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

OSCAR ANCÍZAR CARRILLO URIBE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE INGENIERÍA DE SISTEMAS, ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
MEDELLÍN, COLOMBIA
2022

ÍNDICE

Contenido

TABLA DE ILUSTRACIONES

1. RESUMEN

El presente documento se presenta como resumen del seminario especializado en RedTeam & BlueTeam, dentro de él se encontrará toda la información desarrollada durante el seminario, las diferentes etapas con su respectivo detalle.

La seguridad informática se destaca como un proceso que protege los activos informáticos de las organizaciones y en los últimos años ha cobrado gran importancia debido al impacto que han tenido los diferentes ataques informáticos en diferentes empresas, con el fin de profundizar en los conocimientos, durante el seminario se desarrolló la metodología RedTeam & BlueTeam, con el fin de poder implementarla y conocer las diferentes aplicaciones y métodos de uso.

Con este trabajo se quiere resumir el desarrollo del seminario y de esta manera capturar el conocimiento desarrollado, con el fin de poder establecer un marco de referencia que nos permitirá aplicar estos conocimientos en el mundo real.

2. INTRODUCCIÓN

Teniendo en cuenta que la información se ha convertido en uno de los activos más importantes de las empresas, su transmisión a través de diferentes medios se hace muy importante para el correcto uso de estos, las redes de datos se han utilizado para acortar distancias y aprovechar de manera ágil y eficiente el procesamiento de datos por parte de las organizaciones.

La ciberseguridad tiene una gran cantidad de componentes que la hacen una parte muy complicada en el manejo de una organización, tiene componentes humanos, técnicos, económicos y tecnológicos, adicionalmente el impacto de un incidente de seguridad es catastrófico, ya que el 60% de las empresas cierran a los 6 meses luego de ser víctimas de un ciberataque[1].

Siendo una parte tan importante en el manejo de activos informáticos de las empresas, se hace necesario el proteger de accesos indeseados este recurso, garantizando los 3 pilares de la seguridad de la información, confidencialidad, integridad y disponibilidad, para de esta manera ofrecer a los usuarios acceso a los mismos.

En el presente desarrollaremos las diferentes estrategias BlueTeam & RedTeam, con el fin de profundizar los conocimientos en el tema y desarrollar estrategias que mejoren la ciberseguridad de las organizaciones.

[1] JOHNSON, Robert. (2019). 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked. {En línea}. Fecha {02 de enero de 2019}. Disponible en https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

3. GLOSARIO

Amenazas

Peligro latente de que un evento de cualquier origen sea explotado por un atacante utilizando medios tecnológicos., 13, 32, 35, 36, 37

Ataque informático

Cuando se explota una vulnerabilidad del sistema por parte de alguien que busca algún tipo de beneficio, utilizando herramientas informáticas o explotando deficiencias en seguridad., 36, 39, 40

BlueTeam

Blue Team (seguridad defensiva)

es el equipo de seguridad que defiende a las organizaciones de ataques de una manera proactiva., 6, 8, 38, 40

Pentesting

Una prueba de penetración puede determinar cómo un sistema reacciona a un ataque, si las defensas de un sistema pueden ser violados, y qué información puede ser adquirido desde el sistema, 10, 11, 12

RedTeam

Un Red Team es un ejercicio, el cual consiste en simular un ataque dirigido a una organización, lo que se traduce que un grupo de personas internas o externas a la empresa, comprueban la posibilidad de tener acceso a los sistemas, comprometerlos y el impacto que esto podría tener en el negocio., 6, 8, 38, 40

Riesgos informáticos

Es cualquier activo o sistema que es susceptible de ser atacado, estos deben ser identificados y mitigados efectivamente., 12

Vulnerabilidad

Es una debilidad que tiene el sistema y que puede llegar a ser explotado por un atacante determinado., 4, 12, 13, 26, 27, 29, 32

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Conocer a profundidad las estrategias RedTeam y BlueTeam, con el fin de aplicar dichos conocimientos en el ámbito laboral y de esta manera proteger efectivamente los activos informáticos de una organización.

4.2. OBJETIVOS ESPECÍFICOS

- Resumir el desarrollo de las diferentes actividades del diplomado.
- Definir aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.
- Establecer recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización
- Elaborar conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

5. DESARROLLO DEL INFORME

5.1. ETAPA 1: CONCEPTOS DE SEGURIDAD

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.

Para la protección de datos personales se creó la Ley 1581 de 2012[2], denominada “Por la cual se dictan disposiciones generales para la protección de datos personales.”, esta Ley establece principios para la protección de datos, define los términos generales de los datos y su protección, establece derechos y deberes entre las personas que administran datos personales, define los procedimientos que se deben realizar para la protección de los datos personales, delega en la Superintendencia de Industria y Comercio la responsabilidad para la protección de los datos.

Además, establece sanciones para aquellas entidades que no realicen un correcto manejo de los datos, crea el Registro Nacional de Bases de Datos y regula la transferencia de datos a otros países.

Esta Ley ofrece un buen nivel de protección de datos para los ciudadanos colombianos y les brinda herramientas suficientes para proteger su información, dando como resultado varias sanciones contra empresas que no han cumplido las normas.

Sobre delitos informáticos existe la Ley 1273 de 2009[3] que agrega al código penal los siguientes delitos sobre activos informáticos:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.

---

[2] Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Senado de la República de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[3] Ley 1273 (2009). Modificación al Código Penal. Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Adicionalmente se agregan circunstancias de agravación punitiva que incrementa las penas cuando se presentan las siguientes condiciones:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Y para cualquier tipo de delito ya establecido en el código penal “Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.”

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.

El siguiente es el proceso estandarizado de pentesting:

1. **Planeación y reconocimiento:**

Definición del alcance y los objetivos de una prueba, incluidos los sistemas que se abordarán y los métodos de prueba que se utilizarán.

Recopilación de inteligencia (por ejemplo, nombres de red y dominio, servidor de correo) para comprender mejor cómo funciona un objetivo y sus posibles vulnerabilidades.

Herramienta utilizada:

Zmap: Zmap es un escanner de la red que permite identificar los equipos que pertenecen a una red determinada, con la dirección IP se puede recolectar información de base para el pentesting.

2. **Escaneo:**

En esta etapa se realiza un escaneo de las posibles vulnerabilidades del sistema, tanto del código, como de la red, esta fase es la más importante, ya que detectando las vulnerabilidades es como se puede realizar un ataque con mucho más impacto.

Herramienta utilizada:

NMAP/ZenMap: Esta herramienta permite realizar una detección de todos los puertos en cualquier red, lo que permite identificar posibles objetivos para nuestro ataque.

3. **Ganar acceso:**

De acuerdo con las vulnerabilidades detectadas en el escaneo, los pentesters explotan dichas vulnerabilidades y ganan acceso al sistema, además de buscar la posibilidad de escalar los privilegios con el fin de profundizar el ataque.

Herramienta utilizada:

sqlmap: Esta herramienta permite utilizar inyección SQL para tomar el control de un servidor de base de datos, se puede utilizar tanto en Windows como en Linux, y es una herramienta con una gran cantidad de funciones para atacar diferentes motores de bases de datos.

4. **Acceso Persistente:**

Luego de ganar acceso al sistema, la idea es lograr mantenerlo por el mayor tiempo posible, con el fin de obtener el mayor nivel de privilegios y lograr acceso a la mayor cantidad de sistemas posibles. Esto con el fin de simular un ataque real en el que el atacante permanece en el sistema por mucho tiempo.

Herramienta utilizada:

Kali Linux: Esta distribución de Linux creada específicamente para el pentesting cuenta con gran cantidad de herramientas que permiten realizar todo el proceso de pentesting desde un solo computador, todas las herramientas son opensource y permiten una configuración extendida.

5. **Análisis y Reporte:**

En esta etapa se entregan todos los resultados de las diferentes fases, vulnerabilidades, nivel de impacto, activos afectados, el tiempo que cada pentester estuvo conectado sin ser detectado y qué medidas se deben tomar para disminuir la vulnerabilidad del sistema ante los ataques, identificando de esta manera los riesgos informáticos.

Herramienta utilizada:

Microsoft Word: Se entrega un informe en archivo de texto con toda la información detallada.

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 un framework de herramientas que permite escribir, testear y ejecutar código malicioso, está desarrollada en Ruby y contiene un conjunto de herramientas que permite testear vulnerabilidades, ejecutar ataques y permanecer invisible.

• Nmap: Es una herramienta de escaneo de redes, que permite detectar los dispositivos conectados a una red y obtener información sobre el tipo de dispositivos y sistema operativo de cada uno, esto con el fin de generar un mapa del objetivo que se pretende atacar.

• OpenVas: Es una herramienta que permite descubrir vulnerabilidades en los sistemas, contiene varios tests predeterminados y una interfaz web. Al ser una herramienta open source, cuenta con una gran cantidad de colaboradores, lo que permite corregir falsos positivos de manera ágil y eficaz.

Servicios en línea:

• ExploitDB: Es una base de datos con diferentes exploit encontrados, permite a los especialistas en seguridad mantenerse actualizados con las diferentes vulnerabilidades en diferentes sistemas de manera que puedan estar al día con los posibles ataques y poder remediarlos.

• CVE: Common Vulnerabilities and Exposures, es un sistema desarrollado por el MITRE que permite asignar un ID a una vulnerabilidad detectada e identificada correctamente,permite unificar conceptos para unir esfuerzos en la mitigación de dichas amenazas

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:

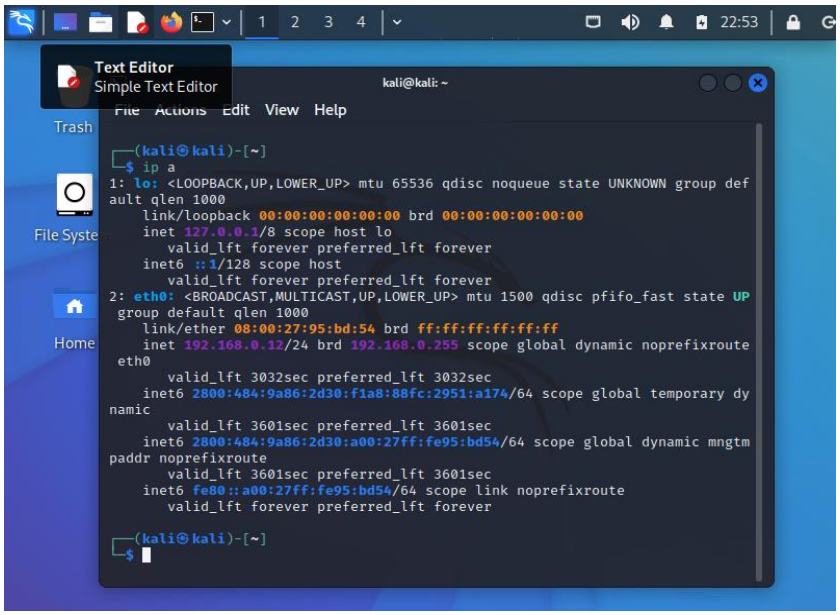
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

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. • 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.

