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

HECTOR PERDOMO ANDRADE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

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

HECTOR PERDOMO ANDRADE

JOHN FREDDY QUINTERO
Tutor(a) o director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

CONTENIDO

pág.

TABLA DE IMÁGENES

GLOSARIO

Activos: un activo es un bien con el cual la organización cuenta, puede ser información o equipos que representa valor monetario o liquides.

Amenazas: es la causa potencial que se pueda materializar un incidente no deseado, que pueda generar daños a un activo de la organización. (ISO/IEC 27000)

Botnet: es un programa maligno diseñado para levantar puertas traseras y así poder seguir teniendo control de equipos en las organizaciones atacadas, tienen capacidad de seguir su propagación dentro de las redes internas desplegando otros malware.

Herramientas: es la serie de mecanismos que utilizan las organizaciones para proteger los activos de información, pueden ser de tipo lógico o físicos.

Malware: es todo el código que se comporte de manera sospechosa puede llegar a dañar el sistema operativo, información, etc. Tiene diferentes categorías según su código fuente pueden ser Troyanos, Gusanos, Spyware, Botnets, etc.

Ramsomware: Es un software malicioso que al infectar los sistemas informáticos realiza un encriptado de la información y borrador de los archivos originales, para posterior pedir un rescate normalmente en criptomonedas.

Riesgo: es la posibilidad que ocurra un evento de seguridad el cual puede una pérdida o daño en un activo de información. Se considera la probabilidad que se pueda materializar. (ISO/IEC 27000).

Seguridad De La Información: es la capacidad que una organización tiene para la preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000)

Spyware: El Spyware o programas espías se utilizan para reunir información concreta sobre los datos existentes y los sistemas del dispositivo. Esto permite supervisar la actividad de una persona en Internet y luego distribuir la información a los posibles ciberdelincuentes. Esto incluye, por ejemplo, opciones de acceso, información de pago, información de tarjetas de crédito e identidades.

Vulnerabilidad: es la debilidad que puede tener un sistema informático, la cual puede llegar a realizarse una explotación y poner en riesgo los activos de las organizaciones.

Red Team: “emulan a los atacantes, utilizando sus mismas herramientas o similares, explotando las vulnerabilidades de seguridad de los sistemas y/o aplicaciones (exploits), técnicas de pivoting (saltar de una máquina a otra) y objetivos (sistemas y/o aplicaciones) de la organización.”[1]

Red Blue: “es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva, realizan una vigilancia constante, analizando patrones y comportamientos que se salen de lo común tanto a nivel de sistemas y aplicaciones como de las personas, en lo relativo a la seguridad de la información.”[2]

[1] UNIR, Red team, Blue team y Purple team, ¿sabes qué son y cómo ayudan a mejorar la seguridad informática? En UNIR abordamos sus funciones y objetivos. [Sitio Web] [Consultado 27 de abril del 2023] Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

INTRODUCCIÓN

Este informe pretende demostrar todas las activades del seminario de profundización de equipos estratégicos en ciberseguridad, donde se realizarán laboratorios controlados para demostrar las actividades que comprenden la ejecución de los procesos que normalmente realizan los equipos Red Team y blue Team, para entender sus aportes de conocimiento con sus capacidades y alcances dentro de las organizaciones que los implementan.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

- Realizar la construcción del informe técnico sobre equipos Red Team y Blue Team.

1.2 OBJETIVOS ESPECÍFICOS

- Describir los aspectos importantes de las estrategias Red Team y Blue Team.
- Crear recomendaciones que aporten valor al endurecimiento de la ciberseguridad de la organización.
- Sustentar con evidencia de video el desarrollo del seminario de profundización.

2 DESARROLLO DEL TRABAJO

2.1 ACTUACIÓN ÉTICA Y LEGAL

2.1.1 ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

La empresa WhiteHouse Security no cuenta con una medida de seguridad suficientemente para el ingreso de personal acorde a los estándares que se requieren para prestar estos servicios, ya que hace unas recomendaciones mínimas, realizar un contrato que se no encuentra acorde a las funciones que desempeñara cada persona contratada, adicional tiene un modelo de contrato deficiente creado por una persona que ya no labora en la compañía.

Considero que no es oportuno dar acceso a la información de una empresa en un proceso selección, porque puede presentarse una fuga de información que puede ser aprovechada ya que no hay ningún soporte legal de confidencialidad con un aspirante en estos casos, puede existir una perdida reputacional con los clientes de WhiteHouse Security.

En la Primera cláusula, esta realizar una obligación a si se identifique que pueda estar llevándose un proceso ilegal, el cual nos puede generar muchos problemas, ya que podemos ser considerados como cómplices. “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” esto tiene algunas obligaciones a participar en actos fuera de las leyes.
En la Cuarta clausula el Ítem 3 menciona lo siguiente: “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros” esta cláusula permite que como profesionales seamos cómplices ya que se puede tomar cualquier abuso a la

información personal o gubernamental estamos obligados a no tomar acciones como instaurar una denuncia.
En el Ítem 4 menciona lo siguiente: “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas”. Lo cual indica que no se puede realizar ninguna denuncia de un acto ilegal que pueda estar realizando la empresa Whitehouse Security porque prima la lealtad así se estén realizando actos que puedan ser considerados delictivos en la legislación colombiana.
En el Ítem 7 menciona lo siguiente: “Responder por el mal uso que le den sus representantes a la información confidencial”, esto hace alusión que todas las acciones que puedan incurrir en delitos hechos por las personas de la alta gerencia de la empresa Whitehouse Security tendremos que responder o ser los directos responsables de estos actos ilegales.
En el Ítem 8 menciona lo siguiente: “Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento”. Si témenos cualquier información obtenida de forma ilegal y el profesional tiene que hacerse responsable ante las autoridades por los delitos que se realicen desde la empresa.

En la Octava clausula, menciona lo siguiente: “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”. Esta busca realizar una mediación entre la organización y el estudiante, pero a su vez indica que, si se llega a comprometer información que este bajo custodia del estudiante este debe exonerar a la empresa, lo cual es una forma de librar responsabilidades ya que ellos emitirían un orden de realizar cualquier procedimiento fuera de la legalidad en la legislación colombiana.

Realizando un análisis de la información del documento se identifica que lo mas seguro es que sobre este acuerdo se esté violando los artículos de la 1273 de 2009.

Artículo 269A Acceso abusivo a un sistema informático.
Artículo 269C Interceptación de datos informáticos.
Artículo 269E Uso de software malicioso.
Artículo 269F Violación de datos personales.
Artículo 269G Suplantación de sitios web para capturar datos personales.
Artículo 269H Circunstancias de agravación punitiva.
Artículo 269I Hurto por medios informáticos.
Artículo 269J Transferencia no consentida de activos.

2.1.2 ¿Existiendo procesos poco confiables en el anexo 3 – acuerdo? Usted como experto en ciberseguridad aplicaría a este trabajo en the whitehouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

La empresa Whitehouse Security ofrece un salario bastante atractivo para desempeñar estas funciones lo cual me hace analizar e identificar todos los alcances que requieren, estar fuera de los códigos de ética de mi profesión y peor a un violando mis convicciones morales para poder obtener un salario, lo cual no estoy interesado en realizar, en el artículo 34 de código de ética de la COPNIA, menciona las prohibiciones especiales a los profesionales respecto a la sociedad y en este articulo existe el parágrafo (a) el cual dice lo siguiente: “Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”[3] Identificar este tipo de cláusulas que pueden generar incluso la perdida de mi tarjeta profesional, me encontraría en la obligación de desistir de cualquier proceso impropia a mi ética profesional.

