ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ANÁLISIS DE VULNERABILIDADES INSIDERS PARA REDES DE CAMPUS ACADÉMICAS APLICANDO LA METODOLOGÍA OSSTMM. CASO PRÁCTICO RED DEL EDIFICIO DE LA FIE-ESPOCH"

Trabajo de titulación

Tipo: Proyecto de investigación

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: BYRON MAURICIO BARRAGÁN GONZÁLEZ

DIRECTOR: ING. MARCO VINICIO RAMOS VALENCIA

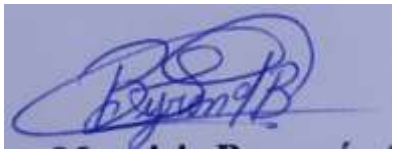
Riobamba – Ecuador

2020

Yo, Byron Mauricio Barragán González, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor (a) asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 04 de marzo de 2020.



Byron Mauricio Barragán González

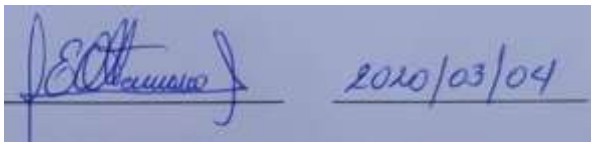
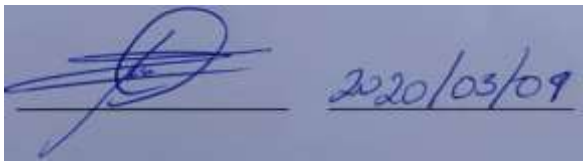
025000665-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

El Tribunal del trabajo de titulación certifica que: El trabajo de titulación: Tipo: Proyecto Investigación, **"ANÁLISIS DE VULNERABILIADES INSIDERS PARA REDES DE CAMPUS ACADÉMICAS APLICANDO LA METODOLOGÍA OSSTMM. CASO PRÁCTICO RED DEL EDIFCIO FIE-ESPOCH"**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMAS	**FECHA**
Ing. Edwin Vinicio Altamirano Santillán **PRESIDENTE DEL TRIBUNAL**		2020/03/04
Ing. Marco Vinicio Ramos Valencia **DIRECTOR DEL TRABAJO DE TITULACIÓN**		2020/03/09
Ing. Alberto Leopoldo Arellano Aucancela **MIEMBRO DE TRIBUNAL**		2020/03/09

DEDICATORIA

Dedico el presente trabajo de titulación y todos mis futuros trabajos a mis padres, quienes han sacrificado mucho por mí y mis hermanos a lo largo de todos estos años de estudios.

Byron

AGRADECIMIENTO

Agradezco a mis padres quienes año tras año me han ayudado e inspirado para seguir adelante y pese a los contratiempos siempre han estado con su cariño y paciencia presentes para mí.

Agradezco a mis amigos quienes en un momento en el que me sentía solo y me había dado por vencido me ayudaron a levantarme y me alentaron a continuar.

Agradezco al grupo de investigación SEGINTE y en especial la ingeniera Ruth Barba quien me ayudo desde el inicio en el desarrollo de este trabajo.

Byron

TABLA DE CONTENIDO

CAPÍTULO II

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

INDICE DE ANEXOS

RESUMEN

El objetivo del presente trabajo de titulación fue analizar las vulnerabilidades insiders relacionadas a la capa de trasporte en la red del edificio de la Facultad de Informática y Electrónica (FIE) de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Para ello se realizó un análisis del tráfico de la red del edificio de la FIE-ESPOCH con la herramienta Nids-Snort con la que determinó las amenazas y ataques a los que está expuesta la red. Se aplicó una adaptación del Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM) para determinar el estado de la seguridad en los canales humano y red de datos del edificio y, además, se determinó las vulnerabilidades insiders existentes realizando un escaneo de vulnerabilidades con la herramienta Nexpose. Posteriormente se realizó la explotación de las vulnerabilidades y amenazas previamente seleccionadas basándose en las más comunes y riesgosas, esto se realizó en un ambiente virtual desarrollado en el simulador GNS3. Finalmente se propuso una guía de solución para las vulnerabilidades y amenazas explotadas, indicando opciones de solución para diferentes sistemas operativos con capturas y pasos a seguir para una correcta aplicación en el sistema o equipo afectado. Como resultado se obtiene que el estado de la seguridad en los canales es bajo debido a la presencia de un gran número de vulnerabilidades en los equipos haciendo falta más controles y limitaciones. Como recomendación se indica que se debe mantener actualizado los equipos para reducir la cantidad de amenazas a la que se encuentran expuestos.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES DE CAMPUS ACADÉMICO>, <VULNERABILIDADES INSIDERS>, <OSSTMM (MANUAL DE LA METODOLOGIA ABIERTA DE COMPROBACION DE LA SEGURIDAD)>, <NIDS-SNORT (SOFTWARE)>, <NEXPOSE (SOFTWARE)>, <ANÁLISIS DE VULNERABILIDADES>, <ANÁLISIS DE TRÁFICO>.

SUMMARY

The objective of this degree work was to analyze the insider vulnerabilities related to the transport layer in the building network of the Informatics and Electronics Faculty (FIE) from the Escuela Superior Politécnica de Chimborazo (ESPOCH). To do so, an analysis of the traffic of the FIE-ESPOCH building network was carried out with the Nids-Snort tool with which the threats and attacks to which the network is exposed were determined. An adaptation of the Open Security Verification Methodology Manual (OSSTMM) was applied to determine the state of security in the building's human channels and data network and, in addition, the existing insider vulnerabilities were determined by performing a vulnerability scan with the Nexpose tool. Subsequently, the exploitation of previously selected vulnerabilities and threats was carried out based on the most common and risky ones, this was done in a virtual environment developed in the GNS3 simulator. Finally, a solution guide for exploited vulnerabilities and threats was proposed, indicating solution options for different operating systems with captures and steps to follow for a correct application on the affected system or equipment. As a result, it was obtained that the security status in the channels is low due to the presence of a large number of vulnerabilities in the equipment, requiring more controls and limitations. As a recommendation, it is advised that equipment should be kept updated to reduce the number of threats to which they are exposed.

Keywords: < TECHNOLOGY AND SCIENCES ENGINEERING>, <ACADEMIC CAMPUS NETWORKS>, <INSIDER VULNERABILITIES>, <OSSTMM (OPEN SAFETY CHECK METHODOLOGY MANUAL)>, <NIDS-SNORT (SOFTWARE)>, <NEXPOSE (SOFTWARE)>, <VULNERABILITY ANALYSIS>, <TRAFFIC ANALYSIS>

INTRODUCCIÓN

En la época actual la información, independientemente de su tipo es de vital importancia para que una entidad u organización pueda trabajar de manera correcta y eficiente, es por esto que en los últimos años se la considera como uno de los activos más valiosos que puede poseer una organización. Debido a su importancia, una correcta gestión de esta garantiza elevar la competitividad de la organización para así obtener beneficios a largo y corto plazo.

Pero no todo se maneja de manera transparente ya que existen personas que muchas de las veces están dentro de la organización (insider) sabiendo cómo funciona el sistema y que su único objetivo es poder acceder a esta información valiosa. Para esto dichas personas se valen de ataques informáticos comprometiendo así la seguridad de los sistemas que maneja la organización. Como resultado estas personas obtienen permisos de acceso y se aprovechan de las vulnerabilidades de dichos sistemas y así tener éxito en la acción maliciosa. Una vez que se encuentran las vulnerabilidades de los sistemas de una organización, no solo se puede realizar el robo de la información, sino que se puede realizar diferentes acciones como daños al sistema o incluso modificación de información.

Para una organización como lo es una universidad el tener conocimiento sobre los incidentes que se pueden causar aprovechando las vulnerabilidades de sus sistemas es muy importante ya que gracias a esto se puede determinar e implementar medidas de corrección para la seguridad de sus sistemas, estas medidas se agrupan y se forman políticas de seguridad de la información las cuales se deben aplicar en la organización. Sin embargo, según un estudio realizado por CEDIA (Padilla Verdugo *et al.*, 2017, p.71) revela que, de un conjunto de universidades encuestadas, únicamente 3 cuentan con políticas de seguridad formalizadas representando el 8%, 22 de manera parcial representando el 60%, mientras que 12 no tiene una política de seguridad representando el 32%. cabe indicar que en este estudio se encuestaron 36 universidades ecuatorianas entre las cuales se encontraba la Escuela Superior Politécnica de Chimborazo (ESPOCH). Este estudio revela también la situación en la que se encuentran las instituciones educativas de nivel superior en Ecuador por lo que encontrar las vulnerabilidades de los sistemas es importante para determinar políticas de seguridad adecuadas o guías de solución para que estas no sean explotadas mediante ataques informáticos.

Esta investigación está repartida en 3 capítulos, el primero de ellos se trata acerca de la información teórica abarcada en el desarrollo de la investigación, el segundo capítulo es el

procedimiento para determinar y analizar las vulnerabilidades de la red y finalmente en el capítulo 3 se presentan los resultados.

Antecedentes

Gracias al desarrollo de las redes de datos a lo largo del tiempo, su uso ha incrementado, esto debido a las facilidades que presenta la utilización de estas redes como son bajo costo de instalación, su fácil configuración y la capacidad de diferentes dispositivos que pueden interconectarse entre sí vía inalámbrica o cableada como lo dice Andrés Serrano en su tesis de ingeniería. (Serrano Flores, 2011, p.1).

Desde la creación de las redes institucionales han existido vulnerabilidades en la seguridad, estas vulnerabilidades se pueden presentar tanto en el exterior como en el interior (insider) de una red institucional, una vulnerabilidad es la debilidad de un sistema por la cual los posibles atacantes pueden realizar sus acciones maliciosas. Las vulnerabilidades que han sido descubiertas son expuestas y posteriormente reparadas o parcheadas por lo general con la implementación de protocolos de seguridad o actualización de sus sistemas. Es muy común que una institución realice un análisis de vulnerabilidades para determinar los riesgos o amenazas que tiene su red valiéndose de métodos y técnicas para realizar los mismos, un ejemplo es el caso de Jairo Manuel Palacios Domínguez que en 2015 desarrolló un trabajo de grado en la Universidad de Sevilla en específico en la Escuela Técnica Superior de Ingeniería Telemática, denominado "Análisis de Vulnerabilidades de una red corporativa mediante herramientas de descubrimientos activas" utilizando para ello herramientas, tales como NMap, OpenVAS, vFeed y Xprobe2. (Palacios, 2015), en este trabajo se exploró vulnerabilidades de la red en puertos e incluso en gestión de nombres y contraseñas de usuario obteniéndose como resultado una mejora de la seguridad de la red de la institución.

En el ámbito nacional en la actualidad las instituciones ya sea públicas o privadas en su mayoría se manejan con redes informáticas para cumplir con su trabajo, de igual manera estas instituciones no están libres de recibir un ataque dentro de su misma institución por ejemplo si el Servicio de Rentas Internas sufriera un ataque informático mucha información sensible seria revelada en el peor de los casos. Una vez más realizar análisis de vulnerabilidades ayuda a mejorar la seguridad de una red. En Ecuador se han realizado trabajos acerca de análisis de vulnerabilidades en una red institucional por ejemplo en 2010 la señorita Angélica Espinoza realizó un trabajo de fin de carrera en la Universidad Técnica Particular de Loja denominado "Análisis de vulnerabilidades de la red LAN de la UTPL" en el cual el principal objetivo fue realizar un análisis de vulnerabilidades enfocado al usuario final, es decir determinar cuáles son

los riesgos y amenazas a las que están expuestos y el impacto en el caso de que estos llegaran a ocurrir. Para la realización de este trabajo se tomó en cuenta un test de intrusión interno en un entorno de laboratorio de pruebas con la guía de un conjunto de procesos híbridos seleccionados de "Open Source Security Testing Methodology Manual" OSSTMM y de "Operationally Critical Threat, Asset, and Vulnerability Evaluation" OCTAVE (Espinosa, 2010, p.XIII), como resultado se encontró que la información sensible como contraseñas y documentos no se encuentran cifrados por lo que un atacante podría estar expuesto a esta información además se generó un plan de acción con estrategias de protección preventivas, correctivas y detectivas para mitigar el impacto de los riesgos.

En el ámbito local, en Riobamba las instituciones públicas y privadas cuentan con redes informáticas las cuales son vulnerables tanto a ataques del exterior como del interior, en la Escuela Superior Politécnica de Chimborazo (ESPOCH) se han desarrollado trabajos de análisis de vulnerabilidades, pero solo para casos específicos, y no en forma general. Por ejemplo, en 2015 Cristhian Vallejo desarrollo un análisis de vulnerabilidades en una red estándar y que incidencia tenía en los dispositivos móviles. Otro ejemplo más reciente y más parecido al tema propuesto es el desarrollado en 2017 por Aida Alvarado y Richard Cabrera denominado Análisis de vulnerabilidades del servidor e-learning de la ESPOCH para la implementación de mejores prácticas de seguridad-acceso. (Alvarado Tapia & Montesdeoca Cabrera, 2017), en el cual utilizando una metodología y simulando ataques lograron determinar vulnerabilidades en ciertos puertos abiertos de la aplicación de e-learning y como solución de dichas vulnerabilidades encontradas implementaron un firewall.

Formulación del problema

¿Cómo analizar vulnerabilidades insiders para la red de campus académica del edificio de la FIE-ESPOCH, aplicando la metodología OSSTMM?

Sistematización del problema

¿Cuál es la gama de vulnerabilidades insider más comunes que sufre una red de campus académica a nivel de la capa de transporte del modelo OSI, aplicado al caso práctico?

¿Es posible determinar las vulnerabilidades insiders a través del uso de la metodología OSSTMM y herramientas de testeo Open Source en la red de campus académica del edificio de la FIE-ESPOCH?

¿Es necesario explotar las vulnerabilidades identificadas para el análisis de posibles daños efectuados?

¿Qué medidas de prevención o corrección son las más adecuadas para aplicar según las vulnerabilidades explotadas?

Justificación Teórica

En conjunto con las redes, las vulnerabilidades insiders han evolucionado partiendo desde una filtración no intencional de información importante por parte de empleados los cuales no tienen conciencia acerca de las consecuencias que puede causar el mal manejo de información sensible, pasando por una mala gestión de contraseñas y nombres de usuario, vulnerabilidades en sistemas operativos o equipos físicos que utilice la institución, hasta un ataque informático realizado por un empleado malicioso que conociendo las vulnerabilidades de la red realiza un ataque específico para explotar esa vulnerabilidad, este usuario malicioso puede ser un experto en ataques informáticos o no necesariamente. Un ataque interno en sí mismo es un término que abarca muchos tipos de acciones maliciosas, desde un robo de datos completamente intencional o fraude cometido con fines de lucro, hasta el sabotaje, espionaje industrial, incluso a errores realizados intencionalmente o no intencionalmente, teniendo estas acciones en común el hecho de que todos ellos están comprometidos por empleados con acceso a la red de la institución. A menudo dichos empleados son gerentes, operadores de bases de datos, programadores o especialistas, que trabajan con datos sensibles, infraestructura o configuraciones crítica de sistemas como lo menciona Rubén Ramiro, Profesional en Tecnologías de la seguridad y ciberseguridad en Telefónica en su blog de ciberseguridad. (Ruben Ramiro, 2017) . Para el caso de una red de una institución educativa como lo es la ESPOCH, puede ser los mismos estudiantes, la planta docente o el sector administrativo que tienen acceso a una cuenta y por ende a la red de campus, cualquier persona que tenga acceso a la red puede ser un atacante potencial. Para el caso práctico se considera la evolución y crecimiento de la red de la ESPOCH y los estudiantes quienes cuentan con acceso a la red de campus y pueden causar daños o acceder a ciertos lugares y robar información, todo esto se puede hacer con la ayuda de internet ya que se puede encontrar mucha información de cómo encontrar vulnerabilidades en una red y que ataques

hacer, se puede encontrar incluso tutoriales con los cuales se pretende el éxito en la acción maliciosa.

En el caso práctico propuesto el análisis será enfocado a encontrar vulnerabilidades insiders, es decir las vulnerabilidades que un usuario que ya está dentro de la red puede encontrar y explotar mediante un ataque informático y cuáles son los posibles daños que puede hacer este usuario malicioso, para esto se tendrá en cuenta versiones del Manual de la Metodología de Testeo de Seguridad OSSTMM por sus siglas en inglés para la realización del análisis, así como también la utilización de herramientas de testeo open source para identificar las vulnerabilidades. Cabe indicar que las vulnerabilidades que se pretende encontrar son las referentes a la capa de transporte del modelo OSI (capa 4). En esta capa lo más vulnerable es la autenticación, la integridad y la confidencialidad de los datos. Los ataques a la capa de transporte van asociados al funcionamiento de los protocolos TCP y UDP. Algunas de las vulnerabilidades más graves es la posibilidad de interceptación de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos también se puede mencionar escaneo de puertos, inundaciones UDP, DoS por sobrecarga de conexiones como algunos de los ataques a esta capa, para el caso práctico propuesto se tendrá en cuenta las siguientes vulnerabilidades y ataques: Fingerprinting, Escaneo de Puertos, UDP Flood, TCP SYN Flood, Connection Flood, Tribe Flood Network y Tfn2k, Land, Sesión Hijaking, TCP Initial Sequence Numbers, Tiny Fragment Attack, Winnuke, Teardrop (Mejia, Ramirez & Rivera, 2012, pp.112-120) como vulnerabilidades más comunes y que puede presentar una red de campus académica como la red del edificio de la FIE-ESPOCH.

Justificación aplicativa

En una primera instancia se tiene a todos los usuarios que desean conectarse a la red de campus, en este caso pueden ser estudiantes, docentes o sector administrativo, y dentro de este grupo también puede estar presente un usuario malicioso (insider) el cual busca hacer un ataque a su conveniencia. Para que estos usuarios puedan acceder a la red deben ser autenticados, esta tarea lo realiza un servidor de autenticación mediante un nombre de usuario y una contraseña que por lo general es el número de cedula de cada usuario. Una vez que los usuarios hayan sido autenticados tienen acceso al servicio de internet y por ende acceso a red, esto en el caso de la red inalámbrica por otro lado se puede conectar por cable y tener acceso a la red. Una vez dentro el usuario malicioso puede realizar ataques según las vulnerabilidades que encuentre en la red de campus. Es aquí en donde entra este trabajo ya que lo que se busca es hacer un análisis de vulnerabilidades insiders en la red del edificio de la FIE-ESPOCH esto debido a la facilidad

de acceso a la infraestructura y además que este trabajo de titulación estará alineado al proyecto del grupo de investigación SEGINTE, denominado “Propuesta de Solución SDN - Sistema de Aprendizaje para identificación y clasificación de amenazas internas que mejoren el control y la seguridad en intranets académicas.” En el edificio de la FIE-ESPOCH se determinará cuáles son los riesgos y vulnerabilidades a la que está expuesta la red y además de proponer una posible guía de solución a dichos riesgos.

Objetivos

Objetivo General

Analizar las vulnerabilidades insiders de la red de campus académica del edificio de la FIE-ESPOCH, aplicando la metodología OSSTMM.

Objetivos Específicos

- Investigar las vulnerabilidades insiders que puede presentar una red de campus académica a nivel de la capa de transporte.
- Aplicar la metodología OSSTMM y herramientas de testeo Open Source para el análisis de vulnerabilidades insider en el edificio de la FIE-ESPOCH.
- Explotar las vulnerabilidades insiders encontradas en la red de campus académica del edificio de la FIE-ESPOCH.
- Proponer una guía de solución a las vulnerabilidades insiders explotadas.

CAPÍTULO I

1. MARCO TEÓRICO

1.1. Redes

Se define a una red como un medio de comunicación al cual acceden las personas, usuarios o grupos de usuarios con el fin de compartir información, algún servicio o recursos. Un ejemplo son las redes telefónicas siendo estas un tipo de red para la comunicación entre dos usuarios.

A lo largo de los años las redes han evolucionado y han sido de gran ayuda para el desarrollo de una organización independientemente de su función, por ejemplo, en una institución educativa como una universidad el uso de una red informática ayuda a las actividades de consulta de los estudiantes, esto gracias al acceso a internet.

Las nuevas tecnologías han permitido a las redes informáticas transportar voz, datos y video asegurando así una convergencia utilizando los mismos medios. Las redes están formadas por equipos llamados nodos, estos nodos utilizan varios medios para poder comunicarse entre sí, estos pueden ser protocolos o lenguajes comprensibles para todos los nodos que pertenecen a una red. Una forma de categorizar a una red es en base a la amplitud y la aplicación que se le dará. (Dordoigne, 2015, p. 36)

Entre los tipos de redes se encuentra las redes de área de campus, este tipo de redes se manifiesta en campus de universidades, pero también se considera a las redes que superen 1000 metros cuadrados, este tipo de red es un conjunto de redes de área local que están interconectadas entre sí para poder compartir información de manera rápida y además de asegurar el acceso a internet en todo el campus para las personas que se conecten a la red.

1.1.1. Redes de área de campus académicas

Este tipo de redes son más utilizadas en el campo educativo, ya sea para universidades, colegios o escuelas. Para el caso de una universidad es de amplia utilidad, por ejemplo, las redes de área de cada una de las facultades de la universidad se interconectan entre sí para compartir un recurso como lo es la información o para acceder a internet, esto último de gran ayuda para los estudiantes en tareas de consulta, así como también para lectura de libros en línea. Todo esto con el único objetivo de mejorar su rendimiento académico. Además, cabe indicar que el tráfico que circula por este tipo de redes es información relacionada con algún trabajo de investigación o desarrollo que realiza la universidad.

1.1.2. Importancia de las redes de área de campus académicas

En la actualidad la mayoría de las universidades en Ecuador posee una red de campus académica esto debido a la importancia que estas tienen para el desarrollo de las actividades académicas. A continuación, se mencionarán aspectos del porqué de la importancia de las redes de área de campus académicas:

- Durante el desarrollo de un proyecto colaborativo entre carreras, acceder a fuentes de consulta y compartir información es de vital necesidad.

- La información que se comparte pasa por canales de banda ancha, con una amplia capacidad que determina así la velocidad a la que se transmite.

- La utilización de este tipo de redes permite a los usuarios finales una gran flexibilidad para desarrollar sus trabajos e investigaciones.

- Permite el desarrollo de nuevas tecnologías, en base a la necesidad y desarrollo de los trabajos realizados.

- Al compartir información permite que proyectos realizados en otros países se repliquen y mejoren con más facilidad o viceversa.

1.1.3. Edificio de la FIE-ESPOCH

El edifico de la FIE-ESPOCH es en el que se realizará el análisis de vulnerabilidades insiders. Actualmente este edificio cuenta con tres pisos, laboratorios de cómputo, aulas de clase, sala de profesores, un auditorio, sala de reuniones, oficinas de administración, un ascensor, baños y un cuarto de servidores donde se ubican los equipos de red. Este edificio cuenta con acceso a internet de manera inalámbrica permitiendo conectar dispositivos móviles o mediante cable en sus laboratorios y oficinas.

1.2. Capa de transporte del modelo OSI

La capa de transporte del modelo OSI trabaja con dos protocolos ampliamente diferenciados, sin embargo, estos se complementan entre sí, estos son: TCP y UDP. TCP está orientado a la conexión mientras que el protocolo UPD es un protocolo sin conexión esto debido que el protocolo UDP envía paquetes entre todas las aplicaciones, dejando que en las capas superiores

del modelo OSI reconstruyan los paquetes enviados según sea la necesidad. Por otro lado, el protocolo TCP agrega confiabilidad en todas las retransmisiones, además controla la congestión y el flujo de los datos.

1.2.1. Protocolo UDP

UDP proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión. (Tanenbaum & Wetherall, 2012, p. 464). Este protocolo tiene un Header o encabezado de 8 bytes de tamaño y un espacio para la carga útil como se puede observar en la figura 1-1.

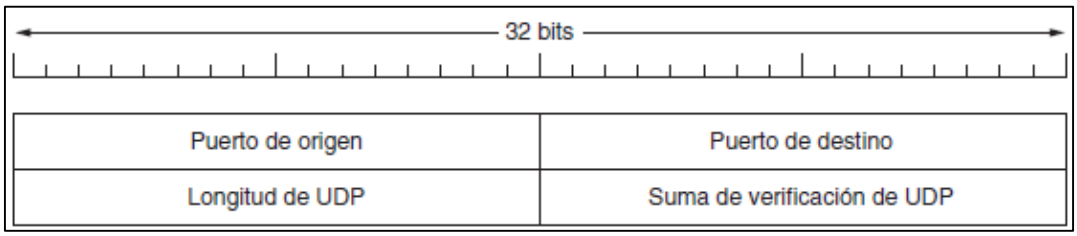


Figura 1-1: Datagrama UDP
Fuente: (Tanenbaum & Wetherall, 2012, p. 465)

En el apartado de longitud de UDP indica la longitud en octetos del datagrama UDP, incluyendo el Header, la longitud máxima de un datagrama UDP es de 65.505 bytes y el valor mínimo es 8 bytes como ya se mencionó. En la figura 3-1 se observa 4 campos, sin embargo, 2 de estos son opcionales; estos son el puerto de origen y la suma de verificación de UDP. UDP no tiene un servidor de estado por lo que en las sesiones no se solicita una respuesta por parte del origen, en estos casos el campo de puerto de origen es puesto a 0. La suma de verificación de UDP también puede ser puesto a 0.

Como ya se mencionó anteriormente el protocolo UDP no se encarga del control de flujo, control de congestión de paquetes o retransmisión cuando se recibe un paquete con errores. Sin embargo, este protocolo es utilizado en la actualidad para aplicaciones a tiempo real como videostreaming, videoconferencias o televisión a tiempo real esto debido a que es más liviano en su encabezado que su contraparte TCP. Un ejemplo de aplicación que utiliza el protocolo UDP es el servicio DNS. En términos más acordes UDP se encarga de construir una interfaz para el uso del protocolo IP, esta interfaz usa puertos para demultiplexar varios procesos.

1.2.2. Protocolo TCP

La entidad TCP emisora y receptora intercambian datos en forma de segmentos. Un segmento TCP consiste en un encabezado fijo de 20 bytes seguido de cero o más bytes de datos. El software de TCP decide qué tan grandes deben ser los segmentos. Hay dos límites que restringen el tamaño de segmento. Primero, cada segmento, incluido el encabezado TCP, debe caber en la carga útil de 65 515 bytes del IP. Segundo, cada enlace tiene una MTU (Unidad Máxima de Transferencia). Cada segmento debe caber en la MTU en el emisor y el receptor, de modo que se pueda enviar y recibir en un solo paquete sin fragmentar. En la práctica, la MTU es por lo general de 1500 bytes (el tamaño de la carga útil en Ethernet) y, por tanto, define el límite superior en el tamaño de segmento. (Tanenbaum & Wetherall, 2012, p. 477)

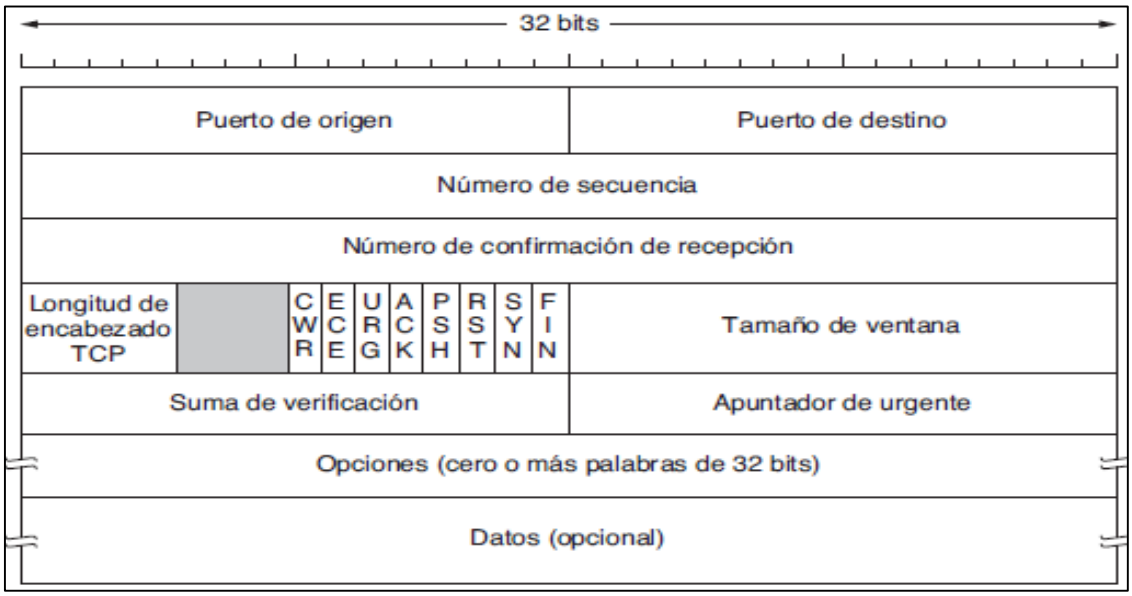


Figura 2-1: Encabezado del protocolo TCP
Fuente: (Tanenbaum & Wetherall, 2012, p. 478)

En la figura 2-1 se muestra el encabezado TCP, cada segmento comienza con un encabezado de formato fijo de 20 bytes. El encabezado fijo puede ir seguido de encabezado de opciones. Después de las opciones, si las hay, pueden continuar hasta 65495 bytes de datos. (Tanenbaum & Wetherall, 2012, pág. 478).

En TCP las conexiones se establecen mediante el acuerdo de tres vías Para establecer una conexión, uno de los lados (digamos que el servidor) espera en forma pasiva una conexión entrante mediante la ejecución de las primitivas LISTEN y ACCEPT en ese orden, ya sea que se especifique un origen determinado o a nadie en particular. El otro lado (digamos que el cliente) ejecuta una primitiva CONNECT en la que especifica la dirección y el puerto con el que se desea conectar, el tamaño máximo de segmento TCP que está dispuesto a aceptar y de manera

opcional algunos datos de usuario (por ejemplo, una contraseña). La primitiva CONNECT envía un segmento TCP con el bit SYN encendido y el bit ACK apagado, y espera una respuesta. Cuando este segmento llega al destino, la entidad TCP de ahí revisa si hay un proceso que haya ejecutado una primitiva LISTEN en el puerto que se indica en el campo Puerto de destino. Si no lo hay, envía una respuesta con el bit RST encendido para rechazar la conexión. Si algún proceso está escuchando en el puerto, ese proceso recibe el segmento TCP entrante y puede entonces aceptar o rechazar la conexión. Si la acepta, se devuelve un segmento de confirmación de recepción. En la figura 3-1 se puede observar este proceso. (Tanenbaum & Wetherall, 2012, p. 481)

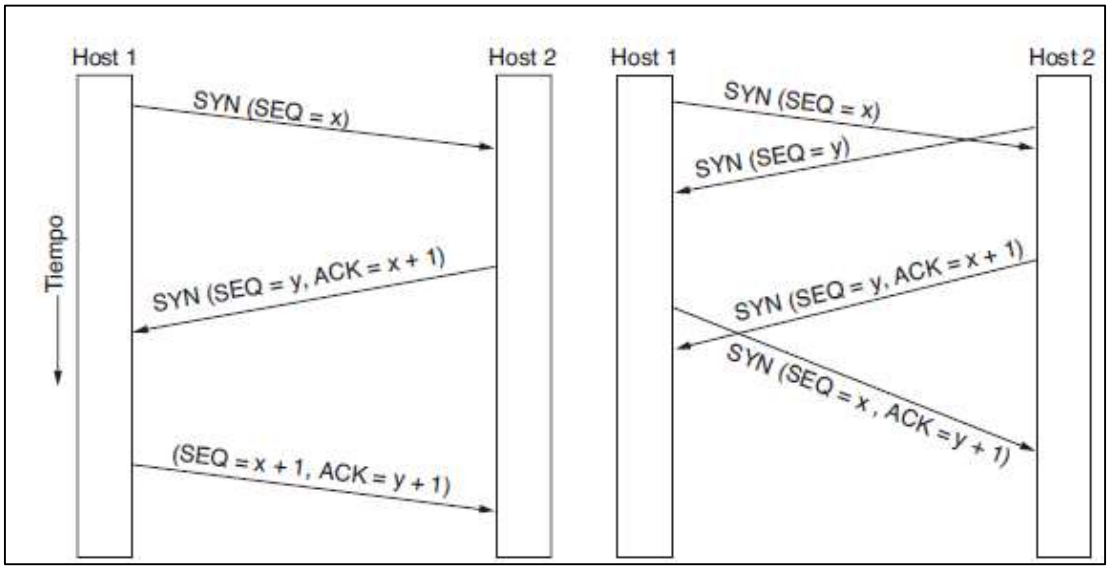


Figura 3-1: Establecimiento de una conexión TCP normal (i) y simultanea (d)
Fuente: (Tanenbaum & Wetherall, 2012, pág. 481)

1.3. Seguridad de redes informáticas

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

1.3.1. Criterios e importancia de la seguridad de redes informáticas

Como se ha mencionado en apartados anteriores en la actualidad las mayorías de las organizaciones utilizan las redes informáticas para el desarrollo de su trabajo y también para

tener acceso a internet y es precisamente por esto último que todos los usuarios pueden ser víctimas de atacantes informáticos. Debido a esto la seguridad de los activos importantes como lo es la información es de vital importancia ya que puede ser robada y causar problemas a la organización incumpliendo así los criterios de la seguridad informática las cuales se mencionan a continuación en la tabla 2-1

Tabla 1-1: Criterios de la seguridad informática

Criterios de la seguridad	Definición
Confidencialidad	Hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados
Integridad de los datos	La integridad de datos es la protección de los datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades no autorizadas
Disponibilidad	Significa tener acceso a la información cuando se requiere. Por ejemplo, un fallo de un disco o un ataque de denegación de servicio pueden causar una violación de la disponibilidad.
Autenticación	El servicio de autenticación se encarga de asegurar la identidad de las entidades que participan en la comunicación. Es decir, el servicio de autenticación evita que un usuario o entidad pueda suplantar la identidad de otro.
Control de acceso	Es la protección de los servicios o recursos de información para evitar puedan ser accesibles por parte de entidades no autorizadas
No repudio	Es el servicio de seguridad que utiliza estas evidencias para proporcionar protección contra la negación de una de las entidades de haber participado en la totalidad o parte de una comunicación.

Fuente: (Soriano, 2014, pp. 31-37)
Realizado por: Byron Barragán, 2020

1.3.2. Seguridad personal

La seguridad en el trabajo comienza en los niveles más básicos, los trabajadores. Cuando se contrata un nuevo empleado, las referencias pueden ser requeridas y verificadas. Es también importante verificar el pasado de los empleados. Después de que la decisión de contratar un empleado es hecha, este debe de ser entrenado e informado de las medidas de seguridad que serán tomadas, incluyendo triturado de toda la información, frecuentemente cambiando y eligiendo la contraseña apropiada y la encriptación de email. (Perpiñan, 2011, p. 9)

1.3.3. Políticas de seguridad

La protección de los sistemas recae en la realización de un análisis de amenazas a las que están expuestos los sistemas. En estos análisis se trata de determinar las pérdidas que podrían ocasionar y sobre todo la probabilidad de que las amenazas se conviertan en ataques. Una vez que el análisis está completa, en base al estudio se proponen políticas de seguridad en las que se detalla reglas, procedimientos y responsabilidades para mitigar las amenazas o reducir sus efectos.(Cifuentes & Narvaez, 2004, p. 5)

1.3.4. Mecanismos de la seguridad informática

Los mecanismos de seguridad ayudan a la implementación de políticas de seguridad. Estos mecanismos de seguridad están compuestos por tres grupos y son:

- **Prevención:** Mecanismos cuyo fin es aumentar la seguridad de un sistema mientras se encuentre en funcionamiento.

- **Detección:** Mecanismos utilizados para la detección de intentos o violaciones de seguridad.

- **Recuperación:** Mecanismos definidos para la recuperación en caso de ser víctimas de un ataque informático. (Cifuentes & Narvaez, 2004, p. 5-6)

1.4. Vulnerabilidades informáticas

Los equipos tanto a nivel de software como hardware no son perfectos esto se lo puede ver en las diferentes versiones que cada cierto tiempo se liberan para así arreglar las vulnerabilidades encontradas y que se pueden explotar con fines maliciosos. Los atacantes informáticos se valen de estas vulnerabilidades para acceder a la red de la organización, pero ¿qué es una vulnerabilidad? A continuación, se dará una definición**.**

1.4.1. Definición de vulnerabilidad

Probabilidad que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los atacantes, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de vulnerabilidades hay que tener en cuenta la vulnerabilidad de cada activo. (Aguilera López, 2010, p.14).

Se entiende como activo a lo más importante de una organización, como se ha mencionado en apartados anteriores un activo es la información confidencial que una organización o empresa maneja. Pero un activo no solo es la información, en si puede ser los equipos de red instalados en la empresa lo cuales también son vulnerables. Los activos son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Se puede observar tipos en la tabla 2-1.

Tabla 2-1: Tipos de activos en una organización

Activo	**Definición**
Datos	Construyen el núcleo de la organización, es toda la información sensible de la organización.
Software	Construido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información.
Hardware	Se trata de los equipos como servidores o terminales que contienen las aplicaciones y a la vez almacena los datos.
Redes	Desde las redes locales de la propia organización hasta las metropolitanas o internet.
Soportes	Los lugares en donde la información queda registrada y almacenada largos periodos de forma permanente.
Instalaciones	Son los lugares que albergan los sistemas de información y de comunicaciones.
Personal	El conjunto de personas que interactúan con el sistema de información.

Servicios	Que se ofrecen a clientes o usuarios.

Fuente: (Aguilera López, 2010, pp. 12-13)
Realizado por: Byron Barragán, 2020

1.4.2. Definición de amenaza

En el campo de la informática se entiende por amenaza la presencia de diferentes factores entre ellos personas, sucesos o máquinas que pueden atacar o hacer vulnerables a los sistemas con la finalidad de causar daños según la vulnerabilidad que se aproveche. (Aguilera López, 2010, p. 13)

1.4.2.1. Clasificación de amenazas

Las amenazas se clasifican en función del tipo de alteración, daño o intervención que se puede causar en cuatro grupos:

- **De interrupción.** El objetivo es deshabilitar el acceso a la información.

- **De interceptación**. Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial.

- **De modificación.** Modificar la información.

- **De fabricación.** Agregarían información falsa en el conjunto de información del sistema. (Aguilera López, 2010, pp. 13-14)

1.4.2.2. Factor insider

En el campo de la seguridad un insider es una persona perteneciente a una organización, independientemente de la acción que realice la misma. El único objetivo de esta persona son acciones maliciosas. Por lo general estas personas tiene acceso a los activos de la organización. Las amenazas insiders pueden ser de dos tipos los cuales son:

- **Accidentales.** Causadas por personas que no tienen una cultura hacia la seguridad de la información, por lo cual no tienen una buena gestión en cuanto a información sensible o no tiene el conocimiento adecuado para el manejo de los equipos de red.

- **Intencionadas.** Este tipo de insider son considerados maliciosos, ya que pueden robar información, modificar o introducir software malicioso en la red valiéndose de las vulnerabilidades presentes en la red. Estas personas pueden tener o no conocimiento de informática. Para una persona que no conozca mucho del ámbito de la informática puede buscar información relacionada al tema en internet y cometer su acción maliciosa.

Para el caso de una red de área de campus académica los posibles insiders pueden ser los mismos estudiantes, el sector administrativo o la planta docente.

1.4.3. Definición de riesgo

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. (Aguilera López, 2010, p. 14)

1.4.4. Definición de ataque

Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza. Los ataques pueden ser activos o pasivos diferenciándose si han sido descubiertos o no y si se lograron mitigar. (Aguilera López, 2010, p. 14)

1.4.5. Vulnerabilidades de la capa de transporte del modelo OSI

Para el desarrollo de este trabajo se tomó en cuenta algunas vulnerabilidades, ataques, amenazas o riesgos que son más comunes en la capa de transporte del modelo OSI, estos están relacionados con los protocolos UDP o TCP a continuación se mencionaran algunas:

1.4.5.1. Fingerprinting

Una técnica que permite extraer información de un sistema concreto, es decir; obtener el sistema operativo que se ejecuta en la maquina destino de la inspección. Esta información junto con la versión del servicio o servidor facilitará la búsqueda de vulnerabilidades asociadas al mismo. (Mejia, Ramirez & Rivera, 2012, p. 112)

Para poder tener éxito en este ataque es necesario tener un puerto ya sea TCP o UDP disponible o abierto. La probabilidad de tener éxito de este ataque es muy elevada en sistemas operativos remotos ya que se basa en realizar un listado de las características propias de una

implementación de la pila frente a otra, ya que la interpretación de las RFCs no siempre son las mismas (Mejia, Ramirez & Rivera, 2012, p. 112)

Existe dos tipos de ataques fingerprinting; activo y pasivo el ataque activo está basado en las respuestas de los sistemas operativos son diferentes si se envían diferentes tipos de paquetes malformados. Utilizando herramientas que puedan comparar estas respuestas con una base de datos con respuestas conocidas de sistemas operativos se puede determinar qué sistema está instalado en el objetivo. Nmap es una herramienta ampliamente utilizada para hacer ataque de fingerprinting activo. (Catoira, 2012a). Por otra parte, un ataque fingerprinting pasivo no es realizado directamente en el sistema objetivo, este tipo de ataque analiza todos los paquetes que envía el objetivo utilizando técnicas de sniffing, una vez detectados y capturados estos paquetes los compara con una base de datos donde se tenga alguna referencia de los distintos paquetes de los sistemas operativos y así poder determinar el sistema operativo. (Catoira, 2012a)

Estos dos tipos de ataques tienen una diferencia considerable y esta es la probabilidad de ser detectado por el objetivo, el ataque activo genera tráfico de red en el objetivo creando sospechas. El ataque pasivo es silencioso ya que lo único que hace es interceptación de paquetes. En la figura 4-1 se observa la utilización de la herramienta Nmap para un ataque activo de fingerprinting.

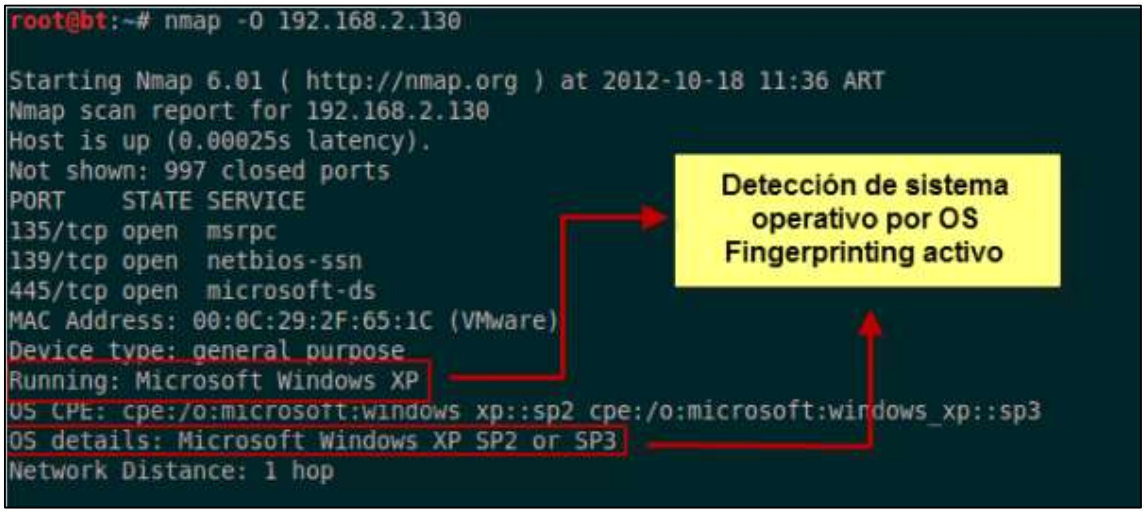


Figura 4-1: Uso de la herramienta Nmap para un ataque activo de fingerprinting
Fuente: (Catoira, 2012a)

Según Catoira un ataque activo de fingerprinting será más efectivo al momento de identificar el sistema operativo debido a que es una método más invasivo y directo y, además, mucho más fácil de realizar. Sin embargo, un ataque pasivo de fingerprinting es una buena técnica para la

identificación de sistema operativo ya que se puede ejecutar pese a que el objetivo este protegido por sistemas de detección de intrusos o con firewalls. (Catoira, 2012ª)

1.4.5.2. Escaneo de puertos

Una técnica, centrada en la búsqueda de vulnerabilidades, basada en una exploración de escaneo de puertos abiertos, tanto UDP como TCP. Consiste en la determinación de las características de una red para identificar los equipos activos desde Internet, así como los servicios que ofrece cada uno. (Mejia, Ramirez & Rivera, 2012, p. 112). El objetivo de un escaneo de puertos es determinar los equipos activos y disponibles a los que se puede llegar o alcanzar desde internet, con esto se puede además determinar los servicios que ofrecen los puertos descubiertos y sobre todo como están organizados los equipos conectados a la red.

Entre los métodos para hacer un escaneo se tiene ping sweep utilizando la herramienta Nmap, esta herramienta realiza un descubrimiento de sistemas mediante un sondeo ping, y que luego emita un listado de los equipos que respondieron al mismo. Permite un reconocimiento liviano de la red objetivo sin llamar mucho la atención. El saber cuántos equipos se encuentran activos es de mayor valor para los atacantes que el listado de cada una de las IP y nombres. Para realizar el ataque la herramienta envía una solicitud de eco ICMP y un paquete TCP al puerto 80 por omisión esperando las respuestas de los equipos activos en red. Cuando un usuario sin privilegios ejecuta Nmap se envía un paquete al puerto 80 del objetivo. Cuando un usuario privilegiado intenta analizar objetivos en la red Ethernet local se utilizan solicitudes ARP (Nmap, 2020). En la figura 5-1 se muestra el procedimiento de un ping sweep.

