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

RICARDO ALFONSO SANABRIA SILVA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

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

Ricardo Alfonso Sanabria Silva

Tutor
John Freddy Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

CONTENIDO

pág.

Tabla de figuras

pág.

GLOSARIO

Amenaza: incidente que se da producto de una explotación de una vulnerabilidad que pone en riesgo el sistema informático.

Antivirus: Software dedicado a la protección de equipos de cómputo centrando en el análisis y eliminación de virus, fortaleciendo la seguridad de los sistemas de información.

Ataque: Son intentos de exponer y violentar la seguridad de los sistemas de información donde se logra acceder y visualizar la información o dañar la misma.

Backup: copia o respaldo de seguridad de información o sistema de datos para prevenir perdida de la información.

BLUE TEAM: Seguridad defensiva que permite conservar la seguridad de la información de las organizaciones, conocido como equipo azul.

Ciberataques: ataques que se generan a las redes digitales de los sistemas de información.

Ciberseguridad: aplicado medidas que se implementan para conservar los recursos de red.

Confidencialidad: categorización que se le da a la información que es privada y que no se está autorizado la divulgación o publicación.

Explotación: proceso mediante el cual se dan intrusiones automatizadas para ser modificado un sistema de información.

Firewall: dispositivo de seguridad de red que monitorea y administra el tráfico generado por las conexiones entrantes y salientes donde permite o restringe su destino.

Informática: se encarga de integrar los diferentes conceptos entre hardware y software para que la información sea procesada.

Malicioso: instrucciones o códigos que intentan dañar los sistemas de información, aprovechándose de las vulnerabilidades para acceder al sistema.

Puertos: en informática los puertos son interfaz física o virtual por medio del cual se accede a los diferentes tipos de información son utilizados para enviar y recibir señales de datos.

RED TEAM: equipos rojos que penetran en los sistemas de información de las organizaciones para posterior ayudar a corregir.

Virus: programas que se alojan en los sistemas de información y que ocasionan daño o propagación de códigos que alteran el normal funcionamiento de los sistemas.

Vulnerabilidad: debilidad informática que es utilizada por los atacantes para alterar sistemas de información.

RESUMEN

El presente informe técnico detalla el desarrollo que ayuda a conseguir el cumplimiento de cada de uno de los objetivos propuestos en cada fase de ejecución que ayudan a que la empresa WhiteHouse Security consiga la seguridad de la información basados en técnicas presentadas por los equipos Red Team y Blue Team. El inicio de la fase se evidencia con el montaje del banco de trabajo desde la documentación de leyes que rigen la seguridad informática, hasta las herramientas que se pueden utilizar por expertos de ciberseguridad para garantizar la proteccion de la información, la fase 2 abarcamos el análisis legal donde se alinean bajo estándares legales que rige la ley y la etica, la fase 3 podemos detallar el análisis del equipo Red Team detallando vulnerabilidades que surgen por la ejecución de aplicaciones y adicional en la fase 4 se analiza el equipo Blue Team para lograr identificar ataques en tiempo real que ayuden a proteger los sistemas de información.

INTRODUCCIÓN

Se elabora este documento con el propósito de agrupar y presentar estrategias de seguridad informática basadas en mecanismos legales y éticos lineados por los equipos Red Team y Blue Team que favorecen el fortalecimiento de la seguridad de la empresa WhiteHose Security.

Los altos niveles de ataques informáticos que se presentan en el mundo dan motivos para resaltar el reto importante que tienen los equipos de ciberseguridad por salvar y mantener disponible la información dentro de los entornos empresariales con retos que permitan fortalecer los estándares de seguridad.

Cada segundo es clave para prevenir ataques cibernéticos con el apoyo de los diferentes referentes como los Blue Team y los equipos de respuesta ante incidentes informáticos que analizan el comportamiento de las redes y las diferentes vulnerabilidades que se tienen.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1.2 OBJETIVOS ESPECÍFICOS

Detallar las leyes relevantes a los delitos informáticos que permitan conocer la regulación en Colombia

Presentar herramientas necesarias para realzar pruebas de penetración y comunicación entre equipos.

Realizar los procesos realizados para llevar a cabo un pentesting según su vulnerabilidad.

Documentar la vulnerabilidad existente en la maquina objetivo para lograr detallar los procesos que se realizan.

Investigar estrategias utilizadas por Blue Team para que los ataques cibernéticos no se repitan.

DESARROLLO DEL TRABAJO

ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

1.1. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

En Colombia contamos con leyes y decretos que sirven para linear el cómo proceder ante un delito informático, protección de datos personales y ciberseguridad, para el caso de la ley contamos con la ley 1273 de 2009 denominado de la protección de la información y de los datos[1] esta ley tiene como característica principal la exposición de sanciones que se tienen al incurrir en atentados contra la integridad, confidencialidad y disponibilidad de los sistemas de información.

Las sanciones que se contemplan en los diferentes delitos informáticos se resaltan en prisión y multas estipuladas en varios artículos descritos de la siguiente forma:

Artículo 269A: Acceso abusivo a un sistema informático. Se contribuye al que sin autorización accede total o parcial a un sistema de información que se encuentra protegido, se sanciona con detención por hasta 96 meses y en multa hasta 1.000 salarios mínimos legales mensuales vigentes[2].

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Quien sin estar autorizado impide el correcto funcionamiento del sistema de información de una red de telecomunicaciones. Se sanciona con detención por hasta 96 meses y en multa.

Artículo 269C: Interceptación de datos informáticos. Quien tome de forma ilegal señales electromagnéticas que le permitan espiar información incurrirá en detención por hasta 72 meses.

Artículo 269D: Daño Informático. Quien destruya un sistema de información tanto componentes físicos como lógicos, se sanciona con detención por hasta 96 meses y en multa hasta 1.000 salarios mínimos legales mensuales vigentes.

[1] DIARIO OFICIAL. AÑO CXLIV. N. 47223. 5, ENERO, 2009. PÁG. 5.

[2] Colombia, P. N. (02 de Septiembre de 2022). https://www.policia.gov.co. Recuperado el 04 de Septiembre de 2022, de https://www.policia.gov.co: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Artículo 269E: Uso de software malicioso. Quien por medio de distribución indebida de aplicaciones altere o dañe sistemas de información. Se sanciona con detención por hasta 96 meses y en multa por hasta 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. Quien acceda a información personal y utilice para divulgarla, 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.

Artículo 269G: Suplantación de sitios web para capturar datos personales. Quien publique páginas web que sustituyan una principal, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Ley 1581 de 2012 estipula lineamientos para el almacenamiento y tratamiento de la información donde se le da derecho al propietario de la información conocer y corregir sea el caso, y por parte del encargado de conservar la información se realice que forma segura.

En Colombia también se estipulan decretos que linean la proteccion de datos personales mediante la ciberseguridad, se tiene el Decreto 1078 del 2015 con modificación por medio del decreto 338 del 8 de marzo de 2022 mediante el cual se da lineamiento normativo del sector de la tecnología de la información y la comunicación que establece rutas de gobernanza de la seguridad informática, creando modelos de seguridad digital.

El gobierno nacional busca por medio de este decreto estructurar la implementación e identificación de datos críticos, para lograr salvaguardar el sistema.

Con el Conpes 3701 que se da el 14 de julio de 2011, se dieron orientación de política de seguridad informática y defensa cibernética, donde se busca coordinar atender y prevenir incidentes o emergencias cibernéticas que pongan en riesgo la seguridad de la información planeando conformar equipos de trabajo especializados en garantizar la seguridad.

Conpes 3854 del 11 de abril de 2016, se reglamenta es grupo de policía nacional especializado en seguridad digital, adicional estipula el grado de importancia que se le sebe dar a la gestión de riesgo de seguridad informática con el propósito de que todas las organizaciones tengan un enfoque de seguridad.

Conpes 3995 del 1 de julio de 2020 La Política Nacional mediante un grupo de Confianza y Seguridad Digital, busca posicionar a Colombia como espacio digital seguro.

1.2. En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Las pruebas de penetración son un conjunto de ataques simulados y dirigidos a un sistema de información con el propósito de detectar posibles vulnerabilidades para posterior ser corregidas y evitar ataques cibernéticos.

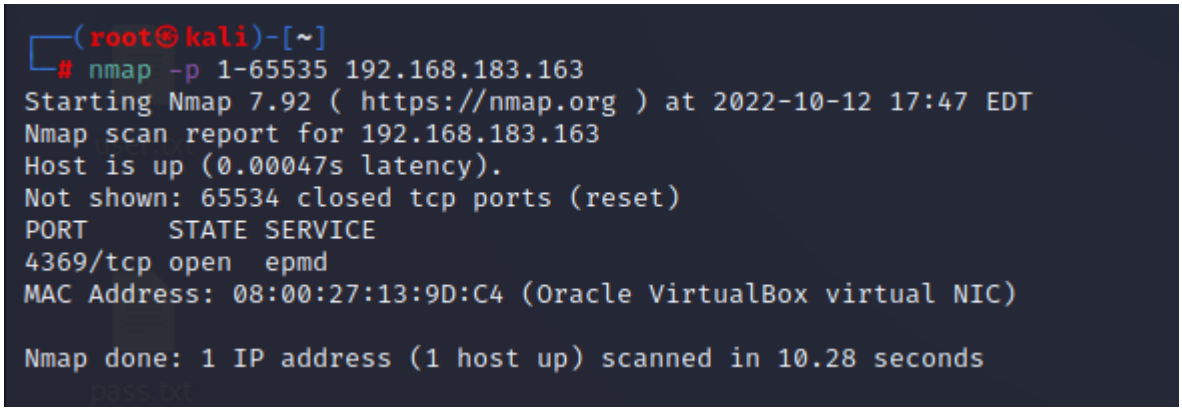
Estas pruebas de penetración tienen fases que conforman lineamientos para estipular las auditorias de ciberseguridad los cuales son: Recopilación de información / Enumeración, análisis de vulnerabilidades, explotación, post – Explotación, reporte.

Detallaremos cada etapa donde definiremos y daremos ejemplos de herramientas que se utilizan.

Recopilación de información / Enumeración:
Es la fase inicial de la prueba de penetración, en esta fase se recopilan datos e información de nuestro objetivo, que será utilizada en todo el proceso, estos datos pueden ser información del dominio, direcciones IP, puertos, versiones y servicios publicados en la red.

La herramienta utilizada en esta fase en Nmap.
Software que funciona en diferentes plataformas de sistema operativo, es de código abierto y es utilizado para analizar redes activas identificando mediante paquetes servicios que están activos dando como resultado los diferentes puertos abiertos.

Figura 1 NMAP



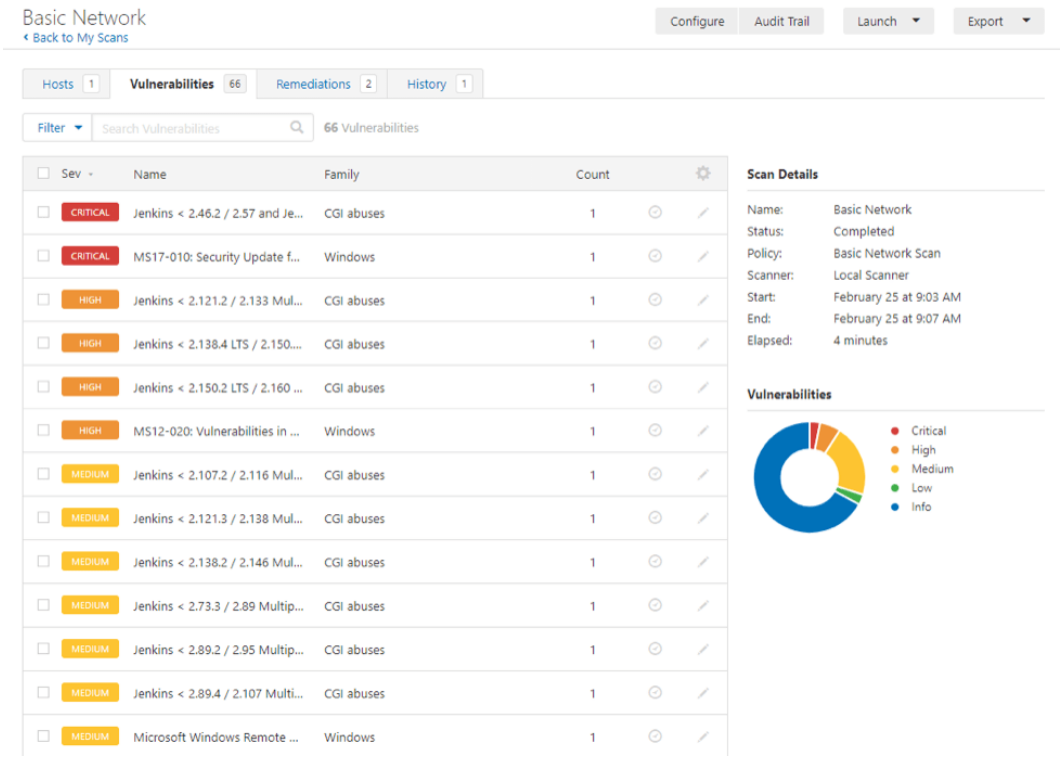
Fuente: Propia

Análisis de vulnerabilidades:
Esta fase contempla en realizar todas las acciones que nos permitan comprometer el sistema a penetrar, enumerar los diferentes fallos que se presenten tanto de autenticación como de operación, configuraciones defectuosas.

Herramienta Nessus
Software de interfaz amigable con fácil publicación de información agrupada y que se origina desde el análisis del sistema en busqueda de vulnerabilidades de diferentes sistemas y equipos conectados a la red.

Los escaneos para la identificación de vulnerabilidades se pueden dar por grupos, para realizar los análisis en diferentes espacio de tiempo, evitando la saturación de la red.
Nessus, posterior a su análisis interno de la red, compara con las bases de datos publicadas para presentar el informe de las vulnerabilidades encontradas y como poder atenderlas.

Figura 2 Herramienta Nessus

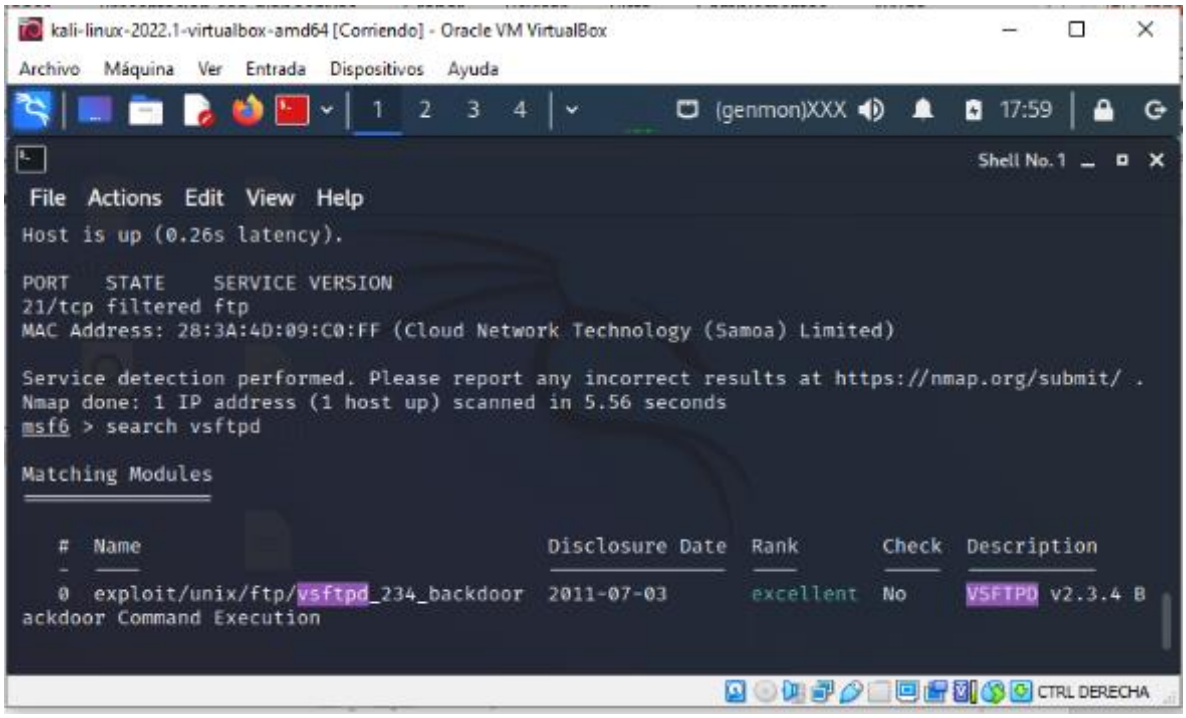


Fuente: Propia

Explotación
Para la fase de explotación se aprovecha las vulnerabilidades e información identificada en las fases anteriores con el propósito de obtener acceso a los sistemas de información.