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

1. Se ve que el equipo con Kali que tiene la dirección IP 192.168.0.12. Ilustración 1.

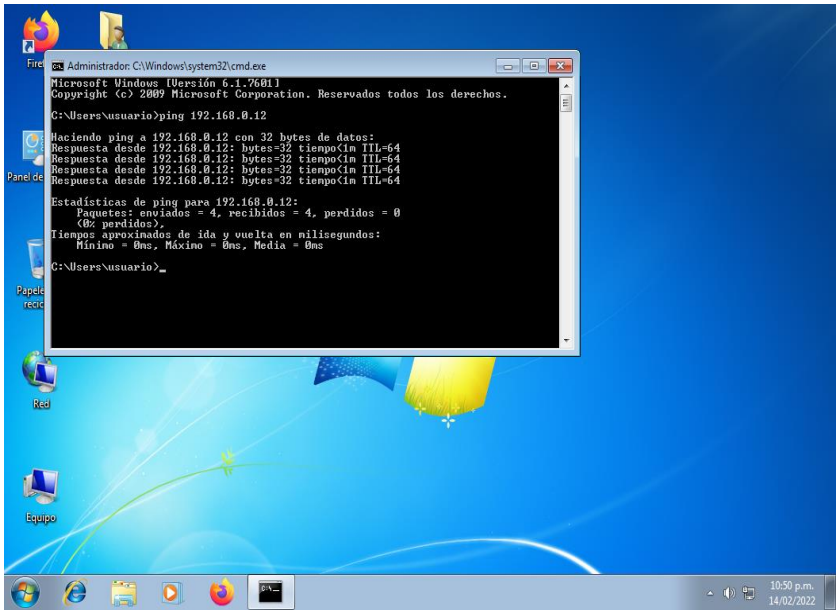
Ilustración 1 Dirección IP del equipo Kali



Fuente: Autor

2. Aquí el primer equipo Windows hace ping al equipo de Kali. Ilustración 2.

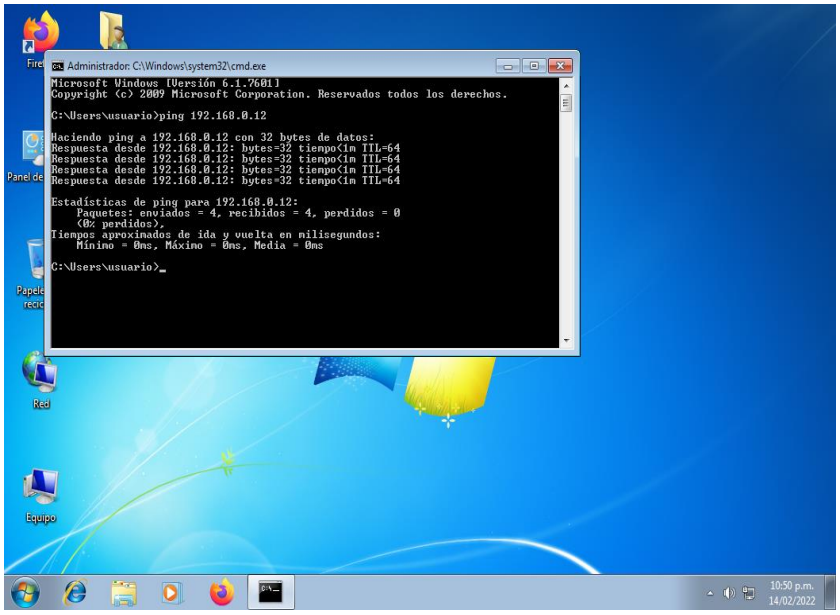
Ilustración 2 Verificación de ping entre equipos configurados.



Fuente: Autor

3. Aquí se ve al segundo equipo Windows haciendo ping al equipo con Kali. Ilustración 3.

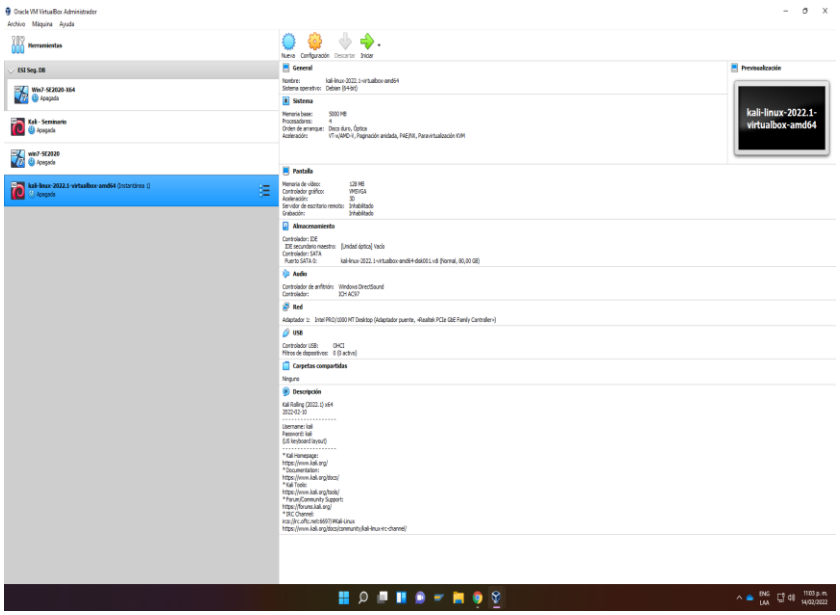
Ilustración 3 Dirección IP del segundo equipo con Windows 7.



Fuente: Autor

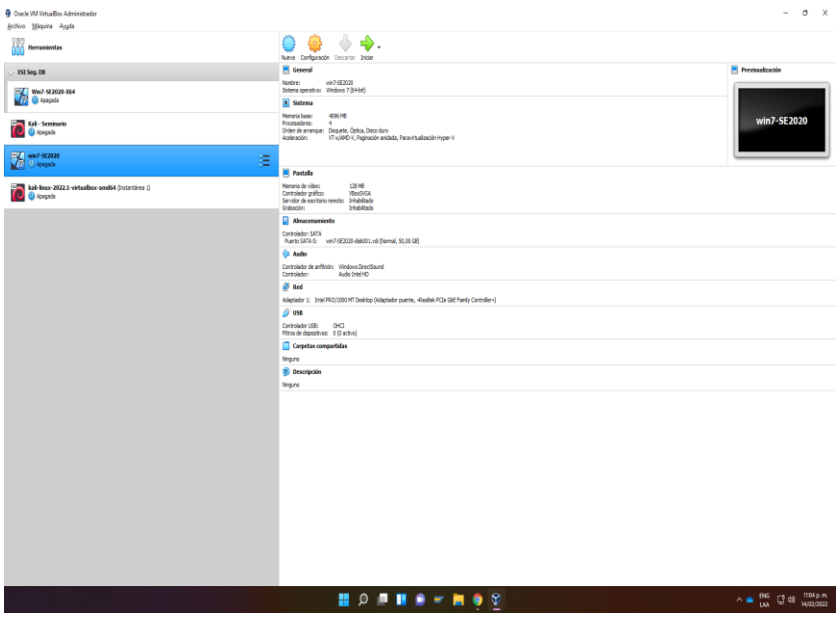
4. Aquí se pueden ver las características técnicas del hardware donde se corren las máquinas virtuales. Ilustración 4, 5 y 6:

Ilustración 4 Características del equipo Kali.



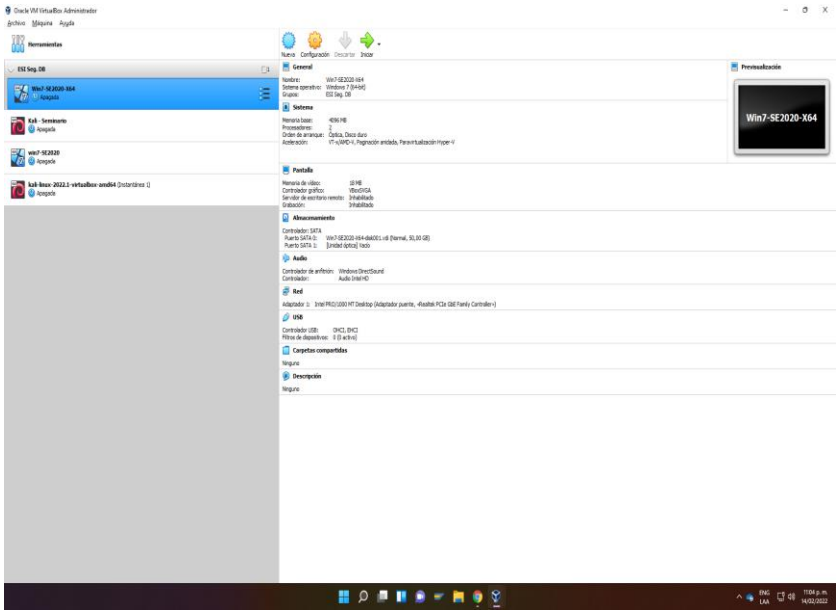
Fuente: Autor

Ilustración 5 Características del equipo Windows 7.



Fuente: Autor

Ilustración 6 Características del Equipo Windows 7x64.



Fuente: Autor

5.2. ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

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.