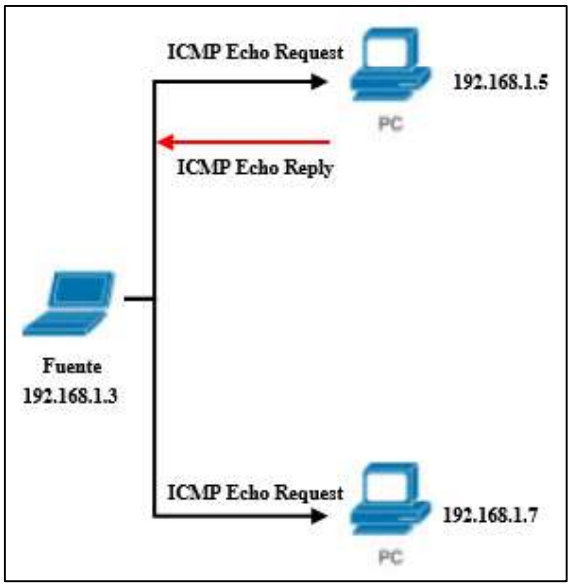


Figura 5-1: Procedimiento para un escaneo Ping
Realizado por: Byron Barragán, 2020.

El procedimiento de la figura 5-1 consiste en enviar un ICMP Echo Request hacia todos los objetivos y solo aquellos que respondan con una ICMP Echo Reply son aquellos equipos que están activos y Nmap arroja una lista de todos estos equipos.

Para listar los puertos la herramienta Nmap envía un paquete con la bandera ACK este paquete indica que se han recibido datos en una conexión TCP establecida, pero se envían sabiendo que la conexión no existe. En este caso los sistemas deberían responder con un paquete RST, lo que sirve para determinar que están activos, esto se realiza para cada puerto (Nmap, 2020). En la figura 6-1 representa como se descubre los puertos.

Figura 6-1: Procedimiento para descubrir puertos abiertos en un objetivo
Realizado por: Byron Barragán, 2020

1.4.5.3. Inundación UDP

Es una Denegación de Servicio (DoS) mediante el protocolo UDP. El ataque puede ser iniciado por el envío de un gran número de paquetes UDP a puertos aleatorios en un host remoto. Para un gran número de paquetes UDP, los sistemas de las víctimas se verán, obligados a enviar muchos paquetes ICMP. Esto impide que el ICMP sea alcanzable por otros clientes. Además, el atacante puede falsificar la dirección IP de los paquetes UDP para así asegurarse que los paquetes de retorno no lleguen a su destino. (Mejia, Ramirez & Rivera, 2012, p. 113). La figura 7-1 muestra un ejemplo de este tipo de ataques.

Como se observa en la figura 7-1 representa una técnica de ataque de inundación UDP, la cual consiste en amplificar el tráfico UDP de los servidores y, además, utilizando una botnet. Al amplificar el tráfico UDP el sistema colapsa no permitiendo que los usuarios legítimos se conecten.

Un ejemplo de este ataque es utilizando el protocolo DNS y los servidores de Google para la amplificación de los paquetes UDP como lo explica Juan Antonio Calles en FluProject. En el menciona que el protocolo DNS soportaba unas respuestas de un tamaño máximo de 512 bytes sobre UDP, la especificación EDNS0 (un parche publicado en la RFC 2671 en 1999) permitió el envío de mensajes de hasta 4096 bytes. Por tanto, a partir de una consulta de unos 75 bytes se

puede provocar una respuesta de hasta 4096 bytes obteniendo un factor de amplificación máximo de aproximadamente de 54:1. Pese a no tener un factor de amplificación muy elevado, está diseñado para estar publicado a Internet, por lo que todos los servidores DNS públicos podrían valer como amplificadores (Calles, 2018) y es por esto la utilización de los servidores de Google.

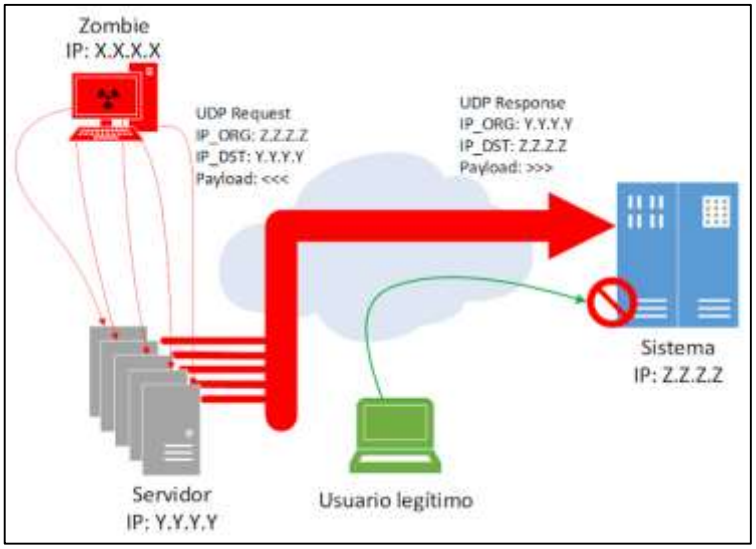


Figura 7-1: Procedimiento de un ataque de inundación UDP
Fuente: (Calles, 2018)

1.4.5.4. Inundación TCP SYN

Este ataque informático se trata del envió exagerado de paquetes para el establecimiento de una conexión se sincronización (SYN) en un sistema. El sistema objetivo víctima del ataque recibe todos los paquetes y reserva una cantidad de memoria (buffer) para poder almacenar todos los datos relacionados de las nuevas solicitudes de sincronización por cada paquete recibido. Como se observó anteriormente el protocolo TCP establece una conexión en tres pasos, por lo que al recibir un paquete de sincronización (SYN) este responde con un paquete de recibo de sincronización (SYN-ACK) y posteriormente espera un paquete de respuesta (ACK) para levantar la conexión, a este proceso se le conoce como Three-way-handshake. En este ataque la conexión nunca se confirma ya que permanece en un estado semiabierto (SYN-RCVD), el atacante no enviará el paquete ACK esperado para el establecimiento de la conexión, sin embargo, la cantidad de memoria continua reservada hasta que se confirme la conexión, mientras tanto continúan llegando más solicitudes de conexión y la memoria se reserva en su totalidad por solicitudes falsas de conexión; cualquier solicitud genuina no podrá establecer conexión por lo que se anula el servicio. (Mejia, Ramirez & Rivera, 2012, p. 114)

La figura 8-1 representa lo antes mencionado, una maquina atacante con una dirección IP falsa envía varios paquetes de sincronización para establecer una sesión TCP, el servidor envía una respuesta para establecer la sincronización, pero esta nunca llega a su destino debido a que la dirección IP es falsa, mientras tanto el atacante continúa enviando paquetes haciendo que la memoria del servidor colapse y no permita que otros usuarios establezcan una sesión TCP.

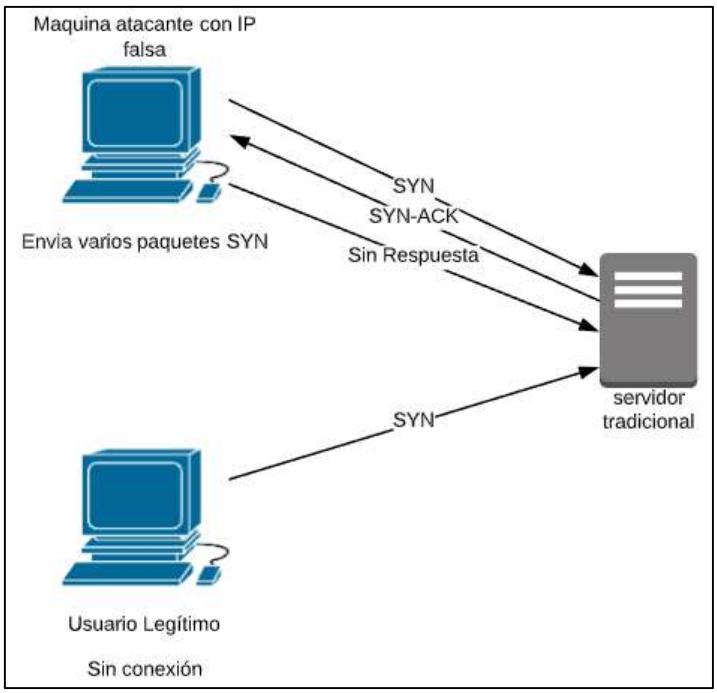


Figura 8-1: Procedimiento de un ataque de inundación SYN, envío de paquetes SYN
Realizado por: Byron Barragán, 2020

1.4.5.5. Connection Flood

Los servicios que funcionan con TCP se orientan hacia la conexión, por ejemplo, SSH, FTP, HTTP, SMTP, NNTP. Estos protocolos tienen definido un límite de conexiones que se pueden manejar al mismo tiempo; si este límite es excedido toda conexión es rechazada. De igual forma que el ataque de inundación SYN, si un atacante puede centralizar el límite definido con conexiones originadas por el mismo, pero no se realiza ninguna comunicación o acción el sistema no responde por lo que se anula el servicio.

Un ejemplo de este ataque es el uso de un cliente para establecer conexiones dirigidas a un sistema, pero el atacante no las finaliza correctamente, haciendo que el servidor y los sockets correspondientes a estas conexiones sigan estando en modo activos y por lo tanto continúen consumiendo recursos, a este estado se le conoce como estado TIME_WAIT. (Mejia, Ramirez & Rivera, 2012, p. 114)

Un ejemplo es la utilización de la herramienta Slowloris la cual envía paquetes HTTP excediendo el límite de conexiones denegando el servicio, esta herramienta tiene como objetivo a servidores web basados en Apache. La figura 9-1 muestra el procedimiento de este ataque.

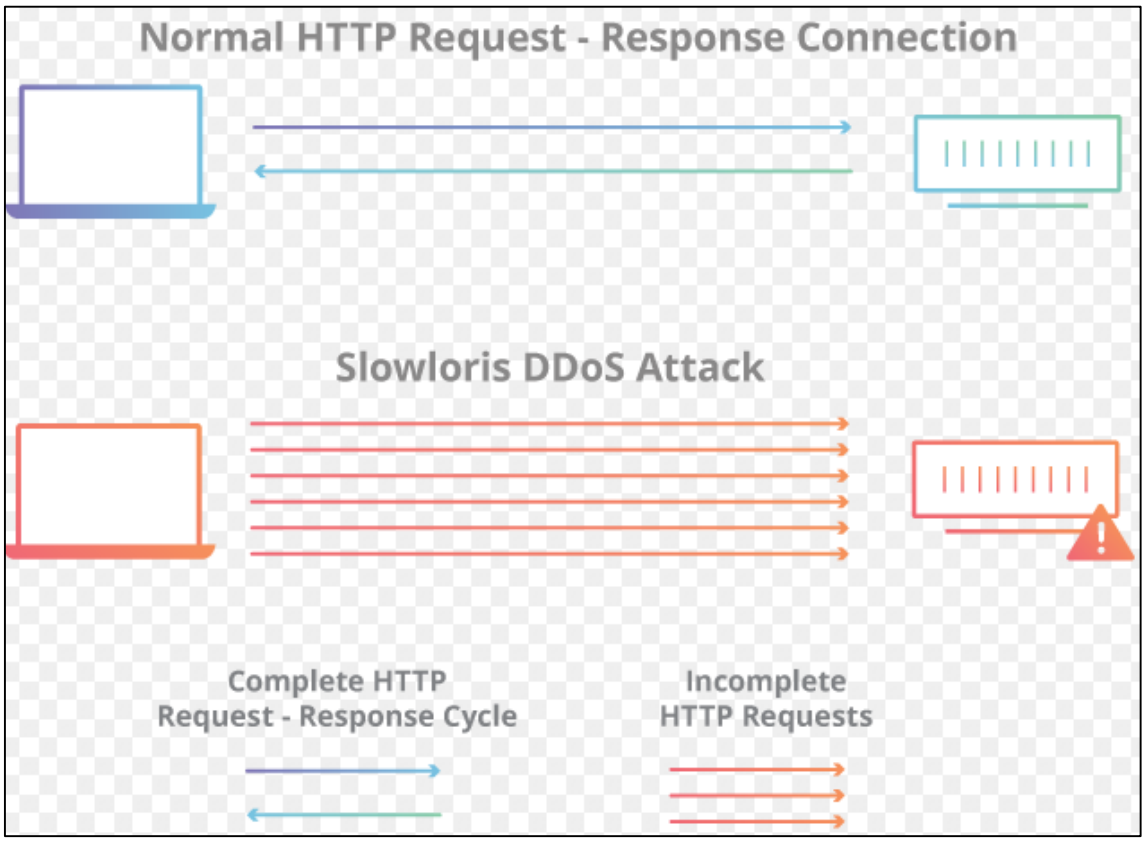


Figura 9-1: Procedimiento de un ataque de inundación de peticiones de conexión con Slowloris
Fuente: (Cloudflare, 2020)

Un ataque Slowloris, se divide en 4 pasos:

- El atacante primero abre múltiples conexiones al servidor de destino mediante el envío de múltiples encabezados parciales de solicitud HTTP.

- El objetivo abre un hilo para cada solicitud entrante, con la intención de cerrar el hilo una vez que se completa la conexión. Para ser eficiente, si una conexión demora demasiado, el servidor excederá el tiempo de espera de la conexión excesivamente larga, liberando el hilo para la próxima solicitud.

- Para evitar que el objetivo exceda el tiempo de espera de las conexiones, el atacante envía periódicamente encabezados de solicitud parciales al objetivo para mantener viva la solicitud.

- El servidor de destino nunca puede liberar ninguna de las conexiones parciales abiertas mientras espera la finalización de la solicitud. Una vez que todos los hilos disponibles están en uso, el servidor no podrá responder a las solicitudes adicionales realizadas desde el tráfico regular, lo que resulta en la denegación de servicio. (Cloudflare, 2020)

1.4.5.6. Land

Mediante este ataque se puede bloquear sistemas, este ataque consiste en enviar paquetes SYN, pero con la particularidad de que las direcciones IP de origen y destino son las mismas, esto también incluye los puertos de origen y destino. Este ataque puede ser detectado por sistemas NIDS tanto puertos como direcciones IP. Existe un caso particular en el que se establezca una conexión a la propia máquina, se envíe por tanto un paquete para establecer la conexión, el sistema IDS lo detecte como un ataque cuando en realidad no lo es. Esto refleja la estrecha línea existente entre un ataque real y una situación convencional. (Mejia, Ramirez & Rivera, 2012, p. 116)

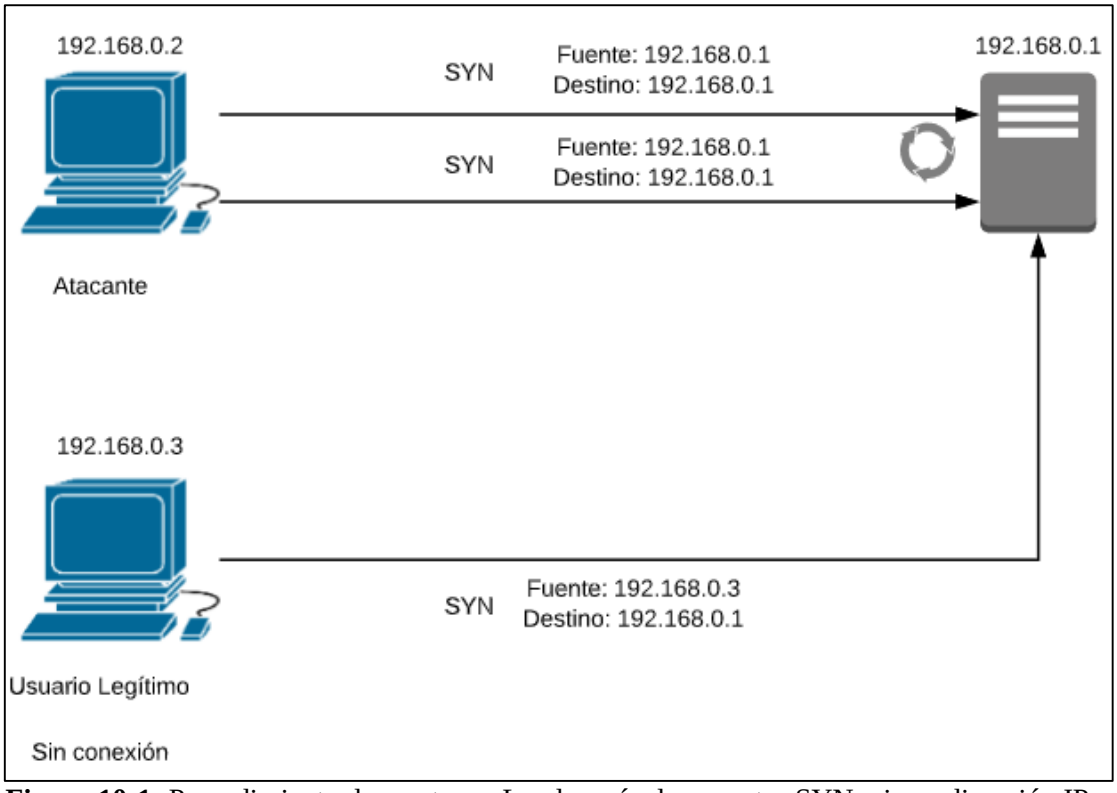


Figura 10-1: Procedimiento de un ataque Land, envío de paquetes SYN misma dirección IP
Realizado por: Byron Barragán, 2020

1.4.5.7. Tiny Fragment attack

Este ataque se basa en la fragmentación, esta se da cuando un paquete supera el tamaño definido de trasmisión es decir el MTU, por lo tanto, el paquete se debe dividir. Las divisiones serán 2

donde la primera incluye la cabecera TCP del paquete original y la segunda división contendrá los datos y la cabecera IP. Para reensamblar los paquetes existe el campo Fragment offset en la cabecea IP el cual indica si existen fragmentos o no y además la relación entre los fragmentos. En si el ataque consiste en fragmentar los paquetes en varias divisiones causando que se llene la memoria. La figura 11-1 muestra la fragmentación de los paquetes. (Mejia, Ramirez & Rivera, 2012, p. 118)

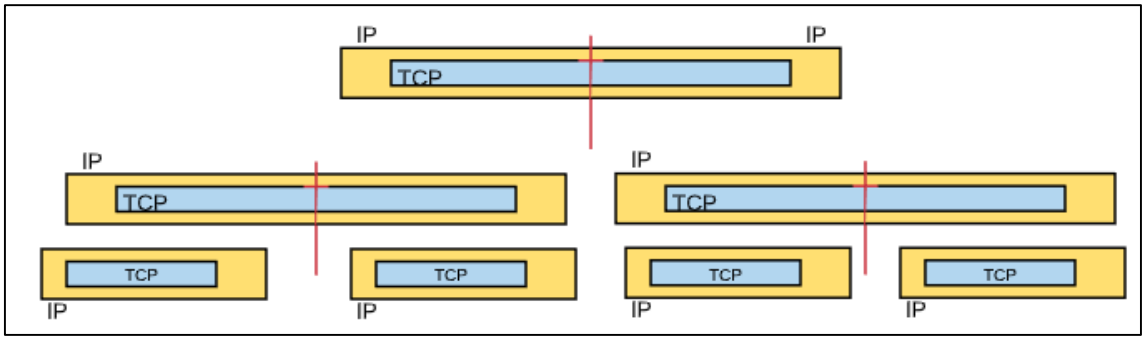


Figura 11-1: Fragmentación de paquetes TCP
Realizado por: Byron Barragán, 2020

1.4.5.8. Session Hijacking

La información que se trasmite en las redes de datos tiene una gran importancia como ya se ha mencionado anteriormente, por lo tanto, las medidas de seguridad deben ser acorde a la importancia de estos datos. Mientras los datos fluyen por la red, este tipo de ataque intenta secuestrar una sesión ya iniciada. Con la sesión establecida el atacante procede a introducir paquetes en medio aparentando ser paquetes de la fuente original. Este tipo de ataques también se conoce como "Man in The Middle Attack", ya que el atacante debe situarse entre el equipo que estableció la conexión original y la víctima. (Mejia, Ramirez & Rivera, 2012, p. 116)

En general el proceso de control de la sesión secuestrada se emplea con técnicas como Source-Routing para que todos los paquetes con la información valiosa regresen al atacante y no al destino habitual. Finalmente, para la extracción de la información se utiliza de un sniifer completando así el ataque. (Mejia, Ramirez & Rivera, 2012, p. 116) La figura 12-1 representa lo antes descrito.

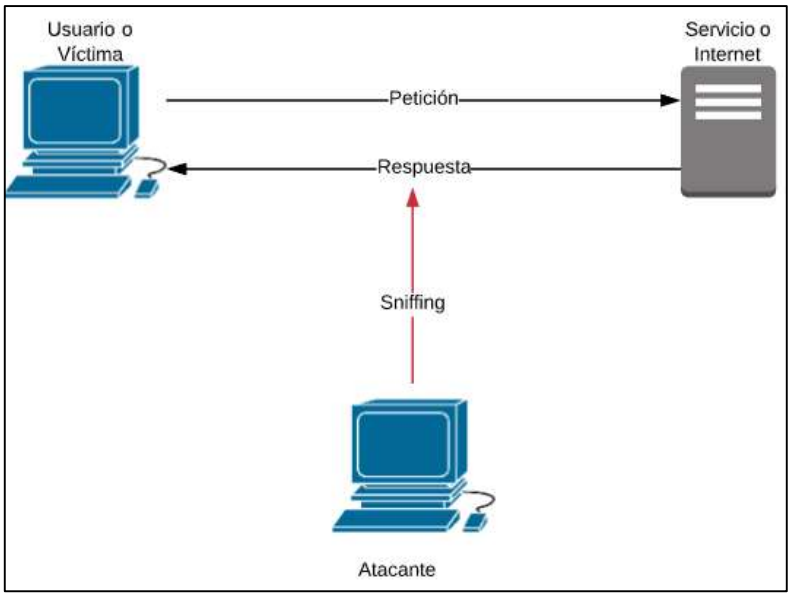


Figura 12-1: Procedimiento de un ataque de secuestro de sesión mediante un ataque de "Man in the middle"
Realizado por: Byron Barragán, 2020

1.5. Metodología OSSTMM

Por sus siglas en inglés, El Manual de la Metodología de Testeo de Seguridad (OSSTMM) es un proyecto desarrollado por el Instituto de Seguridad y Metodologías Abiertas, ISECOM. Esta metodología es adoptada para medir la seguridad operativa de las instalaciones físicas, interacciones humanas, y formas de comunicación como inalámbrica, cableada, analógica y digital. (Calvopiña & Pilatuña, 2016, p. 12)

Proporciona una metodología para realizar una prueba de seguridad exhaustiva, aquí denominada auditoría de OSSTMM. Una auditoría OSSTMM es una medición precisa de la seguridad a un nivel operativo que está libre de suposiciones y evidencia anecdótica. Como metodología está diseñada para ser consistente y repetible. Como proyecto de código abierto, permite que cualquier probador de seguridad aporte ideas para realizar pruebas de seguridad más precisas, procesables y eficientes. Además, permite la libre difusión de información y propiedad intelectual. (ISECOM & Herzog, 2010)

1.5.1. Antes de aplicar la metodología OSSTMM

Para comenzar a realizar una prueba OSSTMM, deberá realizar un seguimiento de lo que prueba (los objetivos), cómo los prueba (las partes de los objetivos que se probaron y no las herramientas o técnicas utilizadas), los tipos de controles descubiertos y lo que no hizo. Prueba (objetivos y partes de los objetivos). Luego puede realizar la prueba como está acostumbrado con el objetivo de poder responder las preguntas en el Informe de auditoría de la prueba de

seguridad (STAR) disponible en el manual OSSTMM o como su propio documento. El STAR proporciona la información de prueba específica sobre el estado del alcance para los beneficios de tener una declaración clara de las métricas de seguridad y detalles para comparaciones con pruebas de seguridad anteriores o promedios de pruebas de la industria. Como se puede ver, este enfoque significa que se requiere muy poco tiempo además de una prueba estándar y la formalización del informe. Se ha informado que esta metodología en realidad reduce el tiempo de prueba e informe debido a las eficiencias introducidas en el proceso. No debe haber ninguna razón económica o de tiempo para evitar el uso del OSSTMM y no se hacen restricciones irrazonables al probador. (ISECOM & Herzog, 2010)

Este Manual es catalogado como un estándar profesional para el testeo de seguridad en cualquier entorno desde el exterior al interior, es decir, testea la seguridad desde un entorno no privilegiado hacia un entorno privilegiado para evadir los componentes de seguridad, procesos y alarmas, y así ganar acceso privilegiado. El objetivo de este es crear un método aceptado para ejecutar un test de seguridad minucioso y cabal. (Calvopiña & Pilatuña, 2016, p. 12)

1.5.2. Fases de la metodología OSSTMM

Existen cuatro fases en la que se divide la ejecución de esta metodología.

- **Fase de inducción.** En la fase de inducción, el analista comienza la auditoría con el entendimiento de los requisitos de la auditoría, el alcance y las limitaciones de la auditoría. Esta fase consta de los módulos: Revisión de la postura, Logística, Verificación de la detección activa.

- **Fase de interacción.** En la fase de interacción, el núcleo de la prueba de seguridad básica requiere conocer el alcance en relación con las interacciones con los objetivos transmitidos a las interacciones con los activos. Esta fase consta de los siguientes módulos: Visibilidad de la auditoria, verificación de acceso, comprobación de confianza, controles de verificación.

- **Fase Indagatoria.** En esta fase, los distintos tipos de valor o de perjuicio de la información de un activo fuera de lugar y mal administrado salen a la luz. Esta fase consta de los siguientes módulos: Proceso de verificación, verificación de configuraciones, validación de propiedad, revisión de segregación, verificación de exposición, exploración de inteligencia competitiva.

- **Fase de intervención.** Esta es a menudo la fase final de una prueba de seguridad para asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas. Adicionalmente, la información para hacer estas pruebas no puede ser conocida hasta que las anteriores fases se hayan llevado a cabo. Esta fase consta de los siguientes módulos: Verificación de cuarentena, privilegios de auditoria, validación de supervivencia, revisión de alertas y registros. (Calvopiña & Pilatuña, 2016, pp. 13-14)

1.6. Pruebas de penetración

Las pruebas de penetración son prácticas que son utilizadas por un auditor informático para determinar la seguridad de un sistema además de tener como objetivo encontrar las vulnerabilidades que se pueden explotar tanto por un atacante desde afuera como adentro.

1.6.1. Fases de las pruebas de penetración.

- **Fase de reconocimiento:** La primera etapa es la más importante por lo que en esta se toma bastante tiempo. se deben definir objetivos y recopilar toda la información disponible para luego poder utilizarla en las demás fases y determinar la seguridad operacional. La información requerida abarca desde nombres y direcciones de correo electrónico de empleados de la organización, hasta la topología de la red, direcciones IP y demás información según lo indique el manual.

- **Fase de escaneo:** Basándose en la información obtenida en la fase anterior se determina los posibles sectores de los ataques, entre los posibles sectores de ataque se puede determinar son los puertos y sus respectivos servicios. En esta fase se realiza un escaneo de vulnerabilidades conocidas.

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

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

- **Fase de mantenimiento de acceso**: Como el nombre lo indica el objetivo es mantener el acceso comprometiendo así el sistema y tenerlo a disposición de quien lo ha atacado manteniéndolo activo durante un tiempo. (Catoira, 2012b)

1.6.2. Herramientas de testeo Open Source

Las herramientas open Source conocidas por ser de código abierto es decir un tipo de software que se distribuye con una licencia que le da libertad al usuario final de poder utilizar el código fuente para diversas actividades o para una comprensión mejor del programa. Estos programas son de gran ayuda hacia los programadores ya que pueden añadir opciones y corregir algunos problemas que se puedan encontrar, una vez compilado el programa tendrá un mejor diseño en comparación con el diseño original pudiendo incluso distribuir su trabajo. (Tecnología Fácil, 2015)

1.7. Sistema de detección de intrusos en red (NIDS)

Partamos desde un IDS, un IDS por sus siglas en inglés (Intruder Detection System), es una herramienta para la seguridad que consiste en la detección, monitorización de la data y de todas las acciones que ocurran en la red informática, las acciones que se detecten son aquellas que pueden comprometer la seguridad del sistema.

Un IDS para la detección busca parámetros los cuales so definidos con anterioridad o por el mismo IDS en un conjunto de reglas, siendo estas las que determinaran si las acciones en la red o el host son sospechosas o maliciosas. Cabe indicar que estos sistemas son más orientados a alertar sobre dichas acciones maliciosas mas no para detener un ataque.

Un NIDS es un tipo de IDS, este tipo actúa sobre la red de la organización capturando y analizando la data de la red, algo así como un sniffer revisando el tráfico de la red buscando parámetros que indiquen algún tipo de ataque. Esto se puede realizar a tiempo real utilizando un puerto en modo promiscuo configurando un puerto espejo el cual escucha todo el tráfico de la red y lo analiza.

1.7.1. Snort como NIDS

Snort es un NIDS, es decir, Sistema de Detección de Intrusos basados en red. Este sistema puede detectar ataques en la red, registrar y alertar sobre acciones maliciosas como ataques informáticos, intentos de explotar vulnerabilidades, escaneo de puertos, análisis de protocolos entre otros, estos se definen como patrones en un conjunto de reglas analizando a tiempo real.

Este sistema tiene licencia GPL (General Public License), es gratuito y tiene soporte para varias plataformas como Windows o linux, una de las ventajas de Snort es que tiene definido ya un conjunto de reglas para utilizar en la detección actualizando estas ante casos de ataques o vulnerabilidades nuevas según informes de seguridad de entidades de seguridad.

1.8. Escaneo de vulnerabilidades en red

Mediante una herramienta se realiza un análisis e identificación de todos los dispositivos que se encuentren conectados a la red, tras finalizar el análisis se genera un reporte de todas las vulnerabilidades encontradas para así tomar acciones correctivas. Con esto lo que se busca es proteger y mejorar la seguridad frente a acciones maliciosas de algún agresor cibernético externo o interno.

1.8.1. Nexpose como escáner de vulnerabilidades de red.

Nexpose es una herramienta desarrollada por Rapid7, es capaz de escanear redes, sitios web, bases de datos, aplicaciones web, sistemas operativos y máquinas virtuales. Es multiplataforma, es decir, se puede instalar en Windows, Linux o máquinas virtuales. Ofrece una interfaz gráfica amigable para usuario accediendo desde un portal web. En este portal se crean los sitios que se van a escanear siendo estos sitios las direcciones IP de los activos además de seleccionar las preferencias de escaneo, planificar el análisis y proporcionar las credenciales.
Como resultado del escaneo se genera un reporte con una lista de los activos y las vulnerabilidades encontradas con posibles soluciones.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Etapas del trabajo

El trabajo de titulación está dividido en tres etapas, cada una se realiza terminada la etapa anterior, a continuación, se muestra un cuadro de las etapas y las funciones que se deben realizar en cada una:

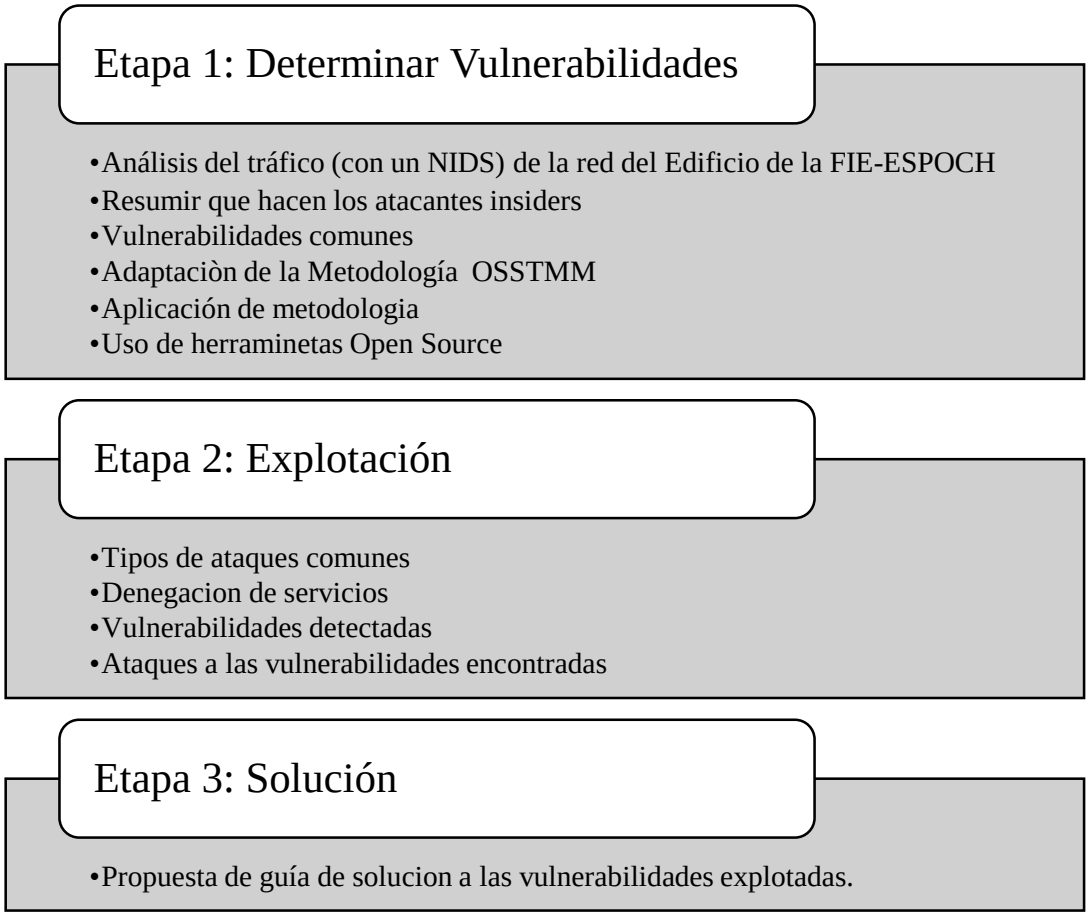


Gráfico 1-2: Etapas para el desarrollo del trabajo de titulación
Realizado por: Byron Barragán, 2020

En el gráfico1-2 se encuentran las etapas en las que se divide el trabajo de titulación, la primera etapa denominada "Determinar vulnerabilidades" se toma en cuenta la realización de una investigación acerca de vulnerabilidades y ataques más comunes en la capa de transporte teniendo en cuenta las acciones que un insider puede hacer, seguido un análisis de tráfico en la red del edificio de la FIE-ESPOCH utilizando un Sistema de detección de intrusos basado en red (NIDS) esto con el objetivo de determinar ataques que se realicen en el nodo de la FIE, haciendo énfasis en posibles ataques insiders acorde a la investigación previa. Durante el proceso de análisis de tráfico se aplica las fases de la metodología OSSTMM en la red del

edificio de la FIE-ESPOCH utilizando herramientas de testeo y análisis Open Source, obteniendo las vulnerabilidades de la red. La segunda etapa denominada “explotación”, en base a las vulnerabilidades encontradas en la etapa anterior se realiza un análisis de los posibles daños mediante la explotación de estas. La tercera etapa denominada “solución” se propone una guía de solución a las vulnerabilidades explotadas y a los ataques que se realizaron.

2.2. Etapa 1: Determinar vulnerabilidades

En esta etapa se realiza primero una investigación para estar preparado de los posibles ataques que se pueden encontrar durante el análisis del sistema de detección de intrusos basado en red (NIDS) en la red del edificio de la FIE-ESPOCH.

2.2.1. ¿Qué puede hacer un insider en la red a nivel de la capa de transporte?

Como se mencionó anteriormente la capa de transporte tiene la función de proveer calidad de servicio cuando es requerido, además de confiabilidad, control del flujo de paquetes y errores durante las sesiones de la comunicación. Esta capa envía paquetes TCP y UDP en datagramas IP. Los ataques más comunes hacia esta capa son los de denegación de servicios (DoS) y denegación de servicios distribuidos (DDoS) utilizando protocolos propios de esta capa. Estos ataques comprometen la autenticación, integridad, disponibilidad y confidencialidad.

Existe una serie de ataques que aprovechan las fallas en los diseños de los protocolos de esta capa. Una de las vulnerabilidades más graves contra estos mecanismos de control o protocolos es la interceptación de sesiones TCP con el objetivo de secuestrarlas para acciones maliciosas. Estos ataques de secuestro se aprovechan de la poca autenticación de los equipos involucrados en una sesión, se puede mencionar Ataques LAND, Inundación SYN o ataques meterpreter según lo menciona Aitor B Fernández ingeniero en redes y seguridad (Fernández, 2018). El ataque LAND se trata de enviar paquetes que contengan la misma dirección IP de origen y destino haciendo que los sistemas se bloqueen y se vuelvan inestables convirtiéndose este en un ataque de denegación de servicio. Por otro lado, el ataque de inundación SYN consiste en que el atacante envía paquetes de sincronización repetidamente a los puertos de un servidor, estos paquetes tienen direcciones IP falsas lo que provoca que la conexión no termine después el servidor intenta responder con paquetes de sincronización (SYN) y reconocimiento (ACK), y con un paquete RST desde cada puerto cerrado, la victima devolverá un paquete ACK para confirmar que se recibió el paquete SYN/ACK desde el servidor, y entonces comenzará la comunicación. Sin embargo, en un ataque de inundación SYN, el paquete ACK nunca es devuelto por el atacante. En su lugar, envía repetidamente paquetes SYN a todos los puertos del

servidor teniendo como resultado corrupción de memoria lo que desencadena en un ataque de denegación de servicio.

Los puertos abiertos representan una vulnerabilidad que un atacante ya sea insider o no puede explotar a su conveniencia. Descubriendo puertos abiertos puede tomar control del activo informático víctima y así hacerse con la información valiosa de la víctima. Para la capa de transporte los puertos UDP y TCP son los objetivos de los ataques, como se vio en el capítulo anterior en las cabeceras de los protocolos UDP y TCP están los apartados de puerto de origen y destino, con esta información se puede ingresar al equipo víctima y operar dentro de este precisamente por este puerto que se encuentra abierto. (Fernández, 2018). Es por eso por lo que se debe realizar una auditoría de puertos abiertos en la organización. Por ejemplo, un ataque meterpreter generando un malware utilizando un puerto abierto es capaz de oír todas las sesiones activas en el equipo victima e incluso robar información sin que el usuario víctima no se entere para después iniciar conexiones hacia fuera continuando con ataques fingerprinting y obtener información de los equipos conectados a la red.

Al igual que un malware, un troyano se vale de puertos abiertos para poder operar, por ejemplo, un troyano criptomineros. Del mismo modo que el punto anterior la auditoría de puertos abiertos y además la utilización de un NIDS puede ser de gran ayuda para determinar tráfico relacionado a un troyano y el puerto que utiliza, es de gran importancia revisar puertos TCP y UDP abiertos. (Fernández, 2018) Con la ayuda de NIDS-SNORT se presentará las amenazas descubiertas.

2.2.2. Escenario de estudio, edificio de la FIE-ESPOCH

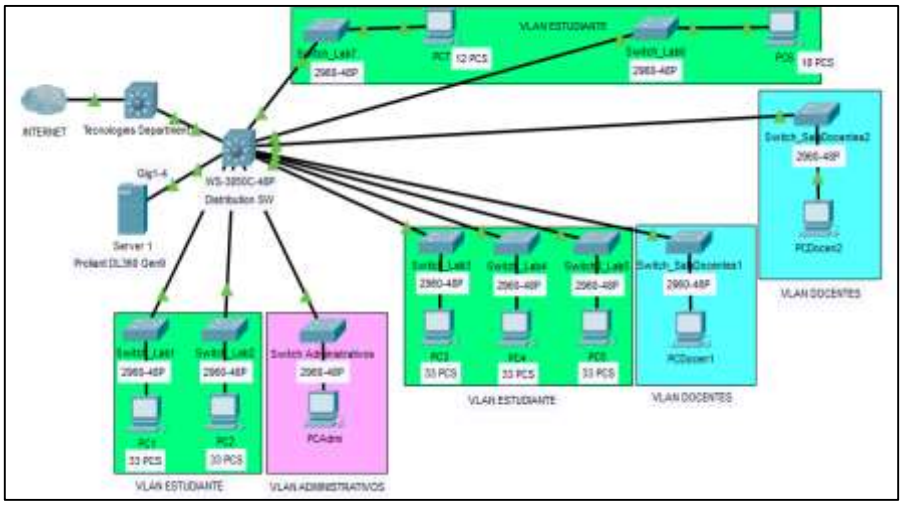


Figura 1-2: Escenario del edificio de la FIE-ESPOCH
Realizado por: Byron Barragán, 2020

En la Figura 1-2 se observa la infraestructura física del escenario de estudio que incluye: 7 laboratorios, 2 salas de profesores y un área administrativa. El equipamiento es de marca CISCO, posee un switch de distribución WS-3850C-48P, al que se conectan 10 switchs de acceso 2960-48P. En el edificio de la FIE-ESPOCH se instaló un servidor HP G9 como se observa en la figura, el cual se conecta también al switch de distribución donde se habilitó tres puertos espejo para realizar el análisis de la intranet e identificar las amenazas internas. El periodo de análisis que se consideró es el de mayor carga en la red. En el servidor corre tres máquinas virtuales con sistema operativo CentOS versión 7. Estas máquinas virtuales poseen un adaptador de red que está escuchando desde el puerto espejo, el cual recibe todo el tráfico generado en las Vlans y en todas las maquinas conectadas a la red del edificio. La red está dividida en tres Vlans estas son: Estudiantes, Docentes y Administrativos. Para el análisis del tráfico se configuró un puerto espejo para cada Vlan, el cual se conecta a cada máquina virtual teniendo así una máquina virtual por Vlan.

2.2.3. Snort como sistema de detección de intrusos (NIDS) en el edificio de la FIE-ESPOCH

Para el análisis de la red y determinar amenazas insiders se utiliza el sistema de detección de intrusos basado en red NIDS-SNORT. Este sistema se instaló en cada máquina virtual para el análisis del tráfico en las Vlans. Estas máquinas virtuales poseen dos adaptadores de red virtuales cada una, estos son: ens160 el cual tiene una dirección IP perteneciente a su respectiva Vlan y el otro adaptador de red ens192 está conectado a tres puertos espejo uno por Vlan en el switch de distribución del edificio; estos puertos reciben todo el tráfico generado en cada Vlan.

2.2.3.1. ¿Por qué NIDS-SNORT?

Se escoge Snort por algunos factores: su gran escalabilidad, facilidad que tiene para ejecutarse en varios sistemas operativos, capacidad de almacenar paquetes de red, análisis a tiempo real, es de código abierto, gratuito, siendo el hecho que posee la capacidad de generar alertas sobre actividad maliciosa en la red el factor más importante. Las alertas se pueden analizar después y generar acciones correctivas en base de la amenaza detectada. Por ejemplo, definir reglas propias las que se aplicaran en los futuros análisis. Otro factor en la elección es el soporte que presta la comunidad de Snort. Las reglas de la comunidad y las reglas registradas de usuario se pueden obtener gratuitamente en la página oficial https://www.snort.org. En este conjunto de reglas se pueden encontrar algunas definidas para backdoors, ataques de denegación de servicio, denegación de servicios distribuidos, fingerprinting, Inundaciones FTP, ataques desde una página web, uso de Nmap, detección de troyanos, detección de malware, entre otras. Siendo

estas amenazas las más comunes que se pueden encontrar en la red como se trató en apartados anteriores. Además, Snort es más eficiente en redes en las que la cantidad de tráfico es menor y las velocidades de internet son menores a los 100 Mbps. Esto en comparación a su principal competidor Suricata.

2.2.3.2. Instalación y configuración de NIDS-SNORT

Se puede descargar todos los archivos necesarios para su instalación en la página oficial, https://www.snort.org e incluso se encuentra pasos para su correcta instalación en diferentes distribuciones Linux siendo una de ellas CentOS.

- Instalación

El proceso de instalación de NIDS-SNORT es sencillo lo primero que se debe hacer es preparar el servidor instalando todas las bibliotecas necesarias para el trabajo de Snort. Este proceso se lo realiza desde la consola del sistema operativo en donde ejecutará el sistema NIDS. Ingresando la siguiente línea de comando:

sudo yum install -y gcc flex bison zlib libpcap pcre libdnet tcpdump

La última versión de NIDS-SNORT requiere libnghttp2, que se puede descargar de los paquetes adicionales para Enterprise Linux (EPEL) e instalarlos utilizando los comandos que se encuentran debajo:

sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
sudo yum install -y libnghttp2

Una vez preparado el servidor la instalación continua con el comando YUM como lo indica las siguientes líneas de comando:

sudo yum install https://www.snort.org/downloads/snort/daq-2.0.6-1.centos7.x86_64.rpm
sudo yum install https://www.snort.org/downloads/snort/snort-2.9.12-1.centos7.x86_64.rpm

Snort utiliza ciertas bibliotecas de adquisición de datos llamadas (DAQ) estas bibliotecas son de captura de paquetes. Snort se actualiza cada cierto tiempo por lo que se recomienda verificar la versión disponible en la página oficial https://www.snort.org/, en caso de una nueva versión, simplemente se reemplaza el número de versión en los comandos antes mostrados.

Puede que el primer comando en ciertos casos no se ejecute debido a las nuevas versiones de Snort por lo que el segundo comando ya abarcará las bibliotecas necesarias.

- Configuración

Primero se debe descargar las reglas de la comunidad, el comando que sigue son los necesarios para utilizar Snort con estas reglas.

wget https://www.snort.org/rules/community -O ~/community.tar.gz
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-rules/* /etc/snort/rules

Para poder acceder a las reglas registradas de usuario es necesario registrarse en la página de Snort y obtener un código OINK el cual es el que dará acceso a estas reglas, una vez registrado en la página web se puede encontrar el código en detalles de cuenta de usuario. Una vez adquirido el código OINK se lo reemplaza en el siguiente comando.

wget https://www.snort.org/rules/snortrules-snapshot-29120.tar.gz?oinkcode=oinkcode -O ~/registered.tar.gz
sudo tar -xvf ~/registered.tar.gz -C /etc/Snort

Los conjuntos de reglas para los usuarios registrados incluyen una gran cantidad de reglas útiles de detección preconfiguradas. Se puede habilitar estas reglas adicionales descomentando sus inclusiones hacia el final del archivo snort.conf.

Luego de la instalación de NIDS-SNORT y la obtención de las reglas de la comunidad y las de usuario Snort se debe editar el archivo de configuración ***/etc/snort/snort.conf***, indicando la red a analizar, los directorios donde se encuentran las reglas que se aplicarán para el análisis, configurar la salida para unified2 para iniciar sesión con el nombre de archivo de Snort.log e incluir las reglas de usuario Snort. En la parte final del archivo se ingresa las siguientes líneas de comando:

include $RULE_PATH/local.rules
include $RULE_PATH/community.rules

Para la ejecución de Snort se escribe lo siguiente:

sudo snort -A console -i ens192 -u snort -g snort -c /etc/snort/snort.conf

Esta línea indica que mostrará las alertas en consola escuchando por la interfaz ens192 utilizando el usuario Snort, el grupo de usuarios Snort, aplicando el archivo de configuración Snort.conf. Para detener el análisis se presiona ***Ctrl+c.***

2.2.3.3. Alertas y reglas de la comunidad

Snort tiene la capacidad de almacenar paquetes en logs, los cuales contienen detalles de todas las alertas, así como también una estadística de la cantidad de tráfico que se analizó en el tiempo de ejecución. Snort puede funcionar en tres modos, modo sniffer presentando todos los paquetes de red en consola, modo Packet logger capturando los paquetes de la red para su posterior análisis y modo detector de intrusos analizando todos los paquetes contra un conjunto de reglas definidas por el usuario como por la comunidad de Snort, cabe indicar que este modo es a tiempo real.

Referente a las reglas de la comunidad, estas pertenecen a una base de datos que se actualiza a través de internet, es decir los usuarios de Snort pueden crear una regla de detección a un tipo de ataque nuevo y cargarlo para que sea añadido en la base de datos y ser detectado en otra red que utilice Snort como NIDS. Cuando Snort está funcionando en modo NIDS, si encuentra un paquete que coincida con las reglas definidas en el conjunto de reglas, este paquete se guarda y salta una alerta en consola donde se puede apreciar donde y cuando se realizó el ataque. Snort también ofrece la opción de incluir reglas de detección locales, los usuarios de Snort pueden configurar una alerta para un determinado tipo de tráfico, protocolo, o puerto según las necesidades de la organización. La sintaxis para establecer alertas es fácil de entender y se puede encontrar ejemplos para una correcta escritura. En la figura 2-2 se puede observar un ejemplo de alerta local en la cual se entiende que aparecerá una alerta en consola cuando el tráfico del protocolo ICMP sea detectado desde cualquier red por cualquier puerto hacia cualquier red indicando el mensaje de la alerta y su identificación. Para el análisis que se realizó Snort estaba en modo NIDS, de esta manera se registró todas las alertas que se generaron en el análisis del tráfico a tiempo real de la red del edificio de la FIE-ESPOCH.

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

Figura 2-2 Ejemplo de establecimiento de una alerta local en Snort
Realizado por: Byron Barragán, 2020

2.2.3.4. Procedimiento de análisis de Snort de la red del edificio de la FIE-ESPOCH

Una vez configuradas las máquinas virtuales e instalado NIDS-SNORT, el análisis de tráfico de cada una de las Vlans empieza. Para el caso de la Vlan Estudiantes el análisis tuvo una primera prueba el 2 de mayo de 2019 aproximadamente a las 8 AM, se analizó el tráfico durante todo el día con la finalidad de comprobar el funcionamiento, registro de alertas y paquetes. El análisis inició formalmente el 6 de mayo a las 8 AM y culminó el 7 de junio. El horario que se tomó en cuenta para el análisis fue de todos los días incluidos fines de semana las 24 horas, exceptuando los días feriados, se debe indicar que cada día se registraba la cantidad de paquetes analizados, así como también las alertas que se daban en la Vlan con sus respectivas direcciones IP de origen y destino, cada alerta tiene un identificador el cual puede ser consultado en la página oficial de Snort para más información y posibles soluciones, en el registro de alertas se documentó el identificador, la fecha, hora de cada alerta, número total de alertas en el día y algunas observaciones presentadas durante el análisis.

Para el caso de la Vlan Docentes el análisis inició el 17 de junio de 2019 y culminó el 17 de julio. El procedimiento para el análisis fue el mismo que se aplicó en Vlan Estudiantes, es decir, el mismo horario y procedimiento de registro.

Para el caso de Vlan Administrativos el análisis inició el 17 de junio de 2019 y culminó el 17 de julio. El procedimiento para el análisis fue el mismo que se aplicó en Vlan Estudiantes y Vlan Docentes, es decir, el mismo horario y procedimiento de registro.

2.2.4. Parámetros de la metodología OSSTMM.

La metodología OSSTMM se maneja definiendo un alcance, el alcance es el entorno de seguridad operativo total posible para cualquier interacción con cualquier activo que pueda incluir también los componentes físicos de las medidas de seguridad. El alcance se compone de tres clases, de las cuales hay cinco canales: canales de seguridad de redes de datos y telecomunicaciones de la clase COMSEC, canales de seguridad física y humana de la clase PHYSSEC, y el canal de seguridad inalámbrico de espectro completo de la clase SPECSEC. Las clases son de designaciones oficiales actualmente en uso en la industria de la seguridad. (ISECOM & Herzog, 2010, p. 34)

Tabla 1-2: División de clases y canales de la metodología OSSTMM

Clase	**Canal**	**Descripción**
Seguridad Física	Humano	Comprende el elemento humano de la

(PHYSSEC)		comunicación donde la interacción es física o psicológica.
	Físico	Pruebas de seguridad física donde el canal es tanto de naturaleza física como no electrónica. Comprende el elemento físico de seguridad donde la interacción requiere fuerza o un transmisor de energía
Seguridad del Espectro (SPECSEC)	Inalámbrico	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar en el espectro EM. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales y EMSEC que son emanaciones no atadas por cables
Seguridad de las Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digitales o analógicas, donde la interacción es a través de un teléfono establecido o como líneas de red.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción es a través de cables establecidos y líneas de redes cableadas.

Fuente: (ISECOM & Herzog, 2010, p. 35)
Realizado por: Byron Barragán, 2020

En la Tabla 1-2 se observa el alcance que la metodología OSSTMM tiene en cuenta para la realización de una auditoria. Para la realización de este trabajo de titulación solo se tomarán en cuenta los canales Humano y Redes de Datos ya que son los que se adecuan a la investigación del grupo SEGINTE. La selección de estos canales es debido a que el canal humano se relaciona con el perfil de los usuarios que utilizan la red, dentro de estos puede estar un usuario insider por lo cual se analizará la seguridad de este canal enfocándose hacia este tipo de usuarios y el canal de redes de datos para analizar la seguridad actual de la red cableada del edificio de la FIE-ESPOCH.

OSSTMM también define métricas para la evaluación de la seguridad operacional de cada canal. La información de cada uno de los canales auditados se encuentra resumida en el Rav, un Rav es una medida de escala de la superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula mediante el equilibrio cuantitativo entre operaciones, limitaciones y controles. Tener los Ravs es entender cuánta superficie de ataque está expuesta. En esta escala, 100 Rav es el equilibrio perfecto y cualquier cosa menos es muy poco control y por lo tanto una mayor superficie de ataque. Por otro lado, más de 100 Rav muestra más controles de los que son necesarios, lo que puede significar un problema, ya que los controles a menudo agregan interacciones dentro de un alcance, así como problemas de limitaciones y mantenimiento. El Rav es en realidad múltiples cálculos separados de Porosidad, Controles y Limitaciones, que cuando se combinan mostrarán el tamaño de una superficie de ataque. (ISECOM & Herzog, 2010, p. 63)

Existen dos maneras para calcular el estado actual de la seguridad operacional de cada canal una de manera manual aplicando formulas definidas en la metodología o de manera automatizada utilizando una hoja de cálculo del Rav la cual se puede descargar del sitio web oficial de ISECOM, en esta hoja de cálculo se ingresa los valores numéricos de cada ítem y el resultado se obtendrá de forma automática. Para este trabajo se toma en cuenta la manera automatizada.

A continuación, se mencionan los ítems para el cálculo del Rav:

- Porosidad: Se mide como la suma de Visibilidad, Acceso y Confianza.
- Limitaciones: Vulnerabilidad, Debilidad, Preocupación, Exposición y Anomalía.
- Controles
    - Clase A: Autenticación, Indemnización, Resistencia, Subyugación, Continuidad.
    - Clase B: No-Repudio, Confidencialidad, Privacidad, Integridad y Alarma.

En la tabla 2-2 se puede apreciar de mejor manera todos los ítems y sus relaciones, necesarios para el cálculo del Rav de cada canal que se va a auditar.

Tabla 2-2: Porosidad, Controles y limitaciones en la metodología OSSTMM

Categoría		**Seguridad Operacional (Porosidad)**	**Limitaciones**
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	**Clase A**	Autenticación	Debilidad

		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B	No repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalía

Fuente: (ISECOM & Herzog, 2010, p. 79)
Realizado por: Byron Barragán, 2020

2.2.4.1. Fases de la metodología OSSTMM para el canal humano.

Fase 1: Inducción

Esta fase consta de: Revisión de la postura, Logística y Verificación de detección activa. A continuación, se explica brevemente cada una.

Revisión de la postura

Los estudios iniciales de la postura incluyen las leyes, la ética, las políticas, los reglamentos de la industria y la cultura política que influyen en los requisitos de seguridad y privacidad para el alcance. (ISECOM & Herzog, 2010, p. 106)

Los puntos que trata son: Políticas, Legislación, Regulaciones, Cultura, Relaciones, Economía y Cultura Regional.

Logística

Preparación del entorno de prueba de canal necesario para evitar errores que conducen a resultados de prueba inexactos. (ISECOM & Herzog, 2010, p. 107). Los puntos que trata son: Equipos de comunicación, Comunicaciones, Tiempo

- Equipos de comunicación: Comunicaciones que proporcionan identificación al receptor, como identificación de llamadas, servicio de FAX, registro de direcciones IP o servidores de correo electrónico.
- Comunicaciones: Idioma
- Tiempo: Zona horaria, horarios de trabajo.

Verificación de detección activa

Determinación de los controles activos y pasivos para detectar una intrusión. (ISECOM & Herzog, 2010, p. 108). Los puntos que tratan son: Monitoreo de canal, Moderación de canales, Supervisión y asistencia de operador.

- Monitoreo de canal: Canales de soporte para los servicios que se prestan en el alcance. Ejemplo: Chat, correo electrónico, etc.
- Moderación de canales: Procedimientos que se llevan a cabo si los canales de soporte presentan fallas o no se encuentran habilitados.
- Supervisión y asistencia de operador: Si se realiza los procedimientos con previa autorización y con el personal adecuado.

Fase 2: Interacción

La fase de interacción cuenta con: Auditoria de la Visibilidad, Verificación de acceso, Verificación de confianza y Verificación de controles.

Auditoria de la visibilidad

Pruebas de enumeración y verificación para la visibilidad del personal con el que es posible la interacción a través de diferentes formas. (ISECOM & Herzog, 2010, p. 109). Los puntos que trata son: Identificación de acceso y enumeración de personal.

- Identificación de acceso: Interacciones con el personal de acceso.
- Enumeración personal: Enumeración de la cantidad de personal o áreas dentro del alcance con acceso autorizado y no autorizado a los activos ejemplo. Cuarto de telecomunicaciones.

Verificación de acceso

Pruebas para la enumeración de puntos de acceso al personal dentro del alcance.(ISECOM & Herzog, 2010, p. 109). Los puntos que trata son: Proceso de acceso, Autoridad, y Autenticación.

- Proceso de acceso: Procesos que se debe realizar para acceder a los activos.
- Autoridad: Determinar hasta donde puede acceder una persona con permisos de autoridad y los métodos utilizados.

- Autenticación: Enumeración de las deficiencias del personal para que solo las partes identificables, autorizadas y previstas tenga acceso.

Verificación de confianza

Pruebas de confianza entre el personal dentro del alcance donde la confianza se refiere al acceso a la información o los activos físicos. (ISECOM & Herzog, 2010, p. 110). Los puntos que trata son: Tergiversación, Fraude, no dirección, Phishing, Abuso de recursos, In Terrorem.

Todos estos puntos tratan sobre requerimientos y como acceder a los activos en el alcance. Para Fraude y Phishing se trata de documentar que pasa si se presentan requerimientos fraudulentos o intentos de acceder a los activos de distintas formas a las establecidas.

Verificación de controles (Controles de clase B)

Pruebas para enumerar los tipos de controles utilizados para proteger el valor de los activos. (ISECOM & Herzog, 2010, p. 111). Estos puntos son los controles definidos de clase B.

- No repudio: Deficiencias que el personal de acceso posee que desafían al repudio.
- Confidencialidad: Deficiencias de la comunicación con el personal utilizando líneas seguras, cifrado, interacciones personales "silenciadas" o "cerradas" para proteger la confidencialidad de los activos.
- Privacidad: Deficiencias de todos los segmentos de comunicación con el personal a través de un canal para proteger la privacidad.
- Integridad: Deficiencias en todos los segmentos de comunicación con el personal, donde los activos se transportan a través de un canal para proteger y asegurar que la información o los activos físicos no se puedan cambiar.
- Alarma: Sistemas que proporcionan seguridad física.

<u>Fase 3: Indagatoria o Investigación</u>

Esta fase consta de: Verificación de Procesos, Verificación de Entrenamiento, Validación de la Propiedad, Revisión de Segregación, Verificación de Exposición y Exploración de Inteligencia Competitiva.

Verificación de procesos

Pruebas para examinar el mantenimiento de la conciencia de seguridad funcional del personal en los procesos, se relaciona con la revisión de la postura. (ISECOM & Herzog, 2010, p. 112). Los puntos que trata son: Mantenimiento, Desinformación, Diligencia e indemnización.

- Mantenimiento: Revisión de la conciencia de los trabajadores hacia la seguridad. Se relaciona con la revisión de postura.
- Desinformación: En qué medida las notificaciones de seguridad del personal y las noticias de seguridad se pueden ampliar o alterar con información errónea.
- Diligencia: Brechas entre la práctica y los requisitos según lo determinado en la revisión de postura.
- Indemnización: Abuso o elusión de la política del empleado, seguro, no divulgación, no competencia, contratos de responsabilidad, o renuncias con todo el personal de acceso.

Verificación de entrenamiento

Pruebas para examinar la capacidad de eludir o interrumpir la educación y la capacitación sobre la conciencia funcional de la seguridad en el personal. (ISECOM & Herzog, 2010, p. 113). Los puntos que trata son: Mapeo Educativo, Interrupción de Política, Mapeo de Conciencia, Hijacking.

- Mapeo educativo: Cada qué periodo se realiza cursos educativos o capacitaciones acerca de seguridad dirigido a todos los trabajadores.
- Interrupción de política: Auto vigilancia del personal por la interrupción o la no conformidad de la política de seguridad.
- Mapeo de conciencia: Brechas en los procesos de capacitación.
- Hijacking: Hasta qué punto una persona no oficial proporciona información errónea sobre política de seguridad.

Validación de la propiedad

Pruebas para examinar la información y la propiedad física disponible o proporcionada por personal que puede ser ilegal o poco ético. (ISECOM & Herzog, 2010, p. 114). Los puntos que trata son: Compartir, Mercado negro y Canales de venta.

- Compartir: Verificación del grado en que la propiedad con licencia individual, privada, falsificada, reproducida, no libre o no abierta se comparte entre el personal. Se relaciona con la revisión de la postura.

- Mercado negro: La medida en que la propiedad con licencia individual, privada, falsificada, reproducida, no libre o no abierta se promociona, comercializa o vende entre el personal o la organización.
- Canales de venta: Negocios públicos, fuera de alcance, subastas o ventas de propiedades que brinden información de contacto a través de canales que se originen dentro del alcance.

Revisión de segregación

Pruebas para la separación apropiada de los activos de información privada o personal de la información comercial. (ISECOM & Herzog, 2010, p. 115). Los puntos que tratan son: Asignación de contención de privacidad, Información evidente y divulgación.

- Asignación de contención de privacidad: Guardias de los activos de información privada dentro del alcance, qué información se almacena, cómo y dónde se almacena la información, y a través de qué canal se comunica la información. Se relaciona con la revisión de la postura
- Información evidente y divulgación: Información con respecto a la persona responsable de los activos. Tales como nombres, raza, sexo, religión, días de vacaciones, páginas web personales, hojas de vida publicadas, afiliaciones personales, consultas de directorio, sucursales bancarias, registro electoral.
- Limitaciones: Revisión de las fases anteriores conteo de los errores y anomalías. Esta se divide en vulnerabilidades, debilidades, Preocupación, Exposición y Anomalías. Se aplica para el cálculo final de RAV.

Verificación de exposición

Pruebas para descubrir información que proporciona o conduce a un acceso autenticado o permite el acceso no deseado a múltiples ubicaciones con la misma autenticación. (ISECOM & Herzog, 2010, p. 116) Los puntos que tratan son: Mapeo de exposición y Perfilado.

- Mapeo de exposición: Revisión de información personal con respecto a la organización, como organigramas, títulos de personal clave, etc.
- Perfilado: Perfiles, habilidades de los empleados, las escalas salariales, la información del canal y la puerta de enlace, las tecnologías y la dirección.

Exploración de inteligencia competitiva

Pruebas de búsqueda de propiedades que pueden analizarse como inteligencia empresarial. (ISECOM & Herzog, 2010, p. 116). Los puntos que tratan son: Molienda comercial, Entorno empresarial y organizacional.

- Molienda comercial: Responsables de los activos comerciales dentro del alcance, qué información se almacena, cómo y dónde la información se almacena y a través de qué canales se comunica la información personal.
- Entorno empresarial: Detalles comerciales del personal de la puerta de enlace individual, tales como alianzas, socios, principales clientes, proveedores, distribuidores, inversores, etc.
- Entorno organizacional: Tipos de revelaciones de activos comerciales de los guardianes en operaciones, procesos etc.

Fase 4: Intervención

Esta fase consta de: Verificación de cuarentena, Privilegios de auditoria y continuidad de servicio**.**

Verificación de cuarentena

Pruebas para verificar el correcto posicionamiento y contención de contactos agresivos u hostiles en los puntos de entrada. (ISECOM & Herzog, 2010, p. 117). Los puntos que trata son: Identificación del proceso de contención y Niveles de contención.

- Identificación del proceso de contención: Métodos y procesos de cuarentena en las puertas de acceso en todos los canales para contactos agresivos y hostiles como vendedores, etc.
- Niveles de contención: Estado de contención, el período de tiempo y todos los canales donde la interacción con los responsables tiene métodos de cuarentena.

Privilegios de auditoria

Pruebas en las que se proporcionan credenciales al usuario y se otorga permiso para probar con esas credenciales. (ISECOM & Herzog, 2010, p. 117). Los puntos que trata son: Subyugación, Identificación, Autorización, Escalamiento de permisos y Discriminación.

- Subyugación: Deficiencias de los activos comunicados a través de canales donde esos controles no son necesarios.

Continuidad de servicio

Determinar y medir la resistencia de los controladores de acceso dentro del alcance a cambios excesivos u hostiles diseñados para causar fallas en el servicio. (ISECOM & Herzog, 2010, p. 118).

- Resistencia: Deficiencias en todos los canales del personal dentro del alcance mediante el cual eliminar o silenciar al personal de la puerta de enlace permitirá el acceso directo a los activos.
- Continuidad: Deficiencias de todo el personal con respecto a los retrasos en el acceso y el tiempo de respuesta del servicio.

Todo lo resumido anteriormente se puede representar en un diagrama mostrado en la figura 3-2

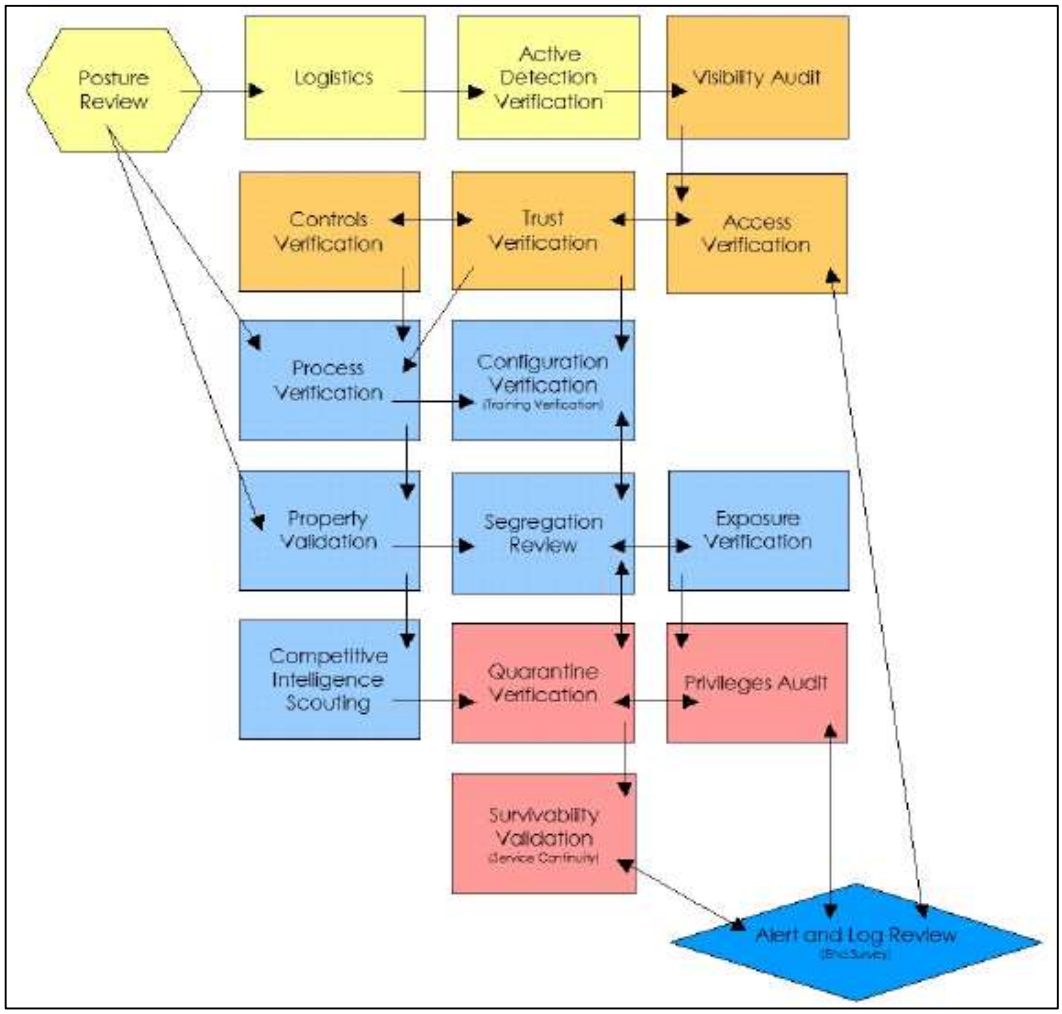


Figura 3-2: Diagrama de la metodología OSSTMM
Fuente: (ISECOM & Herzog, 2010, p. 103)

2.2.4.2. Adaptación de la metodología OSSTMM para su aplicación en el canal humano en el edificio de la FIE-ESPOCH.

Para la auditoria del canal humano se ha propuesto un análisis propio que incluye: actividades evaluadas en la red de campus académica y pruebas de la metodología.

Fase 1: Inducción

Revisión de la postura

Los puntos para considerar en la adaptación son: Políticas, Legislación y regulaciones, Cultura, Relaciones. No se tomó en cuenta: Economía y cultura regional

- Economía: No se tiene acceso a la información de salarios de los trabajadores en el escenario.
- Cultura regional: No influye la cultura regional o jerarquía

Logística

- Equipos de comunicación: En el edificio donde se aplica la metodología solo cuenta con servicio de internet e identificador de llamadas, no cuenta con servicio de FAX, registro de direcciones IP, credenciales de localización o servidores de correo electrónico etc.
- Comunicaciones: español.
- Tiempo: Se revisa zona horaria, los horarios de clase cambian de acuerdo con cada profesor según el periodo por lo que no se tomó en cuenta; sector administrativo el horario está completamente definido.

Verificación de detección activa

El edificio solo cuenta con servicio de acceso a internet y telefonía. El soporte técnico y los diferentes inconvenientes son atendidos por los ingenieros encargados de los laboratorios del edifico. No se toma en cuenta Verificación de detección activa en la adaptación por lo antes mencionado.

La fase de inducción se realizará con una lista de verificación de la seguridad abarcando todos los puntos propios de la fase.

Fase 2: Interacción

En esta fase se busca calcular el valor de la seguridad operacional o porosidad y los valores de los controles de interacción clase A y B

Auditoria de la visibilidad

- Identificación de acceso: Se trata de las interacciones de los técnicos con los estudiantes, docentes y administrativos además de los procesos que manejan.
- Enumeración personal: El personal dentro del alcance con acceso autorizado y no autorizado a los activos, en este caso el cuarto de telecomunicaciones, laboratorios, aulas y equipos.

Verificación de acceso

- Proceso de acceso: Relacionado con los procesos y métodos para acceder a los activos del edificio por lo que se contabiliza los escenarios donde puede ocurrir una interacción sin que se necesite una autorización.
- Autoridad: Solo los técnicos pueden prestar los activos del edificio por lo que este punto no se toma en cuenta.
- Autenticación: En este punto se va a contabilizar los métodos por los cuales se puede interactuar con el personal de recepción y acceso. Este es un control de clase A.

Verificación de confianza

Todos estos puntos hacen referencia a procesos, pruebas de requerimientos y como acceder a los activos en el edificio. Para Fraude y Phishing los documentos de solicitación de préstamo de laboratorios son redactados por las secretarias de cada escuela por lo que no existe algún tipo de fraude; no se toma en cuenta estos dos puntos. El abuso de los recursos es un punto importante, los técnicos entran en esta categoría. Se resumió en el conteo de los procesos para que los estudiantes ingresen a los activos.

Verificación de controles (Controles de clase B)

Los puntos que se manejan en verificación de controles se basan en las actividades que se realiza diariamente en el edificio. A continuación, se presenta cada punto y lo que toma en cuenta para hacer un conteo. Al ser estos controles de clase B es importante saber que se va a contar para le calculo final de la seguridad operacional del canal humano.

- No repudio: Contabilizar quiénes del personal de recepción identifican y registran adecuadamente el acceso o las interacciones con los activos para obtener evidencia específica para impugnar el repudio del edifico.
- Confidencialidad: Contabilizar los segmentos de comunicación con los encargados dentro del alcance que son eficientes.
- Privacidad: Contabilizar los métodos eficientes para asegurar este control.
- Integridad: Contabilizar los métodos eficientes aplicados en el alcance para proteger y asegurar que la información de los activos físicos no pueda ser cambiados, conmutados, redirigidos o invertidos sin que las partes involucradas tengan conocimiento de ello.
- Alarma: Contabilizar los sistemas de advertencia en caso de alguna emergencia.

Fase 3: Indagatoria o Investigación

Verificación de procesos

- Mantenimiento: Se relaciona con la revisión de postura. En la lista de verificación de la seguridad se indaga acerca de cursos de capacitación sobre seguridad hacia el personal (Estudiantes docentes y administrativos).
- Desinformación y Diligencia: No se toma en cuenta este punto ya que no existe cursos de capacitación de seguridad, solo cursos impartidos por el proveedor de servicios. (Esta información se obtuvo en la lista de verificación de la seguridad).
- Indemnización: Contabilizar los documentos legales a los que deben someterse los estudiantes o docentes del alcance para la utilización de ciertos activos o información. Se debe indicar que es un control de clase A.

Verificación de entrenamiento

En general se refiere a la capacitación acerca de la seguridad informática a los trabajadores en este caso docentes y personal técnico, como se mostró en la fase de inducción no existe capacitación más que por el proveedor de servicios y no en seguridad. Por lo que no se toma en cuenta.

- Interrupción de política: En el edificio cuenta con cámaras que están instaladas en los laboratorios mas no en las aulas de clases.
- Hijacking: No aplica ya que la cantidad de estudiantes es grande.

Validación de la propiedad

- Mercado negro: Todos los programas utilizados en los laboratorios son distribuidos a los estudiantes si se solicita, solo algunos de estos programas tienen licencias.
- Canales de venta: Al ser distribuidos abiertamente no se tiene control de lo que el estudiante hace con el software.

Revisión de segregación

- Asignación de contención de privacidad: Como se maneja la privacidad en el alcance.
- Limitaciones: Revisión de las fases anteriores conteo de los errores y anomalías. Esta se divide en vulnerabilidades, debilidades, Preocupación, Exposición y Anomalías. Se aplica para el cálculo final de RAV.

Verificación de exposición

- Mapeo de exposición: Esta información no se puede proporcionar.
- Perfilado: Esta información no se puede proporcionar.

Por esta razón Verificación de exposición no se toma en cuenta para la adaptación de la metodología del canal humano.

Exploración de inteligencia competitiva

Este punto está más relacionado a empresas debido a esto no se toma en cuenta ya que la ESPOCH es una institución educativa.

Fase 4: Intervención

Verificación de cuarentena

No se toma en cuenta para la adaptación de la auditoria del canal humano, no aplica a un ambiente educativo.

Privilegios de auditoria

- Subyugación: es un control de clase A, contabilizar los métodos por los cuales se puede interactuar con el personal de recepción.

- Identificación, Autorización, Escalamiento de permisos, discriminación; Todo se realiza con previa identificación. En concordancia con la fase de inducción.

Continuidad de servicio

- Resistencia: Contabilizar los encargados que permiten acceder sin autorización a los activos del cuarto de telecomunicaciones.
- Continuidad: Contabilizar el total de encargados que genera conflictos en cuanto a retrasos de acceso. Este es un control de clase A

El siguiente diagrama indica cómo se va a realizar la auditoria en el canal humano en el edificio de la FIE-ESPOCH.

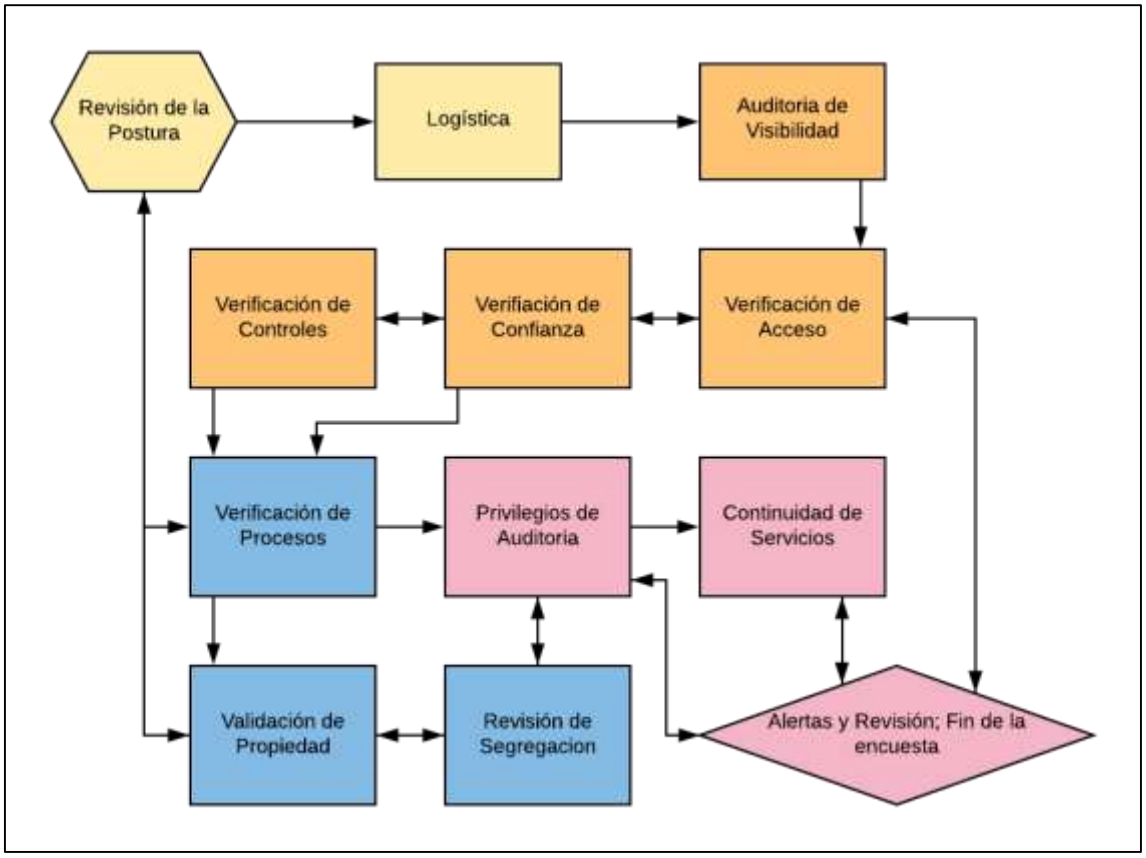


Gráfico 2-2: Adaptación de la metodología OSSTMM para el canal humano en la FIE-ESPOCH
Realizado por: Byron Barragán, 2020

En la figura 4-2, el color amarillo representa la fase de inducción, donde se determina el estado actual de la seguridad en la organización. En esta fase tenemos Revisión de la postura y logística.

El color naranja representa la fase de interacción, en esta fase se busca calcular el valor de la seguridad operacional o porosidad, así como también los valores de los controles de interacción clase A y B, para el cálculo de la porosidad se toma en cuenta la auditoria de la visibilidad, verificación de acceso y verificación de confianza como se observa en la tabla 14-3, sin embargo, no se especifica cuáles son debido a acuerdos de confidencialidad para realizar el presente trabajo. Para el cálculo de los controles de interacción de clase A se realizan conteos que se pueden encontrar en la tabla 15-3 donde los controles son: autenticación, indemnización, resistencia, subyugación y continuidad.

Para el cálculo de los controles de interacción clase B tenemos verificación de procesos como alarmas e interacciones con ellas y también verificación de controles. Este conteo se muestra en la tabla 16-3. Los controles de clase B son el no repudio, confidencialidad, privacidad, integridad.

El color Azul representa la fase indagatoria, en esta fase se busca calcular el valor de las limitaciones, para este cálculo tenemos revisión de segregación, verificación de procesos y validación de propiedad, se tiene en cuenta los valores de vulnerabilidad, debilidad, preocupación exposición y anomalías como se observa en la tabla 17-3.

Una vez calculado los valores totales se ingresa en la hoja de cálculo proporcionada por la página web de ISECOM y se obtiene como resultado el valor del RAV de la seguridad en el canal auditado, y la fase de intervención entra en desarrollo, en esta fase lo que se hace es una revisión de todos los valores obtenidos y se interpreta el resultado del RAV para generar acciones correctivas basado en la fase de inducción en verificación de accesos o también generar alertas según el resultado obtenidos gracias a los privilegios de auditoria.

2.2.4.3. Adaptación de la metodología OSSTMM para su aplicación en el canal de red de datos en el edificio de la FIE-ESPOCH.

Para la auditoria del canal de red de datos se ha propuesto un análisis propio que incluye: actividades evaluadas en la red de campus y pruebas de la metodología.

Fase 1: Inducción

Esta fase consta de: Revisión de la postura, Logística y Verificación de detección activa. La fase de inducción del canal red de datos se desarrolló en la fase de inducción del canal humano teniendo en cuenta una lista de verificación de seguridad realizado al DTIC, esta lista de

seguridad abarca temas de la fase de inducción del canal de red de datos. En esta fase se toma en cuenta revisión de la postura y logística.

Fase 2: Interacción

La fase de interacción cuenta con: Auditoria de la visibilidad, Verificación de acceso, Verificación de confianza y Verificación de controles.

Auditoria de la visibilidad

Encuesta de red:

- Identifique el perímetro del (los) segmento (s) de la red.
- Use un sniffer de la red para identificar los protocolos emanantes en la red.
- Verificar el broadcast requests difusión y las respuestas de todos los objetivos.
- Verificar y examinar el uso del tráfico y los protocolos de enrutamiento para todos los destinos
- Verifique las respuestas de ICMP de todos los objetivos.
- Rastree la ruta los paquetes TCP a todos los destinos para los puertos SSH, SMTP, HTTP y HTTPS.
- Rastree la ruta de los paquetes UDP a todos los destinos para los puertos DNS y SNMP.

Enumeración:

- Verifique las respuestas de las solicitudes de paquetes UDP a diferentes puertos.
- Verifique las respuestas de solicitud de servicio a los puertos de malware conocidos o creados.
- Verifique las respuestas de las solicitudes de paquetes TCP a diferentes puertos.

Verificación de acceso

Red:

- Manipular el servicio de red y el enrutamiento para acceder a restricciones pasadas dentro del alcance. (Test de alcance)
- Solicite servicios de troyanos comunes y conocidos que utilizan UDP, TCP o ICMP para las conexiones.

Servicios:

- Escaneo de puertos (descubrir puertos abiertos)

Autenticación:

- Enumere los accesos que requieren autenticación y documente todos los privilegios descubiertos que se pueden usar para proporcionar acceso.
- Verifique la solidez de la autenticación a través de descifrar las contraseñas.

Verificación de confianza

Spoofing:

- Pruebe las medidas para acceder a la propiedad dentro del alcance mediante la suplantación.

Abuso de recursos:

- Comprobar cómo se utilizan los recursos.

Verificación de controles

No repudio:

- Enumerar y probar el uso o las deficiencias de los demonios y los sistemas para identificar adecuadamente y registrar el acceso o las interacciones a la propiedad para obtener evidencia específica para desafiar el repudio.
- Identificar los métodos de identificación que derrotan el repudio.

Confidencialidad:

- Verificar los métodos aceptables utilizados para la confidencialidad.

Privacidad:

- Enumere los servicios dentro del alcance de las comunicaciones o los activos transportados mediante el uso de herramientas para proteger la privacidad de la interacción y el proceso de proporcionar activos solo a aquellos que están autorizados.

Integridad:

- Enumere las deficiencias de integridad cuando utilice un proceso documentado, firmas, cifrado, hash o marcas para garantizar que el activo no se pueda cambiar, redirigir o revertir sin que las partes involucradas lo conozcan.

<u>Fase 3: Investigación</u>

Verificación de procesos

Indemnización:

- Documentar y enumerar los objetivos y servicios que están protegidos contra el abuso o elusión de la póliza del empleado, están asegurados por robo o daños, o usan responsabilidad y exenciones de responsabilidad de permisos.

Verificación de la configuración

Mapa de Limitaciones

- Compruebe si hay servicios / funciones innecesarios o no utilizados disponibles.
- Compruebe las credenciales por defecto.
- Identifique si alguna vulnerabilidad conocida reside en los sistemas. (escáner de vulnerabilidades)

Validación de la propiedad

Mercado negro

- Verifique hasta qué punto la propiedad o la organización promueve, comercializa o vende propiedad con licencia individual, privada, falsificada, reproducida, no gratuita o no abierta.

Revisión de la segregación

Divulgación:

- Verificar que la información privada y la propiedad intelectual confidencial, como documentos, contratos de servicio, claves de SO / Software, etc. no estén disponibles para nadie sin los privilegios adecuados.

Limitaciones:

- Verifique que existan consideraciones de diseño o alternativas de canal para que las personas con limitaciones físicas interactúen con el objetivo.

Verificación de exposición

Enumeración de la exposición:

- Enumere las exposiciones del sistema, servicio y aplicación que detallan el diseño, tipo, versión o estado de los objetivos o de recursos fuera del alcance, como por ejemplo de publicaciones o fugas.

<u>Fase 4: Intervención</u>

Verificación de cuarentena

Identificación del proceso de contención:

- Identifique métodos de cuarentena para contactos agresivos y hostiles, como malware, puntos de acceso no autorizados, dispositivos de almacenamiento no autorizados, etc.

Niveles de contención:

- Verificar las medidas de detección presentes para la detección de intentos de acceso a los recursos protegidos.

Validación de supervivencia

Resistencia:

- Verifique los puntos únicos de falla (puntos de estrangulamiento) en la infraestructura donde el cambio o la falla pueden causar una interrupción del servicio.

Continuidad:

- Enumere las deficiencias de todos los objetivos con respecto a los retrasos de acceso y los tiempos de respuesta del servicio a través de sistemas de respaldo o el cambio a canales alternativos.

Revisión de alertas y registros

Alarma:

- Verifique el uso de un sistema de advertencia, registro o mensaje localizado o de alcance amplio para cada puerta de acceso a través de cada canal donde el personal detecte una situación sospechosa como elusión, ingeniería social o actividad fraudulenta.

La siguiente figura indica cómo se va a realizar la auditoria del canal de red de datos en el edificio de la FIE-ESPOCH.

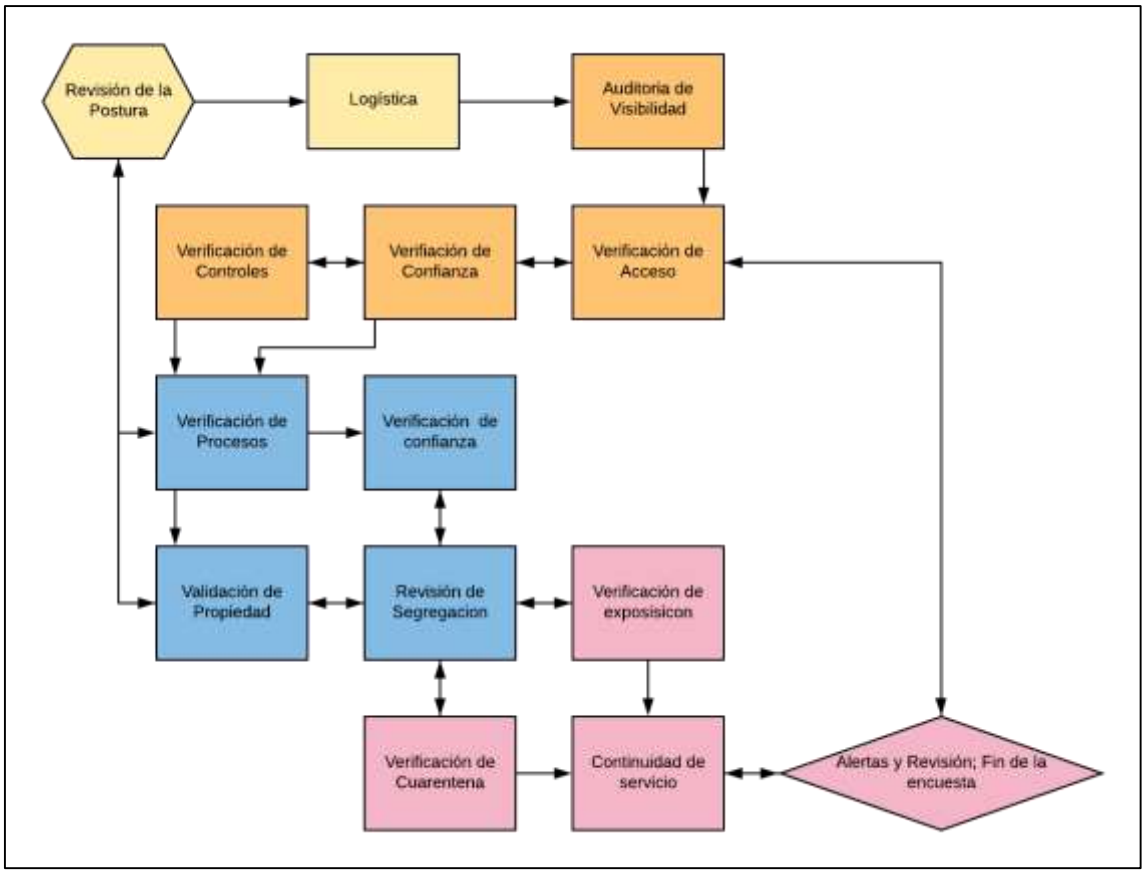


Gráfico 3-2: Adaptación de la metodología OSSTMM para el de red de datos en la FIE-ESPOCH
Realizado por: Byron Barragán, 2020

En la figura 5-2, el color amarillo representa la fase de inducción, donde se determina el estado actual de la seguridad en la organización. En esta fase tenemos Revisión de la postura y logística. Como se mencionó anteriormente esta fase se la realiza al igual que la auditoria del canal humano.

El color naranja representa la fase de interacción, en esta fase se busca calcular el valor de la seguridad operacional o porosidad, así como también los valores de los controles de interacción clase A y B, para el cálculo de la porosidad se toma en cuenta la auditoria de la visibilidad, verificación de acceso y verificación de confianza como se observa en la tabla 19-3, sin embargo, por el mismo motivo que en la auditoria del canal humano no se especifica cuáles son por temas de confidencialidad para la realización de este trabajo. Para el cálculo de los controles de interacción de clase A se realizan conteos que se pueden encontrar en la tabla 20-3 donde los controles son: autenticación, indemnización, resistencia, subyugación y continuidad.

Para el cálculo de los controles de interacción clase B tenemos verificación de procesos como alarmas e interacciones con ellas y también verificación de controles. Este conteo se muestra en

la tabla 21-3. Los controles de clase B son el no repudio, confidencialidad, privacidad, integridad.

El color Azul representa la fase indagatoria, en esta fase se busca calcular el valor de las limitaciones, para este cálculo tenemos revisión de segregación, verificación de procesos, verificación de confianza y validación de propiedad, se tiene en cuenta los valores de vulnerabilidad, debilidad, preocupación exposición y anomalías como se observa en la tabla 22-3.

Una vez calculado los valores totales se ingresa en la hoja de cálculo proporcionada por la página web de ISECOM y se obtiene como resultado el valor del RAV de la seguridad en el canal auditado, y la fase de intervención entra en desarrollo, en esta fase lo que se hace es una revisión de todos los valores obtenidos esto en los puntos de verificación de cuarentena, verificación de exposición después se interpreta el resultado del RAV para generar acciones correctivas basado en la fase de inducción en verificación de accesos o también generar alertas según el resultado obtenidos.

2.2.5. Nexpose como escáner de vulnerabilidades de red en el edificio de la FIE-ESPOCH

Para encontrar las vulnerabilidades se va a utilizar el escáner Nexpose desarrollado por Rapid7. Este escáner cuenta con una interfaz gráfica de usuario vía portal web, es aquí donde se puede crear sitios para escaneo, programar análisis y gestionar las vulnerabilidades que se encuentren además de generar reportes para una exposición de la situación actual de la seguridad que se encuentra la organización. Concretamente en el edifico de FIE-ESPOCH se instaló el escáner en una máquina virtual con distribución CentOS 7 la misma máquina que se utiliza para el análisis del tráfico en las Vlans. Una vez instalado se define cada sitio de escaneo es decir un sitio para cada Vlan, indicando el tipo de escaneo y también dando permisos con las credenciales adecuadas para que el escaneo sea completo. Los resultados se presentan en la interfaz de usuario y se genera un reporte de los resultados para su análisis y gestión.