2.1.3 Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

La operación Andrómeda fue una operación coordinada por las fuerzas militares todo con el fin de obtener información sobre un proceso de paz que se iba a dar con el gobierno nacional y grupos ilegales, con la misión de buscar información declararon algunos objetivos que serían intervenidos, pero por algunas razones no realizaron suficiente control sobre el personal que está realizando las actividades se cometieron actos delictivos violando las leyes colombianas un informe presentado por las fuerzas militares indican: “se encontraron fallas de seguridad que evidenciaron indisciplina y falta de control del personal que visitaba la dependencia. No se tenía control sobre las actividades realizadas por el personal militar y civil ajeno a la Operación Andrómeda. Muchas de ellas que ingresaban, tenían un alto conocimiento y capacidades a nivel informático, sin embargo, trabajaban sin supervisión alguna” lo cual deja en evidencia las circunstancias de poca ética y abrochamientos de los recursos tecnológicos y alto conocimiento de ciertas personas que fueron implicadas en la violación de sistemas de información, logrando adquirir mucha información de personas que fueron declarados objetivos para interceptar, manipular y tener todo tipo de información que pudiese

[3] COPNIA, código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Sitio Web]. [Consultado el 20 de febrero de 2023]. Recuperado de: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

involucrarlos de alguna manera “Chuzadas”[4], todo dirigido y articulado por personal militar dirigidos por políticos de altos cargos en el gobierno.
Esta operación genero una alerta a todas las entidades de inteligencia y ministerios ya que se aprovecharon ciertos vacíos para vulnerar derechos de algunas personas influyentes en la política de Colombia.

2.2 **EJECUCIÓN PRUEBAS DE INTRUSIÓN**

2.2.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

Kali Linux “(anteriormente conocido como BackTrack Linux) es una distribución de Linux basada en Debian de código abierto destinada a pruebas de penetración avanzadas y auditorías de seguridad. Kali Linux contiene varios cientos de herramientas destinadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Kali Linux es una solución multiplataforma, accesible y disponible gratuitamente para profesionales y aficionados a la seguridad de la información.”[5]

Nmap “(“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" se pueden ejecutar diferentes tipos de escaneo TCP, UDP, ICMP, tiene capacidad de escanear las redes de manera oculta la cual genera dificultades para que un firewall pueda identificar un ataque.”[6]

Esta herramienta cuenta con un sin número de comandos y script que se pueden utilizar, con el fin de identificar todos los hosts sobre una red corporativa, incluso tiene la capacidad de realizar análisis sobre la red de internet, se puede identificar si tiene un firewall realizando filtrado de paquetes o que puertos se encuentran abiertos para explotar vulnerabilidades, se puede realizar un escaneo incluso sobre direccionamiento de IPV6.

---

[4] SEMANA, El informe que sacudió el caso de la fachada Andrómeda [Sitio Web]. [Consultado el 18 de febrero de 2023]. Recuperado de: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

[5] KALI. [Sitio Web]. Kali Linux2 [Consultado 8 de marzo 2023] Disponible en: https://www.kali.org/docs/introduction/kali-linux-history/

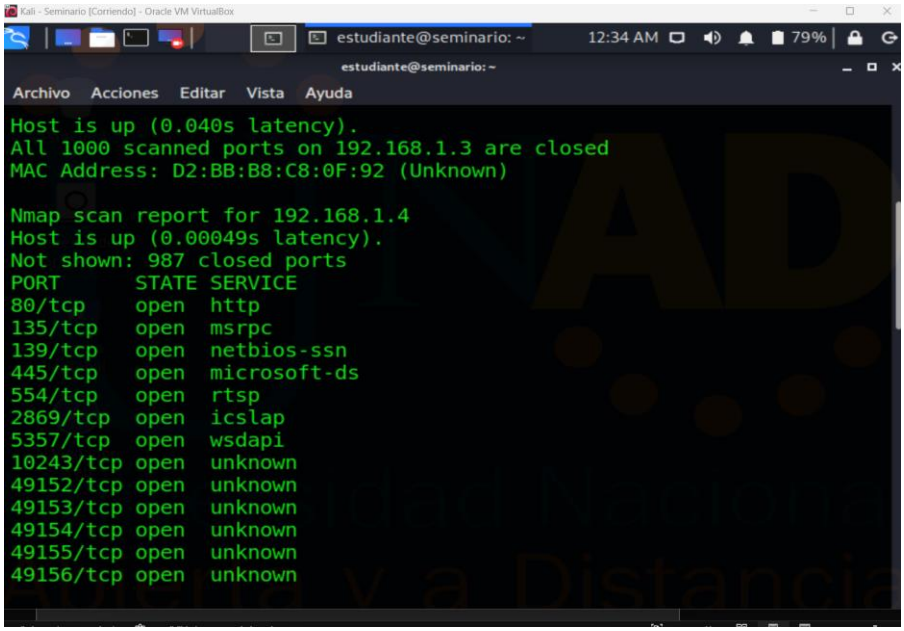
[6] NMAP, Documentation [Sitio Web]. Kali Linux2 [Consultado 8 de marzo 2023] Disponible en: https://nmap.org/docs.html

Mestaspolit Proyecto de código abierto y gratuito el cual realiza un reconocimiento de las posibles debilidades de seguridad que puede tener un sistema de información tiene alcance de explotación de vulnerabilidades con el fin de crear evidencias de penetración para implementar un modelo de protección. Se puede integrar con otras herramientas como Nessus y NMAP.

Nota: para iniciar la actividad se debió instalar la aplicación Rejetto 2.3 y bajar los servicios de firewall en la maquina Windows 7 X64

2.2.1.1 Se realiza un análisis sobre la red escaneando con herramienta NMAP para identificar los equipos que se encuentren en la red identificando los servicios, “nmap 192.168.1.0/24”

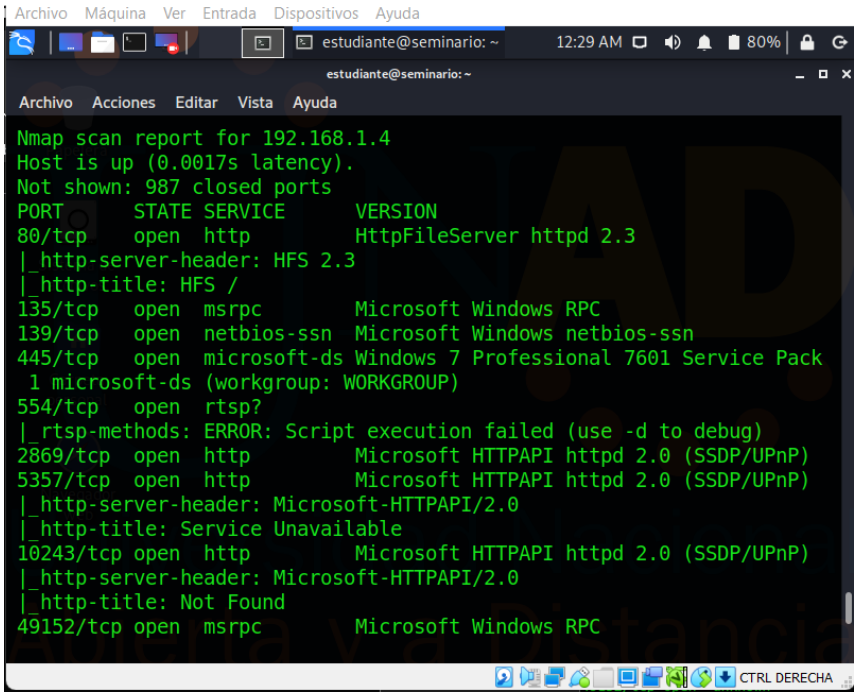
Ilustración 1 escaneo de la red con NMAP



Fuente: “Elaboración Propia”

2.2.1.2 Se realiza un escaneo de puertos sobre la maquina identificada para saber cuáles esta abiertos y poder identificar cada uno de los servicios que se puedan comprometer.

