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

RAÚL RICARDO VÁSQUEZ AVILEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CAUCASIA ANTIOQUIA

2024

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

RAÚL RICARDO VÁSQUEZ AVILEZ

Seminario especializado:

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM

Director del curso:

LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÁA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CAUCASIA ANTIOQUIA

2024

CONTENIDO

Pág.

TABLA DE FIGURAS

TABLA DE TABLAS

TABLA DE ANEXOS

GLOSARIO

AMENAZA**:** es una situación o acción que puede poner en riesgo la seguridad de los sistemas informáticos, la información y los datos almacenados en ellos.

BLUE TEAM**:** es un equipo de profesionales en ciberseguridad que es responsable de la defensa y protección de los sistemas y redes internas contra posibles ataques cibernéticos.

CIBERSEGURIDAD**:** es el conjunto de medidas y mecanismos que se utilizan para proteger los sistemas informáticos, redes, dispositivos y datos de posibles ataques, daños, robo o acceso no autorizado.

EXPLOIT**:** es un programa informático que permite la explotación de una vulnerabilidad en un equipo o sistema.

FOOTPRINTING**:** se refiere al proceso de recopilar información y datos sobre un objetivo específico, como una empresa, organización o sistema informático, con el objetivo de obtener una comprensión detallada de su infraestructura, sistemas y vulnerabilidades.

HARDENING**:** se refiere a un conjunto de técnicas y medidas que se aplican para fortalecer y proteger los sistemas informáticos contra posibles amenazas y ataques maliciosos.

METASPLOIT**:** es una herramienta de ciberseguridad que tiene diferentes funcionalidades, y cuenta con gran cantidad de exploit, es muy usada para pentesting.

METERPRETER**:** Una Meterpreter es un tipo de herramienta utilizada en ciberseguridad que permite a un atacante acceder y controlar de forma remota un sistema informático comprometido.

MSFVENOM**:** es una herramienta informática utilizada para generar payloads.

MULTI HANDLER**:** es una utilidad de metasploit, que permite al usuario configurar y controlar diferentes tipos de sesiones de explotación remota en un solo lugar.

PAYLOAD**:** Es un programa informático comúnmente conocido como carga útil, que se encarga de proveer comunicación a nivel de red entre un equipo atacante y un equipo víctima.

PURPLE TEAM**:** es un equipo de profesionales de ciberseguridad que combina la parte de blue team y red team

RED TEAM**:** es un equipo de profesionales de seguridad informática que se encarga de simular ataques y vulnerabilidades en una red o sistema, con el fin de identificar posibles fallos de seguridad y fortalecer las defensas de la organización.

VULNERABILIDAD**:** se refiere a una debilidad o defecto en los sistemas, redes, dispositivos o aplicaciones que pueden ser explotadas por atacantes para acceder, dañar, robar o comprometer información confidencial.

RESUMEN

En cuanto a las capacidades técnicas, los equipos Red Team deben contar con conocimientos avanzados en seguridad de redes, sistemas operativos, aplicaciones y herramientas de hacking. Deben ser capaces de identificar y explotar vulnerabilidades en la infraestructura de la organización y simular ataques realistas. Por otro lado, los equipos Blue Team deben tener un sólido conocimiento de los sistemas de defensa, como firewalls, detección de intrusiones y análisis forense, así como habilidades en administración de redes y sistemas.

Además de las habilidades técnicas, es importante que los equipos Red Team y Blue Team tengan una comprensión profunda de la normativa legal y regulatoria en cuanto a seguridad de la información. Esto incluye leyes de protección de datos, privacidad y notificación de violación de datos, entre otras. Deben ser capaces de aplicar estas normas a su trabajo y garantizar que la organización esté en cumplimiento.

En términos de capacidades de gestión, los equipos Red Team y Blue Team deben tener habilidades de liderazgo y trabajo en equipo. Deben poder comunicarse eficazmente y colaborar con otros departamentos de la organización, como el de seguridad de la información y el de TI. Además, deben ser capaces de planificar y ejecutar estrategias de seguridad, así como de realizar informes y análisis de riesgos.

Otra habilidad importante para estos equipos es la capacidad de adaptación y actualización constante.

Palabras clave: Blue team, Metasploit, Msfvenom, Payload, Red team,

ABSTRACT

In terms of technical capabilities, Red Team teams must have advanced knowledge of network security, operating systems, applications and hacking tools. They must be able to identify and exploit vulnerabilities in the organization's infrastructure and simulate realistic attacks. On the other hand, Blue Teams must have a solid knowledge of defense systems, such as firewalls, intrusion detection and forensics, as well as network and systems administration skills.

In addition to technical skills, it is important for Red Team and Blue Team teams to have a deep understanding of legal and regulatory standards regarding information security. This includes data protection, privacy and data breach notification laws, among others. They must be able to apply these standards to their work and ensure that the organization is in compliance.

In terms of management capabilities, Red Team and Blue Team must have leadership and teamwork skills. They must be able to communicate effectively and collaborate with other departments in the organization, such as information security and IT. Additionally, they must be able to plan and execute security strategies, as well as perform risk analysis and reporting.

Another important skill for these teams is the ability to adapt and constantly update.

Key words: Blue team, Metasploit, Msfvenom, Payload, Red team,

INTRODUCCION

Los equipos Red Team y Blue Team se han vuelto esenciales en el ámbito de la ciberseguridad, especialmente en el contexto de un mundo cada vez más digitalizado y conectado. Estos equipos complementarios, pero con diferentes funciones, tienen como objetivo principal proteger los sistemas y redes de una organización de posibles ataques y vulnerabilidades. Sin embargo, para cumplir con eficacia su misión, es fundamental que cuenten con ciertas capacidades técnicas, legales y de gestión.

En cuanto a las capacidades técnicas, los integrantes del equipo Red Team deben poseer conocimientos avanzados en seguridad informática, sistemas operativos, redes, lenguajes de programación y herramientas de hacking ético. Deben estar al día con las últimas técnicas y metodologías utilizadas por los hackers para poder simular ataques reales y descubrir posibles vulnerabilidades en los sistemas de la organización. Por otro lado, el equipo Blue Team debe contar con habilidades en análisis de logs, monitoreo de la red, implementación de medidas de seguridad y capacidad para responder de manera rápida y efectiva a los ataques.

En cuanto a las capacidades legales, los equipos Red Team y Blue Team deben tener un profundo conocimiento de las leyes y regulaciones relacionadas con la ciberseguridad, así como de las políticas y normativas internas de la organización a la que prestan sus servicios. Esto les permitirá enmarcar sus actuaciones dentro de la legalidad y evitar posibles problemas legales.

Por último, es igualmente importante que estos equipos cuenten con capacidades de gestión para poder trabajar de manera coordinada y efectiva. Esto incluye habilidades de comunicación, trabajo en equipo, liderazgo y gestión de proyectos. Además, deben ser capaces de adaptarse a los cambios y tomar decisiones rápidas en situaciones de crisis.

las capacidades técnicas, legales y de gestión son fundamentales para que los equipos Red Team y Blue Team puedan llevar a cabo su misión de proteger los sistemas de una organización contra posibles amenazas y vulnerabilidades. Por lo tanto, es esencial invertir en la formación y el desarrollo de estas capacidades para garantizar una ciberseguridad eficaz y eficiente.

JUSTIFICACION

Los equipos Red Team y Blue Team son fundamentales en la ciberseguridad de una organización, ya que trabajan en conjunto para simular ataques y defenderse de ellos. Por lo tanto, es importante que cuenten con capacidades técnicas, legales y de gestión sólidas para garantizar una protección efectiva contra posibles amenazas.

En la actualidad, las empresas e instituciones enfrentan constantemente amenazas cibernéticas que pueden afectar su integridad y seguridad. Por ello, se hace cada vez más necesario contar con equipos especializados en ciberseguridad, específicamente en la detección y respuesta ante ataques, conocidos como equipos red team y blue team. Estos equipos tienen roles diferenciados pero complementarios, ya que mientras red team se encarga de simular ataques para evaluar la seguridad de la organización, el blue team se enfoca en la detección y respuesta ante ataques reales.