2.2.5.1. ¿Por qué Nexpose?

El escáner Nexpose se considera como líder en el sector del escaneo de vulnerabilidades debido a extensa y actualizada base de datos de vulnerabilidades de Rapid7. (Villora, 2018 p. 37).
A continuación, se muestra una tabla comparativa de herramientas de escáner de vulnerabilidades de red y de aplicaciones web realizada por Henry Quishpe en su trabajo de titulación. A esta tabla se le suma las características de Nexpose.

Tabla 3-2: Comparación de escáner de vulnerabilidades

Características	Nessus	OpenVas	OWASP	Retina	Nexpose
Licencia	Libre/Pagada	Libre	Libre	Libre/Pagada	Libre/Pagada
Multiplataforma	Si	Si	Si	Si	Si
Tiempo promedio de un análisis	Corto	Largo	Corto	Medio	Largo
Clasificación de vulnerabilidades	Si	Si	Si	Si	Si
Presenta soluciones a las vulnerabilidades	Si	Si	Si	Si	Si
Configuración	Fácil	Fácil	Difícil	Fácil	Fácil
Exportación de resultados	HTML, CSV, Nessus y Nessus data.	PDF, HTML, XML, etc.	PDF, HTML, XML, CSV.	PDF, HTML, XML, etc.	PDF, HTML, XML, CSV. Variedad en reportes.
Programación de escaneos	Si	Si	Si	Si	Si
Soporte	Única empresa	Varias empresas	Varias empresas	Única empresa	Única empresa
Consumo de recursos	Bajo	Medio	Bajo	Medio	Medio
Escaneo a cualquier equipo	Si	Si	No, solo para web	Si	Si

Fuente: (Quishpe, 2016, p. 51)
Realizado por: Byron Barragán, 2020

Para la selección se realiza un análisis de las características que tiene cada herramienta de gestión de vulnerabilidades, entre las características que se evalúan se tiene:
Tipo de licencia, la Tabla 4-2 muestra los tipos de licencia con su respectivo valor.

Tabla 4-2: Valoración considerada para tipos de licencia

Tipo de Licencia	Libre	Libre/Pagada	Pagada
Valoración	3	2	1

Realizado por: Byron Barragán, 2020

Tiene capacidad de funcionar en varias plataformas, la Tabla 5-2 muestra la valoración para esta característica.

Tabla 5-2: Valoración considerada para la característica multiplataforma

Multiplataforma	**Si**	**No**
Valoración	2	1

Realizado por: Byron Barragán, 2020

Integración con la herramienta metasploit, para la explotación de las vulnerabilidades encontradas. La Tabla 6-2 muestra la valoración considerada.

Tabla 6-2: Valoración considerada para la característica Integración con Metasploit

Integración con Metasploit	**Si**	**No**
Valoración	2	1

Realizado por: Byron Barragán, 2020

Tiempo del escaneo, aquí se considera un mayor tiempo de escaneo como mayor valoración ya que se relaciona con la comparación con un repositorio más amplio en vulnerabilidades. La Tabla 7-2 muestra la valoración considerada.

Tabla 7-2: Valoración considerada para la característica Tiempo de escaneo

Tiempo de escaneo	**Corto**	**Medio**	**Largo**
Valoración	1	2	3

Realizado por: Byron Barragán, 2020

Variedad en tipos de reporte que se puede generar con los resultados, la Tabla 8-2 muestra la valoración considerada, esta información es tomada de la página web de la empresa essays Professors en la cual se presenta una comparación entre Nessus y Nexpose. (Essays Professors, 2020)

Tabla 8-2: Valoración considerada para la característica Variedad de reportes

Variedad de reportes	**Si**	**No**
Valoración	2	1

Realizado por: Byron Barragán, 2020

Se evalúa además el contenido de los reportes generados, esta información se tomó de una publicación en la revista Información tecnológica Volumen 24. La Tabla 9-2 muestra la valoración considerada. (Franco et al, 2013, p 13-22)

Tabla 9-2: Valoración considerada para la característica contenido de los reportes

Contenido de los reportes	**Bajo**	**Medio**	**Alto**
Valoración	1	2	3

Fuente: (Franco et al, 2013, p 13-22)
Realizado por: Byron Barragán, 2020

Consumo de recursos por parte de la herramienta, en la Tabla 10-2 se muestra la valoración considerada

Tabla 10-2: Valoración considerada para la característica de consumo de recursos

Consumo de recursos	**Bajo**	**Medio**	**Alto**
Valoración	3	2	1

Realizado por: Byron Barragán, 2020

Mayor número de vulnerabilidades detectadas, esta información se tomó de página web de la empresa essays Professors (Essays Professors, 2020) y la revista Información tecnológica Volumen 24 (Franco et al, 2013, p 13-22). La Tabla 11-2 muestra la valoración considerada.

Tabla 11-2: Valoración considerada para la característica de mayor número de vulnerabilidades detectadas

Mayor número de vulnerabilidades	**Bajo**	**Medio**	**Alto**
Valoración	1	2	3

Realizado por: Byron Barragán, 2020

Considerando las características y las valoraciones mostradas en las tablas desde la 4-2 hasta 11-2 se compara las herramientas: Nexpose considerado como líder según Villora y Nessus su principal competidor, para su aplicación en este trabajo de titulación obteniéndose lo que se muestra a continuación en la Tabla 12-2

Tabla 12-2: Comparación de las características de Nessus y Nexpose

Característica	**Nessus**	**Nexpose**
Licencia	2	2
Multiplataforma	2	2
Integración con Metasploit	1	2
Tiempo de escaneo	1	3
Variedad de reportes	1	2
Contenido de reportes	2	3
Consumo de recursos	3	2
Mayor detección de vulnerabilidades.	1	2
Total	13	18

Realizado por: Byron Barragán, 2020

Como se observa en la Tabla 12-2 la herramienta Nexpose tiene una valoración mayor por lo que se utiliza para un escaneo en el edificio de FIE-ESPOCH y determinar las vulnerabilidades.

Entre las características de Nexpose se puede mencionar la capacidad de funcionar en varias plataformas incluido máquinas virtuales, del mismo modo el análisis y escaneo de vulnerabilidades se en máquinas físicas, virtuales e incluso en la nube.
Nexpose posee una plataforma altamente integrada, con capacidades de gestionar casi todos los aspectos de la seguridad de una empresa. (Quishpe, 2016, p. 40)

Cuenta con extensas bases de datos de vulnerabilidades y un eficiente sistema de puntuación propio además de una interfaz muy amigable e intuitiva. (Quishpe, 2016, p. 41)
Nexpose cuenta con dos versiones una de pago y una libre, para la aplicación en este trabajo se toma en cuenta la versión libre con una versión de prueba de 30 días, cabe indicar que la diferencia entre la versión libre y la versión pagada es la cantidad de activos que puede analizar al mismo tiempo, mientras que la versión pagada puede analizar un número indefinido, la versión libre analiza solo 32, es decir 32 direcciones IP.

Después del escaneo se presenta en la interfaz gráfica los resultados obtenidos, todas las vulnerabilidades encontradas en los equipos del sitio creado. El siguiente paso es generar un reporte de todas las vulnerabilidades obtenidas, Nexpose no se centra en la calidad de los informes, pero muestra la información necesaria para entender el riego al que está expuesto el sitio escaneado. En estos reportes se muestra también las soluciones para las vulnerabilidades encontradas, es con la información de estos reportes que se pretende elaborar la guía de solución para las vulnerabilidades que presenten más riesgo en la red del edificio de la FIE-EPOCH. Es por esto y también la compatibilidad de Nexpose con Metasploit la razón de la elección de Nexpose para el escaneo de la red.

2.2.5.2. Instalación de Nexpose

Nexpose se instala en una máquina virtual de CentOS 7 del servidor utilizado para el análisis de amenazas de las Vlans es decir, en una máquina por Vlan, el proceso de instalación y logeo se lo puede encontrar detallado en la página de Rapid7 https://nexpose.help.rapid7.com/docs/install#section-linux, todos los archivos necesarios para la instalación se los descarga desde la misma página teniendo encuentra el sistema operativo en donde se va a instalar, para este caso Linux. Para obtener una key de prueba de Nexpose por 30 días se debe registrar en Nexpose y la key llegara al correo de registro. Con todos estos requisitos se procede a la instalación donde lo primero que se debe hacer es asegurarnos que el paquete screen este en el sistema, de no ser ese el caso se lo debe instalar con la siguiente línea de comando.

yum install screen

Luego debemos tener el instalador y el archivo de comprobación en el mismo directorio, desde una ventana de terminal ingresar al directorio en donde se encuentran los archivos y ejecutamos reemplazando el nombre del instalador lo siguiente.

md5sum -c <installer_file_name>.md5sum

La respuesta de este comando debe ser OK de no ser así se debe descargar el instalador nuevamente. Luego ejecutar lo siguiente para modificar los permisos del instalador reemplazando con el nombre del instalador.

chmod +x <installer_file_name>

Finalmente se ejecuta el instalador y siga las instrucciones de este indicando las credenciales de logeo.

./<installer_file_name>

Una vez instalado, desde el navegador se conecta a la interfaz de usuario de Nexpose ingresando a https://localhost:3780. Después de ingresar a la interfaz aparecerá un mensaje de inicio de sesión donde se ingresa las credenciales que se indicaron durante la instalación, después de iniciar sesión correctamente ingresa la key de activación enviada al correo y estará listo para configurar y escanear la red.

2.3. Etapa 2: Explotación

En la etapa de explotación se selecciona las vulnerabilidades y amenazas en base a los resultados obtenidos en los análisis del tráfico de la red del edificio, es decir, ataques y amenazas detectadas y, además, el reporte generado por la herramienta Nexpose como resultado de las pruebas de la metodología OSSTMM en el canal de red de datos. En el reporte se tendrá más a consideración las vulnerabilidades que se relacionen a la capa de transporte, vulnerabilidades más comunes y las más riesgosas. De igual manera en el análisis de tráfico se definen los ataques más comunes y se replican en el escenario virtual. Todo esto basado además en lo revisado en la sección 2.2.1 y los resultados de amenazas y vulnerabilidades tratadas en la investigación del grupo SEGINTE.

Debido a que la explotación puede comprometer la seguridad y el estado de los equipos físicos reales en el edificio además de no contar con el permiso adecuado para esta etapa, se decidió realizar la etapa de explotación en un escenario virtual desarrollado en el simulador GNS3 en el cual se encuentren las vulnerabilidades ya seleccionadas previamente. Este proceso sirve como punto de partida para las pruebas acerca de amenazas y vulnerabilidades en escenarios reales controlados del grupo de investigación SEGINTE. La simulación se realiza en una computadora marca Alienware 17 R5 con procesador Intel(R) Core (TM) i9-8950hk CPU @ 2.90 GHz de octava generación con 32 Gb de memoria ram.

2.3.1. Metasploit

Metasploit merece una mención aparte entre los productos de Rapid7, al tratarse del famoso software para tests de penetración de equipos de seguridad ofensiva. Este producto es considerado sin lugar a duda el mejor en su área y es utilizado por todo el mundo por su gran base de datos de exploits proveniente de Rapid7 y su versatilidad para realizar ataques.
(Villora, 2018 p. 37)

Para explotar las vulnerabilidades se usará algunos módulos de metasploit para así hacer ataques según los resultados de los análisis, pruebas y escaneos.

2.4. Etapa 3: Solución

Para la etapa 3: solución se propone una guía de solución indicando pasos a seguir para las vulnerabilidades y amenazas seleccionadas y explotadas en la etapa anterior. Para evaluar la guía se realizará una comparación del antes y después de la aplicación de la guía en el escenario virtual. Se evaluará si se puede explotar o no la vulnerabilidad o amenaza con los valores: Si, No o Se detectó.

CAPITULO III

3. RESULTADOS Y ANÁLISIS

3.1. Resultados de la etapa 1: Determinar Vulnerabilidades

3.1.1. Amenazas detectadas en la red del edificio de la FIE-ESPOCH

La cantidad de amenazas detectadas en las tres Vlans difieren siendo la Vlan Estudiantes la que tiene más variedad de amenazas seguida de la Vlan Docentes y Administrativos, sin embargo, la cantidad de alertas generadas en la Vlan Docentes es mucho mayor con respecto a las otras, esto es debido a que en esta Vlan una amenaza generaba varias alertas lo que indica un ataque continuo que duraba alrededor de una a dos horas, concretamente un troyano criptominero y un malware como se verá más adelante. Esto no se daba en las Vlans Estudiantes y Administrativos siendo esta última en la que menos alertas y amenazas se detectaron.

3.1.1.1. Amenazas detectadas en la VLAN Estudiantes

Para el caso de la Vlan Estudiantes y gracias a la ayuda de la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH, el análisis tuvo una primera prueba el 2 de mayo de 2019 aproximadamente a las 8 AM, se analizó el tráfico durante todo el día con la finalidad de comprobar el funcionamiento, registro de alertas y paquetes. El análisis se hizo en dos periodos; el primero inició el 6 de mayo a las 8 AM y culminó el 7 de junio, el segundo periodo inició el 8 de junio y terminó el 7 de julio, siendo estos periodos los que más carga maneja la red del edifico con un promedio de 77 equipos activos en la Vlan, esta información se puede observar con más detalle en el anexo A. El procedimiento que se siguió es el que se mencionó en el capítulo 2, se obtuvieron los siguientes resultados:

Tabla 1-3: Resumen de paquetes analizados por Snort en la Vlan Estudiantes

Primer Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes recibidos	14985362784	100%
Total paquetes analizados	14221538803	94,90%
Total paquetes Drop	763823981	5,09%
Segundo Periodo		
Total paquetes recibidos	12825235869	100%
Total paquetes analizados	12662984676	98,73%
Total paquetes Drop	162251193	1,26%

Realizado por: Byron Barragán, 2020

En la tabla 1-3 se observa la cantidad de paquetes que recibió Snort de los cuales en el primer periodo analizó el 94,90% teniendo un porcentaje de drop de paquetes de 5,09% este porcentaje relativamente alto de drop de paquetes es debido a que Snort por defecto tiene configurado una longitud de cola predeterminada y algunos paquetes son demasiado grandes en data excediendo este límite haciendo que Snort haga un esfuerzo extra para analizar el paquete y en algunos casos se descarta haciendo que en consola aparezca una mensaje que indica la presencia de paquetes demasiado grandes para el análisis. En el segundo periodo se añadió más reglas registradas de usuario Snort al archivo de configuración y además se aumentó la longitud de cola predeterminada, concretamente se duplicó utilizando el comando ***cc set ips snortsettings max_queued_bytes 2097152*** gracias a esto el porcentaje de drop de paquetes de este periodo bajó a 1,26% analizando el 98,73% de los paquetes recibidos por Snort. La información detallada de este registro de paquetes se puede encontrar en el anexo B.

Snort además de mostrar una estadística de paquetes analizados también muestra la cantidad de paquetes analizados por protocolo, teniendo en cuenta la capa de transporte se registró la cantidad de paquetes TCP, UDP, TCP6, UDP6 y su porcentaje del total de paquetes analizados, de igual manera esto se puede encontrar en el anexo B. En el anexo C se muestra como Snort presentaba los resultados del análisis. En la tabla 2-3 se encuentra un resumen.

Tabla 2-3: Resumen de paquetes analizados de la capa de transporte en la Vlan Estudiantes

Primer Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes TCP	11585999571	77,32%
Total paquetes UDP	1279268131	8,54%
Total paquetes TCP6	875117340	5,84%
Total paquetes UDP6	199491190	1,33%
Segundo Periodo		
Total paquetes TCP	11178320367	87,16%
Total paquetes UDP	576667337	4,50%
Total paquetes TCP6	255697924	1,99%
Total paquetes UDP6	203551224	1,59%

Realizado por: Byron Barragán, 2020

La cantidad de alertas se registró todos los días a las 9 AM, cabe indicar que las alertas de los fines de semana se registraban los lunes, así como también la cantidad de paquetes que se analizaron, sin embargo, no se presentaron alertas a excepción del sábado 19 de mayo en donde se registró una, esta alerta sumada a las 6 que se registraron el día 2 de mayo suman un total de 985 para el primer periodo. En el segundo periodo se registró 21 alertas el sábado 22 de junio y se las sumo al día 24 de junio, estas alertas en conjunto con las demás registradas suman 123 para el segundo periodo. En la tabla 3-3 y la tabla 4-3 se presenta un resumen de las alertas

registradas por día en el primer periodo y segundo periodo respectivamente. En el anexo D se encuentra esta información más detallada.

Tabla 3-3: Resumen de alertas registradas en la Vlan Estudiantes en el primer periodo

Semana 1		**Semana 2**		**Semana 3**		**Semana 4**		**Semana 5**	
Fecha	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**
06/05	157	13/05	3	20/05	62	27/05	4	03/06	4
07/05	41	14/05	363	21/05	20	28/05	2	04/06	1
08/05	60	15/05	14	22/05	11	29/05	4	05/06	6
09/05	3	16/05	3	23/05	5	30/05	2	06/06	13
10/05	194	17/05	1	24/05	Feriado	31/05	5	07/06	0
Total	**455**	**Total**	**384**	**Total**	**98**	**Total**	**17**	**Total**	**24**

Realizado por: Byron Barragán, 2020

Tabla 4-3: Resumen de alertas registradas en la Vlan Estudiantes en el segundo periodo

Semana 1		**Semana 2**		**Semana 3**		**Semana 4**		**Semana 5**	
Fecha	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**
10/06	0	17/06	1	24/05	27	01/07	5	06/07	0
11/06	0	18/06	6	25/05	3	02/07	1	07/07	0
12/06	35	19/06	11	26/05	1	03/07	0	08/07	0
13/06	5	20/06	13	27/05	1	04/07	0		
14/06	9	21/06	2	28/05	3	05/07	0		
Total	**49**	**Total**	**33**	**Total**	**35**	**Total**	**6**	**Total**	**0**

Realizado por: Byron Barragán, 2020

Como se puede notar la cantidad de alertas registradas en el segundo periodo disminuyó considerablemente en comparación al primer periodo, esto se da porque el periodo académico estaba por terminar por lo que los laboratorios fueron utilizados para evaluaciones finales a los estudiantes mas no para impartir clases. Debido a estos se detuvo el análisis ya que la ESPOCH entro en receso académico.

Las amenazas que se registraron son variadas en esta Vlan, en general se registró presencia de malware, troyanos, archivos basura, uso de exploit y ejecución de scripts maliciosos los cuales fueron detectados por Snort en el tráfico de la Vlan. Las direcciones IP que se registraron fueron distintas, es decir los objetivos fueron distintas computadoras conectadas en la Vlan Estudiantes. En algunos casos una vez que se registraban las alertas estas continuaban mostrándose en pantalla por lo que se registraba una hora de inicio y fin del ataque independientemente de la cantidad de alertas que aparecieron en pantalla ya que pertenecían al

mismo ataque, un ejemplo es el que ocurrió el 14 de mayo siendo el día con mayor número de alertas registradas en primer periodo y el día 12 de junio para el segundo periodo. En la tabla 5-3 se muestra un resumen de todas las amenazas detectadas por Snort en el periodo con su respectivo identificador de alerta de Snort.

Tabla 5-3: Resumen de amenazas registradas en la Vlan Estudiantes en el primer periodo

Identificador	Significado	Descripción
1-40357:3	Troyano Instantaccess.exe	Redirige a un sitio malicioso que muestra advertencias que indican que su computadora está infectada y que necesita ejecutar el análisis instant-access.exe de inmediato.
1-31046:6	Exploit kit	Este evento se genera cuando una estructura de URL coincide con la estructura utilizada por el kit de explotación de Angler.
1-43459:2	Malware Win.Trojan.Doublepulsar	Implementación del Backdoor Doublepulsar, se puede utilizar para ejecutar malware en la maquina víctima.
Sin identificar	Gran afluencia de paquetes demasiados grandes.	Snort no puede analizar debido a su configuración de cola predeterminada.
1-46237:1	Troyano Criptominero Miner64	Es un archivo ejecutable que forma parte de BitcoinMiner desarrollado por Ufasoft. Este evento se genera cuando la muestra del minero se ha descargado y ejecutado en la PC infectada.
1-45549:1	Troyano Criptominero XMRig	Este evento se genera cuando XMRig intenta iniciar sesión en una API de grupo de minería jsonrpc.
1-48080:1	Troyano Ramnit	Este evento se genera cuando se detecta Win.Trojan.Ramnit en una red. El troyano Ramnit hace que los equipos infectados operen como una botnet centralizada, aunque su arquitectura implica la división en otras redes independientes.
1-46486:1	Troyano LittleInstaller	Este evento se genera cuando una computadora con Slimware instalado se comunica con el servidor de control para actualizaciones. Provoca anuncios no deseados.
1-41573:4	Intento de robo de información utilizando vulnerabilidades de Microsoft Edge	Microsoft Edge permite a los atacantes remotos obtener información confidencial a través de

		un sitio web diseñado, también conocido como "Vulnerabilidad de divulgación de información de Microsoft Edge". Esta vulnerabilidad se asocia a windows 10
1-41337:2	Malware Sysch	Este evento se genera cuando se detecta actividad relacionada con malware. Una aplicación que realiza secretamente otras acciones que afectan la información personal o confidencial almacenada en el dispositivo, y / o el control del dispositivo. Está asociado con el sistema operativo Android.
1-40356:3	Troyano Instantaccess.exe en su versión antigua	Redirige a un sitio malicioso que muestra advertencias que indican que su computadora está infectada y que necesita ejecutar el análisis instant-access.exe de inmediato.
1-35549:1	Malware Troyano ZeuS	Este troyano es utilizado para instalar el ransomware CryptoLocker en una maquina víctima.
1-35030:1	Troyano Zbot o Zeus, indistintamente de su versión	Una versión del malware troyano Zeus. Este troyano es utilizado para instalar el ransomware CryptoLocker en una maquina víctima.
1-25074:1	Troyano Banker	Troyanos que roban información bancaria de un sistema afectado.
1-23605:12	Archivo malicioso.	Denominado Armadillo, poca información acerca de esta alerta se sabe que es de origen ruso
1-47102:1	Uso de Exploit	Este evento se genera cuando un atacante intenta explotar una vulnerabilidad de confusión de tipo en Microsoft Edge o CVE-2018-8298
1-46659:2	Uso de Exploit	Intento de explotar un doble gratis en Adobe Acrobat Reader.
1-32691:1	Uso de script	Intento de denegación de servicio utilizando internet Explorer

Realizado por: Byron Barragán, 2020

Al revisar la tabla 5-3 se observa variedad en las amenazas, destacando el intento de ataque de denegación de servicios que se registró el 30 de mayo, el ataque para la ejecución del Backdoor Doublepulsar explotando la vulnerabilidad del protocolo SMB en todas sus versiones que a su vez está relacionado con ransomware y también las amenazas de robo de información bancaria. La alerta que más se registró en el primer periodo es 1-41573:4, una vulnerabilidad de Windows

10. Cabe indicar que el sistema operativo instalado en las computadoras del edificio durante el análisis fue Windows 7 hasta que migraron a Windows 10 al iniciar el siguiente periodo académico, sin embargo la vulnerabilidad 1-41573:4 pertenece a Windows 10 y es debido a que los estudiantes conectaban un cable de red a sus computadoras portátiles las cuales tiene instalado el sistema operativo Windows 10, al conectarse y asignarles una dirección IP mediante DHCP se conectaba a la Vlan Estudiantes y Snort detectaba el tráfico y la amenaza. Muchas de las amenazas detectadas se relacionan con el uso de internet, los estudiantes de manera no intencionada abrieron páginas sospechosas infectando la red por lo que se consideran insiders no intencionados. La cantidad de veces que se registró una alerta en el primer periodo se puede observar en el anexo E.

En el segundo periodo las alertas registradas disminuyeron por los motivos antes mencionados. En la tabla 6-3 se presenta un resumen de las amenazas detectadas en el segundo periodo.

Tabla 6-3: Resumen de amenazas registradas en la Vlan Estudiantes en el segundo periodo

Identificador	Significado	Descripción
1-46237:3	Troyano Criptominero Miner64	Es un archivo ejecutable que forma parte de BitcoinMiner desarrollado por Ufasoft. Este evento se genera cuando la muestra del minero se ha descargado y ejecutado en la PC infectada.
1-40060:1	Troyano Hadsruda	Software no deseado. Algunos programas no deseados intentan parecer inocentes para convencerlo de que los instale en su PC. Pueden realizar cambios en su PC sin su consentimiento, o comprometer el rendimiento de su PC.
1-45549:1	Troyano Criptominero XMRig	Este evento se genera cuando XMRig intenta iniciar sesión en una API de grupo de minería jsonrpc.
1-46486:1	Troyano LittleInstaller	Este evento se genera cuando una computadora con Slimware instalado se comunica con el servidor de control para actualizaciones. Provoca anuncios no deseados.
1-43909:3	Uso Exploit	Archivo Adobe Acrobat Reader JPEG 2000, intento de corrupción de memoria de mosaico.
1-46894:1	Gusano SysinfY2X	Este evento se genera cuando se observa una solicitud HTTP GET saliente que coincide con el URI

		utilizado por SysinfY2X / Forbix para descargar y ejecutar programas maliciosos en una computadora infectada.
1-40356:3	Troyano Instantaccess.exe en su versión antigua	Redirige a un sitio malicioso que muestra advertencias que indican que su computadora está infectada y que necesita ejecutar el análisis instant-access.exe de inmediato.
1-41573:4	Intento de robo de información utilizando vulnerabilidades de Microsoft Edge	Microsoft Edge permite a los atacantes remotos obtener información confidencial a través de un sitio web diseñado, también conocido como "Vulnerabilidad de divulgación de información de Microsoft Edge". Esta vulnerabilidad se asocia a windows 10
1-23605:12	Archivo malicioso.	Denominado Armadillo, poca información acerca de esta alerta se sabe que es de origen ruso.
1-8470:19	superspy 2.0 beta	Ejecución de un Backdoor en la maquina víctima.
1-31289:5	Intento de obtener acceso Server-WEBAPP	SERVER-WEBAPP /etc/passwd Este evento se genera cuando se observa una respuesta del servidor HTTP que contiene datos de un archivo / etc / passwd. Intento de obtener acceso a ese path.
1-47519:1	Ejecución de código remoto	Ejecución remota de código a la biblioteca de fuentes de Windows. Un atacante que explotó con éxito la vulnerabilidad podría tomar el control del sistema afectado. Un atacante podría entonces instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.
1-32691:1	Uso de script	Intento de denegación de servicio utilizando internet Explorer
1-31407:4	Ejecución de código arbitrario	Vulnerabilidad de uso después de libre en Adobe Reader y Acrobat 10.x antes del 10.1.10 y 11.x antes del 11.0.07 en Windows y OS X permite a los atacantes ejecutar código arbitrario a través de vectores no especificados.
1-46371:1	Moonify TLS server hello	Respuesta del servidor para iniciar

		una conexión ssl con servidores de minería de datos de criptomoneda
1-44912:2	Adobe Acrobat Pro tamaño de marcador invalido APP13.	Este evento se genera cuando un marcador APP13 con formato incorrecto en JPEG que, cuando está incrustado en XPS, provoca una lectura no válida en Adobe Acrobat Pro.

Realizado por: Byron Barragán, 2020

La amenaza que más se registró en este periodo fue la de intento de robo de información 1-41573:4 utilizando una vulnerabilidad de Windows 10 que como se mencionó antes se aplica más a las computadoras portátiles de los estudiantes, los troyanos más registrados son 1-35549:1 y 1-35030:1, son troyanos que consumen los recursos de la computadora haciéndola más lenta, en el periodo anterior también se detectaron, pero con más frecuencia es el primer periodo. A diferencia del periodo anterior en este hay más variedad de amenazas, muchas de ellas siendo la ejecución de código arbitrario valiéndose de vulnerabilidades de aplicaciones como Adobe. De igual manera las amenazas detectadas se relacionan con internet por lo que los estudiantes al navegar por internet pueden dar paso a que estas amenazas se desarrollen. En el anexo E se puede observar la cantidad de veces que se registraron las amenazas en el segundo periodo.

3.1.1.2. Amenazas detectadas en la VLAN Docentes

Para el caso de la Vlan Docentes el análisis se hizo en un periodo; inició el 17 de junio a las 8 AM y culminó el 17 de julio. El análisis se realizó en un periodo debido a que la configuración para el acceso a la Vlan Docentes se realizó después gracias a la ayuda de la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH. El procedimiento que se siguió se mencionó en el capítulo 2, se obtuvieron los siguientes resultados:

Tabla 7-3: Resumen de paquetes analizados por Snort en la Vlan Docentes

Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes recibidos	548884339	100%
Total paquetes analizados	545328509	99,35%
Total paquetes Drop	3555783	0,65%

Realizado por: Byron Barragán, 2020

En la tabla 7-3 se observa la cantidad de paquetes que recibió Snort, analizó el 99,35% tenido un porcentaje de drop de paquetes de 0,65% para este periodo ya se tiene configurado la longitud de cola predeterminada y se añadieron más reglas registradas de usuario Snort al

archivo de configuración es por esto por lo que el porcentaje de drop de paquetes es bajo además de que la cantidad de tráfico que circula por esta Vlan es menor en comparación a la Vlan Estudiantes. La información detallada de este registro de paquetes se puede encontrar en el anexo F.

La cantidad de paquetes TCP, UDP, TCP6, UDP6 y su porcentaje del total de paquetes analizados se muestra en la tabla 8-3.

Tabla 8-3: Resumen de paquetes analizados de la capa de transporte en la Vlan Docentes

Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes TCP	336657452	61,33%
Total paquetes UDP	139023595	25,33%
Total paquetes TCP6	5621	0,001%
Total paquetes UDP6	41051513	7,479%

Realizado por: Byron Barragán, 2020

La cantidad de alertas se registró todos los días a las 9 Am, cabe indicar que las alertas de los fines de semana se registraban los días lunes, así como también la cantidad de paquetes que se analizaron, a diferencia de la Vlan Estudiantes la cantidad de alertas registradas es mucho mayor sumando un total de 393106 alertas, esto es debido que una sola amenaza generaba varias alertas indicando un ataque continuo que duraba alrededor de 4 horas en busca de puertos abiertos y generando anuncios no deseados en la maquina víctima. No hay variedad de amenazas, pero si una gran cantidad de alertas. En la tabla 9-3 se presenta un resumen de las alertas registradas por día en este periodo. En el anexo G se encuentra esta información más detallada.

Tabla 9-3: Resumen de alertas diarias registradas en la Vlan Docentes

Semana 1		**Semana 2**		**Semana 3**		**Semana 4**		**Semana 5**	
Fecha	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**	**Fecha**	**Alertas**
17/06	16	24/06	49839	01/07	159897	08/07	97	15/07	0
18/06	10926	25/06	425	02/07		09/07	221	16/07	20
19/06		26/06	0	03/07	96467	10/07	47841	17/07	56
20/06		27/06	294	04/07		11/07	25746	--	--
21/06	540	28/06	147	05/07	309	12/07	265	--	--
Total	11482	**Total**	50705	**Total**	256673	**Total**	74170	**Total**	76

Realizado por: Byron Barragán, 2020

Como se observa en la tabla 9-3 algunos días están unidos ya que durante esos días las alertas continuaban por lo que el análisis no se detenía para su registro sino hasta que el ataque terminara. Después de esto el análisis se detuvo ya que la ESPOCH entro en receso académico.

Las amenazas que se registraron se pueden encontrar también en la Vlan Estudiantes, en general se registró presencia de malware, troyanos, archivos basura y ejecución de scripts maliciosos. Las direcciones IP que se registraron de las amenazas fueron las mismas solo variando el puerto por el cual se conectaban, es decir los objetivos fueron computadoras infectadas con malware o troyanos y cada vez que se encendía la computadora empezaba automáticamente a ejecutarse también debe indicarse que esta computadora puede ser una portátil propia del docente. Los días 3 y 4 de julio son los que más alertas se registraron siendo un ataque que duro 2 días. En la tabla 10-3 se muestra un resumen de todas las amenazas detectadas por Snort en el periodo con su respectivo identificador de alerta de Snort. En el anexo H se muestra más información sobre las amenazas detectadas.

Tabla 10-3: Resumen de amenazas registradas en la Vlan Docentes

Identificador	Significado	
1-48118:1	Troyano ITranslator	Troyanos que muestran anuncios no deseados sin utilizar o tener acceso al navegador
1-48116:1	Troyano ITranslator diferente versión	Troyanos que muestran anuncios no deseados sin utilizar o tener acceso al navegador
1-46237:3	Troyano Criptominero Miner64	Es un archivo ejecutable que forma parte de BitcoinMiner desarrollado por Ufasoft. Este evento se genera cuando la muestra del minero se ha descargado y ejecutado en la PC infectada.
1-45549:1	Troyano Criptominero XMRig	Este evento se genera cuando XMRig intenta iniciar sesión en una API de grupo de minería jsonrpc.
1-35030:1	Troyano Zbot o Zeus, indistintamente de su versión	Una versión del malware troyano Zeus. Este troyano es utilizado para instalar el ransomware CryptoLocker en una maquina víctima.
1-32691:1	Uso de script	Intento de denegación de servicio utilizando internet Explorer
1-35549:1	Malware Troyano ZeuS	Este troyano es utilizado para instalar el ransomware

		CryptoLocker en una maquina víctima.

Realizado por: Byron Barragán, 2020

Se observa en la tabla 10-3 que las amenazas detectadas en esta Vlan son las mismas que la Vlan estudiantes a excepción de las amenazas 1-48118:1 y 1-48116:1 las cuales trabajan en conjunto generando tráfico de anuncios no deseados en las computadoras, es precisamente estas amenazas las que generaban un número alto de alertas, la dirección IP que mostraba Snort para esta alerta siempre fue la misma solo variando el puerto por lo que esta amenaza trata de conectarse primero haciendo un escaneo de puertos revisando uno por uno, es por eso que la duración de este ataque es de entre 1 a 4 horas aproximadamente. Fuera de estas amenazas se tiene que mencionar que se suma la actividad de los troyanos criptomineros como Miner64, XMRig, ZeuS y el intento de ataque de denegación de servicios a internet Explorer 9. Siendo las amenazas 1-35030:1 y 1-35549:1 las más registradas.

3.1.1.3. Amenazas detectadas en la VLAN Administrativos

Para el caso de la Vlan Docentes el análisis se hizo en un periodo; inició el 17 de junio a las 8 AM y culminó el 17 de julio. El análisis se realizó en un periodo debido a que la configuración para el acceso a la Vlan Administrativos se realizó después gracias a la ayuda de la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH. El procedimiento que se siguió se mencionó en el capítulo 2; se obtuvieron los siguientes resultados:

Tabla 11-3: Resumen de paquetes analizados por Snort en la Vlan Administrativos

Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes recibidos	389006844	100%
Total paquetes analizados	386385688	99,33%
Total paquetes Drop	2620083	0,67%

Realizado por: Byron Barragán, 2020

En la tabla 11-3 se observa la cantidad de paquetes que recibió Snort, analizó el 99,33% tenido un porcentaje de drop de paquetes de 0,67% para este periodo ya se tiene configurado la longitud de cola predeterminada y se añadieron más reglas registradas de usuario Snort al archivo de configuración es por esto que el porcentaje de drop de paquetes es bajo además de que la cantidad de tráfico que circula por esta Vlan es menor en comparación a la Vlan Estudiantes y Docentes. La información detallada de este registro de paquetes se puede encontrar en el anexo I.

La cantidad de paquetes TCP, UDP, TCP6, UDP6 y su porcentaje del total de paquetes analizados se muestra en la tabla 12-3.

Tabla 12-3 Resumen de paquetes analizados de la capa de transporte en la Vlan Administrativos

Periodo		
Descripción	**# de paquetes**	**Porcentaje del total**
Total paquetes TCP	265381232	68,22%
Total paquetes UDP	72901268	18,74%
Total paquetes TCP6	7	0%
Total paquetes UDP6	5783579	1,49%

Realizado por: Byron Barragán, 2020

Como resultado en la Vlan Administrativos se registró 1 alerta el 8 de julio de 2019, esta alerta se generó cuando un atacante intentó explotar una vulnerabilidad de confusión de tipos en Microsoft Edge o CVE-2018-8298. La Vlan administrativos es la que menos alertas, amenazas y tráfico tiene. El análisis se detuvo porque la ESPOCH entro en receso académico.

3.1.2. Resultados de la adaptación de la metodología OSSTMM para el canal humano en el edificio de la FIE-ESPOCH

Después de adaptar la metodología para su aplicación en el edificio de la FIE-ESPOCH se pone en marcha la fase de inducción con una entrevista a la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH obteniéndose los siguientes resultados.

3.1.2.1. Resultados de la fase de inducción aplicada al canal Humano de la FIE-ESPOCH.

En la fase de inducción el propósito es obtener información referente a políticas de seguridad, cultura, procedimientos que se realizan o normas que se aplican todo referente a la seguridad. Para esta fase se realizó lo siguiente:

- Revisión de forma general la situación del edificio de la ESPOCH en cuanto a políticas de seguridad, cultura, procedimientos y normas que se aplican.
- Revisión algunos detalles pertenecientes al canal humano como horarios y formas de administración de los activos pertenecientes al edificio.
- Uso de una lista de verificación de seguridad para determinar la existencia de controles en caso de ciertos ataques a la seguridad informática.

A continuación, se muestra la lista de verificación de seguridad que se utilizó en la fase de inducción.

Tabla 13-3: Lista de verificación de la seguridad informática aplicada en la ESPOCH

Seguridad de los Datos						
Indicador	**Aspecto a Evaluar**	**Cumple**		**Riesgo**		
		SI	**NO**	**Bajo**	**Medio**	**Alto**
1	La organización tiene definidas políticas de seguridad informática.	x		x		
2	Las políticas de seguridad informática son revisadas periódicamente.	x		x		
3	Se dispone de un inventario de activos tecnológicos	x		x		
4	Se monitoriza y registra la actualización, instalación de software en equipos.	x		x		
5	Se tiene definido perfiles de usuario para evitar la instalación de cualquier tipo de software en los pc de usuarios finales.	x			x	
6	Dispone implementado listas de control de acceso (ACL)	x		x		
7	Se tiene software antivirus licenciado instalado en cada uno de los computadores que cuenta el edificio.		x			x
8	Se tiene instalado antimalware en los equipos del edificio.		x			x
9	Se dispone de repositorios externos para salvaguardar backups y datos relevantes.		x		x	
Seguridad de la Infraestructura y Servicios						
Indicador	**Aspecto a Evaluar**	**Cumple**		**Riesgo**		
		SI	**NO**	**Bajo**	**Medio**	**Alto**
11	Se dispone de Firewall.	x		x		
12	Se han definido perímetros de seguridad (DMZ) en la intranet para equipos con información valiosa o sistemas sensibles.	x		x		
13	Se dispone implementado un sistema de protección anti DDoS.	x		x		
14	Dispone de redundancia de hardware.	x		x		
15	Dispone de redundancia de software.		x	x		

16	Dispone de redundancia en el software del firewall.	x		x		
17	La organización cuenta con procesos para brindar mantenimiento preventivo al software.	x		x		
18	La organización cuenta con procesos para brindar mantenimiento preventivo de hardware.	x		x		
19	Dispone de contratos externos de soporte.	x				x
20	Dispone de UPS en cada estación de trabajo.		x		x	
21	Las instalaciones eléctricas cuentan con bajada a tierra.	x		x		
Controles de Acceso						
Indicador	**Aspecto a Evaluar**	**Cumple**		**Riesgo**		
		SI	**NO**	**Bajo**	**Medio**	**Alto**
22	Se ha definido e implementado un proceso para la creación de usuarios y contraseñas.	x			x	
23	Se ha definido un proceso de altas y bajas de usuario.		x			x
24	Se dispone de controles de acceso lógico a los servicios críticos de T.I que dispone la organización.	x		x		
25	Se monitoriza y registra la actividad de accesos lógicos en los equipos críticos que dispone.	x		x		
26	En los equipos de los usuarios finales dispone de dos cuentas de inicio de una como administrador y otra como usuario normal.		x		x	
27	Se dispone de controles de acceso físico al Data Center de la organización.	x		x		
28	Se monitoriza y registra la actividad de accesos físicos al Data Center de la organización.	x		x		
29	Se monitoriza y autentica las conexiones a la red inalámbrica de la organización.	x		x		
Planes de Respaldo						
Indicador	**Aspecto a Evaluar**	**Cumple**		**Riesgo**		
		SI	**NO**	**Bajo**	**Medio**	**Alto**
30	Se tiene establecido políticas de backup en caso de desastres.		x			x
31	Se ha documentado e implementado un proceso		x			x

	para gestión de incidentes de seguridad informática.					
32	Se ha definido planes de continuidad y de respaldos de información crítica.		x			x
33	Dispone la organización de respaldos de energía eléctrica en caso de fallas.	x		x		
34	Dispone de cuartos de acometidas para los servicios provistos por proveedores externos.	x		x		
Hábitos Seguros y Preparación						
Indicador	**Aspecto a Evaluar**	**Cumple**		**Riesgo**		
		SI	**NO**	**Bajo**	**Medio**	**Alto**
35	Cuenta con políticas de seguridad de los equipos respecto al consumo de alimentos y bebidas.		x		x	
36	Cuenta con planes de capacitación al personal sobre seguridad informática		x			x
37	Se dispone de un plan manejo seguro de datos críticos.	x		x		
38	Se destruyen discos duros catalogados como dañados.		x			x
39	El personal se conduce y aplica hábitos seguros de manejo de la información.	x		x		
40	En general, la actitud hacia la aplicación de normas de seguridad es positiva.		x			x

Fuente: (Gordon Revelo & Pacheco Villamar, 2018, pp. 7-8)
Realizado por: Byron Barragán, 2020

La tabla 13-3 fue adaptada a las actividades que se realizan en el edificio de la FIE-ESPOCH, fue tomada de un proyecto realizado y publicado por Diego Gordon y Rubén Pacheco en la revista Electrónica de Computación, Informática, Biomédica y Electrónica "ReCIBE". La información presentada en esta tabla fue proporcionada por el personal encargado de los equipos y laboratorios del edificio y también por la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH.

En esta tabla se puede observar que en el edificio y en si en la institución si tienen definidas políticas de seguridad informática las cuales son revisadas periódicamente o cuando se presente un incidente. Cuenta con un firewall en el cual se controla ciertos tipos de ataques entre ellos el mencionado de denegación de servicio, este firewall cuenta con redundancia a nivel de hardware, sin embargo, la redundancia a nivel de software es solo en el firewall mas no en

servidores. Se ha definido un perímetro de seguridad (DMZ) por secciones, pero no se ha hecho ninguna documentación acerca de ello. Procesos como la creación de usuarios y contraseñas si están implementados sin embargo un proceso de baja de usuarios no. Los datos críticos de cada servicio tienen un respaldo el cual se maneja de forma manual. Los discos duros catalogados como dañados son reingresados a bodega en donde se determinará si se destruye o no, este proceso es encargado a control de bienes de la institución. Con lo que respecta a seguridad no hay planes de capacitación a los empleados por parte de la institución, pero si hay planes de capacitación por parte del proveedor de servicio. En forma general las políticas aún están en desarrollo ya que se están definiendo nuevos procesos de los cuales se definirán nuevas políticas.

Por otro lado, los controles en el edificio por parte de los encargados de los equipos y laboratorios están completamente definidos sobre todo el acceso al cuarto de telecomunicaciones y las acciones que se deben realizar para reservar un laboratorio o la utilización de un equipo, más adelante en la fase de interacción se contabilizará estos procesos para el cálculo de la porosidad. Los activos del edificio son laboratorios informáticos, equipos de oficina, equipos utilizados para prácticas de los estudiantes. El idioma que se maneja es español y la zona horaria es GTM-5.

3.1.2.2. Resultados de la fase de interacción aplicada al canal Humano de la FIE-ESPOCH.

Para esta fase se realizó de igual manera que en la fase anterior una entrevista, pero esta vez a los encargados de los equipos y laboratorios del edificio de la FIE-ESPOCH, en la tabla 14-3 se observan los resultados mostrando un valor numérico, sin embargo, no se especifica la razón de este valor por concepto de seguridad. Estas tablas fueron tomadas y adaptadas de un trabajo de auditoria a la seguridad de una empresa publicado por la revista científica de la universidad de Cuenca "Maskana".

Tabla 14-3: Cálculo de la Porosidad en el canal humano

Seguridad Operacional (Porosidad)		
Ítem	**Prueba**	**Total**
Auditoria de la Visibilidad	Conteo de departamentos o áreas del edificio de la FIE-ESPOCH que están autorizados previa identificación a realizar interacciones con el cuarto de telecomunicaciones y demás activos.	**4**
Verificación de Acceso	Conteo de escenarios donde puede ocurrir una interacción sin que se necesite una autorización.	**1**
Verificación de Confianza	Conteo de los procesos de acceso de los estudiantes, docentes y administrativos a la información o a los activos físicos.	**3**

Fuente: (Bracho Ortega *et al.*, 2017, p. 314)
Realizado por: Byron Barragán, 2020

El siguiente paso es el cálculo de los controles, estos son formas que se establecen en una institución en este caso lo que se contabiliza son que controles existen para el acceso a los activos del edificio. Algunos de estos controles de clase A se encuentran previstos en otras fases, sin embargo, para el cálculo de los controles se los ubica en esta sección, pero se los realizó según el orden establecido en la adaptación de la metodología.

Tabla 15-3: Cálculo de los controles clase A en el canal humano

Controles de Interacción Clase A		
Ítem	**Prueba**	**Total**
Autenticación	Conteo los métodos por los cuales se puede interactuar con el personal de recepción o encargado.	**3**
Indemnización	Conteo de los documentos legales a los que deben someterse los estudiantes, docentes o administrativos del edificio de la FIE-ESPOCH para la utilización de ciertos activos o información.	**3**
Resistencia	Conteo del personal encargado que permiten acceder sin autorización a los activos del cuarto de telecomunicaciones.	**0**
Subyugación	Conteo los activos que pueden ser comunicados a través de canales en los cuales los controles no son necesarios, pueden ser eludidos o ignorados	**20**
Continuidad	Conteo del total de encargados que genera conflictos en cuanto a retrasos de acceso.	**0**

Fuente: (Bracho Ortega *et al.*, 2017, p. 315)
Realizado por: Byron Barragán, 2020

Tabla 16-3: Cálculo de los controles clase B en el canal humano

Controles de Interacción Clase B		
Ítem	**Prueba**	**Total**
No-Repudio	Conteo de quiénes del personal encargado identifican y registran adecuadamente el acceso o las interacciones con los activos del edifico de la FIE-ESPOCH.	**3**
Confidencialidad	Conteo de los segmentos de comunicación con los encargados dentro del alcance que son eficientes.	**3**
Privacidad	Conteo de los métodos eficientes para asegurar este control.	**1**
Integridad	Conteo de los métodos eficientes aplicados en el edificio de FIE-ESPOCH para proteger y asegurar que la información de los activos físicos no pueda ser cambiada, conmutada, redirigida o invertida sin que las partes involucradas tengan conocimiento de ello.	**1**
Alarma	Conteo de sistemas de advertencia o sistemas de alarma en todo	**1**

	el alcance.	

Fuente: (Bracho Ortega *et al.*, 2017, p. 315)
Realizado por: Byron Barragán, 2020

3.1.2.3. Resultados de la fase de investigación aplicada al canal Humano de la FIE-ESPOCH.

El cálculo de las limitaciones se realizó en esta fase. En la tabla 17-3 representa las limitaciones, en este punto se debe indicar que el sector de los administrativos y docentes no es controlado por lo que supone un factor de riesgo alto. En la fase de inducción se encontró que no se realiza cursos de capacitación sobre la seguridad al personal por parte de la institución, pero si se realiza capacitación por parte del proveedor de servicios. El edificio cuenta con una instalación de cámaras de seguridad en los laboratorios donde se encuentran los activos, sin embargo, no están instaladas en las aulas de clase, en las oficinas ni en la sala de profesores.

Como se mencionó en la adaptación de la metodología se provee a los estudiantes los instaladores del software utilizado para las diferentes asignaturas, estos archivos cuentan con las instrucciones de instalación para su correcto uso. Una vez entregado los archivos no se controla lo que el estudiante realice con ellos. En el punto de revisión de segregación se mencionan las limitaciones, en la tabla 17-3 se puede ver lo que se realizó para este cálculo.

Tabla 17-3: Cálculo de las limitaciones en el canal humano

Limitaciones		
Ítem	**Prueba**	**Total**
Vulnerabilidad	Conteo de las fallas o errores por las cuales una persona o proceso puede ganar o denegar el acceso a los demás.	**2**
Debilidad	Conteo de las posibles fallas o errores que pueden presentarse en los controles de Clase A.	**1**
Preocupación	Conteo de las posibles fallas o errores que pueden presentarse en los controles de Clase B.	**1**
Exposición	Conteo de las acciones injustificadas, fallas o errores que proporcionen una visibilidad directa o indirecta de los activos.	**2**
Anomalías	Conteo de los elementos desconocidos que no pueden tomarse en cuenta en las operaciones normales en la red del edificio de la FIE-ESPOCH.	**2**

Fuente: (Bracho Ortega *et al.*, 2017, p. 315)
Realizado por: Byron Barragán, 2020

3.1.2.4. Resultados de la fase de intervención aplicada al canal Humano de la FIE-ESPOCH.

En esta fase se presenta el estado actual de la seguridad operacional aplicado en el canal humano del edificio de la FIE-ESPOCH. Como se indicó anteriormente todos estos valores son ingresados en la hoja de cálculo que proporciona ISECOM en su sitio oficial dando como resultado el estado de la seguridad representando en un Rav. Existen dos expresiones que permiten realizar una interpretación de los valores obtenidos en la seguridad actual del canal auditado, la primera es Seguridad Δ como se muestra en el gráfico 1-3, marcada de color rojo, que no es nada más que el equilibrio que existe entre los valores numéricos de la porosidad, los controles y las limitaciones. Por lo tanto, dependiendo del signo que éste posea: positivo (+) o negativo (-), se pueden considerar los siguientes aspectos: un delta positivo muestra lo mucho que se gasta en controles o, incluso, si el exceso de gasto es demasiado en un tipo de control; un delta negativo muestra una falta de controles o que se controlan a sí mismos con limitaciones que no pueden proteger adecuadamente al objetivo. (Bracho Ortega *et al.*, 2017, p. 317). En base a lo anterior y observando el gráfico 1-3 se determinó que la seguridad del canal humano es de 85.77 Rav indicando que hace falta controles además de que existen ciertas limitaciones al momento de proporcionar seguridad. El delta negativo (-13.92) indica el nivel de brechas de seguridad las cuales pueden ser aprovechadas por un atacante insider.

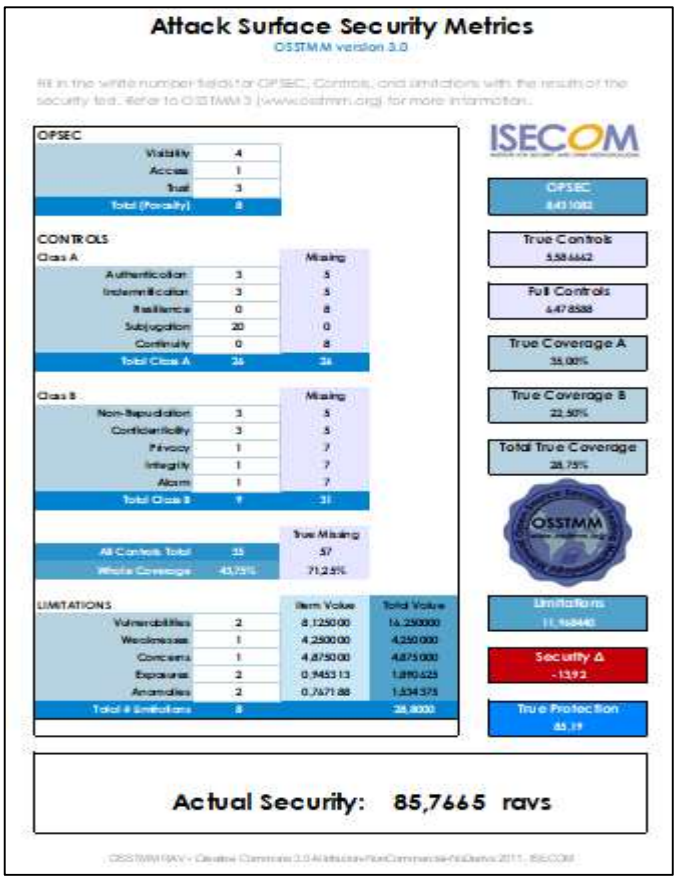


Gráfico 1-3: Resultado del cálculo del canal humano en el edifico de la FIE-ESPOCH.
Realizado por: Byron Barragán, 2020

3.1.3. Resultados de la adaptación de la metodología OSSTMM para el canal de red de datos en el edificio de la FIE-ESPOCH.

Como se mencionó en la fase de inducción del canal humano, los resultados obtenidos aplican también para la fase de inducción del canal de red de datos ya que la lista de verificación de la seguridad utilizada abarca áreas de los dos canales por lo que no se repite los resultados en esta sección.

3.1.3.1. Resultados de la fase de interacción aplicada al canal de Red de Datos de la FIE-ESPOCH.

Auditoria de la visibilidad

Encuesta de red:

- Red en el edificio de la FIE-ESPOCH

Existe 3 segmentos en la red del edificio de la FIE-ESPOCH, estas ya se mencionaron anteriormente: Estudiantes, Docentes y Administrativos.

Estudiantes: 172.25.2xx.xxx/23

Docentes: 172.25.2xx.xxx/24

Administrativos: 172.25.2xx.xxx/24

- Identificación de protocolos emanantes de la red del edifico de la FIE-ESPOCH

Utilizando Wireshark se analizó tráfico en las tres Vlans como resultado se registró los siguientes protocolos mostrado en la tabla 18-3

Tabla 18-3: Compilación de protocolos emanantes en las 3 Vlans

IPV4	DNS	ICMP	UDP6
TCP	Bootstrap Protocol	EIGRP	RIPng
RTCP	HTTPS	ARP	DHCP6
SSL	NetBIOS Datagram Service	Logical-Link Control	ICMP6
HTTP	SMB	STP	DHCP
UDP	SMB Mailslot Protocol	IPV6	SNMP
NetBIOS Name service	Microsoft Windows Browser Protocol	TCP6	Session initation Protocol

Realizado por: Byron Barragán, 2020

- Ping broadcast a todos los objetivos.

Se realizó un ping broadcast a todos los equipos activos en las tres Vlans, sin embargo, no un hubo respuesta en ninguno de los casos, el único que contesto fue la puerta de enlace predeterminada.

- Protocolos de enrutamiento en el alcance.

Se registraron dos protocolos de enrutamiento: EIGRP Y RIPng.

- Verifique las respuestas de ICMP de todos los objetivos.

Las respuestas de paquetes ICMP hacia todos los objetivos activos se registró en el anexo J. Este proceso se realizó en un día en el que presentaba mayor número de computadoras activas durante las 10 AM Y 3 PM.

- Rastree la ruta los paquetes TCP a todos los destinos para los puertos SSH, SMTP, HTTP y HTTPS.

Todos los objetivos pertenecen a la misma Vlan en el edificio por lo que un rastreo solo muestra como ruta la dirección de la puerta de enlace per determinada. Las herramientas utilizadas fue TCPing y TCProute. Los puertos 22 (SSH), 80 (HTTP) Y 443 (HTTPS) no están abiertos en todos los objetivos por lo que la comunicación por este puerto no se puede dar, sin embargo, en los objetivos que si están abiertos estos puertos la comunicación fue exitosa. Por otro lado, el puerto 25 (SMTP) no se encuentra abierto en ningún objetivo, la comunicación no fue exitosa.

- Rastree la ruta de los paquetes UDP a todos los destinos para los puertos DNS y SNMP.

De igual manera que lo descrito anteriormente el puerto 53 (DNS) no se encuentra abierto en todos los objetivos, sin embargo, en los objetivos que si encuentra abierto este puerto la comunicación fue exitosa, concretamente solo en 5 equipos se encontró este puerto abierto. Por otro lado, el puerto 161 (SNMP) no está abierto en ningún objetivo. Las herramientas utilizadas fue TCPing y TCProute.

Enumeración:

- Verifique las respuestas de las solicitudes de paquetes UDP a diferentes puertos.

Se utilizó las herramientas TCPing Y TCProute, se trató comunicar con los puertos UDP: 23, 53, 214, 1701 siendo estos puertos los más comunes en los sistemas, sin embargo, no se encuentra abiertos a excepción del puerto 53 en algunos objetivos, solo en este puerto la respuesta fue exitosa.

- Verifique las respuestas de solicitud de servicio a los puertos de malware conocidos o creados.

En la fase de explotación se utilizó malware para consumir recursos de la computadora víctima, los resultados se presentarán más adelante, cabe indicar que este proceso en el ambiente real no se pudo realizar ya que existe el riesgo de infectar a toda la red por lo que se decidió realizar esto en un ambiente virtual controlado, para evitar daños en al ambiente real.

- Verifique las respuestas de las solicitudes de paquetes TCP a diferentes puertos.

Realizando una auditoría de puertos abiertos en los objetivos se pudo determinar los principales puertos abiertos en la mayoría de los objetivos, utilizando la herramienta TCPing y TCProute se comprobó que la comunicación y las respuestas fueron exitosas, algunos de los puertos puestos a prueba son: 554, 8080 9090 (posible puerto usado en malware) y puertos altos generalmente utilizados por malware.

Verificación de acceso

Red:

- Manipular el servicio de red y el enrutamiento para acceder a restricciones pasadas dentro del alcance. (Test de alcance)

No se puede manipular el enrutamiento ya que esto se encarga Dirección de Tecnologías de la Información y Comunicación de la ESPOCH y no se tiene acceso.

- Solicite servicios de troyanos comunes y conocidos que utilizan UDP, TCP o ICMP para las conexiones.

De igual manera que en enumeración, esto se realizó en un ambiente virtual controlado por el riego de infectar a toda la red, los resultados se presentarán más adelante.

Servicios:

- Escaneo de puertos (descubrir puertos abiertos)

Los puertos abiertos más comunes en los objetivos: 22, 80, 443, 445, 111, 8080, 9090, 49152 – 49165. En el anexo P se muestra algunos objetivos auditados, se debe indicar que estos objetivos no representan mucho riesgo, la información de los puertos abiertos encontrados en objetivos con información confidencial se reserva.

Autenticación:

- Enumere los accesos que requieren autenticación y documente todos los privilegios descubiertos que se pueden usar para proporcionar acceso.

En la tabla 19-3 se presenta el valor numérico de este conteo, por razones de seguridad no se puede especificar a que pertenece este valor.

- Verifique la solidez de la autenticación a través de descifrar las contraseñas.

Los equipos utilizados en el edificio no cuentan con contraseña sin embargo estas computadoras están en estado congelado, es decir, cualquier cambio, programa o información que se maneje durante este encendida al apagarse se elimina y regresa al estado en el que fue congelada. Las contraseñas que se trataron de descifrar fueron las del sistema de monitorización de cámaras instaladas utilizando la herramienta para descifrar contraseñas Brutus, no se tuvo éxito. Las contraseñas son robustas.

Verificación de confianza

Abuso de recursos:

- Comprobar cómo se utilizan los recursos o activos de red.

Los recursos con lo que cuenta el edificio de la FIE-ESPOCH son utilizados por los estudiantes, docentes y administrativos, por parte de los estudiantes y docentes los recursos que usan son los laboratorios con los equipos presentes en estos y además otros necesarios para el desarrollo de sus tareas y clases, estos equipos son pedidos con anterioridad a los técnicos encargados de los mismos, los docentes y administrativos utilizan una computadora instalada en su lugar de trabajo con acceso a internet.

Tabla 19-3: Cálculo de la Porosidad en el canal de red de datos

Seguridad Operacional (Porosidad)		
Ítem	**Prueba**	**Total**
Auditoria de la Visibilidad	Identifique el perímetro del (los) segmento (s) de la red.	**3**
Verificación de Acceso	Conteo de los métodos de acceso y revise todos los privilegios descubiertos que se pueden usar para proporcionar acceso.	**3**
Verificación de la Confianza	Las medidas para acceder a la propiedad dentro del alcance mediante la suplantación de su dirección de red como uno de los hosts de confianza.	**0**

Realizado por: Byron Barragán, 2020

Verificación de controles

En la tabla 20- 3 se muestra los controles de interacción Clase B, al igual se muestra un valor numérico y no se especifica a que pertenece cada valor por razones de seguridad.

Tabla 20-3: Cálculo de los controles clase B en el canal de red de datos

Controles de Interacción Clase B		
Ítem	**Prueba**	**Total**
No-Repudio	Conteo del uso o las deficiencias de los sistemas para identificar adecuadamente y registrar el acceso. Métodos de identificación que derrotan el repudio.	**0**
Confidencialidad	Conteo de los métodos aceptables utilizados para la confidencialidad.	**1**
Privacidad	Conteo de los servicios dentro del alcance de las comunicaciones, privacidad de la interacción	**2**
Integridad	Conteo de las deficiencias de integridad cuando utilice un proceso documentado, firmas, cifrado, hash o marcas para garantizar que el activo no se pueda cambiar, redirigir o revertir sin que las partes involucradas lo conozcan.	**0**
Alarma	Enumeración del uso de un sistema de advertencia, registro o mensaje donde el personal detecte una situación sospechosa por sospecha de intentos de elusión, ingeniería social o actividad fraudulenta.	**1**

Realizado por: Byron Barragán, 2020

3.1.3.2. Resultados de la fase de investigación aplicada al canal de Red de Datos de la FIE-ESPOCH.

A diferencia de del canal humano, en el canal de red de datos los controles de clase A se calculan en la fase de investigación, en la tabla 21-3 se muestra un valor numérico de esto controles.

Tabla 21-3: Cálculo de los controles clase A en el canal de red datos.

Controles de Interacción Clase A		
Ítem	**Prueba**	**Total**
Autenticación	Conteo de los accesos que requieren autenticación con todos los privilegios descubiertos que se pueden usar para proporcionar acceso.	**4**
Indemnización	Coteo de los objetivos y servicios que están protegidos contra el abuso o están asegurados por robo o daños, o usan	**230**

	responsabilidad y exenciones de responsabilidad de permisos.	
Resistencia	Los puntos únicos de falla en la infraestructura donde el cambio o la falla pueden causar una interrupción del servicio.	**11**
Subyugación	Conteo de los servicios en los cuales los controles no son necesarios, pueden ser eludidos o ignorados	**0**
Continuidad	Conteo de las deficiencias de todos los objetivos con respecto a los retrasos de acceso y los tiempos de respuesta del servicio a través de sistemas de respaldo o el cambio a canales alternativos.	**17**

Realizado por: Byron Barragán, 2020

En la fase de investigación también se determina las limitaciones, las cuales se presentan en la tabla 22-3.

Tabla 22-3: Cálculo de las limitaciones de la canal de red de datos

Limitaciones		
Ítem	**Prueba**	**Total**
Vulnerabilidad	Identifique si alguna vulnerabilidad conocida reside en los sistemas. (Uso de Nexpose)	**1082**
Debilidad	Contabilizar las posibles fallas o errores que pueden presentarse en los controles de Clase A.	**5**
Preocupación	Contabilizar las posibles fallas o errores que pueden presentarse en los controles de Clase B.	**5**
Exposición	Enumere las exposiciones del sistema, servicio y aplicación que detallan el diseño, tipo, versión o estado de los objetivos o de recursos fuera del alcance, como por ejemplo de publicaciones o fugas.	**0**
Anomalías	Contabilizar los elementos desconocidos que no pueden tomarse en cuenta en las operaciones normales en la red del edificio de la FIE-ESPOCH.	**2**

Realizado por: Byron Barragán, 2020

Vulnerabilidad fue realizado por Nexpose, con la ayuda de este escáner de vulnerabilidades se pudo definir todas las vulnerabilidades que se encuentran en los sistemas del edificio de la FIE-ESPOCH. Más adelante se detallará este resultado.

Verificación de la configuración

Mapa de Limitaciones

- Compruebe si hay servicios / funciones innecesarios o no utilizados disponibles.

El servicio de alarma contra incendios está actualmente desactivado, fuera de este servicio los demás están operativos en el edificio. En cuanto a equipos existen algunos equipos a la espera del proceso de dada de baja por la unidad de control de bienes mientras tanto se encuentran guardados.

- Compruebe las credenciales por defecto.

Las credenciales por defecto no están configuradas, todas fueron cambiadas.

Validación de la propiedad

Mercado negro

- Todos los programas utilizados en los laboratorios son distribuidos a los estudiantes si se solicita, solo algunos de estos programas tienen licencias. Lo que se hacen con los programas después de proporcionar a los estudiantes es desconocido.

Revisión de la segregación

Divulgación:

- Toda información es proporcionada previa solicitud, esta información es confidencial no se proporciona fácilmente.

Limitaciones:

- Si existen consideraciones para la interacción con los objetivos por parte de personas con limitaciones físicas.

3.1.3.3. Resultados de la fase de intervención aplicada al canal de Red de Datos de la FIE-ESPOCH.

Verificación de cuarentena

Identificación del proceso de contención:

- Identifique métodos de cuarentena para contactos agresivos y hostiles, como malware, puntos de acceso no autorizados, dispositivos de almacenamiento no autorizados, etc.

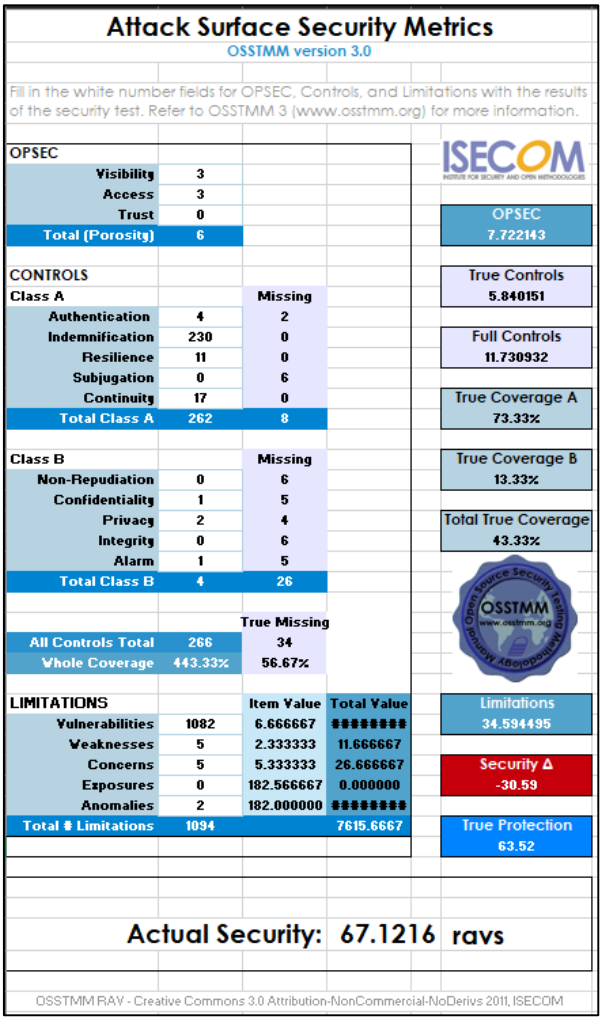
Según el análisis del tráfico con Snort se detectó algunos agentes de malware y continuaban durante el análisis por lo que no existe un proceso de cuarentena en caso de infección de malware o troyanos en una computadora dentro de las Vlans.

Niveles de contención:

- Verificar las medidas de detección presentes para la detección de intentos de acceso a los recursos protegidos.

No existen medidas de detección ya que los equipos están resguardados correctamente.

Finalmente se obtiene el valor del Rav ingresando los valores numéricos en la hoja de cálculo proporcionada de ISECOM. En el gráfico 2-3 se presenta el resultado obtenido:



Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	3		
Access	3		
Trust	0		
Total (Porosity)	6		

CONTROLS		
Class A		Missing
Authentication	4	2
Indemnification	230	0
Resilience	11	0
Subjugation	0	6
Continuity	17	0
Total Class A	262	8
Class B		Missing
Non-Repudiation	0	6
Confidentiality	1	5
Privacy	2	4
Integrity	0	6
Alarm	1	5
Total Class B	4	26
		True Missing
All Controls Total	266	34
Whole Coverage	443.33%	56.67%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	1082	6.666667	########
Weaknesses	5	2.333333	11.666667
Concerns	5	5.333333	26.666667
Exposures	0	182.566667	0.000000
Anomalies	2	182.000000	########
Total # Limitations	1094		7615.6667

OPSEC	7.722143
True Controls	5.840151
Full Controls	11.730932
True Coverage A	73.33%
True Coverage B	13.33%
Total True Coverage	43.33%
Limitations	34.594495
Security Δ	-30.59
True Protection	63.52

Actual Security: 67.1216 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Gráfico 2-3: Resultado de la auditoria del canal de datos en el edifico de la FIE-ESPOCH.
Realizado por: Byron Barragán, 2020

En base a lo anterior y observando el gráfico 2-3 se determinó que la seguridad del canal de red de datos es de 67.1216 Rav indicando que hace falta controles además de la presencia de varias vulnerabilidades conocidas en los sistemas. El delta negativo (-30.59) indica el nivel de brechas de seguridad las cuales pueden ser aprovechadas por un atacante insider.

3.1.4. Resultados del escaneo de Nexpose en las Vlans en el edificio de la FIE-ESPOCH

Para el escaneo, Nexpose se instaló en un host perteneciente a las Vlans, para ello se configuró en la herramienta un sitio de escaneo con la red de las Vlans y se definió un tipo de escaneo

completo indicando las credenciales de acceso de todos los equipos que se van a analizar. El escaneo tardó alrededor de 25 minutos en completarse. Posteriormente se generó un informe con los resultados, se escogió un informe de tipo ejecutivo para visualizar las vulnerabilidades clasificadas por riego, sistema operativo, tipo y además sus soluciones. En el anexo K se muestra la pantalla principal de Nexpose y los sitios de escaneo configurados.

3.1.4.1. Resultado del escaneo de Nexpose en la Vlan Estudiantes.

Toda la información y gráficos que se describen a continuación fueron tomados del informe ejecutivo que se generó con Nexpose después del escaneo. Se encontraron 400 vulnerabilidades durante el análisis. De estas, 30 son vulnerabilidades críticas, son relativamente fáciles de explotar por los atacantes y pueden proporcionarles un control total de los sistemas afectados. 296 vulnerabilidades son graves. Las vulnerabilidades graves a menudo son más difíciles de explotar y pueden no proporcionar el mismo acceso a los sistemas afectados. Además, se descubrieron 74 vulnerabilidades moderadas. Estas a menudo proporcionan información a los atacantes que pueden ayudarlos a montar ataques posteriores. Estas también deben repararse de manera oportuna. Se descubrió que existen vulnerabilidades críticas en 6 de los sistemas, lo que los hace más susceptibles a los ataques. En los demás sistemas se encontraron vulnerabilidades moderadas y graves. No se encontraron vulnerabilidades en 2 sistemas. En el gráfico 3-3 se presenta un diagrama representando lo antes descrito.

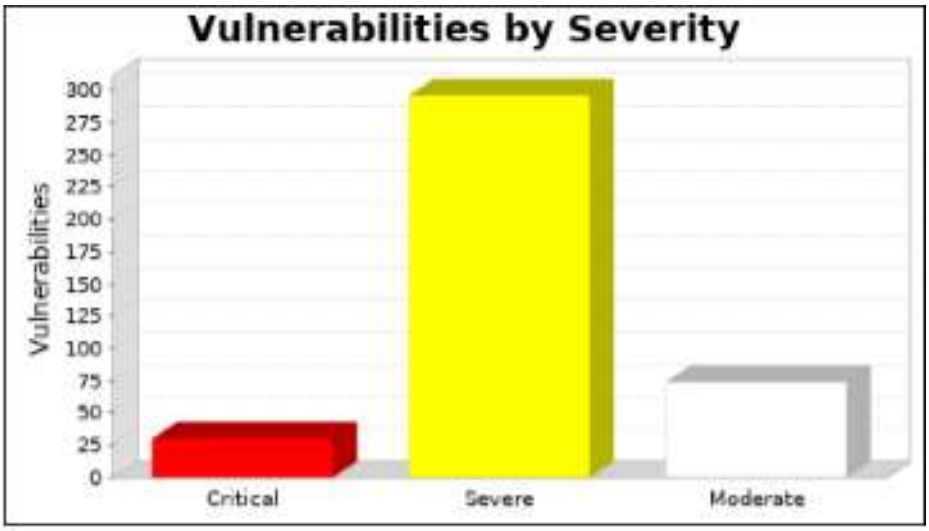


Gráfico 3-3: Clasificación de las vulnerabilidades encontradas según severidad en la Vlan Estudiantes.
Realizado por: Byron Barragán, 2020

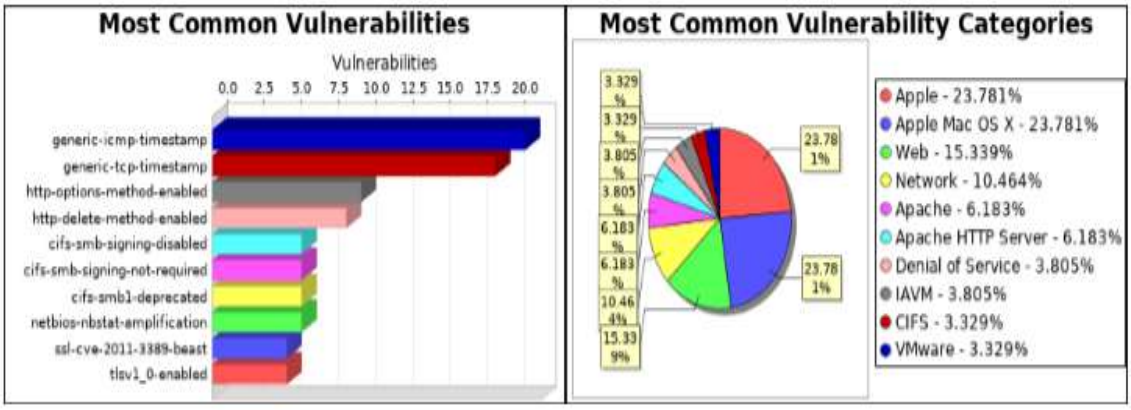


Gráfico 4-3: Vulnerabilidades (i) y categoría de vulnerabilidades (d) más comunes en la Vlan Estudiantes.
Realizado por: Byron Barragán, 2020

El gráfico 4-3 muestra que se encontró 21 ocurrencias de la vulnerabilidad generic-icmp-timestamp, y 18 ocurrencias de generic-tcp-timestamp por lo que son las vulnerabilidades más comunes. Hubo 200 instancias de vulnerabilidad en las categorías Apple y Apple Mac OS X, lo que las convierte en las categorías de vulnerabilidad más comunes. Esta categoría de vulnerabilidades se da por los equipos Apple que están instalados en uno de los laboratorios y necesitan una actualización de sistema operativo para solucionar estas vulnerabilidades ya que se encuentran en un estado muy obsoleto. Además, se determinó que se debe actualizar el sistema operativo Windows 7 siendo este sistema el que predomina en los equipos escaneados. Nexpose les asigna un valor propio de riesgo, con esto puede dividir las vulnerabilidades encontradas según el riesgo como se muestra en el gráfico 5-3.

Gráfico 5-3: Vulnerabilidades según el riesgo en la Vlan Estudiantes.
Realizado por: Byron Barragán, 2020

La vulnerabilidad http-options-method-enabled tiene un puntaje de riesgo de 5643 siendo una vulnerabilidad moderada. La vulnerabilidad cifs-smb-signing-disabled y todas las demás que se relacionan con el protocolo SMB (Server Message Block) tienen un puntaje de riesgo entre 3000 a 5000 siendo una vulnerabilidad grave. El protocolo SMB permite la compartición de

archivos e impresoras en red por lo que si un atacante explota la vulnerabilidad con existo puede continuar con las demás computadoras o equipos que están conectados en la red con el protocolo SMB activado. Según el informe generado, véase el anexo L, los equipos no permiten la firma SMB. La firma SMB le permite al destinatario de los paquetes SMB confirmar su autenticidad y ayuda a prevenir ataques de hombre en el medio contra SMB. La firma SMB se puede configurar de tres maneras: deshabilitada por completo (menos segura), habilitada y requerida (más segura).

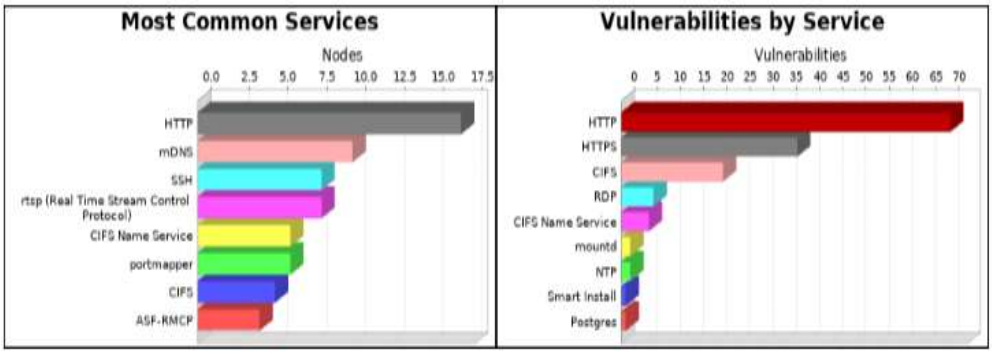


Gráfico 6-3: Servicios (i) Vulnerabilidades por servicios (d) en la Vlan Estudiantes.
Realizado por: Byron Barragán, 2020

En el gráfico 6-3 se observa que el servicio más utilizado en la mayoría de los equipos escaneados y a su vez el servicio con mayor número de vulnerabilidades es HTTP (HiperText Tranfer Protocol) con 71 vulnerabilidades detectadas durante el escaneo.

3.1.4.2. Resultado del escaneo de Nexpose en la Vlan Docentes.

Toda la información y gráficos que se describen a continuación fueron tomados del informe ejecutivo que se generó con Nexpose después del escaneo. Se encontraron 682 vulnerabilidades durante este análisis. De estas, 93 eran vulnerabilidades críticas. Son relativamente fáciles de explotar por los atacantes y pueden proporcionarles un control total de los sistemas afectados. 555 vulnerabilidades fueron graves. Las vulnerabilidades graves a menudo son más difíciles de explotar y pueden no proporcionar el mismo acceso a los sistemas afectados. Se descubrieron 34 vulnerabilidades moderadas. Estos a menudo proporcionan información a los atacantes que pueden ayudarlos a montar ataques posteriores en su red. Estos también deben repararse de manera oportuna, Se descubrió que existen vulnerabilidades críticas en 4 de los sistemas escaneados, lo que los hace más susceptibles a los ataques. Se encontró, además, que 7 sistemas tienen vulnerabilidades graves y moderadas en 10 sistemas. Ningún sistema estaba libre de vulnerabilidades. En el gráfico 7-3 se puede observar lo antes descrito.

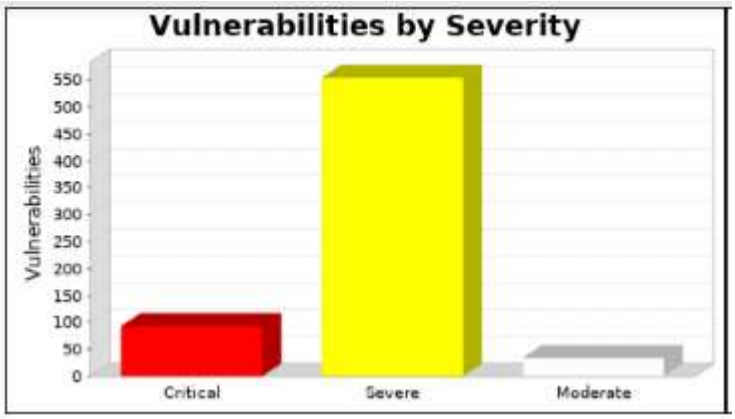


Gráfico 7-3 Clasificación de las vulnerabilidades encontradas según severidad en la Vlan Docentes.
Realizado por: Byron Barragán, 2020

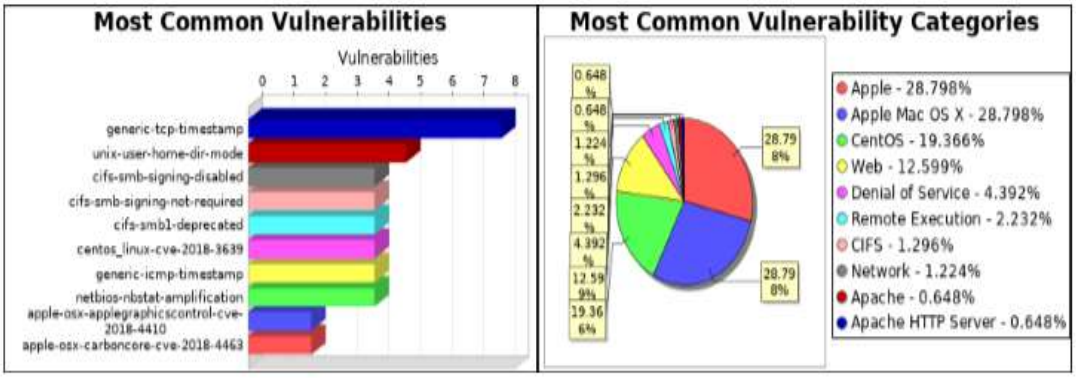


Gráfico 8-3: Vulnerabilidades (i) y categoría de vulnerabilidades (d) más comunes en la Vlan Docentes.
Realizado por: Byron Barragán, 2020

Como se observa en el gráfico 8-3 hubo 8 ocurrencias de la vulnerabilidad generic-tcp-timestamp, por lo que es la vulnerabilidad más común. Hubo 400 instancias de vulnerabilidad en las categorías Apple y Apple Mac OS X, lo que las convierte en las categorías de vulnerabilidad más comunes. Se determinó que se debe actualizar el sistema operativo Windows 7 siendo este sistema el que predomina en los equipos escaneados. Además, se debe actualizar el sistema operativo Apple de las computadoras de esta Vlan ya que la mayoría de las vulnerabilidades se encontraron en este sistema siendo una versión muy obsoleta lo que indica las vulnerabilidades. Nexpose les asigna un valor propio de riesgo, con esto puede dividir las vulnerabilidades encontradas según el riesgo como se muestra en el gráfico 9-3.

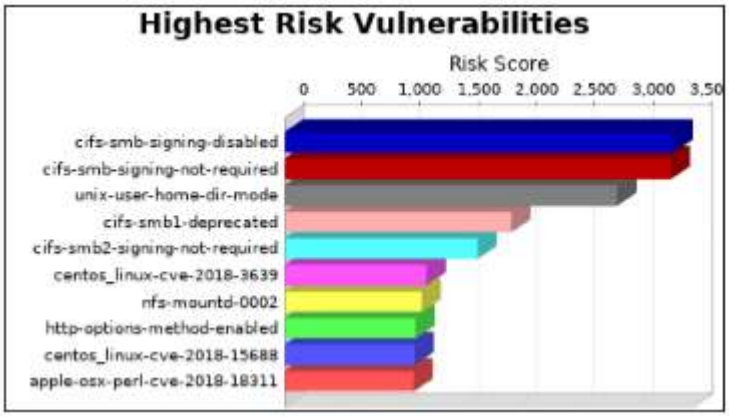


Gráfico 9-3: Vulnerabilidades según el riesgo en la Vlan Docentes.
Realizado por: Byron Barragán, 2020

La vulnerabilidad cifs-smb-signing-disabled y todas las demás que se relacionan con el protocolo SMB (Server Message Block) tienen un puntaje de riesgo de alrededor de 3342 siendo una vulnerabilidad grave. Como ya se mencionó se relaciona con el protocolo SMB Según el informe generado, véase el anexo M, los equipos no permiten la firma SMB, la forma de explotación se mencionó anteriormente.

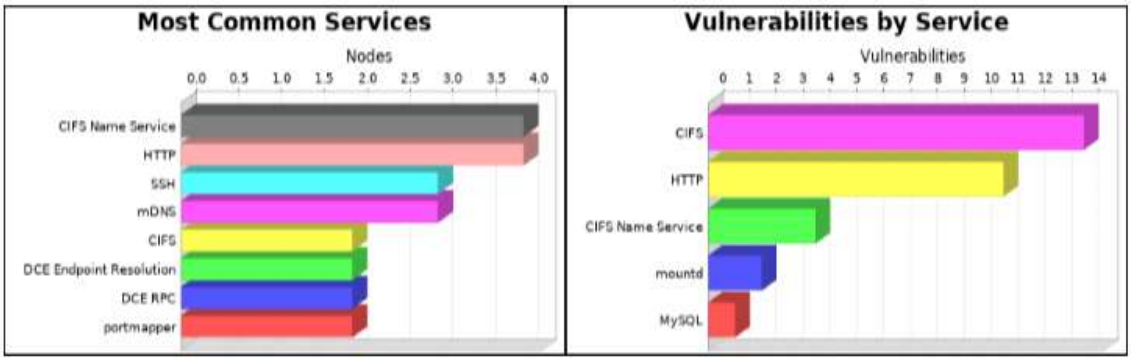


Gráfico 10-3: Servicios (i) Vulnerabilidades por servicios (d) en la Vlan Docentes.
Realizado por: Byron Barragán, 2020

En el gráfico 10-3 se observa que los servicios más utilizados en la mayoría de los equipos escaneados son HTTP y CIFS Name Service relacionado a internet, este último con 14 vulnerabilidades y HTTP con 11 vulnerabilidades detectadas durante el escaneo.

En Vlan Administrativos no se realizó un escaneo con Nexpose debido a que durante el análisis de Snort solo se encontró una amenaza por lo que esta Vlan no se consideró como un objetivo de un atacante insiders en el edificio de la FIE-ESPOCH.

3.1.4.3. Vulnerabilidades consideradas para la fase de explotación.

Para la selección de las vulnerabilidades a explotar, se relacionó los resultados obtenidos con Snort y Nexpose, es decir, si las amenazas detectadas con Snort tienen relación con las vulnerabilidades encontradas con Nexpose. Esto se hizo debido a que solo se encontró una vulnerabilidad de la capa de transporte siendo esta generic-tcp-timestamp. A continuación, en la tabla 23- 3 se muestra la relación de los resultados, vulnerabilidades y amenazas.

Tabla 23-3: Relación entre los resultados de Snort y Nexpose

Análisis con Snort			**Escaneo con Nexpose**
ID	**Amenaza**	**Descripción**	**Vulnerabilidad**
1-40357:3	Troyano Instantaccess.exe	Redirige a un sitio malicioso que muestra anuncios para ejecutar el análisis instant-access.exe	Se determinó un 15.339% de vulnerabilidades web en Vlan Estudiantes y un 12.599% en Vlan Docentes. Las cuales pueden ser explotadas con malware.
1-31046:6	Exploit kit	Este evento se genera cuando una estructura de URL coincide con la estructura utilizada por el kit de explotación de Angler.	
1-43459:2	Doublepulsar y Eternalblue	Implementación del Backdoor Doublepulsar, se puede utilizar para ejecutar software malicioso en la maquina víctima.	Firma de Server Message Block (SMB) esta deshabilitada. No se requiere firma SMBv1 SMBv2 Se utiliza el protocolo SMBv1 que está en desuso. MS17-010
1-46237:1	Troyano Miner64	Es un archivo ejecutable que forma parte de BitcoinMiner desarrollado por Ufasoft. Este evento se genera cuando la muestra del minero se ha ejecutado.	Se determinó un 15.339% de vulnerabilidades web en Vlan Estudiantes y un 12.599% en Vlan Docentes. Las cuales pueden ser explotadas con malware, Troyanos etc.
1-45549:1	Troyano XMRig	Este evento se genera cuando XMRig intenta iniciar sesión en una API de grupo de minería jsonrpc.	
1-48080:1	Troyano Ramnit	El troyano Ramnit hace que los equipos infectados operen como una botnet centralizada.	
1-46486:1	Troyano LittleInstaller	Este evento se genera cuando una computadora con Slimware se comunica con el servidor de control para actualizaciones. Provoca anuncios no deseados.	
1-41573:4	Robo de información	Microsoft Edge permite a los atacantes remotos obtener información confidencial a través de un sitio web diseñado, también conocido como "Vulnerabilidad de divulgación	Más del 70% de los objetivos activos durante el escaneo tiene sistema operativo Windows 7. Siendo vulnerable a las amenazas 1-43459:2, 1-41573:4, 1-47102:1 y 1-32691:1

		de información de Microsoft Edge".	
1-41337:2	Malware Sysch	Realiza secretamente otras acciones que afectan la información personal almacenada en el dispositivo, y o el control del dispositivo. Está asociado con el sistema operativo Android.	Se determinó un 15.339% de vulnerabilidades web en Vlan Estudiantes y un 12.599% en Vlan Docentes. Las cuales pueden ser explotadas con malware.
1-40356:3	Troyano Instantaccess .exe otra versión	Redirige a un sitio malicioso que muestra advertencias que indican que su computadora está infectada y que necesita ejecutar el análisis instant-access.exe de inmediato.	
1-35549:1	Malware Troyano ZeuS	Este troyano es utilizado para instalar el ransomware CryptoLocker en una computadora víctima.	
1-35030:1	Troyano Zbot o Zeus	Una versión del malware troyano Zeus. Este troyano es utilizado para instalar el ransomware CryptoLocker en una computadora víctima.	
1-25074:1	Troyano Banker	Troyanos que roban información bancaria de un sistema afectado.	
1-23605:12	Archivo malicioso.	Denominado Armadillo, poca información acerca de esta alerta se sabe que es de origen ruso	Se determinó un 15.339% de vulnerabilidades web en Vlan Estudiantes y un 12.599% en Vlan Docentes. Las cuales pueden ser explotadas con malware o inyección de código.
1-47102:1	Uso de Exploit	Este evento se genera cuando un atacante intenta explotar una vulnerabilidad de confusión de tipo en Microsoft Edge o CVE-2018-8298	Más de 70% de los objetivos activos durante el escaneo tiene sistema operativo Windows 7. Siendo vulnerable a la amenaza 1-43459:2, 1-41573:4, 1-47102:1 y 1-32691:1
1-46659:2	Uso de Exploit	Intento de explotar un doble gratis en Adobe Acrobat Reader.	Vulnerabilidad CVE-2018-4990, la explotación exitosa puede llevar a la ejecución de código malicioso.
1-32691:1	Uso de script	Intento de denegación de servicio utilizando internet Explorer 9.	Más de 70% de los objetivos activos durante el escaneo tiene sistema operativo Windows 7. Siendo vulnerable a la amenaza 1-43459:2, 1-41573:4, 1-47102:1 y 1-32691:1 Se determinó que alrededor del 8% de las vulnerabilidades pertenecen a la categoría de

			denegación de servicio.

Realizado por: Byron Barragán, 2020

Como se puede ver en la tabla 23-3 existe una relación entre los resultados de Snort y Nexpose y tomando en cuenta en la sección 2.3 se decidió explotar las siguientes vulnerabilidades mostradas en la tabla 24-3.

