CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Diego Fernando Moreno Moreno

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
MANTA
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Diego Fernando Moreno Moreno

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

M.Sc. JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
MANTA
2023

RESUMEN

La tecnología ha evolucionado de forma impresionante los últimos 120 años, y es que hoy en día ya podemos controlar dispositivos electrónicos y digitales con la voz y los pulsos eléctricos de nuestro cuerpo. Y así como esta tecnología evoluciona, también hay las personas que quieren obtener un beneficio propio de forma ilegal a estos servicios digitales y es por eso por lo que la seguridad informática también está tomando grandes avances tecnológicos con el fin de resguardar la información digital y nuestra forma de interactuar con ella. Las personas que se especializan en este ámbito deben de saber que no es aprender lo que ya se sabe sino descubrir formas diferentes de como poder brindar la seguridad a los sistemas informáticos puesto que la delincuencia está encontrando formas nuevas de como cometer sus actos delictivos sin dejar rastro o huellas de los incidentes realizados.

Se presentará información clave para saber cómo aplicar una seguridad efectiva dentro de una organización de la cual ha demostrado tener falencias y vulnerabilidades. Se revisaran temas desde el marco teórico, legal y practicas con algunos de sus sistemas informáticos para evidenciar las fallas más comunes de seguridad y poder brindar las mejores recomendaciones de ciberseguridad desde la vista de los equipos blue team y red team, los cuales hoy en día son una de las formas de probar el nivel de seguridad existente dentro de una organización para saber que tan débil o robusto están dichos sistemas y que tanto saben de cómo detectar, contener y erradicar una amenaza cibernética.

CONTENIDO

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA: se refieren a circunstancias o eventos de seguridad cibernética que pueden causar daños a la organización objetivo.

CIBERSEGURIDAD: Conjunto de herramientas, políticas, metodologías y elementos destinados al control de la seguridad informática a un espacio digital.

BLUE TEAM: son personas expertas en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa y sus defensas.

FIREWALL: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

INCIDENTE: acciones maliciosas de acceder o dañar un sistema de computadoras o redes.

RED TEAM: son personas expertas en ciberseguridad especializados en simular un ataque dirigido a una organización de forma controlada y con previa autorización de la organización para conocer las fallas de seguridad informática.

VULNERABILIDAD: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de esta.

INTRODUCCIÓN

La seguridad informática se ha vuelto un término muy común dentro de las organizaciones o espacios digitales puesto que las amenazas cibernéticas se han vuelto más comunes optando por diferentes formas de cometer los actos delictivos y que mezclados, por ejemplo, la ingeniería social, están cumpliendo con sus propósitos de causar daño a la sociedad.

Una de las mejores formas de validar como se encuentre la seguridad dentro de un espacio digital es el uso de las capacidades técnicas de blue team y red team los cuales son dos equipos compuestos principalmente de personas especializadas en seguridad informática encargados de realizar la evaluación y auditoria a los sistemas informáticos y que también relazan simulaciones de ataques para probar la robustes del mismo.

En el presente informe técnico se realizará el análisis a un ataque realizado a la empresa The WhiteHose Security, quien fue la encargada de buscar personal especializado en el tema con el finde de poder hallar las causas de la brecha de seguridad y con el mismo informe enfocar su búsqueda de personal nuevo para su área de seguridad informática con el fin de poder fortalecerse para que en futuro no sufra de los mismos incidentes.

Con este incidente la empresa busca encontrar al mejorar personal de seguridad informática y poder hacerlo parte de su equipo para pueda continuar con su legado de una empresa prestigiosa y de calidad que brinda confianza y tranquilidad a sus clientes que tiene contratados sus servicios como fidelizar a los clientes nuevos.

1. OBJETIVOS

1.1 OBJETIVOS GENERAL

Evaluar las estrategias del Blue Team y Red Team para identificar las brechas de seguridad dentro de The WhiteHose Security y poder seleccionar a los mejores expertos que harán parte de esta prestigiosa organización según sus resultados y recomendaciones.

1.2 OBJETIVOS ESPECÍFICOS

Analizar las acciones de Blue Team y Red Team de The WhiteHose Security en el marco de los criterios éticos y legales.

Analizar y demostrar las vulnerabilidades a partir del uso de metodologías y técnicas de intrusión sobre el ataque que sufrió The WhiteHose Security en sus sistemas informáticos.

Diagnosticar medidas de contención en base a los datos encontrados de la brecha de seguridad y recomendar estrategias que endurezcan los aspectos de seguridad informática dentro de la organización.

2 INFORME TECNICO

2.1 ANÁLISIS DE LA LEGISLACIÓN RELACIONADA CON DELITOS INFORMÁTICOS.

En Colombia actualmente hay leyes y decretos con las cuales se tiene el control para los delitos informáticos y protección de datos personales las cuales son aplicables para aquellas personas actoras de algunos de dichas menciones dentro de estas leyes y decreto de los cuales son sancionables.

2.1.1. Delitos informáticos: son aquellas acciones que se realizan en el campo digital, espacio digital o de internet que son ilegales, delictivas, antiéticas o no autorizadas con el fin de vulnerar o dañar los bienes patrimoniales o no de otras personas o entidades. [1]

2.1.1.1. **Ley 1273 del 2009**: esta ley hace una modificación al código penal para poder crear un bien jurídico y que con la aparición de las herramientas informáticas se intenta proteger los bienes de las personas o entidades de las cuales este haciendo uso de los espacios digitales. Esta se denomina *"de la protección de la información y de los datos".* Esto para preservar integralmente las estructuras informáticas que hacen uso de las tecnologías de la información y las de las comunicaciones.

Esta ley cuenta con 10 artículos de los cuales sus principales características es tratar los delitos relacionados con el acceso abusivo de un sistema informático (Art. 269A), obstaculización ilegítima de sistema informático o red de telecomunicación (Art. 269B), interceptación de datos informáticos (Art. 269C), daño informático (Art. 269D), uso de software malicioso (Art. 269E), violación de datos personales (Art. 269F), suplantación de sitios web para capturar datos personales (Art. 269G), circunstancias de agravación punitiva (Art. 269H), hurto por medios informáticos y semejantes (Art. 2691) y transferencia no consentida de activos (Art. 269J)[2]

2.1.2. Protección de datos personales: esta con sagrado dentro de la constitución política de Colombia como u derecho fundamental y que pueden tener todas las personas para mantener su integridad personal o familiar, al buen nombre y a

[1] SOGNIFICADOS. Qué Son Los Delitos Informáticos. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.significados.com/delitos-informaticos/

[2] "COLOMBIA. LEY 1273 DE 2009. De La Protección De La Información Y De Los Datos. (05 de enero de 2009). de la protección de la información y de los
datos En: Diario Oficial. enero, 2009. Nro. 47223. p. 1-5"

conocer, actualizar y rectificar los datos e información que se haya recogido sobre ellos en banco de datos y archivo de entidades privadas y públicas.

2.1.2.1. Ley 1581 de 2012: con esta ley más con lo consagrado en la constitución política de Colombia, se busca el reconocimiento y protección del derecho que tiene las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Esta ley es un complemento a la regulación vigente de la constitución política. Es más aplicable a las bases de datos o archivos que puedan contener datos personales de cualquier persona natural o entidad. Pero hay cierto cubrimiento de esta ley, es decir, a estos datos no aplicaría la ley mencionada: información de uso personal o doméstico, información que tiene por finalidad la seguridad y defensa nacional, información que tiene por finalidad la prevención, detección, monitoreo y control del lavado de activos y financiación del terrorismo, información que tiene por finalidad de inteligencia y contrainteligencia.[3]

2.2 ANÁLISIS SOBRE EL EJERCICIO DE PENTESTING

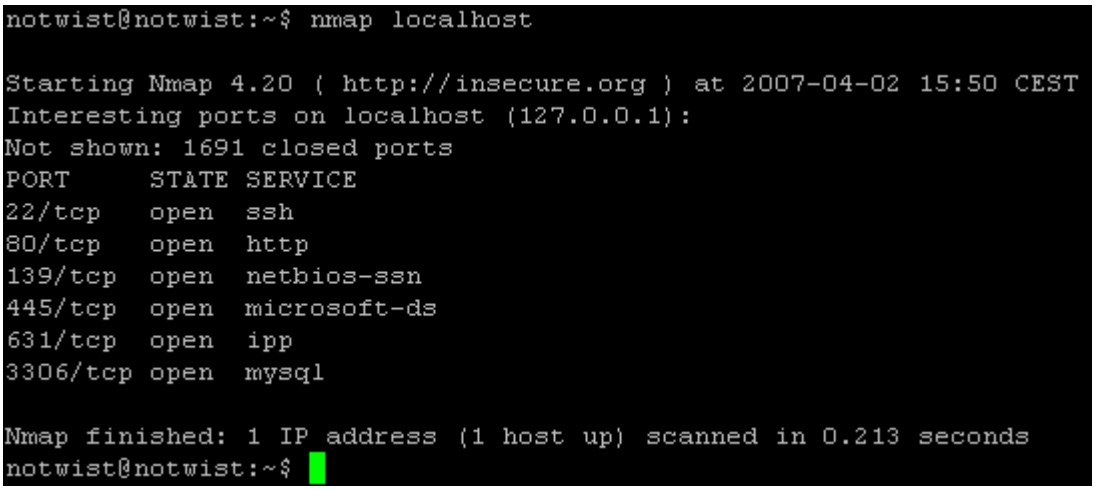
El pentesting es un conjunto de acciones que realiza un experto en seguridad informática contra un sistema informático o estructura compleja con el fin de poder detectar las posibles vulnerabilidades que pueda tener dicho sistema y posterior poder corregir dichas vulnerabilidades y salvaguardar la información de los delincuentes informáticos que pueden explotar estas vulnerabilidades y causar danos al sistema o robos de información.

El pentesting normalmente maneja 5 fases:

2.2.1. Recopilación de información: en esta fase el experto en seguridad informática realiza un escaneo de sistema con el fin de detectar vulnerabilidades y como se encuentra compuesto el sistema (su infraestructura). También hace el uso de herramientas con el fin de detectar dichas vulnerabilidades como por ejemplo **Nmap**, el cual hace rastreo de puertos y análisis de redes como se observa en la figura 1, para poder obtener información de la cual sea relevante y así controlar y gestionar los sistemas. Esta es una de las herramientas más usadas para la auditoria de sistemas como la seguridad de estos y realizar monitoreo constate de las redes y puertos.

[3] COLOMBIA. LEY ESTATUTARIA 1581 DE 2012. Protección De Datos Personales. (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. octubre, 2012. Nro. 47223. p. 1-11

Figura 1 Nmap

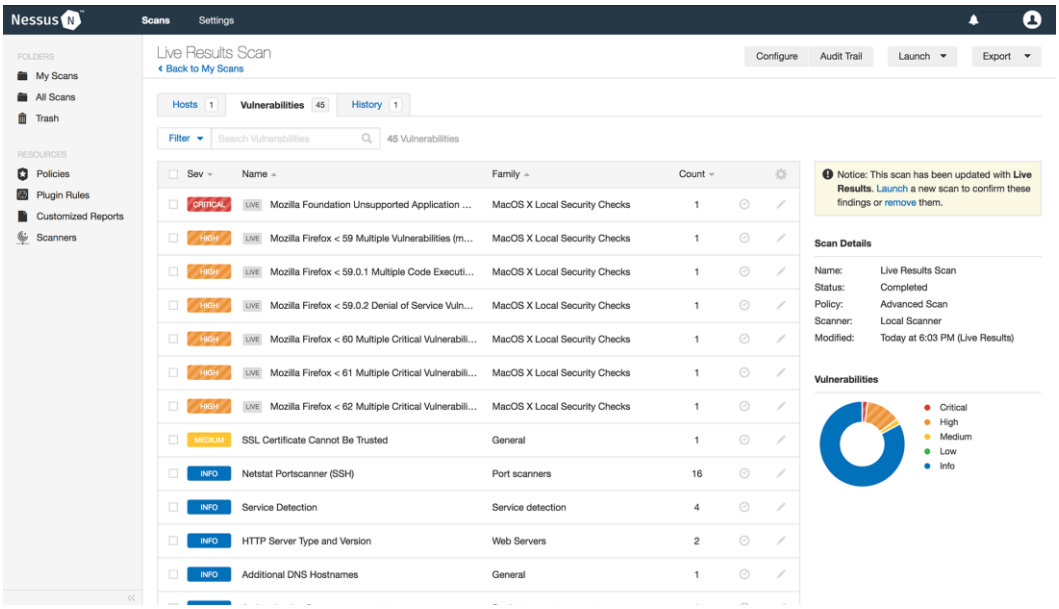


Fuente: Nmap 2023

2.2.2. Análisis de vulnerabilidades: después de haber detectado las vulnerabilidades dentro del sistema informático, estas las podemos comenzar a analizar comparando con su código CVE (Common Vulnerabilities and Exposures), en español “Vulnerabilidades y exposiciones comunes” y si esta vulnerabilidad esta descrita ya con dicho código para poder entender el porqué de la vulnerabilidad y saber cuál es la medida correctiva. Estas vulnerabilidades, el experto las puede clasificar por nivel de criticidad, si tiene solución, nivel de exposición, etc. Las diferentes medidas en que las dese clasificar el experto para que pueda tener un mejor panorama de este.

Pero también podemos ahorrarnos montón de trabajo al poder usar algunas de las herramientas que existen para la clasificación de las vulnerabilidades como **Nessus** el cual puede escanear vulnerabilidades y se apoya o relaciona con NMap formando un equipo conjunto, luego de haber detectado algo inusual, empieza a comparar con una larga lista de plugins dichas firmas para saber que puede ser una vulnerabilidad o no y al terminar, nos mostrara cuales fueron las vulnerabilidades que encontró y las clasifica según su riesgo para que el experto sepa qué hacer con el siguiente paso como se observa en la figura 2.

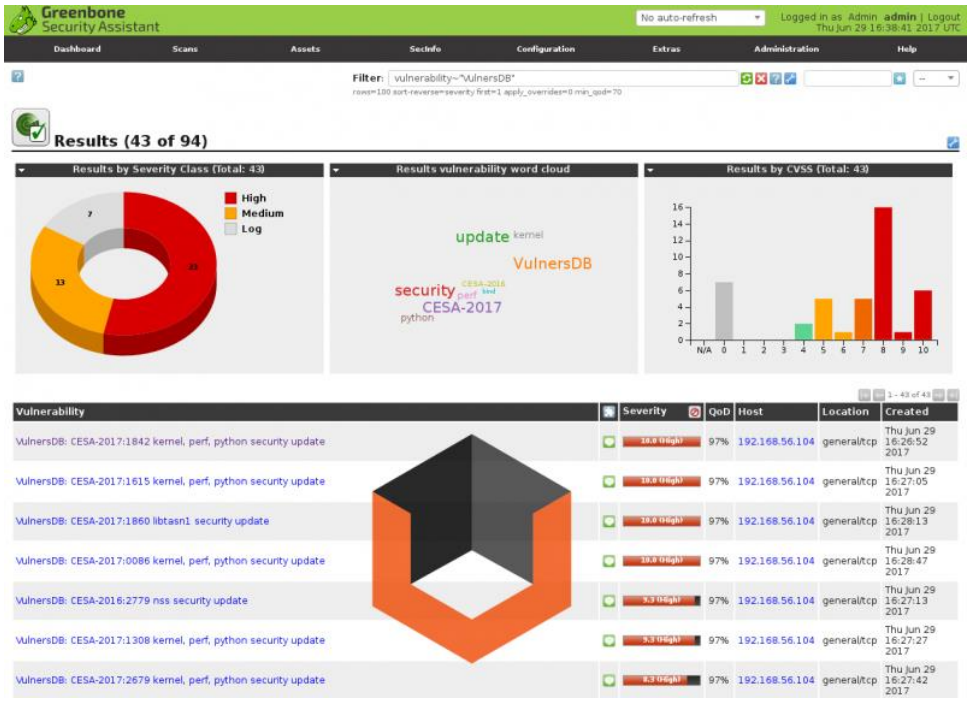
Figura 2 Nessus



Fuente: TENABLE. Nessus. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.tenable.com/sites/all/themes/tenablefourteen/img/nessus/nessus-live-results_large.png

2.2.3. Explotación de vulnerabilidades: en esta fase se realiza la explotación de la vulnerabilidad para conocer que provecho se pude obtener de la misma y si estas las podemos usar como puerta de entrada al sistema que se realiza la prueba. Esta se puede ejecutar por medio de Herramienta de las cuales Nessus puede funcionar, pero hay otras como **OpenVAS** el cual es muy completo y nos puede ayudar desde detectar vulnerabilidades, analizarlas y explotarlas ya que a esta herramienta cuenta con más de 50.000 test y datos de vulnerabilidades conocidas y alimentadas a diario por la empresa y por parte de la comunidad y sus expertos. Esta herramienta cuenta con pruebas autenticadas, pruebas no autenticadas, cuenta con protocolos industriales y de Internet de alto y bajo nivel, ajustes personalizados de rendimiento para exploraciones a gran escala., desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad como se observa en la figura 3.

Figura 3 Open VAS

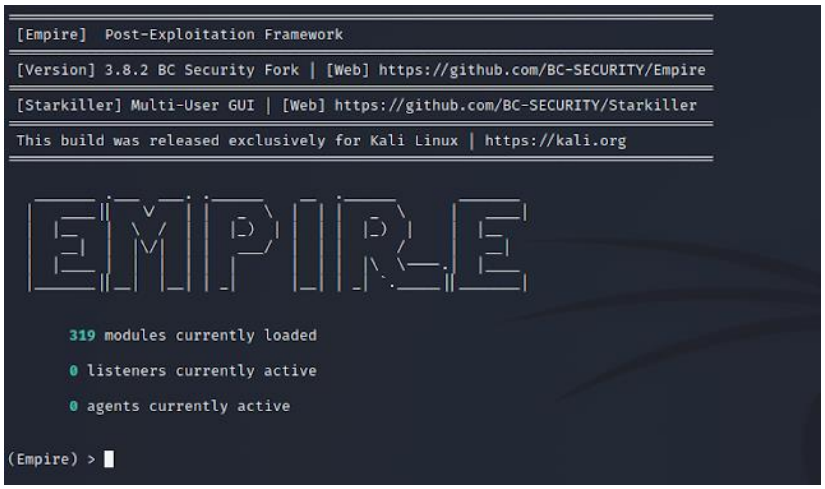


Fuente: GREENBONE. Openvass. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.mancomun.gal/wp-content/uploads/2022/02/vulners_openvas_vulnerabilities_logo-800x576.png

2.2.4. Post Explotación: Como su nombre lo indica, es lo sucedió después de la explotación y pues no siempre se puede aplicar ya que es manejada cuando se logra ingresar a un sistema informático después de haber explotado una vulnerabilidad. Por lo que el objetivo de esta fase es la escalación de permisos o privilegios para obtener una cuenta con todos los privilegios habilitados sobre el sistema. Si esto es logrado, en esta fase se realiza la obtención de información confidencial, evasión de mecanismos de autenticación, realizar acciones del lado de los usuarios, acceder a otros sistemas o servicios accesibles desde el sistema comprometido, realizar acciones sin el consentimiento y/o conocimiento de la organización comprometida.

Para estos casos podemos usar la herramienta **Empire** la cual es una herramienta que ha ido creciendo con la función de penetración con powershell la cual nos permite hacer uso de objetivos como usestarger ASPX, escalada por servicios mal configurados y escalada y pivoting. En la figura 4 podemos observar la interfaz:

Figura 4 Empire

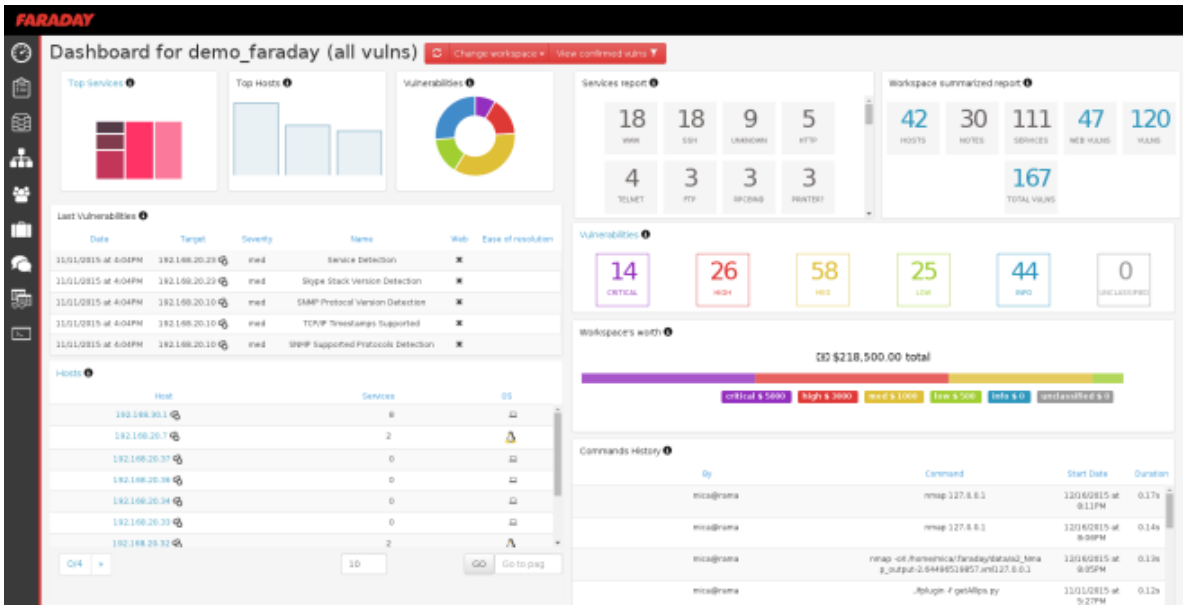


Fuente: BLOG.HACKER. Framework Post Explotación Powershell-Empire. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://blog.elhacker.net/2021/12/framework-powershell-empire-post-explotacion-pentesting.html

2.2.4. Reporte: Ya en esta fase se genera el reporte por parte del experto en seguridad informática y encargado de la prueba de pentesting, donde entrega un informe detallado de las vulnerabilidades encontradas, el nivel de riesgo y las acciones para erradicarlas y mantener el sistema seguro.

Para esta fase podemos usar **Faraday** la cual nos permite distribuir, diseñar, indexar y analizar todos los datos recopilados durante la prueba de pentesting mostrándonos un Shell mostrando los detalles resumidos y de fácil compresión para los lectores como se observa en la figura 5.

Figura 5 Faraday



Fuente: REDESZONE. Faraday, Una Completa Plataforma De Pentest Y Análisis De Vulnerabilidades. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.redeszone.net/app/uploads-redeszone.net/2016/07/Faraday-655x333.png

2.3 EXPLICACIÓN DE LAS HERRAMIENTAS Y SERVICIOS UTILIZADOS EN CIBERSEGURIDAD

La ciberseguridad hoy en día se ha vuelto más común de lo que se sabía, puesto que cada vez es más las herramientas digitales creadas para las personas logren facilitar sus labores y dar privacidad a sus datos. Así como el mundo digital avanza, también los delincuentes buscan la forma de ocasionar delitos en contra de dichos sistemas informáticos y por ende las personas o entidades buscando expertos ene le tema para poder proteger sus bienes digitales. Para ello se han diseñado dichas herramientas las cuales ayudan a la detección y prevención de amenazas como son:

2.3.1. Metasploit: este es una herramienta de código abierto la cual nos ayuda a identificar vulnerabilidades de seguridad en sistemas informáticos. Fue desarrollada por Perl y Ruby enfocada para auditores de seguridad y los famosos equipos red team y blue team.

2.3.1.1. Características: es una herramienta completa y que contiene muchos exploits, que es como una base de datos de todas las vulnerabilidades conocidas y también tiene los payloads, que son módulos donde se contienen códigos para

explotar dicha vulnerabilidad. Cuenta también con encoders, que son códigos cifrados para evadir los antivirus o sistemas de seguridad perimetral.

Esta también interactúa con Nmap y Nessus, descritas anteriormente y que se analizaran a continuación.

Los malwares detectados nos permite exportarlos en cualquier formato sin importa el sistema operativo.

Este es multiplataforma y es gratuito, pero tiene una versión de pago y en esta nos ofrece exploit ya desarrollados mientras que la versión gratuita tiene todas las vulnerabilidades públicas.

2.3.2. Nmap: (Network Mapper) es una herramienta de código abierto la cual es usada para escanear una red y los puertos y así obtener información relevante sobre los sistemas que conforman dicha red. Es usada para las auditorias de seguridad de sistemas informáticos y es una de las más populares que existen.

Esta disponible para Linux, IOs y Windows y con esta herramienta podemos realizar diferentes tipos de escaneos:

a) Ping/ARP. Son escaneos muy útiles a la hora de conocer qué host se encuentran activos en la red (ping), o para obtener información específica sobre los hosts activos (ARP).
b) TCP connect. Para realizar una conexión completa de todos los puertos. También realiza otros escaneos TCP, como el ACK (para saber si el puerto está abierto, cerrado o existe un firewall en medio), el UDP o el TCP SYN.
c) Sondeo de lista. Este escaneo tiene la finalidad de obtener los nombres de equipo de los distintos dispositivos conectados a la red, sin la necesidad de enviar un paquete para ello (realizando una resolución inversa de DNS).
FIN. Para determinar si el host se encuentra tras un cortafuego.

2.3.2.1. Características: esta herramienta se destaca por sus funciones las cuales comprenden:

a) Mapear una red: consiste en identificar los dispositivos que se encuentran conectados a una red, bien sean servidores, ordenadores, dispositivos móviles, enrutador o conmutadores, aportando información sobre cómo se conectan a la red.

b) Identificar servicios en ejecución: identificar servicios que se están ejecutando en la red como servidores de correo o servidores web, por ejemplo, ofrece información sobre el tipo de aplicaciones y sus versiones que se están utilizando para ejecutar estos servicios.

c) Realizar una auditoría de seguridad: se realiza una completa auditoría de seguridad de una red, gracias a la cantidad de información que es capaz de ofrecer.

d) Detectar sistemas operativos: analizar una red para detectar el sistema operativo que están utilizando los distintos equipos que se conectan a la red, así como la versión de este (a esta función se la conoce como OS fingerprinting).

2.3.3. OpenVas: es otra herramienta para el escaneo de vulnerabilidades la cual puede identificar diferentes problemas de bajo a alto riesgo y que según sus cifras oficiales cuenta con más de 50.000 test y datos de vulnerabilidades conocidas y alimentadas a diario por la empresa y por parte de la comunidad y sus expertos.

Este nos sirve para realizar las siguientes funciones:

a) Pruebas autenticadas.
b) Pruebas no autenticadas.
c) Cuenta con protocolos industriales y de Internet de alto y bajo nivel.
d) Ajustes personalizados de rendimiento para exploraciones a gran escala.
e) Desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

2.3.3.1. Características: cuenta con una licencia publica general de GNU, muy llamativo para los que trabajan con este tipo de software y otras como su i) extensa y definida documentación, ii) posibilidad desde línea de comandos y en modo gráfico con una interfaz con utilidades y repleta de datos de interés, capaz de sacar informes de interés y iii) una comunidad que ofrece bastante tutoriales y apoyo a la hora de explotar vulnerabilidades, por su web y por otros foros como Reddit, por ejemplo.

2.3.4. ExploitDB: ya como mencionamos con Nmap, los exploit son una base da información sobre las vulnerabilidades los cuales son usados para en caso de detectar una en un sistema informático, usar dicho exploit para comparar y ver la forma de poder explotarla. Por lo que entra la herramienta ExploitDB, que es una aplicación web la cual reúne todas las bases de datos de exploits públicos conocidos que también permiten la consulta, descarga y aplicados por los pentesters en todo el mundo.

Es un proyecto sin ánimo de lucro y fue desarrollado por la compañía Offensive Security misma creadora del sistema operativo Kali Linux.

2.3.4. CVE: (Common Vulnerabilities and Exposures), es un listado que existe en la web y conforman todas las fallas de seguridad y de las cuales esta disponibles al público. Estos CVE, se les asigna un número de identificación (ID). Esta consulta

se puede realizar en el sitio web: https://cve.mitre.org/ donde podemos buscar con palabras relacionales o por código del CVE, es decir, si detectamos en nuestros sistemas una vulnerabilidad y esta emite algún código como por Nmap o la buscamos por medio de palabra relacionales, podemos saber mejor sobre esta vulnerabilidad y así tomar medidas correctivas y poder mitigar.

Por ejemplo: **CVE-2021-24074:** aplicable en los protocolos IPV4, donde el atacante se aprovecha del *source routing* para realizar una ejecución de código remota donde el atacante puede instalar programas, ver, cambiar o borrar información, así como crear nuevas cuentas dentro del servidor.

Solución: i). Bloqueo de conexiones *Source Routing, loose source routing y malformed IPv4 en el zone protection del Firewall,* específicamente donde este estos servicios de cara al internet.

2.4 ANÁLISIS DE LOS ANEXOS ESCENARIO 2 Y ACUERDO DESDE EL PUNTO DE VISTA LEGAL Y NO ÉTICO

Realizando las lecturas requeridas se evidencia en el acuerdo de confidencialidad procesos ilegales y no éticos de los cuales se explican a continuación:

> ***Primera. Objeto:*** *en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios,* ***autoridades legales****, asesores o cualquier persona relacionada con ella, la información confidencial o* ***sobre procesos ilegales*** *dentro de Whitehouse Security no podrán ser divulgados.*

Este proceso es irregular ya que da a conocer a la parte receptora que la empresa si realiza procesos ilegales de los cuales no especifica, pero, por ende, da a entender que hay procesos irregulares dentro de la empresa y que aun así no se le permite al receptor divulgar, por lo que en lo legal infringe la ley y en lo ético como profesionales en la seguridad informática. Además, no se puede obligar a una persona natural, entregar información a autoridades legales puesto que, así sea una empresa y sus datos confidenciales, si está en un proceso de investigación, deben de colaborar con la justicia del país en pro de hallar y resolver los casos que estas mismas lleven a cabo.

> *Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como* ***"datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".***

Este proceso es irregular ya que hace entender a la parte receptora que realizan procesos de acceso abusivo a la información y no indican en ninguna otra sección del acuerdo que este proceso está sujeto a previa autorización de la empresa que contrata los servicios y vigilancia por el Mintic, el cual es encargado, y autoridad competente del estado como lo es un juez el cual puede dar el permiso para que alguien actúe conforme a lo requerido para acceder de forma abusiva a la información por lo diferentes hechos que el juez considere.

> *3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.*
>
> *4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.*

Estos dos procesos tienen un mismo fin y dan a entender al receptor que si durante el proceso o actividades que realice evidencia actividades sospechosas, espionaje, ilegal donde se intervenga la apropiación de información de terceros, no debe de ser denunciada. Pues esto proceso son ilegales y no éticos que y como deber de buenos profesionales si se debe denunciar ya que están consagrados en la ey como delitos informáticos.

> *7. Responder por el mal uso que le den sus representantes a la información confidencial.*
>
> *8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.*

Estos dos procesos tienen el mismo fin y es que hacen entender a la parte receptora que en caso de que la empresa realice un mal proceso a la información confidencial, sea el receptor quien responda, librándose de toda culpa los directos responsables de la mala manipulación de la información.

> *Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.*

Este proceso hace entender al receptor que, si hay información ilegal que maneja la empresa y en caso de llegar esta información a sus manos y presentar inconvenientes, se acuda a personas privadas para que la empresa no quede

incurrida con responsabilidades legales, y ya viendo los anteriores términos la culpa pasaría directamente al receptor que posea dicha información quedando como culpable de las faltas legales que se hayan cometido para obtener dicha información.

Se observa que hay muchas faltas ilegales y no éticas en el acuerdo de confidencialidad y pues como se describe en el Anexo 2, el abogado que realizo dicho documento busca de una forma indirecta hacer quedar mal el nombre de la empresa y buscando que sea investigada legalmente acarreando costes de atenciones y personal para ser defendida, pues aun así no se pude asegurar que la empresa incurra en las faltas que se cree en el acuerdo este realizando.

2.5 ANÁLISIS DE LOS ANEXOS, EN RELACIÓN CON LA VULNERACIÓN DE LA LEY 1273 ARGUMENTANDO CUALQUIER PROCESO ILEGAL.

Efectivamente el acuerdo de confidencialidad si vulnera ciertos artículos de la ley 1273 de 2009 la cual rige para Colombia, siendo los siguientes:

***Artículo 269A**. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

Este artículo es aplicable al acuerdo de confidencialidad analizado ya que en el menciona la obtención de datos en proceso ilegales como las chuzadas, interceptación de información y accesos abusivos a sistemas, es decir, realzan procesos de acceso abusivo de información y que el receptor no debe de divulgar, por ende, se puede aplicar el artículo para iniciar un proceso de investigación sobre el mismo.

Se sabe en Colombia que para realizar dichos accesos, este debe estar autorizado por un juez como autoridad legal y que esta sea procedente con el proceso de investigación que se esté llevando, mas no una empresa que prestas servicios de ciberseguridad no debe tener dichos permisos.

***Artículo 269C.** INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses*

Este articulo nos relaciona con el acuerdo ya que este menciona que hay datos que se obtiene de forma ilegal y otros procesos de obtención de información con proceso de acceso abusivo y que no indican que este previo autorizado por orden judicial y el cual estaría violando el articulo como tal

Artículo 269F*. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

Este artículo se puede aplicar al acuerdo de confidencialidad ya que hablan específicamente de obtención de datos ilegales de terceros que posiblemente sea un beneficio propio ara la empresa o por contrato de otra empresa que decida adquirir dicha información. Estaría incurriendo en el delito que menciona el articulo y del cual el receptor estaría entrando como cómplice.

También podemos tomar como referente otras leyes de las cuales manejan la línea ética de las empresas como lo es la ley 1778 de 2016, o la más conocida como la ley antisoborno, el código de procedimiento penal ley 906 de 2004 el cual habla de empresas involucradas en casos tipificados y el estatuto de anticorrupción ley 1474 de 2011 la cual define y tipifica los elemento de corrupción privada, administración desleal, evasión fiscal, soborno transaccional y las acciones que la empresa debe tomar para evitar ser objetos de investigación y más específicamente la línea ética. Estas leyes se pueden aplicar antes de que el receptor de la información acepte el acuerdo de confidencialidad pueda denunciar los delitos y fallas de este.

2.6 ANÁLISIS DE LA PROPUESTA LABORAL, TENIENDO PRESENTE EN CUENTA LA REVISIÓN DESDE EL PUNTO DE VISTA LEGAL Y ÉTICO

El código de ética para el ejercicio de la ingeniería en general y sus profesiones a fines y auxiliares donde se definen el catálogo de las conductas profesionales que se exigen y prohíben o que inhabilitan a los ingenieros en general siendo este nuestro marco legal y al estar aplicando a este acuerdo de confidencialidad, estaría faltando a este código, y estar colocando en riesgos mi carrera, titulo y honra de mi nombre ya que como sabemos, dicho acuerdo cuenta con fallos en sus procesos, proceso que van en contra del código de ética.

El Código de Ética Profesional contenido en la Ley 842 de 2003, está compuesto de manera general por tres capítulos; el primero, de disposiciones especiales (Artículos 29 y 30); el segundo, con los deberes, las obligaciones y las prohibiciones (Artículos

31 a 44) y, el tercero, con las inhabilidades e incompatibilidades en relación con el ejercicio de la profesión (Artículo 45).

Si aplico a esta oferta puedo conllevar a la imposición de alguna de las siguientes sanciones:

1. Amonestación Escrita, en el caso de las faltas leves.
2. Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios.
3. La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

En este código, en el artículo 31, habla sobre los deberes generales, el artículo 32 de las prohibiciones generales, el artículo 33 de los deberes especiales, el artículo 34 de las prohibiciones especiales.

Para nuestro caso estaríamos faltando al ARTÍCULO 41. DEBERES DE LOS PROFESIONALES QUE SE DESEMPEÑEN EN CALIDAD DE SERVIDORES PÚBLICOS O PRIVADOS. Son deberes de los profesionales que se desempeñen en funciones públicas o privadas, los siguientes:

a) Actuar de manera imparcial, cuando por las funciones de su cargo público o privado, sean responsables de fijar, preparar o evaluar pliegos de condiciones de licitaciones o concursos;

b) Sentencia C-570 de 2004, Corte Constitucional. Inexequible. Los profesionales que se hallen ligados entre sí por razón de jerarquía, ya sea en la administración pública o privada, se deben mutuamente, independiente y sin perjuicio de aquella relación, el respeto y el trato impuesto por su condición de colegas.

El ARTÍCULO 43. DEBERES DE LOS PROFESIONALES EN LOS CONCURSOS O LICITACIONES. Son deberes de los profesionales en los concursos o licitaciones:

a) Los profesionales que se dispongan a participar en un concurso o licitación por invitación pública o privada y consideren que las bases pudieren transgredir las normas de la ética profesional, deberán denunciar ante el Consejo Profesional respectivo la existencia de dicha transgresión;

b) Sentencia C-570 de 2004, Corte Constitucional. Inexequible. Los profesionales que participen en un concurso o licitación están obligados a observar la más estricta disciplina y el máximo respeto hacia los miembros del jurado o junta de selección, los funcionarios y los demás participantes.

Si aplico a esta oferta puedo recibir también las sanciones del capítulo III de código de ética COPNIA y todo su contenido.

2.7 ANÁLISIS DEL CASO "OPERACIÓN ANDROMEDA BUGGLY" DESDE SU POSICIÓN TENIENDO EN CUENTA LOS ASPECTOS LEGALES Y ÉTICOS.

La operación Andrómeda Buggly, se sabe que fue creado por las fuerzas militares para poder buscar conocimientos y personas con capacidades técnicas en hacking y así obtener información y herramientas de las personas civiles y poder "supuestamente" realizar inteligencia en su momento a las Farc y el ELN.

Pero según lo que la fiscala posterior sanciono, fueron delitos de espionaje y violación de datos personales a varios militares puesto que estaban usando software malicioso para realzar el espionaje a otros dispositivos, donde no se pudo confirmar si era a las Farc o personas civiles.[4]

Sabiendo que se si se cometieron diferentes actos delictivos que infringen las normas de nuestro país, mi posición ante esta operación va encontrar de todo lo ético y legal que se puede conocer, ya que si las personas que visitaban este lugar para asistir a sus actividades supieran que era para ayudar a las fuerzas militares en obtener conocimientos y capacidades para bien propio y si un compensación justa, dichas personas no asistirían a este lugar, denunciandolo por robo de intelecto sin previo consentimiento.

La idea de tener un lugar donde se pueda observar el talento de las personas con conociendo en ciberseguridad está bien, siempre y cuando se le s informe previamente y que las personas que asistan es porque quieren y saben los fines de dicho proceso y que si es para poder obtener un trabajo o realizar una actividad especifica, esta esté vigilada por las autoridades legales y que está bajo un contrato laboral por los servicios que las fuerzas militares requiera y no estar usando fachadas para logara sus fines ilegalmente.

2.8 INFORME DE HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS PARA DAR SOLUCIÓN AL ESCENARIO DE RED TEAM DE ACUERDO CON LOS PASOS DEL PENTESTING.

Se recibe pruebas del equipo forense sobre la maquina o sistema operativo que esta presentado la fuga de información.

[4] ENTER.CO. Detrás De Buggly: La Historia De La Fachada Andrómeda. [Sitio Web]. [Consultado: 23 de febrero de 2023]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Para realizar el análisis de esta copia de servidor se requiere ejecutar el sistema operativo en una maquina por lo que se opta la opción de los virtualizadores digitales y se selecciona el VirtualBox de Oracle.

Podemos revisar la maquina con algunas acciones dentro de la misma, pero para poder obtener mejor información hacemos uso de otra máquina virtual que herramientas más avanzadas y de mejor capacidad para una examen completo y profundo que en este caso el sistema operativo de Kali Linux nos ofrece.

A continuación, mostraremos las herramientas a usar para poder analizar el escenario propuesto según los pasos del pentesting:

2.1.1. Paso 1 Pentesting: Recopilación de información / Enumeración

2.1.1.1. El Kali Linux: es una distribución de Debian diseñada para temas de seguridad muy variados como análisis de redes, ataques inalámbricos, análisis forenses y otros. Contiene herramientas para llevar a cabo todas estas pruebas de seguridad y análisis.

Kali nos funciona para:

1. Recopilación de información
2. Análisis de vulnerabilidad
3. Ataques inalámbricos
4. Aplicaciones web
5. Herramientas de explotación
6. Pruebas de estrés
7. Herramientas forenses
8. Sniffing y Spoofing
9. Ataques con contraseña
10. Mantener el acceso
11. Ingeniería inversa
12. Herramientas de información
13. Hacking de hardware

Sus principales características son:

1. Está disponible gratuitamente y hacer uso de forma profesional y personal.
2. Tiene más de 600 herramientas para trabajar todas sus funcionalidades ya mencionadas.
3. Cuenta con un gran soporte técnico en diferentes idiomas.
4. No requiere ser instalado puesto que este se puede usar en línea que permite utilizarlo desde dispositivos portátiles en casi cualquier sistema.
5. Está desarrollado en un entorno seguro, permitiendo tener garantías acerca de datos y fallos.

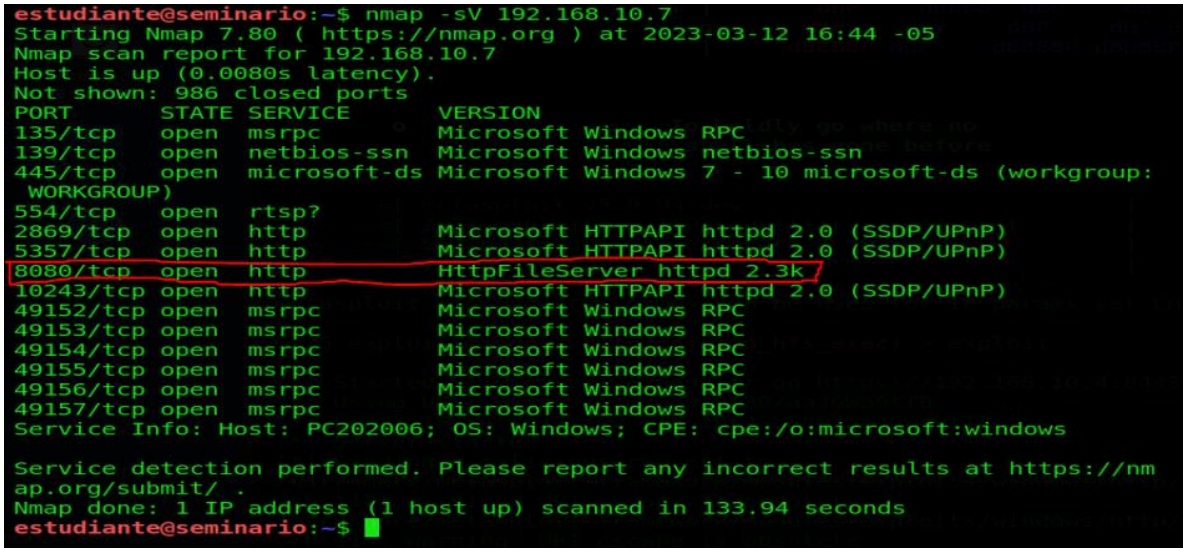
6. Usa el estándar de jerarquía de sistema de archivos (FHS) que permite bibliotecas, archivos de soporte, etc.

2.1.1.2. Nmap: La siguiente herramienta a usar es Nmap la cual dentro del primer paso de pentesting y para ayudar en el análisis del caso problema, nos dará un escaneo de puerto completos e identificar si hay fugas de información. Esta herramienta se ejecuta desde Kali Linux.

Nmap es un programa de código abierto, creado en 1998 por Gordon Lyon, funciona para realizar escaneos de redes, puertos y dispositivos. Con esta herramienta se puede determinar qué dispositivos están conectados en una red, qué puertos tiene activos y qué servicios se hallan en ellos.

Para poder dar uso de esta herramienta, debemos de tenerla instalada en el sistema operativo de Kali, conocer la IP de nuestra red en Kali donde se abre una terminal y con el comando *hostname -I* conoceremos el rango, luego con el comando nmap -n, la dirección IP y un rango de búsqueda, identificara los dispositivos conectados, por ejemplo, si nuestra IP de Kali es 192.168.10.4 para el comando Nmap seria *nmap -n 192.168.10.0/24* le estamos indicando a Nmap que busque todas las IP que este n el rango de 0 a 24. Cuando encontremos la Ip donde queremos realizar el escaneo de puertos usamos el comando *Nmap -sV* y la dirección IP para hallar los puertos y servicios activos como se observa en la figura 6.

Figura 6 Puerto abiertos y servicios en Windows



Fuente: Autoría Propia

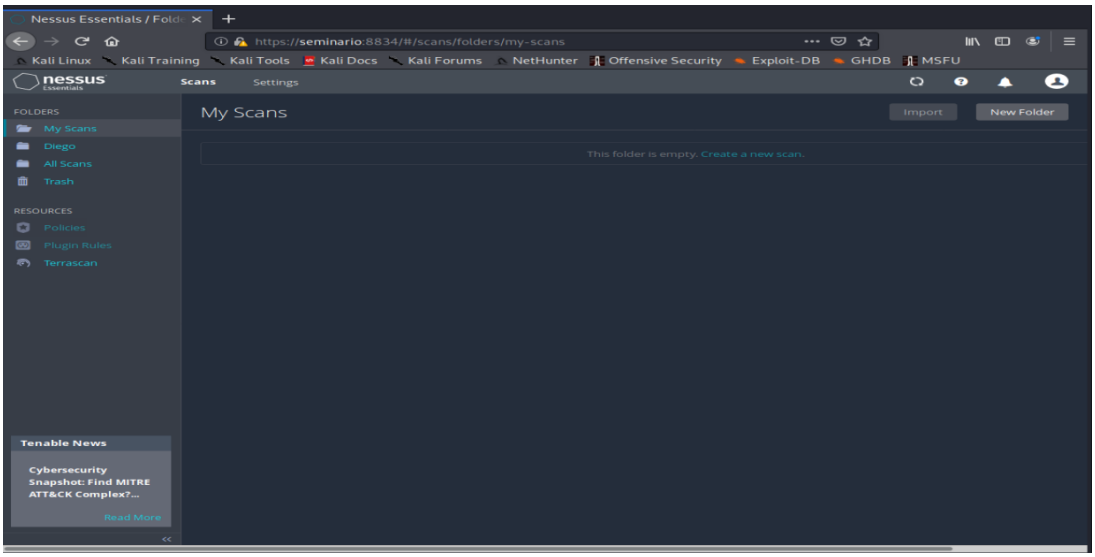
2.1.2. Paso 2 Pentesting: Análisis De Vulnerabilidades: al identificar los posibles servicios activos y puertos abiertos realizamos un análisis de vulnerabilidades de

dichos servicios y puertos por lo que la herramienta **Nessus** nos dará dicha información.

Esta herramienta es de código abierto y tiende a ser una aplicación de seguridad como profesional para realizar pruebas de penetración contando con características como:

1. Servidor proxy de interceptación.
2. Rastreadores webs tradicionales y por AJAX.
3. Escáner automatizado.
4. Escáner pasivo.
5. Navegación forzada.
6. Fuzzer
7. Soporte para WebSocket.
8. Lenguajes de scripting y compatibilidad con Plug-n-Hack.

Figura 7 Entorno Nessus y análisis de vulnerabilidades

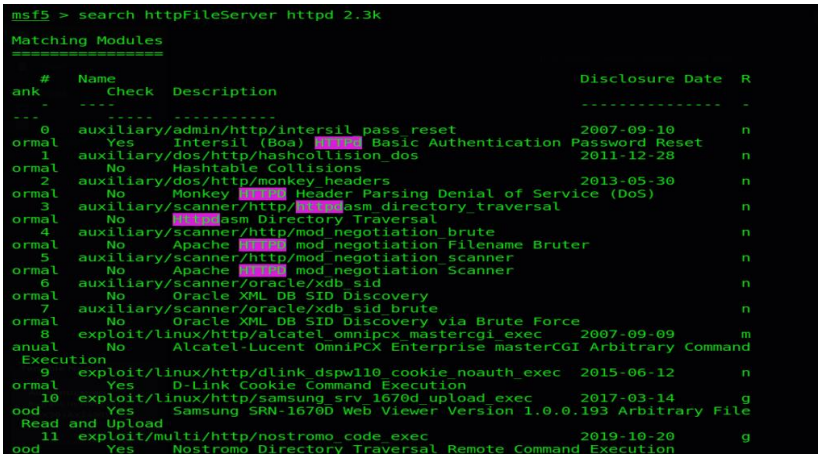


Fuente: Autoría Propia

2.1.3. Paso 3 Pentesting: Explotación De Vulnerabilidades: en este paso y con la identificación de las vulnerabilidades halladas del paso anterior, usaremos la herramienta **metasploit table,** la cual nos permitirá por medio de exploits intentar acceder al sistema por medio de los puertos hallados

Esta herramienta también es de código abierto diseñada para la seguridad informática sobre vulnerabilidades de seguridad, pero usaremos más específicamente el metasploit framework el cual podemos desarrollar y ejecutar exploits y el cual será muy útil para explotar la vulnerabilidad de Redejjit 2.3 como se observa en la figura 8.

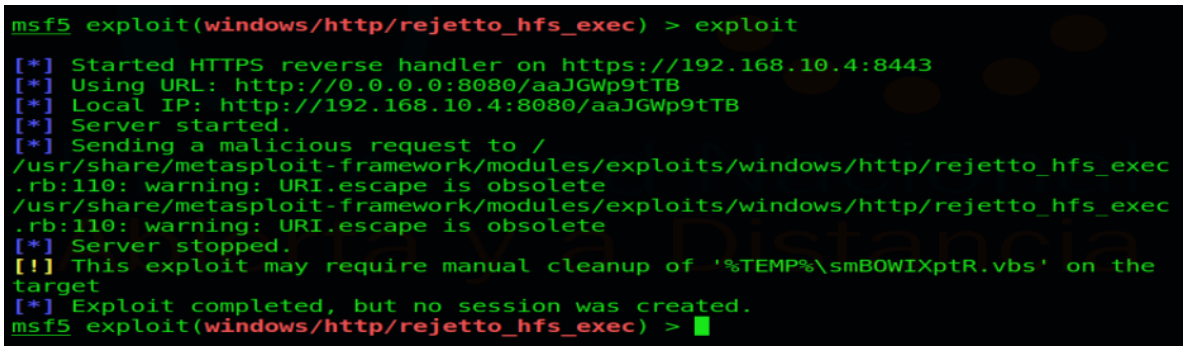
Figura 8 Metasploit y búsqueda de vulnerabilidades



Fuente: Autoría Propia

2.1.4. Paso 4 Pentesting: Post explotación: para este paso usaremos la misma herramienta de **metasploit** ya que se nos facilita continuar con la misma firma para poder realizar la creación de usuario administrador y sus privilegios con el fin de poder demostrar la falla existente. En la figura 9 observaremos el acceso a la maquina atacada.

Figura 9 Acceso maquina atacada



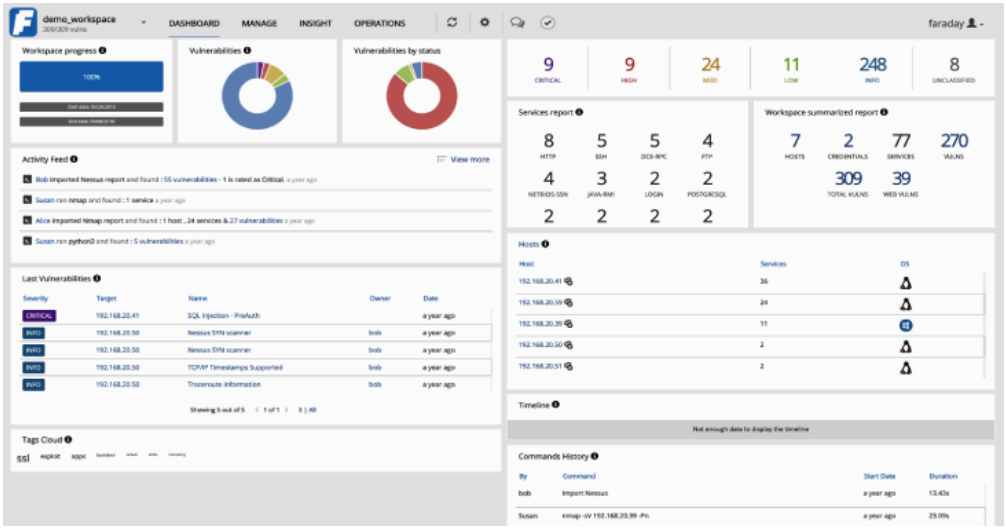
Fuente: Autoría Propia

2.1.5. Paso 5 Pentesting: Reporte: en el último paso del pentesting, se usará la herramienta de **Faraday** la cual es un IDE donde se pueden ejecutar aplicaciones que haya realizado algún análisis de vulnerabilidad y post explotación, tomando sus registros y montándolos de forma visual como reporte para entenderlos de forma sencilla.

Esta herramienta nos permite distribuir, indexar y analizar todos los datos recopilados durante una auditoría de seguridad la cual comprende información de

los sistemas, configuraciones, aplicaciones, redes y prácticamente cualquier elemento de una red como se observa en la figura 10.

Figura 10 Interfaz y reporte con faraday



Fuente: Autoría Propia

Al aplicar estos pasos de pentesting, puede existir la posibilidad que se logre identificar la vulnerabilidad y las amenazas que puede llegar alcanzar cada una como su daño dentro de la compaña del cual está sufriendo la fuga de información.

2.9 INFORME CON ANÁLISIS DEL CASO DE RED TEAM, QUE PERMITIÓ DAR SOLUCIÓN AL FALLO IDENTIFICADO.

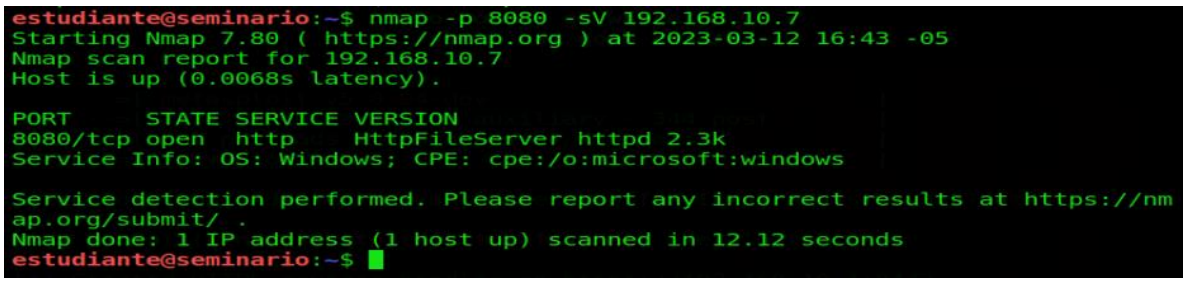
Para que el equipo de Red Team haya podido dar con el daño, inicialmente se investiga las aplicaciones de la maquina afectada y sus funciones, después de haber analizado el sistema se observa la aplicación Rejjeto 2.3 la cual es un sistema que permite el envío y recepción de información o archivos de forma local o como servidor para poder compartir información con personas o destinos específicos. Este usa el protocolo HFS (Servidor de archivos HTTP) del tipo P2P servidor WEB del cual su diseño es con el fin de compartir archivos que usan tecnología web para ser más compatible con el internet moderno.

Los usuarios pueden descargar la información de este servidor sin instalar ningún programa especial y los pueden hacer por cualquier ID, por ejemplo, Firefox o Google Chrome.

Al hacer el escaneo de los puertos con la herramienta **Nmap**, se evidencia en la figura 11 que este servidor maneja el puerto 8080 y que este está abierto y que posiblemente puede terminar en una Shell reversa y una sesión abierta de meterpreter. Lo que implicaría que los usuarios hábiles pueden elevar privilegios a

usuarios o crear sus propios usuarios Administradores y controlar el sistema anfitrión.

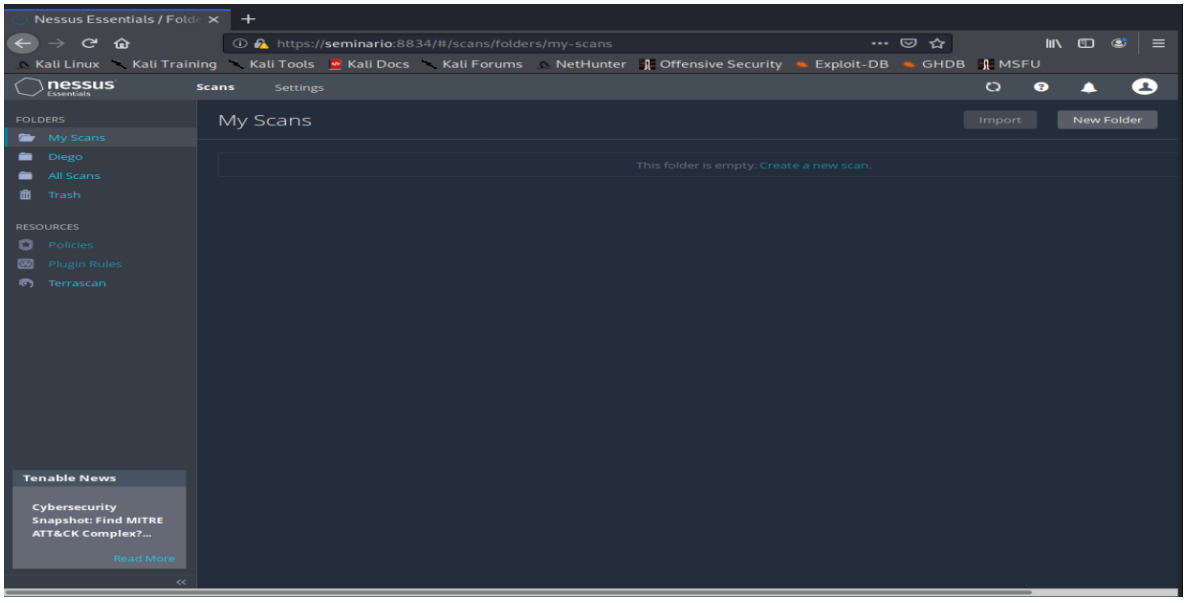
Figura 11 Escaneo especifico a puerto 8080 con Nmap



Fuente: Autoría Propia

También se hace un análisis de vulnerabilidades con **Metasploit** o **Nessus** como se observa en la figura 12**.**

Figura 12 Interfaz y análisis de Nessus



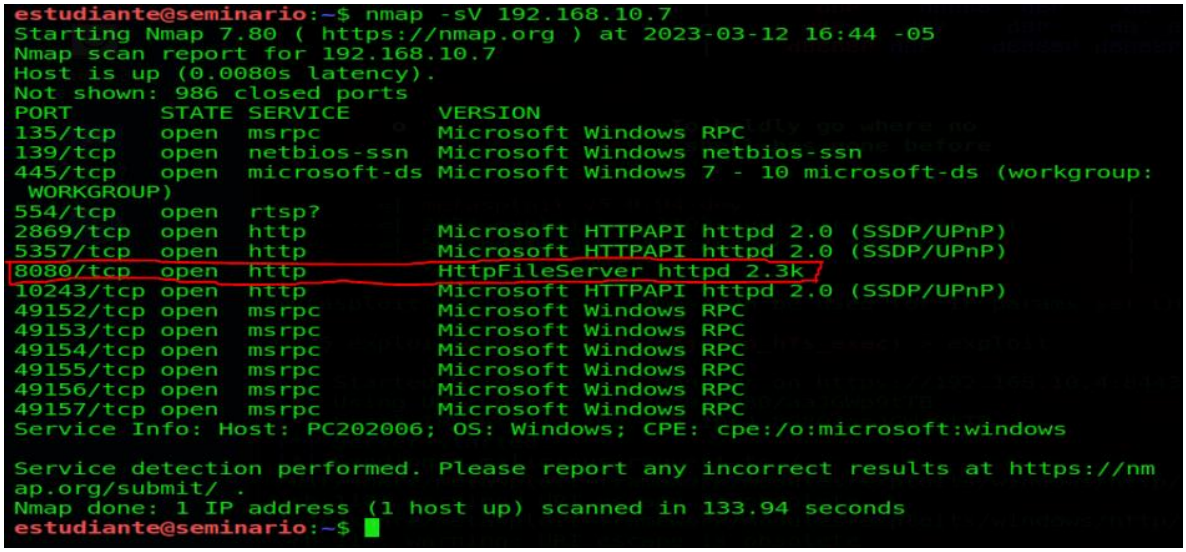
Fuente: Autoría Propia

Para dar solución al problema inicialmente se verifica las versiones de Rejjeto y si hay disponibles, actualizarlas inmediato, de lo contrario suspender inmediatamente el uso de esta herramienta, realizar un backup al sistema operativo y posterior formatear ella memoria y reinstalar el sistema operativo con sus respectivos parches actualizados.

2.10 INFORME DE HERRAMIENTAS UTILIZADAS PARA DAR IDENTIFICAR FALLOS EN EL ESCENARIO PROPUESTO.

Las herramientas utilizadas para la identificación de fallos fue Nmap la cual nos indica que puertos están abiertos y que versión de este se está ejecutando, Para esta situación, el puerto que abre la aplicación es el puerto 8080 como se observa en la figura 13.

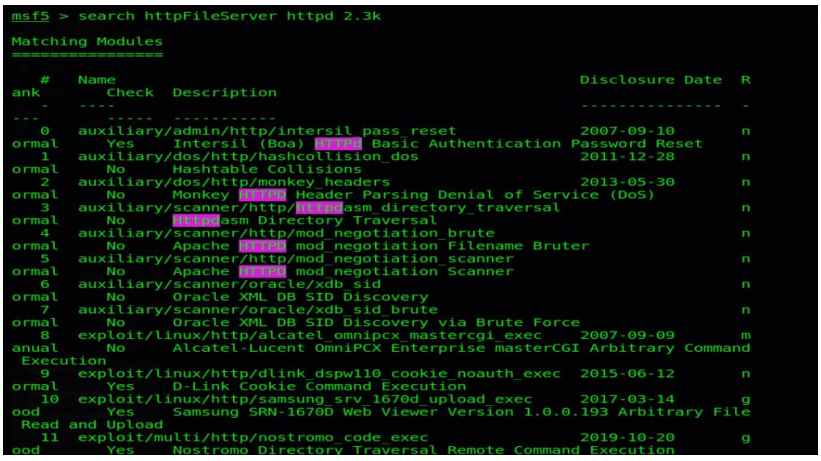
Figura 13 Puerto abiertos y servicios en Windows



Fuente: Autoría Propia

Posterior de haber identificado la versión, usamos la herramienta de metasploit la cual al ingresar la versión encontrada por Nmap, este nos mostrar la serie de vulnerabilidades que puedan existir sobre dicha versión y poder encontrar los fallos de fuga de información. En la figura 14 podemos observar los diferentes fallos hallados lo cual nos demuestra que tenemos una fuga de información o fallo en la seguridad de esta y con esta detección ya se pude tomar decisiones sobre como poder mitigar la vulnerabilidad y posterior analizar los sistemas y verificar si ha ocasionado algún daño interno de la compañía.

Figura 14 Búsqueda de los exploit según la versión del puerto



Fuente: Autoría Propia

2.11 ANÁLISIS DEL ATAQUE PRESENTADO A CADA UNA DE LAS MAQUINAS IDENTIFICADAS.

Ya identificado el ataque, podemos decir que, las afectaciones que pueden causar un ataque de este tipo son grandes, ya que el atacante podía elevar privilegios, crear usuario de tipo administrador y copiar archivos, de los cuales puede hacer inyecciones SQL, ataque de ransomware, etc.
¿Pero quién puede estar detrás de este ataque?, pueden ser personas denominadas hackers que actúan de forma independiente y que normalmente los hacen por un beneficio económico.

También están los grupos organizados que tiene distintas finalidades como terroristas o ideológicas (Activistas).

Los mismos gobiernos pueden estar detrás de un ataque que se enmarcan de forma estratégica para una guerra cibernética y como destino puede ser sistemas informáticos de otros gobiernos o activos importantes de entidades públicas o privadas.

Las empresas privadas las cuales pueden estar realizando algún trabajo de espionaje cibernético del cual puede ser acciones autorizadas por un ente de control legal o de forma ilegal.

El análisis que ha presento a la compañía del caso estudio, se desconoce aún la fuente del mismo, pero lo que se sabe es que explotaron una vulnerabilidad que poseía una aplicación de intercambio de archivos WEB, por ende los riesgos o afectaciones económicas son elevados ya que para una pyme puede perder información y tener danos a la estructura informática de su empresa y el valor redonde sobre los cien millones de pesos colombianos, donde se incluyen coste de

negocio perdido, las mejoras de software y sistemas y los gastos extra en personal interno y en asesoramiento experto.

Si hablamos del ataque solo a la máquina de Windows 7, podríamos decir que la afectación más elevada es una denegación de servicios o ataque DoS, el cual inhabilita el sistema y se captura la información de este, pero solo de forma local, ya que también puede crear un puente dentro de toda red y así acceder a toda la infraestructura tecnológica y causar daños más grandes como los descritos anteriormente.

En la figura 15 podemos observar de forma gráfica el ataque que se realizado al Windows 7.

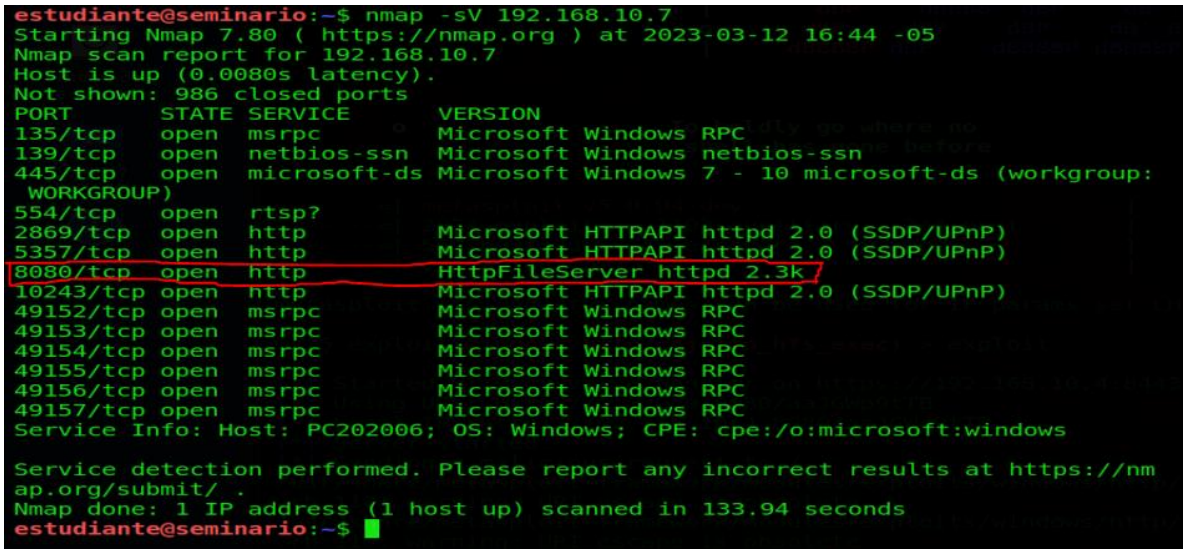
Figura 15 Grafica de ataque

Fuente: Autoría Propia

2.12 INFORME DE LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Teniendo la copia de del servidor afectado procedemos a aplicar los pasos del pentesting ya mencionados y hallados las posibles fugas de información, se procede con la herramienta metasploit, realizar la búsqueda de las vulnerabilidades sobre la herramienta rejetto y el servicio de HFS. En la figura 16 observamos la identificación del servicio activo y en que puerto se está ejecutando

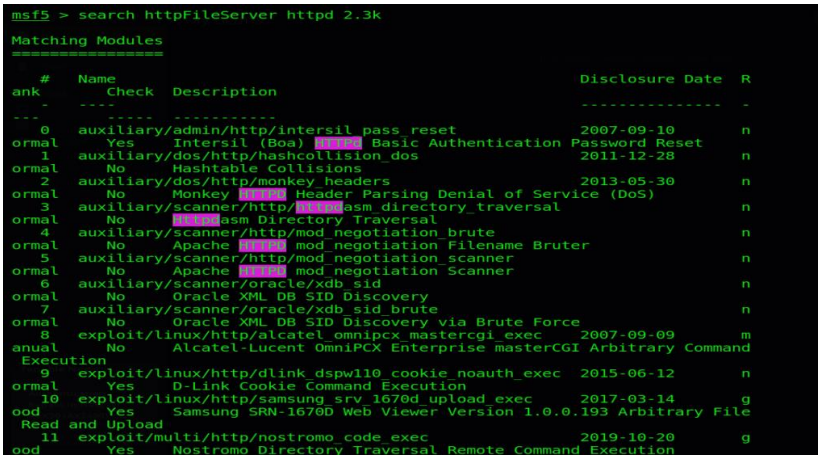
Figura 16 Puerto abiertos y servicios en Windows



Fuente: Autoría Propia

En la figura 17 realizamos la búsqueda de los exploit relacionados con el servicio que se está ejecutando

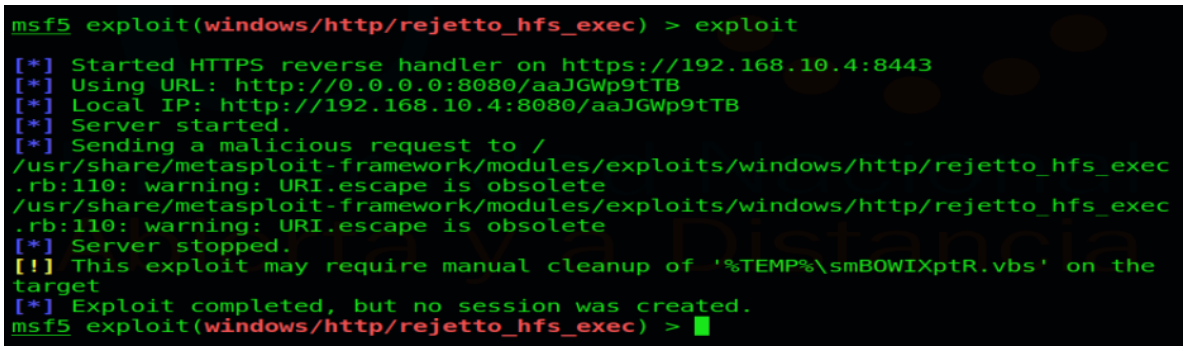
Figura 17 búsqueda de esploit para el puerto 80



Fuente: Autoría Propia

Y en la figura 18 con ayuda de los payload lanzamos el ataque a la maquina windows

Figura 18 ejecución de ataque



Fuente: Autoría Propia

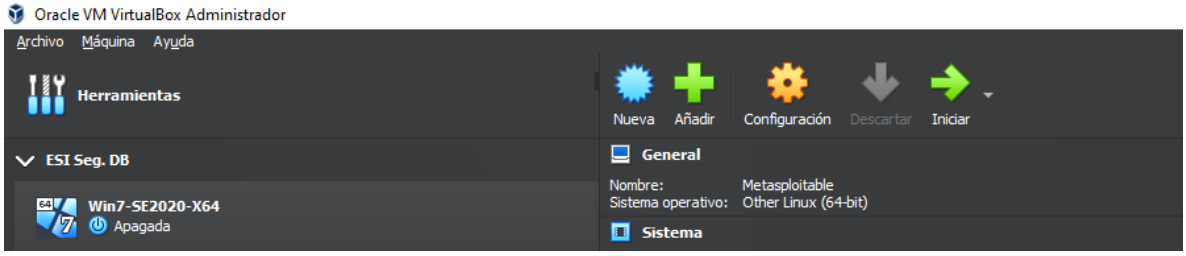
Y así podemos realizar las búsquedas de vulnerabilidades en cualquiera de los puertos que escaneo nmap, cada servicio es buscado con la herramienta de metasploit y validar si hay algún exploit para realizar el ataque

2.13 EVIDENCIA DE LA EXPLOTACIÓN DE LA VULNERABILIDAD IDENTIFICADA.

En esta sección evidenciaremos el proceso de pentesting realizado desde la instalación de las maquinas virtual con sus herramientas hasta lograr la explotación de una vulnerabilidad.

Esta máquina es una Windows 7 con arquitectura de 64 bits. Esta copia se monta en un sistema virtualizado de sistemas operativos: VirtualBox para poder abrir el archivo dentro de un sistema controlado como se observa en la figura 19:

Figura 19 Maquina Windows 7 x64



Fuente: Autoría Propia

Para realizarle un escaneo usamos las herramientas que contiene el programa Kali Linux el cual se monta en el mismo sistema virtualizado y configurando las máquinas para que tengan conexión entre estas mismas como se observa en la figura 20:

Figura 20 Maquinas Windows 7 y Kali Linux

Fuente: Autoría Propia

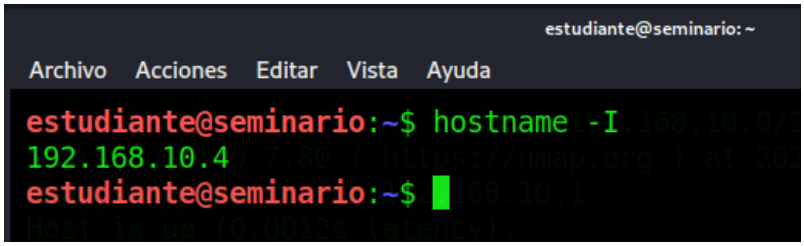
Comenzaremos con la recopilación de información en la cual tendremos que encender la maquina con la vulnerabilidad en este caso Windows 7 y la maquina con las que realizaremos las pruebas que él es Kali, como se observa en la figura 21.

Figura 21 Maquinas Windows 7 y Kali Linux corriendo

Fuente: Autoría Propia

2.6.1. Recopilación de información: Hacemos uso de la herramienta **Nmap**. Identificaremos la IP de Kali para saber sobre que rango realizar el escanear de la red con el comando *Hostname -I* como se observa en la figura 22.

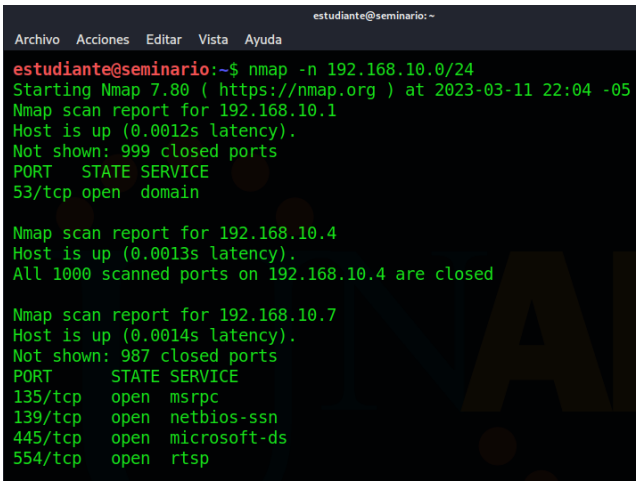
Figura 22 Identificación de IP Kali



Fuente: Autoría Propia

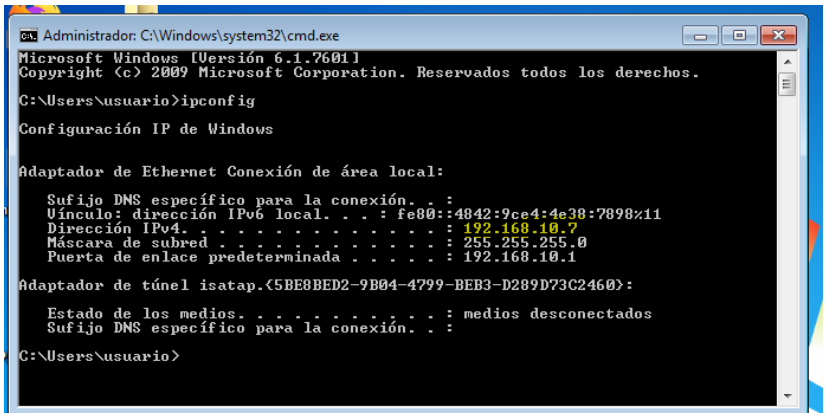
Luego, procedemos *nmap -N 192.168.10.0/24* para poder conocer todas las IP dentro de la red como se observa en la figura 5. Ha reconocido dos direcciones IP, la del local que es 192.168.10.4 y otra IP que es la 192.168.10.7 de la cual debería ser la dirección de Windows 7 la cual se corrobora en la figura 23.

Figura 23 Identificación de todas las IP dentro de la red



Fuente: Autoría Propia

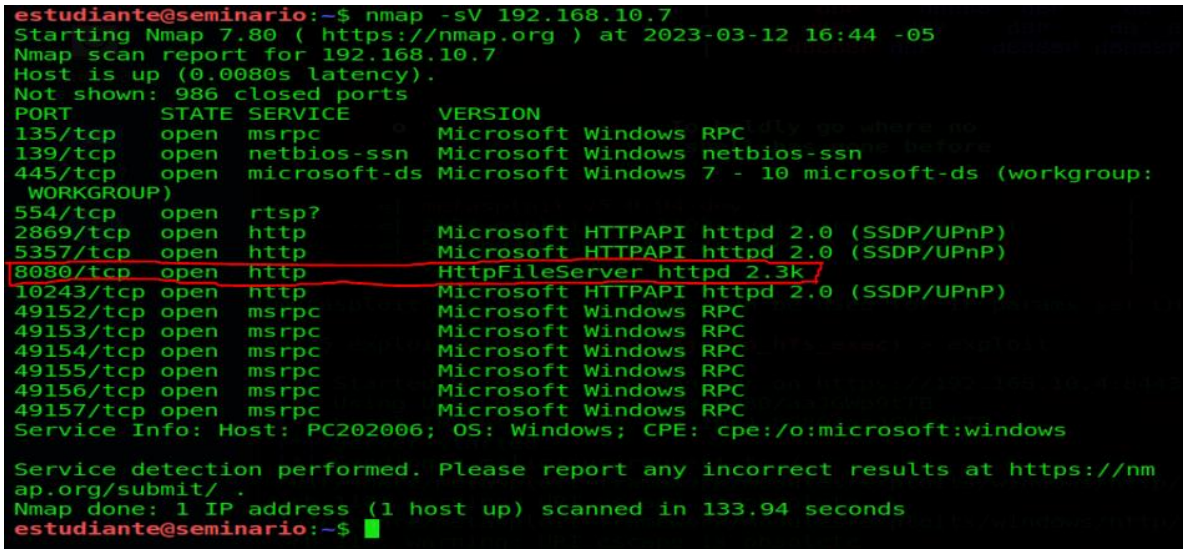
Figura 24 comprobación de IP de Windows



Fuente: Autoría Propia

Con la figura 24 comprobamos que tenemos conexión entre las dos máquinas. Ahora procedemos con el comando *nmap -sV 192.168.10.7* para identificar en detalle los puertos de esta misma y sus versiones como se observa en la figura 25

Figura 25 Puerto abiertos y servicios en Windows

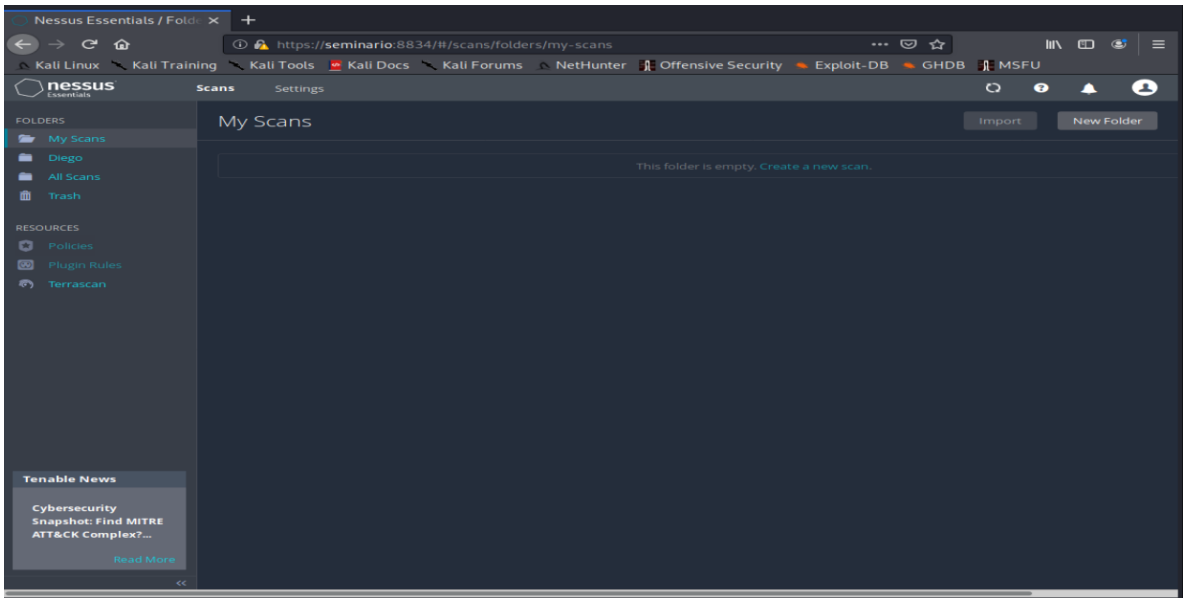


Fuente: Autoría Propia

Se identifica el puerto 80 con el servicio de HFS (httpfileserver httpd 2.3k) el cual es el mismo de la aplicación Rejjeto y el que está permitiendo la fuga de información. Sobre este puerto comenzaremos a analizar las vulnerabilidades según su servicio

2.6.2. Análisis de vulnerabilidades: como se mencionaba en los informes técnico previo usaremos la aplicación Nessus para analizar las posibles vulnerabilidades de este servicio. Para poder ejecutar esta aplicación se debe de instalar en nuestro sistema operativo del Kali Linux previamente para ver tener la interfaz de la figura 26.

Figura 26 Entorno Nessus y análisis de vulnerabilidades

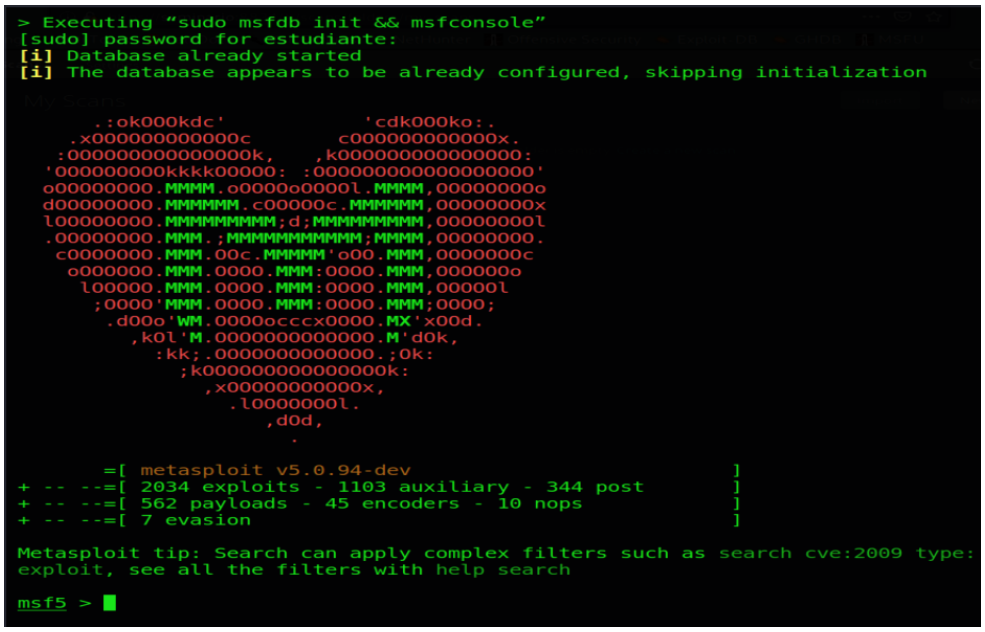


Fuente: Autoría Propia

Al instalar Nessus, procedemos con crear un nuevo scan y despues con digitar el destino y puerto hallado con Nmap para analizar dicha vulnerabilidad y obtener como resultado el nivel de criticidad del sistema completo y las vulnerabilidades de cada puerto

2.6.3. Explotación de Vulnerabilidad: desde nuestra terminal de Kali procedemos a iniciar los servicios de metasploit el con el cual intentaremos explotar a la vulnerabilidad de Rejjeto del puerto 80 con el comando sudo *service postgresql start* y luego ejecutamos el comando *sudo msfdb init,* esto con el fin de iniciar los servicios de la base de datos de metasploit. Por último, procedemos con inicar la herramienta con el comando *sudo msfconsole,* y poder visualizar la interfaz que se observa en la figura 27:

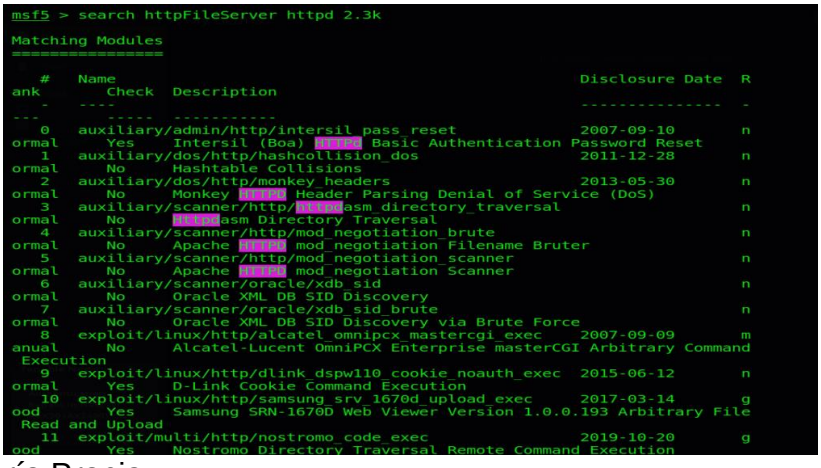
Figura 27 Interfaz Metasploit



Fuente: Autoría Propia

Continuamos con la búsqueda de la vulnerabilidad por lo que escribimos la palabra *Search* en la consola y posterior colocamos el nombre del servicio del puerto 80 que encontramos con Nmap para hallar los diferentes esploit asociados como se observa en la figura 28:

Figura 28 búsqueda de esploit para el puerto 8080

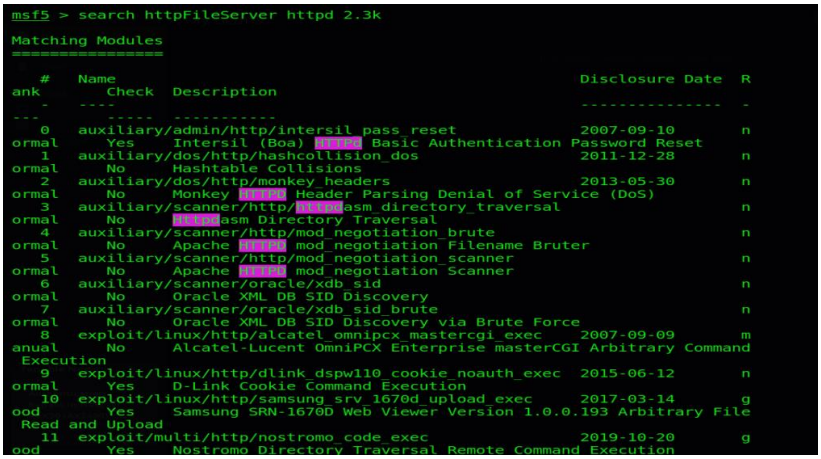


Fuente: Autoría Propia

Usaremos el exploit adecuado para la vulnerabilidad, el cual es el que menciona a la de Rejjeto y que para usarlo escribimos la acción *use 18* o *use*

exploit/windows/http/rejetto_hfs_exec, según el listado de exploits como se observa en la figura 29

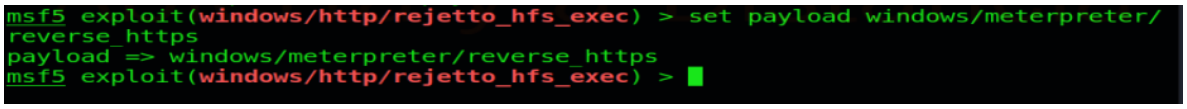
Figura 29 Selección de exploit para explotación de vulnerabilidad



Fuente: Autoría Propia

2.6.3. Post - Explotación de Vulnerabilidad: aquí en adelante se mostrará los pasos para explotar vulnerabilidad y acceder al sistema atacado, por lo que seguiremos con la herramienta de metasploit donde con el comando *show payloads* asignaremos un payload como se observas en la figura 30, este payload es una de las muchas opciones que podemos escoger:

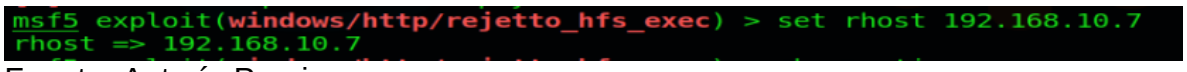
Figura 30 Selección de payload para explotación de vulnerabilidad



Fuente: Autoría Propia

Luego asignamos la IP que vamos a atacar la cual es la del Windows 7 y que sabemos es la 192.168.10.7 con el comando *rhost 192.168.10.7* como se observa en la figura 31

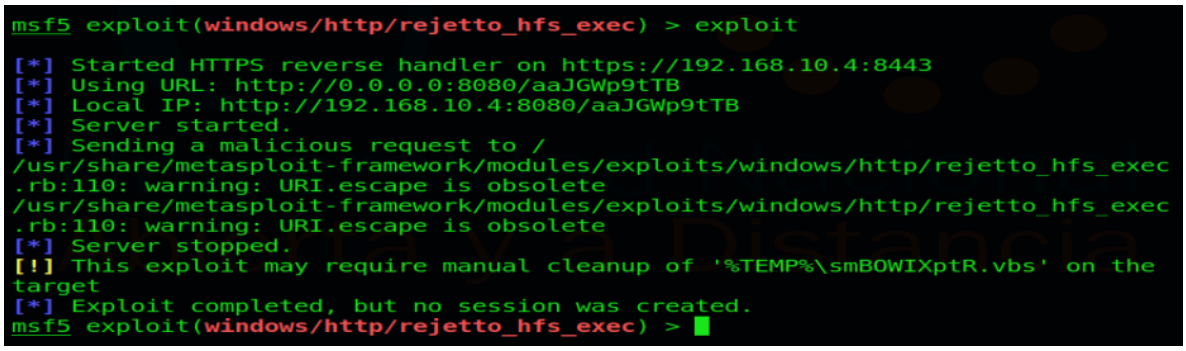
Figura 31 envío de IP destino para explotación de vulnerabilidad



Fuente: Autoría Propia

Y para lanzar el ataque escribimos el comando exploit como se observa en la figura 32.

Figura 32 ejecución de ataque



Fuente: Autoría Propia

Lastimosamente el OVA compartido por el curso no contaba con la versión de Rejetto que era vulnerable, por lo que se buscó en la red y no se encontró. Se procedió con la descarga de otra versión que era la 2.3.k la cual está ya parcheada y por ende no se pudo tener acceso a la máquina. Lo ideal, es que se lograra acceder al Shell por reversa de meterpreter el cual es el del payload seleccionado.

2.14 ANÁLISIS CON ACCIONES NECESARIAS PARA CONTENER UN ATAQUE EN TIEMPO REAL.

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

En caso de encontrarme con un ataque en tiempo real, comenzaría a revisar las zonas donde se esté presentado la afectación, es decir, para asegurar que se está sufriendo de un ataque en tiempo real se debe tener la plena seguridad que si existe y ello se verifica con el daño que está provocando.

Cuando se detecta un incidente de seguridad dentro de una organización pasa ser un momento crítico por lo que se debe de actuar con rapidez y de buena manera para reducir significativamente el impacto del daño.

Buscar la fuente del ataque debe ser rápido, indagaría que herramientas se cuenta dentro de la organización para la seguridad informática y así identificar con cual podemos identificar el ataque. Los antivirus de los computadores serian una herramienta buena para ejecutar un escaneo rápido, posterior seguiría con el firewall perimetral para evidenciar algún flujo fuera de lo normal. Estas serían las herramientas con las que podría identificar el ataque, ya después usaría una herramienta de escaneo como Nmap, para saber que puertos están abiertos y que aplicaciones o servicios funcionan con dicho puerto, lo asocio con los datos preliminares encontrados para hallar la fuente y por qué medio estamos siendo atacados.

Continuamos con el despliegue del equipo de seguridad si contamos con personal responsable quien han sido entrenados para saber cómo responder al ataque.

Identificamos el tipo de ataque para saber cómo está sucediendo y en donde nos vamos a enfocar la atención para dictar la mejor forma de contenerlo y recuperarnos del mismo. Mismo debemos de comprender su origen, alcance e impacto.

Conociendo más sobre el ataque que está sucediendo, se procede con cerrar la brecha, es decir, identificaremos y cerraremos todo el acceso que los delincuentes puedan tener al sistema, comenzando por el puerto donde estén accediendo.

Para el caso estudio planteado en la anterior actividad, se sabía sobre la herramienta que usaba un puerto para trasmitir archivo en la WEB, por lo que la acción inmediata es detener los servicios de dicho puerto y cerrarlo posterior, de ser necesario, desinstalar la aplicación de forma local. En caso de no poderlo hacer los pasos a seguir seri de forma efectiva:

a) Desconectar la red afectada de Internet
b) Deshabilitar todo acceso remoto a la red
c) Redirigir el tráfico de red
d) Cambiar todas las contraseñas vulnerables

Con esto podremos impedir que el atacante continue con su plan y antes de volver a colocar los sistemas en línea debemos de evaluar y repara los danos ocasionados, documentar los registros y eventos que dicho ataque haya dejado y si se cuenta con un equipo de análisis forense, la tera sería mejor.

Una vez contenido el ataque se debe de revisar el sistema por completo y saber si hay danos críticos, que datos pudieron ser afectados, identificar a cuantos sistemas accedió y verificar que no hayan quedado puntos de entrada o brechas. También sería necesario restaurar los datos que hayan sido comprometidos con las copias de seguridad que existiesen de los mismos. También reinstalar los sistemas operativos y reemplazar o arreglar el hardware que se haya dañado.

Ya por último se hace un comunicado sobre el ataque sucedido comenzando con aquellos que haya afectado siendo lo más franco y trasparente para mantener la confianza de los clientes y público en general.

Como recomendación es importante realizar los cambios en los sistemas informáticos con los debidos procedimientos para reducir en mínimo un posible ataque en futuro, es decir, usar el incidente para mejorar la seguridad cibernética y aprender de lo sucedido.

2.15 INFORME DE ACCIONES DE HARDENIZACIÓN A IMPLEMENTAR PARA EVITAR QUE SUCEDAN ATAQUES DE SEGURIDAD INFORMÁTICA.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

El hardening es el endurecer el sistema informático para reducir las vulnerabilidades que pueda tener un sistema, también lo llaman endurecimiento informático.[5]

Evidenciando el ataque descrito en el anexo, las medias de hardenizacion para evitar que el ataque se repita seria:

a) Cambiar todas las claves que se tengan y crear una política de escritorio seguro con una periodicidad de cambio de claves máxima de cada 3 meses con estructura de cifrado que contenga números, letras mayúsculas y minúsculas y caracteres especial de mínimo 8 dígitos.

b) Desinstalación todo el software que sea innecesario, que no se use según el rol del empleado o cliente.

c) Dar de baja a los usuarios inactivos o que hayan retirado de la compañía que se han innecesarios.

d) Deshabilitar todos los servicios que no se están utilizado en cada puerto según el rol de los empleados y clientes.

e) Aumentar la seguridad de los servicios o procesos que si tendrán que ser utilizados creando políticas en los firewalls para filtrado dinámico de paquetes y filtrado en base de firmas de dichos servicios.

f) Cerrar puertos que se encuentren sin uso a nivel general. Esto depende también de las funciones de cada empleado.

g) Utilizar copias de seguridad de datos importantes como respaldo y ser almacenados en un disco duro físico que no tenga acceso a la red.

h) Instalación de un firewall en caso de no poseer uno o que exista alguno pero que no sea completamente funcional para las necesidades de la organización.

[5] CISET. Que Es El Hardening informático. [Sitio Web]. [Consultado: 24 de marzo de 2023]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

i) Actualización de los sistemas operativos y software para obtener los parches de seguridad más recientes o nuevas herramientas de protección que le fabricante desea incluir.

j) Implantar un DLP (Data Loss Prevention) para evitar la fuga de datos y monitorear constantemente el flujo de información.

También podemos hacer hardenizacion con los usuarios donde por medio de capacitaciones podemos enseñarles a:

a) No abrir archivos desconocidos.
b) No descargar desde paginas no oficiales
c) Tener contraseñas robustas.
d) Tener cuidado con los correos electrónicos.
e) Tener nuestros sistemas operativos actualizados.
f) Tener un programa antivirus activado.

2.16 ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE EL EQUIPO DE BLUE TEAM Y EL EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS.

¿Describa con sus palabras las diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos?

El blue team es el encargado de diagnosticar las defensas actuales dentro de una organización y puede proponer mejoras con el fin de poder repelar un ataque informático con más eficacias.

Se apoya con el red team para realizar simulacros de ataques a los sistemas para poder observar los patrones y comportamientos de protocoles defensivos dentro de las organizaciones.

Estas simulaciones las hacen con el fin de poder reforzar la seguridad dentro de una empresa o analizar la seguridad después de haber sucedido un ataque informático y poder observar los puntos débiles de la seguridad, como un estudio forense.

El equipo de respuesta de incidentes es el personal capacitado y especializado en defensa y seguridad e la información el cual debe de estar preparado para cualquier ataque que sucedía en la vida real a la organización u organizaciones que estén protegiendo.

Mientras que el blue team realiza simulacros y testeo de la seguridad, el equipo de respuesta de incidentes actúa cuando este sucediendo un ataque en tiempo real del cual deben de identificar, contener, erradicar y tratar de recuperar la información de los daños ocasionados por el mismo.

Estos equipos pueden aprender uno del otro y posiblemente pueden actuar en conjunto si la organización así lo permite, mientras tanto el equipo de respuestas de incidentes es quién deberá erradicar cualquier ataque en tiempo real y el bleu team realizando los simulacros y testeo para mejorar la seguridad.

Las herramientas utilizadas para la identificación de fallos fue Nmap la cual nos indica que puertos están abiertos y que versión de este se está ejecutando, Para esta situación, el puerto que abre la aplicación es el puerto 8080.

2.17 ANÁLISIS SOBRE LA PERTINENCIA DE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" COMO PROPUESTA DE ASEGURAMIENTO POR PARTE DE UN EQUIPO DE BLUE TEAM.

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Comencemos por saber que son los CIS. Los CIS son un conjunto prioritario y prescriptivo de las mejores prácticas de seguridad informática que en su mayoría son acciones defensivas que ayuda a prevenir cualquier tipo de ataque desde los más peligrosos hasta los no tan peligrosos.

Esta practicas son creadas por un grupo de personas especializadas en las tecnologías de la información y con base a los datos de ataque sucedidos en la vida real y las defensas existentes efectivas contra dichos ataques.

Estos dan una orientación especifica y un camino entendible para que cada organización pueda implementar y logren poder cumplir sus objetivos sin preocupasen tanto por la seguridad informática.[6]

Para un equipo BlueTeam, sea requerido trabajar con estos CIS, estaría totalmente de acuerdo ya que con ellos podría desarrollar estructura fundamental para cada uno de los programas de seguridad informática y un marco para toda la estrategia de seguridad que la empresa haya requerido.

Se pude hacer una centralización en un conjunto de técnicas y medidas específicas y eficaces que estén disponibles para mejorar la seguridad en la organización.

Al tener prácticas y protocolos en base a los ataques sucedidos en el mundo real, podemos enfocar nuestra seguridad según estos hechos.

[6] MANAGENGINE. ¿Qué Son Y Cómo Implementar Los Controles De Cis (Cis Controls)?. [Sitio Web]. [Consultado: 26 de marzo de 2023]. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Y, por último, trabajaría con estos CIS ya que cumplen con las marcos y normas como lo son: ciberseguridad NIST, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP y FISMA

2.18 ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE UN SIEM.

Explique y redacte las funciones y características principales de lo que es un SIEM.

Los SIEM son un tipo de solución a la seguridad informática donde ayudan a muchas organizaciones a analizar y detectar amenazas y el cómo responder a cada una de ellas antes de que estas causen daños dentro de dicha organización.

Se combina la administración de información de seguridad (SIM) y la administración de ventos de seguridad (SEM) en solo sistema de administración de la seguridad para recopilar la información de registros de evento de distintas fuentes y validar cual se sale de las normas establecida en tiempo real y con base en ello toma las decisiones adecuadas para evitar cualquier ataque.

Estas tecnologías ha evolucionado con la inteligencia artificial logrando detectar amenazas y dando la respuesta a los incidentes con más inteligencia y rapidez.[7]

2.18.1 Las funciones es recopilar, almacenar y analizar grandes volúmenes de datos de todas las aplicaciones que la organización tenga bajo su funcionamiento, también de dispositivos, servidores y de los mismos usuarios en tiempo real con el fin de que los equipos de seguridad pueden detectar y contener los ataques cibernéticos. Estas herramientas funcionan con reglas ya predeterminadas por la organización que ayudan al demás personal de seguridad de cómo defenderse de los ataques y generar las alertas respectivas.

2.18.2 Las características más comunes de los SIEM son:

a) Administración de registros: recopilan grandes cantidades de datos en un solo lugar, los organizan y luego determinan si existe algún tipo de amenaza, ataque o vulneración dentro de los sistemas informáticos de una organización.

b) Correlación de eventos: Seguidamente, los datos se clasifican para identificar relaciones y patrones a fin de detectar amenazas potenciales y responder a ellas de forma oportuna y eficaz.

[7] MICROSOFT. ¿Qué Es Siem?. [Sitio Web]. [Consultado: 26 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

c) Supervisión de incidentes y respuesta a ellos: supervisa los incidentes de seguridad en la red de una organización y proporciona alertas y auditorías de toda la actividad relacionada con un incidente en caso de haber detectado uno.

2.19 INFORME DE ELECCIÓN DE 3 HERRAMIENTAS QUE PERMITAN CONTENER ATAQUES INFORMÁTICOS.

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Las herramientas de contención son aquellas que tiene la capacidad de detectar un ataque y poder contenerlos para que este prosiga y posterior se pude avisar al equipo de seguridad o que esta misma herramienta pueda erradicar las amenazas contenida, para ello mencionaremos 3 herramientas que pueden contener un ataque:

a) Software antivirus: para todos los sistemas informáticos y dispositivos de uso final conectados a la red, se debe de contar con dicho software de procedencia confiable.
   Estos programas cuentan con medidas de detección, contención y erradicación de ataques cibernéticos. Pueden colocar los dispositivos que estén atacados en estado de cuarentena y eliminar ciertos elementos maliciosos. En el mercado existen muchas soluciones diferentes que pueden integrar más herramientas, pero todos los antivirus son necesarios dentro de cada dispositivo para la protección de los datos contenidos.

b) Firewall perimetral de red: estos proporcionan por medio de su función principal de filtrado de paquete de datos, una protección en tiempo real de que información puede pasar y que información es detenida, contenida y que posterior alertado al equipo de seguridad para que pueda tomar las acciones respectivas para la eliminación de esta. Hoy en día los firewalls pueden ser de tipo software o hardware y se están integrando con nuevas herramientas de seguridad ya que estos se ubican en la red perimetral, según la OSI en la capa 3, donde se separa la información del mundo externo a nuestra organización y que esta herramienta es la primea defensa que podamos contar para contener las amenazas existentes en la red.

Servidor proxy: estos servidores son categorizados como una muy buena herramienta de contención y bloqueo de amenazas cibernéticas, ya que se pueden bloquear sitios web catalogados como peligrosos p prohibidos dentro del ambiente laboral. También permite establecer un sistema de autentificación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

2.20 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Lo mas importante en las estrategias de seguridad informática es estar al tanto de formas o tipos de ataques más recientes ya que con ellos se puede conocer estas modalidades e implementar las formas de detección, contención y erradicación dentro de nuestros medios digitales.

La mayoría de los ataques lo realizan a organizaciones de las cuales pueden obtener grandes cantidades de dinero, siendo este el objetivo mas usado por los delincuentes o dependiendo el fin de este, es decir, ataques a espacios pequeños como el de un hogar, no les seria muy productivo, sin embargo, usan modalidades en combinación con la ingeniería social de la cual lanzan como una red y esperan a ver quien puede caer en ella.

La mejor forma de desarrollo de los equipos red and blue es estar actualizados con todos los temas de ciberseguridad y forma de ataques nuevos de los cuales pueden tomar como base para poder mejorar sus prácticas e implementar dentro e sus auditorias que realizan, así logran fortalecer de mejor manera los sistemas informáticos que estén analizando y estén preparados para todo tipo de ataque.

3 CONCLUSIONES

En conclusión, para el despliegue de estrategias en RedTeam & BlueTeam es conocer la seguridad informática en la organización como fundamento para conservar la confidencialidad de los datos personales. Con el anterior informe técnico se logra la identificación del alcance que como profesionales en la seguridad y con los marcos éticos y legales nos ayudan s proceder ante situación de ataques cibernéticos.

Las pruebas simuladas en el banco de trabajo logran demostrar que las vulnerabilidades en los sistemas informáticos van a existir y ahí es donde el delincuente puede hallarla y explotarla según su objetivo de ataque. Por ende es necesaria hacer el uso de elementos para el escaneo y detección de intrusos en nuestros espacios digitales para prevenir cualquier tipo de ataque.

Hacer un buen uso de los conocimientos para robustecer nuestros sistemas informáticos es una de las mejores estrategias a implementar y realzar las pruebas de los equipos red and Blue como teste de penetración, son las formas mas efectivas en fortalecer nuestra seguridad.

Nos ha quedado claro que la seguridad informática no es solo la seguridad que nos brinda un antivirus instalada en algún dispositivo, sino es la forma de como actuamos ante una sospecha de brecha de seguridad. Cuando navegamos en paginas no seguras, desconocidas, descargamos contenido de estas páginas, abrimos correos electrónicos con archivos o enlaces sospechoso o activamos servicios por los puertos de nuestros dispositivos son falencias que solo nosotros podemos crear, es decir, si hay un ataque cibernético, es por causa de un fallo humano en la implementación de estas medidas y el control del manejo de la información de forma interna.

Todo puede ser seguro si actuamos de forma correcta y hacemos caso a los expertos en seguridad, expertos de confianza y con grandes capacidades.

4. RECOMENDACIONES

La seguridad informática es un tema que esta tomando fuerza con los avances tecnológicos, pero en términos generales, esta depende bastante de las decisiones que tome el equipo humano, es decir, dentro de una organización, la seguridad informática va a depender del personal de seguridad y de sus capacidades técnicas para detectar, contener y erradicar un ataque cibernético.

La mejor recomendación para temas de seguridad informática y que contribuyen a la mejora de las técnicas para RedTeam & BlueTeam es contar con personal especializado para realizar las actuaciones de los mismos, la instalación de los nuevos dispositivos de hardware, si se contrata servicios de terceros, que sean empresas comprometidas y de confianza y que si se ha de realizar algún contrato, sea de forma personal y si se va dedicar empleados para la seguridad informática, que su selección sea en función a lo que se desea cuidar, es decir, si hablamos de servidores que manejan grandes cantidades de datos, contar con personal que se especializa en dicho tema, pero si es por seguridad perimetral y datos pocos pero de alta confidencialidad, también personal específico para este tema.

La seguridad informática esta tomando fuerza con distintas metodologías, técnicas y elementos para ser implementada, así que, para optar con la mejor decisión, se debe contar con personal especializado para la valoración y en función de mi espacio digital ellos informaran que tipo de seguridad necesita y el perfil del personal apto para esta.

Otras recomendaciones no tan generales, pero que pueden ayudar a robustecer la seguridad es:

a) Tener cuidado con lo que se publica en redes sociales.
b) Mantener control sobre las configuraciones de privacidad. En lo posible mantenerlas activas.
c) Navegar en páginas segura, de confianza y capacitar de esta estrategia a todos los empleados.
d) Mantener la a la red en modo protegido, en los firewalls se puede encontrar esta opción.
e) Mantener especial cuidado con las descargas de la red externa.
f) Creación y cambio periódico de contraseñas y que estas sean robustas, es decir, mínimo 8 caracteres alfanuméricas entre minúsculas y mayúsculas con signos especiales.
g) Adquirir software legal y mantenerlo actualizado, en especial los antivirus

h) No cargar y transportar información por memorias USB o Pendrives en ambientes públicos (mejor usar en ambientes privados).
i) Tener cuidado con los enlaces y archivos que llegan a los correos electrónicos, en caso de dudas, consultar con un experto.
j) Especial atención cuando se va a usar servicios de proxy o redes inalámbricas públicas. Estas normalmente están usadas por hackers para robar información a quien se conecta.
k) Si se dese enviar información por medio de la internet y es confidencial. Se recomienda encriptar la información y colocar claves de seguridad o contraseñas robustas como se mención en el punto f.[8]

[8] UNCUYO. Tips De Ciberseguridad. [Sitio Web]. [Consultado: 01 de abril de 2023]. Disponible en: https://www.uncuyo.edu.ar/desarrollo/siete-tips-para-mantener-la-seguridad-informatica-y-evitar-el-robo-de-informacion

BIBLIOGRAFÍA

BLOG.HACKER. Framework Post Explotación Powershell-Empire. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://blog.elhacker.net/2021/12/framework-powershell-empire-post-explotacion-pentesting.html

CISET. Que Es El Hardening Informático. [Sitio Web]. [Consultado: 24 de marzo de 2023]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

COLOMBIA. LEY 1273 DE 2009. De La Protección De La Información Y De Los Datos. (05 de enero de 2009). de la protección de la información y de los datos En: Diario Oficial. enero, 2009. Nro. 47223. p. 1-5

COLOMBIA. LEY ESTATUTARIA 1581 DE 2012. Protección De Datos Personales. (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En: Diario Oficial. octubre, 2012. Nro. 47223. p. 1-11

ENTER.CO. Detrás De Buggly: La Historia De La Fachada Andrómeda. [Sitio Web]. [Consultado: 23 de febrero de 2023]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

GAVIRIA, RAÚL. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

GREENBONE. Openvass. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.mancomun.gal/wp-content/uploads/2022/02/vulners_openvas_vulnerabilities_logo-800x576.png

MANAGENGINE. ¿Qué Son Y Cómo Implementar Los Controles De Cis (Cis Controls)?. [Sitio Web]. [Consultado: 26 de marzo de 2023]. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

MICROSOFT. ¿Qué Es Siem?. [Sitio Web]. [Consultado: 26 de marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

REDESZONE. Faraday, Una Completa Plataforma De Pentest Y Análisis De Vulnerabilidades. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en:

https://www.redeszone.net/app/uploads-redeszone.net/2016/07/Faraday-655x333.png

TENABLE. Nessus. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.tenable.com/sites/all/themes/tenablefourteen/img/nessus/nessus-live-results_large.png

REVISTA SEGURIDAD. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

SIGNIFICADOS. Qué Son Los Delitos Informáticos. [Sitio Web]. [Consultado: 11 de febrero de 2023]. Disponible en: https://www.significados.com/delitos-informaticos/

UNCUYO. Tips De Ciberseguridad. [Sitio Web]. [Consultado: 01 de abril de 2023]. Disponible en: https://www.uncuyo.edu.ar/desarrollo/siete-tips-para-mantener-la-seguridad-informatica-y-evitar-el-robo-de-informacion