Para que estos equipos puedan cumplir de manera efectiva sus funciones, es necesario que cuenten con capacidades técnicas, legales y de gestión adecuadas.

En primer lugar, es fundamental que los equipos red team y blue team tengan un amplio conocimiento técnico en ciberseguridad, incluyendo herramientas y técnicas de hacking ético, inteligencia de amenazas, análisis forense, entre otros. Además, deben mantenerse actualizados en un entorno en constante evolución, ya que los ciberdelincuentes están en constante búsqueda de nuevas vulnerabilidades para explotar.

Otra capacidad clave para estos equipos es contar con conocimientos legales, especialmente en temas de ciberseguridad y protección de datos. Esto es esencial para garantizar que su trabajo se realice en cumplimiento con las leyes y regulaciones aplicables, evitando posibles sanciones y riesgos legales para la organización.

Además, los equipos red team y blue team deben tener habilidades de gestión y comunicación efectivas. Esto les permitirá coordinarse y trabajar en conjunto de manera eficiente, ya que deben ser capaces de responder rápidamente a los incidentes para mitigar su impacto en la organización. También es importante que puedan informar de manera clara y concisa a la dirección y otros miembros de la empresa sobre las amenazas identificadas y las medidas tomadas para abordarlas.

Otro aspecto clave en la gestión de estos equipos es tener procesos y protocolos claros y definidos. Esto garantizará una respuesta rápida y efectiva ante un ataque, minimizando el tiempo de inactividad y el impacto en la organización. Además, la documentación adecuada permite el seguimiento y la mejora continua de los procesos y procedimientos de seguridad de la compañía.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar de un laboratorio virtualizado de pruebas, a fin de recomendar acciones de seguridad para la empresa caso de estudio "HackerHouse". Teniendo en cuenta la legislación colombiana y las normas éticas.

OBJETIVOS ESPECIFICOS

- Reconocer la legislación colombiana que rige a los equipos red team y blue team, para desarrollar labores que no vallan en contra de la ley y la ética.

- Realizar un laboratorio virtualizado de pruebas, para poder ejecutar pruebas red team y blue team, ayudando a la organización a mejorar su seguridad.

- Recomendar acciones de seguridad para la empresa caso de estudio “HackerHouse”, teniendo en cuenta los resultados obtenidos en las pruebas red team y blue team.

1. LEGISLACION COLOMBIANA QUE PARA LOS EQUIPOS RED TEAM Y BLUE TEAM

No existe una legislación específica en Colombia que regule a equipos Red Team y Blue Team. Sin embargo, estos equipos deben cumplir con la normativa vigente en materia de protección de datos personales y ciberseguridad, que incluyen leyes y decretos como:

1.1 LEY 1273 DE 2009

En Colombia es una modificación al Código Penal que introduce un nuevo bien jurídico tutelado, denominado “de la protección de la información y de los datos”[1]. Esta ley busca preservar integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones. A continuación, se presenta un resumen de los artículos más relevantes:

Artículo 269A: Acceso abusivo a un sistema informático. Establece penas de prisión y multas para aquellos que accedan sin autorización o se mantengan dentro de un sistema informático en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Penaliza a aquellos que impidan u obstaculicen el funcionamiento o el acceso normal a un sistema informático o a una red de telecomunicaciones.

[1] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 [en línea]. (5, enero,2009) [consultado el 3, marzo,2024], Ley de la protección de la información y de los datos. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Artículo 269C: Interceptación de datos informáticos. Establece penas para aquellos que intercepten datos informáticos sin orden judicial previa.

Artículo 269D: Daño Informático. Penaliza a aquellos que destruyan, dañen, borren, deterioren, alteren o supriman datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso. Penaliza a aquellos que produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

1.2 LEY 1581 DE 2012

La Ley 1581 de 2012 tiene como objetivo desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.[2]Esta ley aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

En cuanto a las multas, la Superintendencia de Industria y Comercio puede imponer multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.

[2] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 [en línea], (17, octubre, 2012) [consultado 5, marzo, 2024]. Ley de la protección de datos personales. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

La entidad encargada de velar por el cumplimiento de las normas sobre protección de datos personales en Colombia es la Superintendencia de Industria y Comercio (SIC), a través de la Delegatura para la Protección de Datos Personales.

1.3 EL CONVENIO BUDAPEST

El Convenio de Budapest[3] es un tratado internacional sobre ciberdelincuencia, adoptado en el año 2001 en la ciudad de Budapest, Hungría. Este convenio tiene como objetivo prevenir y combatir los delitos informáticos, proteger los derechos fundamentales relacionados con el uso de internet, y fomentar la cooperación internacional para investigar y enjuiciar a los responsables de estos delitos.

Colombia es parte del Convenio de Budapest desde el año 2003, lo que significa que se ha comprometido a implementar las medidas necesarias para prevenir y combatir los delitos informáticos en su territorio. Esto incluye la adopción de leyes y políticas adecuadas, y la cooperación con otros países para investigar y enjuiciar a los responsables de delitos cibernéticos.

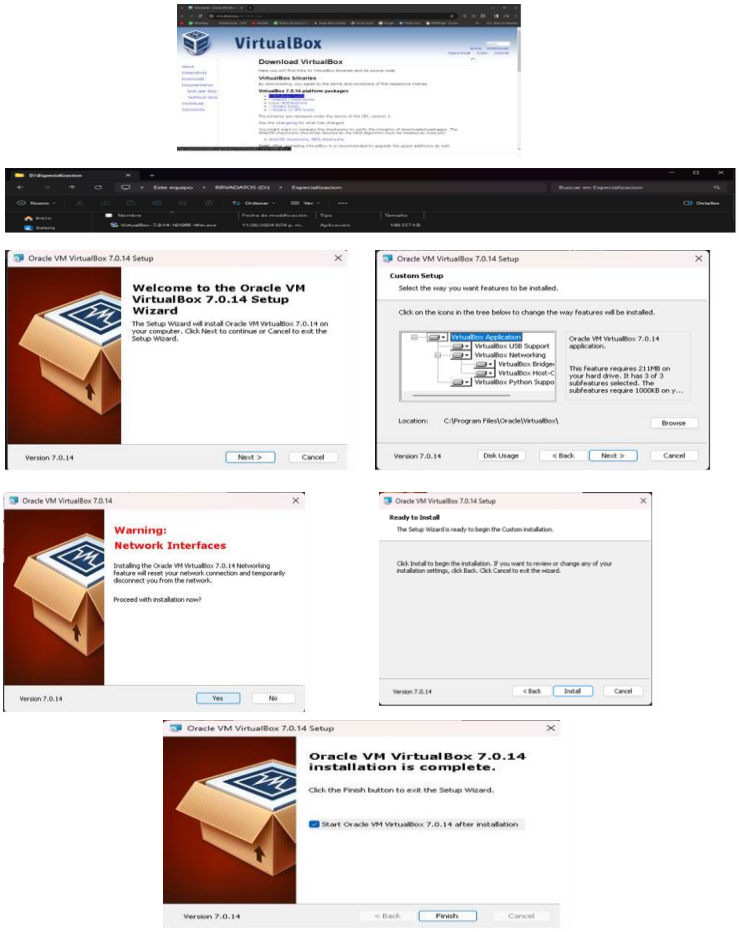
[3] BUDAPEST. SERIE TRATADOS EUROPEOS. Convenio. [en línea] (23, noviembre, 2001) [consultado 7, marzo, 2024]. Convenio sobre la ciberdelincuencia. Disponible en Internet: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

2. LABORATORIO VIRTUALIZADO PARA PRUEBAS RED TEAM Y BLUE TEAM

2.1 IMPLEMENTACIÓN

En primer lugar, se realiza la descarga del software de virtualización de Oracle VirtualBox, se ingresa a la página principal (https://www.virtualbox.org/) y se da clic en la opción de descarga para sistema operativo Windows. Una vez realizada la descarga se puede observar el archivo de instalación en la carpeta de descargas de Windows. Se procede a realizar la instalación del software VirtualBox tal como se muestra en la figura 1:

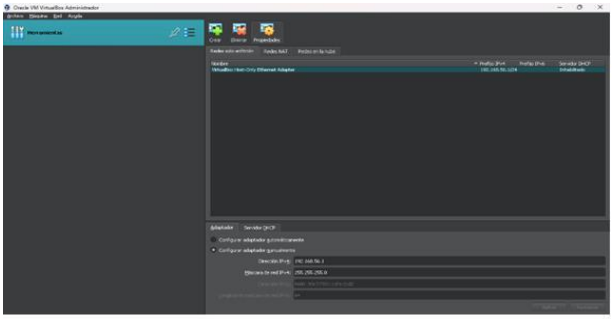
Figura 1. Instalación de Virtual Box



Fuente: El autor.

Una vez finalizada la instalación del software podemos ver la ventana principal de virtual box como se muestra en la figura 2, donde se procederá a instalar las máquinas virtuales para el ambiente de pruebas:

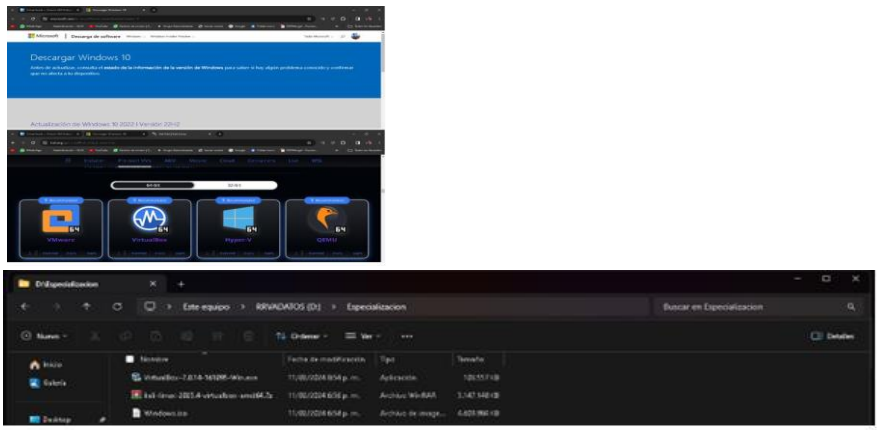
Figura 2. Ventana Principal de Virtual Box



Fuente: El autor.

Luego de esto se procede a descargar Windows 10 y Kali Linux: A continuación, se realiza la descarga de Windows 10 y Kali Linux tal como se muestra en la figura 3.

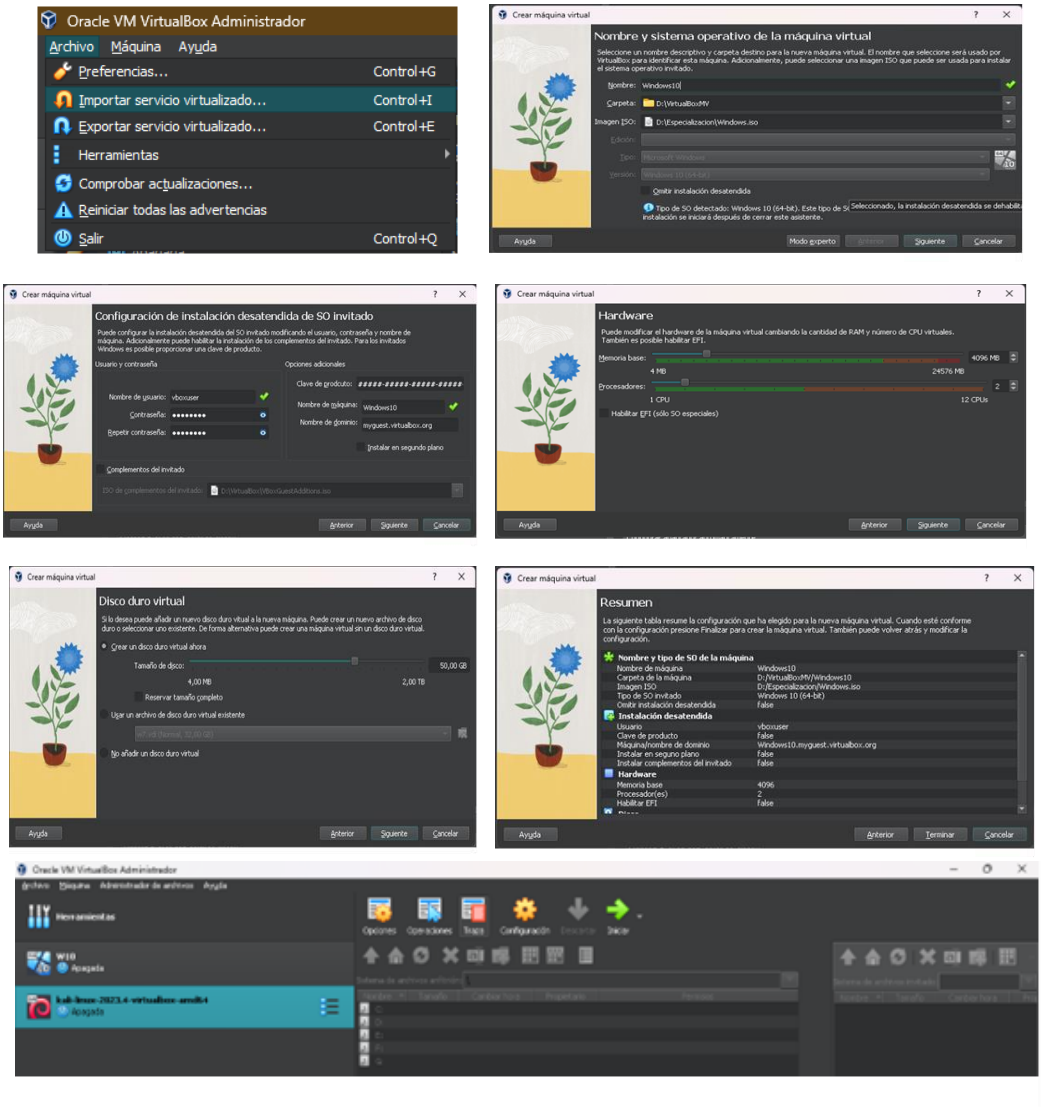
Figura 3. Descarga de W10 y Kali Linux.



Fuente: El autor.

Una vez descargados los archivos, estos se pueden visualizar en la carpeta de descargas, para el sistema operativo Windows se descargó un archivo del tipo iso, mientras que para el sistema operativo Kali Linux, se descargó una imagen virtualizada para virtual box de tipo ova, el cual se instala desde la opción de archivo, importar servicio virtualizado, el proceso se muestra en la figura 4.

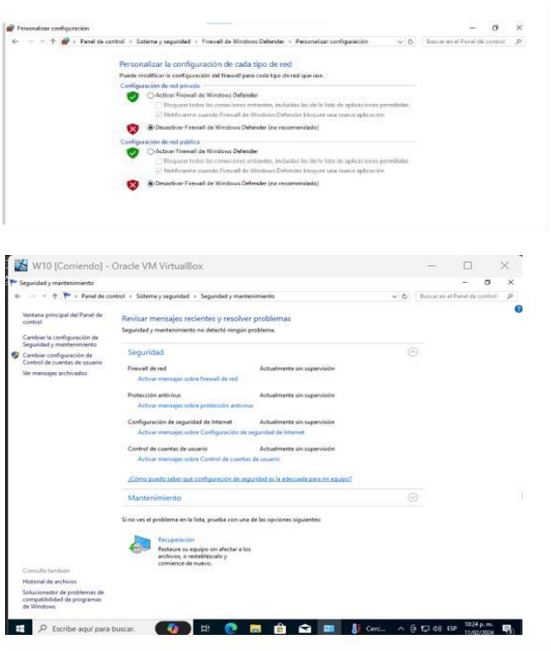
Figura 4. Instalación de W10 y Kali Linux en Virtual Box.