La herramienta para esta fase es Metasploit Framework
Metasploit se caracteriza por ser un sistema de código abierto con capacidad de ser utilizado en ambiente Linux y Windows con una carga de sploit que permite saber las vulnerabilidades históricas y existentes para luego ser comparadas con las que tiene el sistema investigado.

Figura 3 Metasploit Framework

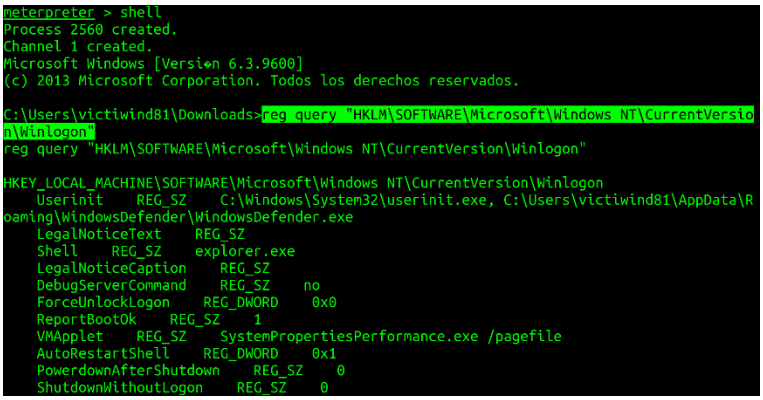


Fuente: Propia

Post – Explotación:
Esta fase se aplica posterior al haber logrado ingresar al sistema vulnerado, con el propósito de identificar que privilegios se tienen y que sistema adicional se puede acceder, se busca tener acceso a información confidencial, sistemas de información ocultos y evadir mecanismos de autenticación.

La herramienta utilizada en esta fase es meterpreter y bajo comando se puede acceder a registros del sistema operativo.

Figura 4 Meterpreter



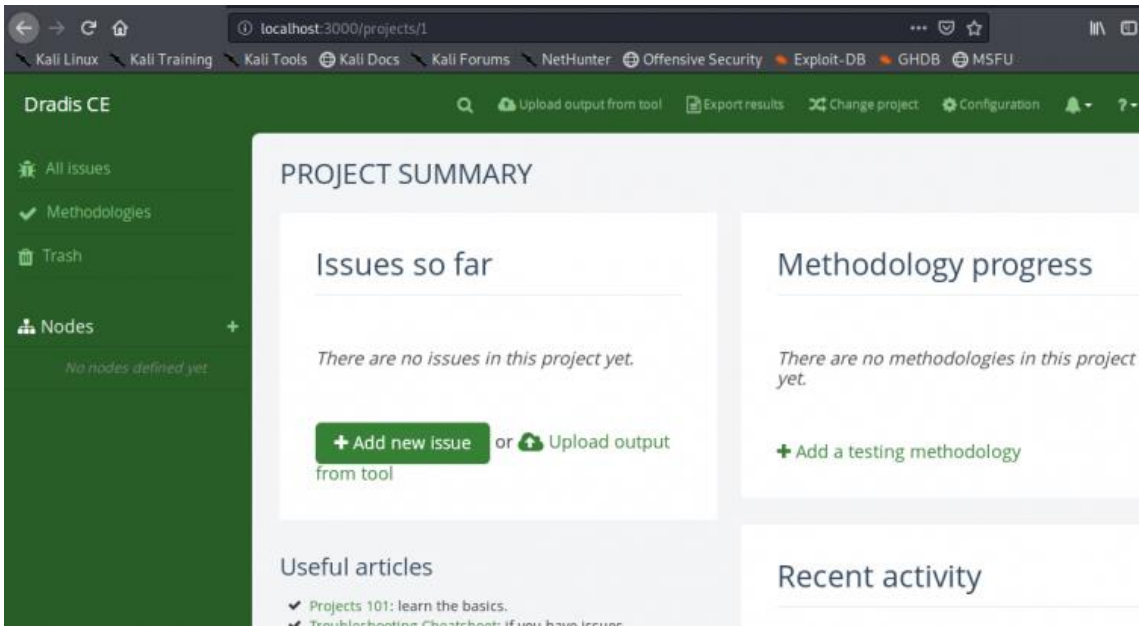
Fuente: Técnicas de Hacking – THW

Reporte.

Para la fase final de las pruebas de penetración se informa las vulnerabilidades aprovechadas para lograr acceder al sistema de información atacado, adicional se relacionan las soluciones propuestas para contrarrestar los fallos de seguridad que se tienen en nuestro sistema.

La herramienta presentada para esta fase es Dradis, es de open source, utilizada para realizar reportes y visualizar informes, puede ser integrada con herramientas utilizadas en las fases anteriores para presentar la información.

Figura 5 Herramienta Dradis



Fuente: byte-mind

1.3. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:
Herramientas:

• Metasploit
Es una aplicación de código abierto especializado en seguridad informática, centrado en proporcionar información de vulnerabilidades en los sistemas y ayuda en las pruebas de penetración, adicional fortalece las firmas de sistemas de detección de intrusos con el descubrimiento de vulnerabilidades.
Dentro de sus aplicaciones se tiene la versión Framework que por medio de exploits se realiza ataques de vulnerabilidad contra un equipo remoto.

Metasploit se puede ejecutar en sistemas operativos Unix, Windows, Linux, Mac OS X, y sirve para explorar vulnerabilidades mediante comandos ya diseñados y que se denominan exploit básicamente es un ataque que usa una vulnerabilidad para causar algún tipo de respuesta, esto introduciendo ordenes que permitan establecer comunicación mediante la red con el dispositivo denominado objetivo.

Los exploit están ya cargados en la herramienta y cada uno tiene su función y van desde escanear la red y dispositivo conectado hasta el ingreso al sistema de información borrando o modificando información sin dejar rastro.

El más común es utilizar Kali Linux para acceder a la consola de metasploit, mediante el comando msfconsole, posterior se utilizan los comando dependiendo de lo que se desee hacer, básicamente se tiene los siguientes comandos Search, use, info, set.

Search es utilizado para encontrar un exploit o un escáner para una vulnerabilidad en particular.

Use es utilizado para ejecutar una secuencia de comando predeterminado.

Info teniendo una cadena seleccionada y activada se puede obtener la información con el comando info.

Set es utilizado para asignar valores a una variable dentro de una secuencia de exploit.

Figura 6 Metasploit

Fuente: Openwebinars

• Nmap

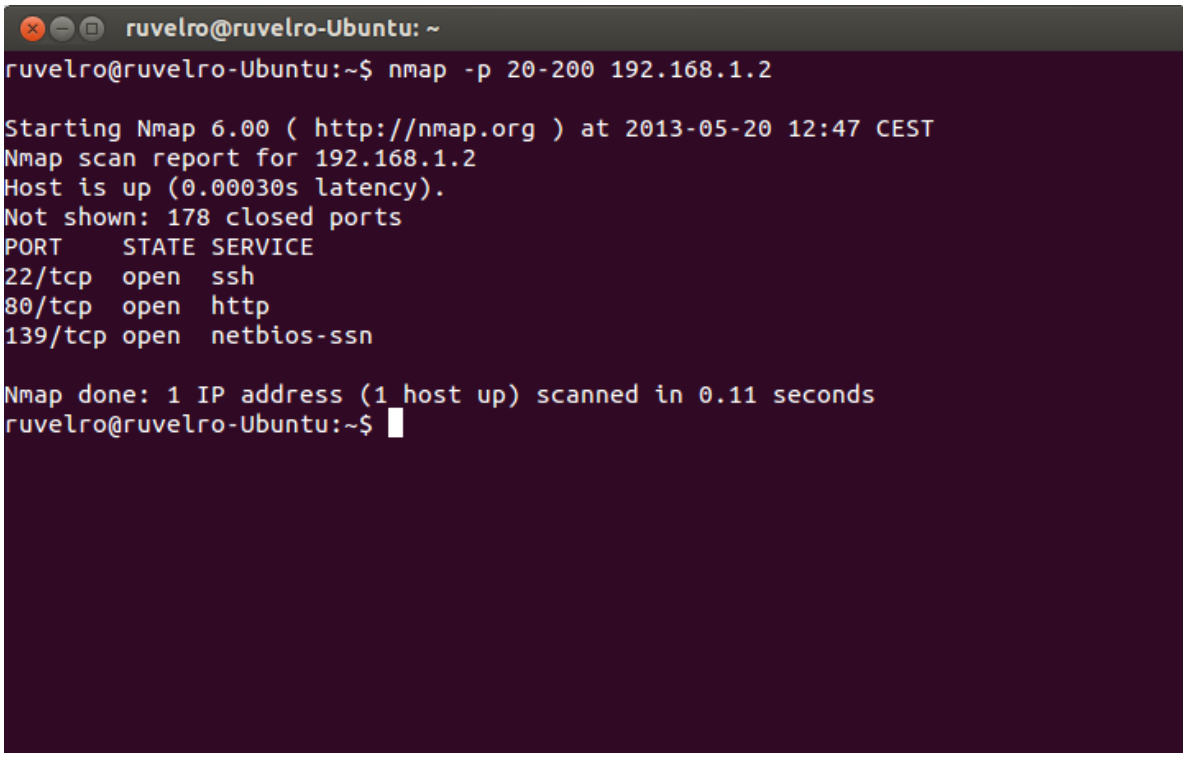
Es un software de código abierto diseñado para rastrear puertos abiertos en un sistema de información, identifica servicios publicados en una red mediante el envío de paquetes definidos y analiza las respuestas obtenidas con esto se descubre que servicios están activos.

Es utilizado para detectar equipos, servicios y sistemas operativos para utilizar esta información como inicio de una prueba de penetración para identificar a que sistema va a intentar intervenir.

El destino del análisis de servicios publicados se dirige a un dispositivo o un rango de dispositivos conectados a la red, su respuesta se basa en equipos que respondan la petición y los servicios disponibles en el momento del escaneo, su interfaz es gráfica y CLI que ambas permiten la introducción de comandos que permite emitir una orden de análisis.

El comando más utilizado en Nmap es la identificación de servicios en un rango de puertos nmap -p [rango] [ip]

Figura 7 Comando Nmap



Fuente: Propia

• OpenVas

Es un software que agrupa servicios y herramientas que se especializan en el escaneo y tratamiento de vulnerabilidades de seguridad en sistemas de información, todos los productos que la componen son de software libre y la mayoría bajo licencia GPL

Tiene como característica, el escaneo concurrente de múltiples modos soporta SSL y sus amplios reportes generados, inicialmente fue una variante de escaneo de seguridad de Nessus hasta el cambio de su modalidad de licenciamiento poniéndose como un sistema de pruebas de penetración.

Servicios en línea:

• ExploitDB

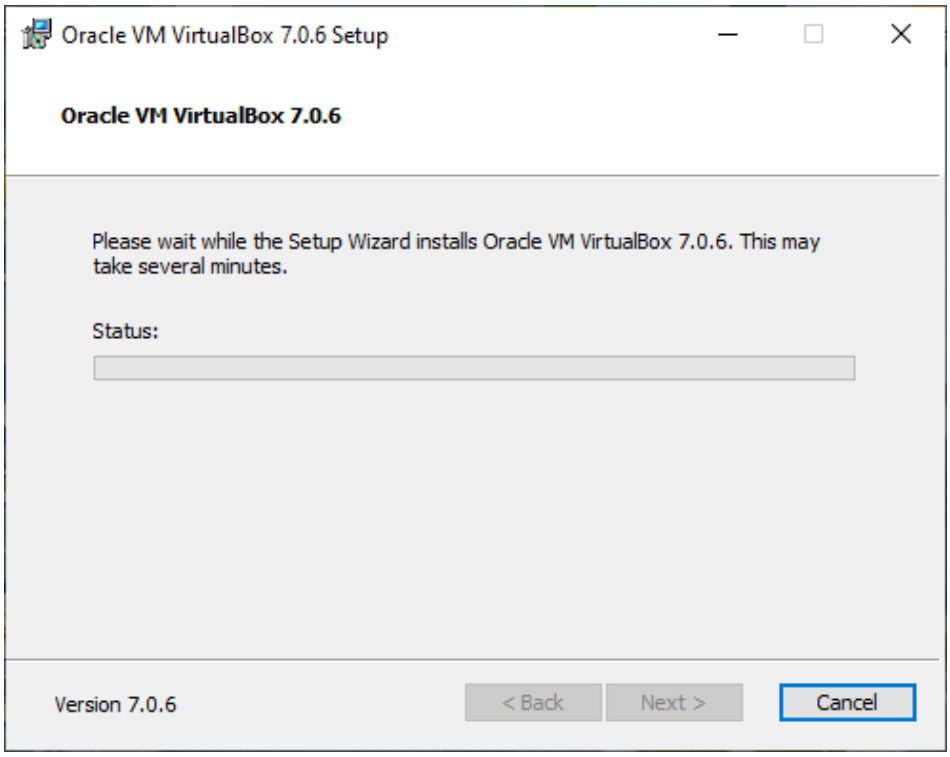
Es una aplicación web que almacena los exploits para vulnerabilidades conocidas y es alimentada por los mismos usuarios que comparten las vulnerabilidades encontradas para que sea utilizado en las mejoras de ciberseguridad de forma gratuita para garantizar la calidad de las auditorias de ciberseguridad.

• CVE
Denominado según sus siglas como vulnerabilidades y exposiciones comunes, es información publicada sobre vulnerabilidades de seguridad conocidas, cada vulnerabilidad encontrada es detallada por el sistema operativo afectado, versión y una posible solución, la identidad de la vulnerabilidad es iniciada con CVE y numeración que ayuda a identificarla en futuras búsquedas y reportes de aplicaciones especializadas en detectar vulnerabilidades y asociarlas con bases de datos publicadas.

1.4. Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1
– Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1
– escenario 1 es lo siguiente:

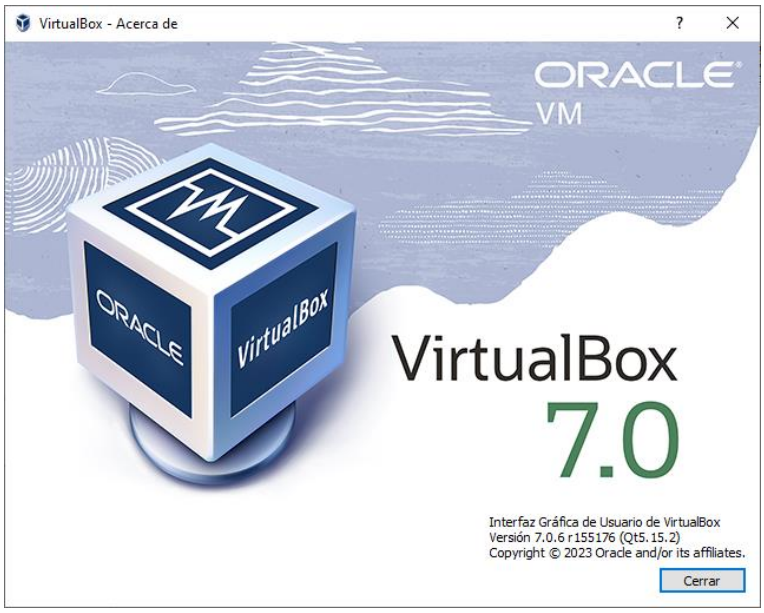
• Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

Figura 8 Instalación VirtualBox en su última versión



Fuente: Propia

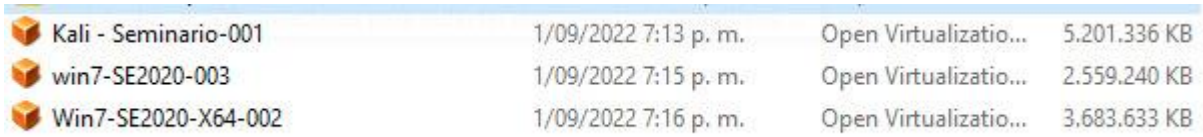
Figura 9 Versión VirtualBox



Fuente Propia

• Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Figura 10 Máquinas Virtuales



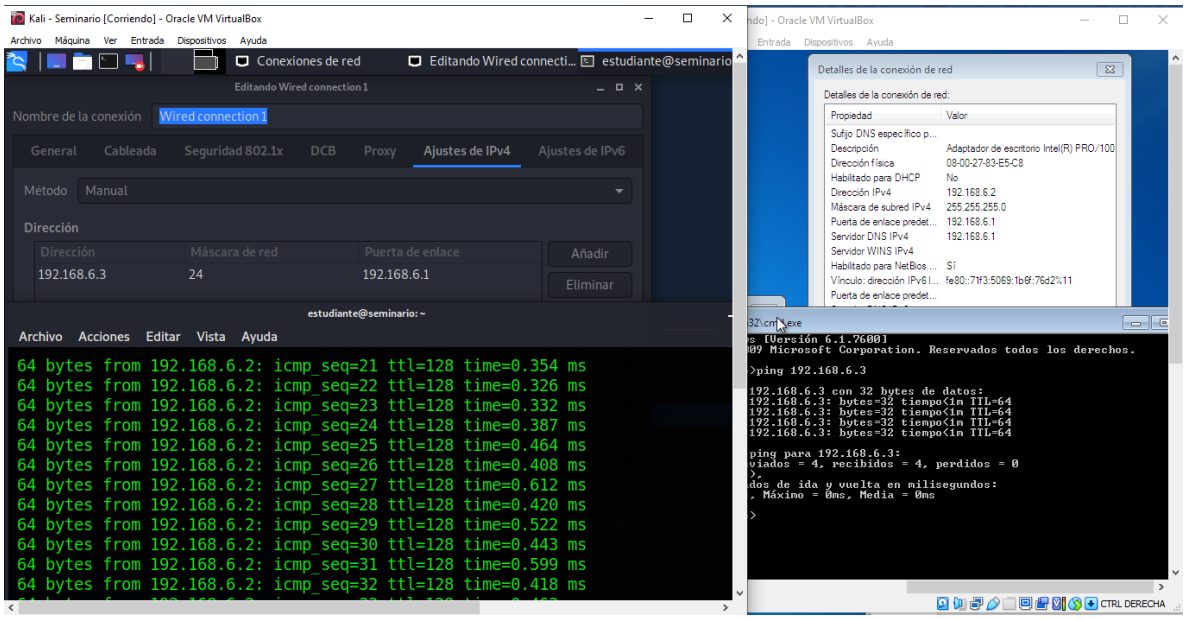
Fuente: Propia

• Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Conexión Kali – Seminario con Win7-SE2020

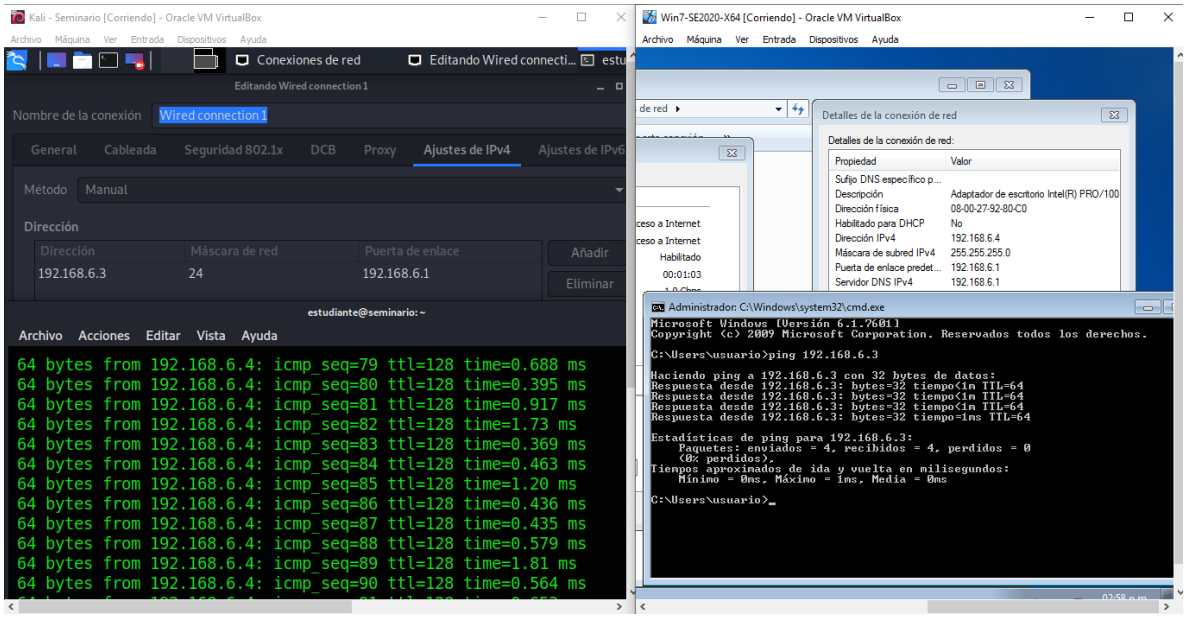
Kali Linux tiene la IP 192.168.6.3 y el equipo Win7-SE2020 tiene la IP 192.168.6.2, podemos evidenciar que existe comunicación por medio de pin entre las maquinas.

Figura 11 Conexión Kali – Seminario con Win7-SE2020



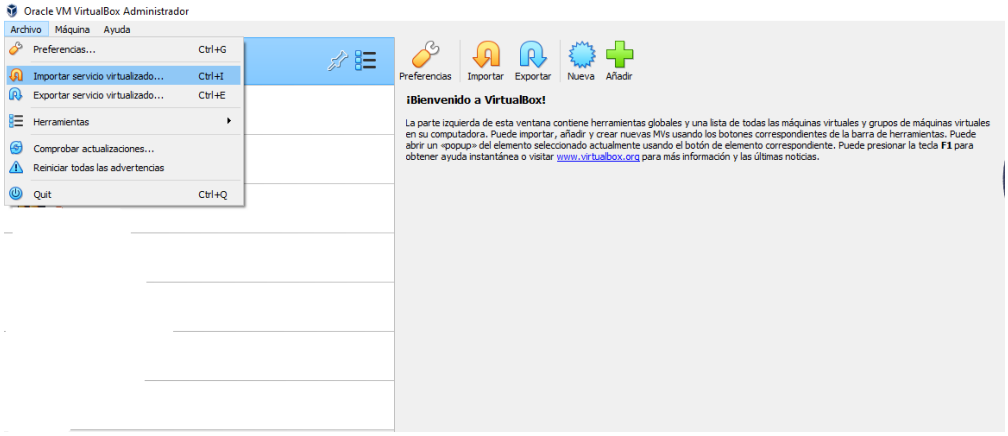
Kali Linux tiene la IP 192.168.6.3 y el equipo Win7-SE2020-X64 tiene la IP 192.168.6.4, podemos evidenciar que existe comunicación por medio de pin entre las maquinas.

Figura 12 Conexión Kali – Seminario con Win7-SE2020-X64



• Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

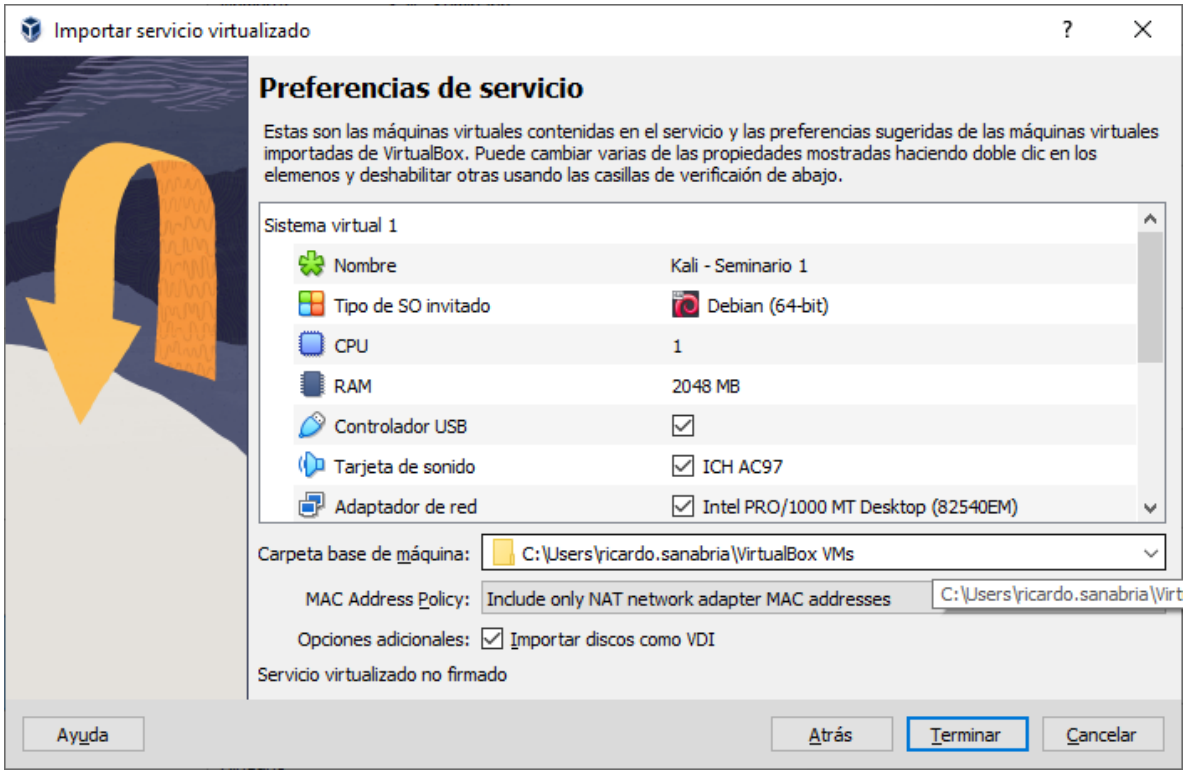
Figura 13 Importamos cada máquina virtual Kali Linux



Fuente: Propia

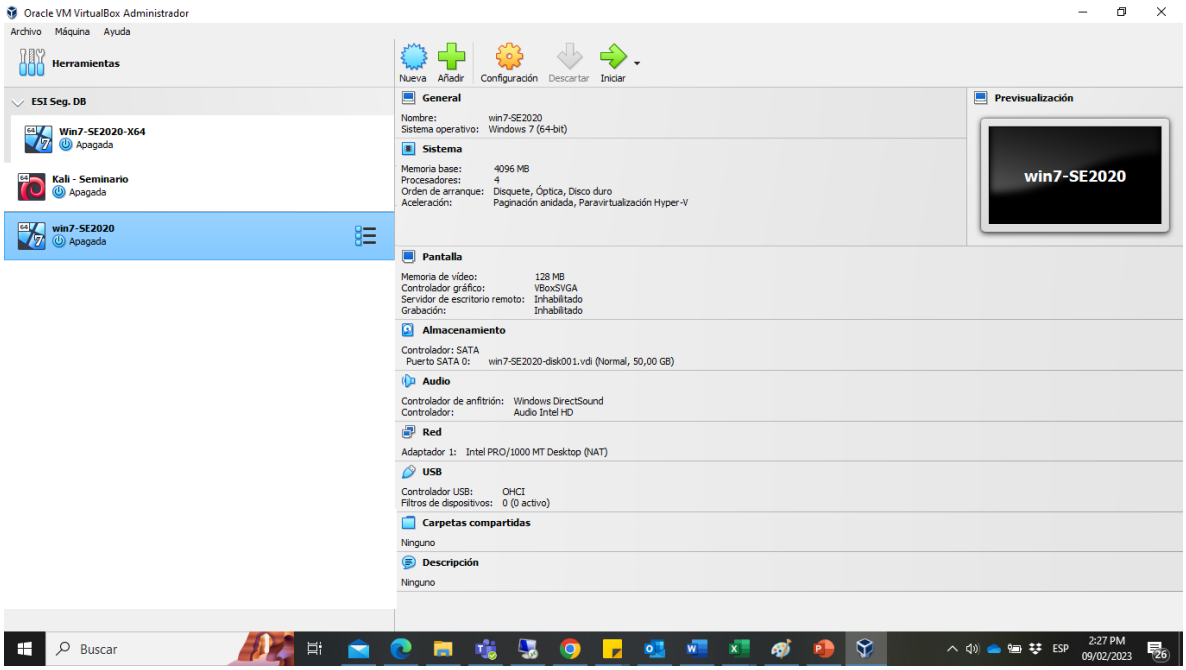
Seleccionamos la máquina que vamos a importar y elegimos donde la va a guardar

Figura 14 Importar servicios Virtualizado



Fuente: Propia

Figura 15 Maquinas Importadas



Fuente: Propia

Las tres máquinas están alojadas en VirtualBox y tienen las siguientes características:

-. Kali – Seminario
Sistema Operativo: Linux
Memoria RAM: 2048 MB
Disco duro: 50GB
Tipo de red: NAT
Procesador: 1CPU
IP: 192.168.6.3

-. Win7-SE2020
Sistema Operativo: Windows 7
Memoria RAM: 4096 MB
Disco duro: 50GB
Tipo de red: NAT
Procesador: 4CPU
IP: 192.168.6.2

-. Win7-SE2020-X64
Sistema Operativo: Windows 7
Memoria RAM: 4096 MB
Disco duro: 50GB

Tipo de red: NAT
Procesador: 4CPU
IP: 192.168.6.4

ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

2.1-. Luego de leer el anexo 2 – escenario 2 y el anexo 3 Acuerdo, logro identificar los siguientes procesos ilegales y poco éticos.

Anexo 2 – Escenario
Fragmento
"Un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal."

El marco legal en los procesos internos se vio empañados por la actuación del abogado que realizó los contratos ya que se vio involucrado en procesos ilegales donde trasmitió su actuar en la documentación elaborada. El mayor error fue que la gerencia no se tomó el tiempo de evaluar el contenido de los contratos que envío a firmar por parte de los postulados.
Dan a entender que el gerente está de acuerdo con el contenido de los documentos aun sabiendo que su abogado realizó procesos ilegales.

Anexo 3 Acuerdo
Fragmento
"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."

Los acuerdos de confidencialidad son legítimos y necesarios para garantizar que la información tratada dentro de la organización se garantiza que será tratada como privada y se evita ser divulgada o utilizada para fines competitivos, ahora bien, no es ético obligar a un empleado en tratar y callar procesos ilegales que se procesen en WhiteHouse y más como se menciona explícitamente en el acuerdo primera cláusula que los procesos ilegales no podrán ser divulgados, está bien que los procesos se deben tratar como confidencial, pero no se deberá permitir realizar o participan en asuntos que van en contra de la ley.

Anexo 3 Acuerdo
Fragmento

“2. 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”.”

La información tratada dentro de la organización es utilizada en su negocio con fines de lucro, solo si esta adquirida legalmente y en caso contrario la información obtenida por Interceptación de información, chuzadas y accesos abusivos a sistemas informáticos, es considerado invasión a la privacidad y va en contra de la ley, ninguna persona o empresa es libre de acceder a información de otra persona.

Anexo 3 Acuerdo
Fragmento
3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

La empresa obligaría bajo este acuerdo a que sus empleados al darse cuenta de actividades sospechosas no deberán denunciar convirtiéndolos en cómplices donde tendrían que actuar de forma inapropiada en las actividades sospechosas de espionaje.
Si por algún motivo que obliga a no denunciar cualquier espionaje que se realice se convierte en cómplice del delito, atentando contra la legalidad y la etica profesional.

Anexo 3 Acuerdo
Fragmento
4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Es adecuado advertir que la información confidencial que se conozca reciba o intercambie en reuniones no se debe divulgar, pero no es ético contemplar que los empleados deban abstenerse de denunciar información ilegal que se trate dentro de la organización obligándolos a que participen de esa ilegalidad sin excluirse de ser cómplices.

Anexo 3 Acuerdo
Fragmento
7. Responder por el mal uso que le den sus representantes a la **información confidencial.**

La información que trate o manipule cada individuo es responsabilidad de quien la manipule y no es viable que una persona se responsabilice de lo que hace otra persona, cada uno es responsable de sus actos, dentro del tratamiento de la información se debe dar secuencia de quien manipula la información y la cadena de custodia de esta.

Anexo 3 Acuerdo
Fragmento
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.

Es evidente que cada persona responde por sus actos, pero no se debería en caso de que la información que se está procesando sea de propiedad de la empresa a la que trabaja, involucrarse desde el inicio sin saber la procedencia de la información no lo hace responsable para responder ante las autoridades.

Anexo 3 Acuerdo
Fragmento
9. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Whitehouse Security**.**

La información que se clasifique como ilegal no debe ser tratada dentro por la empresa y menos estipularse como información que no se deba trasmitir ya que no es pertinente recibirla y tratarla; es poco ético pretender que se reciba información ilegal y se trate para otros fines.

Anexo 3 Acuerdo
Fragmento
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.

Desde un inicio no se debe aceptar la recepción de información ilegal que se impone en la empresa Whitehouse Security, mucho menos procesarla y almacenarla ya que se convierten de inmediato en cómplices del delito, ahora bien, la empresa por librar sus responsabilidades se exime de la tenencia de la información ilegal haciendo total responsable al personal que la posee siendo sin duda un mal procedimiento desde el inicio.

2.2-. Es afirmativo y se encontraron procesos ilegales en el anexo 3, mencionaré los artículos que se especifican en la ley 1273.

Artículo 269A: Acceso abusivo a un sistema informático. Se contribuye al que sin autorización accede total o parcial a un sistema de información que se encuentra

protegido, se sanciona con detención por hasta 96 meses y en multa hasta 1.000 salarios mínimos legales mensuales vigentes[3].

Artículo 269C: Interceptación de datos informáticos. Quien tome de forma ilegal señales electromagnéticas que le permitan espiar información incurrirá en detención por hasta 72 meses.

Artículo 269F: Violación de datos personales. Quien acceda a información personal y utilice para divulgarla, 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.

2.3-. Detalle de los procesos poco confiables del anexo 3 – Acuerdo, conociendo el acuerdo, aceptaría una vinculación laboral con salario de $15.000.000

Como experto en ciberseguridad no aplicaría a la oferta de trabajo de la empresa The WhiteHouse, y mi desistimiento se inclinaría por la cantidad de irregularidades que se tienen en el anexo 3 acuerdos donde se trata explícitamente de la captación ilegal de información por medio de interceptaciones, chuzadas y demás delitos informáticos que se pretende realizar dentro de la organización, más aún donde obligan al empleado a no denunciar en caso de darse cuenta de cualquier proceso ilegal.
Incurrir en delitos penales donde se ve involucrado detención o multas por tratar información ilegal hace que la propuesta pierda garantías a largo plazo y más aún donde la empresa en su octava consideración estipula que se exime de cualquier responsabilidad legal y penal en cuanto se descubra que unos de sus empleados están tratando información ilegal. Es evidente que la empresa The WhiteHouse tiene intención de realizar actos ilegales utilizando a sus expertos en seguridad informática estipulado directamente en sus textos del anexo 3 – acuerdo.

Según el código de etica para el ejercicio de la ingeniería en general y sus profesiones afines, contenido en la ley 842 de 2003 en su artículo 53 contempla las faltas gravísimas y numeral e donde se estipula que es falta gravísima incurrir en algún delito que atente contra su cliente, colega o autoridad de la república, dado a que, si la acción está autorizada de forma legal, la sanción a una falta gravísima da la cancelación definitiva de la matricula profesional.

2.4-. Operación Andrómeda Buggly en Colombia fachada de ciberseguridad con lineamientos de espionaje.

[3] Colombia, P. N. (02 de Septiembre de 2022). https://www.policia.gov.co. Recuperado el 04 de Septiembre de 2022, de https://www.policia.gov.co: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Buggly Ethical Hacking es el nombre que le dio Carlos Betancur al centro de intercambio de conocimiento de hackers en un sector de Bogotá, que se dedicaban a enseñar y aprender conocimientos tecnológicos, centrándose en conformar una comunidad de seguridad informática.
El lugar físicamente ostentaba altas inversiones de recursos económicos que de una u otra forma preguntaban los integrantes sobre su origen, y es desde entonces que se da a conocer la operación Andrómeda que era una central de inteligencia técnica del ejército nacional que se constituye con la misión de conseguir conocimiento de información del hacking ético.
Hasta este punto todo estaba acorde a la ley basados en la legalidad y a la operación etica en los procesos del tratamiento de la información.
Dentro del reclutamiento de hackers no se les indicaba que era una operación militar y desde aquí se quebranta la etica del equipo de trabajo donde se sostenían las personas con mentiras o poca información real de la operación.

La operación Andrómeda se centró en interceptar comunicaciones por medio de monitoreo del espectro donde analizaban la red en busqueda de información dedicada a un blanco especifico donde se obtiene información con software malicioso convirtiéndose en procedimientos ilegales que van en contra de la ley, esto se denunció en junio de 2013 donde se evidenció la existencia de un programa que fue diseñado para espiar computadores el cual enviaba información al centro de operaciones de Buggly.
Parte de la información que se conseguía dentro de Buggly y la fachada de Andrómeda era desviada y filtrada a terceros con fines ilegales, para este caso ingresa la participación de Andres Sepúlveda que es un hackers que se encargaba de realizar las compras de la información y aplicaciones ya desarrolladas y conseguidas por el centro de operaciones, iniciando lo que suponía no era el deber ser del grupo de ciber seguridad desviando la legalidad y etica profesional.

Los involucrados de esta operación se vieron implicados en delitos de espionaje, violación de datos personales y fueron enviados a prisión donde llevaron un proceso legal que definía el grado de culpabilidad según la participación en la captación ilegal de la información encontrada y por ello están privados de la libertad, sanciones económicas, un proceso de investigación en marcha y una carrera profesional destruida.

ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

3.1. Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red team. 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.

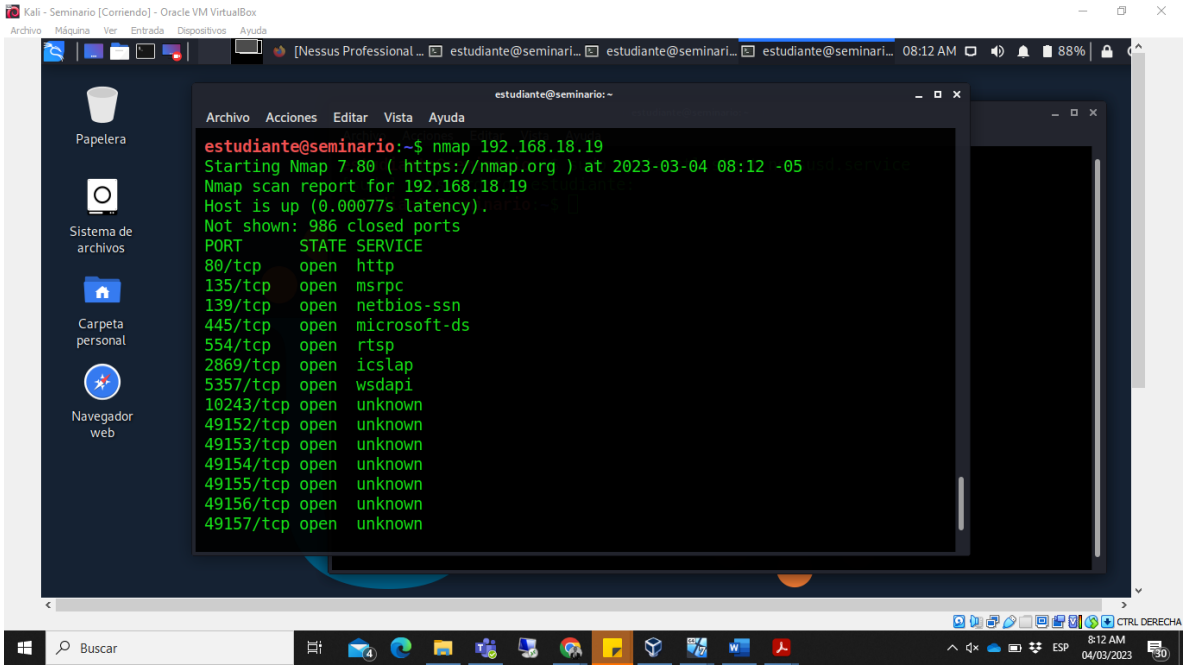
Las herramientas utilizadas para realizar el proceso del anexo 4 fueron:
-. NMAP
-. Nessus
-. Metasploit
-. Meterpreter

PASOS DE UN PENTESTING

Recopilación de información / Enumeración:

Información de NMAP:
Comando nmap 192.168.18.19 IP de la maquina objetivo

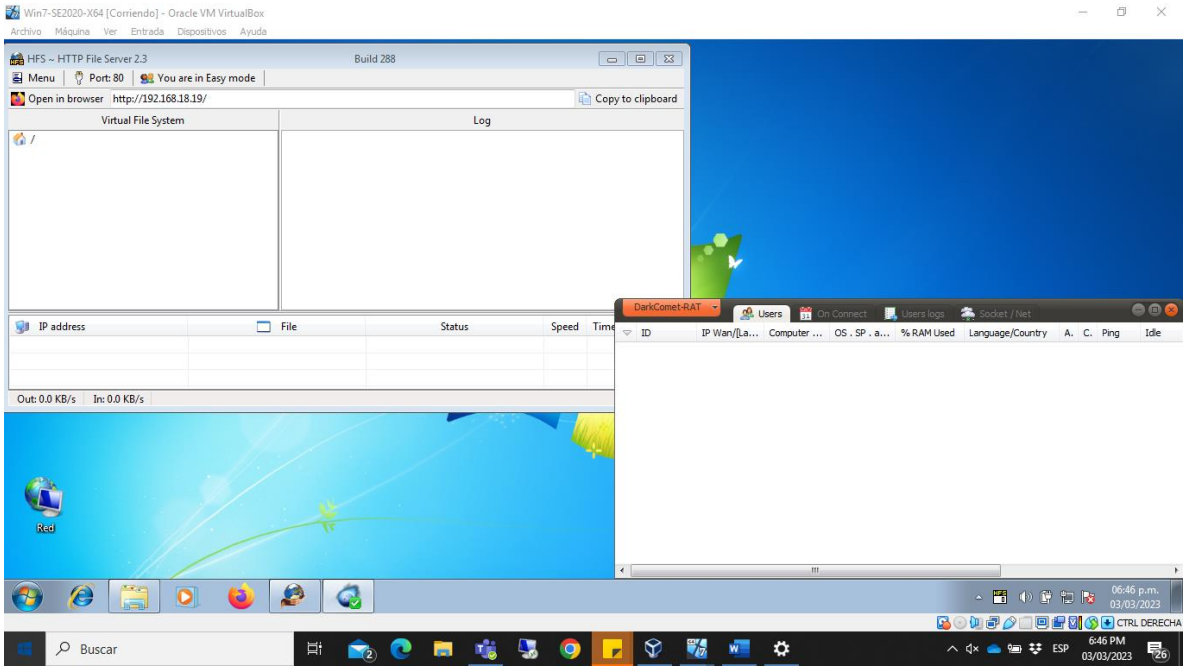
Figura 16 NMAP



Fuente: Propia

Aplicaciones involucradas
-. Rejetto HFS (HTTP File Server)
-. DarkComet

Figura 17 Rejjeto HFS y DarkComet



Fuente: Propia

Análisis de vulnerabilidades:

Instalamos Nessus
Descargamos Nessus de la página oficial, guardamos en Kali Linux y procedemos a la instalación con el comando dpkg -i Nessus.deb ejecutado en símbolo del sistema desde la carpeta donde está el archivo.

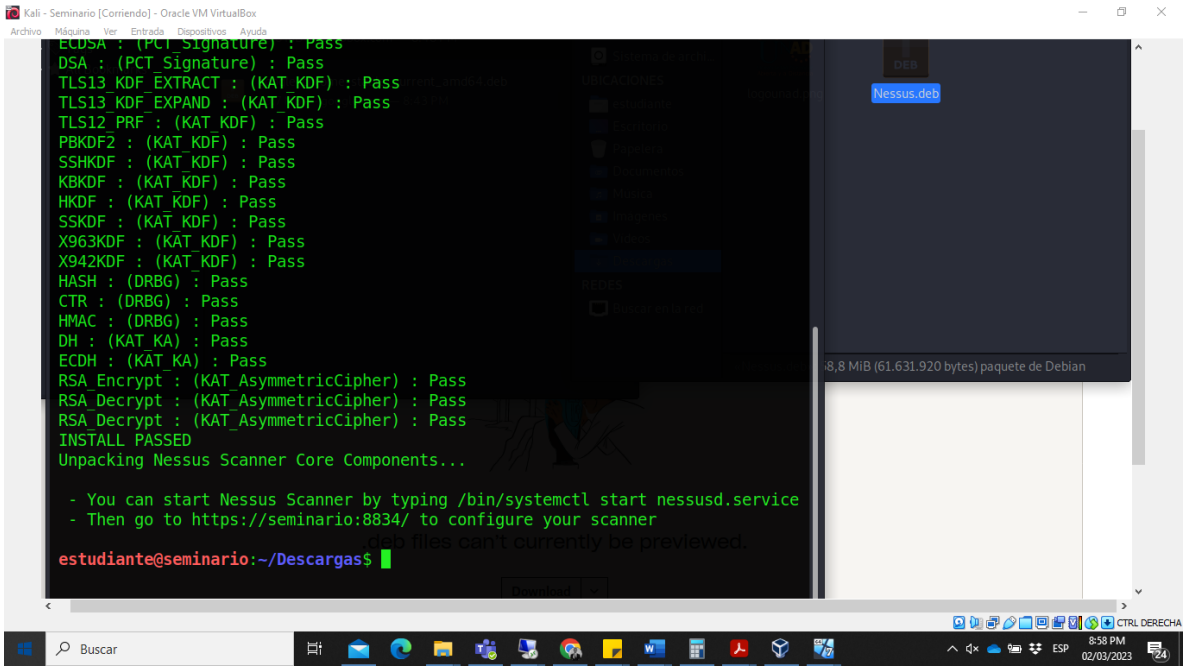
Los comandos utilizados fueron los siguientes:

Instalación Nessus
Sudo dpkg -i Nessus.deb

Activación Nessus
Sudo systemctl start nessusd.service

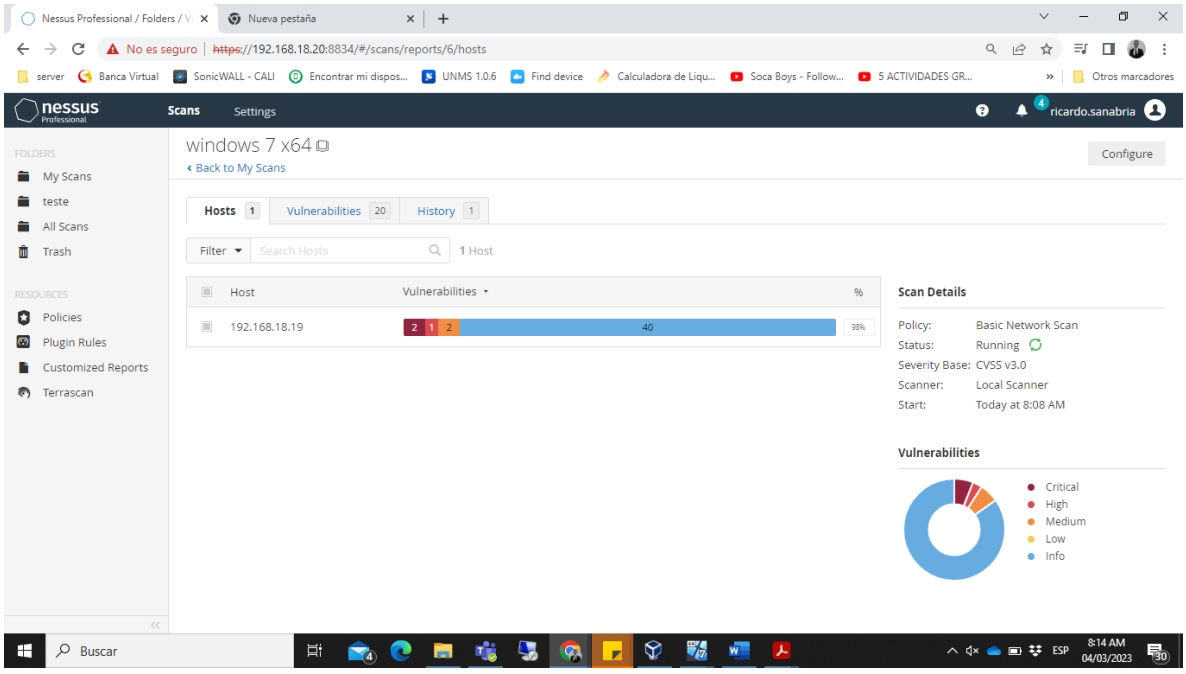
Web
Ingresamos a un navegador web y digitamos https://seminario:8834

Figura 18 Instalación Nessus



Fuente: Propia

Figura 19 Interfaz Web Nessus



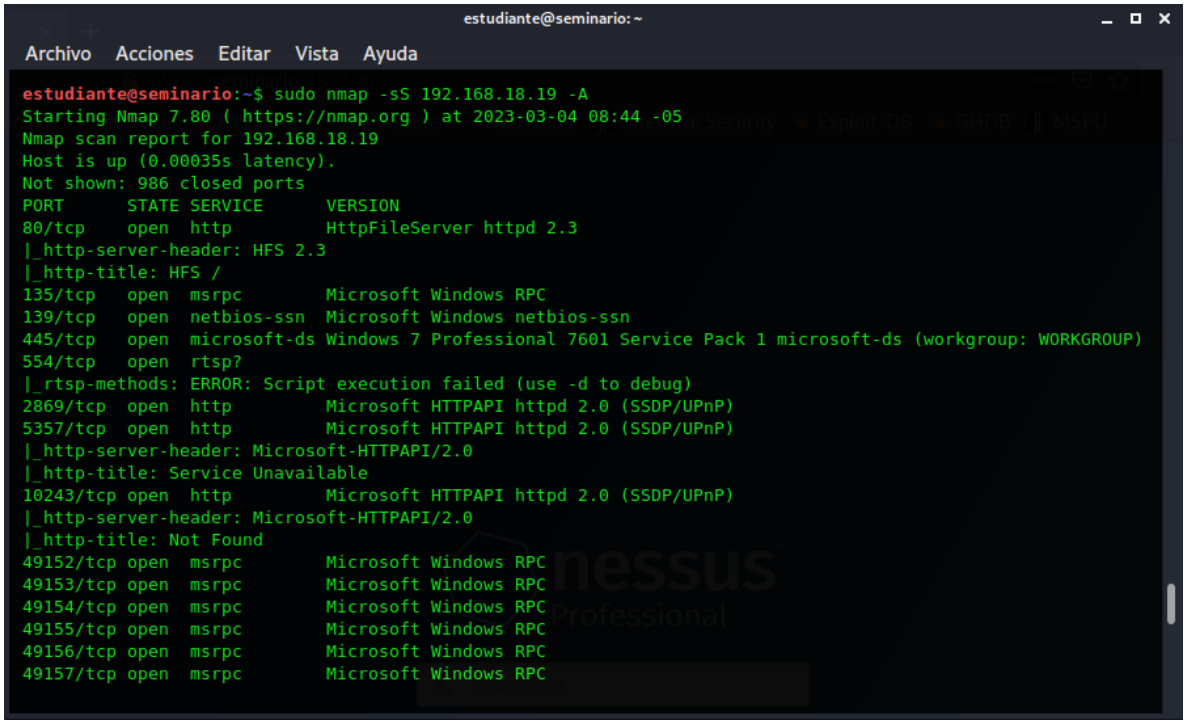
Fuente: Propia

Explotación

Identificaremos los puertos con servicios publicados donde identificamos el uso de la herramienta Rejjeto HFS (HTTP File Server)

Comandos utilizados
Sudo -sS 192.168.18.19 -A
Nos nuestra los puertos con los diferentes servicios abiertos y la versión.

Figura 20 NMAP con servicios



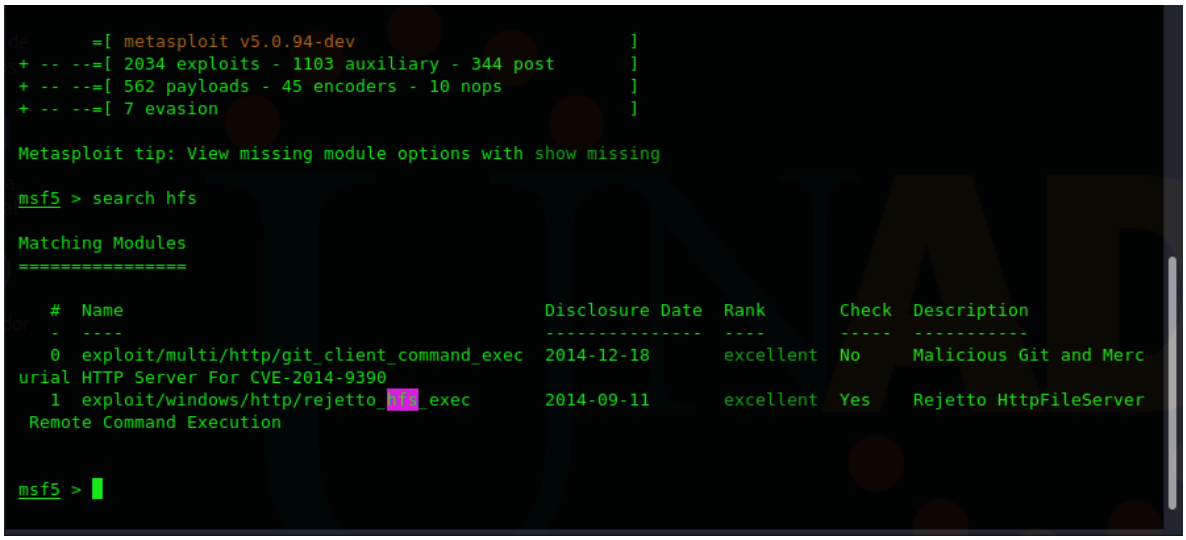
Fuente: Propia

Uso de Metasploit para la identificación de módulos que permitan el inicio del ataque

Para identificar el módulo de ataque hacemos una busqueda de la herramienta hfs que es la que está ejecutándose en la maquina objetivo

Comando
Search hfs

Figura 21 Metasploit



Fuente: Propia

3.2. 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.

Basados en la información del anexo 4 – escenario se indica que una maquina tiene fuga de información y con fallos de seguridad presentado en la maquina Windows 7 x64 generado por la existencia de una aplicación llamada rejetto v. 2.3 que mediante un exploit que asociado a un Shell permite que meterpreter ejecute mediante comandos la manipulación local del equipo en modo administrador.

Se logra listar lo siguiente:

-. Fuga de información
Un equipo conectado a la red con bajos niveles de seguridad, es un objetivo fácil de atacar ocasionando que la información que se contenga sea extraída y utilizada por personal externo a la organización.

-. El equipo Windows 7 x64 tiene una aplicación instalada llamada rejetto v2.3.
Tener aplicaciones ejecutándose en equipos conectados a la red que permitan la apertura de puertos hace que la seguridad del equipo se vea vulnerable, en este caso permitiendo el ingreso de exploit que modifican los registros con privilegios de administrador.

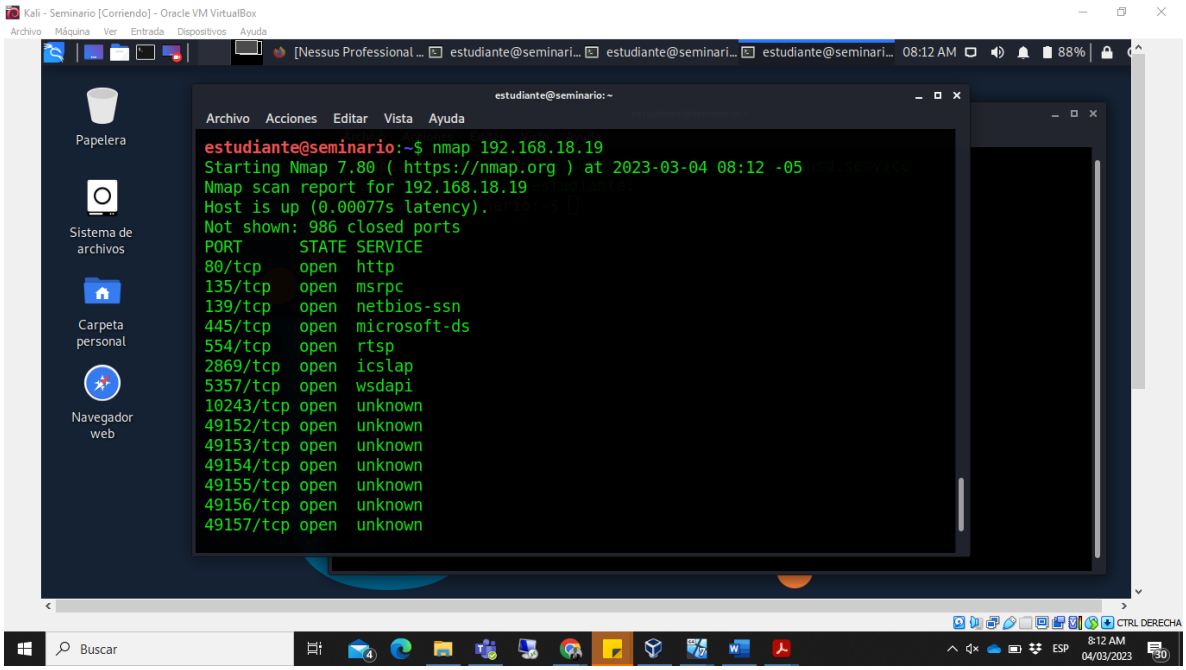
-. Vulnerabilidad en la modificación y creación de usuarios con privilegios de administrador.

El anexo 4 – escenario 3 da una idea de utilizar meterpreter para el ataque que podría recibir el equipo, para este caso es clave investigar la posible creación de usuario local con privilegios de administrador.

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

La herramienta utilizada en esta fase en Nmap.
Software que funciona en diferentes plataformas de sistema operativo, es de código abierto y es utilizado para analizar redes activas identificando mediante paquetes servicios que están activos dando como resultado los diferentes puertos abiertos.

Figura 22 NMAP



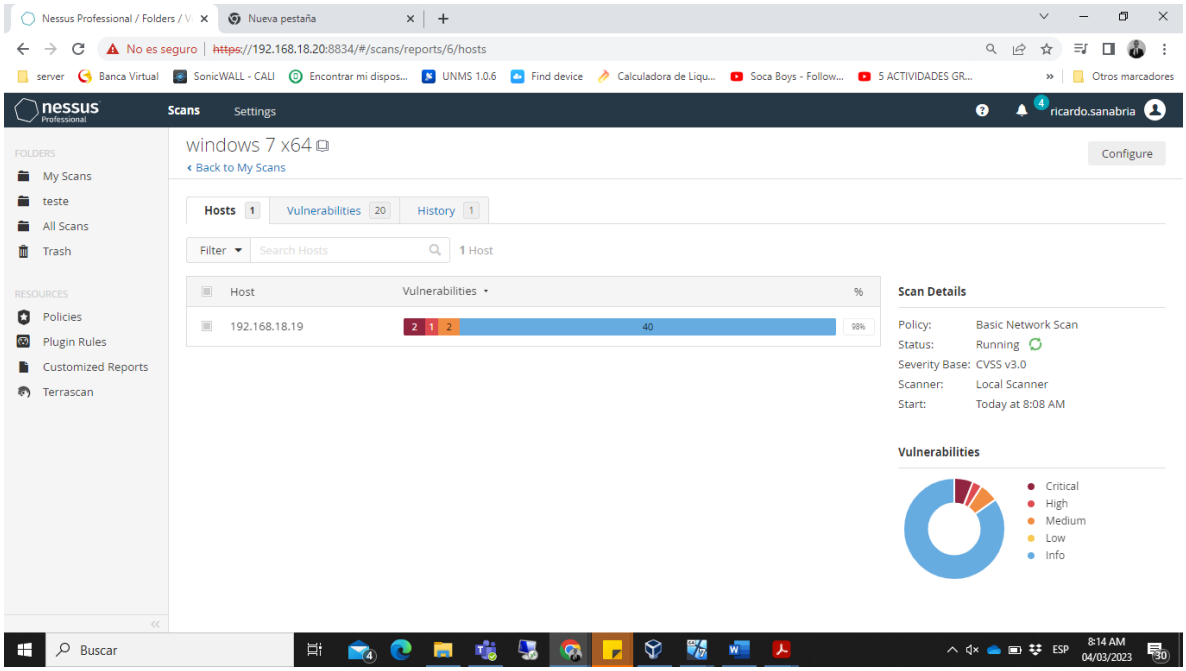
Fuente: Propia

Herramienta Nessus
Software de interfaz amigable con fácil publicación de información agrupada y que se origina desde el análisis del sistema en busqueda de vulnerabilidades de diferentes sistemas y equipos conectados a la red.

Los escaneos para la identificación de vulnerabilidades se pueden dar por grupos, para realizar los análisis en diferentes espacio de tiempo, evitando la saturación de la red.

Nessus, posterior a su análisis interno de la red, compara con las bases de datos publicadas para presentar el informe de las vulnerabilidades encontradas y como poder atenderlas.

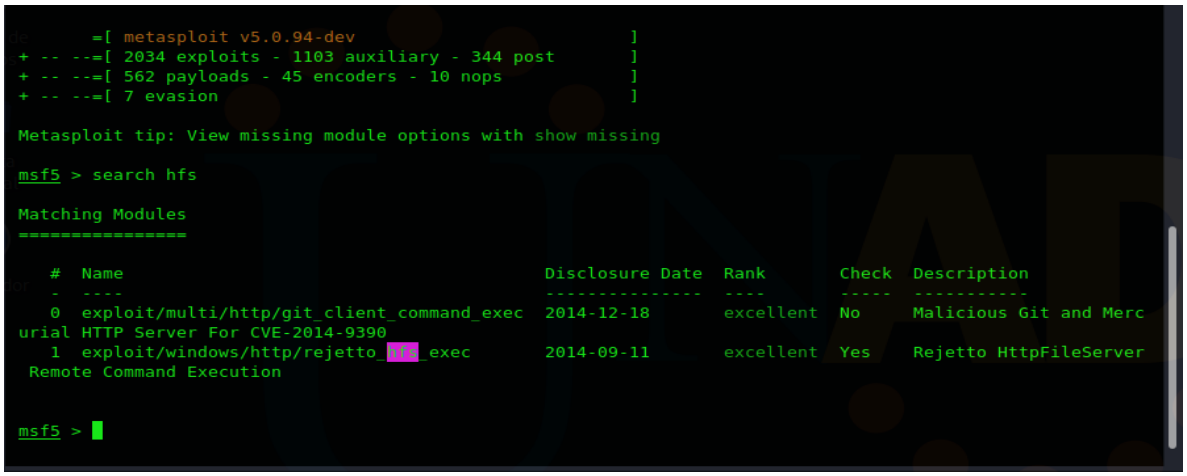
Figura 23 Web Nessus



Fuente: Propia

La herramienta para esta fase es Metasploit Framework
Metasploit se caracteriza por ser un sistema de código abierto con capacidad de ser utilizado en ambiente Linux y Windows con una carga de sploit que permite saber las vulnerabilidades históricas y existentes para luego ser comparadas con las que tiene el sistema investigado.

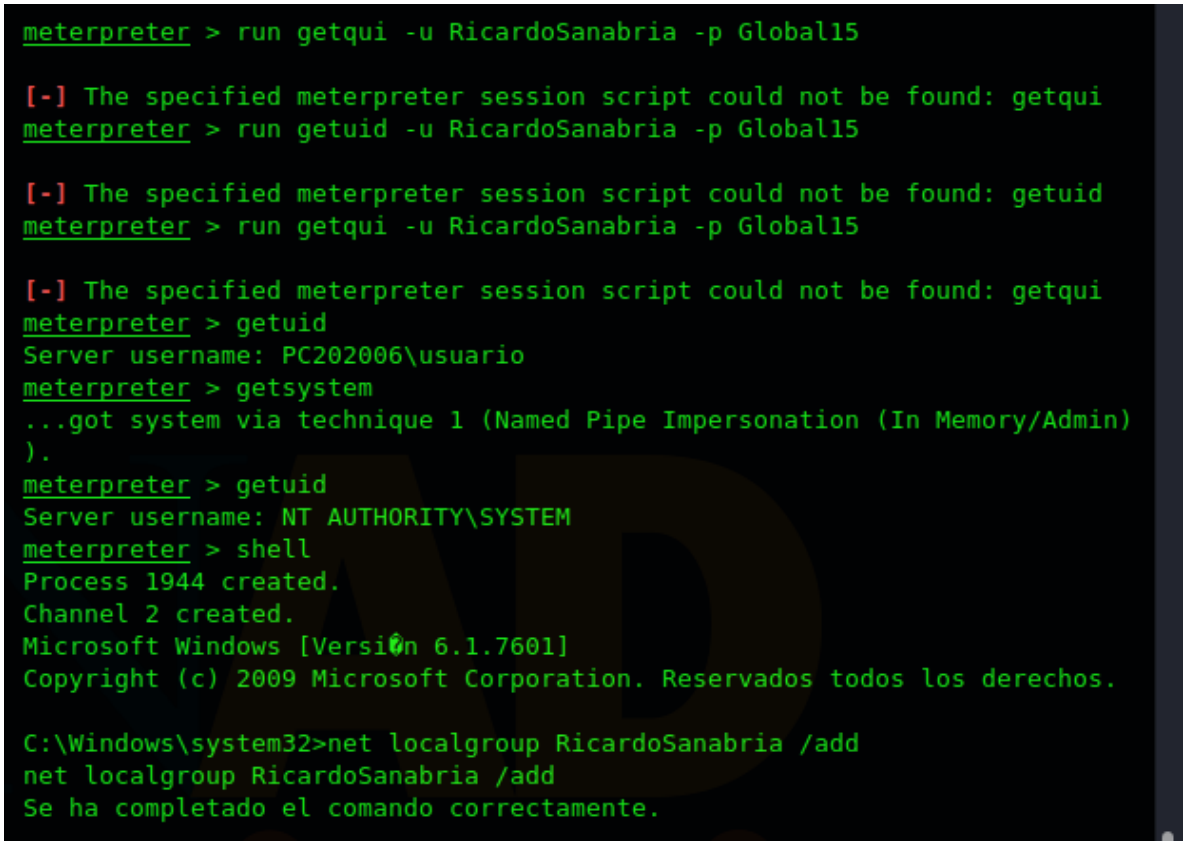
Figura 24 Metasploit Framework



Fuente: Propia

La herramienta utilizada en esta fase es meterpreter y bajo comando se puede acceder a registros del sistema operativo.

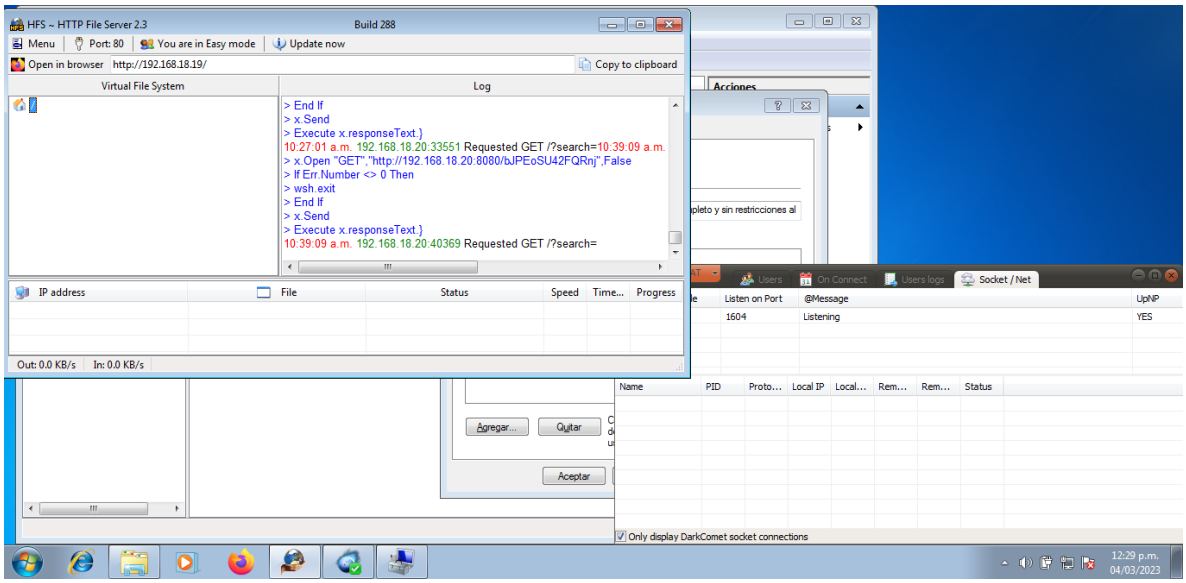
Figura 25 Meterpreter



Fuente: Propia

La aplicación que se describe en el anexo es rejetto v 2.3 y abre el puerto 80 como se evidencia en la imagen.
Un Software tiene el puerto web 80 abierto utilizándolo para recibir conexiones que pueden generar vulnerabilidad en el sistema.

Figura 26 Puerto 80 de Rejetto



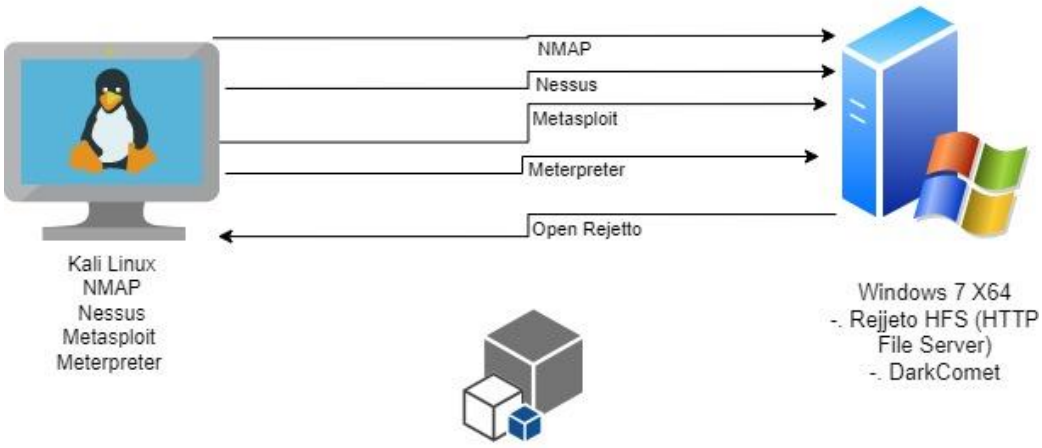
Puerto: Propia

3.4. 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.

El ataque de la maquina Windows 7 x64 se dio mediante la vulnerabilidad que se tiene por la ejecución de la aplicación rejetto v 2.3 que permite recibir conexión mediante exploit que se ejecuta por la herramienta Kali Linux, esta herramienta permite ejecutar NMAP para identificar los puertos abiertos, las aplicaciones que se utilizan mediante meterpreter resuelven comandos para atacar y modificar las configuraciones internas del sistema operativo, desde la creación de usuario como se dio en este caso hasta la asignación de privilegios de administrador.

Como podemos detallar la vulnerabilidad se establece desde que se permite la ejecución de aplicaciones en las terminales conectadas a la red que faciliten la apertura de puertos generando tráfico de entrada y liberando exploit con privilegios de administrador para modificar las configuraciones locales como si se estuviera trabajando en el equipo de forma local.

Figura 27 Ataque Maquina objetivo



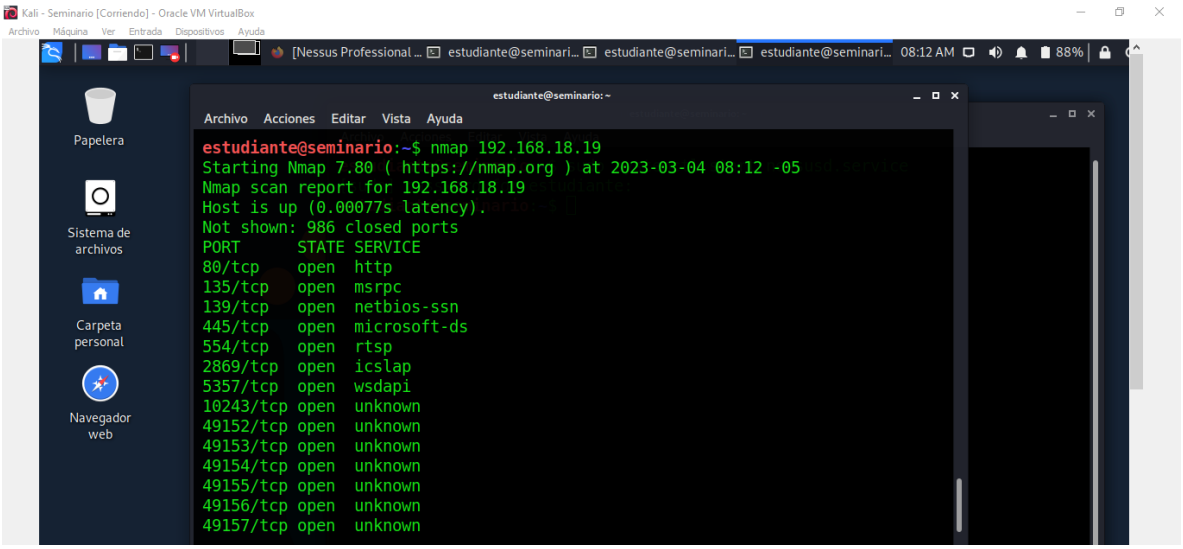
Fuente: Propio

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

Equipo Objetivo:
-. Win7-SE2020-X64
Sistema Operativo: Windows 7
Memoria RAM: 4096 MB
Disco duro: 50GB
Tipo de red: NAT
Procesador: 4CPU
IP: 192.168.18.19

Información de NMAP:
Comando nmap 192.168.18.19 IP de la maquina objetivo

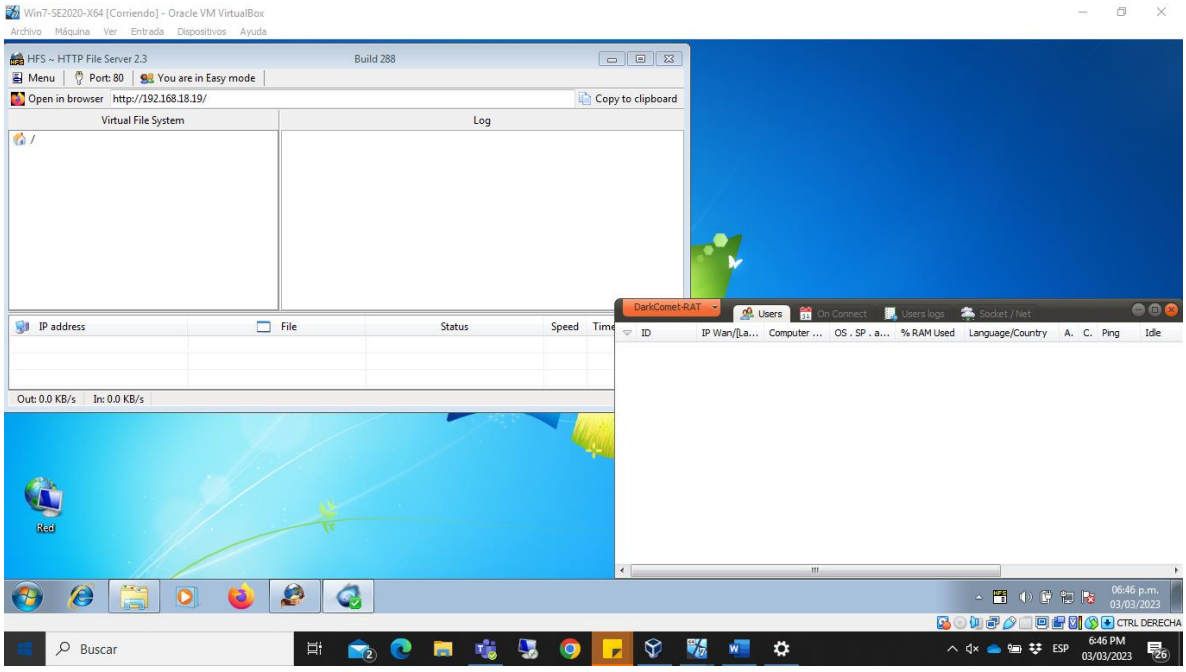
Figura 28 NMAP



Fuente: Propia

Aplicaciones involucradas
-. Rejetto HFS (HTTP File Server)
-. DarkComet

Figura 29 Rejjeto HFS y DarkComet

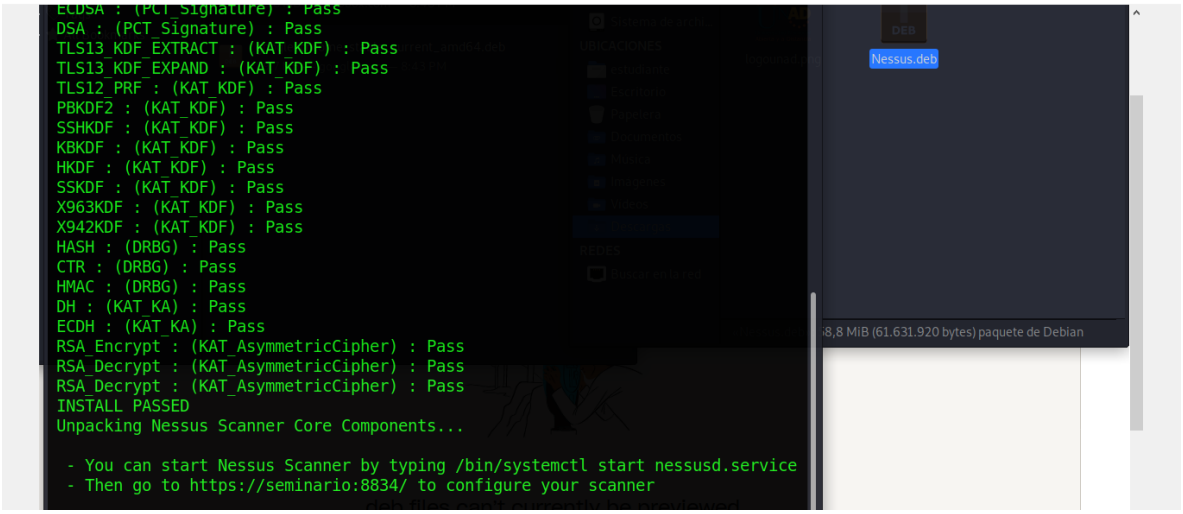


Fuente: Propia

Instalamos Nessus

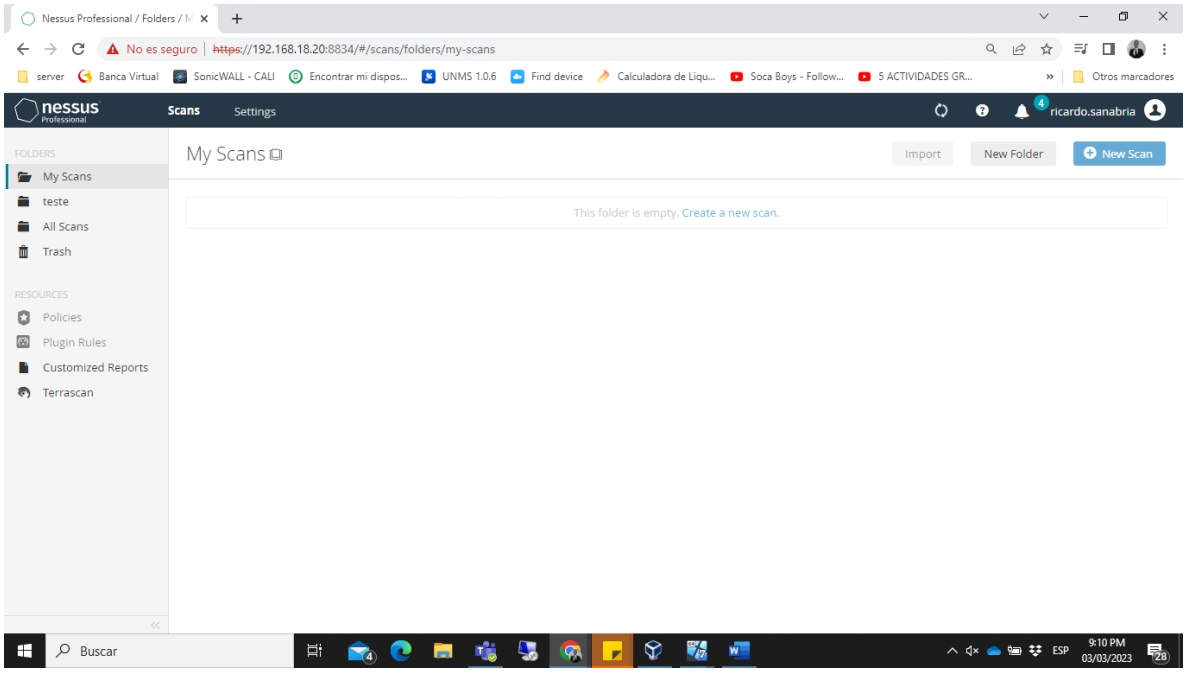
Descargamos Nessus de la página oficial, guardamos en Kali Linux y procedemos a la instalación con el comando dpkg -i Nessus.deb ejecutado en símbolo del sistema desde la carpeta donde está el archivo.

Figura 30 Instalación Nessus



Fuente: Propia

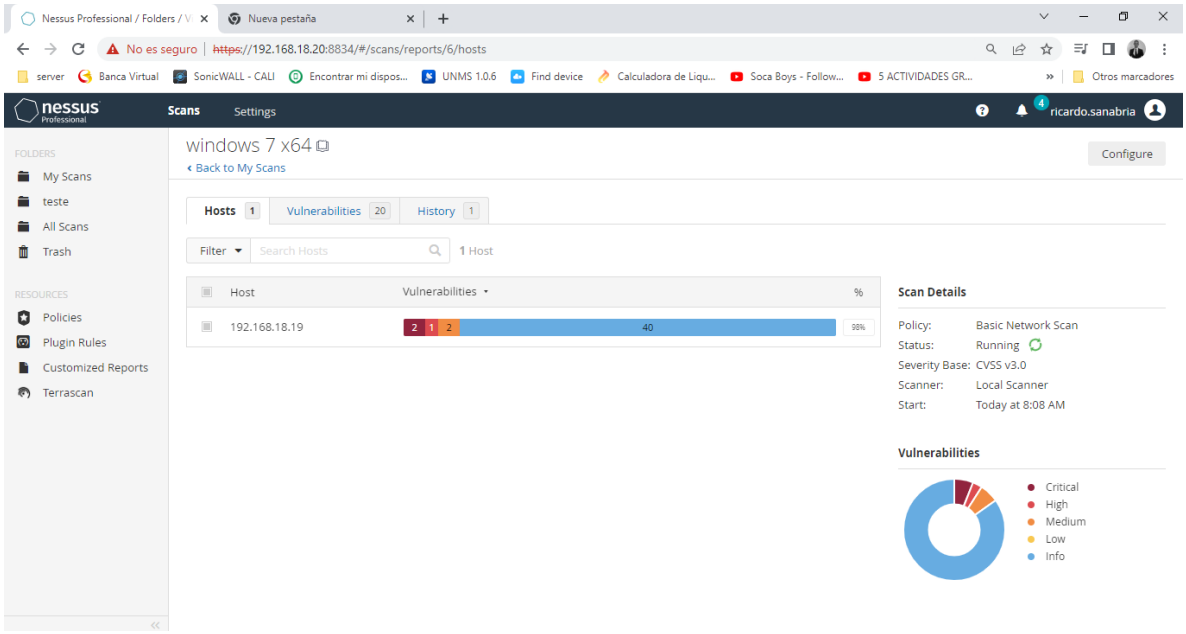
Figura 31 Web Nessus



Fuente: Propia

Adicionamos el escaneo de vulnerabilidades a nuestro sistema objetivo

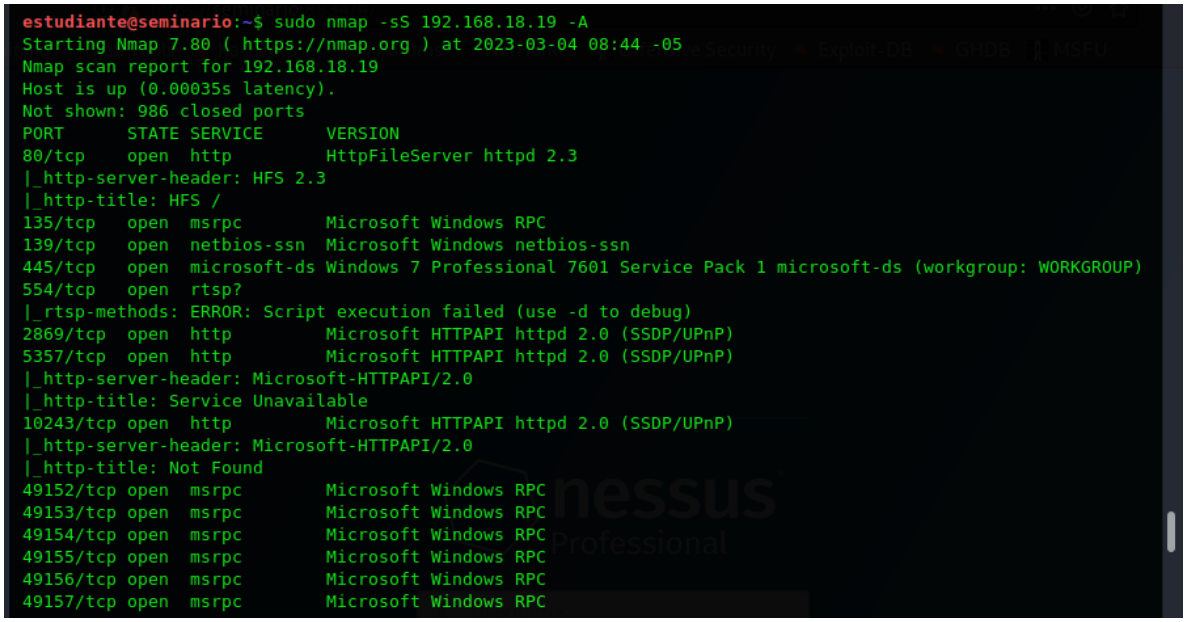
Figura 32 Identificación de vulnerabilidades



Fuente: Propia

Identificaremos los puertos con servicios publicados donde identificamos el uso de la herramienta Rejjeto HFS (HTTP File Server)

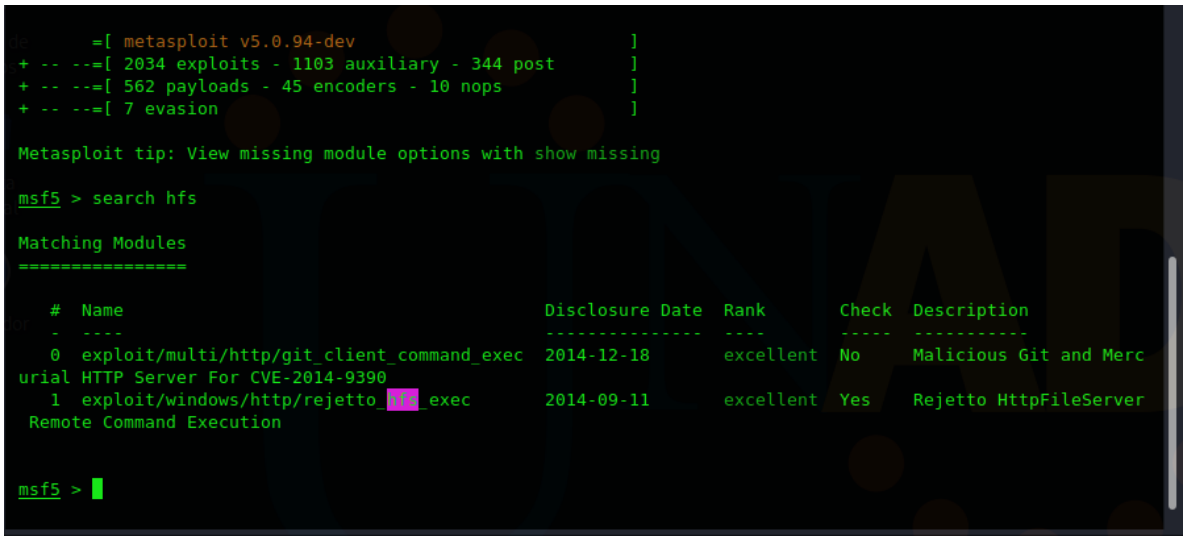
Figura 33 Identificación de puertos y servicios



Fuente: Propia

Creación de usuario en maquina objetivo
Con la ayuda de Metasploit hacemos la busqueda del rejetto_hfs usando el comando search hfs

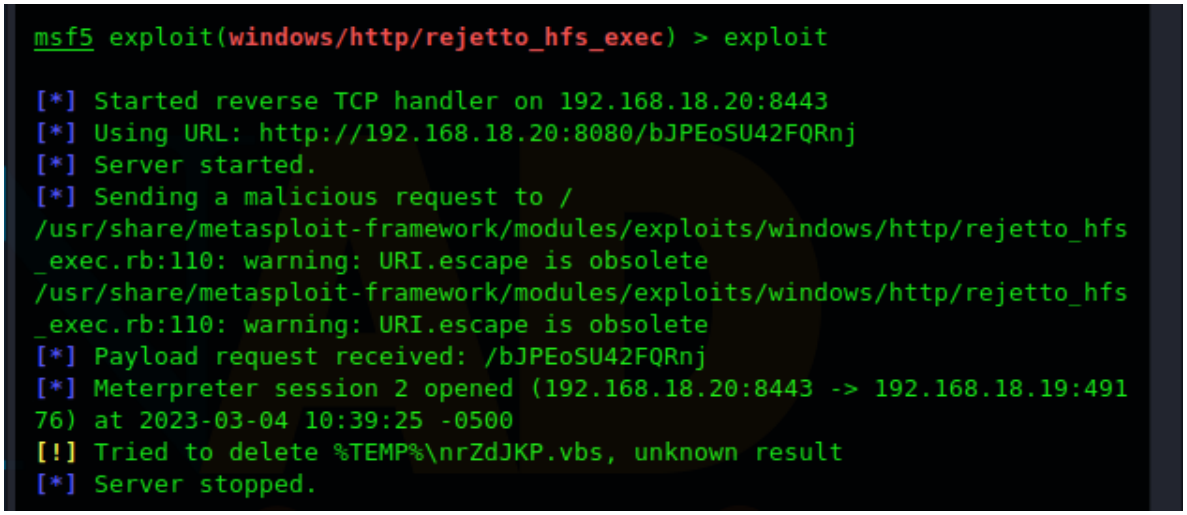
Figura 34 Metasploit



Fuente: Propia

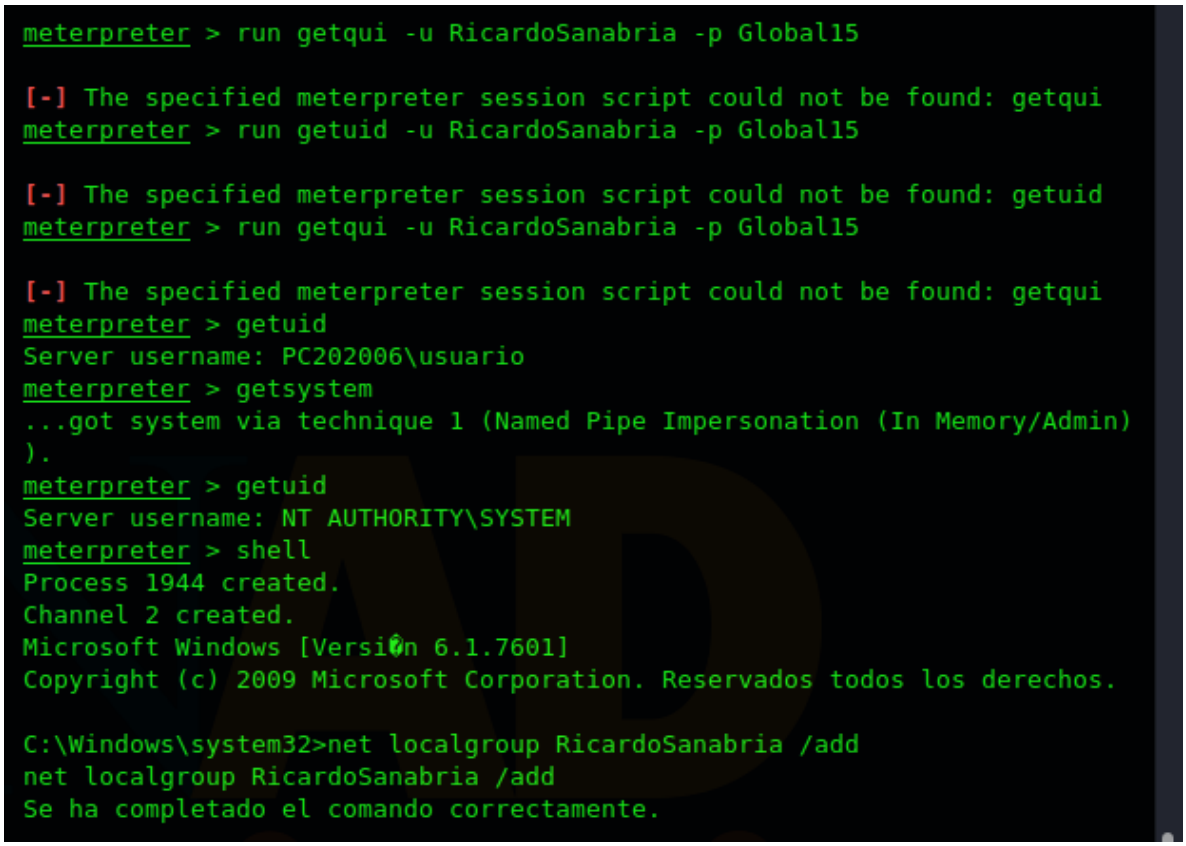
Los parámetros necesarios son los siguientes
IP Atacante: 192.168.18.20
IP objetivo: 192.168.18.19

Figura 35 Exploit



Fuente: Propia

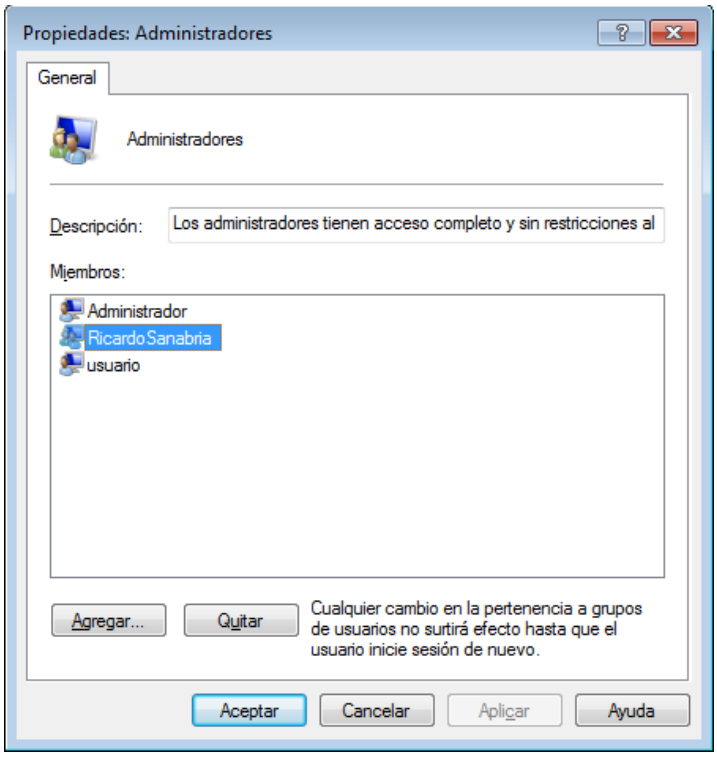
Figura 36 Meterpreter



Fuente: Propio

Con los comandos utilizados anteriormente se da por creado el usuario y los permisos de administrador.

Figura 37 Usuario Creado



Fuente: Propio

Se evidencia la creación del usuario RicardoSanabria y agregado al grupo de Administradores.

ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

Los ataques cibernéticos son creados y propagados con retorno inmediato hacia el atacante, es decir posterior de ser activado un ataque, los sistemas quedan infectados y bloqueados generando fuga de información según sea el propósito del ataque; si el ataque es para tráfico de información o bloqueo de equipo. Si se logra identificar un aumento de tráfico por determinado puerto, segmento de red o equipo especifico, si aún se tiene control de la administración de la red se podría detener el tráfico que se está generando.

Al presenciar un ataque en tiempo real se podría indagar en el tipo de ataque que se está presentando, esto ayudaría a tomar información de primera mano para la investigación de la solución. Técnicamente no sabemos de donde proviene el

ataque cibernético, pero se puede ir descubriendo a medida que se atribuyen el ataque o lugar de mayor impacto; en este punto se conoce como fase de contención permitiendo detener y evitar la propagación del ciberataque.

Contener un ataque mediante control de tráfico desde el firewall de red es pertinente para aislar la maquina o segmento de red afectada permitiendo tener la administración de los tráficos normales que se presentan, ahora bien, si una maquina presenta síntomas de estar infectada y propagando tráfico inusual se puede separar físicamente de la red, reestablecer los servicios de seguridad entre antivirus y antimalware para lograr rescatar y prevenir la perdida de la información.

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

Las medidas de hardenización que se propone para no repetir el ataque registrado en la maquina serían las siguientes:

-. Mantener actualizado el sistema operativo tanto la versión de software como su actualizaciones periódicas.

-. Restringir el uso de aplicaciones que abran puertos web dejando vulnerables los servicios publicados.

-. Establecer y cumplir las políticas de seguridad informática que estipulen los lineamientos de uso.

-. Activar y configurar correctamente las reglas de firewall, antivirus y software de protección o alertas de vulnerabilidades.

-. Habilitar política que restinga la instalación de aplicaciones en el equipo.

-. No abrir archivos o ejecutar programas desconocidos ya que se estaría permitiendo la apertura de puertos o virus que afectan el sistema.

-. Realizar backup periódicos de la información.

-. Verificar los permisos que tienen los usuarios registrados en el equipo, garantizando que roles sean asignados por el administrador del sistema y no modificados por el usuario.

-. Controlar y cerrar puertos de red que no se están utilizando.

-. Monitorear el tráfico de la red para determinar las cargas que se está recibiendo y emitiendo.

-. Capacitar a los usuarios locales sobre el buen uso que se le deben dar a los recursos del sistema

4.3. ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Los equipos Blue Team analiza los sistemas de información para determinar cualquier falencia que pueda vulnerabilidad la seguridad de la información, reúne información para advertir y garantizar la proteccion efectuando una evaluación de riesgo.
La defensa de los Blue Team se marca de manera proactiva realizando vigilancia periódica de los recursos de la red, analizando procesos y comportamientos que se tornan poco comunes y que logren alterar el correcto funcionamiento del sistema.
Como objetivo principal

Los equipos de respuesta a incidentes informáticos, basado en las siglas CERT es un centro especializado en dar respuestas a incidentes de seguridad en la tecnología de la información. Recopila información y estudia ataques de red ya realizados respondiendo a incidentes recibidos, como se indica este equipo responde a incidentes ya sucedidos denominado actuación reactiva.
Dentro de la respuesta ante incidentes del equipo se presenta la investigación del origen del ataque, como se produjo, restablecimiento de los sistemas y gestionar las vulnerabilidades detectadas.

Las diferencias entre un equipo BlueTeam y un equipo de respuesta a incidentes informáticos es que Blue Team actúa de forma preventiva al analizar los sistemas, detectar vulnerabilidades y solucionarlas, mientras que los equipos de respuesta a incidentes informativos actúan de forma reactiva analizando lo sucedido, repararlo y estudiar las vulnerabilidades futuras.

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

Sabemos que el equipo Blue Team trabaja de forma preventiva identificando vulnerabilidades, reportando y corrigiendo para hacer de la red más segura, los CIS center for internet security se encargan de desarrollar, validar y gestionar protecciones que garanticen la seguridad de los sistemas de información personal, empresarial y de gobiernos, para protegerlos de amenazas cibernéticas, desarrollando recomendaciones que permiten la seguridad de la red.

Utilizaría el CIS con el fin de mejorar la seguridad de la red informática mediante el desarrollo, validación y fomento de soluciones que mejoran el uso de los sistemas de información para evaluar vulnerabilidades, realizar monitoreo periódico que permite descubrir amenazas y mejorar la seguridad de la red.

Centralizados en analizar las vulnerabilidades mediante bases reportados por los miembros del CIS implementando buenas prácticas de seguridad informática para las organizaciones.

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

La información sobre seguridad y gestión de eventos SIEM, es un sistema de seguridad que pretende dar respuesta rápida directa ante cualquier amenaza cibernética en los sistemas de información, los SIEM tienen control sobre eventos de seguridad que suceden dentro de las organizaciones que monitorea patrones anormales que permiten la identificación de vulnerabilidades.
Los sistemas SIEM se diseñó para reforzar e incrementar los niveles de seguridad de las organizaciones donde se proporciona la seguridad de los sistemas de información.

Las funciones principales de SIEM es recopilar, almacenar e interpretar los registros que se realizan en tiempo real que permite actuar de formar inmediata ante cualquier evento de seguridad informática.
Construir una base de datos en la principal función de SIEM para lograr un análisis y detención de tendencias y lineamientos de comportamiento de sistemas de información.
Monitorear amenazas que impactan los sistemas de información para garantizar el funcionamiento de los sistemas tanto de hardware como del software.

Las características de SIEM:
-. Centralizar la detección de vulnerabilidades que ayuden a responder efectivamente ante eventos presentados.

-. Encaminar los incidentes a los expertos calificados para dar respuesta rápidamente.

-. Analizar y clasificar las amenazas reportadas para identificar si son reales.

-. Evaluar los reportes de incidentes para documentar rápidamente las soluciones.

-. Documentar y alimentar la base de datos de vulnerabilidades que permiten compartir el conocimiento y métodos de solución.

-. Minimizar los ataques informáticos.

-. Dar cumplimiento a la conservación de proteccion de datos personales.

4.6. 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.

Firewall

La implementación de un firewall agrega niveles de seguridad altos a la red donde se implementa doble filtro de firewall agregando niveles virtualizados que mejoran los servicios de contención de ataques informáticos, con esto se controla todo el tráfico de la red, monitoreando su flujo tanto de entrada como de salida estableciendo esquemas de seguridad y priorización de datos.

La herramienta recomendada es Pfsense es una solución open Source que cuenta con kerner personalizado y que se puede instalar y configurar de forma fácil y guiada, tiene ventajas de administración de red y control de tráfico con monitoreo avanzado de red.

DMZ

La configuración de una Zona DMZ es viable para la separación de los servicios esenciales que son publicados a internet, implementando un servidor proxy que haga las veces de pasarela entre la red pública y los servidores internos de red de la entidad.

IDS/IPS

Resaltando la transformación que tiene los ciberataques, es muy importante que el tráfico de la red sea analizado detalladamente para determinar paquetes sospechosos, para eso es importante implementar una protección denominada IDS/ISP que compara el tráfico con firmas publicadas en bases de datos dando como resultado liberación o retención de paquetes.

Los sistemas IDS/ISP de detección y prevención de intrusos garantizan que la información que se está procesando esté protegida ya que descubren y detienen las amenazas internas de la red.

Un IDS significa sistema de detección de intrusiones, detecta vulnerabilidades en los sistemas de información su función es detectar e informar, este sistema no toma medidas correctivas en tiempo real, se centra en ser un sistema de monitoreo.

Un IPS son el complemento a la protección de IDS estos bloquean amenazas además de detectarlas se caracteriza por ser una protección adicional al cortafuego configurado en la misma red y su función es analizar y tomar decisiones automatizadas dentro de la red de datos.

La función de la detección y prevención de intrusos se basa en dos métodos, detección basada en la firma y la detección basada en las anomalías estadísticas.

La detección basada en la firma busca las vulnerabilidades en una base de firmas previamente almacenadas y ya documentadas, y en vulnerabilidades aleatorios comparados con sistemas en tiempo real.

El software recomendado es Snort protege y se construye con códigos abiertos, implementa reglas que permite la detección de actividades maliciosas y encuentra paquetes para generar alertas.

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

Los equipos Red Team y Blue Team cuentan con un amplio conocimiento de estrategias que conlleven a la seguridad informática dentro de las estrategias podemos detallar el constante análisis y busqueda que se dan a los sistemas de información para descubrir vulnerabilidades, esto permite resaltar el compromiso que se tiene para lograr conservar la información.

La pronta divulgación de los hallazgos que tengan los equipos Red Team y Blue Team consolidan una efectividad en la proteccion de los sistemas de información en los que se pueda evitar ser atacados basados en reportes históricos y bases de datos publicadas, esto hace que todo el trabajo realizado por los equipos de seguridad dé frutos.

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

-. La seguridad de la información es primero sin permitir ninguna excepción.
-. Mantener los equipos actualizados tanto en su versión de firmware como firmas de seguridad.
-. Disponer de copias de seguridad constantes que permitan tener la información disponible.
-. Utilizar métodos de doble autenticación para las contraseñas.
-. Limitar los accesos a los servidores con tiempo de inactividad.
-. Disponer de sistemas de detección de vulnerabilidades.
-. Disponer de protección de antivirus actualizado.
-. Configurar filtros de DNS.

LINK SUSTENTACIÓN

https://youtu.be/1MpD9ne7vZQ

CONCLUSIONES

Se presenta de manera precisa los resultados que se obtuvieron con el desarrollo de los objetivos propuestos; detallando temas relevantes a la contención y prevención de ataques cibernéticos.

Las empresas deben dar importancia al análisis de trafico de red para prevenir ataques cibernéticos, implementando estrategias utilizadas por los equipos Blue Team para anticipar y fortalecer la seguridad de la información.

BIBLIOGRAFÍA

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (2020). Política Nacional de Confianza y Seguridad Digital. (pp. 16-26, 34– 44) https://colaboracion.dnp.gov

LIZA Institute. Infraestructuras: definición, planes, riesgos, amenazas y legislación [en línea]. (28 de octubre de 2019). [Consultado: 30 de agosto de 2022]. Disponible en: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

GONZALEZ, Sol. Ciberataques a la infraestructura crítica de un país y sus consecuencias [en línea]. (10 de marzo de 2022). [Consultado: 31 de agosto de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/

TechTarget Contributor, red teaming. [en línea]. (Abril 2021). [Consultado: 28 de marzo de 2023]. Disponible. https://www.techtarget.com/whatis/definition/red-teaming

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (2020). Política Nacional de Confianza y Seguridad Digital. (pp. 16-26, 34– 44) https://colaboracion.dnp.gov

LIZA Institute. Infraestructuras: definición, planes, riesgos, amenazas y legislación [en línea]. (28 de octubre de 2019). [Consultado: 30 de agosto de 2022]. Disponible en: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

COPNIA. (09 de Octubre de 2003). *https://www.copnia.gov.co*. [en línea]. Consultado el 20 de febrero de 2023, de https://www.copnia.gov.co: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

LEY 1273 DE 2009, DIARIO OFICIAL. AÑO CXLIV. N. 47223. 5, ENERO, 2009. PÁG. 5. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

BORK, Kyle. What is the Penetration Testing Execution Standard? Triaxiom Security [página web]. (10, marzo, 2021). [Consultado el 04, marzo, 2023]. Disponible en Internet: https://www.triaxiomsecurity.com/what-is-the-penetration-testing-execution-standard/.

ASCEND TECHNICAL TEAM. 5 Qualities of a Good Penetration Test [en línea]. (14 julio de 2022) [Consultado: 29 de marzo de 2023] disponible en https://blog.teamascend.com/5-qualities-of-a-good-penetration-test

ALTUBE, Rafael. Kali Linux: Qué es y características principales [en línea]. (05 noviembre de 2021) [Consultado: 03 de marzo de 2023] disponible en https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

MARTINEZ, Edmundo. Como usar herramienta NMAP para escaneo de puertos en equipos de red. [en línea]. (05 de abril de 2022) [Consultado: 04 de marzo de 2023] disponible en https://soporte.syscom.mx/es/articles/3031807-networking-como-usar-herramienta-nmap-para-escaneo-de-puertos-en-equipos-de-red

DAZA, Santiago. Nessus ¿Cómo hallar vulnerabilidades? [en línea]. (04 junio de 2021) [Consultado: 04 de marzo de 2023] disponible en https://behacker.pro/nessus-como-hallar-vulnerabilidades/

Ramiro, Ruben. 25 Tipos de ataques informáticos y cómo prevenirlos [página web]. (20, enero de 2018). [Consultado el 18 de marzo 2023]. Disponible en Internet: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

METDATA. ¿QUÉ HACER EN CASO DE UN CIBERATAQUE? [en línea]. (09 diciembre de 2020) [Consultado: 18 de marzo de 2023] disponible en https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

INCIBE. ¿Qué son y para qué sirven los SIEM, IDS e IPS? [en línea]. (03 septiembre de 2020) [Consultado: 21 de marzo de 2023] disponible en https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips