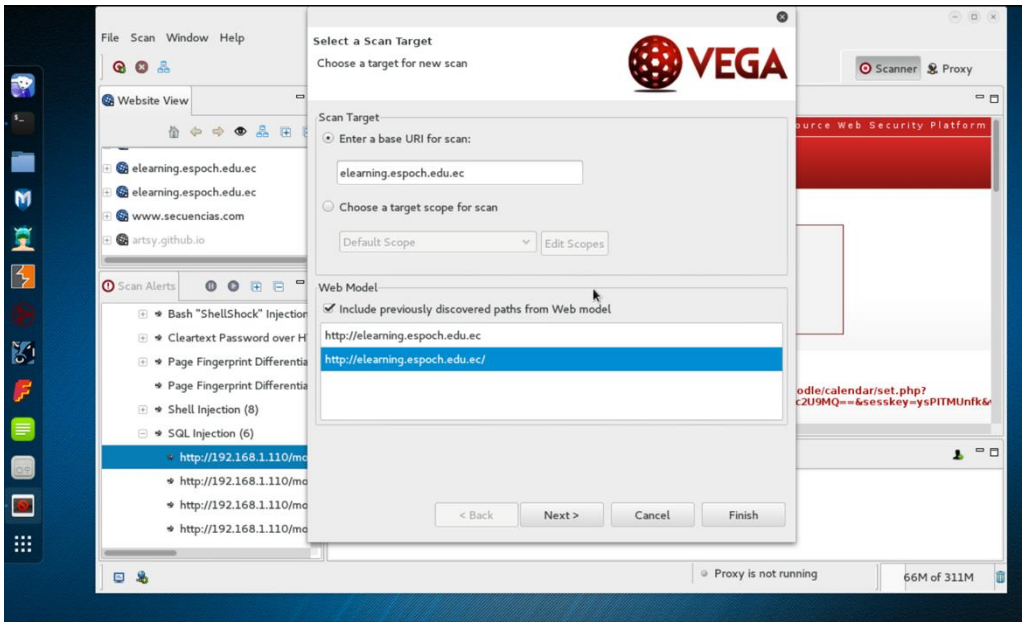
Top 10 de los principales ataques informáticos

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Anexo C: Ataque Inyección SQL en el servidor E-learning de la ESPOCH

En esta fase se procede a realizar un ataque de inyección de mysql que son códigos para vulnerar la base de datos de un servidor que es muy apetecible por los atacantes ya que ahí se encuentra toda la información y los datos de todos los usuarios.

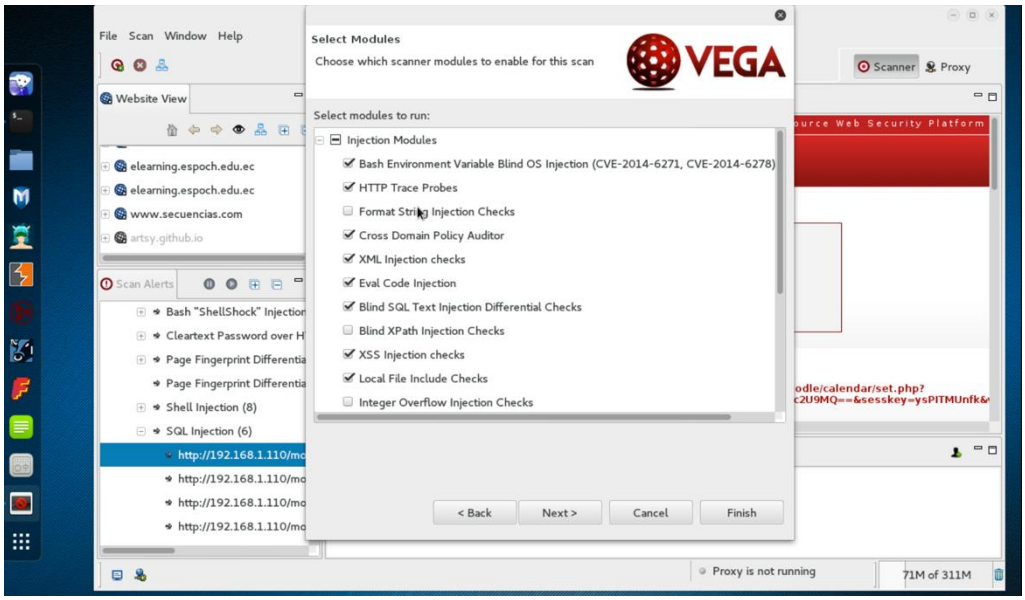
Primero se procede a buscar las vulnerabilidades de bases de datos con la herramienta VEGA de kali linux. Seguido ubicamos el objetivo en nuestro caso es elearning.espoch.edu.ec.



Elección de Objetivo en Vega con kali linux

Realizado por: Montesdeoca, R; Alvarado, A. 2017

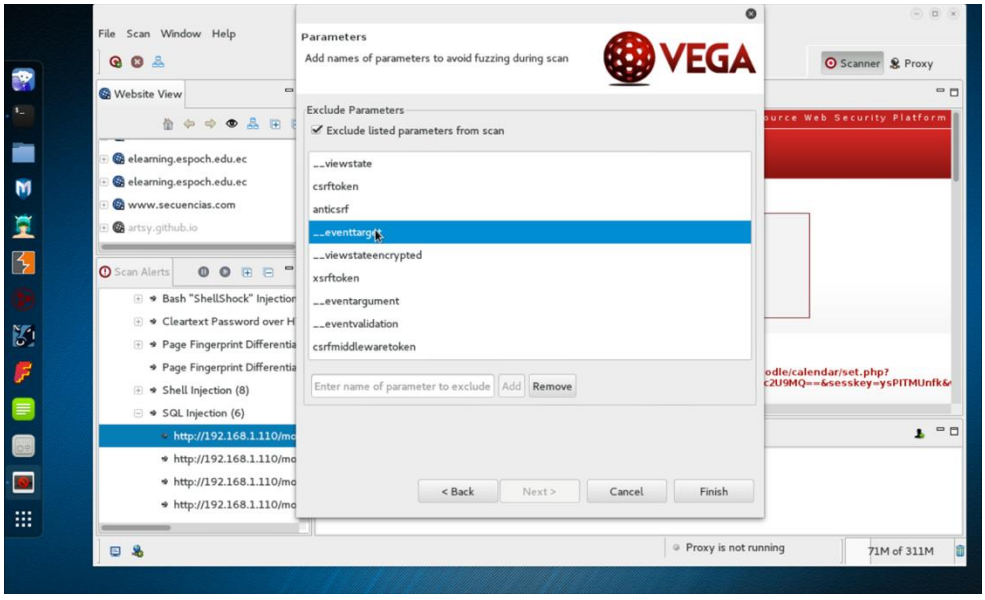
En el siguiente menú elegimos los tipos de ataques disponibles por la herramienta vega. Es importante destacar que debemos seleccionar las herramientas para el ataque de inyección de SQL.



Elección de ataques disponibles

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

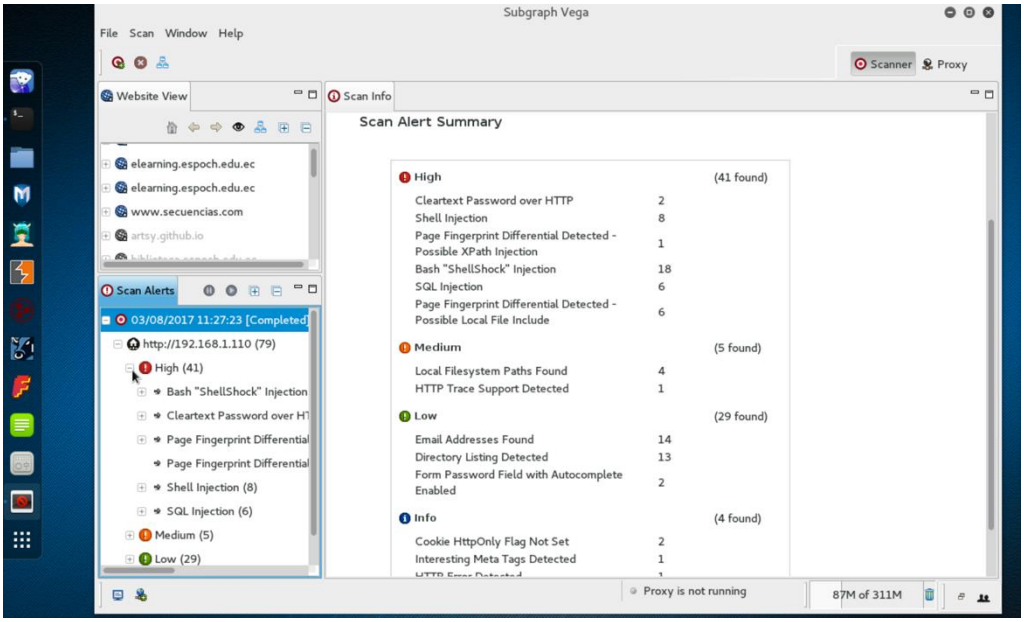
En el paso siguiente se elige Next, seguido de Finish, después automáticamente el programa empezara el escaneo, el escaneo dura entre 2 horas, hasta unas 6 horas, en nuestro caso duro alrededor de 6 horas, el tiempo de escaneo depende de la velocidad de procesador y de la capacidad de la maquina a realizar el escaneo.



Proceso para inicio de escaneo de datos

Realizado por: Montesdeoca, R; Alvarado, A. 2017

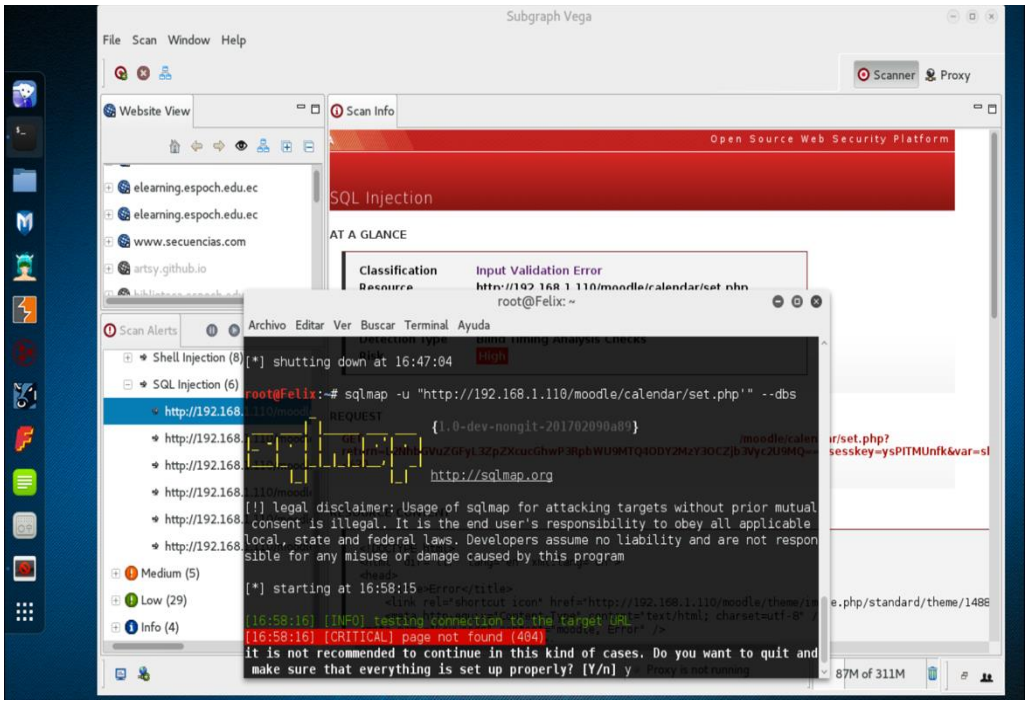
Los resultados que realiza esta herramienta los presenta de la siguiente manera en la figura