Teniendo en cuenta que la Ley 842 de 2003[4] establece en el artículo 31 los deberes generales de los profesionales, entre los que se encuentra:

(f) Denunciar los delitos, contravenciones y faltas contra este Código de Etica, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;

[4] Ley 842 de 2003. Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Los siguientes puntos del acuerdo de confidencialidad con Whitehouse Security son ilegales y no se pueden aceptar, ya que, si se hace, se corre el riesgo de perder la licencia profesional.

Cláusula Primera:

“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.”

El punto 2 de la cláusula 2 que dice:

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”.

Cláusula 4a. punto 3, 4 y 9:

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

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

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.

Teniendo en cuenta la información consignada se puede inferir que los delitos que comete Whitehouse Security son los siguientes:

- Acceso abusivo a sistemas informáticos.
- Interceptación de datos informáticos.
- Violación de datos personales.

Además de otras que se enuncian cuando hablan sobre procesos ilegales, por lo que teniendo en cuenta la Ley 1273 de 2009[5], se evidencia un gran entramado ilegal de actividades que ponen en riesgo al Ingeniero que firme este acuerdo, lo que lo puede poner en riesgo a condenas que van desde los 4 a 8 años por cada delito cometido.

Adicionalmente la Cláusula 8a establece:

Octava. Solución de controversias: Las partes (nombre estudiante

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

Es decir, la empresa Whitehouse Security se lava las manos de todo el proceso legal que pueda ocurrir en el caso de que los delitos sean denunciados.

¿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.

Teniendo en cuenta que la empresa viola el código de ética del COPNIA, al solicitar al firmante que oculte delitos, que se puede inferir que se van a cometer durante la ejecución del trabajo y que, además, la empresa se lava las manos de apoyo legal y hace completamente responsable al ingeniero, **no es recomendable firmar ese contrato**, ya que probablemente le cueste su título y tiempo en la cárcel.

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.

[5] Ley 1273 (2009). Modificación al Código Penal. Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

Según lo que se pude leer de la Operación Andrómeda Buggly en la revista enter.co[6], esta operación fue lanzada por el ejército con el fin de obtener información sobre herramientas para el hacking ético, sin embargo, la misma se salió de control y terminó con 3 personas que fueron enviadas a la cárcel por la venta de secretos del estado, espionaje y violación de datos personales.

Siendo una operación militar, esta se encuentra protegida por el derecho militar y las acciones realizadas para proteger la seguridad nacional, sin embargo, lo grave de este tema es que se vendió información secreta a terceros por parte de los miembros del equipo Andrómeda, lo que es totalmente grave, ya que es información confidencial, irrespetando el derecho de reserva y violando la Ley al compartir dicha información con terceros que no tenían nada que ver en el proceso.

Analizando un poco más allá, se puede ver la inocencia con la que los altos cargos militares abordaron el proceso de inteligencia utilizando hackers, ya que, al no llevar un control detallado de la información levantada y su debido manejo, lo que ocurrió era una tragedia anunciada, ya que este tipo de activos requieren un seguimiento permanente, ya que su facilidad de transporte y manejo, lo hacen un activo muy difícil de controlar.

La seguridad informática es un tema que requiere los más seguros protocolos para el manejo de información, es de vital importancia que los líderes en estos temas reconozcan la delicadeza de los procesos realizados, teniendo en cuenta que los ingenieros de seguridad transitan una línea entre la legalidad e ilegalidad, es de suma importancia que se trate con total seriedad cualquier aproximación al tema por parte de las organizaciones, especialmente aquellas que tienen tanto poder como lo son las militares.

5.3. ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN

Herramientas de software utilizadas:

NMAP: Es una herramienta utilizada para realizar rastreos en redes, permite detectar y rastrear equipos en una red, identificando servicios y puertos abiertos.

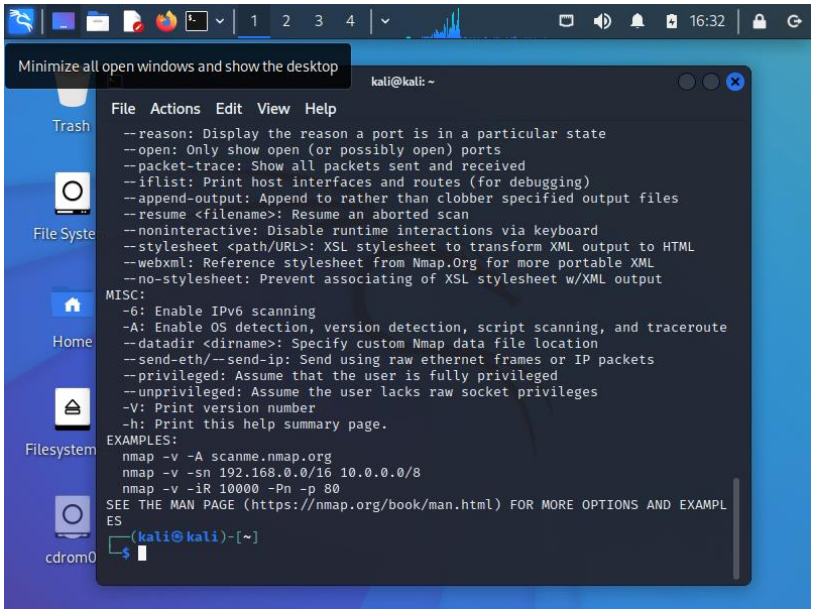
[6] Detrás de Buggly: la historia de la fachada Andrómeda (2015). Revista Enter, https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

METASPLOIT: Esta herramienta de código abierto permite detectar múltiples vulnerabilidades en los sistemas analizados.

Planeación y Reconocimiento:

Para comenzar el proceso de recolección de información, se utiliza NMAP para rastrear los equipos de la red y detectar posibles vulnerabilidades y puertos abiertos disponibles para ser accedidos. Ilustración 7.

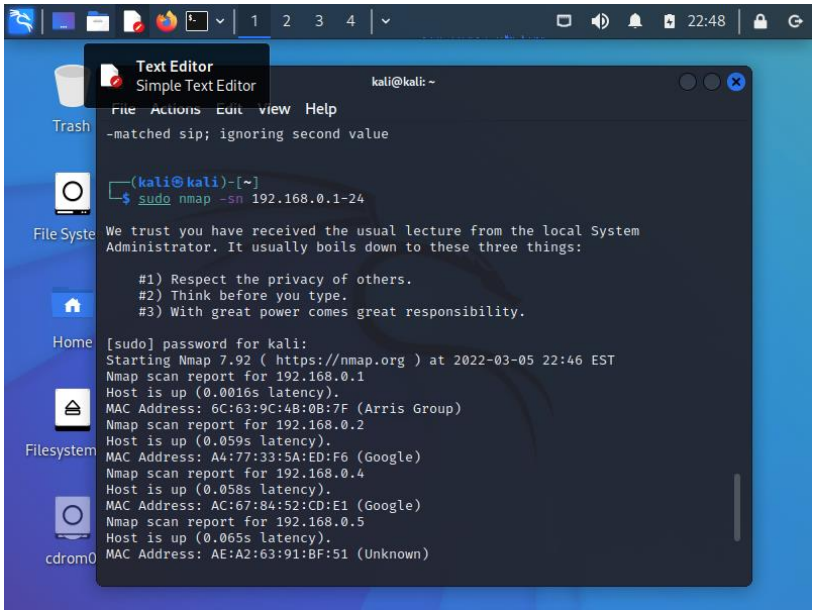
Ilustración 7 Uso de nmap.



Fuente Autor.

Se utiliza el comando sudo nmap -sn 192.168.0.1-24 para escanear las primeras 24 IP de la red, no se usa un ejemplo con un mayor número de puertos por agilidad, este comando nos muestra los equipos encontrados en este rango de direcciones y su estado. Ilustración 8.

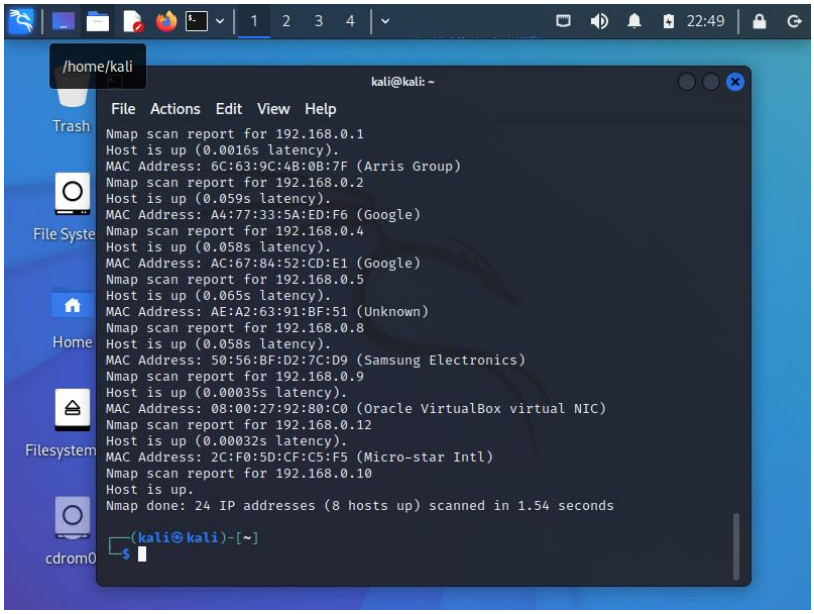
Ilustración 8 Uso de nmap.



Fuente - Autor

El que nos interesa es la máquina virtual ubicada en la IP 192.168.0.9, con lo que se verifica directamente con nmap. Ilustración 9.

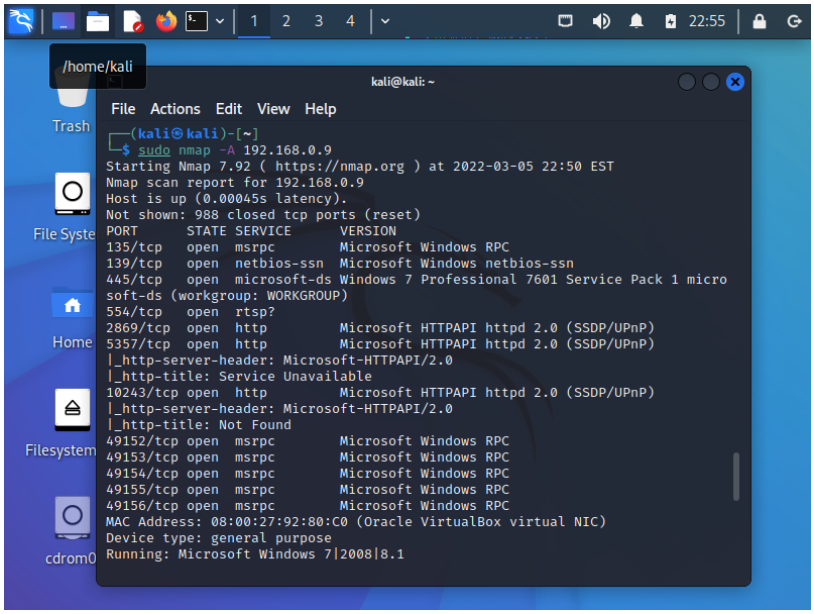
Ilustración 9 Verificación de la IP 192.168.0.9 con nmap.



Fuente - Autor

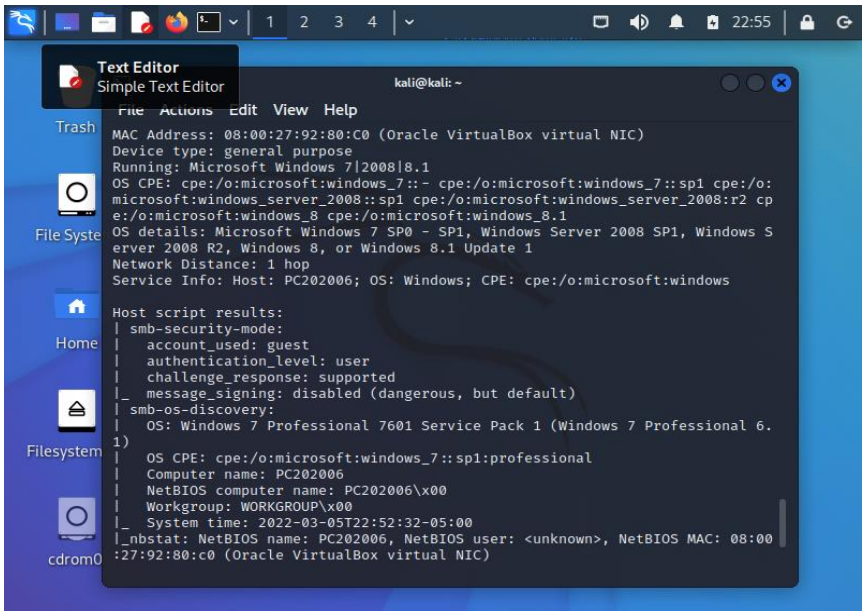
El comando sudo nmap -A 192.168.0.9 permite escanear a profundidad el equipo, detectando puertos abiertos y demás. Ilustración 10, 11 y 12.

Ilustración 10 Escaneo a profundidad de la IP 192.168.0.9 con nmap.



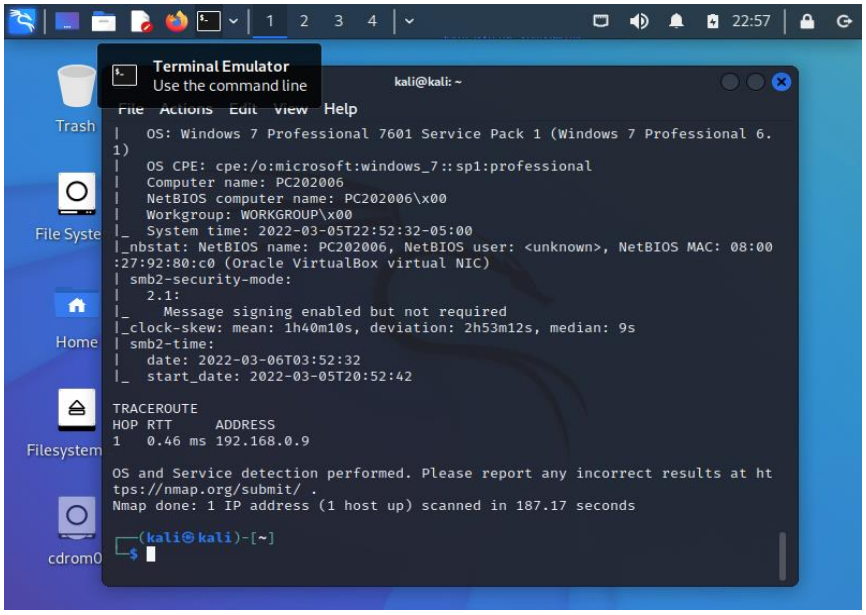
Fuente – Autor

Ilustración 11 Escaneo a profundidad de la IP 192.168.0.9 con nmap.



Fuente - Autor

Ilustración 12 Escaneo a profundidad de la IP 192.168.0.9 con nmap.

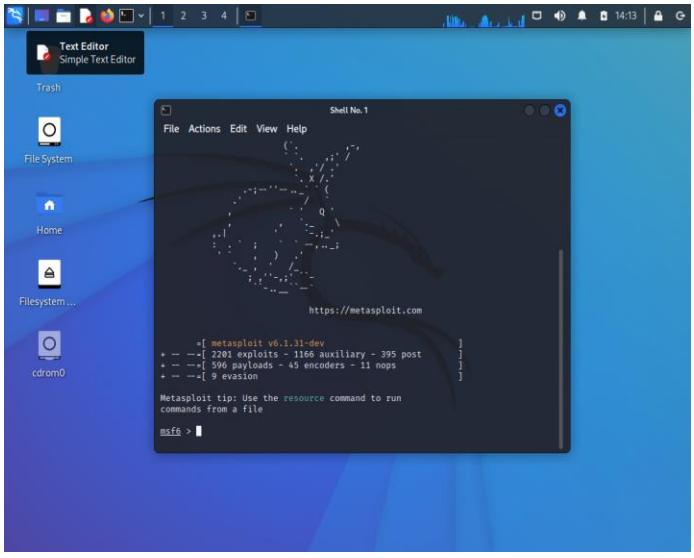


Fuente - Autor

Fase Escaneo:

Se lanza la aplicación metasploit para identificar las vulnerabilidades del sistema. Ilustración 13.

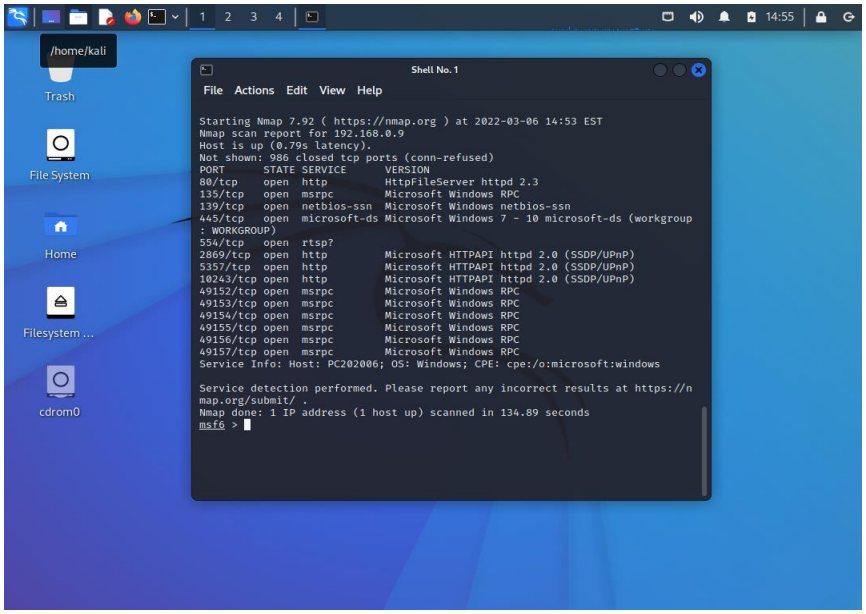
Ilustración 13 Utilización de metasploit.



Fuente - Autor

Se corre el comando nmap -sV 192.168.0.9, lo que permitirá reconocer las vulnerabilidades del equipo y si tiene alguna forma de ser explotado. Ilustración 14.

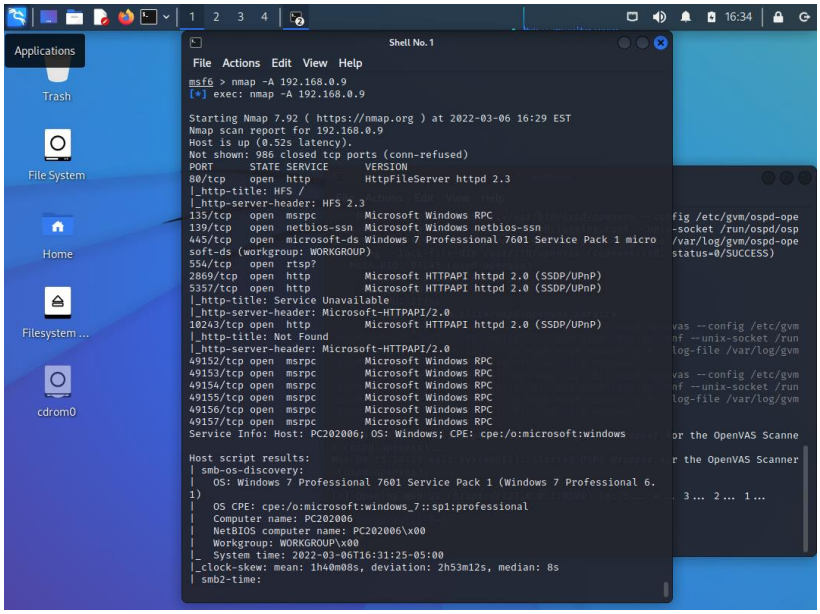
Ilustración 14 nmap utilizado desde metasploit.



Fuente - Autor

También se ejecuta el comando nmap -A para obtener información detallada de los servicios y sistema operativo.

Ilustración 15 Utilización de nmap desde metasploit.