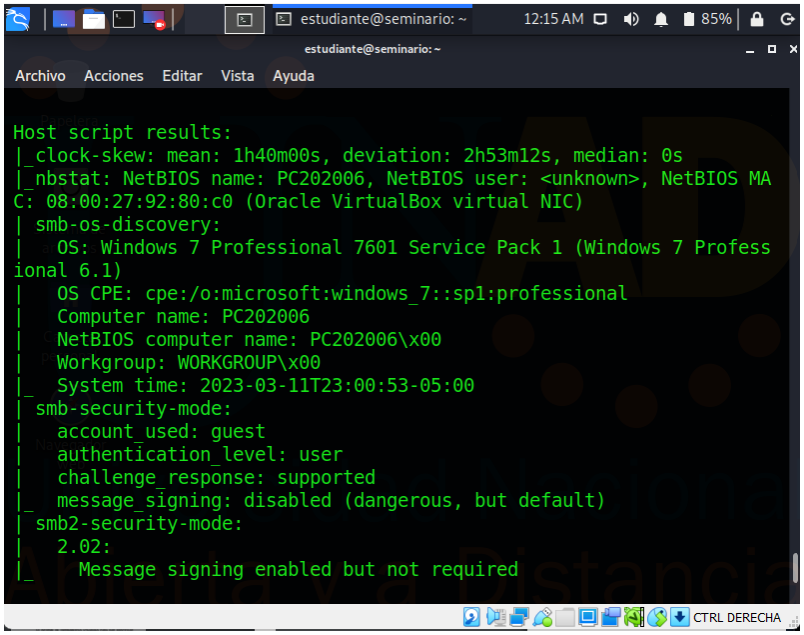
Ilustración 2 Escaneo de servicios expuestos.



Fuente: “Elaboración Propia”

2.2.1.3 Se identifica el equipo con la dirección IP 192.168.1.4 la cual tiene un sistema operativo Windows 7 X64.

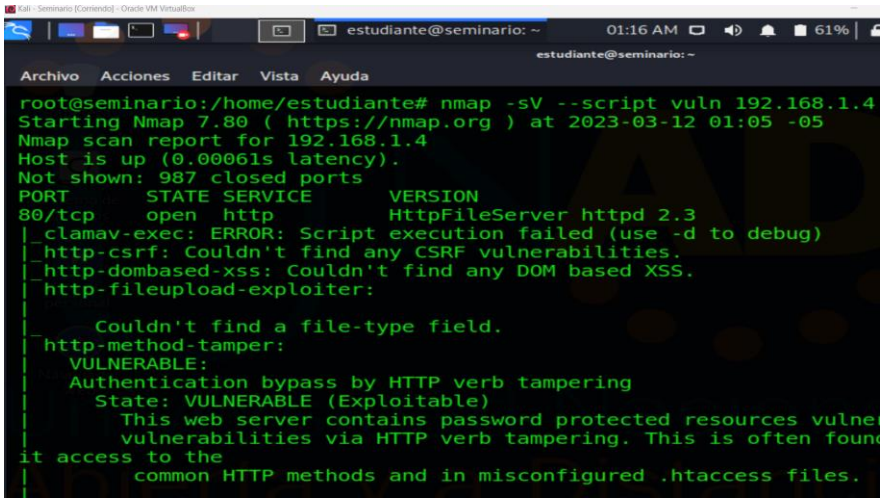
Ilustración 3 Identificación de sistema operativo



Fuente: “Elaboración Propia”

2.2.1.4 Se realiza escaneo de vulnerabilidades con NMAP a la dirección IP 192.168.1.4 y se identifica el servicio que se encuentra expuesto por el puerto 80 el cual es HttpFileServer httpd v. 2.3 el cual tiene vulnerabilidad identificada, el cual es rejjeto. “nmap -sV –script vuln 192.168.1.4”

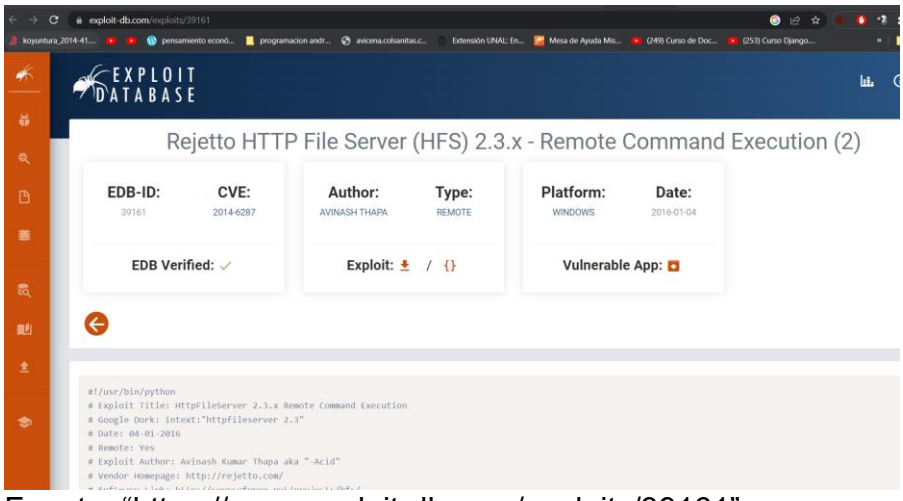
Ilustración 4 Vulnerabilidad identificada



Fuente: “Elaboración Propia”

2.2.1.5 Realizamos búsqueda en internet sobre la vulnerabilidad e identificamos bastante información.

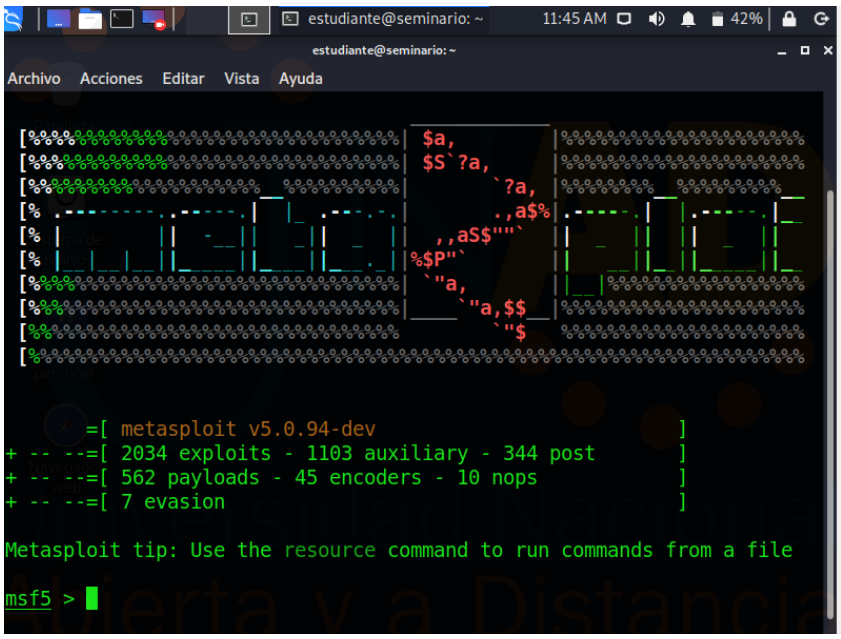
Ilustración 5 Descripción de la vulnerabilidad y exploit.



Fuente: “https://www.exploit-db.com/exploits/39161”

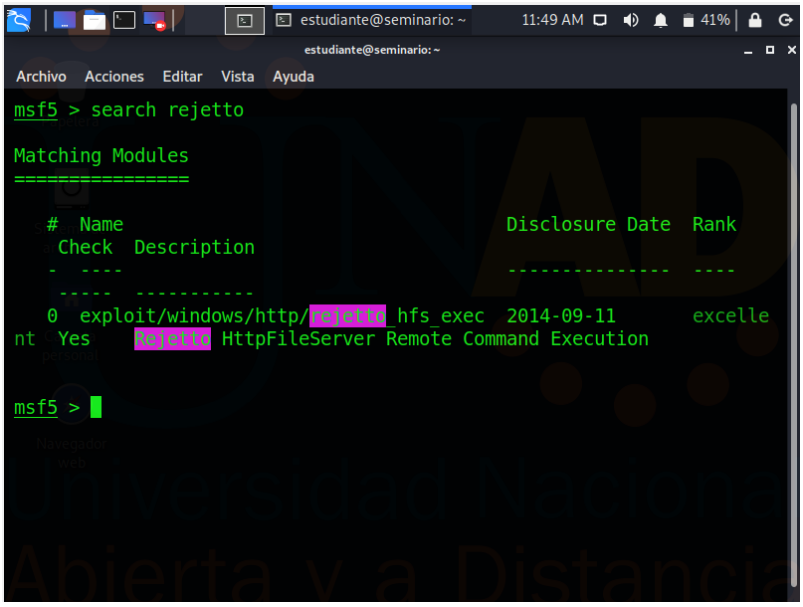
2.2.1.6 Procedemos a iniciar la consola de metaxploit, luego procedemos a realizar la búsqueda del exploit que se requiere para acceder al sistema.