Resultado del ataque hecho por inyección SQL

Realizado por: Montesdeoca, R; Alvarado, A. 2017

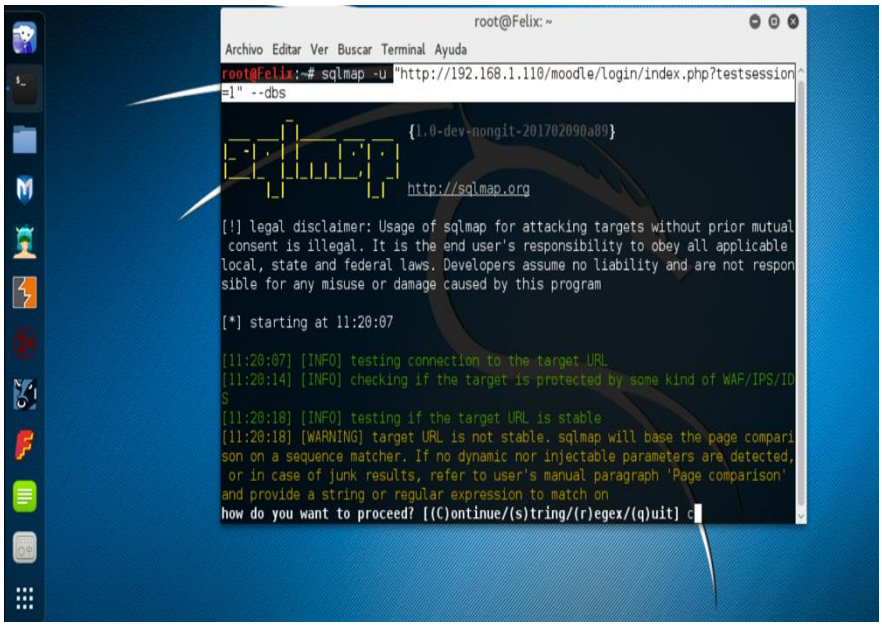
De esa lista de resultados encontramos que nos da la herramienta se ve que 6 posibles ataques de inyección se SQL se pueden atacar, seguido de esos resultados con la herramienta sqlmap de Kali Linux se realiza la respectiva comprobación de cada advertencia de la herramienta.



Comprobación de cada una de las vulnerabilidades que dejo el ataque

Realizado por: Montesdeoca, R; Alvarado, A. 2017

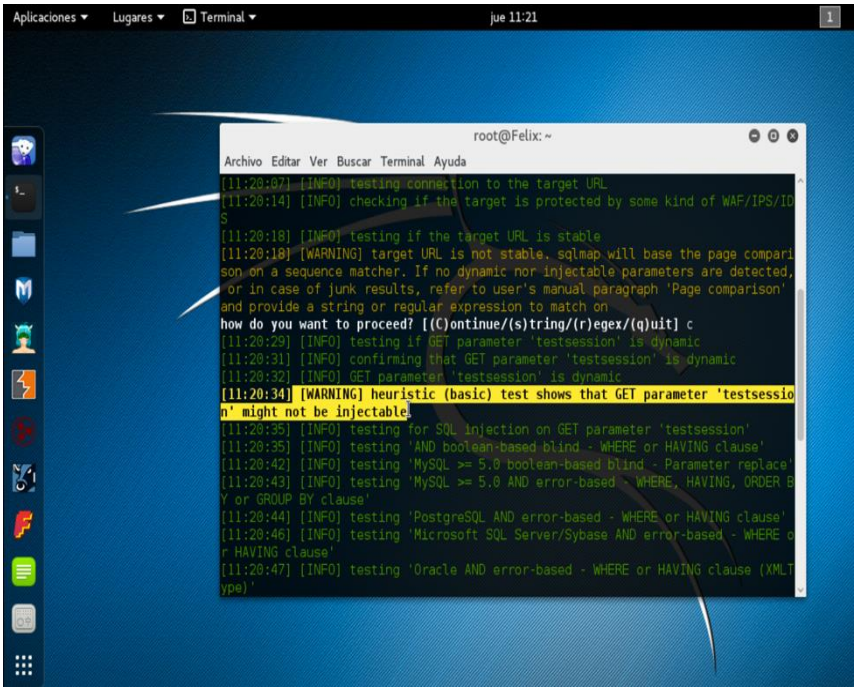
Con la opción –u configuramos la dirección de ataque vulnerable y con el comando –dbs obtenemos la base de datos como se muestra en la siguiente figura.



Proceso para el ingreso a la Base de datos

Realizado por**:** Montesdeoca, Alvarado

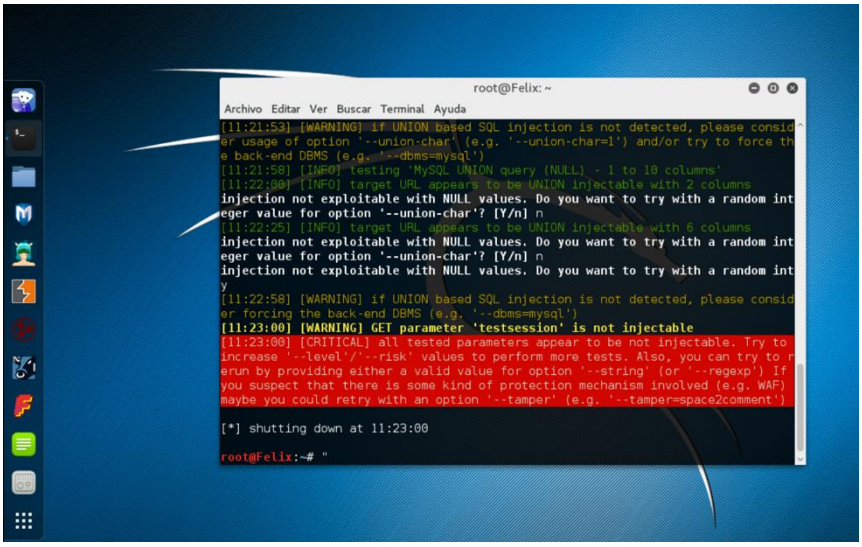
Seguido nos pide ingresar la techa c si deseamos continuar, se escribe c y se pulsa enter y nos arroja los resultados.



Base de Datos

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

En este análisis se observa que la base de datos no es inyectable con códigos SQL.



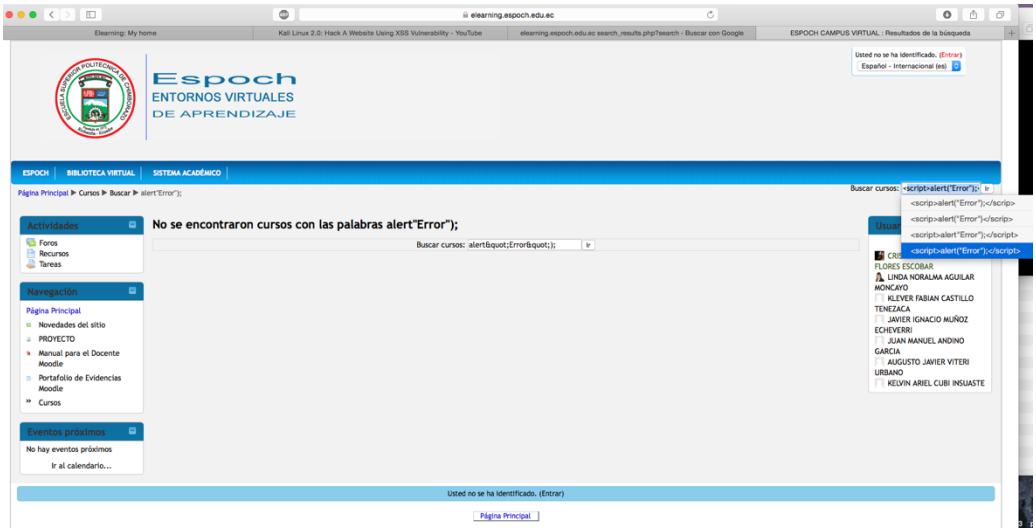
Base de datos no atacable con SQL Inyection

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Resultado de este ataque es que el sitio en análisis, el servidor elearning de la Espoch no es vulnerable a inyección de SQL.

Anexo D: Ataque mediante Cross-Site Script (XXC) al servidor E-learning de la ESPOCH

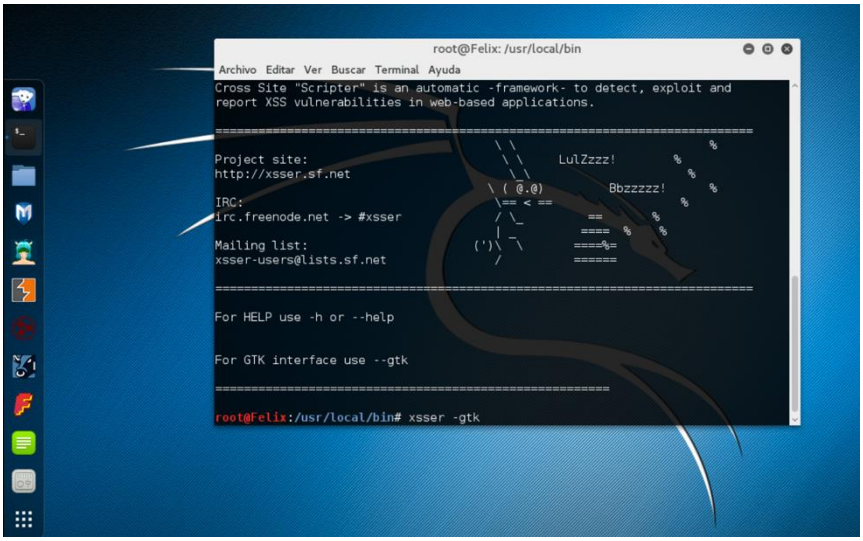
Ataque de Cross-site scripting directamente en la página del elearning de la Espoch si es vulnerable a este ataque, automáticamente tendría acceso y podríamos hacer e ingresar muchas cosas en el servidor alterando el estado actual y original del servidor.



Página principal del elearning de la ESPOCH

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

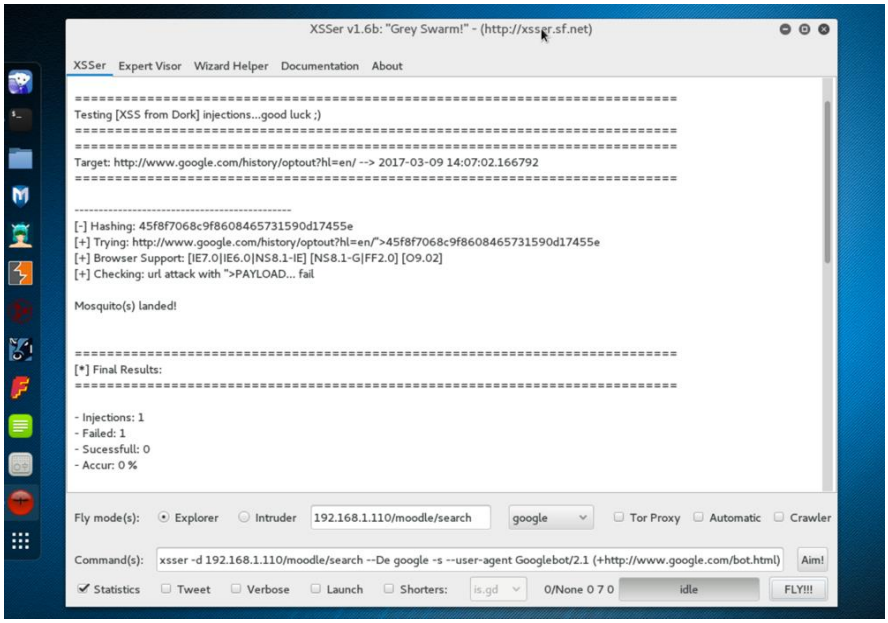
Con la herramienta kali Linux (sser) procedemos a buscar si el e-learning tiene vulnerabilidades y con el comando –gtk ingresamos a la interfaz grafica



Ingreso de comandos

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Siguiendo el ataque dando click en FLY, nos da como resultado que el sitio no es vulnerable al servidor elearning de la Espoch**.**

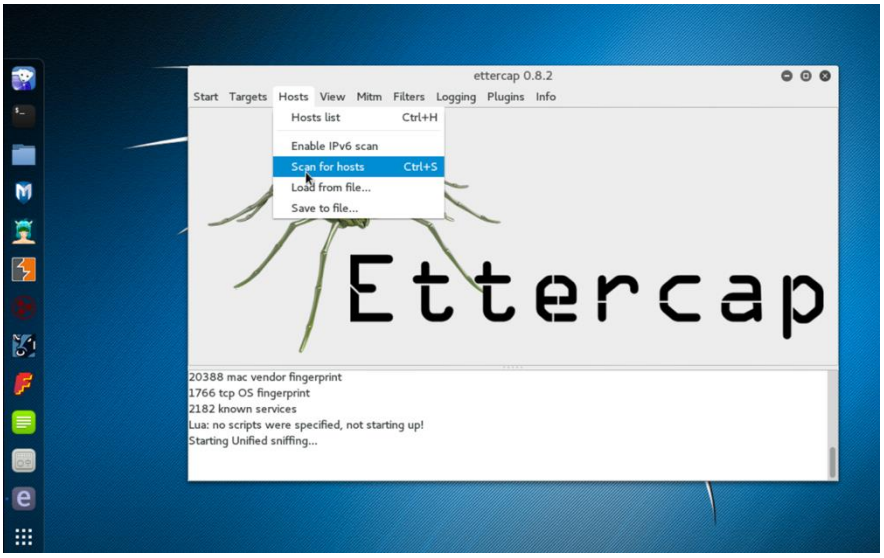


Resultado del ataque Cross site script XSS

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Anexo E: Ataque Sniffing al servidor E-learning de la ESPOCH

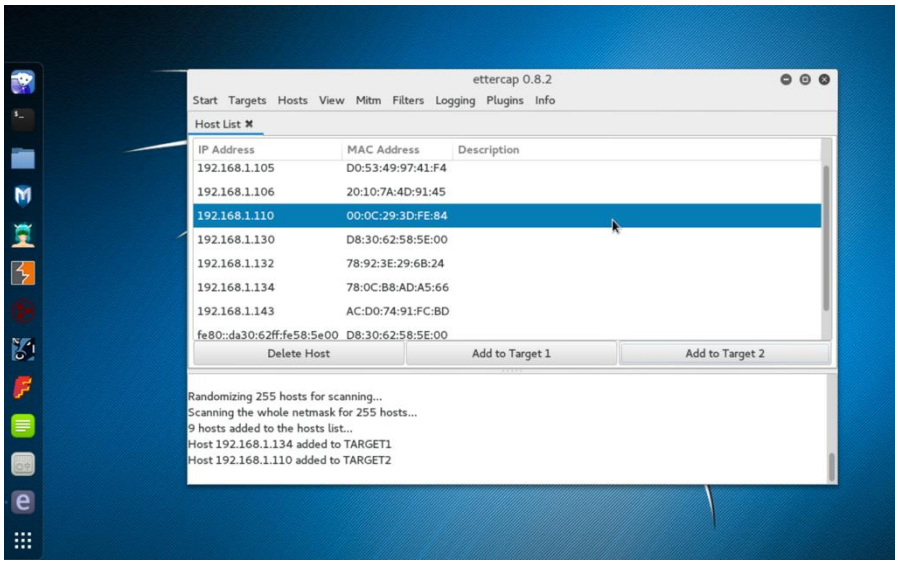
El objetivo del sniffing es espiar las contraseñas que van en texto plano a través del internet, para esto se lo realiza un ataque de hombre en el medio para capturar el trafico además de los nombres de usuarios y passwords. Usando la herramienta Ettercap de Kali Linux se va a realizar el ataque.



Herramienta Ettercap de Kali Linux

Realizado por: Montesdeoca, R; Alvarado, A. 2017

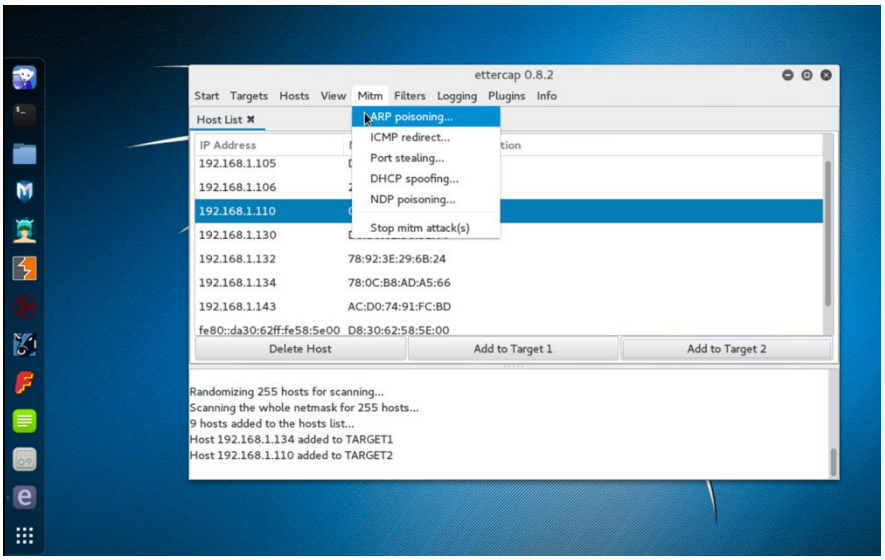
Para empezar el ataque primero debemos buscar cada host (máquina), dentro de la red del servidor en este caso lo hacemos en modo local, buscamos todos los hosts de la red y buscamos el servidor y un host para atacarlo como se lo muestra en la figura.



Host encontrado para atacarlo

Realizado por Montesdeoca, R; Alvarado, A. 2017

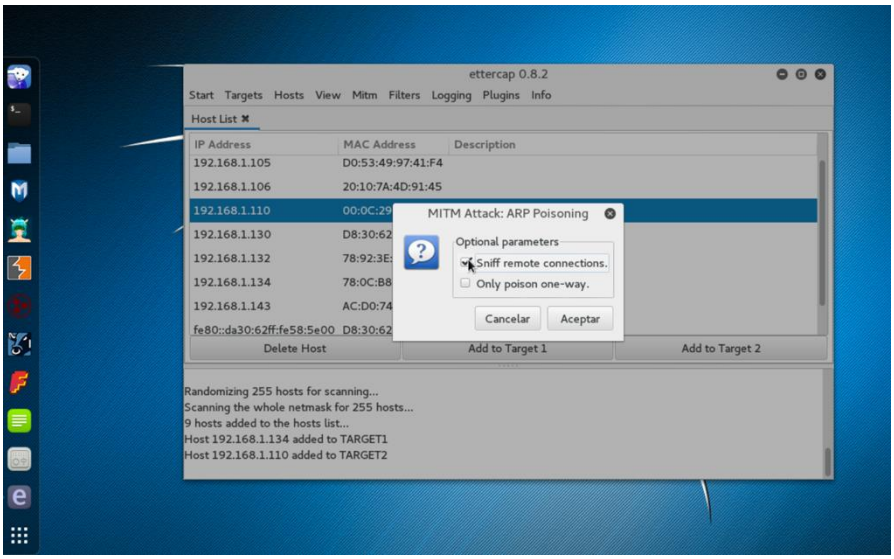
Una vez que se decidió la maquina objetivo y el servidor, se ubica la máquina objetivo en Add to target 1 y al servidor en Add to target 2 Visto en la figura.



Comienzo del ataque al host seleccionado

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

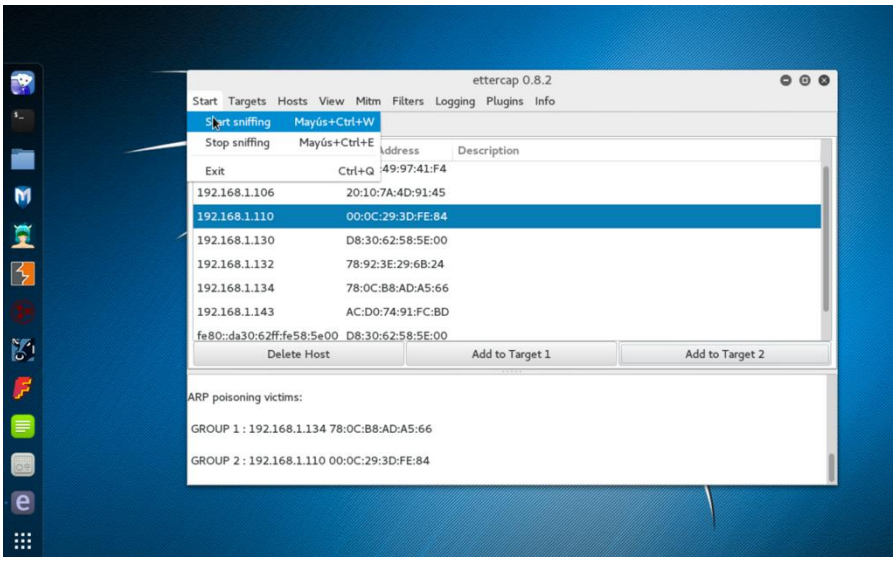
Para iniciar ya la captura de información en el menú Mint en la pestaña ARP poisoning, en la siguiente ventana tenemos dos opciones como se muestra en la figura.