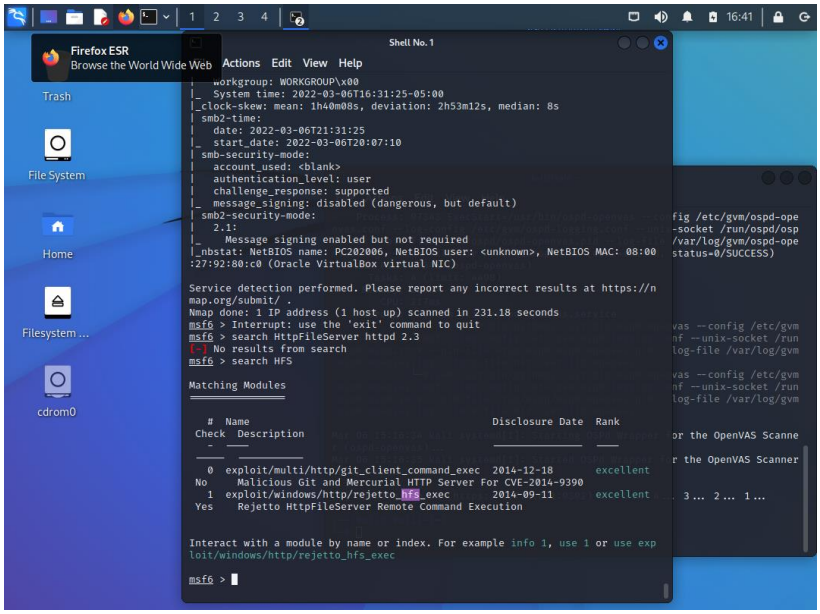
Fuente: Autor

Se detecta que el puerto 80 http se encuentra abierto y está siendo utilizado por HttpFileServer httpd 2.3 con el título HFS.

Ganar acceso:

Se busca en metasploit si existe alguna vulnerabilidad utilizando el comando search HFS, se encuentra lo siguiente. Ilustración 16:

Ilustración 16 Detección de la vulnerabilidad hfs con metasploit.

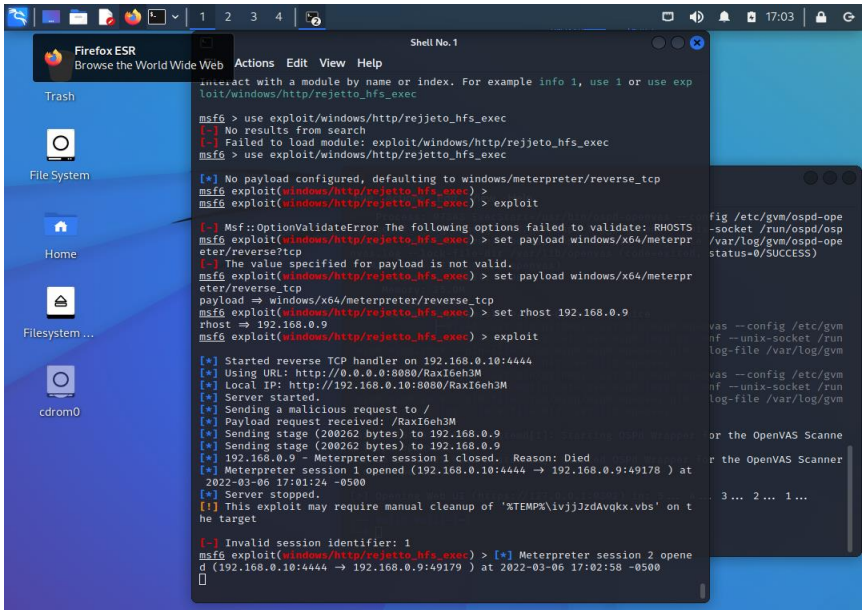


Fuente: Autor

Y se encuentra un posible exploit con rejetto_hfc_exec, para probar si se puede utilizar se corre el comando use exploit/windows/http/rejjeto_hfs_exec al momento de pedir el payload se escribe set payload windows/x64/meterpreter/reverse_tcp esto da la ruta donde se ejecutará el ataque, adicionalmente se configura el host, esto se logra con el comando set rhost 192.168.0.9, esta dirección se ubica en la etapa reconocimiento.

Cuando ya se tiene esto configurado se ejecuta el exploit con el comando exploit, lo que da el siguiente resultado. Ilustración 17:

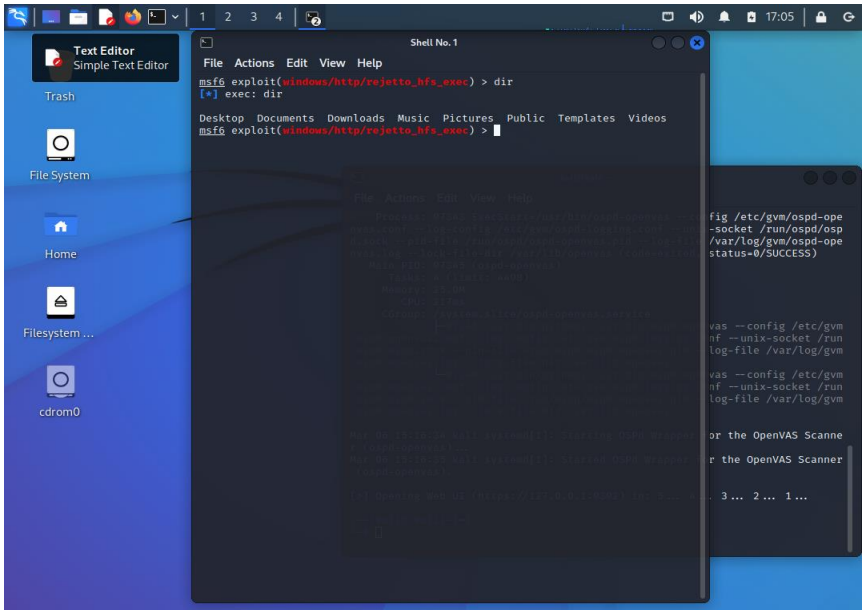
Ilustración 17 Explotación de la vulnerabilidad rejjeto hfs.



Fuente: Autor

Luego de esto se verifica que se tiene acceso al computador ejecutando el comando dir, lo que nos muestra los directorios. Ilustración 18.

Ilustración 18 Verificación del ingreso al equipo atacado mediante el comando dir.

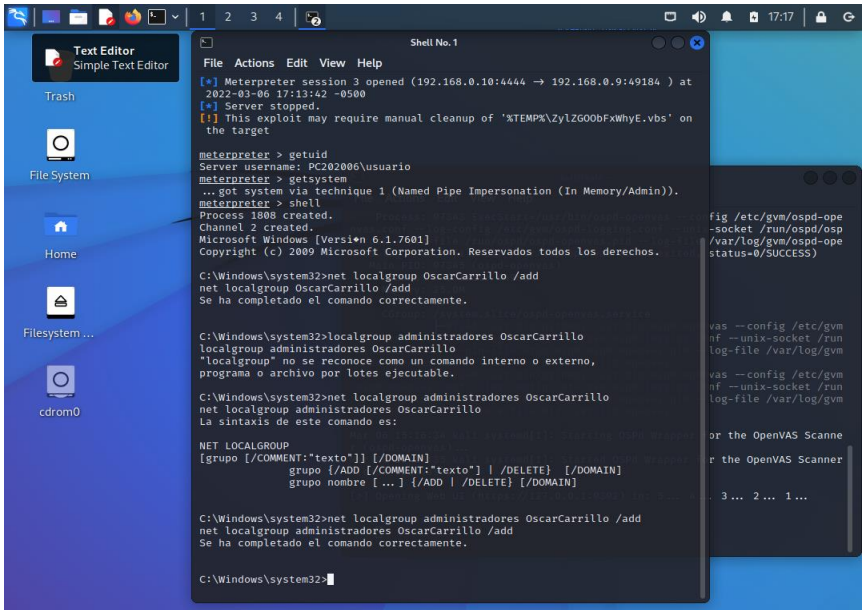


Fuente: Autor

Acceso Persistente:

Ya con acceso al equipo se puede obtener acceso persistente creando un usuario Administrador. Ilustración 19:

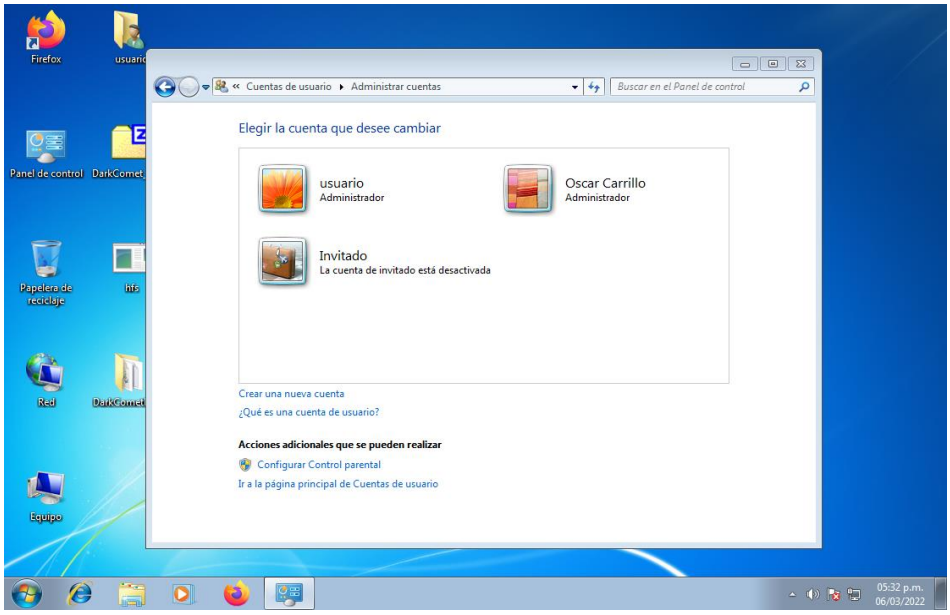
Ilustración 19 Ejecución de comandos para la creación del usuario Administrador.



Fuente: Autor

Se verifica y en el sistema Windows se ha creado el usuario satisfactoriamente. Ilustración 20:

Ilustración 20 Verificación de creación del usuario Administrador.



Fuente: Autor

Análisis y Reporte:

El pentester designado realizó el análisis y estudio de la información, tomándole aproximadamente 8 horas el lograr acceder al sistema y explotar las vulnerabilidades de este.

Se encontró una debilidad en la aplicación HFS que permite el exploit de ejecución de código remoto a través de una vulnerabilidad en el puerto 80, con dicho exploit se puede lograr acceso a la máquina con los permisos necesarios para crear usuarios con permisos de administrador y así lograr expandir los sistemas a los que se tiene acceso.

Con el fin de eliminar esta vulnerabilidad se recomienda eliminar esta aplicación y encontrar otras que cumplan las mismas funciones para eliminar dicha vulnerabilidad del sistema.

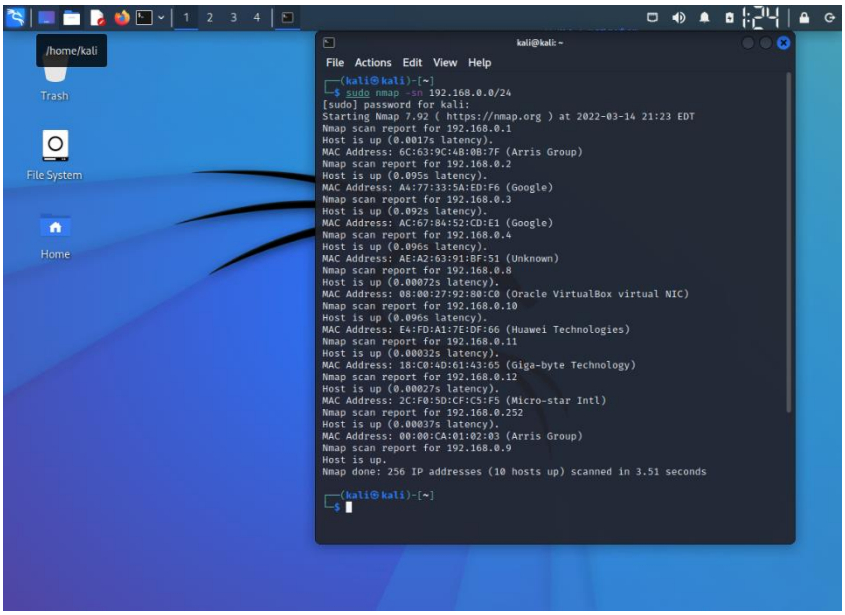
Adicionalmente se recomienda la instalación de un software antivirus y la configuración del firewall que trae por defecto Windows para minimizar la vulnerabilidad del equipo.

5.4. ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICOS

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

Identificar el estado de la red y la existencia de equipos no autorizados conectados a la misma, esto se logra con Nmap a través del comando sudo nmap -sn 192.168.0.0/24, lo que nos permite identificar los equipos, si se cuenta con un inventario de activos y direcciones IP, se puede identificar el equipo que no debe estar conectado y poder realizar procesos de mitigación. Ilustración 21.

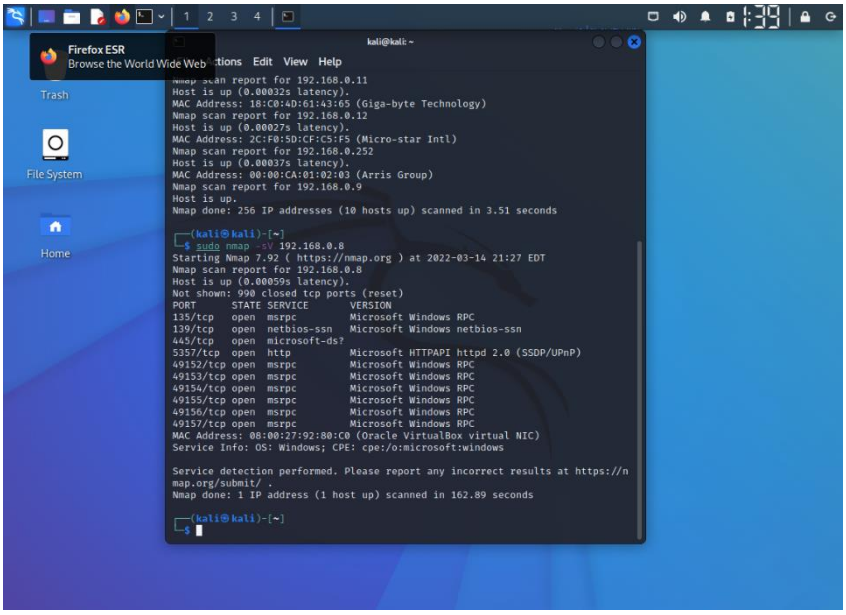
Ilustración 21 Verificación del estado de la red.



Fuente: Autor

Adicionalmente se puede utilizar el comando sudo nmap -sV 192.168.0.9 para verificar los servicios que tiene funcionando el equipo que está siendo atacado y cuál es el objetivo del ataque. Ilustración 22.

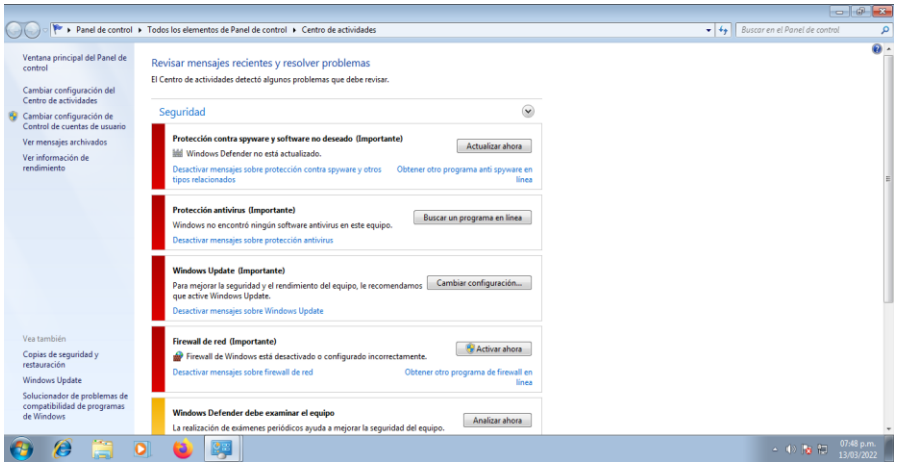
Ilustración 22 Verificación del equipo atacado.



Fuente: Autor

Adicionalmente verificar el estado del equipo que pertenece a la red y comprobar el estado del firewall y demás medidas de seguridad como el Windows Update. Ilustración 23.

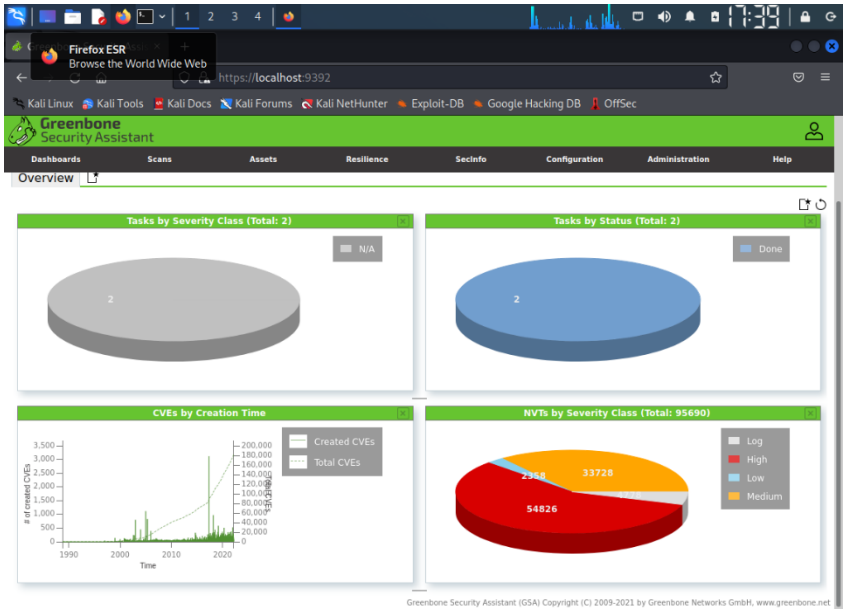
Ilustración 23 Verificación de medidas de seguridad en el equipo atacado.



Fuente: Autor

Verificar el estado de seguridad de los equipos de red, en este caso utilizar por ejemplo OPEN VAS para realizar el monitoreo de vulnerabilidades y amenazas del sistema. Ilustración 24.

Ilustración 24 Verificación de las vulnerabilidades en el equipo.



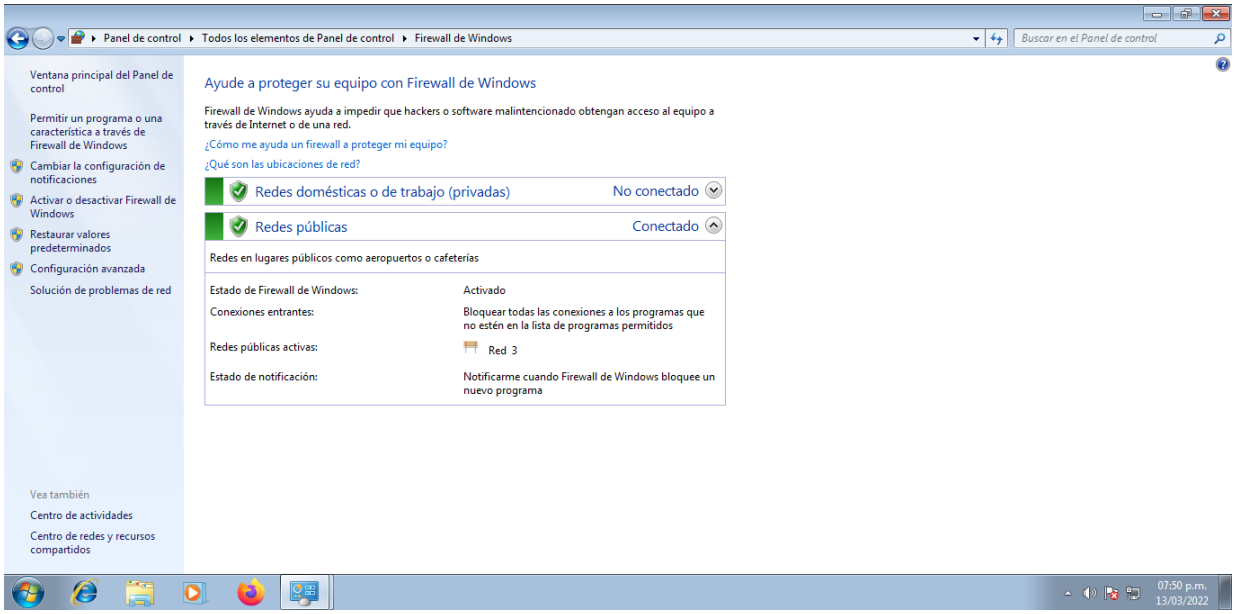
Fuente: Autor

Con base en el análisis del OPENVAS realizaría la mitigación de las amenazas más apremiantes y disminuiría la vulnerabilidad del sistema.

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?

Activar el firewall del equipo. Ilustración 25.

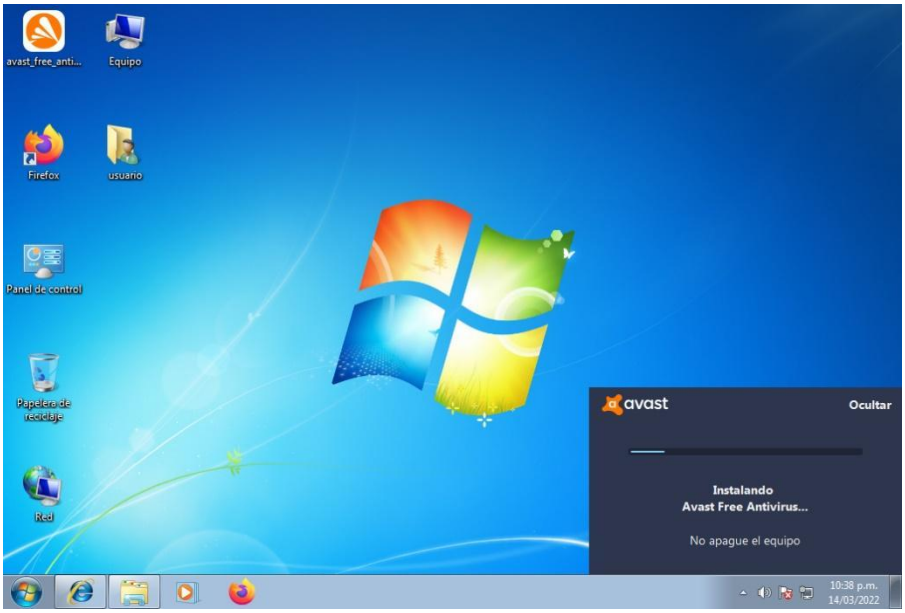
Ilustración 25 Activación del Firewall en el equipo atacado.



Fuente: Autor

Instalación de antivirus en el equipo. Ilustración 26.

Ilustración 26 Instalación antivirus.

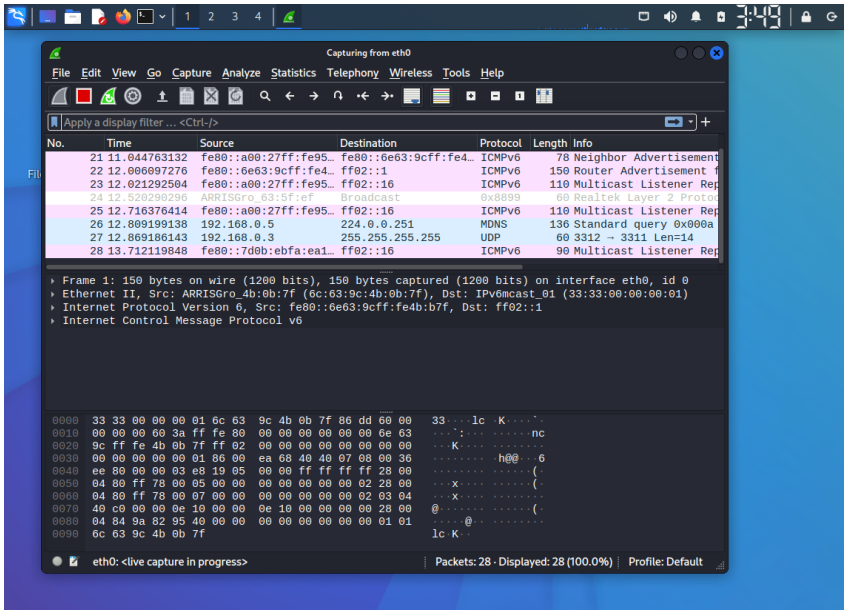


Fuente: Autor

Con estos pasos el equipo estará mucho más protegido ante ataques básicos.

Adicionalmente se debe monitorear la red para verificar que no se estén realizando accesos indeseados, para tal fin se utiliza la herramienta Wireshark. Ilustración 27.

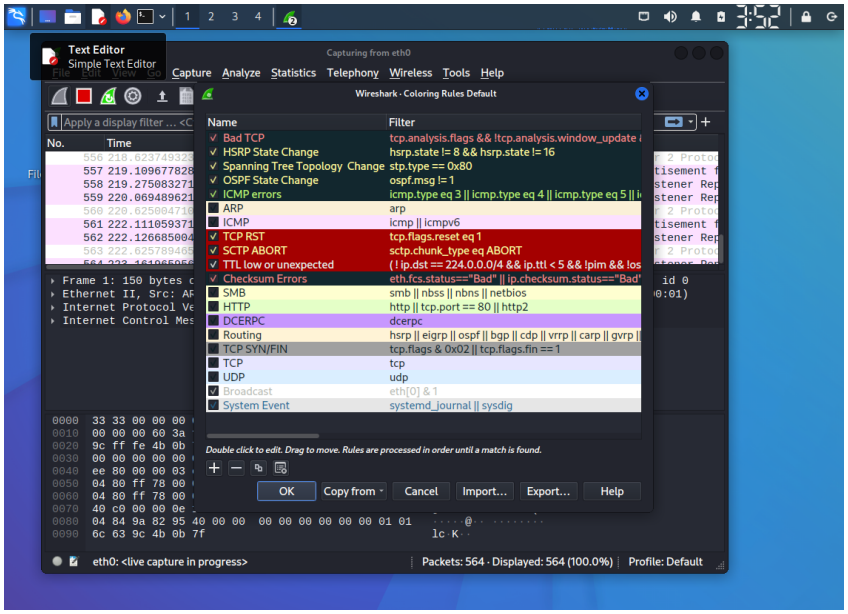
Ilustración 27 Verificación de accesos indeseados con WirkeShark.



Fuente: Autor

Con Wireshark se puede monitorear la transmisión de datos dentro de nuestra red y si alguno de estos presenta algún error o intercepción, para tal fin Wireshark presenta un código de colores que se puede verificar al seleccionar View-> Coloring rules. Ilustración 28.

Ilustración 28 Reglas de color de Wireshark.

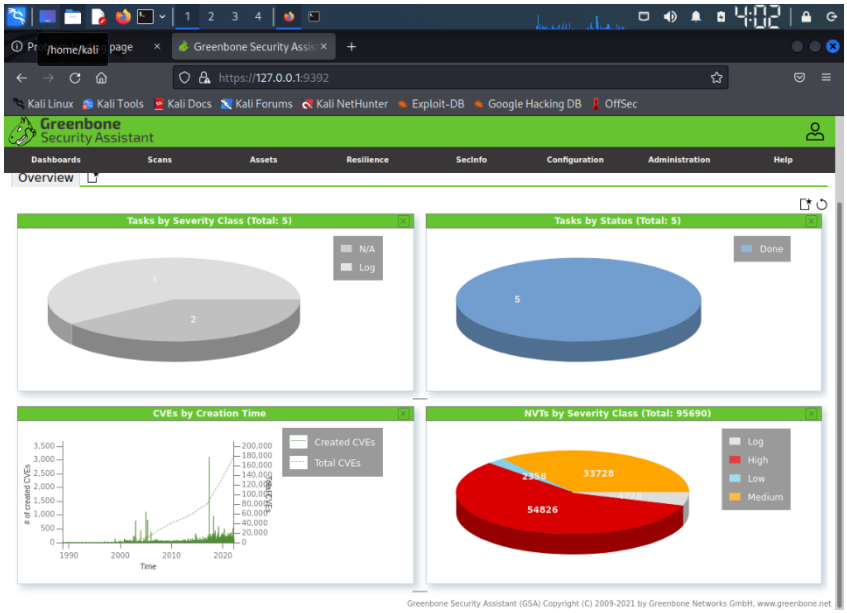


Fuente: Autor

Dentro de estas, las más importantes son, los colores rojos y amarillo, ante estas alertas se debe estar pendiente de la conexión y monitorear detalladamente.

Adicionalmente se recomienda correr diagnósticos programados con OpenVas para detectar vulnerabilidades y amenazas que puedan ser minimizadas. Ilustración 29.

Ilustración 29 Verificación de vulnerabilidades con OpenVas.



Fuente: Autor

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

Un equipo de respuesta a incidentes informáticos (CISRT) por sus siglas en inglés, es un equipo que se encarga de impedir que un ataque informático se extienda y cause más daños de los que puede realizar, normalmente se conforma por un equipo variado de varias dependencias, que busca minimizar no solo los daños internos del ataque sino también los externos, por lo que es normal que hagan parte del equipo líderes de recursos humanos o del área de mercadeo.

Un Blueteam al contrario es un equipo encargado de monitorear y fortalecer la seguridad informática de la organización constantemente, analizando vulnerabilidades y endureciendo los sistemas informáticos para minimizar las afectaciones, a diferencia del CISRT este se centra solo en los activos informáticos de la organización.

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

El CIS (Center for Internet Security por sus siglas en inglés) es una organización sin ánimo de lucro que se encarga de emitir lineamientos y mejores prácticas para establecer un estándar de seguridad informática en las organizaciones.

Para tal fin lo utilizaría como un marco de referencia de buenas prácticas a ser implementadas en mi organización, esto me permitiría tener una guía desarrollada por expertos mundiales en ciberseguridad, lo que garantizaría que mi organización está protegida ante posibles ataques informáticos, adicionalmente estas buenas prácticas y frameworks son completamente gratuitos para ser descargados, lo que disminuye costos de implementación.

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

SIEM significa Seguridad, Información y Manejo de Eventos (Security, Information and Event Management), este software permite monitorear constantemente los activos informáticos para identificar posibles amenazas, principalmente permite guardar en un log las actividades y eventos que producen las aplicaciones, equipos, redes, infraestructura y sistemas para ser analizados y poder obtener una visión general de los activos informáticos.

Principalmente un SIEM se compone de los siguientes sistemas:

- Log management systems (LMS): El Sistema de administración de registros permite el procesamiento y administración centralizada de los logs de los activos informáticos.
- Security information management (SIM): El Administrador de la seguridad de información, ofrece herramientas para automatizar la recolección de registros con un almacenamiento a largo plazo, su respectivo análisis y reporte de los datos almacenados.
- Security event management (SEM): El Administrador de eventos de seguridad permite monitorear en tiempo real los diferentes sistemas y eventos con notificaciones y vistas de consolas.

Estos tres sistemas permiten contar con una visión holística de los activos, lo que permite analizar la información brindada para poder detectar cambios en configuraciones de los diferentes sistemas que podrían significar un rompimiento de las protecciones de seguridad informática.

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.

OSSEC: Es un sistema de detección de intrusos OpenSource que permite identificar varios puntos de información para detectar posibles amenazas, entre las que se encuentran Rootkits, Malware, Usuarios no identificados en la red, cambios de archivos de sistema e información de los activos, entre otras, lo que permite manejar toda la infraestructura para monitorear su comportamiento y estar alerta ante posibles fallas o amenazas.

SNORT: Es otro sistema de detección de intrusos, pero enfocado a la red, este sistema analiza los paquetes transmitidos y cuando detecta incongruencias genera una alerta que permite identificar posibles atacantes.

OPENWIPS: Este sistema de detección de intrusos para sistemas inalámbricos, crea equipos virtuales que capturan información y sirven como puntos de referencia para detectar posibles intrusos a través de la red inalámbrica, dicha información luego es analizada por el servidor y de esta manera genera alertas y respuestas ante los ataques.

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

Teniendo en cuenta que la estrategia RedTeam & BlueTeam corresponde en la creación de equipos que se encarguen de probar las defensas de la estructura informática de una organización, se debe contar con una capacitación constante en nuevas tecnologías y metodologías, así como contar con un equipo preparado para afrontar nuevos retos.

En su artículo “Red team versus blue team: How to run an effective simulation”, David Strom enuncia varias características que deben cumplir los ejercicios Red vs Blue Team, principalmente en temas que no son técnicos y que normalmente son pasados por alto:

- Decidir qué tan realista será el ejercicio: Teniendo en cuenta que estos ejercicios normalmente no se realizan en sistemas en producción, se hace necesario contar con réplicas que permitan simular el estado actual de la organización.

- Especificar las metas: Cuando no se tienen definidos claramente los objetivos, se pueden pasar por alto metas que pueden determinar claramente falencias en el sistema que pueden no ser detectadas porque no se estableció desde el comienzo.
- Decidir como recolectar la información y el análisis posterior: Teniendo en cuenta que el trabajo remoto se ha implementado ampliamente y que estos equipos pueden ser de diferentes países o lenguas, se hace necesario establecer reglas claras para la transmisión de información y la comunicación.
- Escoger el periodo de tiempo: La idea con esto es que no se hagan los ejercicios únicamente como reacción ante un incidente, sino que constantemente se estén realizando para probar adecuadamente las capacidades del sistema y de esta manera poder hacer las correcciones necesarias para su mejora.

5.6. RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

Con el fin de endurecer los aspectos de seguridad en una organización, se recomienda fortalecer los siguientes temas:

- La protección de los datos personales y restringidos debe ser una prioridad en la organización, estos solo deben ser accedidos por el personal autorizado bajo condicione permitidas, se debe establecer el principio del privilegio mínimo, donde se le den a los usuarios el acceso mínimo permitido para realizar sus funciones.
- La protección de los diferentes dispositivos de la organización también debe ser una prioridad, los mismos deben contar con las medidas básicas de seguridad, contraseña y si se puede autenticación en dos pasos.
- Adicionalmente con el trabajo remoto se le deben brindar herramientas a los empleados para que aseguren los dispositivos del hogar o personales donde se almacene o manipule información de la organización, tables, smartphones y portátiles, implementar una VPN para conectarse a los servicios de la empresa es algo que se debe implementar.
- Establecer protocolos y políticas para actuar en el momento en el que se materialice alguna vulnerabilidad, para que de esta manera se tenga claro el paso a paso a seguir si llegan a ocurrir.

- Con el fin de evitar incidentes de espionaje o robo de información, los empleados nuevos deben pasar un periodo de prueba antes de tener acceso a información confidencial o importante de la empresa más allá de sus funciones.
- Participación de los directivos: Los directivos deben estar muy alineados con este enfoque de protección y brindar el presupuesto suficiente y los espacios para concientizar a todos los niveles de la importancia de la seguridad informática.
- Capacitación del equipo de seguridad: Los ataques informáticos siempre se encuentran en evolución y cada día se generan nuevas vulnerabilidades que afectan los sistemas, para tal fin se hace necesario que el equipo de seguridad se encuentre constantemente actualizado ante estas vulnerabilidades.
- Capacitación a los usuarios: Una de las principales vulnerabilidades con las que cuentan las organizaciones son los usuarios, ningún Blue Team puede defender contra la descarga y ejecución de un archivo con un virus, o si se copia información privilegiada y esta se almacena en dispositivos no seguros, por tal motivo los usuarios deben ser capacitados en aspectos básicos de seguridad informática, esto con el fin de que ellos se conviertan en la primera línea de defensa ante un posible ataque informático.
- Implementación de un SIEM en la organización: Los SIEM permiten generar un monitoreo constante de los activos informáticos, por lo que su implementación brindará una capa extra que automáticamente permitirá reconocer las intrusiones, por lo que es importante su implementación para mejorar las capacidades de defensa de una organización.

5.7. CONCLUSIONES QUE PERMITAN LA CONSTRUCCIÓN DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

Ya sea que participemos en equipo BlueTeam o RedTeam es indispensable conocer las Leyes que rigen la seguridad informática del país donde trabajemos.

También se deben conocer las herramientas que se utilizarán, principalmente el Kali Linux es nuestra navaja suiza que nos permitirá desarrollar las actividades con precisión y eficiencia.

Existen una gran cantidad de herramientas utilizadas en el pentesting, conocerlas a fondo es una necesidad para cualquier profesional que quiera desarrollar sus

conocimientos, sin embargo, las más fundamentales y con las que se pueden desarrollar muchas actividades son Nmap, Metasploit y OpenVas.

Adicionalmente se hace necesario tener un buen manejo de la documentación, ya que esta es fundamental durante todas las etapas, especialmente en la de análisis y reporte, por lo que manejar un buen nivel de redacción es vital para el desarrollo de las tareas.

Adicionalmente, el trabajo en equipo es necesario en todas las actividades del BlueTeam o RedTeam, por lo que debemos cultivar las habilidades de comunicación, empatía y tolerancia.

5.8. VIDEO DE LA SUSTENTACIÓN

Video

6. CONCLUSIONES

- La protección ante vulnerabilidades permite mitigar posibles riesgos que se pueden prevenir con medidas básicas de protección.

- Es necesario realizar un monitoreo constante de los diferentes puntos de acceso de la red con el fin de impedir el acceso a usuarios no autorizados que puedan afectar los sistemas.

- Existen herramientas básicas de los sistemas operativos que permiten proteger de manera adecuada los computadores de la red.

- El control de intrusos es necesario para poder contar con herramientas automatizadas que reaccionen ante intento de ingresos no autorizados, lo que remueve el factor humano en el seguimiento de la red.

- El establecimiento de equipos BlueTeam & RedTeam permiten a una organización estar protegida eficientemente ante posibles ataques informáticos.

- La protección ante ataques informáticos es de vital importancia en el momento en que vivimos, ya que la información se convirtió en el activo más importante de las organizaciones.

7. BIBLIOGRAFÍA

- OSSEC. {En línea}. Fecha. {13/03/2022}. Disponible en https://www.ossec.net/
- Snort. {En línea}. Fecha. {13/03/2022}. Disponible en https://www.snort.org/
- OpenWips. {En línea}. Fecha. {13/03/2022}. Disponible en https://openwips-ng.org/
- STROM, David. (2017). (2017). Red team versus blue team: How to run an effective simulation. {En línea}. Fecha {Julio 13, 2018} Disponible en https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparednessred-team-versus-blue-team-how-to-run-an-effective-simulation.html
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Senado de la República de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
- Ley 1273 (2009). Modificación al Código Penal. Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.
- Ley 842 de 2003. Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003
- WAKSMAN, Adam, et al. A red team/blue team assessment of functional analysis methods for malicious circuit identification. En 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE, 2014. p. 1-4.
- Paganini, P. (2016). Cyber security: Red team, Blue team and Purple team. Retrieved July 13, 2018, from https://securityaffairs.co/wordpress/49624/hacking/cyber-red-teamblue-team.html
- JOHNSON, Robert. (2019). 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked. {En línea}. Fecha {02 de enero de 2019} . Disponible en https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/
- DIOGENES, Yuri; OZKAYA, Erdal. Cybersecurity??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing Ltd, 2018.
- RICHTER, Maximilian; SCHWARZ, Klaus; CREUTZBURG, Reiner. Conception and Implementation of Professional Laboratory Exercises in the

field of ICS/SCADA Security Part II: Red Teaming and Blue Teaming. Electronic Imaging, 2021, vol. 2021, no 3, p. 74-1-74-13.

- DALE, Cris. Red, Blue and Purple Teams: Combining Your Security Capabilities for the Best Outcome. SANS Institute. 2020. Disponible en https://www.sans.org/media/analyst-program/red-blue-purple-teams-combining-security-capabilities-outcome-39190.pdf
- CRICHLOW, Matthias Caretta. A study on Blue Team's OPSEC failures. 2020. Tesis de Maestría. University of Twente. Disponible en https://essay.utwente.nl/84945/
- KOKKONEN, Tero; PUUSKA, Samir. Blue team communication and reporting for enhancing situational awareness from white team perspective in cyber security exercises. En Internet of things, smart spaces, and next generation networks and systems. Springer, Cham, 2018. p. 277-288. Disponible en https://link.springer.com/chapter/10.1007/978-3-030-01168-0_26