Tabla 24-3: Vulnerabilidades y amenazas consideradas para la fase de explotación

Vulnerabilidad/Amenaza	Definición	Herramienta
Generic-tcp-timestamp Generic-icmp-timestamp	Se puede utilizar para realizar ataques fingerprinting, obtener información del sistema que será víctima del ataque; fase de reconocimiento de un ataque.	Zenmap Distribución Kali Linux
Vulnerabilidades de SMB MS17-010 Eternalblue	Tener control total de la computadora víctima, con esto se puede hacer robo de información, ejecución de malware, ataques hombre en medio, etc.	Distribución Kali Linux/ Módulos de Metasploit
Amenaza: Malware, Troyanos	Consumo de recursos de la computadora víctima, instalación de software malicioso.	Ejecución de una versión del malware ZeuS.
Vulnerabilidades de tipo denegación de servicio	Denegar el servicio de una página web y todo lo que conlleva el acceso a la misma.	Distribución/Kali Linux/ Scritp Slowloris.
Backdoor Doublepulsar	Tener control total de la computadora víctima mediante SMB e instalación del backdoor Doublepulsar.	Distribucion Kali Linux/ Módulos de Metasploit

Realizado por: Byron Barragán, 2020

En la tabla 24-3 se presentan las amenazas y vulnerabilidades que en la fase de explotación se hizo énfasis, las vulnerabilidades Generic-tcp-timestamp y Generic-icmp-timestamp son las más comunes encontradas en los escaneos de Nexpose en las dos Vlans, por lo que en la fase de explotación se tomó en cuenta estas dos vulnerabilidades para determinar que puede causar un posible insider aprovechándose de la vulnerabilidad. Además, para el caso de la vulnerabilidad Generic-tcp-timestamp, es la única vulnerabilidad de la capa de transporte que se encontró. Generic-icmp-timestamp es una vulnerabilidad de capa de red, sin embargo, se consideró ya que tiene relación con la vulnerabilidad Generic-tcp-timestamp teniendo el mismo objetivo, estas

vulnerabilidades se pueden aprovechar con ataques fingerprinted para eso se decidió utilizar la herramienta Zenmap para hacer un escaneo de puertos y obtener información del sistema al cual se desea realizar un ataque más complejo. Esto forma parte de la etapa de reconocimiento de un ataque informático

La vulnerabilidad cifs-smb-signing-disabled y todas las relacionadas con el protocolo SMB están representadas en la tabla 24-3 como vulnerabilidades SMB, esta vulnerabilidad permite a cualquier usuario compartir archivos sin ninguna clase de autenticación por lo que para la fase explotación se decidió explotar esta vulnerabilidad en conjunto con la vulnerabilidad MS17-010 la cual está presente en el sistema operativo Windows 7 utilizado en las computadoras del edificio de la FIE-ESPOCH. Estas vulnerabilidades representan mucho riesgo como lo muestran los gráficos 5-3 y 9-3 además la vulnerabilidad MS17-010 en su tiempo fue aprovechada en conjunto con un ransomware y un Backdoor denominado Doublepulsar el cual se fue detectado durante el análisis de Snort como se observa en la tabla 23-3 que también se replicó en la fase de explotación.

Durante el análisis de Snort se detectó una gran cantidad de malware y troyanos, en específico el malware ZeuS que es utilizado para instalar el ransomware CriptoLocker, sin embargo, este ransomware no fue detectado en el análisis de Snort, por lo que se decidió replicar este malware en la fase de explotación para determinar cuál es el efecto de este en una computadora.

En el desarrollo del primer objetivo propuesto para este trabajo se mencionó que las amenazas más comunes a la capa de transporte son los ataques de denegación de servicio, por lo que este tipo de amenazas se tuvo a consideración en la fase de explotación.

3.1.5. Escenario virtual para la fase de explotación de vulnerabilidades

La fase de explotación se realizó en un escenario virtual desarrollado en el simulador GNS3, en una computadora portátil Alienware 17 R5 con 32 Gigabytes de memoria ram. Este escenario pertenece al laboratorio de microondas del edificio de la FIE-ESPOCH.

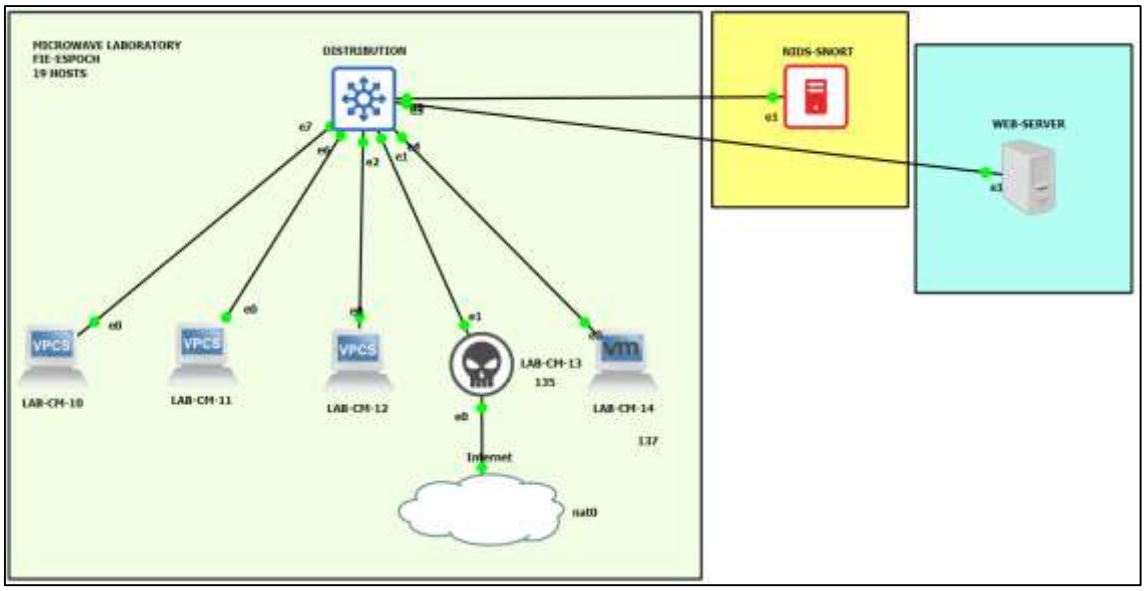


Figura 1-3: Escenario virtual utilizado para la fase de explotación
Realizado por: Byron Barragán, 2020

En la figura 1-3 se muestra el escenario virtual donde se realizó las pruebas de explotación. Este escenario cuenta con un switch al cual se conectan 19 computadoras. En el escenario virtual solo se conectan 6 computadoras debido al uso de la memoria ram que ocupa el simulador ya que estas son máquinas virtuales administradas desde el virtualizador Vmware 15, cada una de estas computadoras tienen 3 gigabytes de memoria ram y dos adaptadores virtuales de red; de estas 6 computadoras; la denominada LAB-CM-13 está representando la computadora atacante o insider, esta es una máquina virtual de Kali Linux desde donde se realizó los ataques, para eso se configuró esta máquina virtual con 4 gigabytes de memoria ram y dos adaptadores virtuales de red. Las demás computadoras simbolizan las víctimas con sistema operativo Windows 7 y, además, todas las computadoras tienen conexión a internet. La computadora LAB-CM-14 es una máquina virtual explotable de Windows 7 siendo esta la victima de los ataques debido a que esta contiene las vulnerabilidades del protocolo SMB. En el escenario se implementó Snort en una máquina virtual con distribución CentOS 7, 3 gigabytes de memoria ram y dos adaptadores virtuales de red, Snort detectará el tráfico de los ataques realizados mostrando alertas; para esto en el switch se configuró un puerto espejo para que todo el tráfico de los demás puertos se copie al puerto configurado y Snort pueda analizar el tráfico, la configuración utilizada en el switch se muestra en el anexo N. Además, se observa un servidor web el cual se instaló en una máquina virtual con distribución CentOS 7, 3 gigabytes de memoria ram y dos adaptadores de red virtuales. Este servidor web se levantó con Apache2 y representa la victima de los ataques de denegación de servicio. Antes de comenzar con la fase de explotación se comprobó que exista conectividad en todo el escenario, el direccionamiento utilizado obedece a la red 192.168.19x.xxx/24.

3.2. Resultados de la etapa 2: Explotación

La etapa de explotación comienza con una fase de reconocimiento con un ataque de fingerprinted aprovechándose la vulnerabilidad generic-tcp-timestamp y generic-icmp-timestamp esto con el objetivo de obtener información del sistema a atacar.

3.2.1. Explotación de Generic-tcp-timestamp y Generic-icmp-timestamp

En el reporte ejecutivo generado por Nexpose en el apartado de la vulnerabilidad de Generic-tcp-timestamp menciona que: "El host remoto respondió con una marca de tiempo TCP. La respuesta de indicación de fecha y hora de TCP se puede usar para aproximar el tiempo de actividad del host remoto, lo que podría ayudar en futuros ataques. Además, algunos sistemas operativos pueden realizarse ataques de fingerprinting y tomar información del sistema en función del comportamiento de su marca de tiempo TCP"; esta indica que se puede explotar esta vulnerabilidad realizando un ataque fingerprinting.

Como se mencionó la computadora LAB-CM-13 es la atacante por lo que desde esta se realizó un ataque fingerprinting, para ello se utilizó la herramienta Zenmap; Zenmap es la interfaz gráfica de Nmap, esta es una herramienta que sirve para escanear una red basándose en solicitudes de conexión. La herramienta Zenmap está instalada pro defeco en la distribución Kali Linux por lo que se ejecuta desde el escritorio obteniéndose la siguiente interfaz de usuario, en ella se indica el tipo de escaneo que se desea realizar y la dirección de red, el escaneo inicia tras hacer clic en scan. El tipo de escaneo que se utilizo es un escaneo intenso hacia todos los puertos TCP. En la figura 2-3 se muestra la interfaz de usuario e inicio del escaneo.

En la figura 3-3 se observa que se descubrió 6 equipos activos en el escaneo siendo estas la dirección IP de la computadora víctima y la dirección IP de la computadora atacante. La dirección IP del servidor web y la dirección IP de Snort. En la figura 4-3 se observa las direcciones IP de cada equipo encontrado.

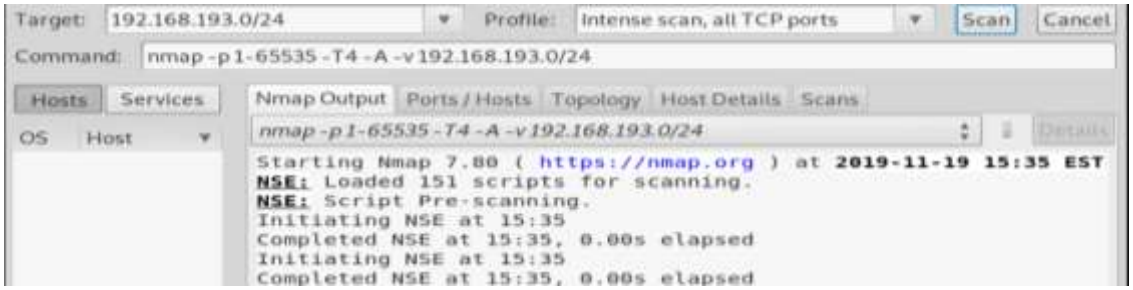


Figura 2-3: Interfaz de usuario de zenmap e inicio del escaneo realizado
Realizado por: Byron Barragán, 2020

El escaneo se demoró alrededor de 20 minutos obteniéndose los siguientes resultados.

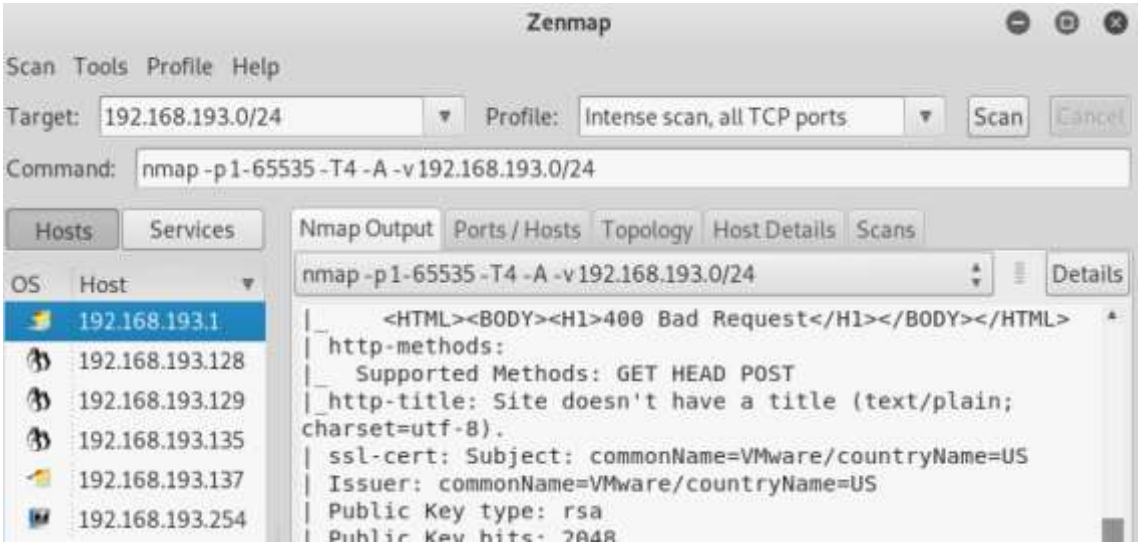


Figura 3-3: Resultado del escaneo intenso a todos los puertos TCP en el escenario virtual.
Realizado por: Byron Barragán, 2020

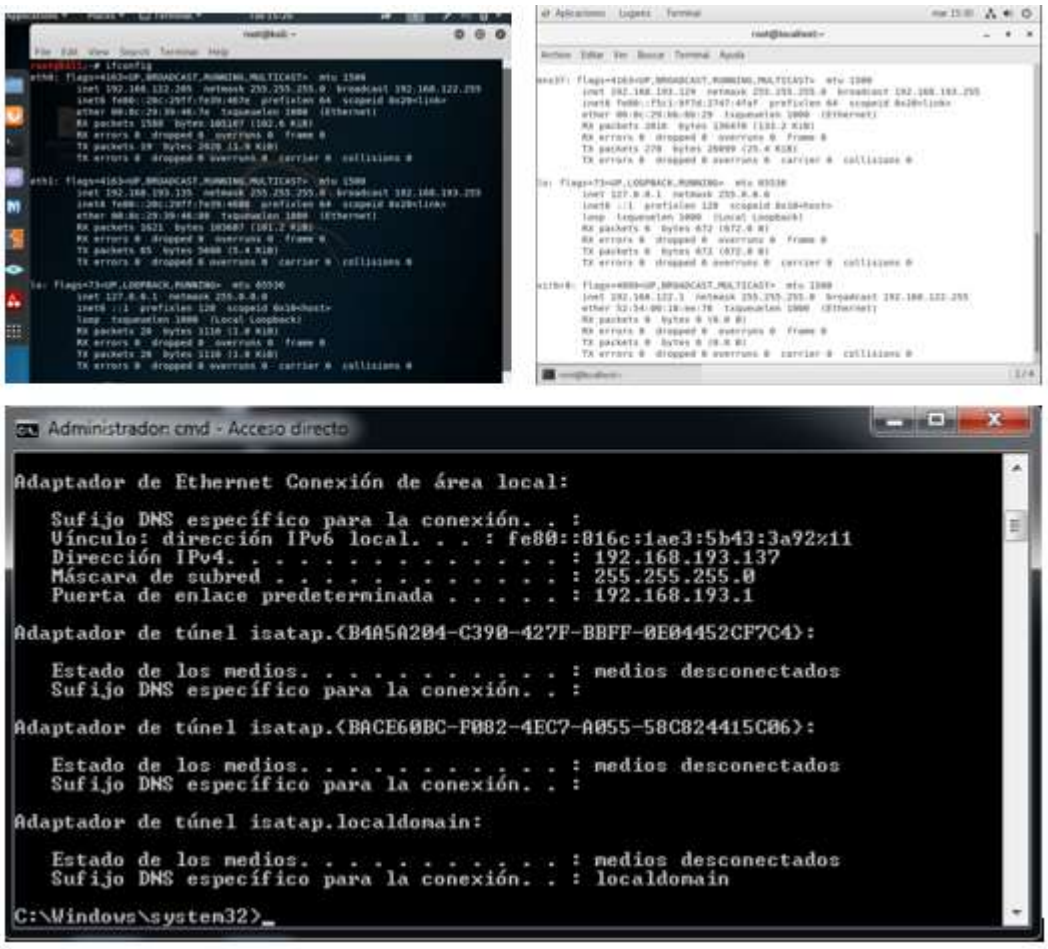


Figura 4-3: Direcciones IP de las máquinas virtuales configuradas en el escenario virtual
Realizado por: Byron Barragán, 2020

Los resultados se pueden presentar de manera específica, es decir, los puertos abiertos que se encontraron, los servicios y procesos que se manejen, la dirección IP, la dirección MAC, la

versión del sistema operativo, e incluso una topología de los equipos conectados. Los resultados obtenidos se muestran en las figuras 5-3 y 6-3.

La figura 5-3 muestra estos resultados indicando los puertos abiertos en la computadora víctima de manera resumida, además del sistema operativo Windows 7, toda esta información será de utilidad para realizar los ataques más adelante. Este ataque fingerprinting sirve como fase de reconocimiento.

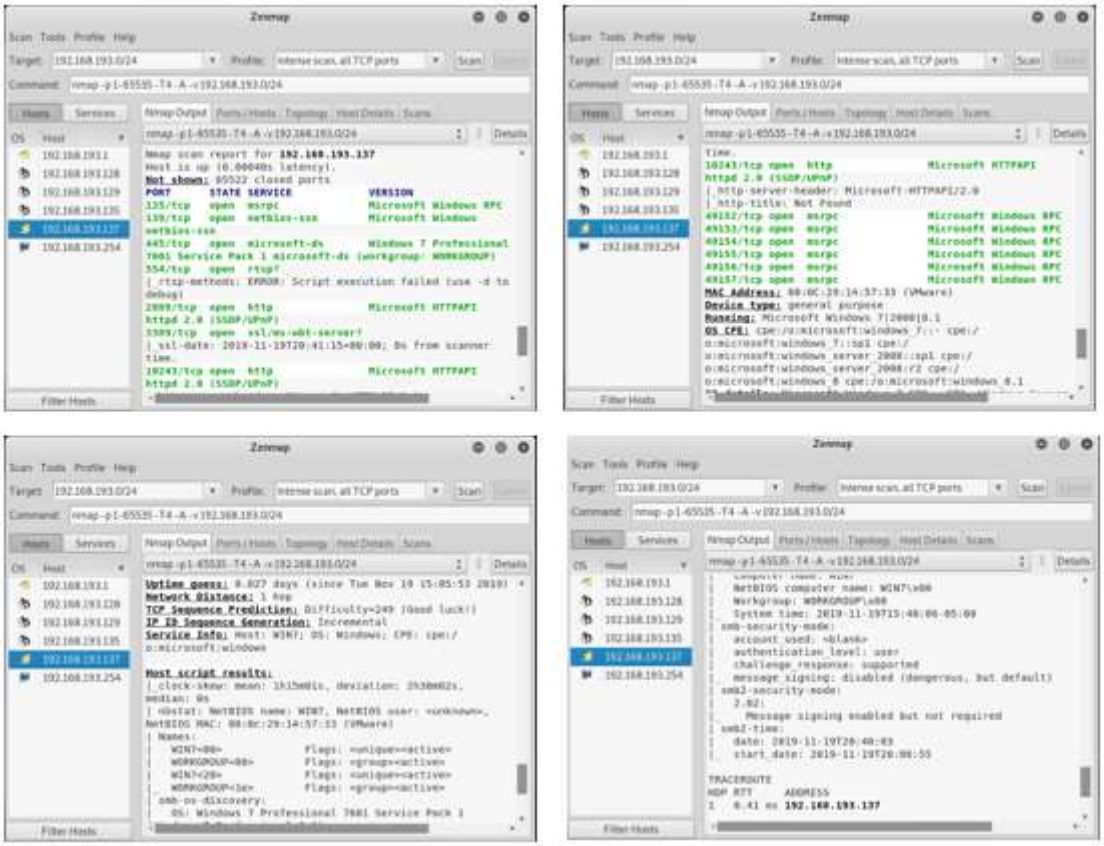


Figura 5-3: Direcciones IP de las máquinas virtuales encontradas en el escaneo.
Realizado por: Byron Barragán, 2020

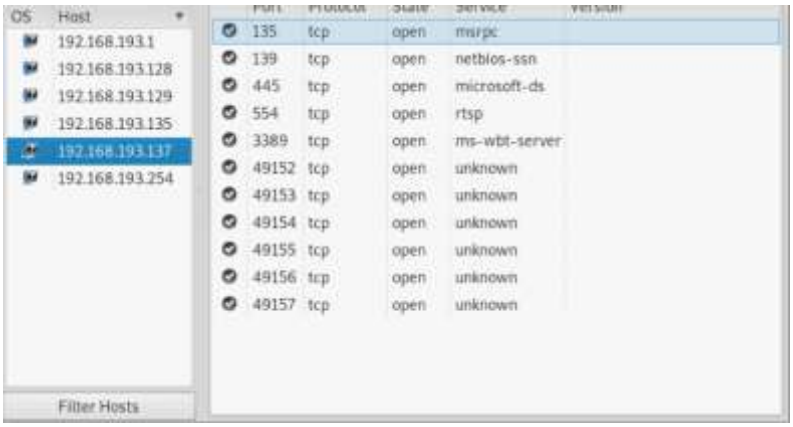


Figura 6-3: Puertos abiertos en LAB-CM-13.
Realizado por: Byron Barragán, 2020

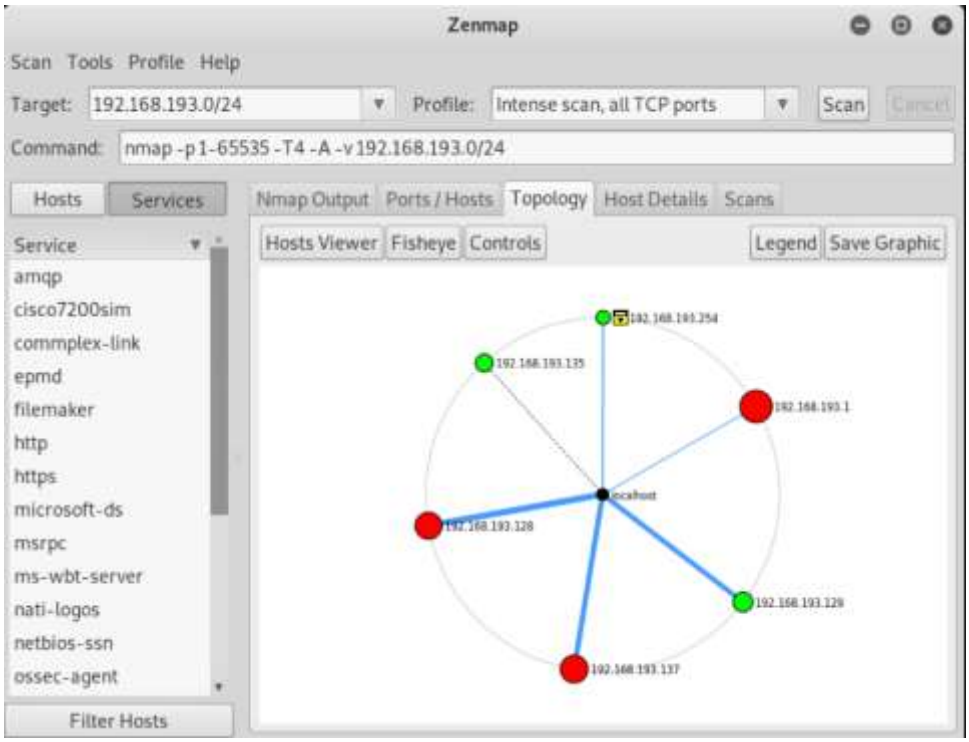


Figura 7-3: Topología de los equipos encontrados durante el escaneo de Zenmap.
Realizado por: Byron Barragán, 2020

Finalmente, en la figura 7-3 muestra la topología de los equipos conectados y encontrados durante el escaneo. La vulnerabilidad se explotó con éxito ya que en base a los resultados obtenidos se puede continuar con la fase de explotación de las siguientes vulnerabilidades y amenazas. Este ataque no fue detectado por Snort.

3.2.2. Explotación de vulnerabilidades SMB.

Para la explotación de las vulnerabilidades SMB, es necesario que el protocolo este activado en la máquina explotable de Windows 7, para Windows 7 este protocolo viene activo por defecto, al estar activado este protocolo permite la compartición de archivos e impresoras en red. La vulnerabilidad MS17-010 o Eternalblue permite a un atacante hacerse con el control de la computadora víctima. Esta vulnerabilidad se la puede explotar con la ayuda de la herramienta Metasploit ya que tiene un módulo específico para la explotación de esta vulnerabilidad trabajando en conjunto con la vulnerabilidad cifs-smb-signing-disabled que permite cualquier conexión sin autenticación, el ataque se realizó desde la computadora LAB-CM-13 hacia la computadora LAB-CM-14 siendo esta ultima la víctima. El ataque se realizó por línea de código en la consola de metasploit.

Gracias al ataque de fingerprinting que se realizó anteriormente con la herramienta Zenmap, se conoce la dirección IP de la maquina víctima, en la figura 8-3 se muestra esta dirección.

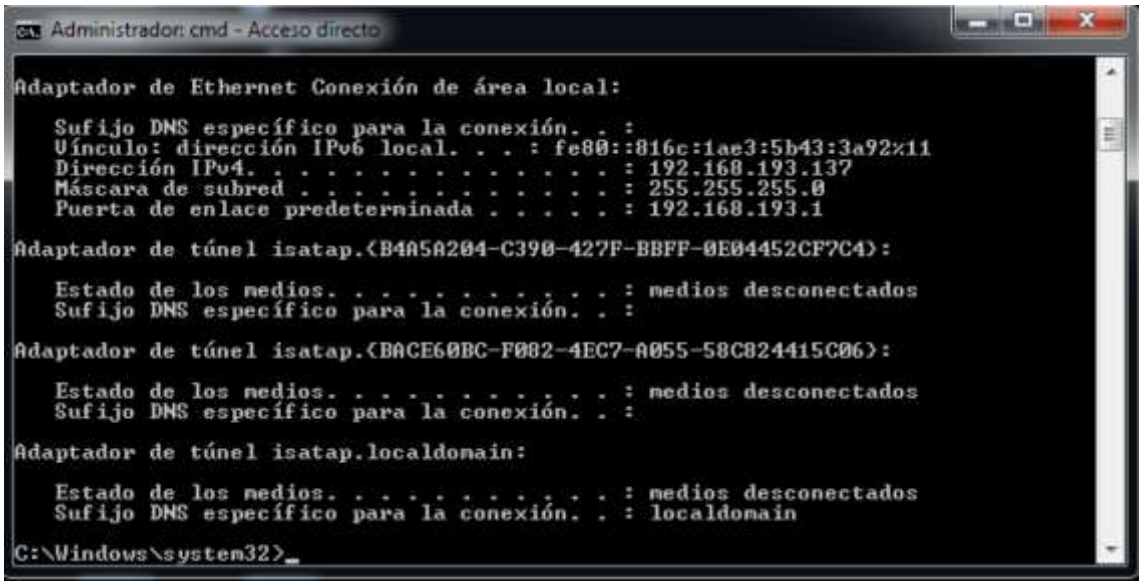


Figura 8-3: Dirección IP de la computadora víctima LAB-CM-14.
Realizado por: Byron Barragán, 2020

En el anexo O se muestra las líneas de código utilizadas para la explotación de la vulnerabilidad, antes de iniciar una consola de metasploit se debe iniciar el servicio postgresql. Después de esto se inicia la consola de metasploit y se busca un escáner para determinar si la víctima tiene la vulnerabilidad, el escáner utilizado es ***auxiliary/scanner/smb/smb_ms17_010,*** ingresando este comando e indicando la dirección IP en donde se realiza el escaneo se ejecuta y arroja el siguiente resultado mostrado en a figura 9-3.

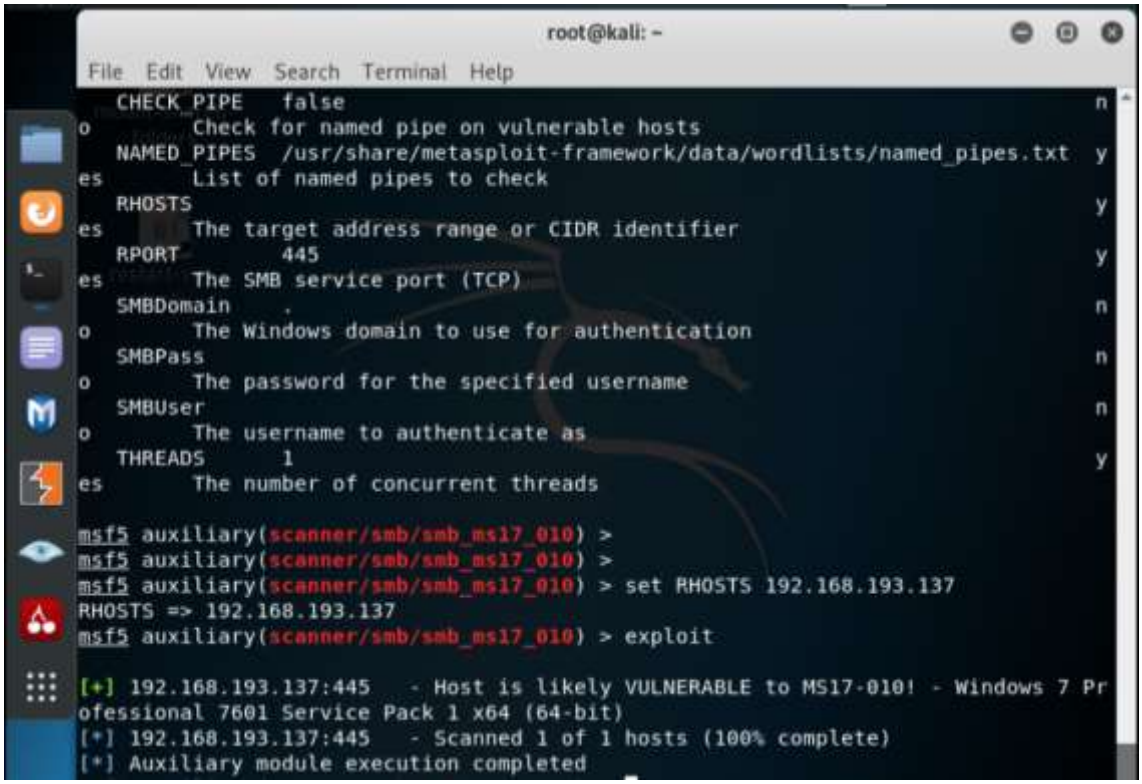


Figura 9-3: Resultado del escáner de metasploit utilizado en la computadora LAB-CM-14.
Realizado por: Byron Barragán, 2020

En la figura 9-3 se muestra el resultado, indicando que la víctima es vulnerable al módulo de metasploit MS17-010 e incluso indica la versión del sistema operativo; Windows 7 Professional 7601 Service Pack 1 x64 (64 bits).

Iniciando una nueva consola de metasploit ahora en cambio se busca el módulo para la explotación, concretamente se realiza una búsqueda de Eternalblue, una vez encontrado se utiliza el módulo con el comando ***use***. Lo que sigue después es indicar la dirección IP de la víctima y el payload, es decir, utilizar una sesión meterpreter mediante TCP para mantener la sesión conectada utilizando el puerto TCP 4444, es importante además indicar desde donde se realiza el ataque por lo que después de indicar la sesión meterpreter se debe indicar la dirección IP local desde donde se realiza el ataque. Este tipo de ataques son fácilmente detectados por un antivirus, debido a esto se debe configurar un encoder, líneas de código que ayudan a burlar a los antivirus, el encoder utilizado es un genérico como se muestra en la figura 10-3.

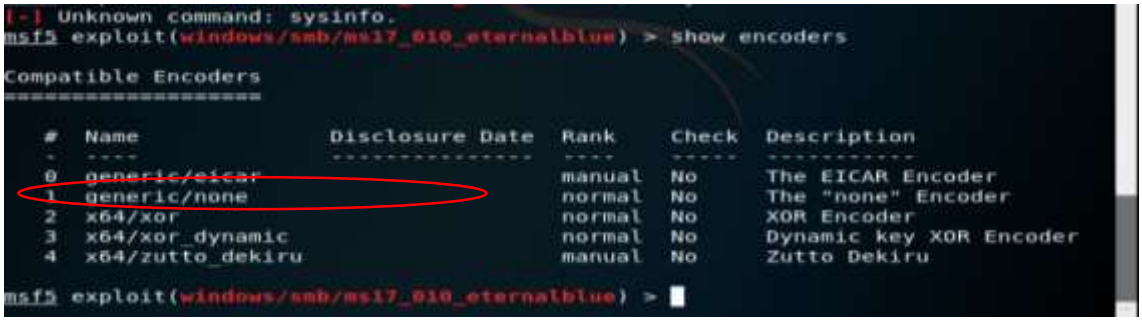


Figura 10-3: Encoder utilizado para burlar el antivirus en la computadora LAB-CM-14.
Realizado por: Byron Barragán, 2020

Finalmente, con el comando ***exploit*** se pone marcha el ataque, si no existe un error durante la configuración del módulo de ataque mostrará lo que se observa en la figura 11-3.

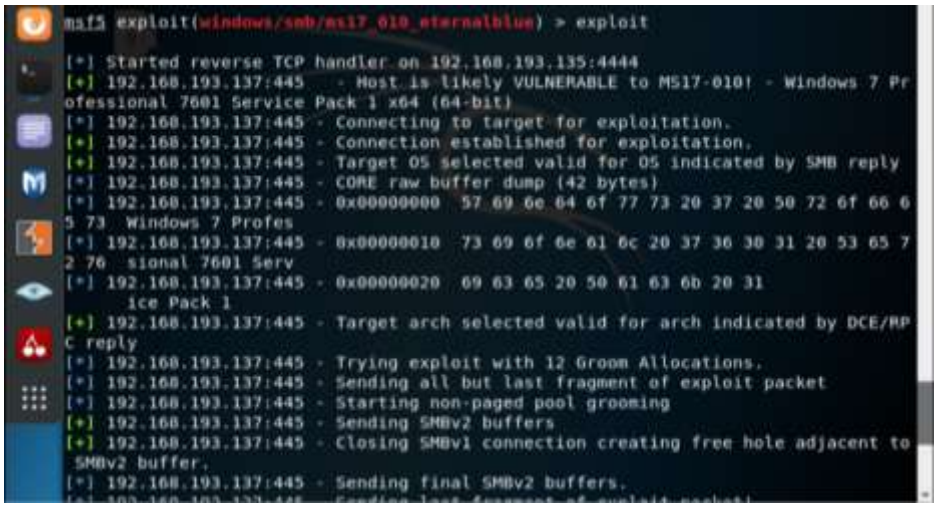


Figura 11-3: Ejecución del módulo de ataque MS17-010 Eternalblue.
Realizado por: Byron Barragán, 2020

Después de esperar unos segundos la sesión inicia indicando que el ataque se realizó con éxito, una vez iniciada la sesión meterpreter tenemos acceso total a la víctima. Para comprobar esto se puede ingresar el comando ***sysinfo*** y nos mostrará la información del sistema en el que nos encontramos. La figura 12-3 muestra lo antes descrito.

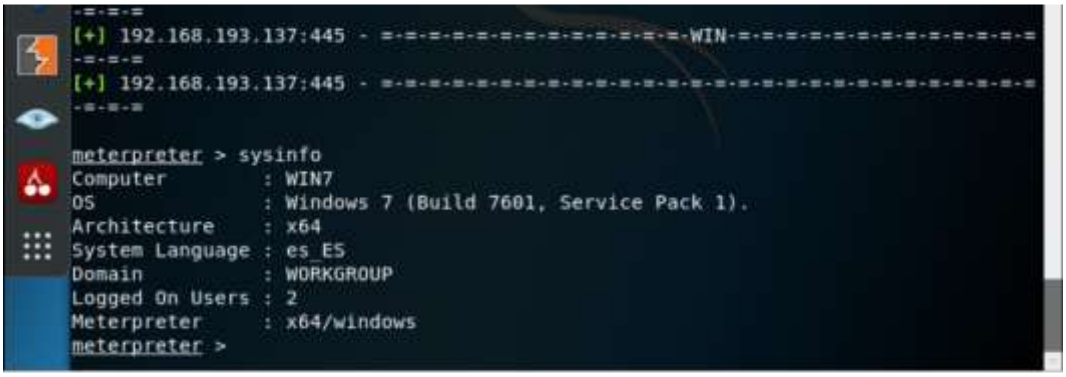


Figura 12-3: Información del sistema LAB-CM-14; sistema atacado.
Realizado por: Byron Barragán, 2020

Una vez que la sesión esta iniciada es cuestión de aplicar los comandos para observar a tiempo real lo que hace la víctima, copiar archivos, mandar mensajes, ver procesos que se ejecuten en la computadora víctima, tomar capturas de pantalla y almacenar todo tipo de información en la máquina local etc. Por ejemplo, con el comando ***run vnc*** se puede ver a tiempo real lo que el usuario de la computadora víctima está realizando. La figura 13-3 muestra la ejecución de este comando desde la consola de la sesión iniciada en metasploit.

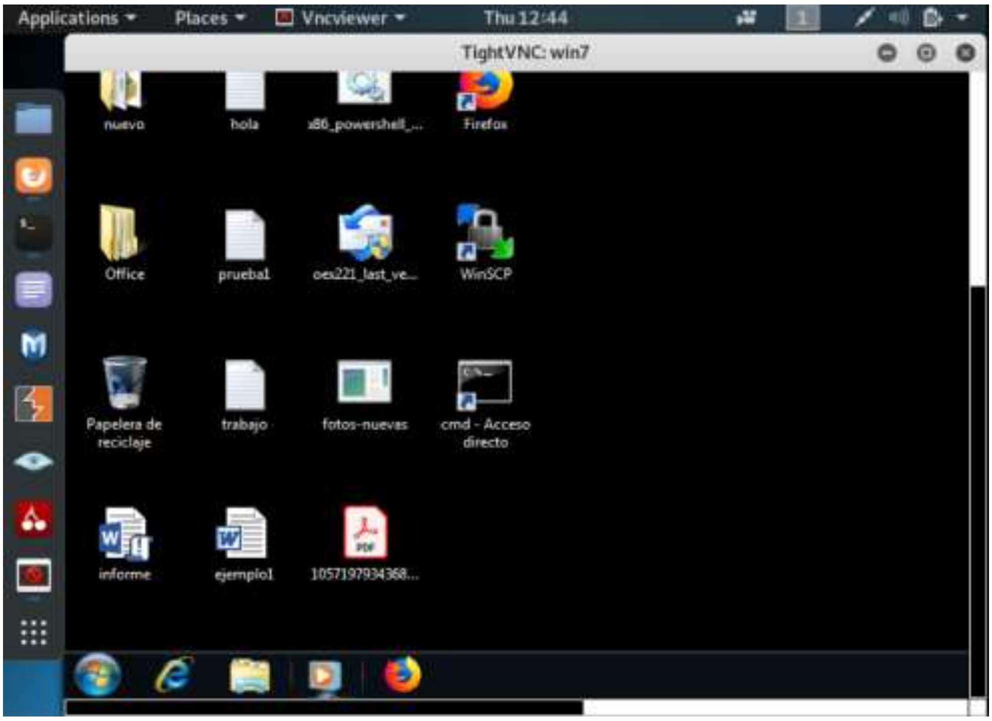


Figura 13-3: Resultado de la ejecución del comando run VNC desde la máquina atacante.
Realizado por: Byron Barragán, 2020

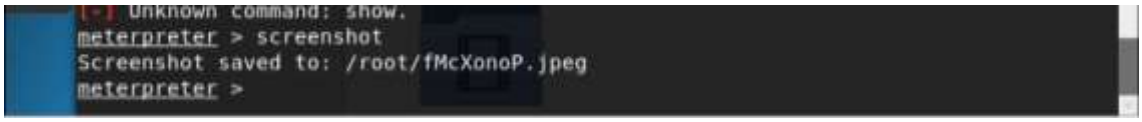


Figura 14-3: Resultado del comando screenshot.
Realizado por: Byron Barragán, 2020

La figura 14-3 indica otro comando que se puede utilizar, tomando una captura de pantalla del usuario guardándose en la ruta especificada como lo muestra la figura 15-3.

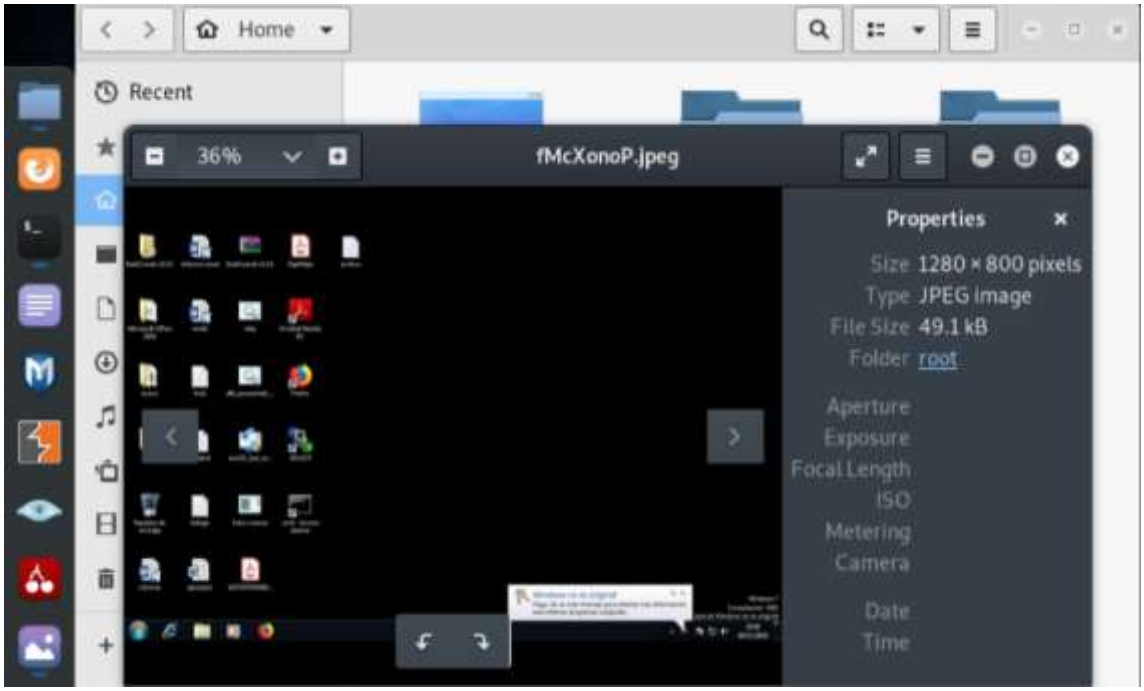


Figura 15-3 Ubicación de la captura de pantalla tomada con el comando screenshot.
Realizado por: Byron Barragán, 2020

Figura 16-3: Línea de comando para ejecutar una ventana de CMD desde la máquina atacante.
Realizado por: Byron Barragán, 2020

Figura 17-3: Ejecución del comando ipconfig desde la máquina atacante.
Realizado por: Byron Barragán, 2020

Las figuras 16 y 17 del presente capítulo muestran otro comando que se puede utilizar, en este caso para abrir una ventana de CMD. En la tabla 25-3 se muestran algunos comandos probados durante la sesión iniciada.

Tabla 25-3: Comandos probados durante el ataque a la computadora LAB-CM-14.

Comando	Descripción
Run vnc	Observar a tiempo real desde una sesión vnc que es lo que hace el usuario de la máquina víctima.
Getuid	Obtener la identificación de la máquina víctima.
Ps	Listar todos los procesos que están en ejecución en la máquina víctima.
Execute –f cmd.exe –i –H	Ejecutar una sesión de cmd desde la máquina atacante.
Keyscan_start	Iniciar un sniffer para el tráfico de la maquina víctima.
Keyscan_dump	Capturar tráfico de la máquina víctima y almacenar en la maquina atacante.
Screenshot	Tomar una captura de pantalla de la víctima y almacenarla en la maquina atacante.

Realizado por: Byron Barragán, 2020

La vulnerabilidad se explotó con éxito, desde la víctima el antivirus no detecto ninguna acción sospechosa, sin embargo, Snort si detectó este ataque, en la figura 18-3 se muestra la alerta generada por Snort durante el ataque.

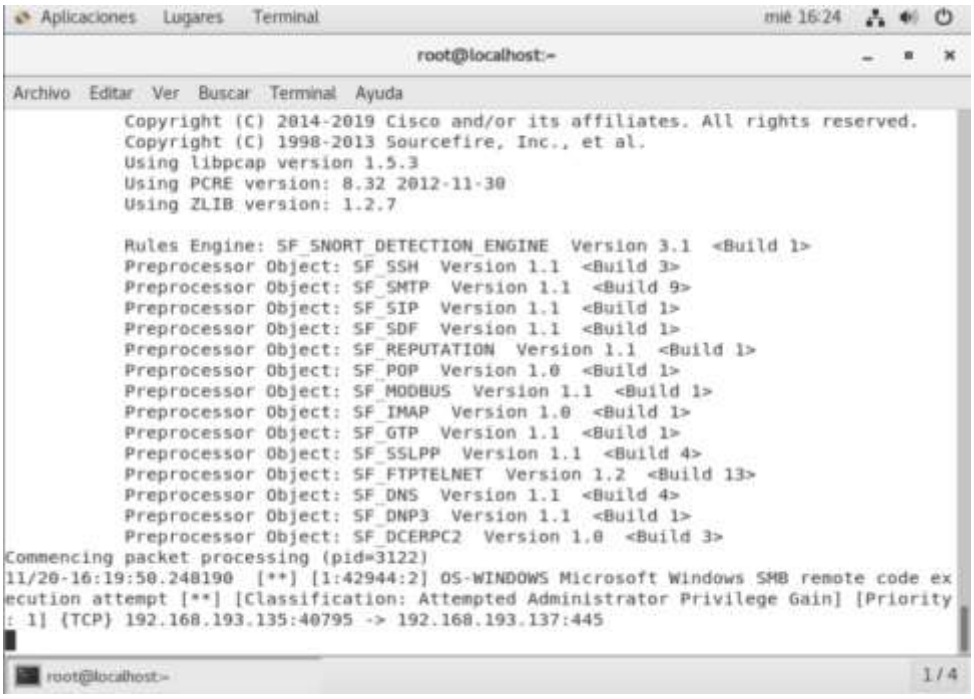


Figura 18-3: Alerta generada por Snort durante el ataque a la computadora LAB-CM-14.
Realizado por: Byron Barragán, 2020

Como se mencionó anteriormente esta vulnerabilidad se puede complementar con la ejecución del Backdoor Doublepulsar que nos permite acceder a la víctima, para ello se utiliza las siguientes líneas de código para implementar este Backdoor en la víctima.