Ilustración 6 Consola de metaxploit



Fuente: “Elaboración Propia”

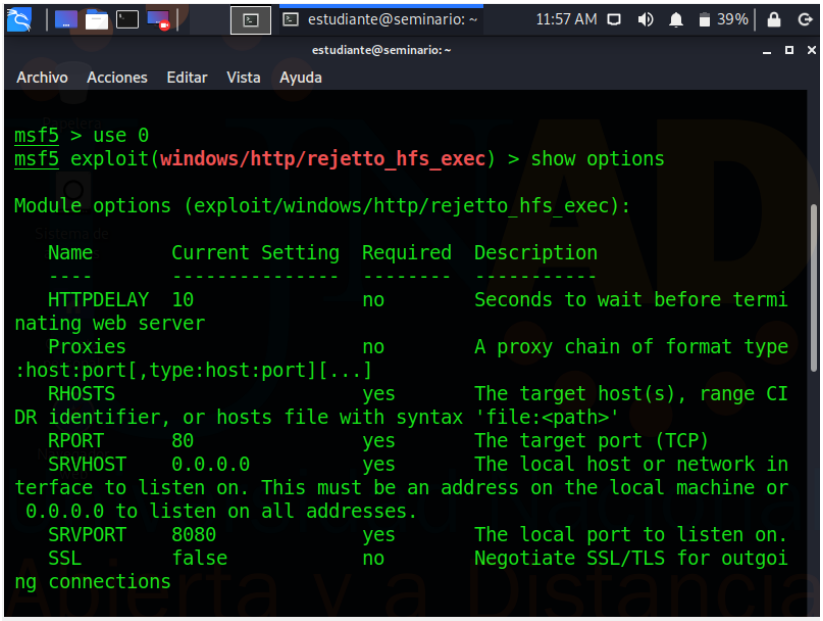
Ilustración 7 Búsqueda del Xploit.



Fuente: “Elaboración Propia”

2.2.1.7 Procedemos a realizar el uso del xploit para intentar iniciar en una sesión en el Windows con una sesión de manera arbitraria.

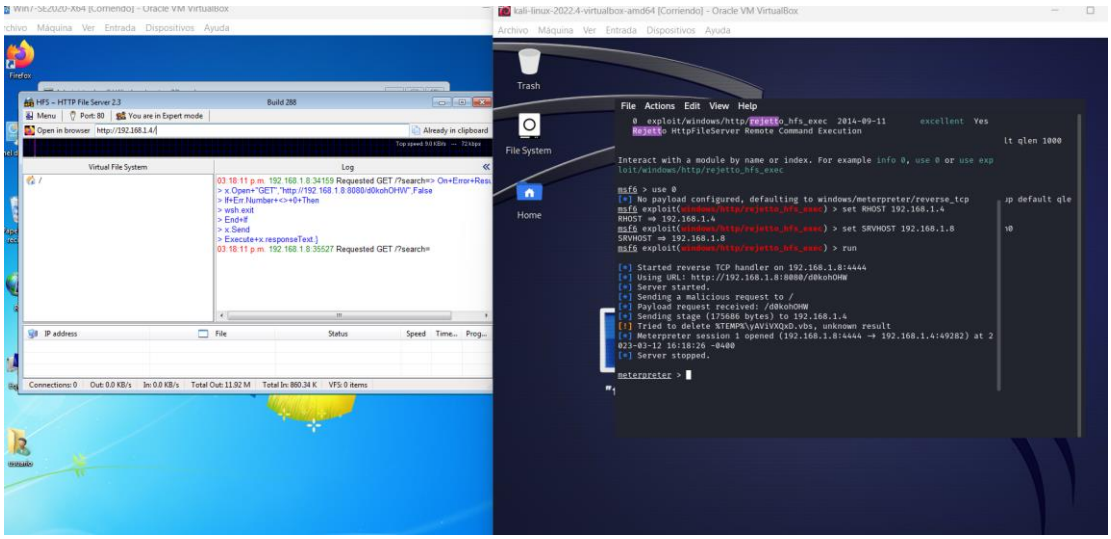
Ilustración 8 Opciones para usar xploit



Fuente: “Elaboración Propia”

Se realiza la explotación, se presentó errores con la maquina proporcionada por la UNAD para el laboratorio y fue necesario descargar una versión de Kali. Donde podemos identificar que fue efectiva.

Ilustración 9 Intrusión arbitraria al equipo Windows.



Fuente: “Elaboración Propia”

2.2.2 A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64."

Anexo 4 "La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos."

La información "tiene instalada una aplicación llamada Rejetto v. 2.3 bajo un Windows 7 con arquitectura X64" es importante para el análisis ya que se identifica donde se pudo haber generado la explotación y el sistema operativo donde estaba implementada la aplicación.

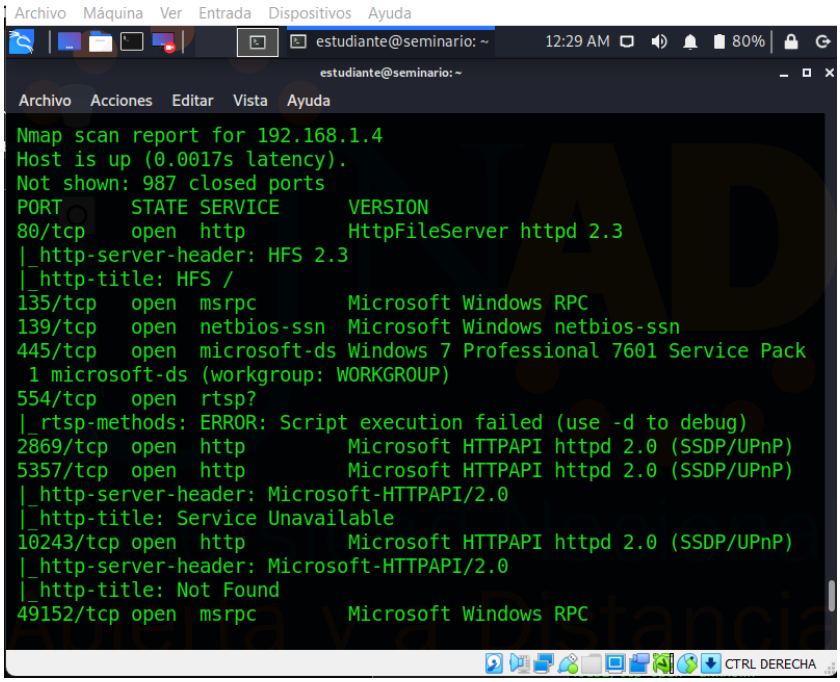
La información "exploit que puede terminar en una Shell reversa" también nos brinda información sobre el mecanismo el cual podemos considerar una aplicación de explotación como meterpreter.

La información "escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema" también nos brinda que se forzaron los privilegios del usuario mediante un mecanismo de engaño al sistema, para permitir la creación de un usuario.

2.2.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"? ¿Qué puerto abre la aplicación específica en el anexo?

Con la herramienta NMAP realizamos un escaneo de la red y los puertos abiertos, de esta manera identificamos que tiene el puerto 80 abierto como se evidencia.

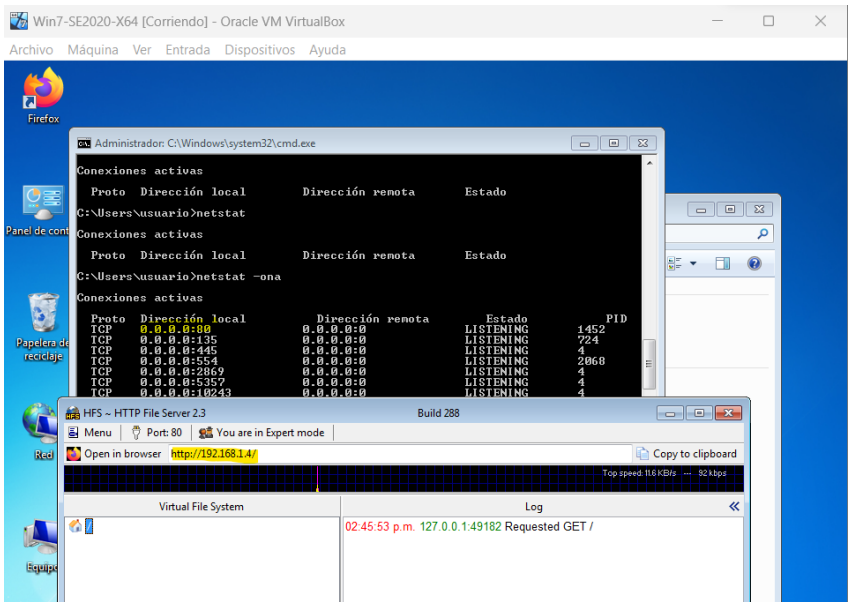
Ilustración 10 Identificación de puertos abiertos.



Fuente: “Elaboración Propia”

En el equipo con Windows 7 X64 se están ejecutando servicios los cuales están en estado listening a través del puerto 80 el cual se permite desde cualquier dirección que este en la red.

Ilustración 11 Puertos abiertos en el Windows



Fuente: “Elaboración Propia”

2.2.4 Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

La máquina puede ser afectada ya que, a través de una conexión arbitraria ejecutada por la vulnerabilidad identificada, se pueden llegar a tener varias complicaciones, porque esta infiltración genero un comprometimiento de toda la información que se encuentra en esta máquina, adicional puede estar comprometida parte de la infraestructura, ya que se pueden realizar escanear de las redes que existan más servicios e información que se pueda interceptar o robar.

Los atacantes por lo general definen su objetivo por cualquier motivo sea político, económico, etc.
Posterior a eso inician buscando información identificando los activos, usuarios, buscando cualquier cosa que puedan aprovechar para llegar sus objetivos.

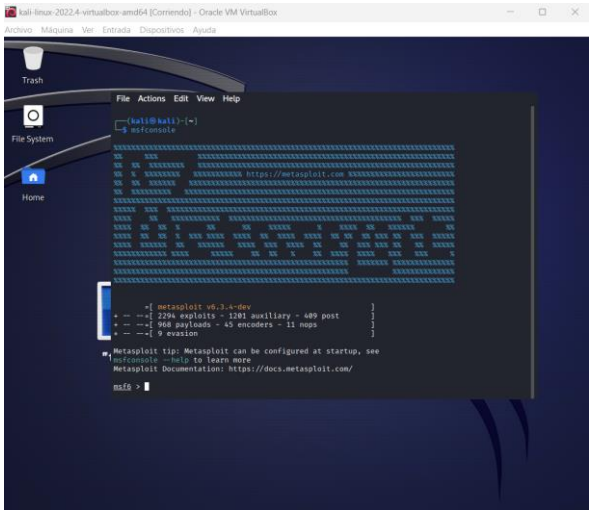
Ilustración 12 Como funciona un ataque

Fuente: “https://geekflare.com/es/web-penetration-testing-tools/ "

2.2.4.1 Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.”

2.2.4.1.1 Inicializamos la consola de metaxploit, para poder realizar la búsqueda de los scripts para iniciar cualquier posible explotación.

Ilustración 13 Inicio de consola,

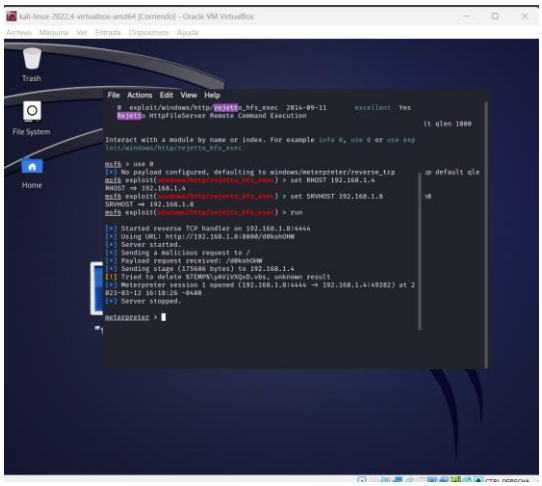


Fuente: “Elaboración Propia”

2.2.4.2 Se ejecuto un exploit a través de la consola de metaxploit “exploit/windows/http/rejetto_hfs_exec” el cual crea una conexión de manera arbitraria y ejecuta un Shell inversa de meterpreter para tomar control de la máquina.

Para ejecutar solo debemos setear dos parámetros para poder iniciar el ataque que son:
Set RHOST <IP remota>
Set SRVHOST <IP local de atacante>

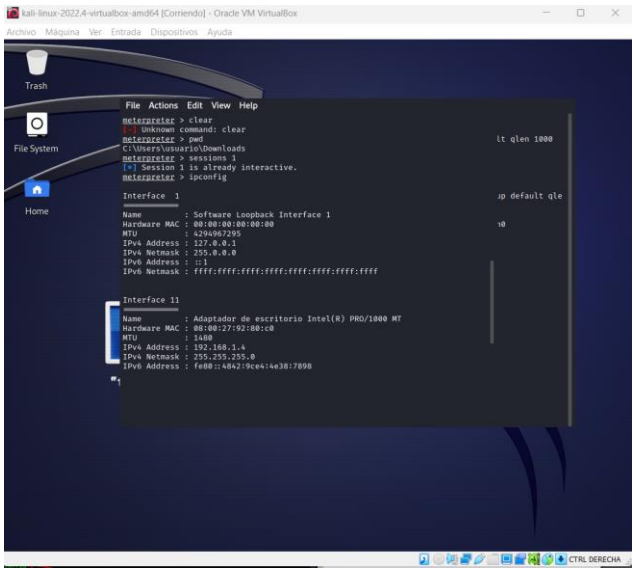
Ilustración 14 Explotación de vulnerabilidad.



Fuente: “Elaboración Propia”

2.2.4.3 Posterior a esta conexión iniciamos la sesión, se realiza la prueba de comandos sobre la terminal, como sesión, ipconfig la cual nos trae información que ya en otras Ilustraciones hemos identificado, etc.

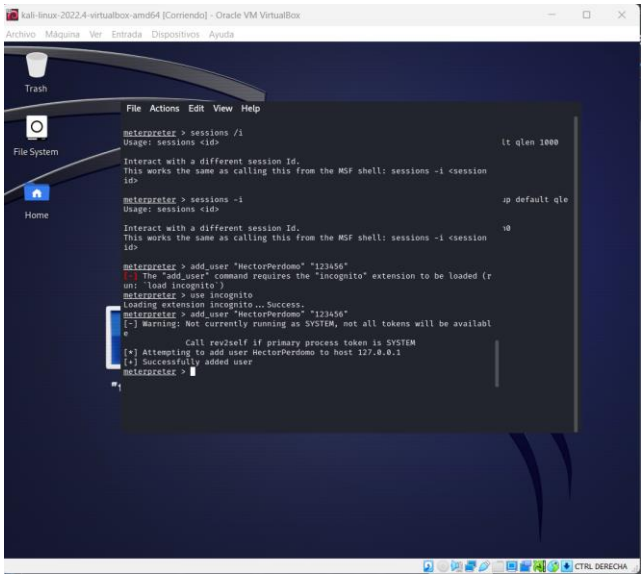
Ilustración 15 Prueba de comandos



Fuente: “Elaboración Propia”

2.2.4.4 Se procede a realizar la creación de un usuario para dejar la evidencia que si se pudo realizar la instrucción a la máquina.

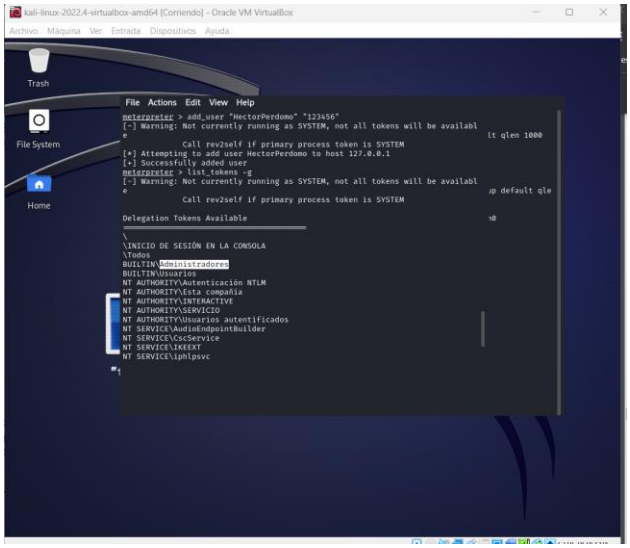
Ilustración 16 Creación de Usuario



Fuente: “Elaboración Propia”

2.2.4.5 Realizamos la lista de los grupos en el equipo para saber a cuál debemos asignar el usuario que creamos.

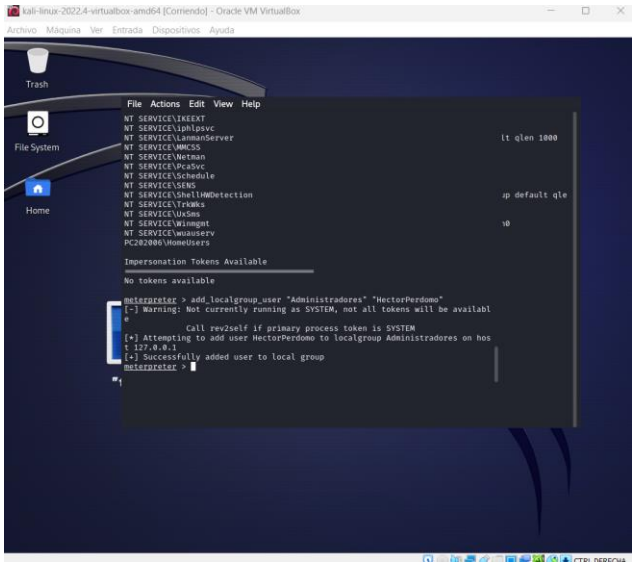
Ilustración 17 Listar grupos.



Fuente: “Elaboración Propia”

2.2.4.6 Asignamos el usuario al grupo de administradores de la máquina.

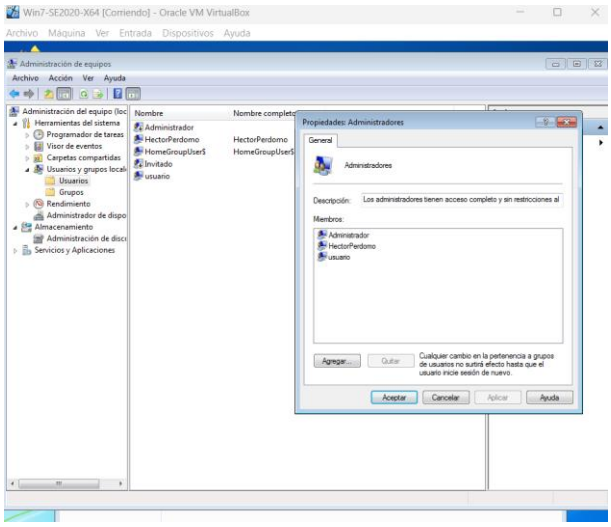
Ilustración 18 Asignación de grupo Administradores



Fuente: “Elaboración Propia”

2.2.4.7 Validación que el usuario aparezca creado en la maquina Windows para garantizar la efectividad del ataque.

Ilustración 19 Usuario creado de manera correcta.



Fuente: “Elaboración Propia”

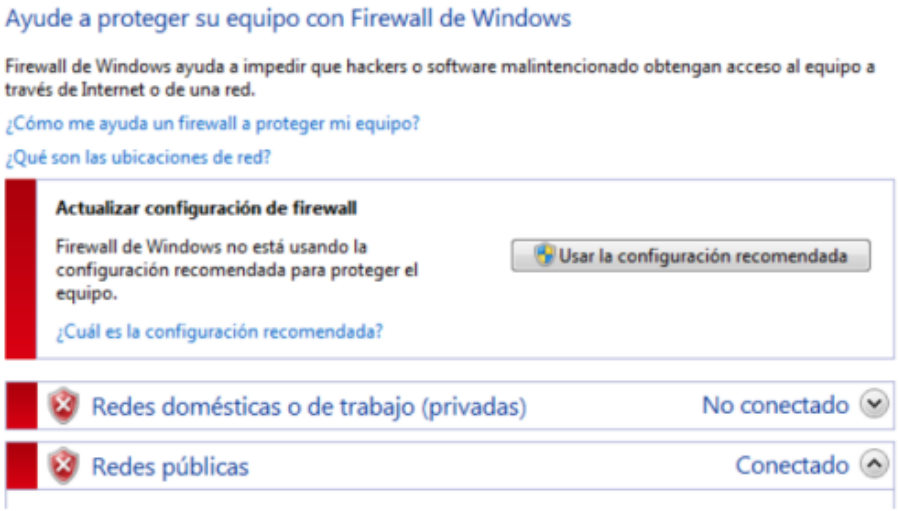
De esta manera podemos identificar los pasos que se ejecutaron para llevar a cabo el ataque que del cual se fue víctima por los delincuentes que se aprovecharon de una vulnerabilidad y lograron obtener todo el control de esta máquina Windows 7 X64.

2.3 CONTENCIÓN DE ATAQUES INFORMÁTICOS

2.3.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Lo primera identificación debe ser donde se identificó el ataque y que comportamiento está teniendo y cuáles son los posibles activos que están comprometidos e identificar que otros equipos puedan estar en la red.
Hacer un análisis del comportamiento del equipo Windows 7 x64, que puertos está utilizando, los destinos que está accediendo, verificación del firewall que se encuentre arriba, que tenga activo el Antivirus.

Ilustración 20 Firewall de Windows



Fuente: “Elaboración Propia”

Realizar la identificación de vulnerabilidades sobre los activos que se encuentran en la red de datos.

Descargar una herramienta que me pueda hacer análisis de tráfico sobre la red para identificar los comportamientos que se presentan, identificando todo lo anómalo que se pueda observar.

Para estos casos pueden ser herramientas como:

- Wireshark.
- Snort.
- Suricata.

Las dos primeras cuentas con inteligencia para detección de comportamientos anómalos sobre las redes de datos internas en las organizaciones, con identificación y análisis de posibles vectores de ataques.

Realizar la actualización de todos los parches de seguridad que se encuentren habilitados para instalación del sistema operativo y aplicaciones de terceros que puedan estar instaladas en el equipo Windows 7 x64.

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

Realizar actualización del sistema operativo ya que este se encuentra bastante vulnerable debido a que no cuenta con soporte directo de Microsoft.

Mantener actualizado con los parches de seguridad más recientes que se hayan liberado por parte del fabricante.

Tener una herramienta EDR para realizar contención de malware que se pueda instalar y ejecutar en el equipo.

Tener una herramienta de análisis de red para identificar cualquier comportamiento inusual hacia direcciones IP públicas.

Deshabilitar protocolos RPC para no permitir la ejecución remota de aplicaciones o programas.

Tener un sistema de respaldo sobre los datos que pueda contener un sistema de información, los cuales se debe garantizar que se encuentren cifrados.

Limitar los usuarios de las aplicaciones para que no tengan privilegios adicionales a los de poder ejecutar la aplicación para la cual fueron creados.

Aplicar políticas de entrada y salida por los puertos estrictamente necesarios en el firewall del equipo.

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

Los equipos Blue Team, están integrados por personas expertas en ciberseguridad, que tienen visión de la organización desde el interior al exterior con tareas específicas de protección de los activos de la organización, creando robustes en los controles que se puedan diseñar.
Evalúan los riesgos identificando las amenazas y debilidades que puedan tener los activos, identifican los riegos categorizándolos, para generar planes de acción y mitigación reduciendo el impacto y reducir la materialización.

Los equipos de respuestas a incidentes informáticos son los encargados de analizar todos los informes que generan las herramientas de seguridad para dar respuesta a las posibles vulnerabilidades que se identifiquen en los activos de información, amenazas que puedan surgir a través de la red, son integrados por especialistas en seguridad informática.

2.3.4 ¿Si dentro de un equipo blueteam le indican que debe trabajar con CIS “center for internet security” usted lo utilizaría para qué fin?

Los controles “se derivan de patrones de ataque generalizados. Específicamente, los informes de amenazas más confiables identifican patrones de ataque, que luego se examinan en una amplia comunidad de profesionales confiables de la industria y el gobierno que saben cómo funcionan los ataques. Estos expertos provienen de

una amplia gama de sectores, incluidos el comercio minorista, la fabricación, la atención médica, la educación, las agencias gubernamentales y la defensa."[7]

Son importante debido a su función de minimizar los riesgos a posibles ataques que puedan afectar la seguridad y custodia de los datos a los que puede estar expuestos una organización, buscan mitigar amenazas y son implementados por casi todos los marcos de ciberseguridad.

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

La definición de un SIEM (Security Information and Event Management), es una herramienta diseñada para hacer la correlación de eventos de ciberseguridad, su función principal es al analizar en tiempo real las fuentes que se integren como pueden ser Firewall, WAF, servidores, SW, entre otros.

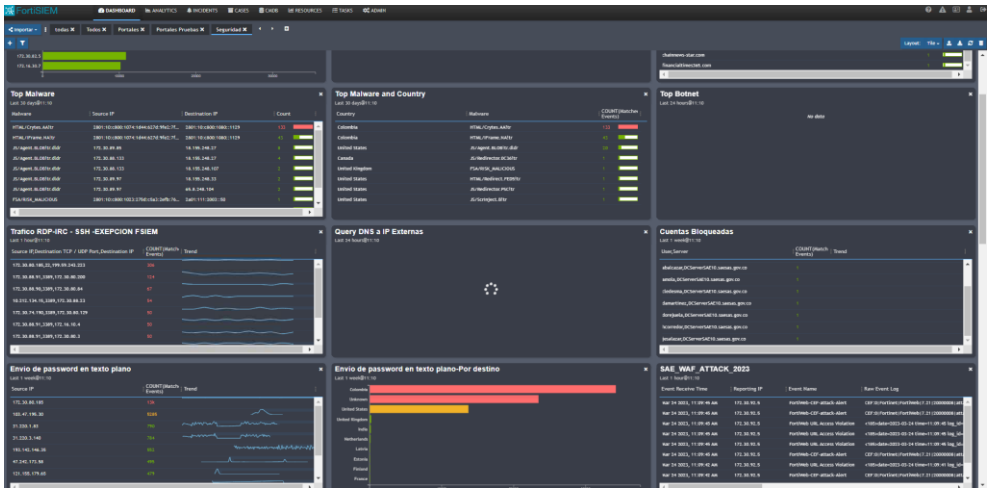
Se crean reglas de correlación y se analizan los eventos que se reporten según su criticidad, los cuales pueden generar una alerta en el sistema, programar un correo, una acción de contención, etc.

Podemos realizar muchas actividades con estos dispositivos como integración a los IoC para mejorar su respuesta, integraciones con SOAR para ejecutar acciones desencadenadas de contención a estos eventos críticos.

Se pueden tener reportes en tiempo real sobre lo que esta ocurriendo en las organizaciones parametrizados en DASHBOARD mostrando información de manera precisa.

[7] CIBERSEGURIDAD, GUÍA COMPLETA SOBRE CONTROLES DE SEGURIDAD CIS [Sitio Web] [Consultado marzo de 2023] Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

Ilustración 21 DashBoard Seguridad



Fuente: “Elaboración Propia”

2.3.6 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.

2.3.6.1 FIREWALL NGFW

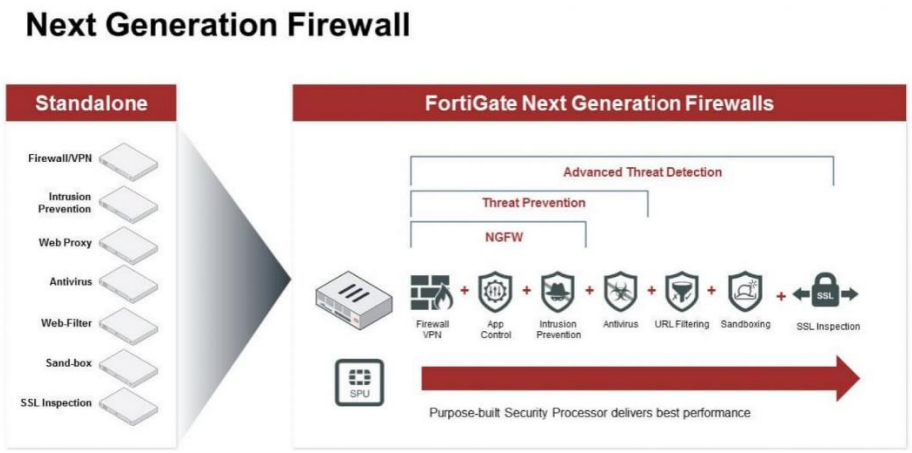
Son dispositivos de seguridad que permiten, tener el control sobre el tráfico de las redes internas de una organización logrando controlar todas las comunicaciones de los dispositivos internos hacia internet o internamente, permiten la creación de redes seguras y proporcionan una protección amplia, integrada y automatizada contra amenazas emergentes y sofisticadas.

Algunas de sus características principales son:

- Control de aplicaciones.
- Prevención de intrusiones.
- Antivirus.
- Filtrado de URL.
- Sandboxing.
- Inspección SSL.[8]

[8] QUANTI, Que es FortiGate: Conociendo el Firewall [Sitio Web] [Consultado marzo de 2023] Disponible en: https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/

Ilustración 22 Características Firewall NGFW



Fuente: “https://www.adaptixnetworks.com/firewalls-nueva-generacion/”

2.3.6.2 IDS SURICATA

Suricata es un motor de red de alto rendimiento IDS (Intrusion Detection System), IPS y seguridad de red, desarrollado por el OISF, “esta es una aplicación de código abierto multiplataforma y es propiedad de una fundación sin ánimo de lucro de la comunidad Open Information Security Foundation (OISF).”[9]

Está basado “en un conjunto de reglas desarrolladas externamente para supervisar el tráfico de la red y proporcionar alertas al administrador del sistema cuando se producen eventos sospechosos. Diseñada para ser compatible con los componentes de seguridad de red existentes, ofrece funcionalidad de salida unificada y opciones de biblioteca conectables para aceptar llamadas de otras aplicaciones. Como un motor de múltiples hilos, ofrece una mayor velocidad y eficiencia en el análisis de tráfico de red.”[10]

las características principales son:

[9] UBUNLOG, Suricata 4.0 detecta intrusos y supervisa el tráfico de la red [Sitio Web] [Consultado marzo de 2023] Disponible en: https://ubunlog.com/suricata-4-0-supervisa-el-trafico-de-la-red/

[10] RCSI, Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio [Sitio Web] [Consultado marzo de 2023] Disponible en: https://revistas.unsm.edu.pe/index.php/rcsi/article/view/363#:~:text=Se%20identific%C3%B3%20que%20Snort%20posee,evidenci%C3%B3%20mejores%20%C3%ADndices%20de%20efectividad.

- “Inspección del tráfico de red empleando tanto reglas configurables como reglas ya predefinidas para detectar amenazas y comportamientos sospechosos.
- Soporte para scripts en Lua para la detección de amenazas más complejas
- Integración con otras herramientas como Kibana, Elasticsearch, Splunk…
- Detección automática de protocolos
- Inspección y registro de peticiones de varios protocolos como HTTP, DNS, TSL/SSL…”[11]

Ilustración 23 Suricata

Fuente: “https://suricata.io/”

2.3.6.3 EDR Antivirus

Un sistema EDR “se caracteriza por aunar varios elementos de detección y de tecnologías, como, por ejemplo, la inteligencia artificial y el Big Data, que permiten mejorar de forma programada y autónoma la detección y prevención de amenazas complejas, así como su posterior eliminación o mitigación.”[12]

[11] MANCOMUN, Suricata [Sitio Web] [Consultado marzo de 2023] Disponible en: https://www.mancomun.gal/es/solucion-tic/suricata/

[12] INCIBE, Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa [Sitio Web] [Consultado marzo de 2023] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

2.4 **SOCIALIZACIÓN DE INFORME TÉCNICO**

2.4.1 Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

los aspectos importantes para definir las estrategias de ciberseguridad parten desde la necesidad que tienen las organizaciones para salvaguardar los activos de información, ya que se ha incrementado el número de ataques recibidos hacia la región de América y el caribe, con Brasil como país más atacado seguido de Colombia, México, Perú y chile.
Los ataques se realizan hoy en día tienen vectores de ataque (ATP) bastante sofisticados que para lograr identificarlos debemos tener muy buenos sistemas de contención y alertas puesto que podemos darnos cuenta cuando ya estén comprometidos los activos.
La construcción de estos equipos debe tener objetivos claros los temas que se abordarían en estas actividades, se debe garantizar la selección de los recursos humados que sean especialistas en este campo, las clausulas de los contratos deben ser analizadas para que se encuentren dentro de la legalidad de la legislación colombiana.
Basados en los códigos de ética que aplica en Colombia por la entidad competente como es la COPNIA para las ingenierías cumpliendo todos los artículos de deberes y obligaciones que se estipulan en el código de ética.

2.4.2 Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

Para mantener el cumplimento de los pilares fundamentales de la seguridad de la información confidencialidad, integridad y disponibilidad (CID) debemos realizar una identificación de los activos de información que tiene la organización para realizar los análisis a cuál pilar puede estar expuesto al riesgo.
Se debe analizar cuales serían los posibles vectores de ataque que puede recibir la organización y definir cuales son sus activos mas importantes para buscar los mecanismos de defensa para estos activos, existen varias herramientas que nos pueden ayudar a endurecer la seguridad en las entidades, como Firewall, Waf, IDS, que nos permiten tener un nivel de seguridad más alto.
Algunos de los ataques que más efectividad tienen a nivel mundial es mediante el engaño a los usuarios, para este tipo de vector las recomendaciones es la continua capacitación recurrente a los funcionarios de la organización, enseñando los métodos más comunes que utilizan los delincuentes, para que estén preparados cuando reciban información potencialmente peligrosa para ellos y la organización.

- Crear y mantener esquemas de backups de la información de los funcionarios y aplicaciones, en diferentes sistemas.

- Hacer una revisión de la procedencia de correo que se puedan recibir con documentos adjuntos que se desconozca el remitente o el fin del correo.
- Mantener los sistemas operativos actualizados de usuarios y servidores que tengan aplicaciones.
- Tener instalados sistemas de EDR para garantizar una mayor tasa de identificación de cualquier ataque.
- Tener un plan ante la posible materialización de un riesgo, como aislamiento de un end-point comprometido.

CONCLUSIONES

La identificación de las vulnerabilidades en los equipos o activos de información es de vital importancia debido a las implicaciones que puede llegar a tener comprometiendo los activos de información y deben ser manejar de acuerdo con su criticidad y tratadas de acuerdo con el grado que representen.

Al surgir la necesidad de estar interconectados y usar el servicio de internet casi que 7x24 para ofrecer servicios hacia los usuarios estando en casa ha hecho que también se generen brechas de inseguridad en las plataformas que son aprovechadas por delincuentes para sacar algún partido, es necesario estar realizando mejoras a los sistemas de información.

Los equipos Red Team y Blue Team, realizan grandes aportes a las organizaciones debido a sus funciones principales que son identificar cualquier vulnerabilidad que pueda presentar una organización y buscar a su vez la forma de dar solución mitigando las vulnerabilidades que se logren identificar.

BIBLIOGRAFÍA

CIBERSEGURIDAD, GUÍA COMPLETA SOBRE CONTROLES DE SEGURIDAD CIS [Sitio Web] [Consultado marzo 16 de 2023] Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

DIGI INTERNACIONAL [Sitio web]. Zigbee vs. Bluetooth: Cómo elegir el protocolo adecuado para su aplicación IoT [Consultado el 28 de septiembre de 2022]. Recuperado de https://es.digi.com/blog/post/zigbee-vs-bluetooth-choosing-the-right-protocol

EXPLOITDATABE, SEO Panel 4.6.0 - Remote Code Execution (2) [Sitio Web]. [Consultado 8 de marzo 2023] Disponible en: https://geekflare.com/es/web-penetration-testing-tools/

GEEKFLARE, 11 herramientas gratuitas de prueba de penetración en línea (Pentest) para probar la seguridad de la aplicación [Sitio Web]. [Consultado 8 de marzo 2023] Disponible en: https://intelequia.com/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

HANDBOOK, Red Team Roles [Sitio Web] [Consultado 27 de abril del 2023] Disponible en: https://handbook.gitlab.com/job-families/security/red-team/

INCIBE, Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa [Sitio Web] [Consultado marzo de 2023] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

INE, Understading Red Team Roles [Sitio Web] [Consultado 27 de abril del 2023] Disponible en: https://ine.com/blog/understanding-red-team-roles

INTELEQUIA, RED TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD [Sitio Web]. [Consultado 8 de marzo 2023] Disponible en: https://www.exploit-db.com/exploits/49525

MANCOMUN, Suricata [Sitio Web] [Consultado marzo 18 de 2023] Disponible en: https://www.mancomun.gal/es/solucion-tic/suricata/

PURPLESEC, Red Team VS Blue Team: What's The Difference? [Consultado marzo de 2023] Disponible en: https://purplesec.us/red-team-vs-blue-team-cyber-security/

QUANTI, Que es FortiGate: Conociendo el Firewall [Sitio Web] [Consultado marzo de 2023] Disponible en: https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/

RCSI, Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio [Sitio Web] [Consultado marzo 20 de 2023] Disponible en: https://revistas.unsm.edu.pe/index.php/rcsi/article/view/363#:~:text=Se%20identific%C3%B3%20que%20Snort%20posee,evidenci%C3%B3%20mejores%20%C3%ADndices%20de%20efectividad.

TECHTARGET, What is red teaming? [Sitio Web] [Consultado marzo 21 de 2023] Disponible en: https://www.techtarget.com/whatis/definition/red-teaming

UBUNLOG, Suricata 4.0 detecta intrusos y supervisa el tráfico de la red [Sitio Web] [Consultado marzo 21 de 2023] Disponible en: https://ubunlog.com/suricata-4-0-supervisa-el-trafico-de-la-red/

UNIR, Red team, Blue team y Purple team, ¿sabes qué son y cómo ayudan a mejorar la seguridad informática? En UNIR abordamos sus funciones y objetivos. [Sitio Web] [Consultado 27 de abril del 2023] Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/