Fuente: El autor.

Ahora se procede a configurar las opciones de seguridad de la máquina de w10, con las opciones de seguridad, en modo desactivadas, donde se observa el firewall, antivirus, etc.

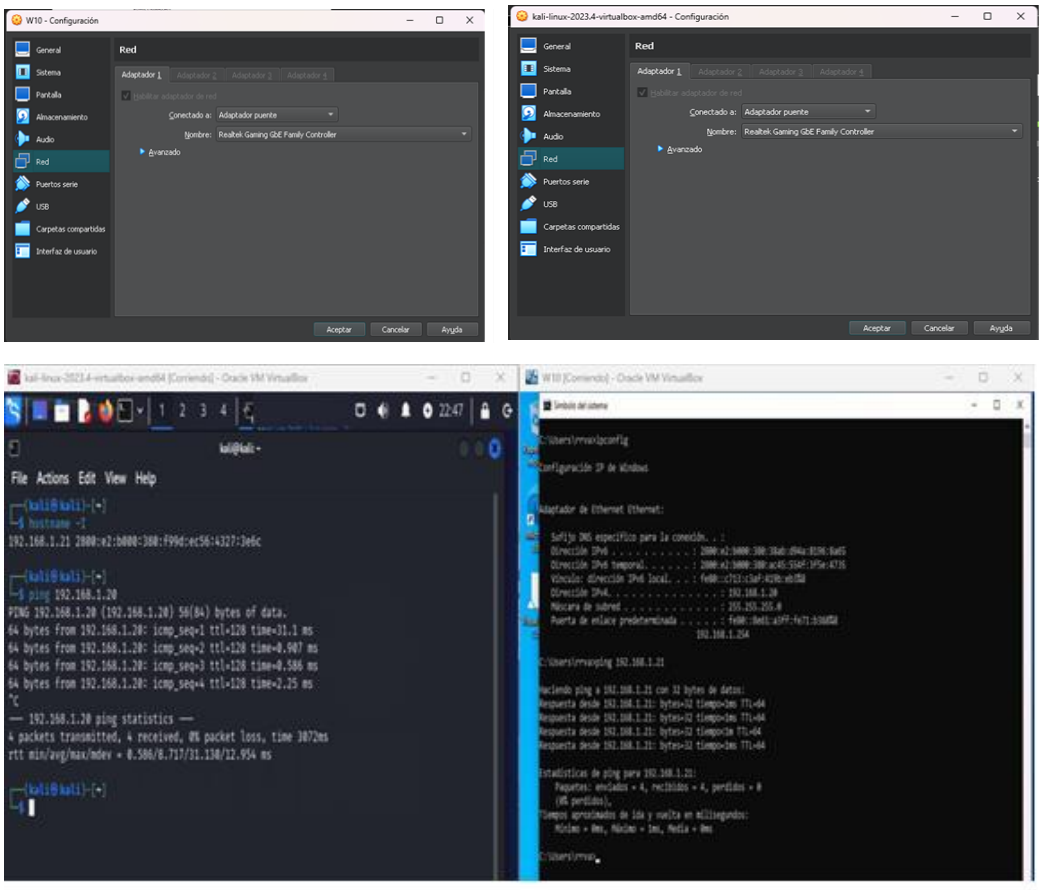
Figura 5. Configuraciones de seguridad en W10



Fuente: El autor.

Luego se procede a realizar la configuración de la red de las 2 máquinas de tal manera que se comunique, entre sí, para esto se establen los adaptadores como conexión de las maquinas w10 y Kali Linux en modo puente o bridge, permitiendo que el router principal les asigne una ip dentro de la misma subred, tal como se observa en la figura 6, donde las maquinas pueden comunicarse, para esto se realiza ping desde las consolas de cada maquina hacia la ip de cada máquina, es decir, desde la maquina W10 se hace ping a la ip de la maquina Kali y desde las maquina kali, se hace ping hacia la ip de la maquina W10, tal como se muestra en la figura 6.

Figura 6. Comunicación de W10 y Kali Linux



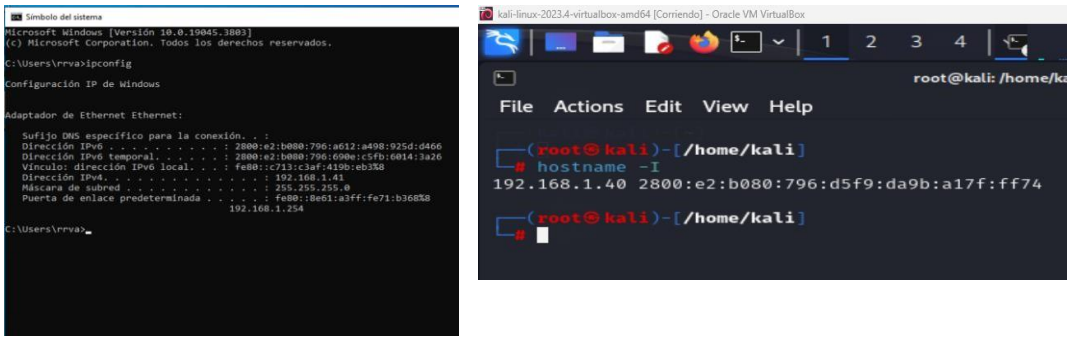
Fuente: El autor.

2.2 PRUEBAS RED TEAM

Para el desarrollo de la implementación de pruebas de red team, se parte de un caso problémico de la empresa Hacker House, en donde se realizó una explotación de una vulnerabilidad debido a que un usuario ejecuto un archivo .exe que permitió a un atacante tomar el control de dicha máquina. Los expertos de Hacker House expresan que la vulnerabilidad pudo ser explotada con la herramienta de kali Linux llamada metasploit y que el archivo .exe pudo haberse creado con la herramienta MsfVenom, por lo tanto, el equipo red team se dispone a recrear el incidente en el ambiente de pruebas:

Teniendo como referencia el ambiente de pruebas de una maquina Linux Yuna Windows en el mismo segmento de red, tenemos la configuración ip de la maquina Windows como se muestra en la figura 7. Y se lista en la tabla 1

Figura 7. Verificación de IP de W10 y Kali Linux.



Fuente: El autor.

En la tabla 1 recolectamos las ips de cada máquina, estas ips nos servirán más adelante para las pruebas de intrusión.

Tabla 1 Equipos e IPs

EQUIPO	SISTEMA OPERATIVO	IP
W10	WINDOWS	192.168.1.41
KL2023	KALI LINUZ	192.168.1.40

Fuente: El autor.

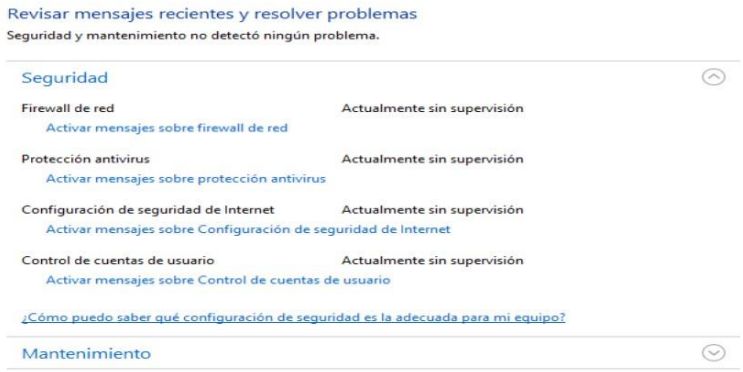
Como se puede observar que están en el mismo segmento de red. Se identifica el sistema operativo de la maquina víctima, el cual es una maquina con sistema operativo Windows y arquitectura x64, como se muestra en la figura 8.

Figura 8. Arquitectura de W10.

Fuente: El autor.

Se evidencia que los dispositivos de seguridad en Windows 10, se encuentran desactivados, protección en tiempo real, antivirus, firewall, lo cual es una falla de seguridad que va a permitir poder vulnerar al equipo w10, la figura 9 muestra que no esta gestionada la seguridad en la maquina Windows 10.

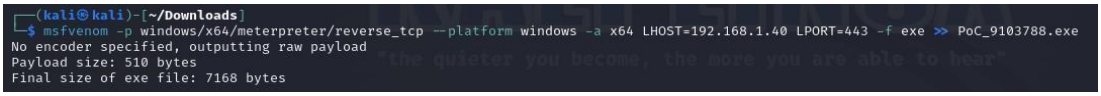
Figura 9. Seguridad no gestionada en W10.



Fuente: El autor.

Se crea el archivo de carga útil por medio de la herramienta msfvenom tal como se muestra en la figura 10, el comando usa varios parámetros para poder generar el malware que servirá como exploit en la maquina víctima. Entre estos parámetros tenemos la arquitectura del sistema operativo, el sistema operativo, el puerto de escucha y la ip.

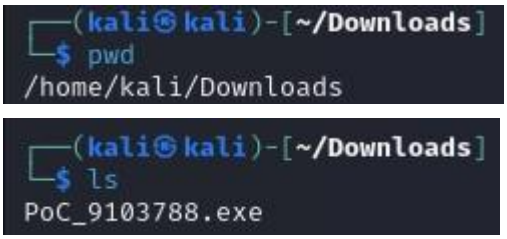
Figura 10. Comando para crear el archivo exe.



Fuente: El autor.

Se puede ver que el directorio actual es /home/kali/Downloads, como el comando se ejecutó de forma correcta, quedó el archivo de carga útil en extensión .exe, el cual se ejecutará desde la maquina victima para poder proporcionar una Shell reversa a la maquina atacante de Kali Linux. Esto se puede observar en la figura 11.

Figura 11. Archivo de carga útil.

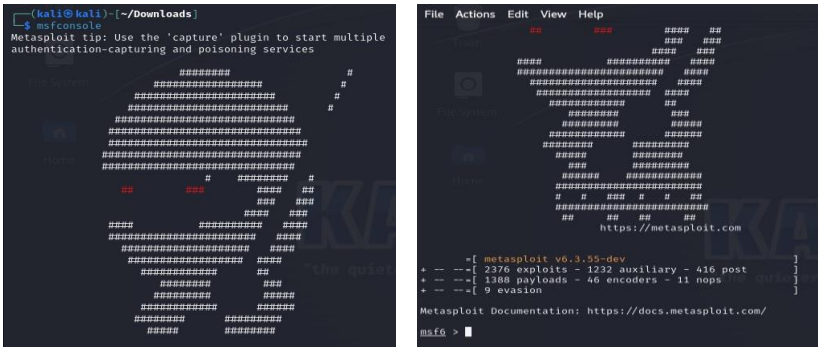


Fuente: El autor.

El archivo exe según el caso problémico Hacker House, es ejecutado desde la maquina víctima y descargado de la herramienta de chat WhatsApp web. Para temas prácticos hago uso de un ftp para enviar el archivo hasta la maquina víctima y lo dejo en el escritorio de la maquina victima para simular que fue descargado de WhatsApp web y dejado en el escritorio. Ahora se simula que el empleado ejecuto el programa, pero antes de esto se debe seguir los pasos previos antes de la explotación de la vulnerabilidad.

En la maquina atacante hacemos uso de la herramienta de Kali Linux metasploit. Para esto digitamos en consola el comando msfconsole como se muestra en la figura 12.

Figura 12. Herramienta metasploit.



Fuente: El autor.

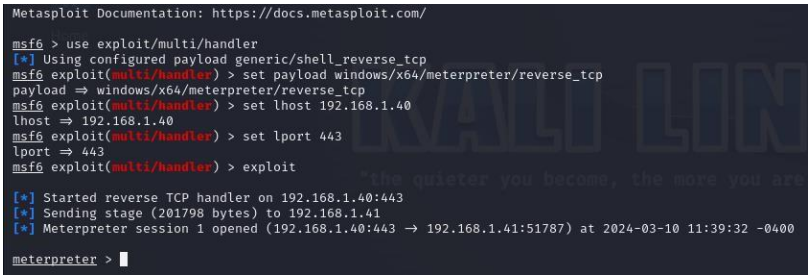
Ahora se utiliza la herramienta de metasploit, se hace uso del exploit multi/handler, se establece el exploit configurando el payload con arquitectura x64, se estable el parámetro LHOST el cual viene a ser la ip de la maquina Linux, y el puerto de escucha LPORT se establece a 443, ya que es un puerto que permanece abierto en la mayoría de maquina Windows. Final mente procedemos a ejecutar el exploit y quedamos a esperas de que se ejecute el archivo en la maquina víctima, es decir, el archivo que se descargó en la maquina víctima, Estos pasos se pueden ver en la figura 13.

Figura 13. metasploit multi handler.

Fuente: El autor.

Ahora se debe simular que el usuario ejecuta el programa exe en la maquina Windows 10, al realizar esto, se puede observar de forma inmediata, que el atacante gano acceso a este equipo por medio de la Shell reversa, tal como se muestra en la figura 12.

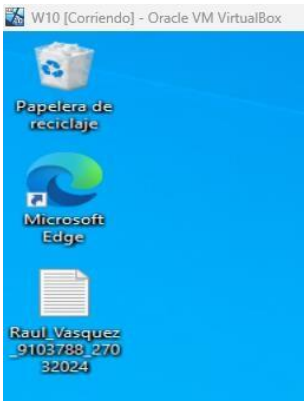
Figura 14. Shell reversa en maquina Kali Linux.



Fuente: El autor.

Ya tenemos acceso al equipo Windows. En el equipo Windows se puede observar que inicialmente, antes de descargar el archivo desde WhatsApp web, en el escritorio se encontraba un archivo de texto, tal como se muestra en la figura 15.

Figura 15. Archivo de Información W10.



Fuente: El autor.

Al descargar el archivo .exe, ya se pueden ver los dos archivos.

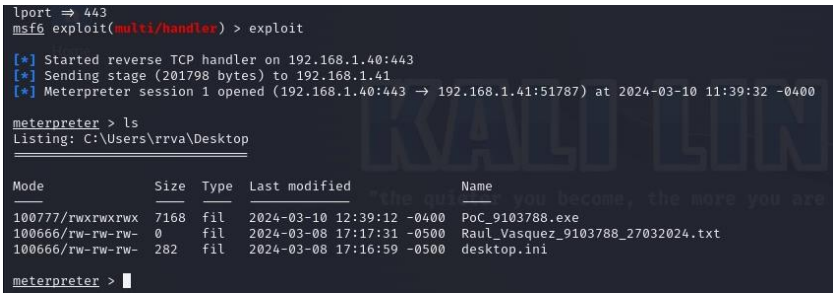
Figura 16. Archivos en el Escritorio previo al ataque.

Fuente: El autor.

Al ejecutar el archivo exe, se dio acceso a la maquina atacante, desde la cual ya podemos ver los archivos que están en el directorio actual, que precisamente es el escritorio de Windows. lo podemos visualizar mediante el comando “ls” de la Shell reversa.

.

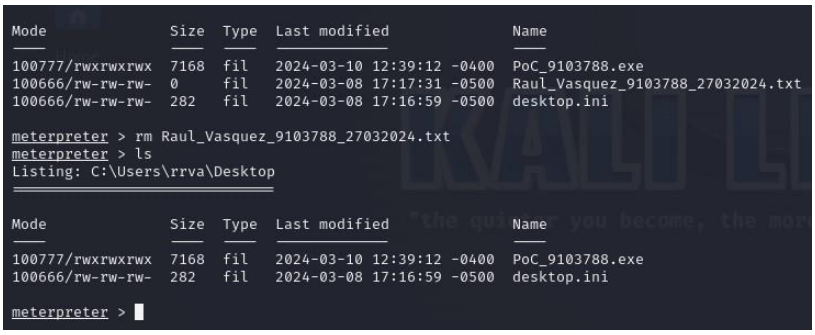
Figura 17. Comando ls en shell reversa



Fuente: El autor.

Para borrar el archivo txt de la maquina victima usamos el comando “rm” de la Shell reversa, tal como se muestra en la figura, al listar directorios (ls) ya no se encuentra el archivo .txt:

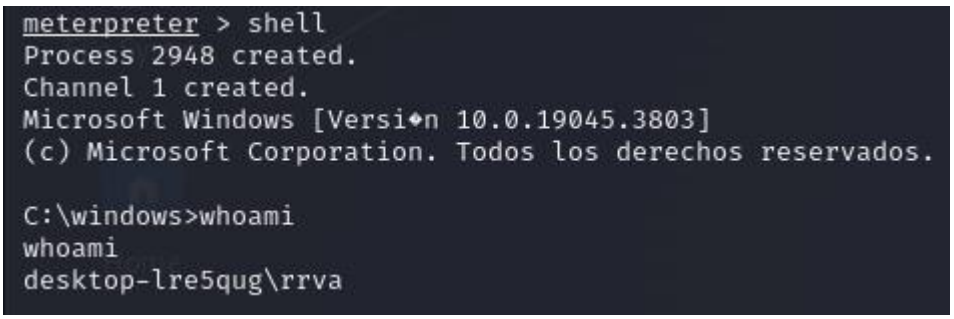
Figura 18. Comando para borrar archivo.



Fuente: El autor.

En el caso de requerir una Shell similar al ambiente Windows podemos hacer uso del comando de la Shell reversa “Shell”, de este modo podemos ejecutar comandos nativos de Windows tal como whoami, el cual muestra el nombre del equipo y el usuario actual:

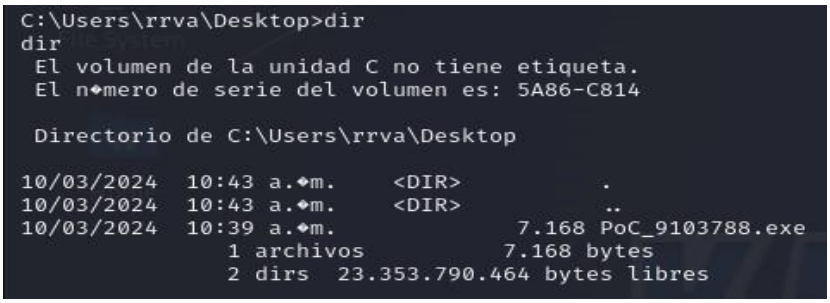
Figura 19. Comando Shell y whoami



Fuente: El autor.

Otro comando que podemos utilizar es el comando dir, que es similar a ls en linux, podemos observar que ya no está el archivo .txt

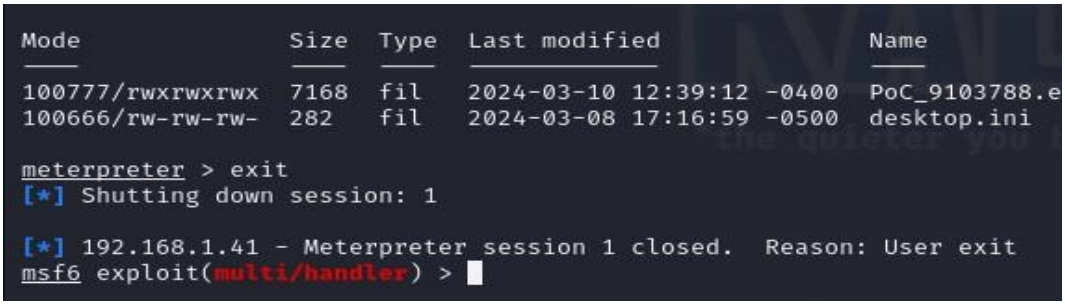
Figura 20. Comando dir



Fuente: El autor.

Para salir de este modo podemos usar el comando “exit” y volvemos a la Shell reversa y si continuamos con este comando seguimos saliendo hasta metasploit y finalmente llegamos a la línea de comandos de linux, dando por finalizado la explotación.

Figura 21. Salir de la shell.



Fuente: El autor.

Finalmente, para salir de metasploit se utiliza la palabra exit

Figura 22. Salir de metasploit.

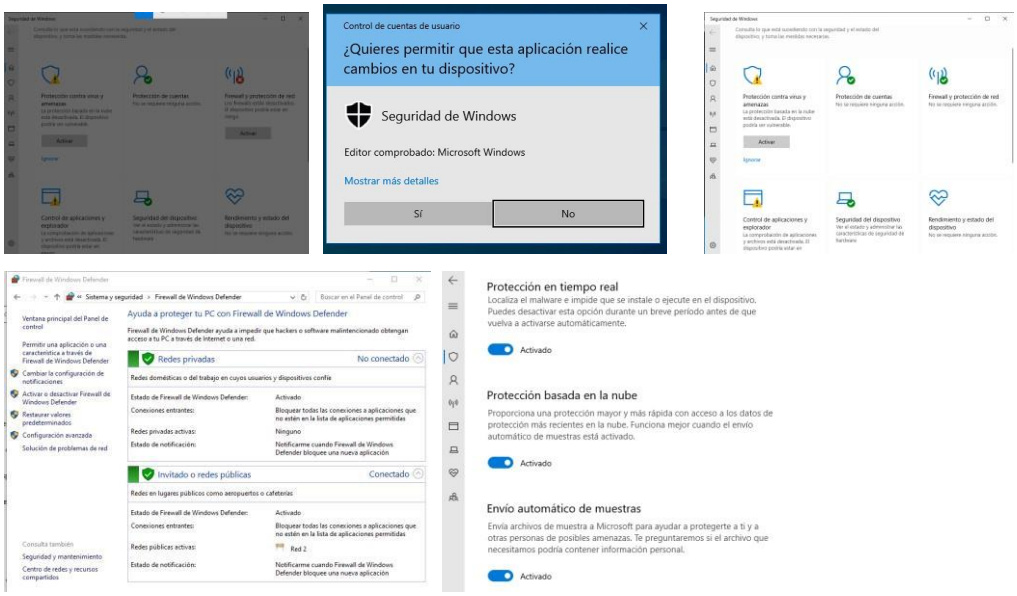
Fuente: El autor.

2.3 PRUEBAS BLUE TEAM

Para la implementación de las pruebas blue team, el caso de la empresa hacker House, requiere que el equipo blue team realice el endurecimiento de las medidas de seguridad (Hardening) en la maquina w10, contenga el ataque y recomiende medidas para que no se vuelva a presentar el incidente informático.

Lo primero que realizo el equipo blue team fue subir todas las defensas del equipo w10, tal como se muestra en la figura 23.

Figura 23. Subir las defensas en w10



Fuente: El autor.

El antivirus activó la protección en tiempo real detectando de inmediato la amenaza el malware que uso el atacante como payload (PoC_9103788.exe) para realizar el acceso

remoto al equipo, en la figura se puede observar como el antivirus bloqueo este programa y lo mando a la cuarentena, como se muestra en la figura

Figura 24. Detección del payload malware.

Fuente: El autor.

Luego de identificado el payload se procedió a eliminar por completo el Payload del sistema, en acciones, quitar, en la ventana del antivirus.

Además, se activó el firewall de Windows, el cual nos permite bloquear cualquier conexión hacia el equipo de acuerdo con las reglas establecidas.

Con esto se mitigo el ataque, al mantener el antivirus actualizado con la protección en tiempo real, este nos protegerá en caso de descargar cualquier archivo malware que tenga en su base de datos.

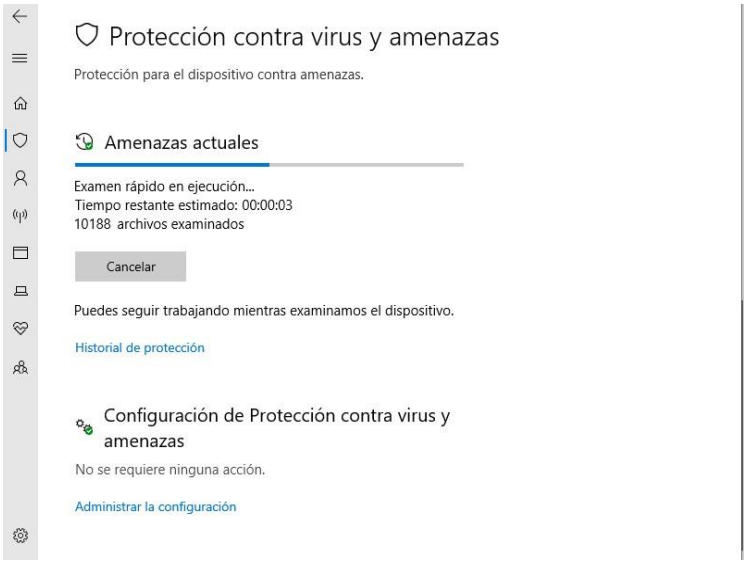
Smart Screen es una herramienta de seguridad integrada en el sistema operativo Windows que tiene como objetivo proteger al usuario de posibles amenazas en línea como malware, phishing y descargas potencialmente riesgosas. Funciona analizando los

archivos y aplicaciones que se descargan desde internet y proporciona una advertencia o bloquea la descarga si se considera una posible amenaza.

Al evaluar el alcance del ataque, nos pudimos dar cuenta que el atacante eliminó un archivo del escritorio, pero no casó mayores daños al sistema operativo, por lo tanto, solo afecto a la información del escritorio.

Se ejecuto un escaneo completo del equipo para verificar que no haya más archivos malware alojados en los discos de almacenamiento del equipo:

Figura 25. Escaneo de amenazas.



Fuente: El autor.

Se activo las actualizaciones automáticas para mantener el equipo con las últimas versiones de software y así estén más protegidos.

Se recomienda mantener las copias de seguridad al día para recuperar los archivos eliminados, si se tenía esta política es posible recuperar toda la información borrada por el ataque o parte de ella.

Aumentar la seguridad del sistema: una vez subsanado el problema, es importante tomar medidas de seguridad adicionales para evitar futuros ataques. Esto puede incluir implementar un sistema de detección de intrusiones, un firewall de última generación, entre otros.

Se dejo como recomendación Capacitar al personal, ya que el eslabón más débil en la cadena de seguridad es el factor humano. Por lo tanto, es importante capacitar al personal en temas de seguridad informática y concienciar sobre la importancia de tomar medidas de seguridad en todo momento.

Monitorear el sistema: finalmente, es necesario monitorear constantemente el sistema en busca de posibles señales de un nuevo ataque o explotación de vulnerabilidades. Esto nos permitirá actuar de manera rápida y efectiva en caso de una nueva amenaza.

3. RECOMENDACIONES

A continuación, se presentan varias recomendaciones que complementan los temas desarrollados para la parte técnica, legal y de gestión de los equipos red team y blue team.

3.1 RECOMENDACIONES ETICA Y LEGALES

Los equipos red team y blue team deben revisar de forma minuciosa los acuerdos que se firmen con las empresas a las cuales les van a prestar sus servicios, ya que se puede presentar, irregularidades, que podría ve comprometido a los equipos en prácticas poco legales, todos debe hacerse acorde a las leyes vigentes en el país correspondiente y con ética.

Según el código de ética de copnia[4], los profesionales de ingeniería deben actuar con dignidad, honradez y responsabilidad en el desempeño de sus funciones, y deben cumplir con las leyes y regulaciones aplicables en su área de trabajo.

Es importante resaltar que tanto las empresas como los empleados deben cumplir con sus obligaciones y responsabilidades establecidas en el acuerdo de confidencialidad para garantizar la seguridad de la información y mantener la confianza de los clientes, pero al mismo tiempo debe tener ética y legalidad.

[4] COLOMBIA. CONCEJO PROFESSIONALNACIONAL DE INGENIERIA [sitio web], BOGOTA: COPNIA [consultado 22 de febrero 2024], disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

3.2 RECOMENDACIONES RED TEAM

CVE (Common Vulnerabilities and Exposures) es un sistema de identificación de vulnerabilidades y exposiciones comunes en el ámbito de la seguridad informática[5]. Cada CVE asigna un identificador único a una vulnerabilidad específica, lo que permite a los profesionales de la seguridad y a los investigadores hacer un seguimiento y referencia precisa de los problemas de seguridad.

El pentesting, también conocido como prueba de penetración, es un proceso que se utiliza para evaluar la seguridad de un sistema informático. este proceso consta de varias etapas:

• recopilación de información / enumeración (footprinting): en esta fase, se recolecta toda la información posible sobre el objetivo. esto puede incluir el escaneo de dominios/ips/puertos/versiones/servicios, el uso de herramientas automatizadas para obtener información del objetivo y la obtención de metadatos.

• análisis de vulnerabilidades: esta fase consiste en realizar todas las posibles acciones que permitan comprometer al objetivo, los usuarios y/o su información.

• explotación de vulnerabilidades: en esta fase, se aprovechan las vulnerabilidades encontradas en la fase anterior.

• post-explotación: esta fase consiste en, una vez logrado entrar al sistema mediante las anteriores fases, lograr credenciales o permisos de administrador, o incluso vulnerar otros

[5] CIBERSEGURIDAD:COM [sitio web], ESPAÑA: WORDPRESS [consultado el 23 de febrero de 2024] disponible en: ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes (ciberseguridad.com).

sistemas de mayor importancia dentro de la organización objetivo mediante técnicas de pivoting o similares.

• reporte: en esta fase, se elabora un informe detallado de los hallazgos y se proporcionan recomendaciones para mitigar las vulnerabilidades encontradas.

la etapa de footprinting es una de las más importantes en el pentesting. esta fase, también conocida como recopilación de información, consiste en recopilar tanta información como sea posible sobre los sistemas y redes objetivo, así como sobre sus propietarios, sin intentar infiltrarse. esta información puede incluir detalles técnicos, como las direcciones de ip, y detalles personales, como los nombres y cargos de los empleados. esta información puede ser invaluable para entender mejor el entorno objetivo y planificar ataques más efectivos.

Contar con un conjunto de herramientas open source, asegura al equipo de red team, poder realizar las diferentes pruebas en el ejercicio del pentesting articulado con los CVE, que proporciona información de vulnerabilidades conocidas y tener en su banco de prueba un kali linux con la herramienta por excelencia metasploit, es sumamente recomendado para que el equipo red team pueda realizar bien su labor.

3.3 RECOMENDACIONES BLUE TEAM

Es una buena recomendación para el equipo de blue team contar con sistemas de detección de intrusiones, para esto se recomienda el uso de SIEM y XDR, a continuación, se muestran las principales diferencias entre cada una de acuerdo a una tabla comparativa:

Tabla 2. Diferencias entre SIEM y XDR

	SIEM	XDR
Significado	Sistema de Información y Eventos de Seguridad	Plataforma de respuesta y detección extendida
Diseño y función	Uno de sus principales objetivos es la gestión de toda la información relacionada con seguridad y eventos en una organización para proporcionar una visión centralizada y completa en tiempo real respecto al estado de la seguridad.	Su diseño incluye una arquitectura que permite la detección de amenazas, análisis de los vectores de ataque, mejorar la comprensión de infracciones y automatizar la respuesta.
Escalabilidad	Tiene un enfoque vertical, lo que significa que se implementa una solución específica para cada funcionalidad. Esto hace que sea difícil escalar la infraestructura	El usar una arquitectura horizontal permite la agregación de datos de múltiples fuentes y el enriquecimiento de los datos con información externa, lo que le da escalabilidad a la solución modular.
Detección y correlación de eventos	El SIEM recolecta y almacena datos de diversas fuentes de eventos de seguridad, y los *correlaciona* para	La plataforma XDR recolecta y *analiza* amplios datos, como registros de firewall, registros de eventos de

	identificar patrones y anomalías que puedan indicar una amenaza.	acceso, correos electrónicos y datos recolectados de endpoints para detectar eventos sospechosos.
Detección de amenazas	Con SIEM, la detección de amenazas se basa en la correlación de eventos. Estos eventos pueden ser agrupados en una única vista para dar una idea de la situación y permitir alertas	XDR utiliza algoritmos de inteligencia artificial y machine learning para identificar patrones y diferenciar entre eventos normales y amenazas potenciales, lo que permite la detección de amenazas avanzadas
Respuesta a incidentes	SIEM tiene en cuenta las alertas y datos históricos para automatizar la respuesta a incidentes,	XDR utiliza algoritmos de inteligencia artificial y machine learning para identificar patrones y diferenciar entre eventos normales y amenazas potenciales, lo que permite la detección de amenazas avanzadas
Integración	SIEM se integra con múltiples herramientas de seguridad para proporcionar una funcionalidad adicional como detección de fraude,	XDR permite una acción contención inmediata en caso de un ataque, aislamiento de dispositivos

	protección de la red y gestión de incidentes	

Fuente: El autor

También se recomienda el uso de herramientas con licencia GPL, tales como SNORT, SURICATA y OSSEC, a continuación, se presenta una breve descripción de cada una:

SNORT

Snort es una herramienta de detección de intrusos y prevención de intrusiones de código abierto bajo la GPL. Utiliza reglas basadas en firmas para identificar e informar sobre posibles ataques de red, como escaneos, intentos de acceso no autorizado o tráfico malicioso. Snort también cuenta con un lenguaje de reglas flexible y una comunidad activa que contribuye con nuevas reglas y actualizaciones constantes.

SURICATA

Suricata8 es otra herramienta de detección de intrusos y prevención de intrusiones de código abierto con licencia GPL. Al igual que Snort, utiliza reglas basadas en firmas para detectar posibles ataques de red, pero también cuenta con un motor de reglas basado en el protocolo y la aplicación que puede detectar patrones de tráfico malicioso más complejos. Suricata es una herramienta más reciente que Snort, pero ha ganado popularidad gracias a su rendimiento y capacidad de inspeccionar tráfico en tiempo real.

OSSEC

Ossec es un sistema de detección de intrusos de host (HIDS) de código abierto con licencia GPL. Se enfoca en la detección de actividad maliciosa en sistemas individuales,

como intentos de acceso no autorizado, modificaciones de archivos críticos y cambios en la configuración del sistema. Además, Ossec puede analizar registros de eventos y realizar correlación de eventos para detectar patrones de

4. CONCLUSIONES

La ejecución de labores en ciberseguridad debe estar siempre enmarcadas dentro de las leyes nacionales y acuerdos internacionales vigentes y código de ética vigente para el ejercicio de la profesión.

Las leyes de protección de sistemas informáticos y la ley de protección de datos personales, son las principales leyes colombianas, así como el convenio Budapest, el cual es un convenio entre varios países del mundo, proporcionan un limite para la ejecución de labores en ciberseguridad, de las cuales los profesionales en ciberseguridad, debemos tener presentes al momento de firmar acuerdo para la ejecución de pruebas de pentesting, para no incurrir en delitos informáticos que nos puedan afectar con sanciones legales o éticas.

La etapa de prueba de vulnerabilidades o intrusiones, permiten a las organizaciones mejorar la seguridad de sus sistemas, redes e infraestructura, permitiendo tomar acciones tempranas para fortalecer la seguridad, el equipo red team se encarga de esta labor.

El fortalecimiento de la seguridad, activación de defensas tales como antimalware, firewall, contraseñas seguras, software de detección de intrusiones, ejecución de archivos sospechosos en ambientes aislados, son labores de las que se encarga el equipo Blue Team, ayudan a las organizaciones a estar protegidas responder ante ataques informáticos.

La colaboración conjunta de los equipos estratégicos red team y blue team, permiten las organizaciones, estar siempre revisando y fortaleciendo la seguridad, en este mundo digital que esta en continuo cambio, y donde las técnicas que utilizan los ciberdelincuentes son cada vez más sofisticadas y difíciles de detectar.

BIBLIOGRAFIA.

- BARRÍA HUIDOBRO, C. "Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio" Editorial ebooks Patagonia – Ediciones UM, 2020. ISBN 9789563560315.

- BEJTLICH, R. Blue Team Operator's Guide: Essential Tools and Techniques for the Cybersecurity Incident Responder [Standards governing body]. (ISO/IEC 1486-3:2016). 2016

- BUDAPEST. SERIE TRATADOS EUROPEOS. Convenio. [en línea] (23, noviembre, 2001) [consultado 7, marzo, 2024]. Convenio sobre la ciberdelincuencia. Disponible en Internet: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

- CCN Cert. "Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6". [sitio web]. [fecha consulta: 26 de marzo de 2024], CCN Cert, 2018. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

- CIS SECURITY. "CIS Center for Internet Security. CIS Benchmarks. [sitio web] [fecha consulta: 27 de marzo de 2024] disponible en: https://www.cisecurity.org/cis-benchmarks/

- CLARK, B. (n.d.). Building and Running a Blue Team [Standards governing body]. [Standard number].

- COLOMBIA. CONCEJO PROFESSIONALNACIONAL DE INGENIERIA [sitio web], BOGOTA: COPNIA [consultado 22 de febrero 2024], disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 [en línea]. (5, enero,2009) [consultado el 3, marzo,2024], Ley de la protección de la información y de los datos. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581 [en línea], (17, octubre, 2012) [consultado 5, marzo, 2024]. Ley de la protección de datos personales. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

- EDWARDS, J., & Davidson, R. The Art of Blue Team: Practical Insights for Your Cybersecurity Program [Standards governing body]. (ISO/IEC 1486:2016). 2016.

- HARMON, M. J., & HOLCOMB, M. O. (2018). Blue Team Operations: Defending against Targeted Attacks. Wiley.

- INCIBE. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. [sitio web], [fecha consulta: 24 de marzo de 2024], INCIBE (2019), disponible en: https://www.incibe.es/PROTEGE-TU-EMPRESA/BLOG/EL-PENTESTING-AUDITANDO-SEGURIDAD-TUS-SISTEMAS

- MINTIC, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [sitio web] [fecha consulta:28 de marzo de 2024], (2018). (p. 14 - 27). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- MINTIC. Guía de Auditoria. [sitio web] [fecha consulta: 23 de marzo de 2024], Mintic. (2018) (pp. 12-19). Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

- MORENO, Patricio. Técnicas de detección de ataques en un sistema SIEM. [sitio web] [fecha consulta: 22 de marzo de 2024], (Security Information and Event Management. Usfq. (pp. 31-63). Disponible en Internet: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

- MURDOCH, D. (n.d.). Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder [Standards governing body]. [Standard number]. (IEC 1486:2016).

- VERDI, J., & KIM, P. Cybersecurity Red Team Strategies: A Practical Guide to Building a Back Doors and Bypassing Defenses. Packt Publishing. 2017

- WHITE, A. J., & Clark, B. Blue Team Field Manual (BTFM). [Standards governing body]. ISO 1486-2. 2017

- ZENKO, M.The Red Team: How to Succeed by Thinking Like the Enemy. Basic Books. (2015).

ANEXO 1. ENLACE AL VIDEO

LINK: https://youtu.be/bvszf9_toey

ANEXO 2. PRUEBA TURNITING