Use exploit/windows/smb/eternalblue_doublepulsar
Set TARGETARCHITECTURE x64
Set PROCESSINJECT Insider.exe
Exploit

Estas líneas indican que se creó un proceso llamado Insider.exe con el cual se puede acceder a la víctima. Este proceso creado se puede observar desde administrador de tareas de Windows en la computadora víctima, cabe indicar que este proceso después de un tiempo se esconde. La figura 19-3 muestra el proceso creado en la víctima.

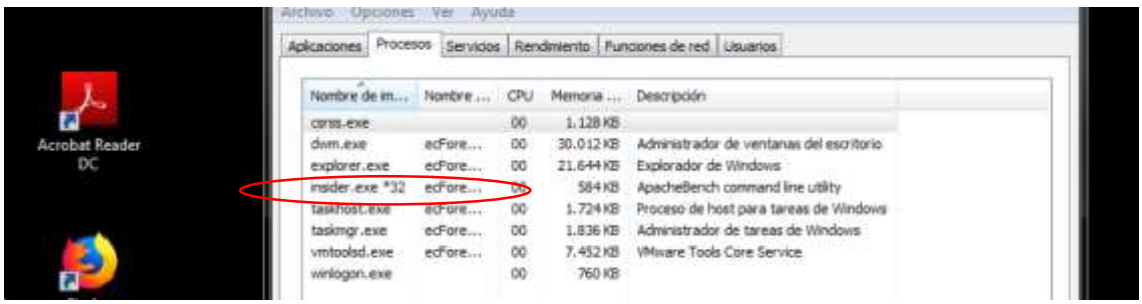


Figura 19-3: Proceso creado en la computadora LAB-CM-14.
Realizado por: Byron Barragán, 2020

Este Backdoor fue detectado de la misma manera por Snort debido a que las amenazas se relacionar teniendo un identificador de alerta igual.

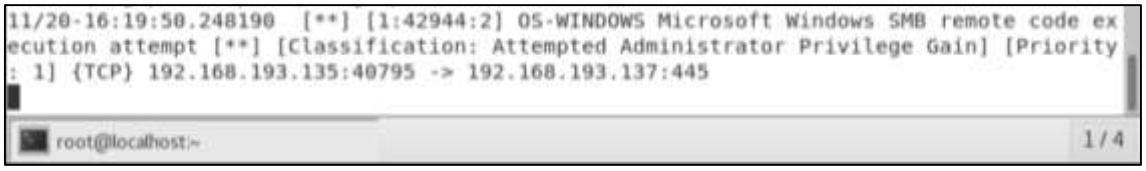


Figura 20-3: Alerta generada por el Backdoor Doublepulsar.
Realizado por: Byron Barragán, 2020

3.2.3. Explotación de vulnerabilidades de tipo denegación de servicio

Como se observó en la tabla 23-3, el 8% de las vulnerabilidades encontradas pertenecen al tipo de denegación de servicio, es decir, que se puede explotar con este tipo de ataques. Para realizar la explotación, en el escenario virtual se instaló un servidor web apache configurado la página por defecto para realizar las pruebas como se observa en la figura 21-3, siendo esta el objetivo del ataque. Para cumplir con el objetivo se utiliza la herramienta Slowloris que permite mediante una línea de comando realizar un ataque de denegación de servicio, usa tráfico HTTP (Hipertext Transfer Protocol) hace una conexión TCP completa y luego requiere solo unos pocos cientos de solicitudes a largo plazo e intervalos regulares. Como resultado, la herramienta no necesita enviar mucho tráfico para agotar las conexiones disponibles en un servidor. eventualmente, todas las conexiones se agotarán y ningún otro servidor podrá conectarse hasta que se liberen al menos algunas de las conexiones retenidas. Esta herramienta fue desarrollada por Robert Hansen y escrita en el lenguaje de programación perl con soporte multiplataforma**.** Slowloris permite que una sola máquina pueda denegar el servicio.

El ataque se va a realizar desde la computadora LAB-CM-13 hacia el servidor web siendo esta último la víctima.

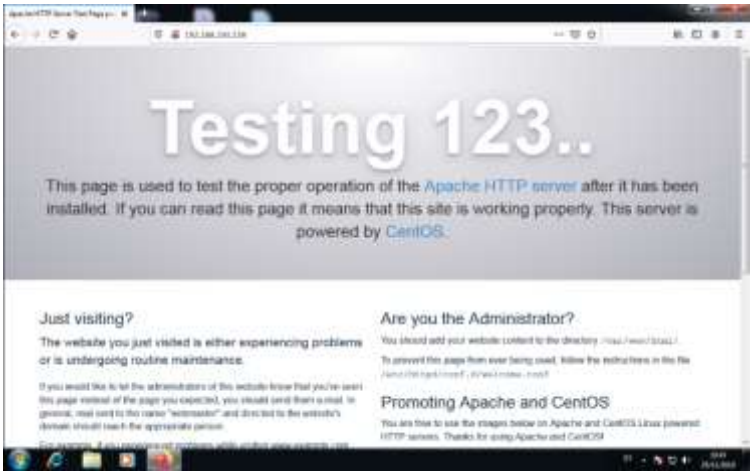


Figura 21-3: Página por defecto de apache, objetivo del ataque.
Realizado por: Byron Barragán, 2020

En apartados anteriores se realizó un escaneo del escenario y se obtuvo las direcciones IP por lo que esa información se utiliza en este ataque. La dirección IP del servidor web apache en el escenario es 192.168.193.138/24 como se observa en la figura 1-3. Primero se debe adquirir la herramienta para ello se abre una ventana del terminal de Kali Linux y se clona la herramienta con la línea de comando:

Git clone https://github.com/llaera/slowloris.pl.git.

Después de la adquisición de la herramienta se ingresa al directorio en donde se guardó la herramienta y se ejecuta la línea de comando para el ataque: ***Perl slowloris.pl –dns 192.168.193.138 –port 80 –time 1 –num 5000 –cache.***

Esta línea indica que se ejecute un ataque hacia la dirección IP del servidor web enviando 5000 paquetes TCP a través del puerto 80 cada 1 segundo y además que se almacenen los paquetes en cache. La definición del número de paquetes para la ejecución del ataque se realizó en base a los logs almacenados de las alertas detectadas con Snort durante el análisis del tráfico, más concretamente se revisó el log almacenado perteneciente al día en que sucedió el intento de ataque de denegación de servicio, se pudo determinar que el ataque tuvo una duración de aproximadamente de 10 minutos en el que se enviaron alrededor de 5000 paquetes en un segundo. Esta información fue tomada como punto de partida ya que se realizaron 30 pruebas cada una variando la cantidad de paquetes que se enviaron durante un segundo registrando el tiempo en el que se daba la denegación al objetivo, la variación de los paquetes se dio hasta duplicar la cantidad de paquetes enviado en la primera prueba, en la tabla 26-3 se puede observar los resultados. Tras la ejecución del comando la página por defecto de apache comenzó a tener dificultades de acceso hasta que finalmente no pudo acceder, en la figura 22-3 muestra la página por defecto durante el ataque. Durante el ataque se ejecutó además Wireshark para comprobar los paquetes que se enviaban durante el ataque. Esto se muestra en la figura 23-3.

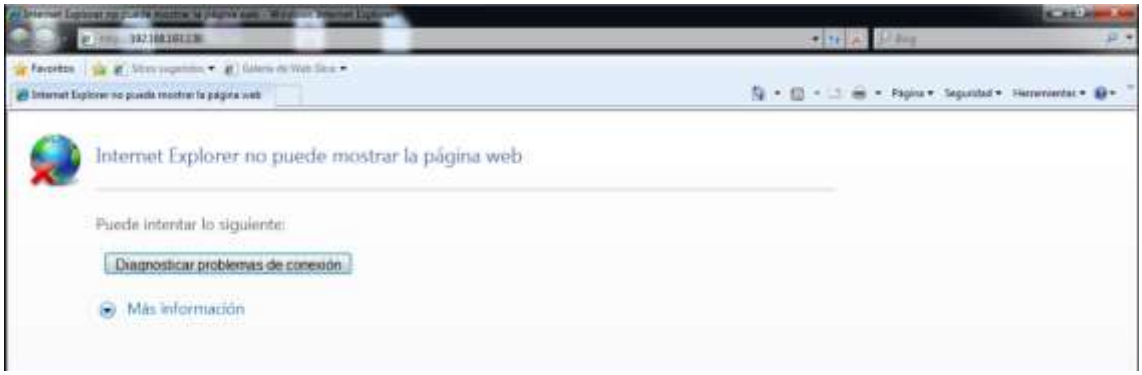


Figura 22-3: Página por defecto de apache, durante la ejecución del ataque
Realizado por: Byron Barragán, 2020

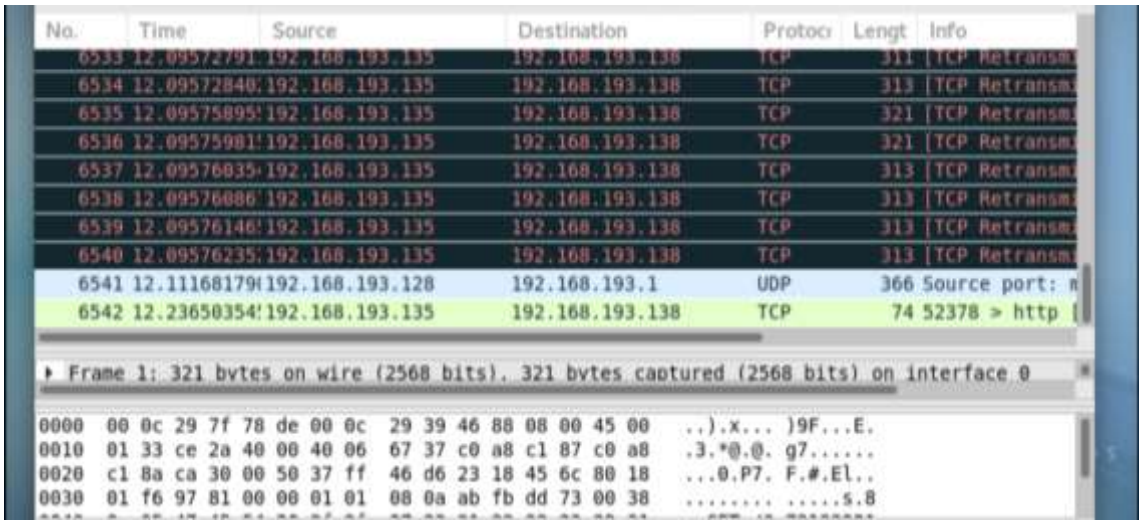


Figura 23-3: Resultados de Wireshark durante la ejecución del ataque
Realizado por: Byron Barragán, 2020

Tabla 26-3: Comandos probados durante el ataque a la computadora LAB-CM-14

Prueba	Tiempo	Paquetes	Tiempo de denegación (Segundos)	Tiempo de recuperación (Segundos)
1	1	5000	87,99	0,5
2	1	5173	70,27	0,5
3	1	5346	68,45	0,5
4	1	5519	68,75	0,5
5	1	5692	69,41	0,5
6	1	5865	71,26	0,5
7	1	6038	68,23	0,5
8	1	6211	67,49	0,5
9	1	6384	64,5	0,5
10	1	6557	65,28	0,5
11	1	6730	66,27	0,5
12	1	6903	64,74	0,5
13	1	7076	63,29	0,5
14	1	7249	67,23	0,5
15	1	7422	68,91	0,5
16	1	7595	61,32	0,5
17	1	7768	60,15	0,5
18	1	7941	62,31	0,5
19	1	8114	64,78	0,5

20	1	8287	68,29	0,5
21	1	8460	63,24	0,5
22	1	8633	59,23	0,5
23	1	8806	57,12	0,5
24	1	8979	59,32	0,5
25	1	9152	60,32	0,5
26	1	9325	59,21	0,5
27	1	9498	57,32	0,5
28	1	9671	55,76	0,5
29	1	9844	53,24	0,5
30	1	10017	56,38	0,5

Realizado por: Byron Barragán, 2020

El objetivo de realizar 30 pruebas fue determinar si al duplicar la cantidad de paquetes el tiempo de denegación se disminuía a la mitad, sin embargo, al observar los resultados de la tabla 26-3 y el Gráfico 11-3 se concluye que el tiempo tiende a disminuir, pero no a la mitad. El tiempo de recuperación no vario en ninguna prueba siempre fue de 0.5 segundos. Un usuario insider puede utilizar esta herramienta para enviar paquetes e intentar denegar un servicio o simplemente ralentizar la red en sí.

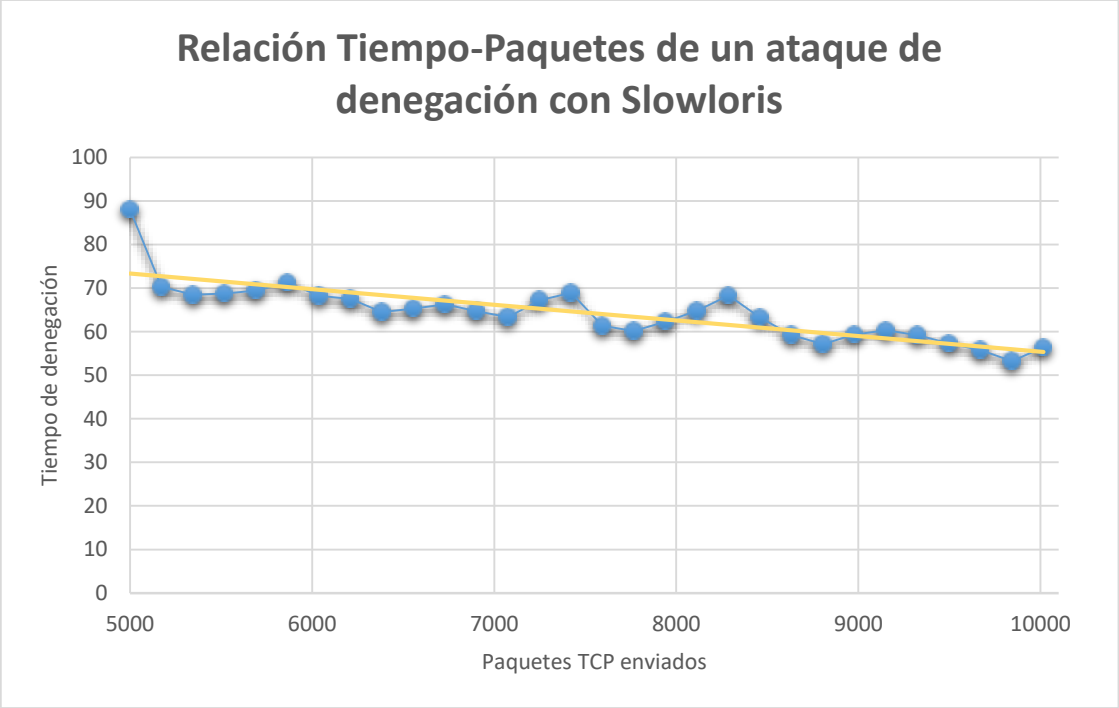


Gráfico 11-3: Relación Tiempo- Paquetes en un ataque de denegación de servicio usando Slowloris

3.2.4. Explotación utilizando Malware ZeuS.

Para la explotación se utiliza una muestra del malware ZeuS y se ejecuta en la computadora víctima. Se seleccionó este malware debido a que fue el que se detectó con más frecuencia durante el análisis con Snort. Como se mencionó anteriormente este malware tiene varias versiones por lo que encontrar una muestra de este malware con la versión exacta que se detectó durante el análisis de tráfico es complicado sin embargo gracias al repositorio de la página web https://www.grc.com/malware.htm se pudo conseguir una versión del malware ZeuS conocido como malware ZeroAccess.

Para esta prueba no se tuvo conectividad entre las máquinas virtuales con la máquina física ya que el malware que se maneja es malicioso y puede contagiar la computadora física.
En la figura 24-3 se observa la descarga de la muestra de malware, esta versión se presenta con una extensión pdf.

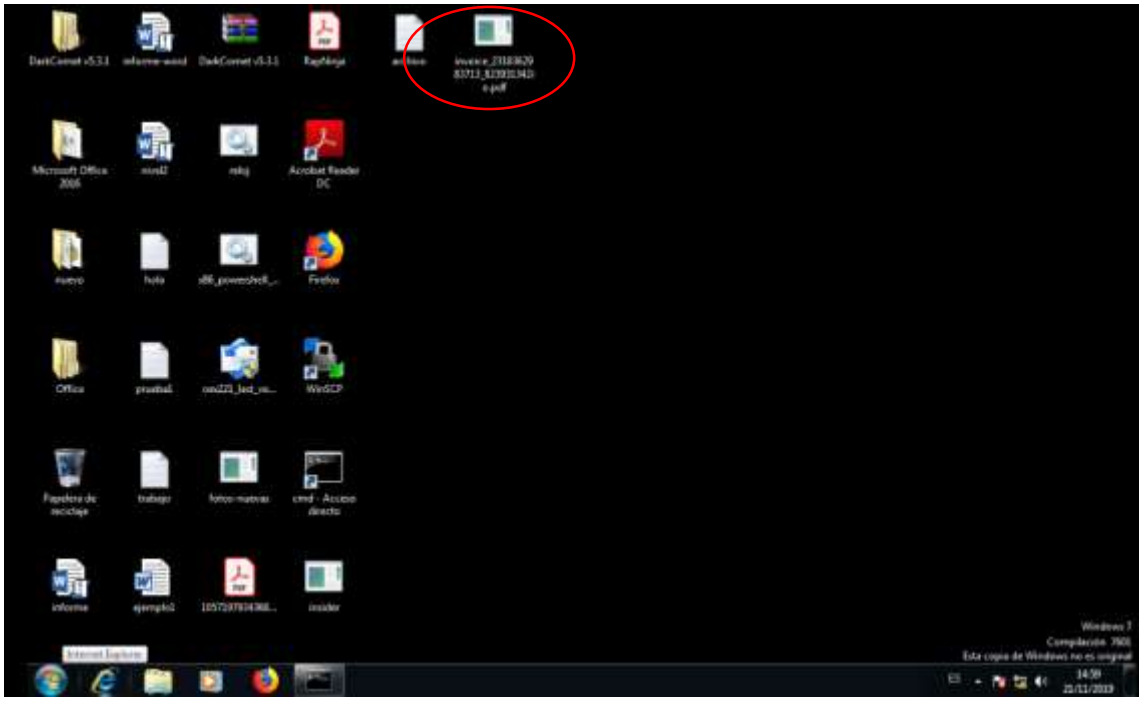


Figura 24-3: Muestra del malware ZeuS
Realizado por: Byron Barragán, 2020

Al ejecutar el malware nos presenta una ventana de error de comunicación y actualización de adobe flash player ya que este malware pretendía ser un instalador de actualización de este programa. Esto se puede observar en la figura 25-3.

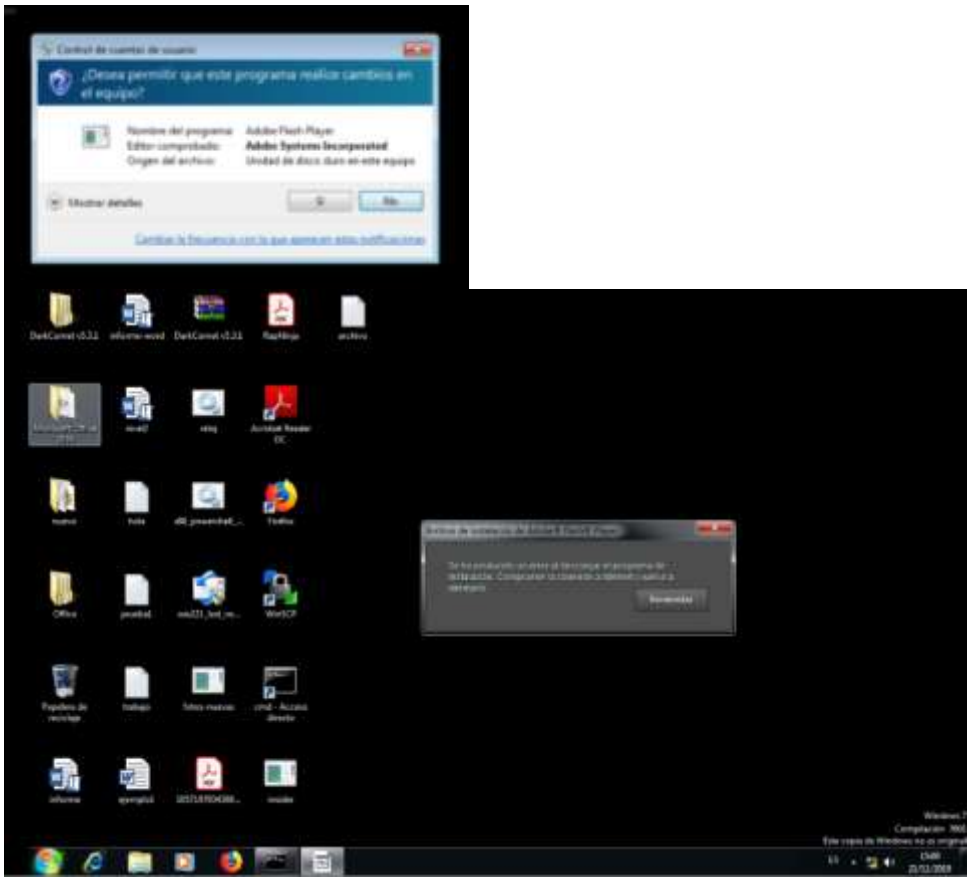


Figura 25-3: Ejecución de la Muestra del malware ZeuS
Realizado por: Byron Barragán, 2020

Como se observa en la figura 25-3 se observa que, durante la ejecución de la muestra del malware, el icono desaparece y aparentemente no ocurrió nada, sin embargo, el malware ya está en ejecución en segundo plano. Snort pudo detectar este malware y mostraba alertas como se puede ver en la figura 26-3

```
Commencing packet processing (pid=3269)
11/21-15:00:18.395603  [**] [1:23492:5] MALWARE-CNC Win.Trojan.ZeroAccess outbound conn
ection [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168
.193.137:61547 -> 85.114.128.127:53
11/21-15:00:18.397196  [**] [1:23492:5] MALWARE-CNC Win.Trojan.ZeroAccess outbound conn
ection [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168
.193.137:61548 -> 85.114.128.127:53
11/21-15:00:18.498329  [**] [1:23492:5] MALWARE-CNC Win.Trojan.ZeroAccess outbound conn
ection [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168
.193.137:61549 -> 85.114.128.127:53
11/21-15:00:18.498448  [**] [1:23492:5] MALWARE-CNC Win.Trojan.ZeroAccess outbound conn
ection [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168
.193.137:61550 -> 85.114.128.127:53
11/21-15:00:18.498662  [**] [1:23492:5] MALWARE-CNC Win.Trojan.ZeroAccess outbound conn
ection [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168
root@localhost:~                                                              1 / 4
```

Figura 26-3: Alertas generadas durante la ejecución del malware
Realizado por: Byron Barragán, 2020

El ataque continuó por 30 minutos y Snort arrojo los siguientes resultados mostrados en la tabla 27-3.

Tabla 27-3: Alertas registradas durante 30 minutos de ataque

Tiempo de ataque	Alertas registradas
10 minutos	1248
20 minutos	1216
30 minutos	1223
Total	3687

Realizado por: Byron Barragán, 2020

Cada 10 minutos el malware generaba alrededor de 1200 alertas teniendo un total de alrededor de 3600 alertas en 30 minutos. Además, se registró la utilización de recursos de memoria en la computadora víctima presentada en la tabla 28-3 y en la figura 27-3.

Tabla 28-3: Porcentaje de utilización de recursos de la máquina víctima

Tiempo de ataque	% de utilización de memoria antes del ataque	% de utilización de memoria durante el ataque
10 minutos	26%	32%
20 minutos	27%	36%
30 minutos	26%	37%

Realizado por: Byron Barragán, 2020

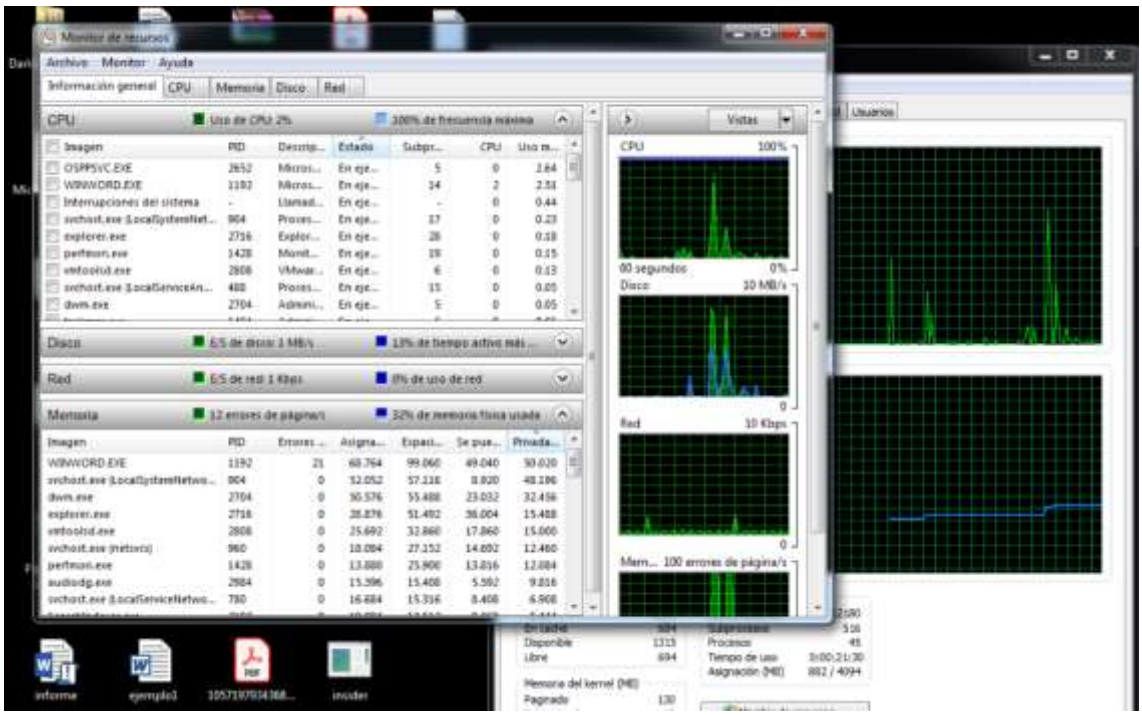


Figura 27-3: Uso de recursos de la máquina víctima

Realizado por: Byron Barragán, 2020

En la tabla 28-3 se observa que el porcentaje de utilización de recursos aumenta conforme el tiempo del ataque aumenta. Aparentemente no hay mucha diferencia, pero por lo general este malware no trabaja solo, sino que se complementa con otras versiones y con el ransomware CryptoLocker aumentando así más el porcentaje de utilización de recursos llegando un punto en que utilizar la computadora víctima del ataque va a ser complicado. Al apagar la maquina victima Snort ya no presenta alertas, sin embargo, al encender las alertas continúan por lo que este es un ataque de malware continuado lo que concuerda con lo detectado con Snort y este malware generando un número elevado de alertas. Un usuario insider puede infectar la computadora víctima dejando una copia de este malware y ejecutarla causando un funcionamiento no eficiente en la computadora víctima.

CAPITULO IV

4. GUIA DE SOLUCION PARA LAS VULNERABILIDADES Y AMENAZAS EXPLOTADAS

4.1. Solución para la vulnerabilidad: Generic-tcp-timestamp y Generic-icmp-timestamp.

Estas vulnerabilidades son las más comunes encontradas por Nexpose, en el reporte ejecutivo generado después del escaneo se presenta posibles soluciones para estas vulnerabilidades en diferentes sistemas operativos, las cuales son desactivar tcp timestamp e icmp timestamp en general, a continuación, se muestra estas soluciones.

- **Sistemas Cisco.**

Ejecutar el comando: ***no ip tcp timestamp***

- **Sistemas FreeBSD y OpenBSD.**

Establecer el valor de net.inet.tcp.rfc1323 en 0 ejecutando el comando: ***sysctl -w net.inet.tcp.rfc1323=0***

Además, coloque el siguiente valor en el archivo de configuración predeterminado de sysctl, generalmente sysctl.conf: ***net.inet.tcp.rfc1323=0***

- **Sistemas operativo Linux.**

Desactivar tcp timestamp estableciendo el valor de net.ipv4.tcp_timestamps en 0 ejecutando el comando: ***sysctl -w net.ipv4.tcp_timestamps=0***

Además, coloque el siguiente valor en el archivo de configuración predeterminado de sysctl, generalmente sysctl.conf: ***net.ipv4.tcp_timestamps=0***

- **Varias Sistemas operativos Windows**

Esta vulnerabilidad fue encontrada en su mayoría en sistemas operativo Windows 7 por lo que esta solución se prueba en el escenario virtual, para ello se ingresa desde el editor del registro del sistema (Windows + r y escribir regedit) a la dirección: ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters,*** incluir un Dword con nombre ***TCP1323Opts*** y poner el valor 1 como se muestra en la figura 1-4.

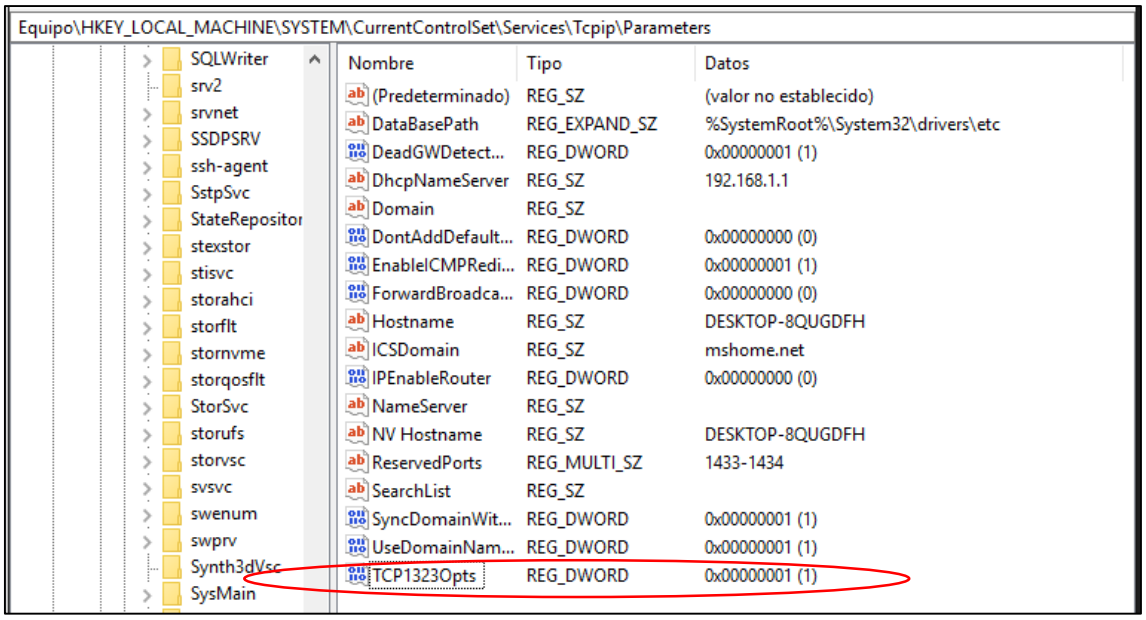


Figura 1-4: Solución, deshabilitar la respuesta de marca de tiempo TCP en Windows
Realizado por: Byron Barragán, 2020

Tcp1323Opts le permite al sistema utilizar el RFC 1323, este RFC en particular funciona con marca de tiempo y escala de ventana de red. La opción que está editando en la figura 1-4 es un valor de dos bits donde el bit inferior especifica si desea utilizar el escalado de la ventana y el bit superior especifica si desea utilizar las marcas de tiempo, en este caso el valor "1" indica que no se desea utilizar las marcas de tiempo TCP.

En algunos sistemas operativos de Windows sobre todo los más actualizados los paquetes TCP timestamp no se pueden deshabilitar de forma fiable. Si la vulnerabilidad tcp-timestamp presenta suficiente riesgo, se debe colocar un firewall capaz de bloquear paquetes tcp-timestamp frente a los objetivos afectados. Este no fue el caso ya que el sistema operativo de las computadoras escaneadas con Nexpose es Windows 7.

4.1.1. Solución contra amenazas de ataques fingerprint.

Se presentan algunas soluciones preventivas para este tipo de ataques como, por ejemplo:

- Instalación de parches de seguridad.
- Utilización de herramientas como VPN (Virtual Private network)
- Configuración de Firewalls en contra de ataques.
- Configuración de sistemas de detección de intrusos en red (NIDS) en los objetivos.

Este último se tiene configurado en el escenario virtual, Con Snort se puede configurar una regla específica para el tráfico de estos tipos de ataques o a su vez instalar otro NIDS que al

momento de realizar un ataque fingerprinting pueda detectarlo como por ejemplo Suricata. En la figura 2-4 se observa una captura de una alerta con el NIDS Suricata.

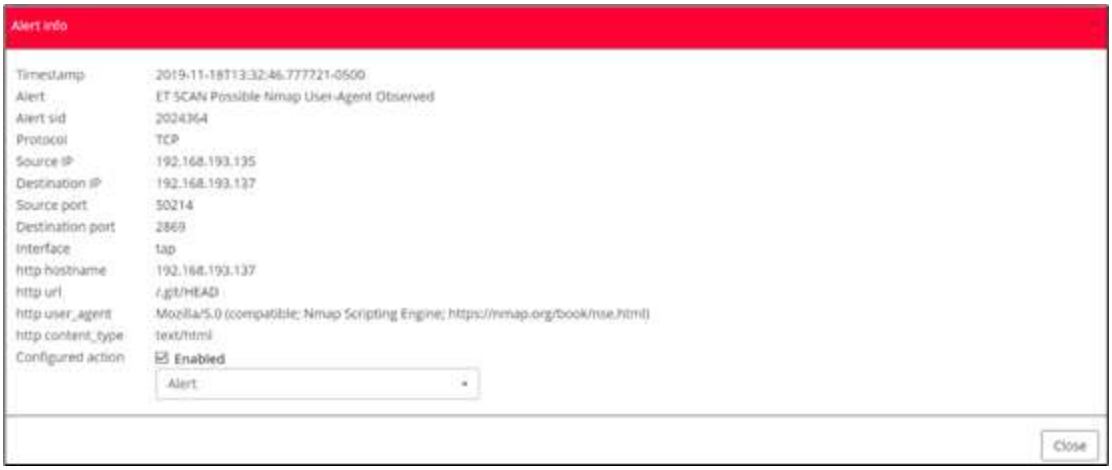


Figura 2-4: Detección del ataque fingerprinting por el NIDS Suricata

La alerta saltó en la interfaz de usuario del NIDS indicando la dirección IP de origen y destino, así como también los puertos que se utilizaron para la conexión. Una vez detectado se puede tomar acciones para detectar quien es el usuario insider.

4.2. Solución para las vulnerabilidades SMB: cifs-smb-signing-disabled, cifs-smb-signing-not-required, cifs-smb2-signing-disabled, MS17-010 (Eternalblue) y Doublepulsar

4.2.1. Solución vulnerabilidades: cifs-smb-signing-disabled, cifs-smb-signing-not-required, cifs-smb2-signing-disabled.

Existen dos soluciones para estas vulnerabilidades, la primera de ellas es activando la utilización de la firma SMB en los equipos de usuario pertenecientes a las Vlans, en el reporte generado con Nexpose indica un enlace hacia el blog escrito por José Barreto miembro del equipo OneDrive de Microsoft en donde se encuentra la configuración de los valores predeterminados para los protocolos SMBv1 y SMBv2. En el blog dice: "Hay dos formas principales de configurar la firma para clientes SMB1 y servidores SMB1. La más fácil es establecer una Política de grupo para configurarla. Así es, por ejemplo, cómo los controladores de dominio están configurados de manera predeterminada para requerir la firma. La otra forma de hacerlo es mediante la configuración del registro. En cada lado (cliente SMB1 y servidor SMB1), la firma SMB1 se puede configurar como Requerida, Activada o Desactivada" (Barreto, 2010). La tabla 1-4 muestra un resumen de la configuración de la firma SMBv1 para cliente y la tabla 2-4 para servidor.

Tabla 1-4: Resumen de la configuración de la firma SMBv1 para cliente

Ajuste	Configuración de directiva de grupo	Claves de registro
Requerida	Firmar digitalmente las comunicaciones (siempre): activado	RequireSecuritySignature = 1
Activado	Firmar digitalmente las comunicaciones (si el servidor está de acuerdo): Activado	EnableSecuritySignature = 1, RequireSecuritySignature = 0
Desactivado	Firmar digitalmente las comunicaciones (si el servidor está de acuerdo): desactivado	EnableSecuritySignature = 0, RequireSecuritySignature = 0

Fuente: (Barreto, 2010)

Tabla 2-4: Resumen de la configuración de la firma SMBv1 para servidor

Ajuste	Configuración de directiva de grupo	Claves de registro
Requerida	Firmar digitalmente las comunicaciones (siempre): activado	RequireSecuritySignature = 1
Activado	Firmar digitalmente las comunicaciones (si el cliente está de acuerdo): activado	EnableSecuritySignature = 1, RequireSecuritySignature = 0
Desactivado	Firmar digitalmente las comunicaciones (si el cliente está de acuerdo): desactivado	EnableSecuritySignature = 0, RequireSecuritySignature = 0

Fuente: (Barreto, 2010)

SMB2 simplificó esta configuración al tener solo una configuración: si era necesario firmar o no. Esto se puede configurar a través de la directiva de grupo o la configuración del registro, en clientes SMB2 y servidores SMB2. En cada lado, la firma se puede configurar como "Requerida" o "No requerida". (Barreto, 2010). En la tabla 3-4 se muestra la configuración de la firma SMBv2 en cliente y servidor.

Tabla 3-4: Resumen de la configuración de la firma SMBv2

Ajuste	Configuración de directiva de grupo	Claves de registro
Requerido	Firmar digitalmente las comunicaciones (siempre): activado	RequireSecuritySignature = 1
No requerido	Firmar digitalmente las comunicaciones (si el servidor está de acuerdo): desactivado	RequireSecuritySignature = 0

Fuente: (Barreto, 2010)

Para realizar la configuración mostrada en las tablas 1-4 y 2-4 se debe editar el registro del sistema tecleando Windows + r y escribiendo regedit. Una vez dentro se debe dirigir a: ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters*** para el caso de SMBv1 y SMBv2 para clientes y para servidor dirigirse a: ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameter*** para SMBv1 y SMBv2. Todas las claves de registro son de tipo DWORD, haciendo clic derecho sobre la clave de registro En la figura 3-4 se muestra la configuración realizada correctamente para cliente y la figura 4-4 la configuración para servidor.

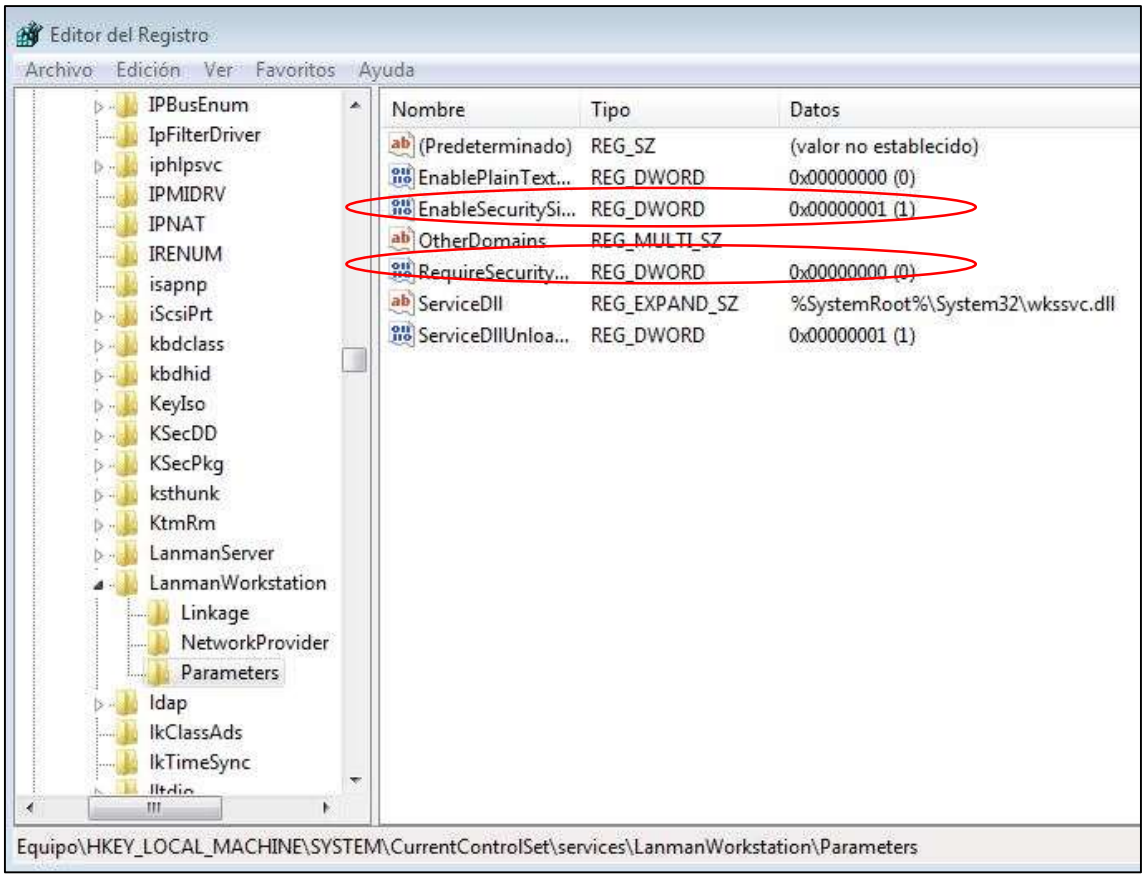


Figura 3-4 Configuración de la activación de la firma SMBv1 para cliente
Realizado por: Byron Barragán, 2020

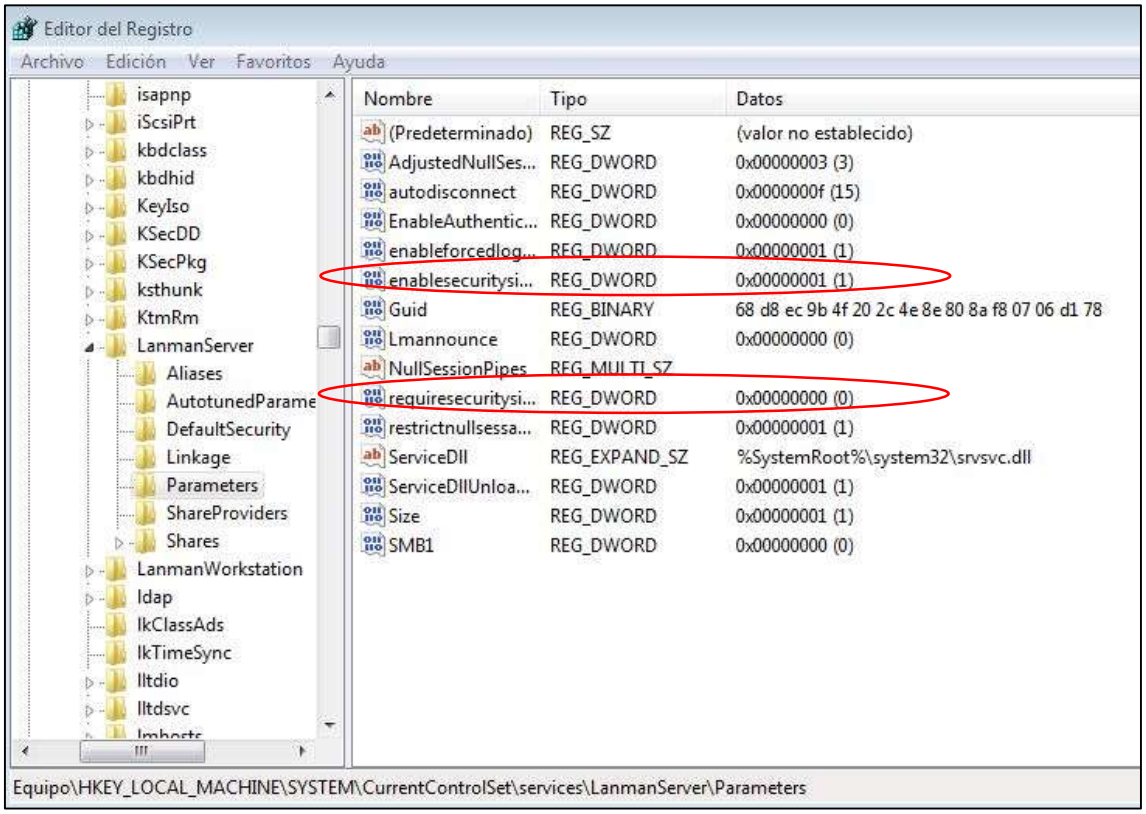


Figura 4-4: Configuración de la activación de la firma SMBv1 para servidor
Realizado por: Byron Barragán, 2020

La otra forma de solucionar las vulnerabilidades es deshabilitando el protocolo SMBv1. Desde 2014 el protocolo SMBv1 está obsoleto por lo que se recomienda deshabilitar esta versión del protocolo, para esto se debe hacer lo siguiente:

Para Windows 8 en adelante:

Se puede desactivar el protocolo SMBv1 de forma gráfica para ello se debe dirigir a panel de control/programas y características, al lado izquierdo de la ventana hacer clic en activar o desactivar características de Windows y finalmente desmarcar la opción Compatibilidad con el protocolo para compartir archivos SMB1.0/CIFS. La figura 5-4 muestra lo antes descrito.