Menú Mint

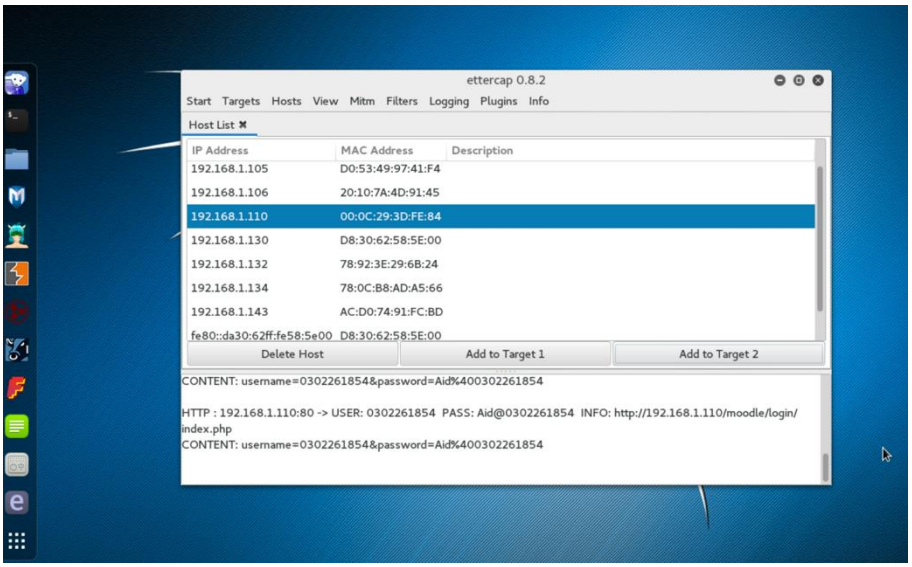
Realizado por: Montesdeoca, R; Alvarado, A. 2017

Dentro del menú Mint se escoge la opción Snuff remote connection, para analizar conexiones remotas dentro de scanner.



Conexiones Remotas
Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Cuando ya está activada esa función se procede a encender el análisis, en el menú Start, y en la pestaña Start sniffing.



Análisis o verificación de contraseñas

Realizado por: Montesdeoca, R; Alvarado, A. 2017

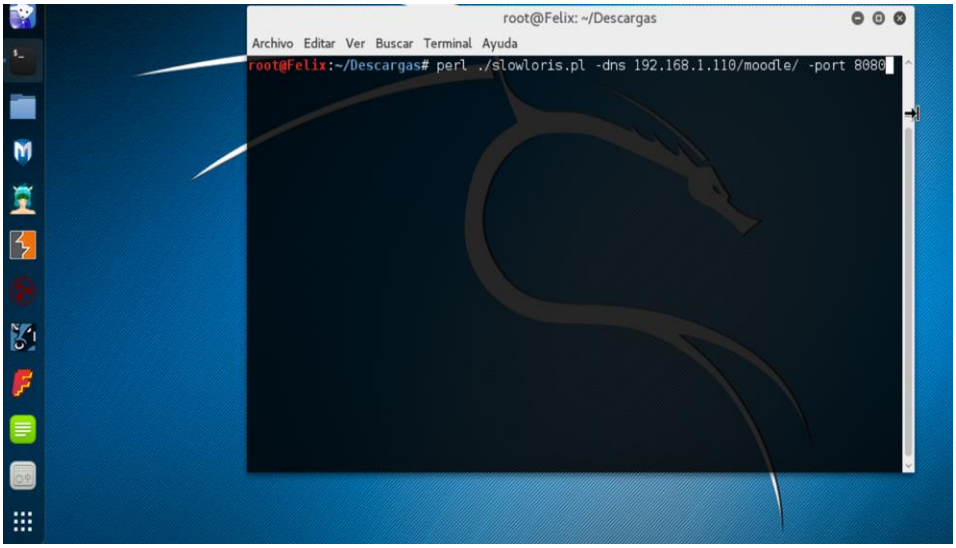
Cuando los usuarios navegan dentro de la página elearning el sniffing captura todos los movimientos, incluso el nombre de usuarios y las contraseñas. Para este caso capturamos el nombre de usuario y contraseña de una alumna que estaba en esa misma red. Por lo que se llegó a la conclusión que el servidor elearning de la Espoch es vulnerable ante este ataque.

Anexo F: Ataque DoS al servidor E-learning de la ESPOCH

El ataque de DoS consiste en atacar al servidor con inundación de paquetes saturando las peticiones, dejando sin servicio a los a los usuarios que se encuentran navegando por la página web.

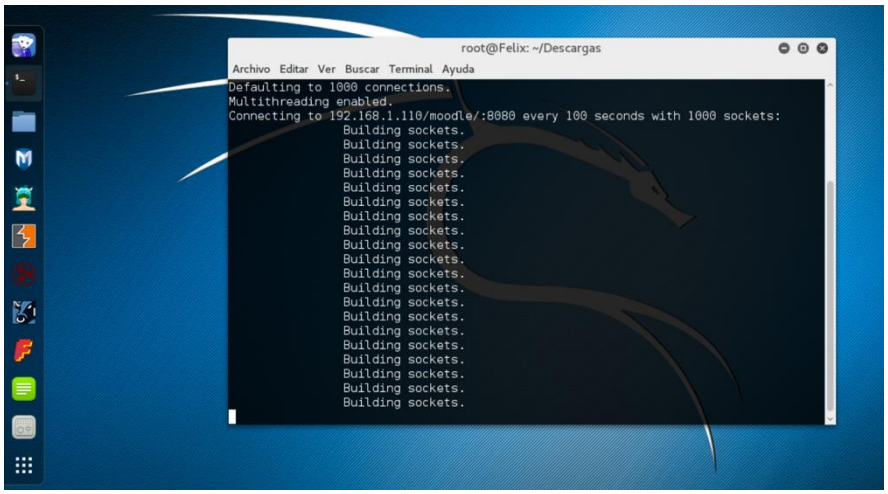
Para no perjudicar la página real del E-learning se procede a realizar un clon del servidor de la página real a una máquina virtual, que simula todas las características de una máquina real. Este ataque se lo realizo en una Red de Área Local (LAN) con 3 máquinas virtuales, una máquina virtual simula al servidor real, la segunda máquina realiza las funciones de atacante y la tercera máquina es un cliente normal.

Para este ataque lo primero que se debe hacer es ejecutar un archivo de kali Linux con el software Perl, a la dirección del servidor, con su respectivo puerto, como es una aplicación web el puerto es 80.



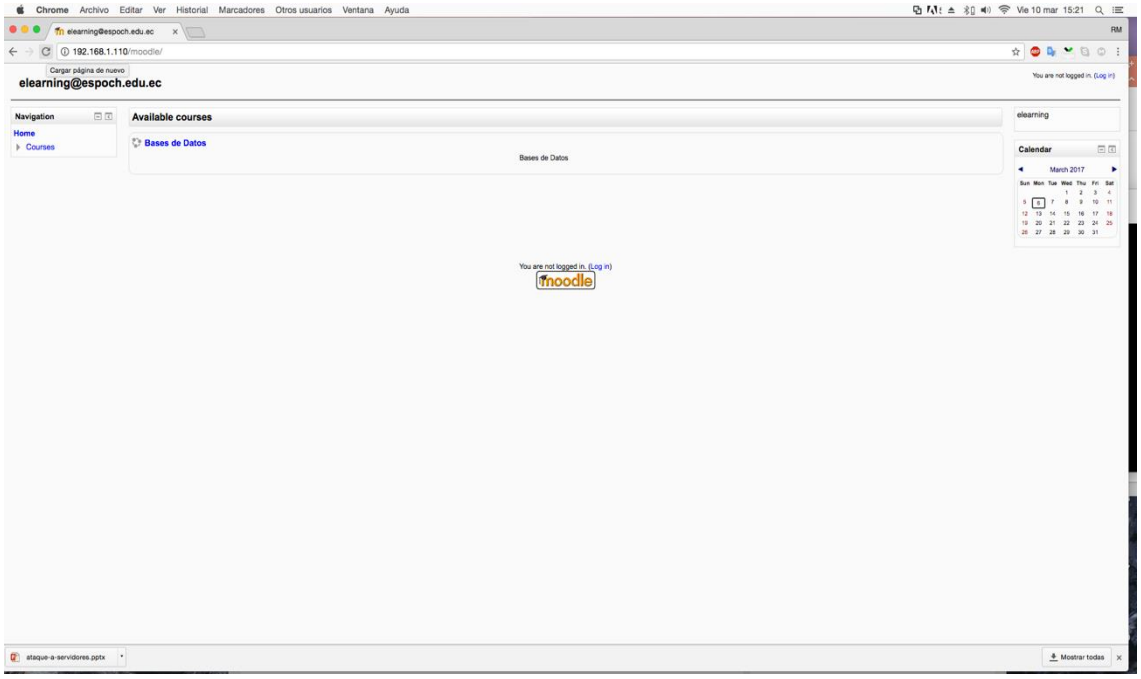
Software Perl
Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Como se ve en la figura, una vez ejecutado el ataque, el programa envía una gran cantidad de paquetes en contra del servidor, los valores son de forma automática van por miles de paquetes saturando la memoria RAM del servidor.



Envió de paquetes al Servidor
Realizado por: Montesdeoca, R; Alvarado, A. 2017

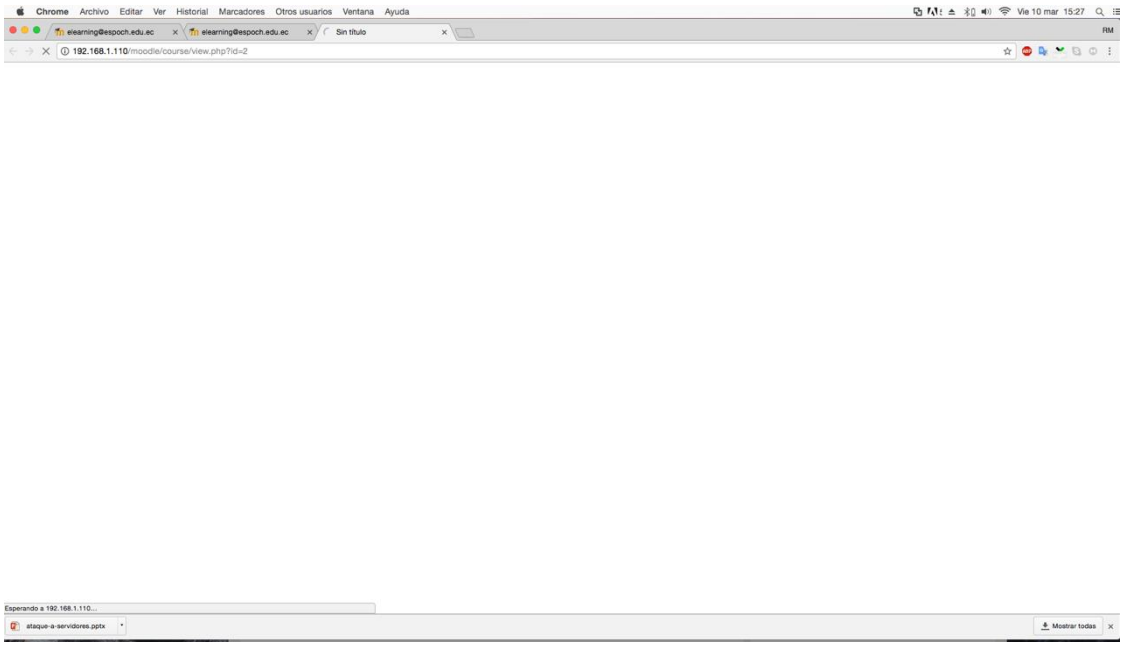
Cuando ya se efectuó el ataque, se procede a comprobar cómo reaccionaría el cliente. Para lo cual nos dirigimos a la máquina del cliente a realizar la respectiva comprobación. Esta sería la página web normal sin ningún tipo de ataque como se lo muestra en la figura:



Página principal del servidor sin ataque DoS

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Cuando está activo el ataque el usuario normal como no sabe lo que está pasando en el servidor ni el ataque que lleva en curso, sus principales quejas serán que el elearning no carga rápido, no puede subir archivos, no tiene conexión y después que no puede ingresar a su escritorio en Moodle.



Página principal del Servidor con el ataque DoS

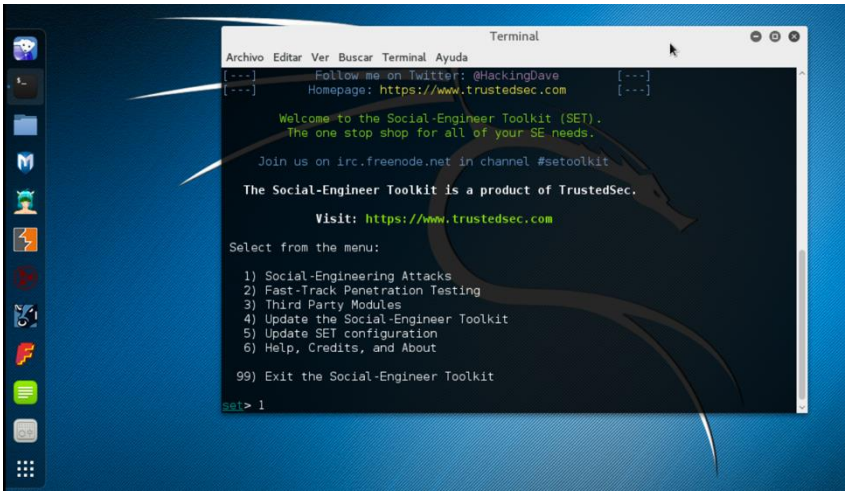
Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Como se ve en la figura la página elearning de la ESPOCH no reacciona y no puede cargar su contenido porque está siendo atacada por una denegación de servicio DoS. Por lo que el servidor es vulnerable ante este ataque.

Anexo G: Ataque Phising al servidor E-learning de la ESPOCH

Este ataque clona la página real por una página alterna y mientras un usuario pone sus contraseñas supuestamente en un sitio seguro el atacante captura toda su información y después le re direcciona a la página oficial como si nada hubiera pasado.

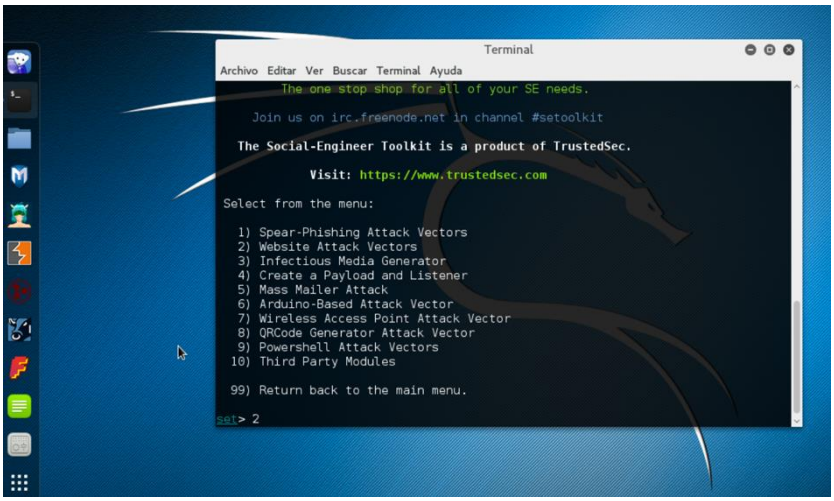
Para este ataque PHISING escogemos del menú la opción 1, que sirve para realizar un ataque de ingeniería social, luego de seleccionar pulsamos enter y en la figura nos muestra el siguiente menú.



Ingreso a SETOOLKIT de kali linux

Realizado por: Montesdeoca, Alvarado

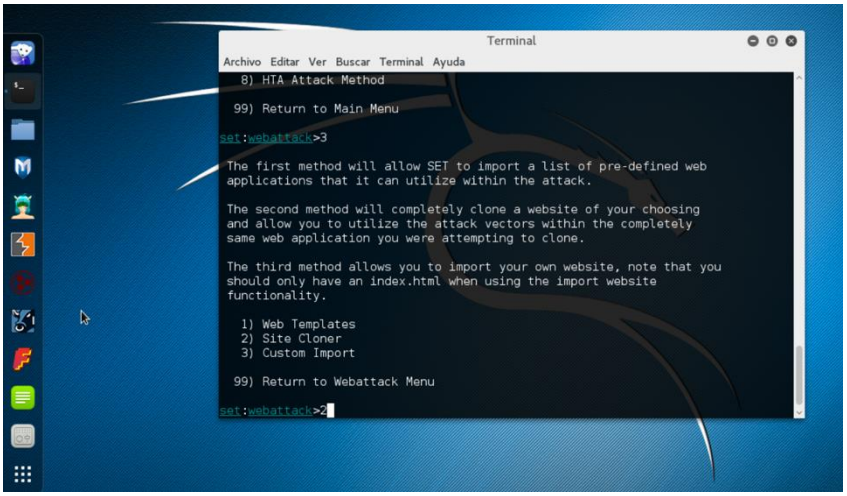
Para la clonación total de la página que vamos a atacar se necesita escoger del menú ataque de vectores del sitio web que es la opción 2 y pulsamos enter.



Menú de vectores de sitio web en Toolkit

Realizado por: Montesdeoca, R; Alvarado, A. 2017

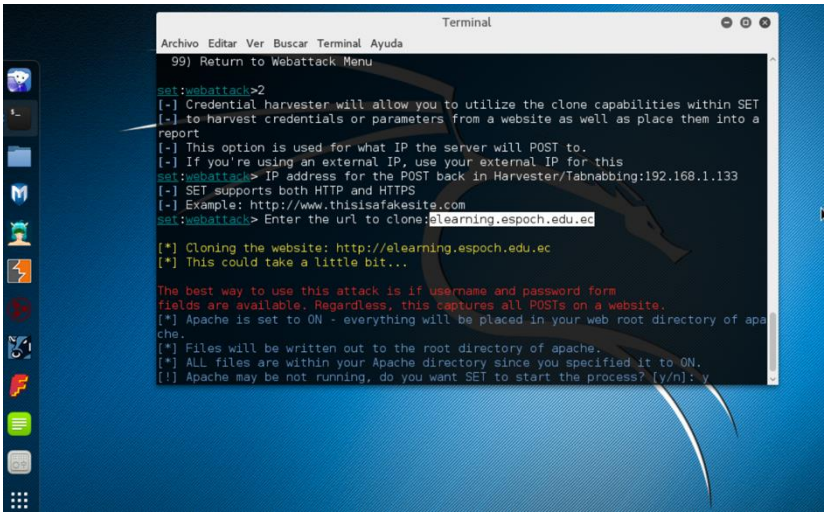
El siguiente paso de este ataque es realizar la clonación total del sitio web en análisis para ello escogemos la opción 2 del menú.



Ingreso a SETOOLKIT de kali linux

Realizado por: Montesdeoca, R; Alvarado, A. 2017

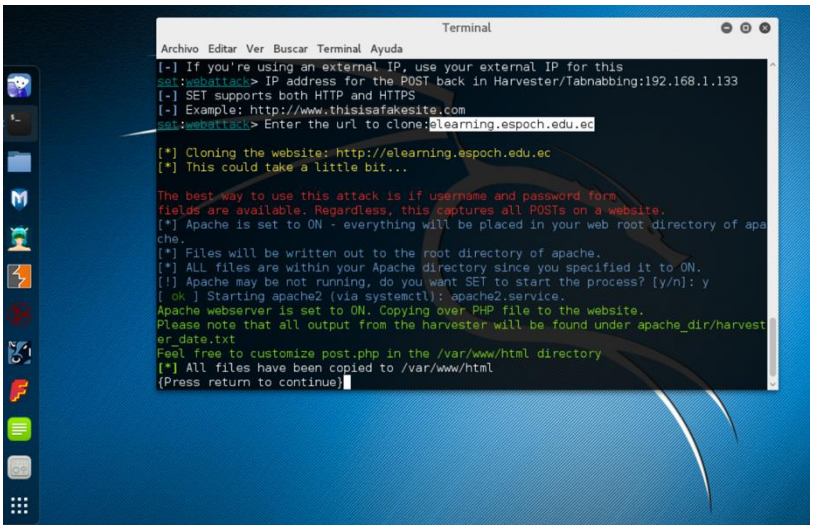
Una vez clonado el sitio web, nos pide la dirección IP de la maquina atacante, pulsamos enter y el ataque está corriendo, para que caigan los usuarios desprevenidos.



Ejecución y puesta en marcha del ataque de Phishing

Realizado por: Montesdeoca, R; Alvarado, A. 2017

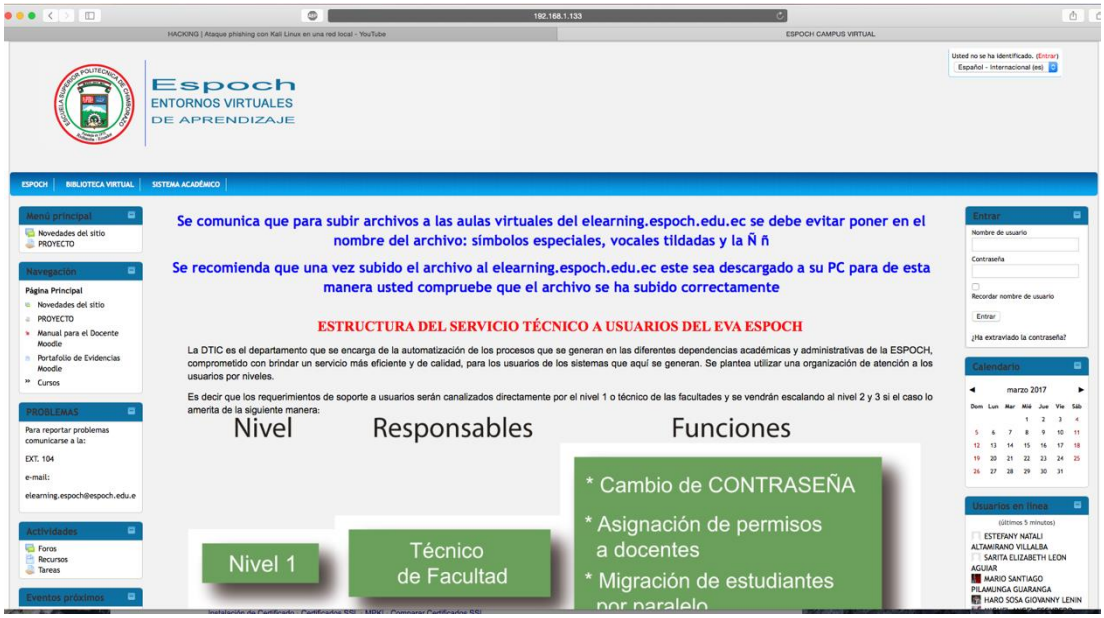
En esta figura vemos que se ha seguido todos los pasos correctamente, el servidor atacante está activo y esperando que los usuarios ingresen a la dirección IP falsa para almacenar las contraseñas de los usuarios.



Ataque activo esperando usuarios

Realizado por: Montesdeoca, R; Alvarado, A. 2017

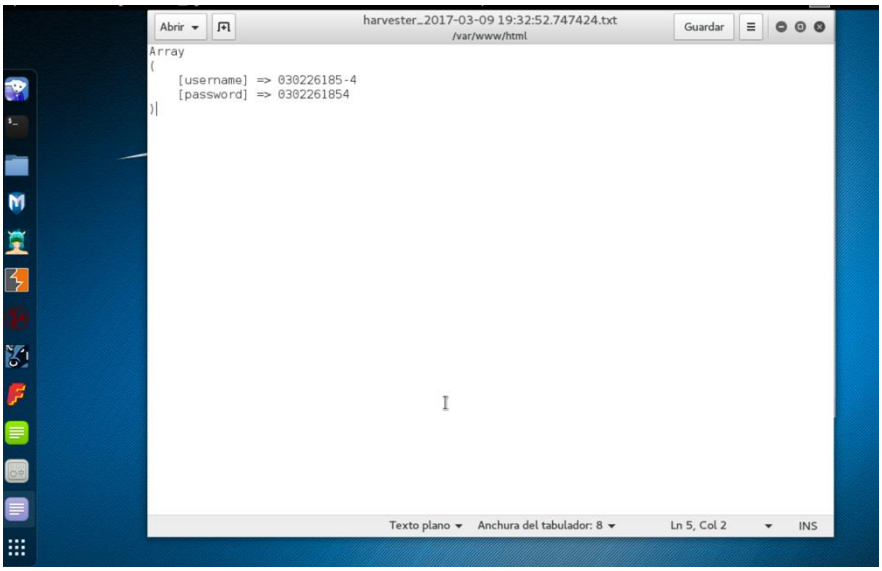
A un usuario normal por medio de correos electrónicos o por medio de mensajes en redes sociales se envía la dirección IP falsa y cuando el usuario habrá el enlace se va a encontrar con la siguiente figura, la página web del E-learning de la ESPOCH idéntica, pero con una IP diferente.



Página Web E-learning clonada

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Cuando un usuario intenta ingresar al E-learning, ingresara sus datos, pero la página web no se habré si no que se redirige a la página real, pero el atacante ya ha conseguido obtener sus datos de ingreso al sitio, como se puede observar en la siguiente figura.



Captura de datos con el ataque de Phishing

Realizado por**:** Montesdeoca, R; Alvarado, A. 2017

Anexo H: Guia de mejores practicas

GUIA DE MEJORES PRÁCTICAS PARA EL SERVIDOR E-LEARNING DE LA ESPOCH

AIDA CONCEPCION ALVARADO TAPIA
RICHARD ALFREDO MONTESDEOCA CABRERA

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO
FACULTAD DE INFORMATICA Y ELECTRONICA
ESCUELA DE INGENIERIA ELECTRONICA EN TELECOMUNICACIONES Y REDES
RIOBAMBA
2017

Introducción

Esta es una guía de propuesta para la implementación de seguridad a las vulnerabilidades encontrados en el servidor E-learning de la Escuela Superior Politécnica de Chimborazo, para luego analizar el funcionamiento con dicha implementación de seguridad al servidor, pero es necesario que se implemente esta guía de mejores prácticas, dicha guía está basada en la seguridad informática de la empresa CSIRT (equipo de respuesta a incidentes y delitos informáticos) que tiene un sistema completo de seguridad informática, y se enfocó en el paso 4 que está relacionado con *Protección a servidores.* (CSIRT, 2010, pág. 5-6). A continuación, se detalla dicha guía que resolverá los problemas de seguridad encontrados en el servidor E-learning de la ESPOCH.

Objetivo de esta Guía

El objetivo primordial de esta guía es ayudar a comprender paso a paso de lo importante de utilizar estos métodos de seguridad para hacer del servidor E-learning de la ESPOCH un sitio seguro y libre de vulnerabilidades

Dirigido a:

Esta Guía va dirigido al Departamento de Desarrollo de las DTIC de la ESPOCH, es decir para las personas encargadas de monitorear, controlar y actualizar el servidor E-learning

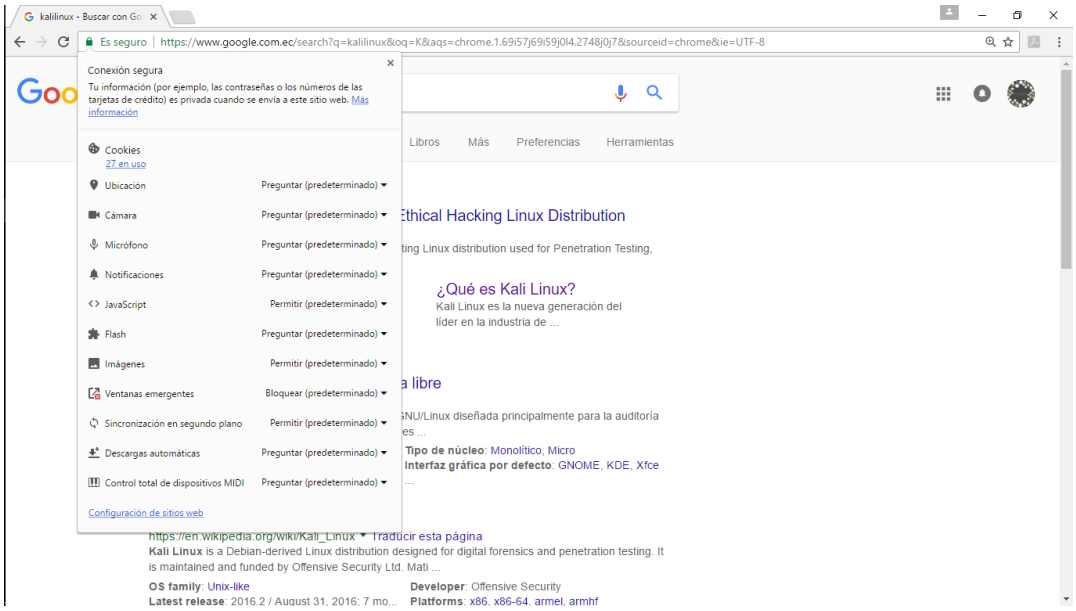
DESARROLLO DE LA GUIA

CERTIFICADOS DE SERVIDOR

Identificar los sitios Web deberá requerir la existencia de una autoridad certificadora (CA) que afirme, mediante los correspondientes certificados de servidor, que éstos son quienes dicen ser antes del establecimiento del canal seguro. Le permitirá establecer comunicaciones seguras con sus clientes, cifrando la conexión usando la tecnología SSL para que no pueda ser leída por terceros. (CSIRT, 2010, pag 5-6).

PROPUESTA 1: CERTIFICACION DE ENCRIPTACION SSL

Un certificado SSL es un archivo informático digital (o un código de tamaño pequeño) que tiene dos funciones específicas: AUTENTIFICACION Y VERIFICACION. El certificado SSL tiene información acerca de la autenticidad de ciertos datos referentes a la identidad de una persona, empresa o sitio web, la cual se mostrará a los visitantes en su sitio web cuando estos hagan clic en el símbolo del candado del navegador o en la marca de confianza.



Detalle de opciones cuando la página está segura con SSL

Realizado por: Montesdeoca, R; Alvarado, A. 2017

CIFRADO DE DATOS: El certificado SSL también posibilita el cifrado. Esto significa que absolutamente nadie, excepto el destinatario deseado, puede interceptar y leer la información confidencial que se intercambia por la Web y lo encripta con 128 bits.

¿Cómo funciona el cifrado SSL?

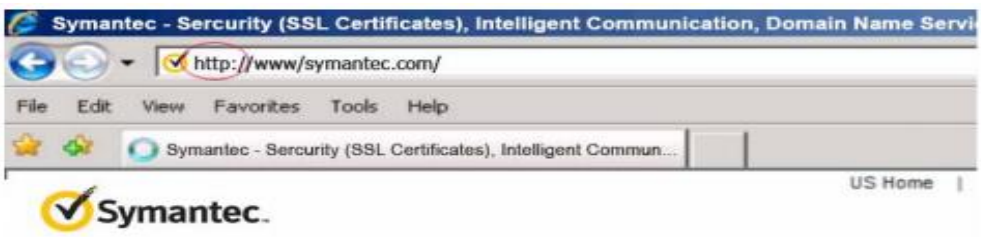
Por ejemplo, si usted cierra y abre las puertas con una llave, el cifrado usa claves para bloquear y desbloquear su información. A menos que tenga la clave correcta, usted no podrá "abrir" la información.
Cada sesión de SSL consta de dos claves:
La clave pública se usa para cifrar (codificar) la información.
La clave privada se usa para descifrar (decodificar) la información y restaurarla a su formato original para que pueda ser leída.

¿Cuál es el proceso con SSL?

Cada certificado SSL que se emite para una entidad verificada por una autoridad de certificación se emite para un dominio de sitio web (dirección de sitio web) y un servidor específico. Cuando una persona usa el navegador para dirigirse a la dirección de un sitio web con un certificado SSL, se establece un protocolo de enlace de SSL (reconocimiento) entre el navegador y el servidor. Se solicita información del servidor, la cual entonces es visible para la persona en su ventana del navegador. Usted notará cambios que indican el inicio de una sesión segura, por ejemplo, aparecerá una marca de confianza. Si hace clic en la marca de confianza, verá información adicional, como el período de validez de un certificado SSL, el dominio asegurado, el tipo de certificado SSL y la autoridad de certificación que emite el certificado. Todo esto significa que se estableció un vínculo seguro para esa sesión con una clave de sesión única y que pueden comenzar las comunicaciones seguras.

¿Cómo saber si un sitio tiene o no un certificado SSL?

Un sitio web estándar sin seguridad SSL muestra "http://" antes de la dirección del sitio web en la barra de direcciones del navegador. Este alias significa "protocolo de transferencia de hipertexto" y es la manera convencional para transmitir información por Internet.



Sitio sin certificado SSL

Realizado por: Aida Alvarado

En cambio, un sitio web protegido con un certificado SSL mostrará “https://” antes de la dirección. Esto significa “HTTP seguro”.

Sitio con certificado SSL

Realizado por: Aida Alvarado

¿Dónde usar un certificado SSL?

Se usaría certificados SSL siempre que se quiera proteger la información, por ejemplo:

- Proteger la comunicación entre el sitio web y el navegador de Internet del cliente.
- Proteger las comunicaciones internas en la intranet corporativa.
- Proteger las comunicaciones de correo electrónico entrante y saliente de la red (o de una dirección personal de correo electrónico).
- Proteger la información entre servidores (tanto internos como externos).
- Proteger la información que se envía y se recibe mediante dispositivos móviles.

¿Qué tipo de certificado SSL nos conviene más?

Con frecuencia, los certificados SSL Extended Validation (EV) ofrecen el estándar de autenticación más alto del sector y proporcionan el mejor nivel de confianza disponible para el cliente. Cuando los consumidores visitan un sitio web protegido con un certificado SSL EV, la barra de direcciones aparece de color verde (en los navegadores de alta seguridad) y se muestra un campo especial con el nombre del propietario legítimo del sitio web junto con el nombre del proveedor de seguridad que emitió el certificado SSL EV. En la barra de direcciones, también se muestra el nombre del titular del certificado y de la autoridad de certificación que lo emite. Esta prueba visual de certeza ha ayudado a incrementar la confianza del consumidor en el comercio electrónico. (Symantec, 2013)

¿**Cómo instalar un certificado SSL?**

Existen varios métodos para instalar certificados SSL auténticos, pero se realizó la instalación del certificado utilizando el método con Apache, a continuación, se detallará paso a paso dicha instalación.

1. **Generar una solicitud de firma de certificado (CSR)**

Antes de cualquier certificado SSL, es necesario generar un CSR (Certificate Signing Request) en el servidor. Este archivo contiene información del servidor y de la clave pública que es necesaria para que genere a clave privada. También se puede generar un CSR desde la línea de comandos de apache así. (Symantec, 2013)

- Abrir la utilidad OpenSSL, que se encuentra en /usr/local/ssl/bin
- Crear un par de claves (privada y pública), una para el servidor y otra para el cliente, con la finalidad que la comunicación sea segura, ingresando el siguiente comando.

```
openssl genrsa -des3 -out www.mydomain.com.key 2048
```

- Crear una frase de acceso (nombre de la clave).
- Iniciar el proceso de generación de CSR. Se deberá ingresar el siguiente comando cuando se solicite crear el archivo CSR.

```
openssl req -new -key www.mydomain.com.key -out www.mydomain.com.c
```

- Completar la información requerida. Se necesita ingresar el código de dos dígitos del país, el estado o la provincia, la ciudad, el nombre completo de la empresa, el nombre de la sección (esto es, IT o Mercadeo), y el nombre común (en general es el nombre de dominio).
- Ingresada la información, ejecutar el comando siguiente para generar el archivo CSR en el servidor.

```
openssl req -noout -text -in www.mydomain.com.csr
```

2. **Solicitar el certificado SSL**

Los servicios más populares incluyen DigiCert, Symantec, GlobalSign, entre otros. El mejor servicio dependerá de las necesidades (certificados múltiples, soluciones empresariales, etc.). Es necesario subir el archivo CSR al servicio de certificados, esto se usa para generar el certificado para el servidor.

3. **Descargar los certificados**

Recibirá el certificado primario por correo electrónico, la clave se verá como en el ejemplo.

```
-----BEGIN CERTIFICATE-----
[Encoded Certificate]
-----END CERTIFICATE-----
```

- Si los certificados están en archivo de texto, se cambia al formato .CRT (security certificate) que contiene toda la información de la empresa, esto es necesario antes de subir el archivo.

- En las claves debe estar 5 guiones en cada lado de las líneas BEGIN CERTIFICATE y END CERTIFICATE.
- No debe haber saltos de línea ni espacios adicionales en la clave.

4. **Subir los certificados al Servidor E-learning**

Se debe crear una carpeta donde se pone todos los certificados y claves, todos deben estar juntos y en la siguiente ruta del servidor, así: /usr/local/ssl/crt

5. **Abrir el archivo "httpd.conf" en el editor de texto**

En algunas versiones del Apache tiene dos archivos distintos para certificación SSL, editar solo uno de ellos "ssl.conf". Añadir las siguientes líneas a la sección de virtual Host, así:

```
SSLCertificateFile /usr/local/ssl/crt/primary.crt
SSLCertificateKeyFile /usr/local/ssl/private/private.key
SSLCertificateChainFile /usr/local/ssl/crt/intermediate.crt
```

- Guardar los cambios y en caso de ser necesario subir nuevamente el archivo.

6. **Reiniciar el servidor**

Cuando el archivo ya este subido y esté operando, se utilizara el certificado SSL reiniciando el servidor. Se utiliza estos comandos "apachectlp stop" o "apachectl startssl"

7. **Comprobar el certificado**

Para comprobar se debe ingresar a la página web del servidor. Conectarse al sitio web usando "https://", esto es para forzar la conexión ssl. El icono de la barra de direcciones deberá estar de color verde, si es así ya está seguro el sitio y esta con certificados SSL. (wikiHow, 2017)

MANTENER LOS SERVIDORES EN UN LUGAR SEGURO.

- *Se deben asegurar de que los servidores no son vulnerables a las catástrofes físicas.*
- *Colocar los equipos en una sala segura y con buena ventilación.*
- *Hacer un registro de los empleados que tienen las llaves de la sala de servidores.* (Mieres, 2010, pág. 5-6).

PROPUESTA 2: Almacenamiento en la Nube

Debido a lo importante que es para una organización situar los servidores de copias de seguridad lejos de sus centros principales de datos para que, en caso de catástrofe regional, el evento no eliminase ambos servidores. Una buena medida, y más económica que los servidores físicos, es guardar la información en una nube, ya que esta puede ofrecerle gran capacidad de almacenamiento y permitirle recuperar datos con rapidez.

Es fundamental examinar la manera en la que los proveedores copian y protegen sus propios sistemas, de esta manera se analizó algunas empresas que proveen estos servicios para realizar copias de seguridad.

Descripción: Comparativa entre las 5 mejores compañías Internacionales proveedoras de servicio en la nube.

EMPRESAS INTERNACIONALES	
NOMBRE DE LA COMPAÑÍA	**DESCRIPCION**
Drobox	• Facilidad en operaciones • 2 Gigabytes de almacenamiento en la nube disponible de forma gratuita y 100Gb por $9,99 mensuales • Diseño practico que brinda y aporta al usuario.
OneDrive o SkyDrive	• 7 Gb de almacenamiento en la nube gratuito • con el pago de 10$, se le otorga 20 Gigabytes extras.
Google Drive	• Adhiere cualquier tipo de extensión • Sincroniza archivos para trabajar desde cualquier lugar y dispositivo. • Enlace público, dando acceso a otros usuarios • Pagando desde $2.49 mensuales
Box	• posee apps para dispositivos móviles iOS y Android. • Al pagar 29.99$ al mes, tu espacio de almacenamiento aumenta 50 Gb más.
Mega	• gran cantidad de servicios y de buena calidad • Ofrece al usuario un total de 50 Gb • con $12 al mes, tendrá una capacidad 500 Gb. • No posee aplicaciones oficiales para dispositivos móviles. • Se puede contar con aplicaciones de terceros que funcionan bien.

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Descripción: La mejor empresa Nacionale proveedora de servicio en la nube.

EMPRESAS NACIONALES	
NOMBRE DE LA COMPAÑÍA	**DESCRIPCION**
TELCONET	• Empresa que provee el servicio de la nube en Ecuador, • Cloud es una tendencia mundial

	• Telconet promociona el uso de la nube desde hace dos años. • Provee tres tipos de paquetes y su target es el sector corporativo. • La demanda en los dos últimos años ha ido creciendo • Cuatro centros de datos en Guayaquil • Precio desde $25 a 100Gb de capacidad

Realizado por: Montesdeoca, R; Alvarado, A. 2017

Estas son las mejores opciones en cuanto a servicio en la nube. Se recomienda ver los cuadros comparativos y escoger la mejor opción que requiere los servidores dependiendo de los requerimientos necesarios ya se nacional o internacional.

PRÁCTICA DE MENOS PRIVILEGIOS.

*Asignar distintos niveles de permisos a los usuarios. En vez de conceder a todos los usuarios el acceso Administrador, debe utilizar los servidores para administrar los equipos cliente. Los servidores de Windows se pueden configurar para conceder a cada usuario acceso únicamente a programas específicos y para definir los privilegios de usuario que se permiten en el servidor. De este modo se garantiza que los usuarios no pueden efectuar cambios que son fundamentales en el funcionamiento del servidor o equipo cliente. (*Mieres, 2010, pag 5-6).

PROPUESTA 3: INTEGRACIÓN DE DMZ (ZONA SEGURA)

DMZ (Zona Desmilitarizada) es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red. La intención de DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido.
Debido a la naturaleza no-trivial de la implementación de DMZ, no se recomienda utilizar un DMZ salvo que tenga una gran familiaridad con las redes. Una DMZ no suele ser un requisito, pero en general es recomendada por los administradores conscientes de seguridad de la red. (TP-Link, 2017)

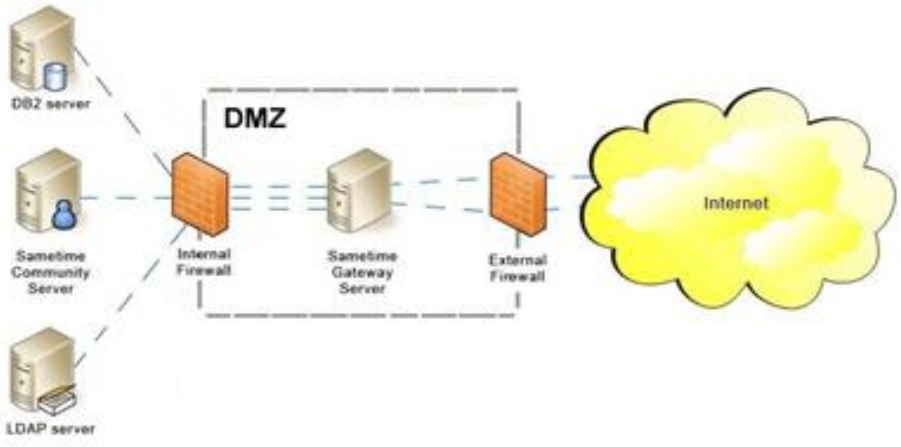
Las políticas de seguridad aplicada en la DMZ, normalmente es la siguiente:

- Tráfico de la red externa hacia la DMZ autorizada;
- Tráfico de la red externa hacia la red interna prohibida;
- Tráfico de la red interna hacia la DMZ autorizada;
- Tráfico de la red interna hacia la red externa autorizada;
- Tráfico de la DMZ hacia la red interna prohibida;

- Tráfico de la DMZ hacia la red externa rechazada.

Arquitectura DMZ

Se habla entonces de una "zona desmilitarizada" (DMZ para DeMilitarized Zone) para designar esta zona aislada que aloja aplicaciones a disposición del público. El DMZ sirve como una zona intermedia entre la red a proteger y la red hostil. (INFORMATICAHOY, 2016)



Funcionamiento de la DMZ en un servidor.
Realizado por: Montesdeoca, R; Alvarado, A. 2017

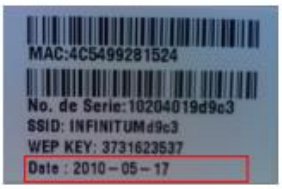
Configuración DMZ

1. **Conectar la PC al modem vía cable o wifi**
2. **Entrar a la interfaz de configuración del modem como se muestra a continuación con los siguientes pasos.**

    - Se abre el explorador de internet y se ingresa la siguiente dirección 192.168.1.254
    - Ingresamos los siguientes datos

      Nombre de Usuario: TELMEX

      Contraseña: se encuentra en la etiqueta, dice Web Key



3. **Interface de configuración**
    - Se selecciona el estado Avanzado
    - Se selecciona Firewal
    - También se selecciona Permitir Todas las Aplicaciones

4. **Configurar de la siguiente manera**

    - En aplicaciones seleccionamos Activado
    - En dirección IP, ingresamos la dirección de la maquina o dispositivo al cual le queremos habilitar DMZ

5. **Seleccionar guardar y así finaliza la configuración DMZ.**

FIREWALL CON DMZ

Un firewall es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya definidas

Hablando de manera genérica, un firewall es un método de protección de servidores o redes, que están conectados a otros servidores o redes, existen diferentes maneras de “colocar” un firewall en la red, de manera muy concreta un firewall es un packet filter (filtrado de paquetes).

Firewall ASA Cisco, este equipo es el más recomendado en cuanto al servicio de protección de servidores que requiere las DTIC. Debido a que la ESPOCH tiene la mayor cantidad de equipos CISCO instalados, el Firewall ASA CISCO cumple con los requerimientos necesarios según la tabla extraída de la página oficial de CISCO.

Características de firewall Cisco ASA

Realizado por: (CISCO, 2015)

Dispositivos adaptables de seguridad de la serie Cisco ASA 5500

SIGLAS
SSC: Tarjeta de servicios de seguridad, **SSM:** Módulo de servicios de seguridad, **AIP-SSM:** Módulo de servicios de seguridad de inspección y prevención avanzadas, **CSC-SSM:** Módulo de servicios de seguridad de control y seguridad de contenidos, **4GE-SSM:** Módulo de servicios de seguridad 4 Gigabit Ethernet

Modelo/licencia de la serie Cisco ASA 5500	Cisco ASA 5505 Base/Security Plus	Cisco ASA 5510 Base/Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Mercado	Oficina pequeña, hogareña /Oficina remota, sucursal / Plataforma de switching de servicios múltiples / Trabajadores móviles empresariales	Empresas en crecimiento y empresas pequeñas	Empresas pequeñas	Empresas medianas	Grandes empresas
Resumen de rendimiento					
Capacidad máxima de procesamiento (Mbps) del firewall	150	300	450	650	1200
Capacidad máxima de procesamiento (Mbps) de VPN 3DES/AES	100	170	225	325	425
Cantidad máxima de sesiones de usuario de VPN de sitio a sitio y de acceso remoto	10 / 25	250	750	5000	5000
Cantidad máxima de sesiones de usuario de VPN SSL1	25	250	750	2500	5000
Cantidad máxima de conexiones	10.000 / 25.000	50.000 / 130.000	280.000	400.000	650.000
Cantidad máxima de conexiones /segundo	3000	6000	9000	20.000	28.000
Paquetes por segundo (64 bytes)	85.000	190.000	320.000	500.000	600.000
Resumen técnico					
Memoria (MB)	256	256	512	1024	4096
Memoria flash del sistema (MB)	64	64	64	64	64
Puertos integrados	Switch de 8 puertos 10/100 con 2 puertos Power over Ethernet	5-10/100	4-10/100/1000, 1-10/100	4-10/100/1000, 1-10/100	8-10/100/1000, 1-10/100
Cantidad máxima de interfaces virtuales (VLAN)	3 (enlaces troncales desactivados) / 20 (enlaces troncales activados)	50/100	150	200	250
Ranura de expansión SSC/SSM	Sí (SSC)	Sí (SSM)	Sí (SSM)	Sí (SSM)	No
Capacidades SSC/SSM					
Compatibilidad SSC/SSM	Futura, SSC	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	CSC-SSM, AIP-SSM, 4GE-SSM	No
Prevención de intrusiones	No disponible	Sí (con AIP-SSM)	Sí (con AIP-SSM)	Sí (con AIP-SSM)	No
Capacidad de procesamiento (Mbps) de mitigación concurrente contra amenazas (firewall + servicios IPS)	No disponible	150 (con AIP-SSM-10) 300 (con AIP-SSM-20)	225 (con AIP-SSM-10) 375 (con AIP-SSM-20)	450 (con AIP-SSM-20)	No disponible
Anti-X (antivirus, antispyware, bloqueo de archivos, antispam, antiphishing y filtrado de URL)	No disponible	Sí (con CSC-SSM)	Sí (con CSC-SSM)	Sí (con CSC-SSM)	No disponible
Cantidad máxima de usuarios por antivirus, antispyware, bloqueo de archivos (sólo CSC-SSM)	No disponible	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	500 (CSC-SSM-10) 1000 (CSC-SSM-20)	No disponible
Características de licencia CSC SSM Plus	No disponible	Antispam, antiphishing, filtrado de URL	Antispam, antiphishing, filtrado de URL	Antispam, antiphishing, filtrado de URL	No disponible
Características					
Seguridad en la capa de aplicaciones	Sí	Sí	Sí	Sí	Sí
Funciones de firewall transparente de capa 2	Sí	Sí	Sí	Sí	Sí
Contextos de seguridad (incluidos/máximos)2	0/0	0/0 / 2/5	2/20	2/50	2/50
Inspección GTP/GPRS2	No disponible	No disponible	Sí	Sí	Sí
Compatibilidad con alta disponibilidad3	No compatible / A/S sin información de estado	No compatible / A/A y A/S	A/A y A/S	A/A y A/S	A/A y A/S
Agrupación de VPN y equilibrio de carga	No disponible	No disponible	Sí	Sí	Sí

CONOCER LAS OPCIONES DE SEGURIDAD.

Los servidores actuales son más seguros que nunca, pero las sólidas configuraciones de seguridad que se encuentran en los productos de servidor de Windows sólo son eficaces si se utilizan del modo adecuado y se supervisan estrechamente. (Mieres, 2010, pag 5-6).

PROPUESTA 4: AMP (Protección avanzado frente a Malware)

AMP aprovecha plenamente las vastas redes de inteligencia de seguridad en la nube proporcionadas por Cisco Collective Security Intelligence, Talos Security Intelligence and Research Group y AMP Threat Grid para ofrecer protección avanzada. AMP también se integra con la tecnología de análisis de malware e inteligencia de amenazas Cisco AMP Thread Grid para mejorar las capacidades y agregar y correlacionar datos a fin de identificar ciberamenazas avanzadas.
La solución AMP puede habilitar la detección, el bloqueo, el análisis continuo y las alertas retrospectivas de malware con:

- Reputación de archivos: analice archivos en línea y bloquee o aplique políticas
- Zona de sandboxing de archivos: analice archivos desconocidos para comprender su verdadero comportamiento
- Retrospección de archivos: continúe analizando archivos para detectar cambios en los niveles de amenaza

Los clientes de AMP obtienen:

- Seguridad avanzada para amenazas avanzadas: derrote amenazas conocidas y desconocidas
- Protección durante todo el ciclo de ataque: antes, durante y después de un ataque
- Visibilidad y control excepcionales: vea más detalles y fije políticas granulares
- Flexibilidad y capacidad de elección: implemente AMP cuándo, dónde y cómo lo necesite
- Servicios gestionados: amplíe su personal con expertos y análisis predictivo de Cisco

Cisco AMP ofrece protección en el más amplio número vectores de ataque y se puede implementar:

- Como una solución basada en la red, integrada en el firewall Cisco ASA dedicado y en appliances de red Cisco FirePOWER
- Como una solución de terminal para equipos PC, Mac, sistemas Linux, dispositivos móviles y entornos virtuales
- Como un appliance virtual de nube privada in-situ con aislamiento físico diseñado para entornos con estrictos requisitos de privacidad
- Como una función integrada en Cisco Cloud Web Security o en los dispositivos Cisco Email y Web Security Appliances
- Como una solución autónoma de análisis de malware y de inteligencia de amenazas usando AMP Threat Grid

Actualmente ofrece la cartera más amplia de soluciones integradas de protección frente a malware avanzado (AMP) de la industria. Los clientes disfrutan de una visibilidad y un control continuos para derrotar al malware en la red extendida y durante todo el ciclo de ataque: antes, durante y después de un ataque.

Antes: Obtiene la mejor inteligencia de amenazas global para fortalecer las defensas de su red.
Durante: Usa esa inteligencia, firmas de archivo conocidas y tecnología de análisis dinámico de archivos para bloquear malware conocido, tipos de archivos que infrinjan las políticas y comunicaciones que intenten infiltrase en su organización.
Después: Analiza continuamente los archivos y el tráfico de la red en busca de amenazas que puedan eludir sus primeras líneas de defensa, logre una profunda visibilidad de la actividad y el comportamiento de la amenaza, y luego responda y contenga rápidamente un ataque activo con unos pocos clics. (CISCO, 2015)

PROPUESTA 5: IPS (SISTEMA DE PREVENCION DE INTRUSOS)

Los sistemas de prevención de intrusiones detectan y bloquean cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red, sin impacto alguno sobre su rendimiento.
El servicio funciona de manera transparente para el usuario, por lo que no requiere ninguna reconfiguración de la red existente a la que se conecta. El servicio de Prevención de intrusiones en la red de Interoute ofrece una compleja capa de protección para las empresas. Utilizando técnicas de reconocimiento de protocolos, identificación y análisis de tráfico, es capaz de detectar, identificar, alertar y proteger a su organización frente a amenazas como (INTEROUTE, 2017)

- Gusanos
- Spyware
- Peer to peer (P2P)
- Ataques de denegación de servicio individuales (DoS) o distribuidos (DDoS)
- Botnets
- Ataques dirigidos contra aplicaciones web
- Salida de datos protegidos o delicados fuera de la red
- Ejecución no autorizada de código JavaScript entre distintos dominios (cross-site scripting)
- Inyección de código SQL
- Desbordamiento de búferes
- Navegación por directorios de una web

Se realizó estos 4 ítems en la guía de mejores prácticas de seguridad al servidor E-learning de la ESPOCH debido a que el departamento de desarrollo de las DTIC, y las políticas de seguridad que ellos tienen, solo permitieron estos cuatro aspectos, porque es una información delicada y no debe estar expuesto a terceros y menos en la red, se podría poner en riesgo el funcionamiento del servidor E-learning de la ESPOCH.