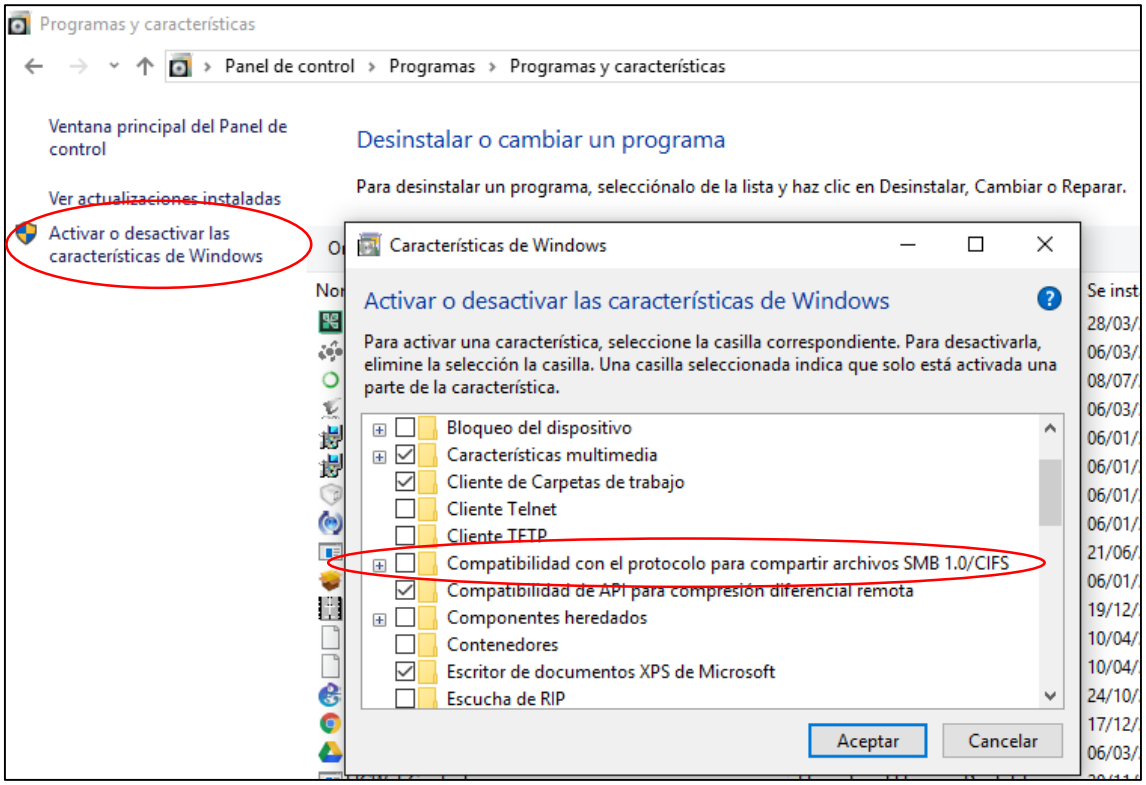


Figura 5-4: Deshabilitación del protocolo SMBv1 en Windows 10
Realizado por: Byron Barragán, 2020

Para Windows 7:

Para deshabilitar SMBv1 como servidor se ingresa a regedit y se dirigirse a: ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameter,*** en esta se crea una nueva clave de registro llamada SMB1 con el valor 0 indicando que esta deshabilitado, el valor 1 indica que está activado. En la figura 6-4 se muestra la clave de registro y el valor creado en Windows 7.

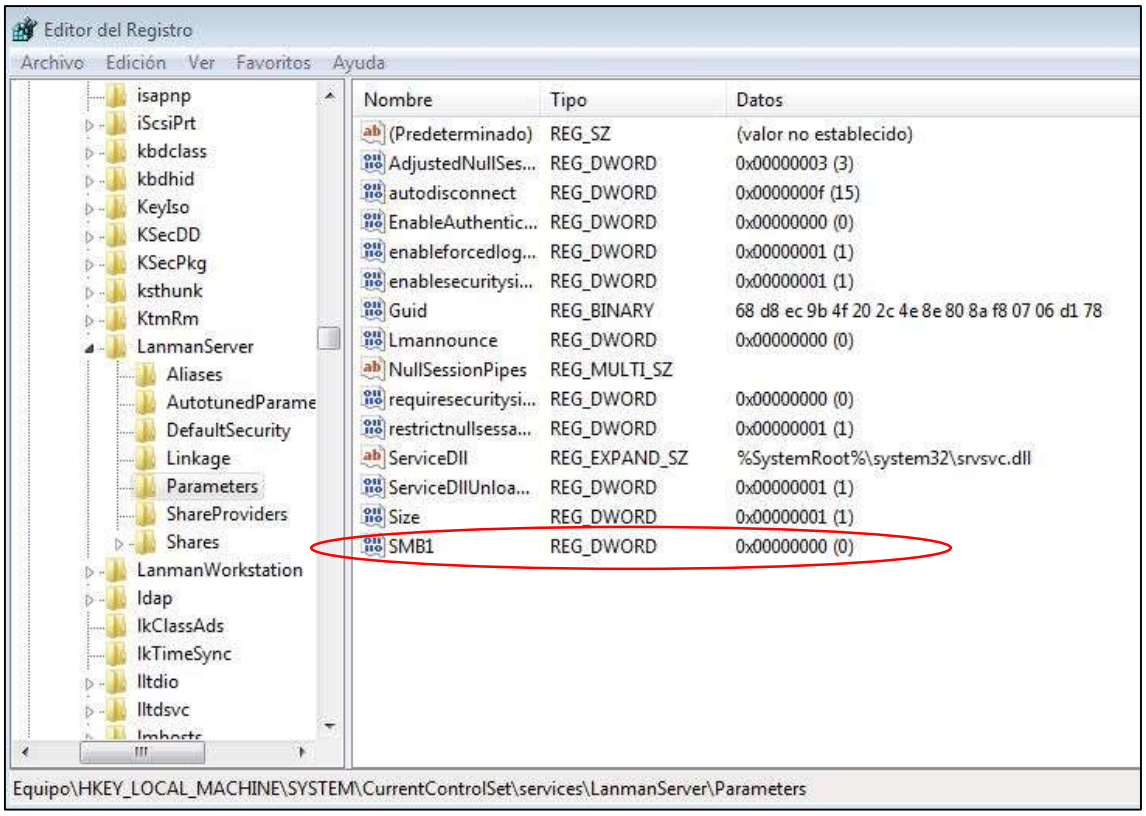


Figura 6-4: Deshabilitación del protocolo SMBv1 en Windows 7
Realizado por: Byron Barragán, 2020

Con esto se deshabilita el protocolo SMBv1 por lo que ya no se ejecuta en el puerto TCP 445. Esta solución también se usa para mitigar la amenaza de Eternalblue ya que se puede bloquear la ejecución del exploit el cual usa este puerto SMB 445 para obtener acceso a la computadora.

4.2.2. Solución para la amenaza Eternalblue y Doublepulsar

Para mitigar estas amenazas desde cualquier versión del sistema operativo Windows se debe acceder al servicio de Windows Update para descargar todas las actualizaciones disponibles, entre ellas estará la actualización que repara la vulnerabilidad MS17-010. En caso de no estar seguro de que la actualización se completó con éxito se puede descargar el parche de seguridad desde el catálogo de Microsoft Update siguiendo los siguientes pasos; esto se aplica para Windows 7 si se necesita para otra versión de Windows se debe buscar en el catálogo el parche correspondiente.

- Ingresar al catálogo de Microsoft Update, en el siguiente enlace http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212&ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-c0ZTd0iDuT_.qHzxdVIEow&epi=TnL5HPStwNw-c0ZTd0iDuT_.qHzxdVIEow&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=(ir__t

f9uguxse9kftn9ekk0sohzlxv2xl3nyf9vbs6ul00)(7593)(1243925)(TnL5HPStwNw-c0ZTd0iDuT_.qHzxdVIEow)()&irclickid=_tf9uguxse9kftn9ekk0sohzlxv2xl3nyf9vbs6ul00 ; encontrar y descargar los parches de seguridad mostrados en la figura 7-4.

Figura 7-4: Parche de seguridad para MS17-010 de Windows 7
Realizado por: Byron Barragán, 2020

- Desconectar el cable de red de la computadora y reiniciar el equipo.
- Ejecutar los parches de seguridad descargados anteriormente.

Figura 8-4: Parches de seguridad descargados para Windows 7
Realizado por: Byron Barragán, 2020

- Reiniciar la computadora para finalizar la instalación.
- Reconectar los cables de red a la computadora.

Después de la instalación si se intenta explotar la vulnerabilidad, está ya no ejecutará con éxito como se observa en la figura 9-4.

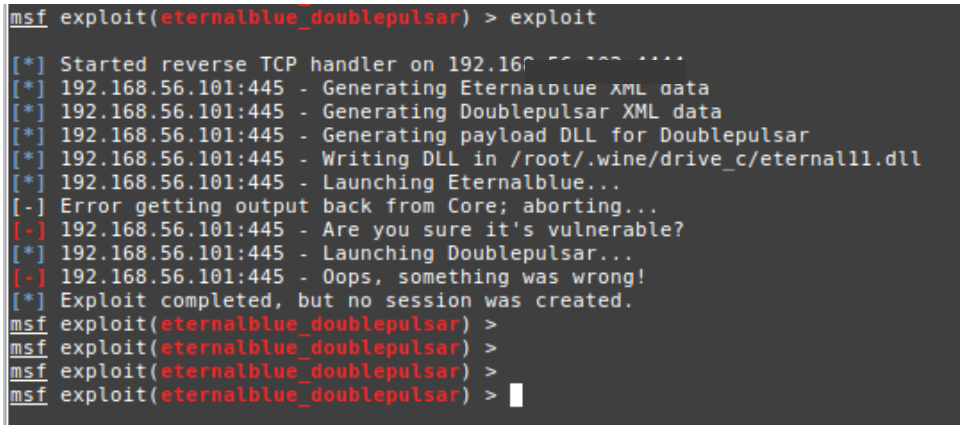


Figura 9-4: Explotación de la vulnerabilidad MS17-010 sin éxito
Realizado por: Byron Barragán, 2020

No se creó la sesión en la víctima, es decir, no se pudo acceder, si no se tiene acceso la amenaza Doublepulsar tampoco se puede desarrollar. Por lo que la amenaza MS17-010 ha sido mitigada.

4.3. Solución para las vulnerabilidades tipo denegación de servicio; Slowloris.

Existen dos soluciones para un ataque Slowloris; La primera solución es la instalación de un mod llamado Mod_qos, este mod ayuda a mitigar un ataque Slowloris hacia un servidor Apache. Esta solución fue tomada de un estudio realizado en Madrid por Samuel Ortega en julio de 2018. Mod_qos permite la realización de filtros para las conexiones entrantes al servidor web y con ello poder mitigar los ataques. (Ortega, 2018, pp. 85-86). La información de este mod se puede observar en el siguiente enlace: ***http://mod-qos.sourceforge.net/***

Para la instalación y después la configuración primero se debe instalar lo siguiente desde una ventana del terminal de CentOS.

yum install openssl-devel.x86_64
yum install pcre-devel.x86_64
yum install httpd-devel.x86_64

Después de la instalación se debe descargar el modo desde el siguiente enlace: ***http://www.mediafire.com/?i35mnrrgzvc5mxk***

Una vez descargado se descomprime utilizando el comando

tar -zxvf mod_qos-10.15.tar.gz.

Se ingresa al directorio del mod

cd mod_qos-10.5

Se ingresa al directorio de apache2

cd apache2

Se ejecuta la compilación, obteniéndose el siguiente resultado

apxs -i -c mod_qos.c

Después de la compilación, se debe editar el archivo de configuración de apache

vi /etc/httpd/conf/httpd.conf

Se escribe la siguiente línea en el archivo de configuración

LoadModule qos_module /usr/lib64/httpd/modules/mod_qos.so

Se crea el archivo de configuración con el nombre mod_qos.conf

touch /etc/httpd/conf.d/qos.conf

En el archivo de configuración recién creado se edita con

vim /etc/httpd/conf.d/qos.conf

y se escribe lo siguiente

```
## QoS Configuracion
<IfModule mod_qos.c>
#Manejo de conexiones hasta 100000 IPs diferentes
QS_ClientEntries 100000
# Se permite solamente 50 connexiones por IP
QS_SrvMaxConnPerIP 50
# Maximo número de conexiones TCP activas 256
MaxClients            256
# Desactivar la directiva keep-alive cuando el 70% de las conexiones TCP estan ocupadas:
QS_SrvMaxConnClose      70%
# Minimo de velocidad para peticiones / respuestas (niega a los clientes lentos que bloquean el servidor ,
#Ejemplo; el script slowloris mantiene las peticiones HTTP :
QS_SrvMinDataRate       150 1200
# Limite de peticiones de encabezados y cuerpo (con cuidado, limita las cargas y las peticiones POST):
# LimitRequestFields      30
# QS_LimitRequestBody     102400
</IfModule>
```

El script controla que tenga un máximo de conexiones de 100000 IP diferentes, es decir se pueden conectar hasta 100000 equipos cada una con 50 conexiones, 256 conexiones TCP activas, además desactivar el keep-alive cuando el 70% de las conexiones TCP estén utilizadas, También con el script se controla la velocidad para peticiones con respuestas, negando a los clientes lentos que intentan bloquear al servidor. La figura 10-4 muestra la edición del archivo de configuración. Después de guardar el archivo de configuración se debe reiniciar el servicio de apache. Con la línea ***service httpd restart***

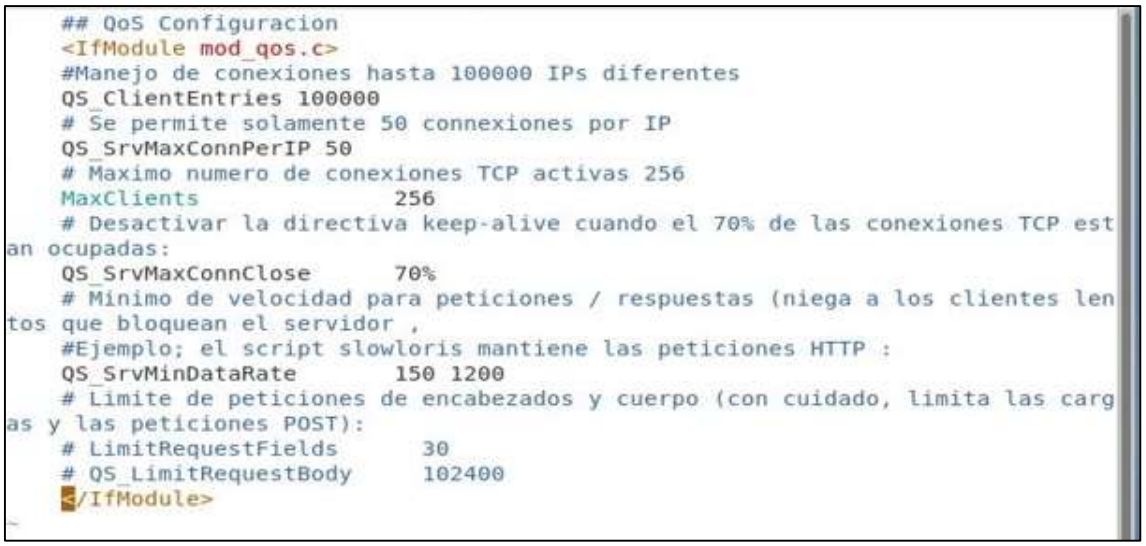


Figura 10-4: Archivo de configuración del mod_qos para Apache
Realizado por: Byron Barragán, 2020

La segunda solución es la creación de una regla de IP tables, la regla creada es ***iptables -I INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 40 -j DROP.*** En la figura 11-4 se muestra esta regla creada.

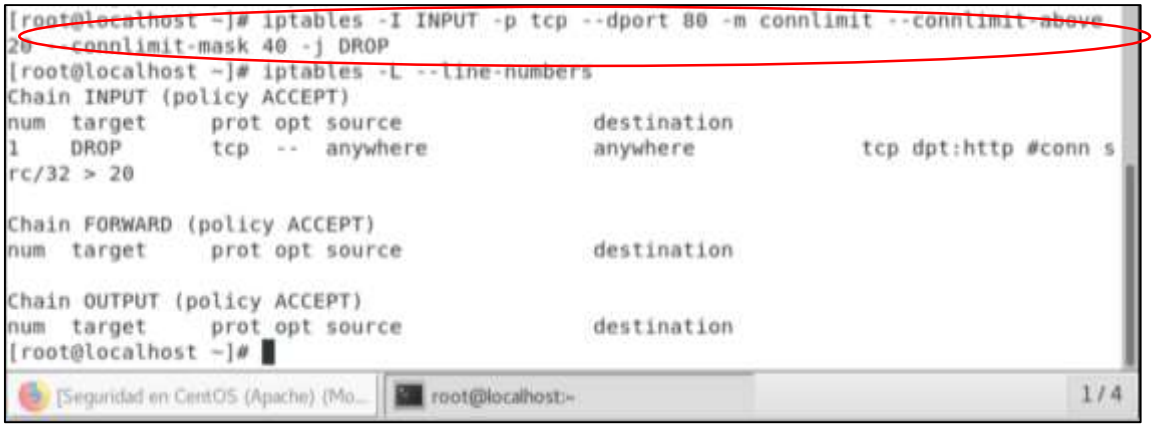


Figura 11-4: Creación de la regla como solución al ataque Slowloris
Realizado por: Byron Barragán, 2020

Al realizar el ataque con Slowloris aplicando la primera solución, este si se realiza con éxito sin embargo se demora más en realizar la denegación. Como lo muestra la figura 12-4.

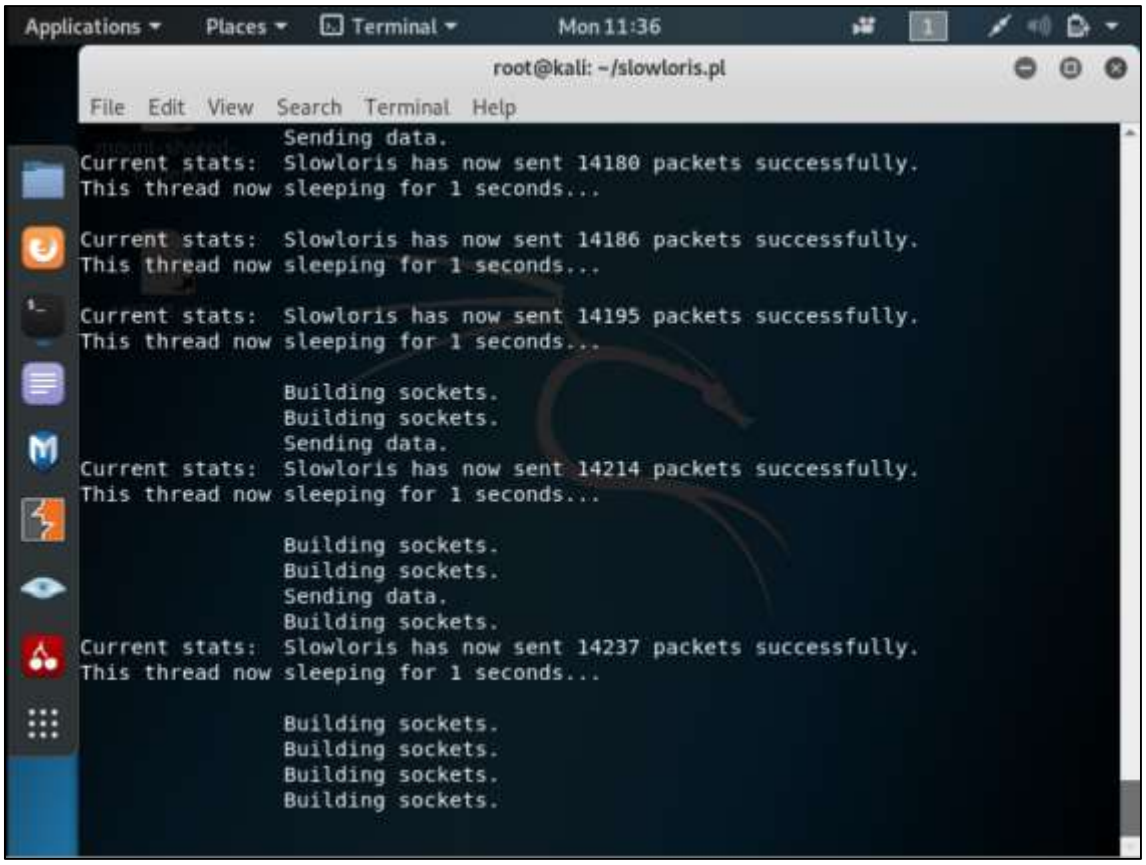


Figura 12-4: Ejecución de ataque Slowloris con el mod_qos instalado
Realizado por: Byron Barragán, 2020

Sin embargo, con la segunda solución la mitigación del ataque es completa, la regla creada deniega las conexiones y el ataque no se realiza con éxito como lo muestra la figura 13-4. En ella se puede observar que los paquetes enviados por el ataque son dropeados y en ningún momento son recibidos por el servidor ya que excede la cantidad de conexiones enviadas.

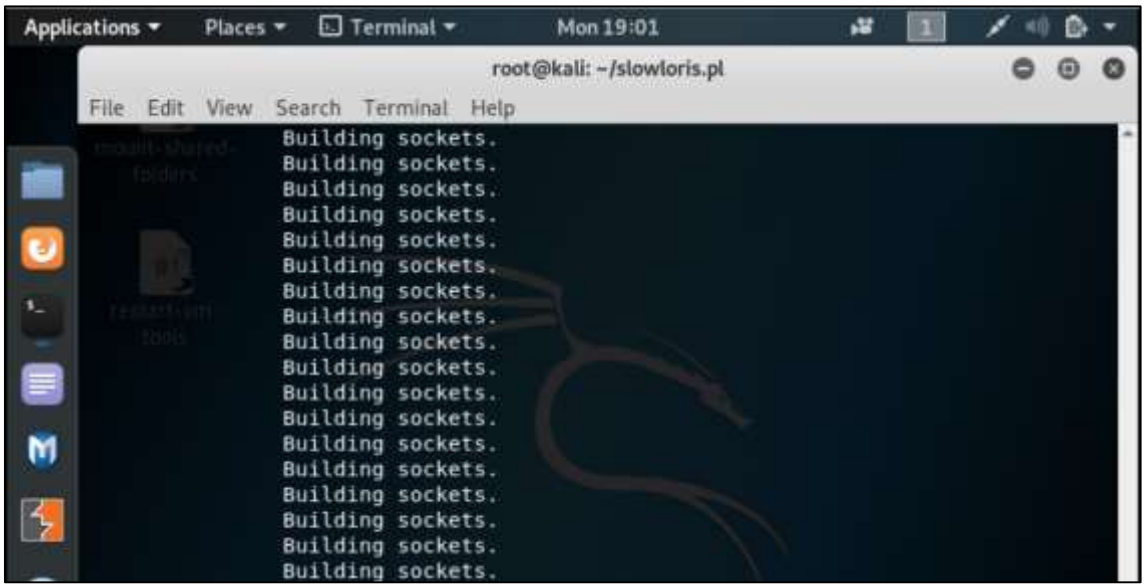


Figura 13-4: Ejecución del ataque Slowloris con la regla de Iptable creada
Realizado por: Byron Barragán, 2020

4.4. Solución para la amenaza del malware ZeuS

Si la computadora está infectada con una versión de este malware debe ser eliminado ya que este se encarga de buscar, reunir y transmitir a terceros información confidencial. Por otra parte, la activación de los archivos de Zeus puede ser instalada de forma clandestina en la carpeta UserProfile\Application Data. Una de las características más peligrosas es que después de que logre infiltrarse se encripta en las configuraciones predeterminadas del sistema, haciendo que su ubicación sea mucho más difícil de determinar por cualquier antivirus.

Para identificar este malware es que puede realizar cambios imprevistos en el sistema, o la creación de nuevos registros, instalación de programas desconocidos sin previo aviso, además se notará una ralentización de todo el sistema.

Para eliminar esta amenaza en la computadora se debe seguir los siguientes pasos:

Eliminar ZeuS con modo seguro y conexión a internet.

- Reiniciar la computadora infectada
- Ingresar a inicio de Windows avanzado, por lo general pulsando F8.
- Después escoger **Solución de problemas** / **Opción avanzada** / **Configuración de inicio** y hacer clic en el botón **Reiniciar**. Seleccionar **Habilitar modo seguro con conexión de red** en la lista de configuraciones de inicio.
- Una vez iniciada la sesión en la cuenta con el malware descargar un antispyware original.
- Eliminar todos los archivos detectados que pertenezcan al malware ZeuS

La instalación y actualización de un antivirus original protege a la computadora y toda la información de las amenazas que se pueden obtener durante la navegación de internet, siendo esto una posible solución frente a la amenaza del malware ZeuS. Además de la utilización de un NIDS ayuda a la detección de esta amenaza para después su eliminación. En la figura 14-4 muestra la detección de este Malware por Snort en diciembre de 2019 en el tráfico de la Vlan Docentes en una computadora de perteneciente a un profesor, como recomendación se informó la instalación de un nuevo antivirus y mantenerlo actualizado. Días después este malware ya no fue detectado por Snort en el tráfico de la Vlan.

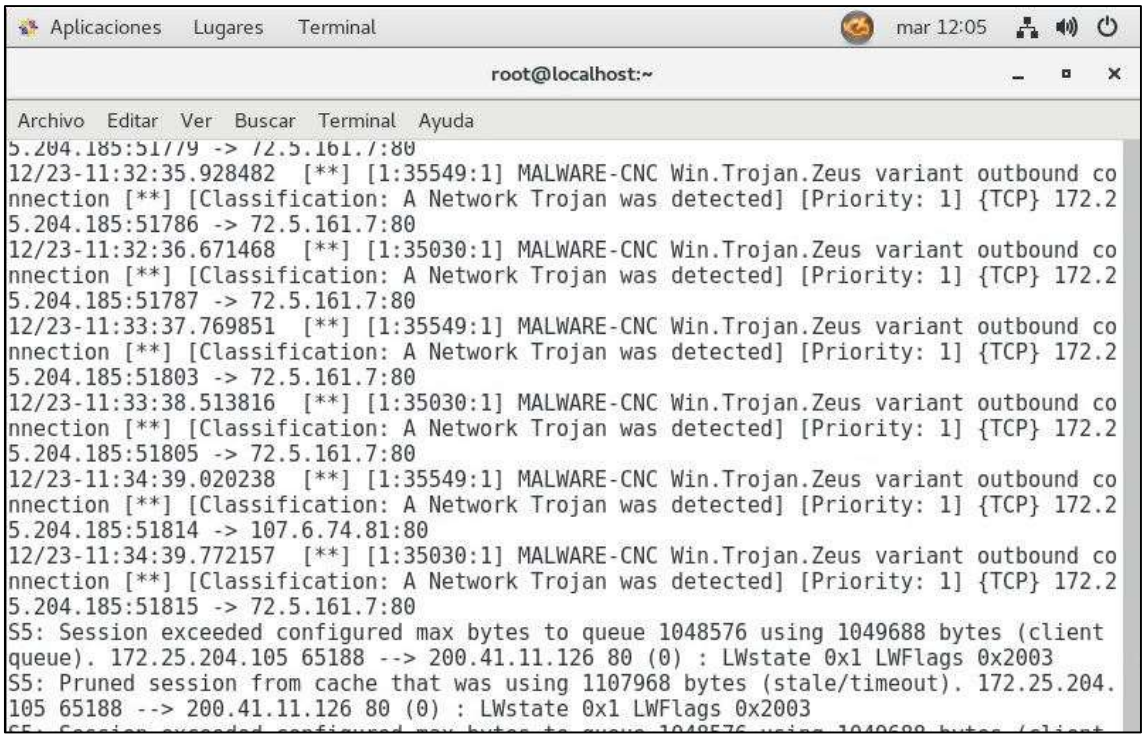


Figura 14-4: Detección del malware ZeuS en la Vlan Docentes
Realizado por: Byron Barragán, 2020

4.5. Comparación antes y después de la aplicación de la guía de solución.

Como se indicó en el capítulo II se evalúa la guía de solución propuesta en este capítulo, para ello se realiza la siguiente pregunta: ¿Se pudo explotar la vulnerabilidad antes y después de aplicar la guía de solución? Con las posibles respuestas: Si, No o Se detectó. Antes de aplicar la guía de solución, todas las vulnerabilidades y amenazas se pudieron explotar correctamente, pero después de la aplicación se obtuvo lo siguiente.

Tabla 4-4: Comparación antes y después de la aplicación de la guía de solución propuesta

Vulnerabilidad/amenaza/ataque	Se explotó antes de la Guía	Se explotó después de la Guía
Generic-tcp-timestamp	Si	Se detectó
Fingerprinting	Si	Se detectó
SMB Eternalblue	Si	No
Doublepulsar	Si	No
DoS- Slowloris	Si	No
Malware ZeuS	Si	No

Realizado por: Byron Barragán, 2020

Como se observa en la tabla 4-4 después de la aplicación de la guía en el escenario virtual, las vulnerabilidades y amenazas no se pudieron explotar por lo que la guía de solución si resuelve

las vulnerabilidades. Para el caso de los ataques Fingerprinting se consideró el valor “se detectó” debido a que se instaló un sistema de detección de intrusos diferente de Snort y se detectó el ataque, sin embargo, no se mitiga ya que para ello se debe tomar otras acciones hacia la persona identificada como insider después de que el ataque se realizara. De igual manera para la vulnerabilidad Generic-tcp-timestamp se consideró el valor “se detectó” debido a que para explotar esta vulnerabilidad se debe realizar un ataque fingerprinting.

CONCLUSIONES

- Se pudo comprobar con Snort que las vulnerabilidades más comunes de la capa de transporte se relacionan con el funcionamiento de los protocolos TCP Y UDP. Snort detectó algunos intentos de ataques de denegación de servicio, variedad de amenazas como malware y troyanos en la red del edificio de la FIE-ESPOCH, comprometiendo la autenticación, integridad, disponibilidad y confidencialidad de los datos.
- Se utilizó la herramienta de código abierto Snort debido al amplio soporte brindado por la comunidad de Snort y su conjunto de reglas definidas para distintos tipos de amenazas entre las que se encuentran las más comunes hacia la capa de trasporte, estas reglas se utilizaron para el análisis del tráfico en el edifico. Con Snort se puede configurar reglas de detección propias de manera sencilla dependiendo de las necesidades de la red en comparación a otros NIDS donde la configuración de reglas propias es más compleja como es el caso de Suricata.
- Se aplicó la metodología en los canales humano y red de datos del edificio, determinando que la seguridad del canal humano es 85.7665 Ravs y una superficie de ataque de 13.92 lo que puede ser aprovechado por un posible atacante insider. Para el caso del canal de red de datos la seguridad es 67.1216 Ravs debido a las 1082 vulnerabilidades encontradas con la herramienta Nexpose y las 394207 alertas de amenazas registradas durante el análisis del tráfico de la red con la herramienta Snort. Siendo la cantidad alta de vulnerabilidades el factor que determina un estado de seguridad bajo en el canal. Por lo que controlar y solucionar las vulnerabilidades encontradas ayudará a mejorar la seguridad del canal.
- Se explotó la vulnerabilidad Generic-tcp-timestamp un escenario virtual desarrollado en el simulador GNS3 con un ataque fingerprinting, un atacante insider puede obtener información acerca del sistema si tiene éxito y puede ser utilizada para futuros ataques. También, se explotó vulnerabilidades relacionadas al protocolo SMB con las cuales un atacante insider puede obtener acceso total al sistema y realizar sus acciones maliciosas. También, se replicó la amenaza ZeuS y se determinó que influye en el rendimiento de la computadora víctima. Finalmente se realizó un ataque de denegación de servicio usando la herramienta Slowloris debido a que los ataques DoS son los más comunes hacia la capa de trasporte.
- Se propuso una guía de solución para las vulnerabilidades y amenazas explotadas en la fase de explotación, en la guía se explica paso por paso lo que se debe hacer para mitigar o instalar un parche de seguridad que ayude a que los ataques recibidos no tengan éxito. Se probó algunas de las soluciones propuestas en el escenario virtual desarrollado con el simulador GNS3 y se comprobó su correcto funcionamiento.

RECOMENDACIONES

- Se recomienda realizar el análisis del tráfico de la red del edificio de la FIE-ESPOCH por más tiempo, esto ayudará a determinar de una mejor manera las amenazas y direcciones IP maliciosas presentes en la red. Informar sobre los resultados obtenidos a la Dirección de Tecnologías de la Información y Comunicación de la ESPOCH para la elaboración de un trabajo de mitigación para estas amenazas.
- Se recomienda la utilización de Snort como Nids para entornos de redes pequeñas, sin embargo, para entornos de redes grandes se recomienda en primera instancia tener en cuenta otros NIDS para realizar un estudio comparativo entre estos y determinar cuál arroja mejores resultados. En el campo real para la seguridad de una organización con entornos de red grandes se recomienda considerar herramientas de pago para garantizar una mejor seguridad de los sistemas.
- Revisar la última versión de la metodología OSSTMM y tomar en cuenta otras metodologías para la creación de una metodología híbrida para obtener un resultado de auditoria mejor y acorde a las necesidades de seguridad de la institución. Se recomienda aplicar la metodología OSSTMM en su totalidad en la ESPOCH para evaluar el estado real de la seguridad del campus académico.
- Se recomienda que, durante la explotación de las amenazas mencionadas en este trabajo, desconectar el cable de red de la computadora física y cortar toda comunicación no esencial entre la maquina física y la máquina virtual ya que la amenaza puede filtrarse hacia la computadora física e infectar a toda la red. Además, se debe considerar un equipo lo suficientemente potente para la realización de la simulación. En caso de que la explotación se realice en equipos reales estar seguro de tener una forma de mitigación o eliminación de la amenaza en caso de posibles imprevistos.
- Antes de aplicar la guía de solución propuesta en este trabajo tener en cuenta la versión del sistema operativo en donde se va a ejecutar la solución, en caso de que no se encuentre la versión del sistema operativo en la guía, aplicar la solución más cerca a su versión de sistema operativo. Nuevamente mantenerse informado sobre nuevas formas de mitigación o soluciones que se puedan aplicar para las vulnerabilidades y amenazas tratadas en este trabajo y actualizar los equipos para reducir las amenazas a las que se encuentran expuesto

BIBLIOGRAFÍA

AGUILERA, Purificacion. *Seguridad informática* [En Línea]. 1ª Edición. Editado por Editex, 2010, pp. 12-14. [Consulta: 28 de Marzo de 2019]. Disponible en: https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=vulnerabilidades+informaticas&ots=PqomWDGHU2&sig=HffIPKV8_5WZWOjn67YKxtTjsaM#v=onepage&q=vulnerabilidades informaticas&f=false

ALVARADO, Aida & MONTESDEOCA, Richard. *Análisis de vulnerabilidades del servidor e-learning de la espoch para la implementación de mejores prácticas de seguridad-acceso* [En Línea] (Tesis). (Ingeniería) Escuela Superior Politecnica de Chimborazo, Facultad de Informática y electrónica, Escuela de Ingeniería en Electrónica telecomunicaciones y Redes, Riobamba-Ecuador. 2017. [Consulta: 10 de Enero de 2019]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/6873

BARRETO, José. *The basic of SMB Singnig (Covering both SMB1 and SMB2.* [En Linea] [Blog] Microsoft/Doc. Estados Unidos, 2010. [Consulta: 27 de Diciembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2

BRACHO, C. *et al.* "Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio". *Revista científica Maskana* [En Linea], 2017, (Ecuador) 8 (número especial), pp. 307-319 [Consulta: 15 de Mayo de 2019]. ISSN 2477-8893. Disponible en: https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1471/1144

CALVOPIÑA, Franklin. & PILATUÑA, Inti. *Análisis y Evaluación de Riesgos y Vulnerabilidades del Nuevo Portal Web de la Escuela Politécnica Nacional, Utilizando Metodologías de Hackeo ético* [En Línea] (Tesis). (Pregrado) Escuela Politecnica Nacional, Facultad de Ingeniería en Sistemas, Quito-Ecuador, 2016 pp. 12-14. [Consulta: 29 de Marzo de 2019]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/16740

CALLES, Juan. *Inundaciones UDP: Técnicas para tocar los… puertos de un servidor* [En Línea]. Fluproject. España, 2018 [Consulta: 29 de Enero de 2020]. Disponible en: https://www.flu-project.com/2018/04/inundaciones-udp-tecnicas-para-tocar.html

CATOIRA, Fernando. *Pentesting: Fingerprinting para detectar sistema operativo* [En Línea]. WeLiveSecurity by ESET. Argentina, 2012a. [Consulta: 29 de Enenro de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2012/10/18/pentesting-fingerprinting-para-detectar-sistema-operativo/

CATOIRA, Fernando. *Penetration Test, ¿en qué consiste?* [En Línea]. WeLiveSecurity by ESET. Argentina, 2012b. [Consulta: 30 de Marzo de 2019]. Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

CIFUENTES, Jesús & NARVAEZ, Cesar. *Manual de deteccion de vulnerabilidades de sistemas operativos linux y unix en redes tcp-ip* [En Línea] (Tesis). (Ingeniería) Universidad Del Valle, Facultad de Ingeniería, Escuela de Ingeniería Eléctrica y Electrónica. Santiago de Cali-Colombia. 2004, p. 5-6. [Consulta: 26 de Marzo de 2019]. Disponible en: https://es.scribd.com/doc/41637606/manual-de-detecciOn-de-vulnerabilidades-de-sistemas-operativos-linux-y-unix-en-redes-tcp-ip

CLOUDFLARE, *Slowloris DDoS Attack* [En Linea]. 2020. Cloudflare [Consulta: 29 de Enenro de 2020]. Disponible en: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/

DORDOIGNE, José. *Redes informáticas : nociones fundamentales : (protocolos, arquitecturas, redes inalámbricas, virtualización, seguridad, IP v6 ...)* [En Línea]. 5ª Edición. Barcelona-España: Editado por ENI, 2015, p. 36. [Consulta: 22 de Marzo de 2019]. Disponible en: https://books.google.es/books?hl=es&lr=&id=Huwy1L0PEq8C&oi=fnd&pg=PA19&dq=redes+informáticas&ots=N_0n7sbWgz&sig=J-DgMKEXcRipMWInAsqO005BGEQ#v=onepage&q&f=false

ESSAYS Professors, *Check out Our Nessus vs NeXpose essay.* [En Linea]. Nicosia- Chipre, 2020. [Consulta: 23 de Octubre de 2019]. Disponible en: https://essaysprofessors.com/samples/comparison/nessus-vs-nexpose.html

ESPINOSA Angélica. *Análisis de Vulnerabilidades de la Red LAN de la UTPL* [En Línea] (Tesis). (Ingeniería) Universidad Tecnica Particular de Loja, Escuela de Ciencias de la Computación, Loja-Ecuador. 2010, p. XIII. [Consulta: 12 de Diciembre de 2018]. Disponible en: http://dspace.utpl.edu.ec/bitstream/123456789/1352/3/Espinosa_Otavalo_Ang%C3%A9lica%20del%20Cisne.pdf

FERNANDEZ, Aitor. *El Modelo OSI, para un pentester (o para un hacker).* [En Linea] [Blog]. Navarra-España, 2018. [Consulta: 27 de Octubre de 2019]. Disponible en: https://es.linkedin.com/in/aitorbfernandez?trk=author_mini-profile_title

FRANCO, David & PEREA, Jorge & TOVAR, Luis. "Herramienta para la deteccion de vulnerabilidades basada en la Identificación de servicios*". Información Tecnológica* [En Linea], 2013 24(5), pp. 13-22. [Consulta: 28 de Enero de 2020]. ISSN 0718-0764. Disponible en: https://scielo.conicyt.cl/pdf/infotec/v24n5/art03.pdf

GORDON, Diego & PACHECO, Ruben. "Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior*". Revista Electrónica de Computación, Informática, Biomédica y Electrónica ReCIBE* [En Linea], 2018 7(1), pp. 1-21. [Consulta: 15 de Mayo de 2019]. ISSN 2007-5448. Disponible en: http://recibe.cucei.udg.mx/ojs/index.php/ReCIBE/article/view/90/84

ISECOM. *OSSTMM 3 – The Open Source Security Testing Methodology Manual* [En Línea]. Version 3.0. Nueva York-USA: ISECOM, 2010. [Consulta: 30 de Marzo de 2019]. Disponible en: http://www.isecom.org/mirror/OSSTMM.3.pdf

MEJIA, Cesar & RAMIREZ, Nini & RIVERA, Juan. *Vulneravilidad, Tipos de ataques y Formas de mitigarlos en las capas del modelo osi en las redes de datos de las organizaciones* [En Línea] (Tesis). (Ingeniería) Universidad Tecnologica De Pereira, Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación, Ingeniería de Sistemas y Computación, Pereira-Colombia. 2012, pp. 112-120. [Consulta: 05 de Marzo de 2019]. Disponible en: https://docplayer.es/2873475-Vulneravilidad-tipos-de-ataques-y-formas-de-mitigarlos-en-las-capas-del-modelo-osi-en-las-redes-de-datos-de-las-organizaciones.html

NMAP, *Descubriendo sistemas* [En línea] Nmap.org [Consulta: 29 de Enenro de 2020]. Disponible en: https://nmap.org/man/es/man-host-discovery.html

ORTEGA, Samuel. *Diseño de un sistema de seguridad para un servidor Web Apache* [En línea] (Trabajo de titulación) (Ingeniería) Universidad Politécnica de Madrid. Madrid – España. 2018. pp. 85-86. [Consulta: 2019-09-01] Disponible en: http://oa.upm.es/53223/1/TFG_SAMUEL_ORTEGA_SANCHO.pdf

PADILLA, Rodrigo. *et al.* *Estado De Las Tecnologías De La Información Y La Comunicación En Las Universidades Ecuatorianas* [En Línea]. Primera Edición. Cuenca-Ecuador: Corporacion Ecuatoriana para el Desarrollo de la Investigación y la Academia CEDIA, 2017, p. 71. [Consulta: 3 de Mayo de 2019]. Disponible en: https://www.cedia.edu.ec/es/libro/ue-tic

PALACIOS, Jairo. *Análisis de Vulnerabilidades de una Red Corporativa mediante Herramientas de Descubrimiento Activas* [En Línea] (Tesis). (Ingeniería) Universidad de Sevilla, Departamento de Ingeniería Telemática, Escuela Técnica Superior de Ingeniería, Sevilla-España. 2015. [Consulta: 16 de Diciembre de 2018]. Disponible en: http://bibing.us.es/proyectos/abreproy/90522/fichero/Memoria+del+Trabajo+Fin+de+Grado.pdf

PERPIÑAN, Antonio. *Seguridad de sistemas gnu/linux* [En Línea]. 1ª Edición. Santo Domingo-Republica Dominicana: Fundación Código Libre Dominicano, 2011, p. 6-9. [Consulta: 23 de Marzo de 2019]. Disponible en: http://highsec.es/wp-

content/uploads/2013/10/Libro-Seguridad-GNU-Linux-Antonio-Perpinan-2011.pdf.

RIVERA, Jonathan. *Fundamentos de Redes Informáticas* [En Línea]. 1ª Edición. Editado por Createspace Independent Publishing Platform, IT Campus Academy, 2015, pp. 10-13. [Consulta: 23 de Marzo de 2019]. Disponible en: https://books.google.es/books?hl=es&lr=lang_es&id=smrOCgAAQBAJ&oi=fnd&pg=PA5&dq=redes+informáticas&ots=-VLKi4erYw&sig=cFG3VmV0the-L1No9xloE7teIWg#v=onepage&q&f=false

QUISPHE, Henry. *Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovable* [En Línea] (Tesis). (Ingeniería) Universidad Nacional de Loja, Carrera de Ingeniería en Sistemas, Loja-Ecuador. 2016, pp. 40-51. [Consulta: 05 de Noviembre de 2019]. Disponible en: https://dspace.unl.edu.ec/jspui/handle/123456789/16039

Ruben Ramiro. *Como prevenir los ataque insiders* [En Linea] [Blog]. Madrid-España, 2017. [Consulta: 27 de Diciembre de 2018]. Disponible en: https://ciberseguridad.blog/como-prevenir-los-ataque-insiders/

SERRANO, Andres. *Análisis De Vulnerabilidades De Seguridades En Redes Inalámbricas Dentro De Un Entorno Empresarial Que Utilizan Cifrado Aes Y Tkip , Wpa Personal Y Wpa2 Personal Del Dmq* [En Línea] (Tesis). (Ingeniería) Pontificia Universidad Católica Del Ecuador, Facultad de Ingeniería, Escuela de Sistemas, Quito-Ecuador. 2011, p. 1. [Consulta: 20 de Diciembre de 2018]. Disponible en: http://repositorio.puce.edu.ec/handle/22000/4642

SORIANO, Miguel. *Seguridad en redes y seguridad de la información* [En Línea]. 1ª Edición. Praga-Republica Checa: *Improvet*, Editado por České vysoké učení technické v Praze, 2014, pp. 31-37. [Consulta: 24 de Marzo de 2019]. Disponible en: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf.

TANENBAUM, Andrew & WETHERALL, David. *Redes de computadoras* [En Línea]. 5ª Edición. México- México: Editado por Luis. M. Cruz Castillo, Bernandino. Gutiérrez

Hernández, & Juan. J. García Guzmán, Pearson Education, Inc, 2012, pp. 15-41, 464-481. [Consulta: 22 de Marzo de 2019]. Disponible en: https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Tecnología Fácil. *¿Qué es Open Source?* [En Línea]. [Consulta: 30 de Marzo de 2019]. Disponible en: https://tecnologia-facil.com/que-es/que-es-open-source/

VILLORA, Borja. *Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques* [En Línea] (Tesis). (Ingeniería) Universidad Politécnica de Valencia, Escuela Tecnica Superior de Ingeniería Informática, Valencia-España. 2018, p. 37. [Consulta: 05 de Noviembre de 2019]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/106947/VILLORA%20-%20Evaluación%20y%20gestión%20de%20vulnerabilidades%3A%20Cómo%20sobrevivir%20en%20el%20mundo%20de%20los%20ciberataques.pdf?sequence=1&isAllowed=y

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

DBRAI

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 02 / 03 / 2020

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: Byron Mauricio Barragán González
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Ingeniería en Electrónica, Telecomunicaciones y Redes
Título a optar: Ingeniero en Electrónica, Telecomunicaciones y Redes
f. Analista de Biblioteca responsable: