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

YESENIA BALLESTAS GUTIERREZ

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

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

YESENIA BALLESTAS GUTIERREZ

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

John F. Quintero
Docente Especialización en Seguridad Informática UNAD

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

Resumen

En resumen, la implementación de ciberseguridad en una organización es esencial para proteger sus activos y operaciones en un mundo digitalmente conectado y en constante evolución. Los beneficios van más allá de la mera protección de datos, ya que también afectan positivamente a la reputación, la eficiencia y la continuidad del negocio.

La implementación de equipos de Red Teams, Blue Teams y Purple Teams en una organización es una estrategia integral para fortalecer la ciberseguridad y garantizar una respuesta efectiva a las amenazas cibernéticas.

Los equipos de Red Team desempeñan un papel fundamental al exponer debilidades y vulnerabilidades en la infraestructura y las políticas de seguridad antes de que los actores maliciosos las exploren. Esta identificación proactiva permite a la organización tomar medidas preventivas para mitigar riesgos.

Los equipos de Blue Team se centran en la detección y respuesta a incidentes en tiempo real. Su capacitación y preparación continuas les permiten tomar medidas inmediatas para limitar el daño en caso de una amenaza cibernética.

La colaboración entre Red Teams y Blue Teams, facilitada por los Purple Teams, impulsa la mejora continua de las defensas cibernéticas. Esto incluye la optimización de políticas, procedimientos y tecnologías de seguridad.

La implementación de estos equipos permite una evaluación más completa y holística de la seguridad cibernética de la organización. Esto no solo abarca la tecnología, sino también la cultura de seguridad y la conciencia de los empleados.

La educación y la concienciación en seguridad se fomentan en toda la organización. La seguridad se convierte en una responsabilidad compartida, desde la alta dirección hasta el personal de nivel operativo.

La práctica regular y la colaboración entre equipos ayudan a la organización a estar mejor preparada para enfrentar las amenazas cibernéticas en constante evolución. Esto incluye amenazas emergentes y nuevas tácticas de ataque.

La implementación de estos equipos ayuda a la organización a cumplir con los requisitos normativos de seguridad de datos, lo que puede proteger su reputación y evitar sanciones.

La ciberseguridad se integra en la estrategia de negocio, lo que garantiza la continuidad de las operaciones y protege la inversión en tecnología y datos.

En resumen, la implementación de equipos de Red Teams, Blue Teams y Purple Teams no solo es esencial para fortalecer la seguridad cibernética de una organización, sino que también promueve una cultura de seguridad, la adaptación a las amenazas

cambiantes y la protección de la reputación empresarial. Estos equipos son una parte crítica de la defensa contra las amenazas cibernéticas en un mundo digitalmente conectado.

Índice

Lista de ilustraciones

Lista de Tablas

1 Glosario

- Blue Team: El equipo Blue Team es responsable de defender los sistemas y las redes de una organización contra ataques. Su objetivo principal es mantener la seguridad y la integridad de los sistemas informáticos.

- Red Team: El equipo Red Team es responsable de realizar pruebas de penetración y evaluar la seguridad de los sistemas y las redes de una organización. Su objetivo principal es identificar vulnerabilidades y debilidades en los sistemas para ayudar a mejorar la seguridad.

- Purple Team: El equipo Purple Team es una combinación del equipo Red Team y el equipo Blue Team. Su objetivo principal es fomentar la colaboración y la comunicación entre los equipos Red y Blue. El equipo Purple Team trabaja en estrecha colaboración con ambos equipos para mejorar la seguridad general de una organización.

- Vulnerabilidad: Es una debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada o activada por una fuente de amenaza.

- Evaluación de vulnerabilidad: Es el proceso de prueba utilizado para identificar y asignar niveles de gravedad a tantos defectos de seguridad como sea posible en un período de tiempo determinado. Este proceso puede involucrar técnicas automatizadas y manuales con diferentes grados de rigor y un énfasis en la cobertura integral.

- Ciberseguridad: Conjunto de prácticas, medidas y tecnologías diseñadas para proteger sistemas, redes y datos contra amenazas y ataques cibernéticos.

- Amenaza Cibernética: Cualquier actividad, evento o entidad que tiene el potencial de comprometer la seguridad de los sistemas de información.

- Ataque Cibernético: Un intento deliberado de dañar, robar, comprometer o acceder no autorizado a sistemas informáticos o datos.

- Firewall: Un dispositivo o software que actúa como una barrera de seguridad entre una red privada y redes externas, controlando el tráfico entrante y saliente.

- Antivirus: Software diseñado para detectar, prevenir y eliminar malware y virus informáticos.

- Autenticación: Proceso de verificar la identidad de un usuario o sistema antes de otorgar acceso a recursos protegidos.

- Autorización: Proceso de determinar qué acciones o recursos tiene permitido acceder o realizar un usuario después de la autenticación.

- Cifrado: Proceso de convertir datos en un formato ilegible para proteger su confidencialidad durante la transmisión o el almacenamiento.

- VPN (Red Privada Virtual): Tecnología que crea una conexión segura y encriptada entre dos puntos en una red, generalmente a través de Internet.

- Phishing: Ataque en el que los atacantes se hacen pasar por entidades legítimas para engañar a las personas y obtener información confidencial.

- Malware: Software malicioso diseñado para dañar, robar o comprometer sistemas y datos. Incluye virus, troyanos, ransomware y spyware.

- Actualización de Software: Aplicar parches y actualizaciones para corregir vulnerabilidades de seguridad en programas y sistemas operativos.

- Política de Seguridad: Conjunto de reglas y directrices que definen cómo se debe gestionar y proteger la seguridad de la información en una organización.

- Evaluación de Vulnerabilidades: Proceso de identificar y evaluar las debilidades y vulnerabilidades en sistemas y aplicaciones para corregirlas.

- Equipo de Respuesta a Incidentes de Seguridad (CSIRT): Grupo de expertos que responden a incidentes de seguridad, investigan amenazas y coordinan la respuesta ante incidentes.

- Control de Acceso: Medidas y políticas que limitan y gestionan el acceso a sistemas y datos solo a usuarios autorizados.

- Seguridad de la Nube: Prácticas y tecnologías para proteger los datos y servicios alojados en entornos de nube pública o privada.

- Seguridad de la Red: Medidas y protocolos para proteger la integridad y la confidencialidad de la comunicación en una red.

- Copias de Seguridad (Backups): Réplicas de datos críticos que se almacenan de forma segura para su recuperación en caso de pérdida o daño.

- Plan de Continuidad del Negocio: Estrategia que garantiza la continuidad de las operaciones de la organización en caso de desastres o incidentes de seguridad.

- Auditoría de Seguridad: Evaluación independiente de los controles y políticas de seguridad para garantizar su cumplimiento y eficacia.

- Criptografía de Clave Pública y Privada: Sistema de cifrado que utiliza un par de claves: una pública para cifrar y una privada para descifrar datos.

- Intrusión: Acceso no autorizado a sistemas o redes, a menudo con la intención de robar información o dañar recursos.

- Multifactor de Autenticación (MFA): Método de seguridad que requiere dos o más formas de autenticación antes de otorgar acceso, como contraseña y token.

- Gestión de Identidad y Acceso (IAM): Conjunto de procesos y tecnologías para administrar y proteger las identidades y el acceso de los usuarios a sistemas y recursos.

2 Introducción

La ciberseguridad se ha convertido en un componente esencial de la estrategia empresarial en la era digital, ya que las amenazas cibernéticas continúan evolucionando y representan un riesgo significativo para la seguridad de los datos y la continuidad de los negocios. En este contexto, la colaboración y la preparación efectiva se han vuelto fundamentales para mantener la seguridad de una organización. Es aquí donde entran en juego las prácticas de Red Teams, Blue Teams y Purple Teams.

Red Teams son equipos de expertos en seguridad cibernética que simulan ataques cibernéticos realistas para evaluar la resistencia de una organización a las amenazas. Su objetivo es descubrir debilidades en las defensas de una organización y, al hacerlo, ayudar a fortalecer la seguridad al identificar vulnerabilidades antes de que los actores maliciosos las exploren.

Blue Teams, por otro lado, son los equipos de defensa. Están encargados de proteger activamente la infraestructura de TI y los datos de una organización contra amenazas cibernéticas. Su enfoque principal es detectar, prevenir y responder a incidentes de seguridad en tiempo real, utilizando tecnología y prácticas de seguridad avanzadas.

Luego, tenemos a los Purple Teams, que representan una fusión de Red Teams y Blue Teams. Estos equipos trabajan juntos para mejorar la seguridad cibernética de una organización. Los Purple Teams no solo identifican debilidades en la infraestructura y las políticas de seguridad (como lo hacen los Red Teams), sino que también colaboran con los Blue Teams para asegurarse de que se tomen medidas efectivas para abordar y corregir esas debilidades.

En este contexto, exploraremos en detalle cómo estas prácticas colaborativas pueden fortalecer la ciberseguridad de una organización y proporcionar una visión más completa y estratégica de las amenazas cibernéticas. La integración efectiva de Red Teams, Blue Teams y Purple Teams no solo ayuda a proteger contra las amenazas actuales, sino que también prepara a una organización para enfrentar los desafíos futuros en el panorama de la ciberseguridad.

3 Objetivo General

Fortalecer la postura de seguridad cibernética de la organización mediante la implementación efectiva de prácticas de Red Teams, Blue Teams y Purple Teams, con el fin de identificar, mitigar y prevenir proactivamente las amenazas cibernéticas, garantizando así la protección de los activos digitales y la continuidad de las operaciones.

3.1 Objetivos Específicos

- Realizar evaluaciones regulares de la infraestructura de TI y las políticas de seguridad de la organización utilizando el equipo Red Team para identificar y documentar vulnerabilidades y debilidades.

- Colaborar estrechamente entre el equipo Blue Team y el equipo Purple Team para mejorar la capacidad de respuesta a incidentes mediante la identificación temprana de amenazas y la implementación de procedimientos y soluciones eficaces.

- Promover la conciencia de seguridad en toda la organización mediante la capacitación continua y la comunicación efectiva, lo que incluye compartir lecciones aprendidas y buenas prácticas de seguridad entre todos los equipos.

4 Evaluación de acciones de los equipos red team & blue team de una organización en el marco de los criterios éticos y legales

4.1 Ley 1273 de 2009 del 05ENE29

"por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Artículo 1. Adicionar al Código Penal un Título VII BIS denominado “De la Protección de la Información y de los datos. (República, 2009)

Definiciones principales: La presente Ley cuenta con dos capítulos denominados:

Capítulo I: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Capítulo II: De los atentados informáticos y otras infracciones.

Al realizar la lectura de los anteriores capítulos se evidencia en su articulado la definición de aspectos relacionados con la protección de la información, soportado en los pilares de confidencialidad, integridad y disponibilidad, de igual manera se da soporte legal a temas relacionados especialmente con la tipificación del hurto por medios informáticos.

De acuerdo con lo anterior se exponen las siguientes definiciones de interés, en el marco de los planteados en la Ley 1273 de 2009:

Capítulo I:

Artículo 269A: **ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** Este articulo está relacionado cuando un ciberdelincuente se aprovecha de la vulnerabilidad en el acceso a un sistema informático, o por falta de procedimientos y/o controles de seguridad informática de una organización o persona.

Articulo 269B: **OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.** Este artículo se aplica cuando un ciberdelincuente bloquea su ingreso en forma ilegal un sistema, o cuando se presentan accesos a cuentas de correos electrónicos sin el debido consentimiento de sus propietarios.

Artículo 269C: **INTERCEPTACIÓN DE DATOS INFORMÁTICOS**. Este articulo se aplica cuando se identifica que una persona utiliza recursos tecnológicos, sin autorización legal capturando información de un sitio oficial, un sistema informático, emisiones electromagnéticas.

Artículo 269D. **DAÑO INFORMÁTICO.** Trata cuando una persona sin autorización, destruya, dañe, borre, deteriore, altere o suprima datos del programa o documentos electrónicos.

Artículo 269E. **USO DE SOFTWARE MALICIOSO.** Está relacionado con la proliferación de malware (produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga) de diferentes tipos en internet causando daño en los dispositivos digitales.

Artículo 269F. **VIOLACIÓN DE DATOS PERSONALES**. La finalidad del presente artículo es la protección de los derechos fundamentales y dignidad humana. Se aplica cuando una persona sin autorización obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales obteniendo información con el objetivo de obtener información personal.

Artículo 269G. **SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.** La finalidad del presente artículo es la protección de los derechos fundamentales y dignidad humana. Se aplica cuando una persona sin autorización diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes obteniendo información personal. Conocido bajo el termino de “Phishing”, cuando un ciberdelincuente utiliza técnicas de engaño para suplantar una página web legitima, un dominio o correo electrónico para obtener información personal.

Artículo 269H. **CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA**. Incremento de las penas listadas anteriormente de la mitad a las tres cuartas partes.

CAPITULO II

Artículo 269I: **HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES**. Manipulación de un sistema informático superando las medidas de seguridad instaladas.

Artículo 269J: **TRANSFERENCIA NO CONSENTIDA DE ACTIVOS**. Manipulación informática no autorizada con el fin de obtener transferencia activos y el que fabrique, introduzca, posea o facilite programa de computador para la comisión de un delito

4.2 Ley 1581 de 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales."

Protege el derecho que tenemos los colombianos a conocer, actualizar y rectificar la información que se haya recogido en bases de datos o archivos que sean susceptibles de tratamiento por entidades de públicas o privadas.

Es de obligatorio cumplimiento e implementación en las entidades la creación de una política de tratamientos de datos públicos, privados y sensibles.

La entidad que vigila la ley de protección de datos personales es la "Superintendencia de Industria y Comercio", quien informa a través de sus diferentes medios la no obligatoriedad de otorgar la información para el tratamiento de datos sensibles a la población colombiana.

Esta ley regula la protección de datos personales, la cual son técnicas jurídicas e informáticas encaminadas a garantizar los derechos de las personas sobre el control de su información personal y sobre los pilares de la seguridad de la información, confidencialidad, integridad y disponibilidad.

Los titulares de los datos personales tenemos derecho a conocer, actualizar y rectificar los datos personales, revocar la autorización y Solicitar la supresión de los datos

Las sanciones de la ley 1581 son realizadas por la Superintendencia de industria y comercio, y las impone a los responsables del tratamiento las cuales se lista textualmente:

a) 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. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) 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;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

4.3. Pentesting

Es un practica de seguridad informática (ataque simulado y controlado malicioso a sistemas informáticos) con el fin de identificar posibles vulnerabilidades. Se realiza con el fin de identificar fallas de seguridad en los sistemas, validar los controles de seguridad aplicados, cumplimiento de las normas de seguridad y privacidad.

4.3.1 Etapas Pentesting

a. Recopilación y planificación:

recolección de la mayor cantidad de información del objetivo. Dependiendo del objetivo se realizan las siguientes actividades:

- ✓ Escaneo de dominios/IPs/puertos/versiones/servicios
- ✓ Dorking
- ✓ Uso de herramientas automatizadas para obtener información de nuestro objetivo
- ✓ Obtención de metadatos

Herramientas más utilizadas:

- ✓ Nmap
- ✓ Dnsmap
- ✓ Dnsrecon
- ✓ Recon-ng
- ✓ SubFinder
- ✓ Etc

b. Análisis de vulnerabilidades:

realizar todas las posibles acciones que nos permitan comprometer a nuestro objetivo, los usuarios y/o su información. Se aprovechan las siguientes vulnerabilidades:

- ✓ Pérdida del control de acceso (Broken Access Control)
- ✓ Fallos criptográficos (Cryptographic Failures)
- ✓ Inyección (Injection)
- ✓ Diseño Inseguro (Insecure Desing)
- ✓ Configuración de seguridad defectuosa (Security Misconfiguration)
- ✓ Componentes vulnerables y obsoletos (Vulnerable and Outdated Components)
- ✓ Fallos de identificación y autenticación (Identification and Authentication Failures)

- ✓ Fallos en el software y en la integridad de los datos (Software and Data Integrity Failures)
- ✓ Fallos en el registro y la supervisión de la seguridad (Security Logging and Monitoring Failures)
- ✓ Falsificación de Solicitud del Lado del Servidor (Server-side Request Forguery o SSRF)

Algunas de las herramientas más usadas en esta fase son las siguientes:

- ✓ Nessus
- ✓ OWASP Zap Proxy
- ✓ BugBounty Recon
- ✓ Vega
- ✓ BurpSuite
- ✓ etc

c. Explotación de Vulnerabilidades:

Aprovechamiento (“explotar”) las vulnerabilidades identificadas en la fase anterior, es decir: ejecutamos exploits contra las vulnerabilidades identificadas o simplemente hacemos uso de credenciales obtenidas en la fase anterior para obtener acceso a los sistemas objetivos.

Algunas de las herramientas más utilizadas son:

- ✓
- ✓ OpenVAS
- ✓ Nessus
- ✓ BeEF
- ✓ Metasploit Framework
- ✓ Routersploit
- ✓ PowerSploit
- ✓ SPARTA
- ✓ Xarp
- ✓ SQLMap
- ✓ BurpSuite
    - ✓ Canvas
    - ✓ etc

d. Post Explotación – escalar privilegios.

La fase de post explotación no siempre es aplicable. Consiste en, una vez logrado entrar al sistema mediante las anteriores fases, lograr credenciales o permisos de administrador, el objetivo de esta fase es escalar privilegios con la finalidad de obtener una cuenta con todos los privilegios habilitados sobre el sistema.

En función de la vulnerabilidad encontrada, se intentarán realizar algunas de las siguientes acciones:

- ✓ Obtener información confidencial
- ✓ Evadir mecanismos de autenticación
- ✓ Realizar acciones del lado de los usuarios
- ✓ Acceder a otros sistemas o servicios accesibles desde el sistema comprometido
- ✓ Realizar acciones sin el consentimiento y/o conocimiento de la organización comprometida

Algunas de las herramientas que podemos utilizar en la fase de post explotación son las siguientes:

- ✓ Empire
- ✓ Enumdb
- ✓ Mimikatz
- ✓ Poet
- ✓ Pwnat
- ✓ TheFatRat
- ✓ AutoSploit
- ✓ RemoteRecon
- ✓ ShellPop
- ✓ Arpag
- ✓ GhostPack
- ✓ Metasploit
- ✓ PowerHub
- ✓ Lolbas and Llolbas
- ✓ PHPSploit
- ✓ Swap_Digger
- ✓ Netcat
- ✓ etc

e. Reporte – Informe

reporte definitivo de vulnerabilidades, comúnmente conocido como “informe de vulnerabilidades”. Es en esta última fase donde se informa las actividades realizadas en el test de intrusión.

Herramientas utilizadas para elaborar informes de vulnerabilidades son:

- ✓ Dradis
- ✓ Faraday
- ✓ Simple Vulnerability Manager
- ✓ etc

4.3.2 Footprinting

Es la primera parte para recolectar información sobre hardware o red. Se trata de un procedimiento de exploración para conocer el objetivo, se debe acumular toda la información posible, puede desarrollase de forma activa o pasiva.

- Huella activa: realizar una huella al ponerse en contacto directo con la máquina de destino.

- Huella pasiva: recopilar información de un sistema ubicado a una distancia remota del atacante.

A través del Footprinting se puede conocer:

- ✓ Sistema operativo de la máquina de destino.
- ✓ Cortafuegos
- ✓ Dirección IP
- ✓ Mapa de red
- ✓ Configuraciones de seguridad de la máquina de destino
- ✓ Identificación de correo electrónico, contraseña
- ✓ Configuraciones de servidor
- ✓ URLs
- ✓ VPN

Fuentes de información :

- Redes sociales
    - Google: uso de «Google Dorks».
    - Ingeniería social
    - Archieve.org: La versión archivada de sitio web.
    - Sitio web de una organización
    - Neo Trace: La pantalla gráfica muestra la ruta entre usted y el sitio remoto, incluidos todos los nodos intermedios y su información.
    - Who is: Este es un sitio web donde se puede conocer información sobre el nombre de dominio, la identificación de correo electrónico, el propietario del dominio, etc.

4.3.3 Metasploit

Metasploit Framework es un marco de código abierto basado en Ruby utilizados por especialistas de seguridad de la información y ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema. Cuenta con varias herramientas de explotación y herramientas de prueba de penetración. Los ciberdelincuentes pueden usar maliciosamente estas mismas capacidades de Metasploit para identificar y explotar vulnerabilidades en un sistema objetivo.

El marco de Metasploit es una herramienta utilizada para investigar vulnerabilidades en redes y servidores. Metasploit tiene funciones avanzadas:

- ✓ Explotación manual
- ✓ Evasión de antivirus e IPS / IDS
- ✓ Pivote de proxy
- ✓ Módulos posteriores a la exploración
- ✓ Limpieza de sesión
- ✓ Reutilización de credenciales
- ✓ Ingeniería social
- ✓ Generador de carga útil
- ✓ VPN pivotante
- ✓ Validación de vulnerabilidades
- ✓ Pruebas de aplicaciones web.

La arquitectura de Metasploit Framework:

Las interfaces son las diferentes plataformas a través de las cuales los usuarios pueden acceder a Metasploit Framework.

Hay cuatro interfaces disponibles:

- ✓ MSFConsole (Metasploit Framework Console): la interfaz Metasploit más utilizada, la consola Metasploit permite a los usuarios acceder a Metasploit Framework a través de una interfaz de línea de comandos interactiva.

- ✓ MSFWeb: una interfaz basada en navegador que permite a los usuarios acceder al marco de Metasploit.

- ✓ Armitage: desarrollado por Raphael Mudge en 2013, Armitage es una interfaz gráfica de usuario basada en Java que permite a los equipos de seguridad colaborar compartiendo su acceso a hosts comprometidos.

- ✓ RPC (llamada a procedimiento remoto): permite a los usuarios manejar mediante programación Metasploit Framework utilizando servicios de llamada a procedimiento remoto (RPC) basados en HTTP. Además del

Ruby nativo de Metasploit, los servicios RPC pueden operar a través de otros lenguajes, como Java, Python y C.

Hay cinco tipos principales de módulos de Metasploit, clasificados según las tareas que realizan:

- ✓ Cargas útiles: las cargas útiles son códigos de shell que realizan las acciones previstas por el usuario una vez que un exploit ha comprometido un sistema objetivo. Se pueden usar para abrir Meterpreters o comandos de shells. Los Meterpreters son cargas útiles sofisticadas que se utilizan durante un ciberataque para ejecutar código y realizar más tareas exploratorias.

- ✓ Exploits: ejecuta secuencias de comandos para aprovechar las debilidades del sistema o de la aplicación y obtener acceso a los sistemas de destino.

- ✓ Publicaciones (módulos posteriores a la explotación): las publicaciones permiten a los usuarios realizar una recopilación de información más profunda e infiltrarse aún más en un sistema de destino después de la explotación. Por ejemplo, las publicaciones se pueden utilizar para realizar la enumeración de servicios.

- ✓ Codificadores: los codificadores ocultan las cargas útiles en tránsito para garantizar que se entreguen correctamente al sistema de destino y eviten la detección del software antivirus, los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS).

- ✓ NOP (No Operation): los generadores NOP crean secuencias aleatorias de bytes para evitar los sistemas de detección y prevención de intrusiones.

- ✓ Auxiliares: los módulos auxiliares incluyen escaneo de vulnerabilidades, escaneo de puertos, fuzzers, sniffers y otras herramientas de explotación.

Las herramientas de Metasploit Framework se pueden utilizar para realizar todas las etapas de las pruebas de penetración, que incluyen:

- ✓ Recopilación de información: mediante el uso de módulos auxiliares: portscan / syn, portscan / tcp, srnb version, db nmap, scanner / ftp / ftp_version y collect / shodan_search.
- ✓ Enumeración: utilizando enumshares smb / srnb, enumusers smb / srnb y smb / srnb_login.
- ✓ Obtener acceso: mediante el uso de exploits y cargas útiles de Metasploit.
- ✓ Escalada de privilegios: mediante el uso de meterpreter-use priv y meterpreter-getsystem.
- ✓ Mantener el acceso: mediante meterpreter, ejecuta la persistencia.

- ✓ Cubriendo pistas: mediante el uso de módulos anti-forenses posteriores a la explotación.

Metasploit también se integra con otras herramientas de ciberseguridad, como Nmap, Nessus y Nexpose para fortalecer sus capacidades.

4.3.4 Que es CVE

El glosario de vulnerabilidades y exposiciones comunes (CVE) es un proyecto de seguridad centrado en software de lanzamiento público, financiado por la División de Seguridad Nacional de EE. UU. y mantenido por MITRE Corporation. Recopila información sobre vulnerabilidades y exposiciones de seguridad, catalogarlas de acuerdo con varios identificadores y proporcionarles ID únicos. MITRE proporciona a cada vulnerabilidad una identificación única. Varios días después de la publicación en la base de datos de vulnerabilidades de Mitre, la Base de Datos Nacional de Vulnerabilidades (NVD) publica el CVE con un análisis de seguridad correspondiente.

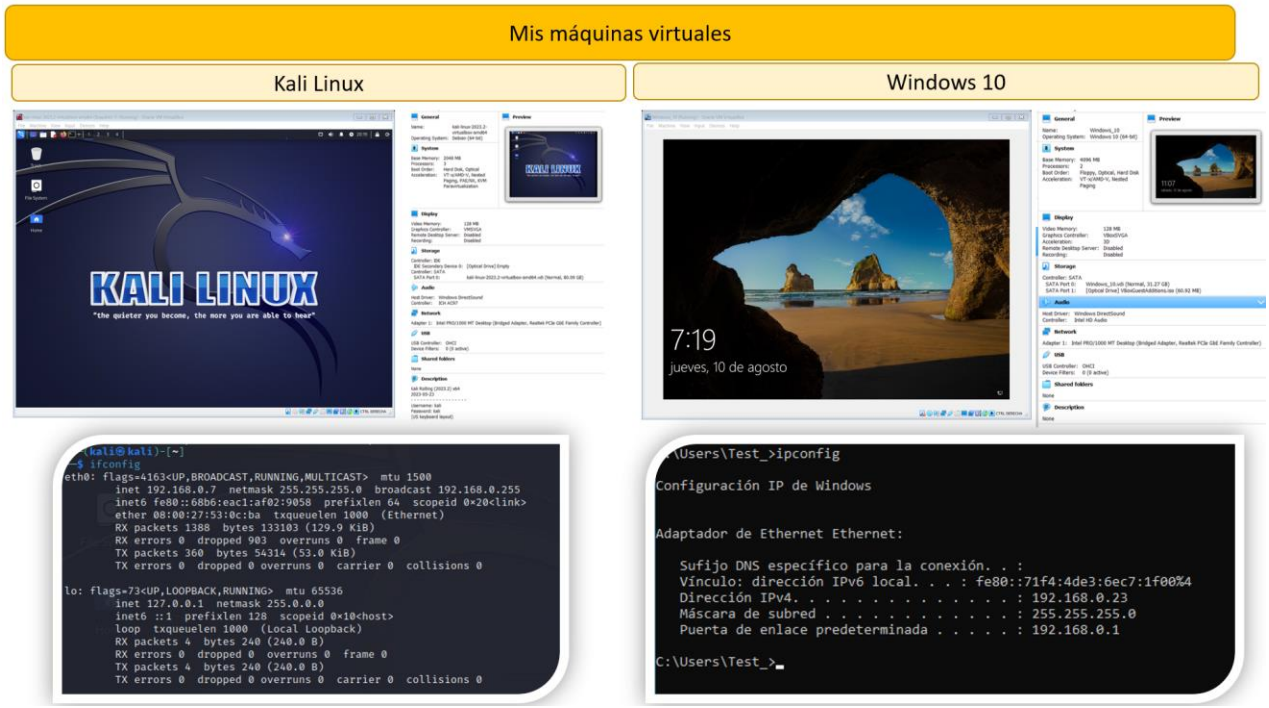
MITRE define la lista CVE como un glosario o diccionario de vulnerabilidades y exposiciones disponibles públicamente, en lugar de una base de datos y, como tal, está destinada a servir como una línea de base de la industria para comunicarse y dialogar en torno a una vulnerabilidad determinada. Según la visión del MITRE, la documentación CVE es el estándar de la industria mediante el cual avisos de seguridad dispares, rastreadores de errores y bases de datos pueden obtener una línea de base uniforme con la que «hablar» entre sí, comunicándose y deliberando sobre la misma vulnerabilidad en un «lenguaje común».

Una vulnerabilidad es una debilidad que puede explotarse en un ciberataque para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la memoria del sistema, instalar diferentes tipos de malware y robar, destruir o modificar datos confidenciales.

El objetivo de CVE es facilitar el intercambio de información sobre vulnerabilidades conocidas entre organizaciones.

4.3.5 Banco de trabajo – virtual box

Ilustración 1 - Visualización Banco de trabajo



Fuente: Realizada por Autor

5 Aspectos éticos y legales

5.1 Identificación párrafo “Acuerdo de Confidencialidad”.

Textos identificados dentro del acuerdo de confidencialidad, con acciones ilegales.

Tabla 1 - Visualización textos para estudio

Texto identificado	
No.	**Información Confidencial**
1	2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”. **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.
2	1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.
3	3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
4	**Octava. Solución de controversias:** Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

Fuente: Realizada por Autor

5.2 Citación Leyes Colombiana

Tabla 2 - Análisis del texto

Texto identificado		
No.	**Ley**	**Articulo**
1 y 4	Código penal colombiano Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones	Artículo 269C código penal: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Este artículo se aplica cuando se identifica que una persona utiliza recursos tecnológicos, sin autorización legal capturando información de un sitio oficial o privado, un sistema informático, emisiones electromagnéticas. La interceptación de las comunicaciones, cualquiera que sea su origen o tecnología, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley, sin embargo; las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación, así como del procesamiento de esta. Para el caso colombiano el ente competente es la Fiscalía General de la Nación, a través de la policía judicial con control posterior ante un juez con funciones de garantías
		Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Este articulo está relacionado cuando un ciberdelincuente se aprovecha de la vulnerabilidad en el acceso a un sistema informático, o por falta de procedimientos y/o controles de seguridad informática de una organización o persona. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

2 y 4	Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales."	La norma en comento hace relación a reconocer y proteger el derecho que tenemos todas las personas a conocer, actualizar, y rectificar las informaciones que se hallan recogido en bases de datos, archivos, que sean susceptibles de tratamiento por entidades de naturaleza pública y privada; lo anterior en concordancia con el artículo 15 de la Constitución Política. La violación de la seguridad de los datos personales, se produce cuando los responsables de la información dan a lugar a título doloso (con intensión) a un incidente de seguridad a la violación de la confidencialidad, disponibilidad integridad de los datos.
3	Código Procedimiento Penal Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la	Artículo 67. DEBER DE DENUNCIAR. Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio. Al tenor del articulo 67 del codigo penal (ley 599 del 2000), obliga a todas las personas el deber de denuncia. En términos generales, el deber de denuncia le asiste a toda persona que tenga conocimiento de un hecho delictivo. Su incumplimiento a ese deber legal tiene como consecuencias la imposicion de una responsabilidad penal. El deber de denunciar tiene, tres límites: la garantía de no autoincriminación, el secreto profesional y el deber de fundamentación suficiente de la denuncia. Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. La finalidad del presente artículo es la protección de los derechos fundamentales y dignidad humana. Se aplica cuando una persona sin autorización obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique y emplee códigos personales obteniendo datos con el objetivo de obtener información personal.

	protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	
4	Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Congreso de la República, con la expedición de la Ley 842 de 2003 incorporó en su Título VI, el Código de Ética Profesional	CAPITULO II. DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder; ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones: b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;

Fuente: Realizada por Autor

La empresa debe ajustar el documento presentado, porque está induciendo y permitiendo realizar labores ilegales con el fin de obtener ganancias, así mismo lo descrito en cada uno de los ítems está lejos de ser un “Acuerdo de Confidencialidad”.

5.3 Responsabilidad ética “Especialista en Seguridad Informática y de la Información

Desde mi óptica profesional y ética, pienso que los especialistas en ciberseguridad, son aquellas con un conocimiento avanzado en tecnología, capaz

de superar obstáculos técnicos, encontrando soluciones a problemas complejos, capaz de descubrir y aprovechar las debilidades o vulnerabilidades en un sistema informático o una red, el cual a nivel ético debe informarlo y si es el caso solucionarlo, no aprovecharlo para bien común o para un tercero, por sus implicaciones tanto ética, morales y judiciales, afectando su imagen reputacional y/o libertad.

Se debe leer la letra menuda y todo el contexto que involucre cualquier actividad que llegue a vulnerar los derechos constitucionales de la persona y/o entidad, y sea orden o requisito para cumplir una labor contractual de manera formal e informal, con esto no afirmo que los profesionales dedicados a esta rama estén cortados con la misma tijera y actúen igual, solo redacto el deber ser.

En Colombia existen debilidad en la regulación y legislación de la protección de la información y los datos, a pesar de que tenemos el código penal, la Ley 1273 de 2009, con el concepto de la protección de la información y de los datos, así mismo la Ley 1581 de 2012, aún falta mucha compresión para que la aplicación correcta, profundizando en esta problemática de penalización en ciberdefensa y seguridad Informática.

Sin embargo, pueden existir las leyes, las penalizaciones, las cárceles, etc., pero si no hay una ética profesional, del entender de lo bueno y lo malo, se presentaran casos en donde se utilicen las técnicas y procedimientos abusivos y sin autorización para obtener información de manera ilegal.

Por lo anterior, yo Yesenia Ballesta Gutierrez, no aceptaría el trabajo, porque no está acorde a lo que personal y profesionalmente soy.

5.4 Noticia de cibercrimen en Colombia - implicaciones legales y éticas

Noticia de cibercrimen en Colombia, punto de vista desde las implicaciones legales y éticas. Listar la ley y articulo de los delitos expuestos.

Ilustración 2 - Visualización noticia

EL NUEVO SIGLO

Domingo - Agosto 20 de 2023

Nación.

Por estafa, cárcel para 2 miembros de 'Los de Rionegro' en Bogotá

Redacción Web Bogotá Agosto 20, 2023 - 01:01 PM

Foto: Fiscalía

El material probatorio obtenido por un fiscal adscrito a la Dirección Especializada contra los Delitos Informáticos permitió que un juez de conocimiento de Bogotá condenara a María Camila Corredor Vargas y a John Marcos Morales Rubio, a penas superiores a los 3 y 6 años de prisión, respectivamente.

Fuente: Noticia extraída de: https://www.elnuevosiglo.com.co/articulos/08-20-2023-por-estafa-carcel-para-2-miembros-de-los-de-rionegro-en-bogota

Noticia presentada por el diario el “El Nuevo Siglo”, en su página oficial el día 20AGO23, en donde informan la captura de dos personas, quienes laboraban en compañías telefónicas, aprovechándose de sus cargos, realizaban consultas de las bases de datos de clientes naturales y corporativos, la modalidad fue la extracción de información personal de sus víctimas para entregarla a una banda de estafadores, los cuales cobraban cheques, desfalcaban cuentas bancarias con documentación falsificada, suplantando la identidad de los titulares de las cuentas.

Tabla 3 - Análisis de la noticia

Delitos imputados	Ley - artículo
Delitos de concierto para delinquir	Código Penal - ARTÍCULO 334. A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa. Concierto para delinquir. Cuando varias personas se concierten con el fin de cometer delitos, cada una de ellas será penada, por esa sola conducta, con prisión de cuarenta y ocho (48) a ciento ocho (108) meses.

Estafa agravada	Código Penal - Artículo 246. Estafa El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños, incurrirá en prisión de treinta y dos (32) a ciento cuarenta y cuatro (144) meses y multa de sesenta y seis puntos sesenta y seis (66.66) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes. En la misma pena incurrirá el que en lotería, rifa o juego, obtenga provecho para sí o para otros, valiéndose de cualquier medio fraudulento para asegurar un determinado resultado. La pena será de prisión de dieciséis (16) a treinta y seis (36) meses y multa hasta de quince (15) salarios mínimos legales mensuales vigentes, cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes. Delito agravado: El que aumenta o acrecienta el reproche en virtud de las condiciones de la víctima o el victimario, así como de las circunstancias o situación particular en que se perpetró el hecho.
Obstaculización ilegítima de sistema informático	Código Penal - Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
Violación de datos personales	Código Penal - Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Fuente: Realizada por Autor

Implicaciones legales y éticas

Al realizar análisis del presente caso, se evidencia que no es necesario tener conocimiento y/o experiencia en Ciberseguridad para cometer delitos que afecten la protección de la información y de los datos, todo depende de la calidad y clasificación de la información y como las entidades la protegen. Por otra parte, la honradez y responsabilidad de los empleados en su uso.

Hay muchos factores que intervienen, pero así la información no está protegida por ética profesional y laboral, no se deben violar los principios de la seguridad de la información, Confidencialidad, disponibilidad e integridad.

6 Ejecución pruebas de intrusión

6.1 Herramientas software utilizadas

Para el presente ejercicio se utilizan las herramientas que a continuación se relacionan, las cuales se trabajaron a partir del enunciado del ejercicio, es de anotar que, si el equipo de cómputo tiene configurado las herramientas de seguridad diseñadas para la protección de la información, el taller tendría otras implicaciones y diferente procedimiento.

- VirtualBox
- Kali Linux
- Windows 10
- Metasploit MSFVENOM
- MSCONSOLE

Para evitar accesos remotos y/o ejecución de programas no autorizados es recomendable realizar lo siguiente:

- Mantener el sistema operativo actualizado, con el fin de corrigen vulnerabilidades conocidas que pueden ser explotadas por atacantes.
- Uso de contraseñas seguras, y únicas para todas las cuentas en línea y dispositivos. Las contraseñas seguras deben tener mínimo 8 caracteres alfanuméricos, números y caracteres especiales.
- Use software antivirus y antimalware, programas que detectan y eliminan malware que puede permitir a los atacantes acceder a su equipo.
- Desactivar el acceso remoto, no es necesita tenerlo activo, en Windows 10, se cambia la configuración abriendo el panel de Propiedades de su Equipo, en opciones de la izquierda pulsar “Configuración de acceso remoto”. Deshabilitar la opción “No permitir las conexiones remotas a este equipo”.
- Configurar los servicios de correo electrónicos reportados como sospechosos en listas negras de dominios para minimizar riesgos con mensajes de dudosa procedencia.
- Configurar herramientas de seguridad para detectar este tipo de amenazas de forma temprana, monitoreo del tráfico de red.
- Mantener documentado los programas instalados en los equipos de cómputos identificando su función.
- No descargar ningún archivo adjunto desde páginas que no sean verificadas como confiables previamente.
- Evitar suministrar información sensible como la dirección de correo en sitios web que no hagan parte de los servicios de la organización.
- Evitar hacer clic sobre enlaces o hipervínculos adjuntos sobre correos de dudosa procedencia.
- Revisar la dirección del remitente de los correos que recibe.

6.2 Información recolectada en la entrevista

Durante la entrevista el administrador del equipo de cómputo informa al equipo Red Team que ejecutó un archivo desde la red social “WhatApp Web” enviado por un compañero de nombre “PoCseminario.exe”, así mismo menciona la siguiente información que es de útil para ambientar e ir identificando vulnerabilidades

- S.O Windows 10 a 64 bits
- Desactivado las siguientes plataformas de seguridad “Firewall”, “Windows Defender”, “Antivirus”

6.3 Herramientas para detectar fallo de seguridad – puerto

Para el ejercicio se utilizó el software “Meterpreter”, payload[1] que se utiliza para ejecutar tareas maliciosas en un ordenador, permite controlar de forma remota las computadoras infectadas, se ejecuta en la memoria de la computadora sin escribir nada en el disco duro del mismo, no crea procesos nuevos, es una herramienta que se utiliza para aprovechar vulnerabilidades existentes en un sistema operativo, se aprovecha por la falta de parches de seguridad en el sistema operativo o en las aplicaciones instaladas.

6.4 Afectación del ataque al equipo Windows 10 x 64

La herramienta msfvenom, que hace parte de Metasploit, es un marco de desarrollo de código abierto utilizado por profesionales de la seguridad informática y los hackers éticos para adelantar pruebas de penetración y evaluaciones de seguridad, sin embargo, también es utilizado por ciberdelincuentes llevar realizar ataques cibernéticos. Esta herramienta al ejecutarse logra afectar los siguientes:

- Aprovechamiento y explotación de Vulnerabilidades en el sistema operativo Windows 10, creando sesión en el equipo de cómputo.
- Backdoor, creación de puerta trasera en la máquina objetivo, permitiendo al atacante acceder y controlar la máquina de forma remota.
- Robo de Datos Sensibles de la máquina objetivo, como contraseñas, documentos o información de tarjetas de crédito.
- Eliminación, modificación de datos, eliminar archivos importantes, modificación o daño del sistema operativo.
- Inyección de código malicioso, almacenamiento y ejecución de malware en el equipo de la víctima.
- Escalada de privilegios, en bases de datos y/o servidor creación de usuarios Administrador.

[1] Malware que realiza la acción maliciosa después de haber realizado una penetración exitosa.

6.5 Explicación y evidencias del procedimiento

6.5.1 Situación problema: Análisis Red team

La organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo. El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos: **Nombre_estudiante_codigo_fecha_actividad**, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

El administrador de la computadora afectada menciona un dato valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre **PoCseminario.exe** el cual procedió a descargar y a ejecutar en la computadora afectada.

El administrador de la computadora afectada menciona las siguientes características de la computadora en general:

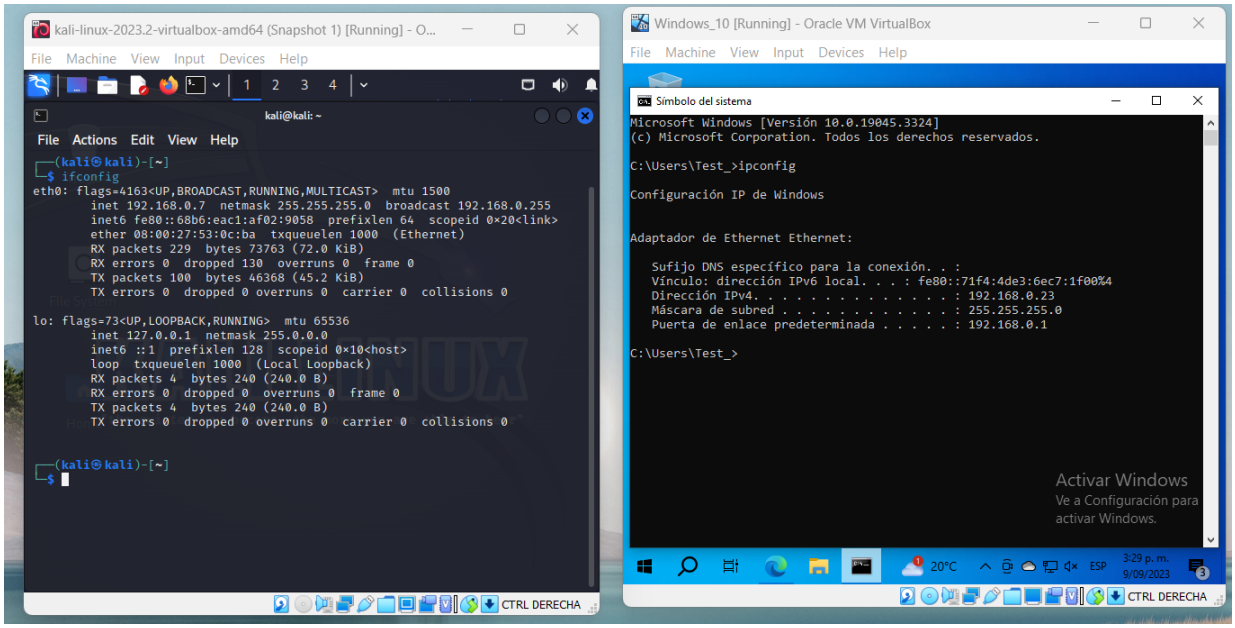
- S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante

Con la información obtenida el equipo Red Team proceden a analizar el escenario el cual debe ser recreado por los estudiantes de seminario para documentar qué fue lo que pasó en la computadora afectada y cómo lograron eliminar el archivo de texto que se encontraba en el escritorio. Uno de los expertos en ciberseguridad de HackerHouse menciona que podría tratarse de un Payload el cual se creó con MSFVNOM y se ejecutó con METASPLOIT. El experto menciona el posible paso a paso para crear un PAYLOAD con extensión .exe para ser ejecutado por la víctima, y posterior a ello como abrir una sesión por medio de METASPLOIT para controlar de manera remota la computadora afectada.

6.5.2 Paso No. 1 – Atacante en la misma red de la victima

- Equipos en la misma red, el atacante se introdujo en la red de la víctima para estar en un mismo fragmento de red.

Ilustración 3 – Visualización de las máquinas en la misma red



Fuente: Realizada por Autor

Tabla 4 - Tabla identificación IP

Información adicional	**Kali Linux**	**Windows 10**
Dirección IP	192.168.0.7	192.168.0.23
Mascara	255.255.255.0	255.255.255.0

Fuente: Realizada por Autor

6.5.3 Paso No. 2 – arquitectura de las Maquinas

Descripción de la estructura básica identificada del equipo de la víctima se está en la misma red que la máquina atacante en el mismo fragmento de red.

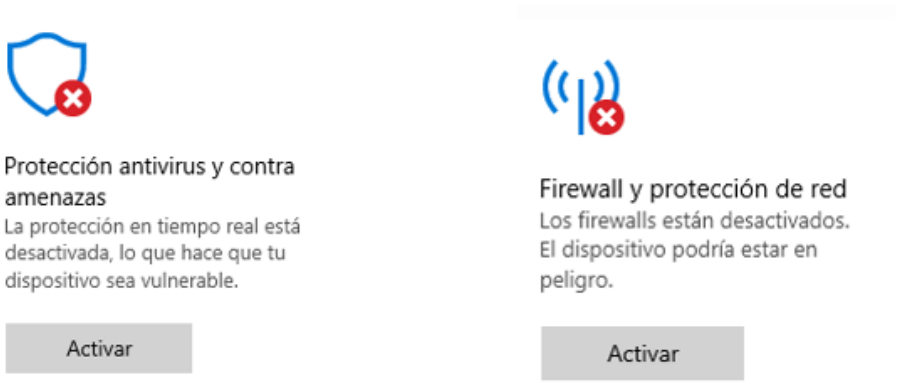
- Información del sistema operativo de la victima

Ilustración 4 - Visualización información Sistema Operativo

Fuente: Realizada por Autor

- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
-

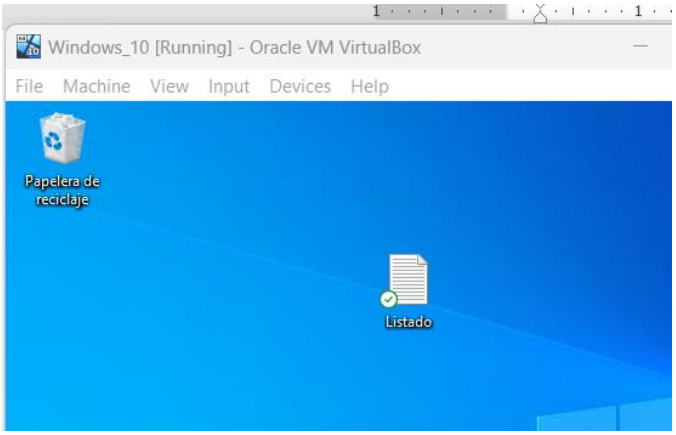
Ilustración 5 - Protección antivirus y contra amenazas DESACTIVADO



Fuente: Realizada por Autor

- Identificación del archivo creado por la víctima, de nombre “Listado.txt”

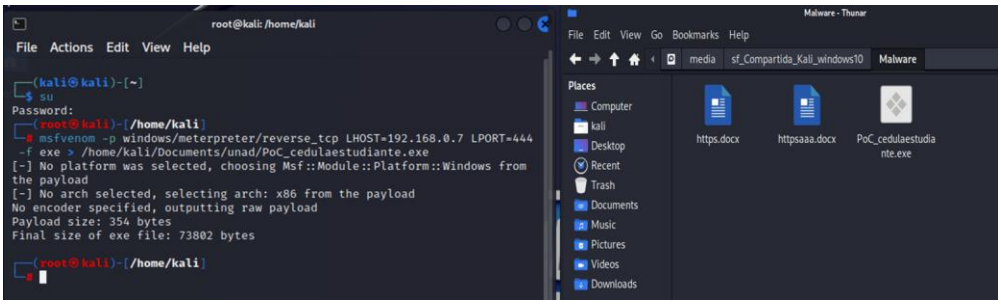
Ilustración 6 - Visualización archivo listado.txt



Fuente: Realizada por Autor

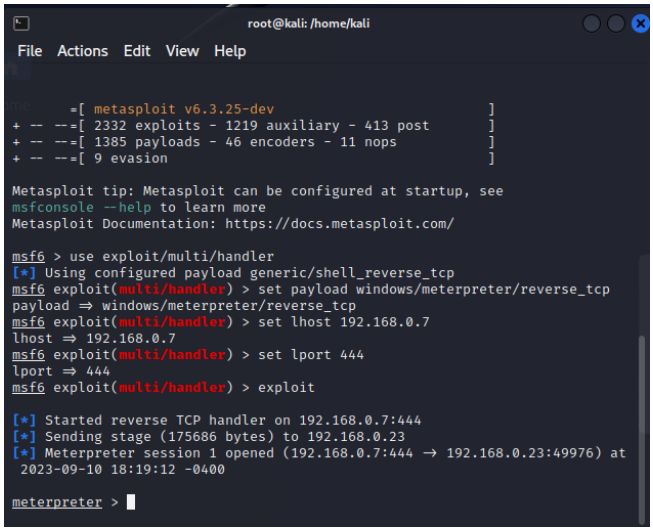
6.5.4 Creando y ejecutando la carga útil msfvenom

Ilustración 7 -Visualización creación carga útil



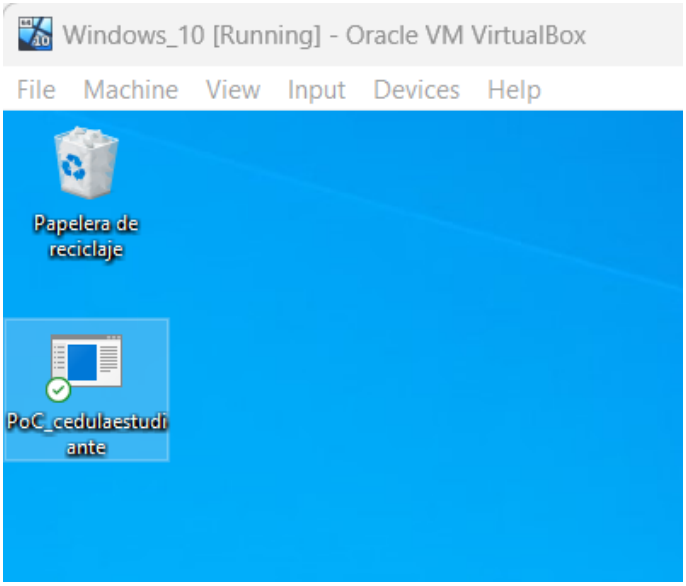
Fuente: Realizada por Autor

Ilustración 8 - Ejecución de msfconsole en una consola



- Ejecución del archivo malicioso

Ilustración 9 - Visualización del payload

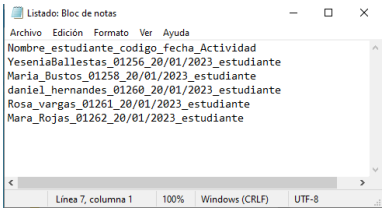
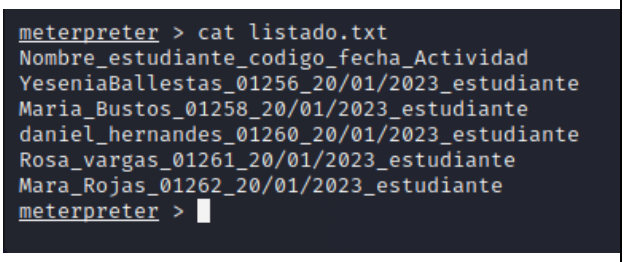
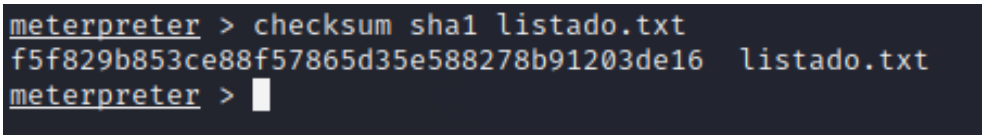


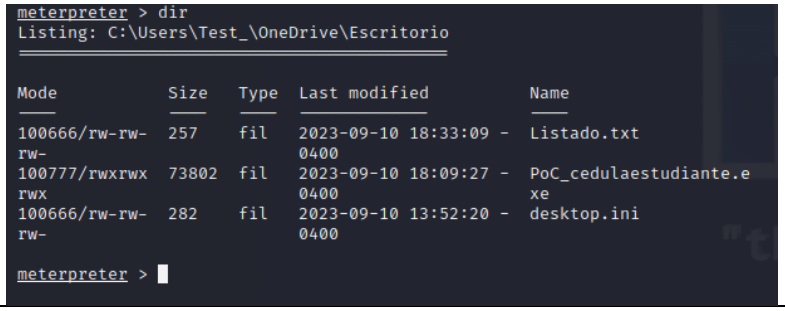
Fuente: Realizada por Autor

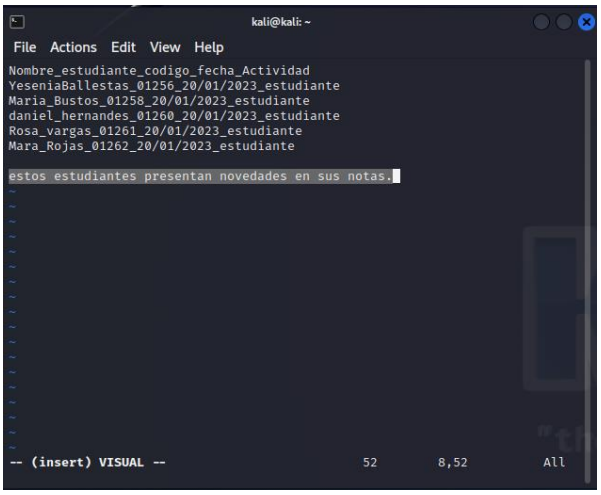
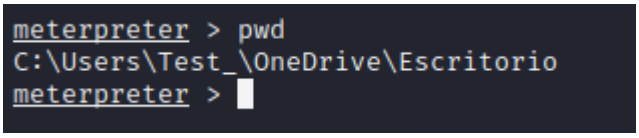
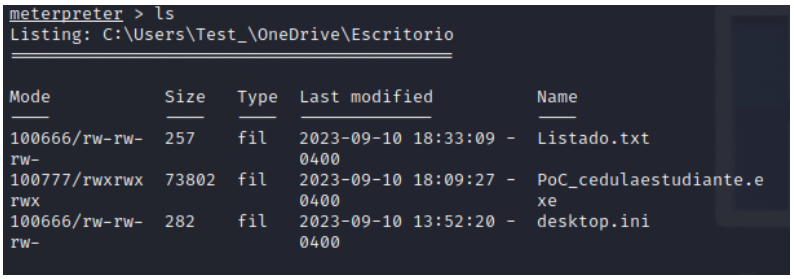
6.5.5 Identificación del objetivo

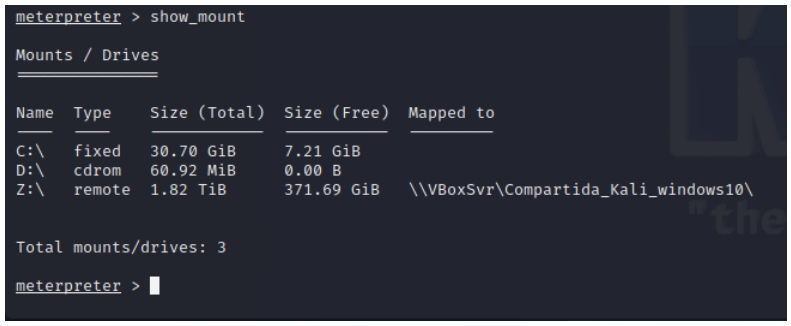
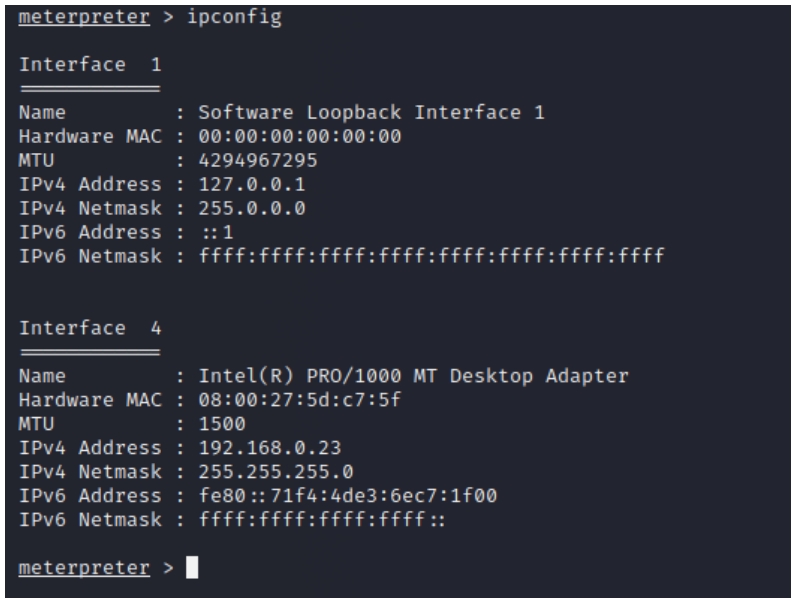
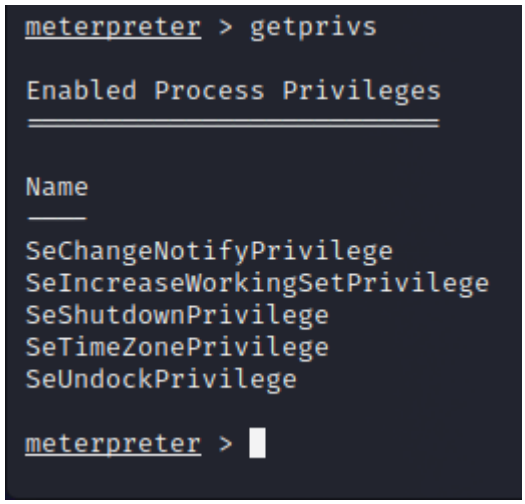
Listado de comandos utilizados por meterpreter para realizar reconocimiento y ubicación del archivo objetivo

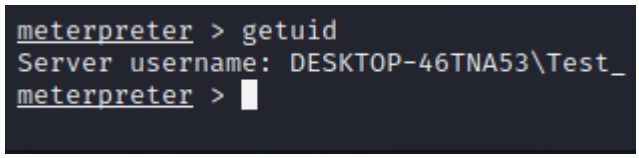
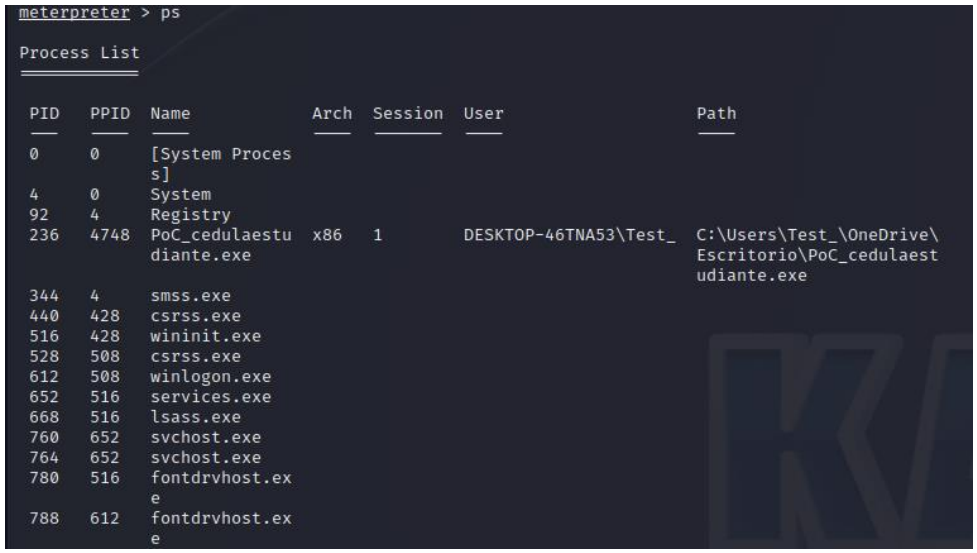
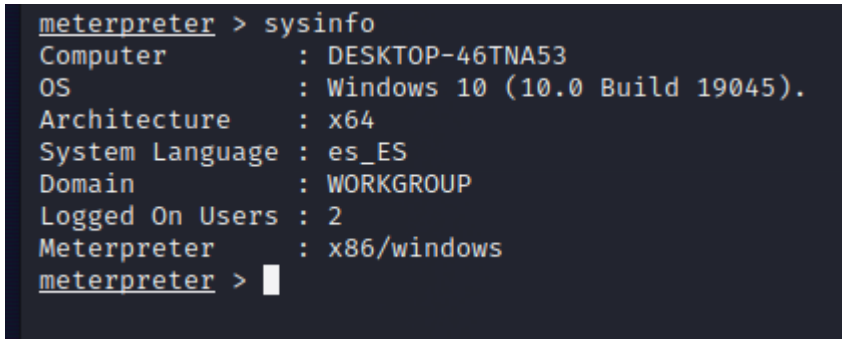
Tabla 5 - Lista de comandos utilizados

<table>
<tr><th>Comando</th><th colspan="2">Sesión Meterpreter</th></tr>
<tr><td>Visualización de un archivo: cat listado.txt</td><td>Ilustración 10 - Visualización contenido listado.txt
 
</td><td>Ilustración 11 -Visualización del archivo vulnerado
 
</td></tr>
<tr><td>Visualizando el hash de un archivo Checksum md5 listado.txt</td><td colspan="2">Ilustración 12 - Hash del archivo objetivo
 
</td></tr>
<tr><td>Visualización contenido comando

dir</td><td colspan="2">Ilustración 13 - Visualización del directorio del pc victima
 
</td></tr>
</table>

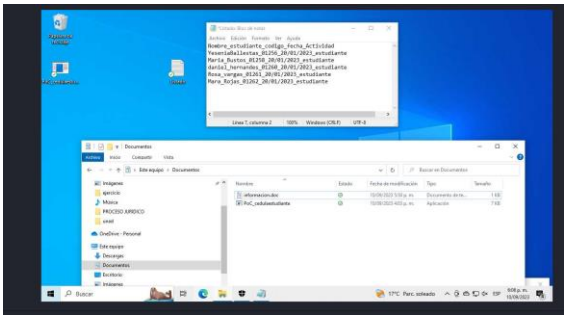
Editando un archivo comando edit listado.txt	*Ilustración 14 - Edición del archivo objetivo* 
Ubicación actual comando pwd	*Ilustración 15 - Visualización ubicación actual* 
Listar directorio con comando ls	*Ilustración 16 - Visualización directorio con LS* 
Buscar archivos por extensión comando Search -f *.docx	*Ilustración 17 - Visualización de búsqueda de archivos* 

Unidades montadas en el equipo de la victima Comando Show_mount	*Ilustración 18 - Visualización de unidades conectadas* 
Visualizar la información de las tarjetas de red comando Ipconfig	*Ilustración 19 - Información del sistema de la victima* 
Obteniendo privilegios getprivs	*Ilustración 20 - Visualización de privilegios configurados* 

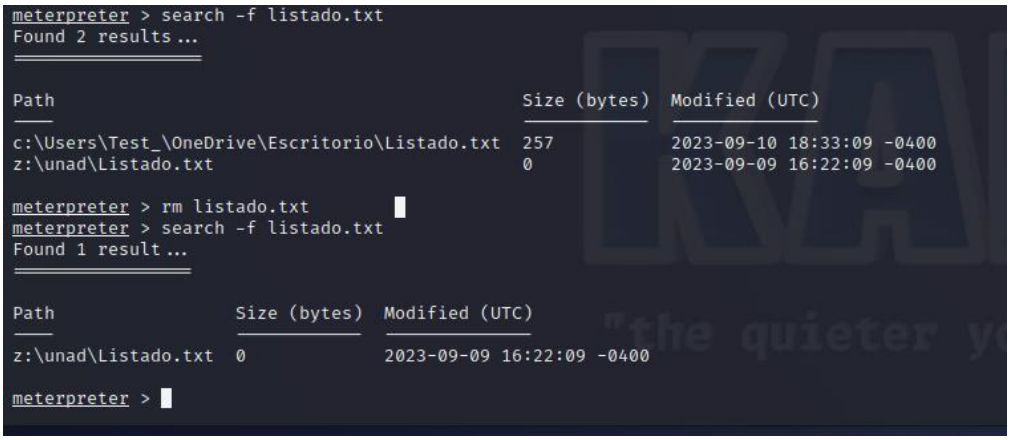
Consultar el tipo de usuario que la maquina victima está ejecutando comando getuid	*Ilustración 21 - Visualización tipo de usuario actual* 
Consultar todos los procesos que están en ejecución comando ps	*Ilustración 22 - Visualización de los procesos en ejecución* 
Obtención de información del sistema remoto como: 1. Nombre de la máquina. 2. Sistema Operativo. 3. Tipo de arquitectura. 4. Lenguaje del sistema operativo. Comando SysInfo	*Ilustración 23 - Información del sistema de la victima* 

Consultar todas las sesiones (o escritorios). Comando Enumdesktops	*Ilustración 24 - Visualización de las sesiones*
	
	`meterpreter > enumdesktops`
	`Enumerating all accessible desktops`
	
	`Desktops`
	`========`
	
	`Session  Station  Name`
	`1  WinSta0  Default`
	`1  Service-0x0-4869d$  sbox_alternate_desktop_0x2238`
	
	`meterpreter >`

Extracción de una imagen del escritorio remoto
 	
Comando Screenshot
	Ilustración 25 - Visualización del comando para copiar pantalla
	
	`meterpreter > screenshot`
	`Screenshot saved to: /home/kali/zcveutjY.jpeg`
	`meterpreter >`

	Ilustración 26 - Visualización del escritorio de la victima 

Control algunos de los componentes del sistema afectado
 	
Comando Uictl
	Ilustración 27 - Visualización de los componentes afectados
	
	`meterpreter > uictl`
	`Usage: uictl [enable/disable] [keyboard/mouse/all]`
	`meterpreter >`

Rm: Con este parámetro podremos eliminar un archivo	*Ilustración 28 - Visualización de la eliminación del archivo objetivo* 

Fuente: Realizada por Autor

7 Contención de ataques informáticos

7.1 Pasos para identificar un ataque informático

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Un experto en ciberseguridad debe identificar, contener y mitigar la amenaza. A continuación, se enumeran y explican estos pasos:

1. Detección de la Anomalía:

En primer lugar, el experto en ciberseguridad debe tener sistemas de detección de amenazas en funcionamiento para identificar actividades inusuales o sospechosas en la red.

Esto puede incluir el monitoreo de registros de eventos, análisis de tráfico de red, inspección de archivos y comportamiento del sistema.

La detección de amenazas se refiere al proceso de identificar actividades, comportamientos o eventos anómalos o maliciosos que podrían indicar la presencia de una amenaza de seguridad en una red o sistema de información. Los sistemas de detección de amenazas son herramientas y tecnologías diseñadas para llevar a cabo esta tarea. Su función principal es monitorear el tráfico de red, los registros de eventos y otros datos relevantes para identificar posibles amenazas cibernéticas y ataques.

Tecnologías conocidas en la detección de amenazas:

- Sistema de Detección de Intrusiones (IDS) : Los IDS analizan el tráfico de red o los registros de eventos en busca de patrones conocidos de ataques o actividades maliciosas. Pueden estar basados en red (NIDS) o basados en host (HIDS).
- Sistema de Prevención de Intrusiones (IPS) : Los IPS son similares a los IDS, pero tienen la capacidad adicional de tomar para bloquear o prevenir los ataques detectados.
- Sistema de Detección de Anomalías (ADS) : Los ADS se enfocan en el comportamiento normal de la red o de los sistemas y alertan sobre desviaciones significativas de este comportamiento. Pueden detectar amenazas desconocidas.
- Plataforma de Análisis de Comportamiento de Usuarios (UEBA) : La UEBA analiza el comportamiento de los usuarios y las entidades en una red para identificar actividades inusuales o sospechosas.
- Firewall de Próxima Generación (NGFW) : Los NGFW no solo actúan como firewalls tradicionales, sino que también incorporan capacidades de detección de amenazas avanzadas.
- Sistema de Detección y Prevención de Amenazas (TDS/TPS) : Estos sistemas combinan capacidades de detección y prevención de amenazas para una protección más completa.

- Inteligencia de Amenazas : La inteligencia de amenazas utiliza información sobre amenazas conocidas para identificar y prevenir posibles ataques.
- Sistema de Registro y Auditoría (SIEM) : Los SIEM centralizan la recopilación y el análisis de registros de eventos de múltiples fuentes para detectar patrones de amenazas.
- Análisis de tráfico en tiempo real : Herramientas que examinan el tráfico de red en tiempo real para identificar actividades sospechosas.

La selección y la implementación de sistemas de detección de amenazas dependerán de las necesidades específicas de seguridad de la organización, el entorno de red y los recursos disponibles. Es importante configurar y mantener adecuadamente estos sistemas, así como tener políticas de respuesta a incidentes claras, para garantizar una detección efectiva y una respuesta adecuada a las amenazas.

2. Confirmación del Ataque:

Una vez que se detecta una anomalía, el experto debe confirmar si se trata realmente de un ataque o simplemente de un evento benigno que parece sospechoso.
Esto implica la revisión de múltiples fuentes de datos y registros para determinar la naturaleza del evento.

3. Identificación del Tipo de Ataque:

Se debe identificar el tipo específico de ataque informático. Puede ser un ataque de malware, un intento de intrusión, un ataque de denegación de servicio (DDoS) u otro tipo de amenaza.

4. Recopilación de Evidencia:

Se recopila evidencia relacionada con el ataque. Esto puede incluir registros de eventos, capturas de tráfico de red, registros de archivos y cualquier otra información relevante.

5. Contención del Ataque:

Una vez confirmado el ataque, se toman medidas para contenerlo y evitar que se propague o cause más daño. Esto podría implicar la desconexión de sistemas comprometidos, la eliminación de malware o la reconfiguración de reglas de firewall, entre otras acciones.

6. Análisis de Causa Raíz:
Se realiza un análisis detallado para determinar cómo y por qué ocurrió el ataque. Esto ayuda a identificar las vulnerabilidades que permitieron que el ataque ocurriera en primer lugar. El análisis de causa raíz es fundamental para evitar futuros ataques similares.

7. Notificación de las Autoridades:

En algunos casos, especialmente si se trata de un ataque cibernético grave, es necesario notificar a las autoridades competentes, como agencias de ciberseguridad gubernamentales o fuerzas del orden.

8. Comunicación Interna y Externa:

Se debe comunicar el incidente a las partes interesadas internas y externas, incluidos los empleados, los clientes y los socios comerciales.

9. Recuperación y Restauración:

Una vez que se ha contenido el ataque y se ha solucionado la vulnerabilidad subyacente, se procede a la recuperación y restauración de los sistemas afectados.

10. Evaluación Posterior al Incidente:

Después del incidente, se realiza una evaluación exhaustiva para revisar lo sucedido, identificar lecciones aprendidas y mejorar las medidas de seguridad en el futuro.

11. Actualizaciones de Seguridad:

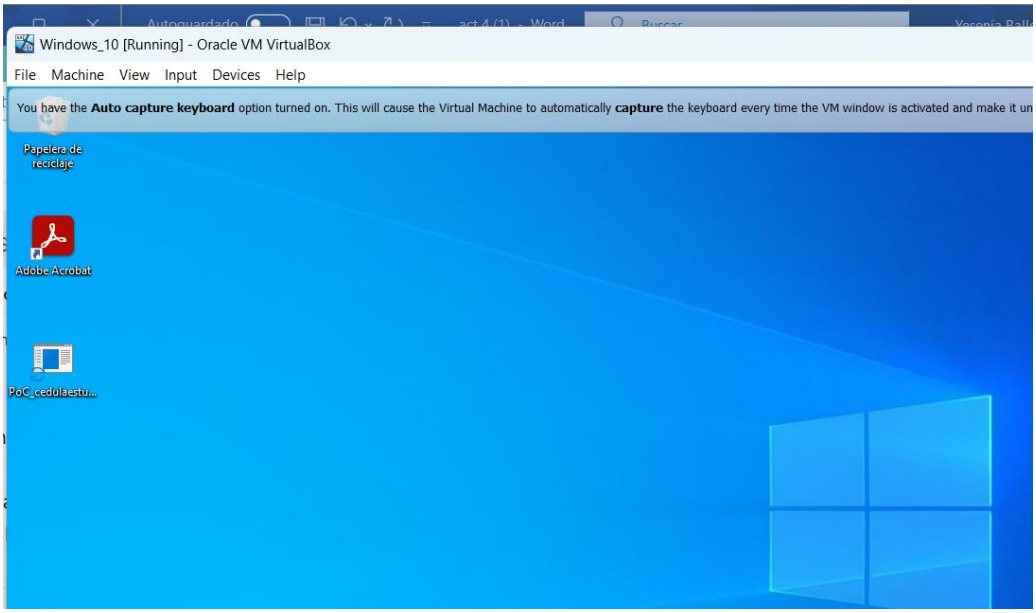
Se implementan actualizaciones y mejoras en la seguridad de la red y los sistemas para prevenir futuros ataques similares. Es importante destacar que la respuesta a un ataque informático debe ser rápida y coordinada para minimizar los daños y las pérdidas. Además, contar con un plan de respuesta a incidentes previamente establecido puede ayudar a agilizar el proceso y garantizar una respuesta eficaz.

7.2 Remediación del sistema ante el evento

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?
Para subsanar un sistema después de un ataque realizado por un Red Team, es importante seguir un proceso ordenado y eficiente. A continuación, se presenta un paso a paso que se puede seguir para mitigar y corregir el evento del Payload después de un ejercicio de Red Team:

- Paso 1: Identificación y Aislamiento del Payload:

Ilustración 29 - Ubicación del payload en la maquina victima



Fuente: Realizada por Autor

Identificar la ubicación y el alcance del payload utilizado por el Red Team en el sistema comprometido.

Aislar la parte afectada del sistema para evitar que el payload siga activo y cause más daño.

Aislar un payload malicioso es una medida importante para mitigar el impacto de un ataque cibernético y evitar que se propague por la red. El aislamiento de la carga útil puede implicar varias acciones, dependiendo de la naturaleza del ataque y de los sistemas afectados.

Identificación del payload malicioso : Antes de aislar la carga útil, se debe identificar y confirmar que existe una.

Aislamiento del sistema afectado : Desconexión de la red para evitar que la carga útil se comunique con otros sistemas y se propague.

Implementación de cortafuegos y reglas de segmentación : Configuración de las reglas de cortafuegos para bloquear el tráfico malicioso entre el sistema comprometido y otros sistemas en la red.

Eliminación de la carga útil : Identificar y eliminar la carga maliciosa del sistema afectado. Esto puede requerir la desinfección de archivos, la eliminación de programas maliciosos o la restauración de sistemas desde copias de seguridad limpias.

- Paso 2: Documentación del Incidente:

Registrar todos los detalles del incidente, incluyendo la fecha, hora, método de ataque, impacto inicial y cualquier otra información relevante. Esta documentación será valiosa para futuras investigaciones y análisis de causa raíz.

Tabla 6 - Tabla ejemplo de reporte incidente

REPORTE DE INCIDENCIAS

N° DE REPORTE: YIPSL - 005
FECHA: [15, 07, 2023 15:00]
ÁREA: [Ventas, producción, etc]
EMPLEADO: [Miguel Morales]
ENCARGADO: [Yesenia Ballestas]
ASUNTO: Falla en el sistema operativo.

- El [miércoles] [15] de [julio] del [2023] a las [15:00] fue reportado por [Miguel Morales] [Auxiliar tesorería] una falla en el sistema operativo de la compañía. El sistema estuvo inactivo durante 2 horas, al ingresar se había borrado y/o desaparecido información.
- Producto de la falla en el sistema se presentó la pérdida de la información contenida en un archivo de Excel, almacenado en el escritorio, con nombres de clientes nuevos que no habían respaldado en la base de datos.
- Se restableció el sistema, sin embargo, en el equipo de cómputo no se logró recuperar el archivo, se buscó la información copias de respaldos de días anterior.
- El sistema fue restablecido.
- Se realizado actualizaciones de parches y activaciones de seguridad.

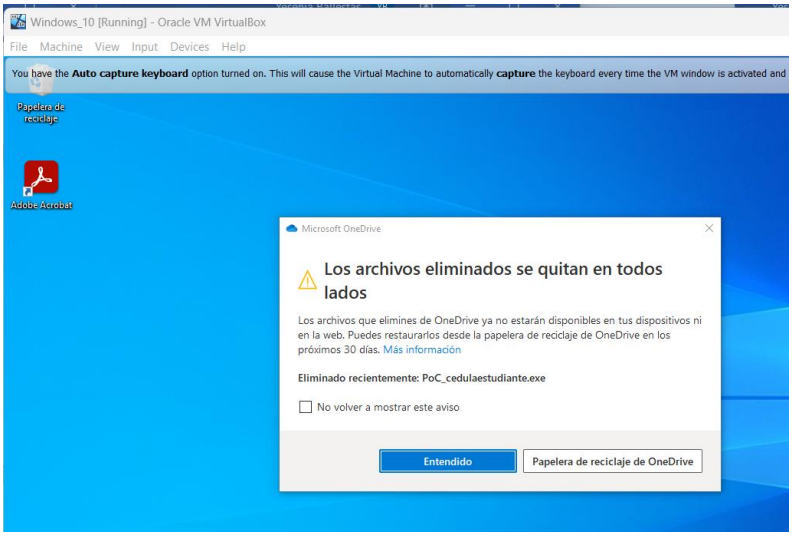
Fuente: Realizada por Autor

- Paso 3: Análisis del Payload:

Realizar un análisis forense del payload para comprender su funcionamiento y conocer las acciones realizadas por el Red Team. Esto puede incluir la extracción y análisis de registros, archivos y otros artefactos relacionados con el ataque.

- Paso 4: Contención y Eliminación del Payload:
-

Ilustración 30 - Visualización de la eliminación del payload



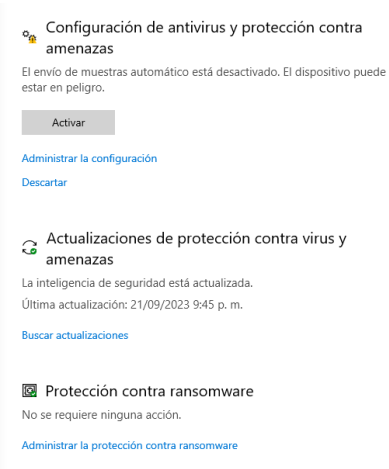
Fuente: Realizada por Autor

Identificar todas las instancias del payload en el sistema y eliminarlo por completo. Restaurar cualquier configuración o archivo modificado o afectado por el payload.

- Paso 5: Restauración de la Configuración de Seguridad:

Restablecer las configuraciones de seguridad y reglas de firewall a su estado anterior al ataque. Revisar y ajustar las políticas de seguridad si es necesario para prevenir futuros ataques similares.

Ilustración 31 - Validación de la configuración de la seguridad

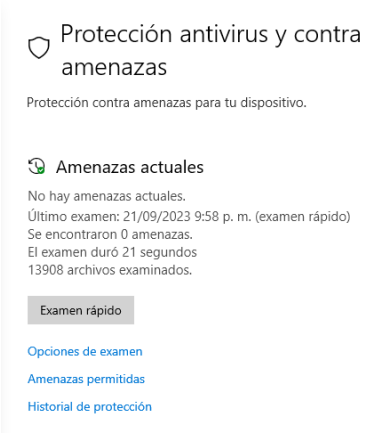


Fuente: Realizada por Autor

- Paso 6: Actualizaciones de Seguridad:

Verificar y actualizar el sistema con las últimas correcciones de seguridad y parches. Esto ayudará a cerrar las posibles vulnerabilidades que fueron explotadas durante el ejercicio de Red Team.

Ilustración 32 - Visualización aplicación de seguridad



Fuente: Realizada por Autor

- Paso 7: Análisis de Causa Raíz:

Realizar un análisis de causa raíz para determinar cómo el payload pudo ingresar y comprometer el sistema. Identificar las debilidades en la seguridad y tomar medidas para fortalecerlas.

- Paso 8: Pruebas de Penetración Interna:

Realizar pruebas de penetración interna para evaluar la efectividad de las correcciones implementadas y asegurarse de que no queden brechas de seguridad. Esto puede incluir la simulación de escenarios similares al ataque original.

- Paso 9: Comunicación y Notificación:

Comunicar el incidente y las medidas tomadas a las partes interesadas internas, como los equipos de TI y seguridad, así como a la dirección de la empresa. Si es necesario, notificar a las autoridades correspondientes y cumplir con las regulaciones de notificación de incidentes.

- Paso 10: Lecciones Aprendidas:

Realizar una revisión post-incidente para identificar lecciones aprendidas y áreas de mejora en la seguridad. Ajustar las políticas y procedimientos de seguridad según sea necesario.

- Paso 11: Monitoreo Continuo:

Establecer un monitoreo continuo de la red y sistemas para detectar posibles amenazas y ataques futuros de manera temprana. Es fundamental aprender de los ejercicios de Red Team y aplicar mejoras en la seguridad para fortalecer la infraestructura y minimizar el riesgo de futuros incidentes.

7.3 Diferencia existe entre equipos Blue Team, Red Team, Purple Team y equipos de respuesta incidentes informáticos

Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

El Purple Team es un equipo que se encarga de realizar ejercicios de simulación de ataques y evaluar la efectividad de las defensas implementadas por el Blue Team. Esto permite al Red Team adaptar y mejorar sus tácticas y técnicas. Por otro lado, los equipos de respuesta a incidentes informáticos, también conocidos como CSIRT (Computer Security Incident Response Team), se dedican a responder y gestionar los incidentes de seguridad informática en una organización.

El Red Team se enfoca en simular ataques cibernéticos para identificar vulnerabilidades y debilidades en los sistemas de seguridad. Su objetivo principal es mejorar la postura de seguridad de una organización al encontrar y explotar vulnerabilidades antes de que los atacantes reales lo hagan.

El Blue Team, por otro lado, se encarga de defender los sistemas y redes de una organización contra ataques cibernéticos. Su objetivo principal es detectar, prevenir y responder a las amenazas de seguridad informática.

En resumen, mientras que el Purple Team se enfoca en la evaluación y mejora de las defensas implementadas por el Blue Team, los equipos de respuesta a incidentes informáticos se dedican a responder y gestionar los incidentes de seguridad informática en una organización.

7.4 ¿Cuál es la función de CIS “Center For Internet Security” dentro de equipos BlueTeam?

¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

El CIS (Center For Internet Security) es una organización sin fines de lucro que se dedica a proteger a las organizaciones públicas y privadas contra las amenazas cibernéticas . Ofrecen herramientas y recursos para mejorar la seguridad de las organizaciones, incluyendo los CIS Controls y los CIS Benchmarks. Los CIS Controls son un conjunto de prácticas recomendadas para la seguridad cibernética que se enfocan en la prevención de ataques, mientras que los CIS Benchmarks son una serie de configuraciones recomendadas para sistemas y aplicaciones que ayudan a protegerlos contra vulnerabilidades conocidas. Además, el CIS también ofrece recursos para la prevención, protección, respuesta y recuperación de amenazas cibernéticas para entidades gubernamentales estatales, locales, tribales y territoriales en los Estados Unidos.

El CIS es una organización global que cuenta con la participación de expertos en seguridad cibernética de todo el mundo. Su objetivo es desarrollar soluciones prácticas y efectivas para proteger a las personas, empresas y gobiernos contra las amenazas cibernéticas.

El Sistema de Información Científica (CIS, por sus siglas) se utiliza comúnmente para buscar y acceder a artículos de investigación científica, revistas académicas y otros recursos relacionados con la ciencia. A continuación, te proporcionaré un pequeño tutorial sobre cómo funciona el CIS y cómo encontrar tutoriales disponibles en él:

Paso 1: Acceso al sitio web de CIS

Abre tu navegador web y ve a la página principal del CIS. Dependiendo de tu ubicación y preferencia, puedes utilizar diferentes plataformas CIS, como Google Scholar, PubMed, IEEE Xplore, Scopus, Web of Science, entre otros. Cada uno tiene su enfoque y alcance particular, así que elige el que mejor se adapte a tus necesidades.

Paso 2: Realizar una Búsqueda

Una vez en la plataforma CIS, verás un cuadro de búsqueda. Ingresa las palabras clave relacionadas con tu área de interés o el tema sobre el que deseas encontrar tutoriales. Por ejemplo, si estás buscando tutoriales sobre inteligencia artificial, puedes escribir "inteligencia artificial tutorial".

Presiona el botón de búsqueda o la lupa para iniciar la búsqueda.

Paso 3: Explorar los Resultados

El CIS te mostrará una lista de resultados relevantes basados en tus palabras clave. Estos resultados pueden incluir artículos académicos, libros, conferencias y, en algunos casos, tutoriales.

Examina los resultados y utiliza las opciones de filtro, como fecha, autor y tipo de publicación, para refinar tu búsqueda y encontrar tutoriales específicos.

Paso 4: Acceder a los Tutoriales

Para encontrar tutoriales, busca en los resultados los documentos que estén etiquetados como tutoriales, guías o materiales educativos. Pueden estar disponibles en formato PDF o enlace a sitios web.

Haz clic en el título del tutorial que te interese para acceder al contenido completo. Algunos tutoriales pueden ser de acceso gratuito, mientras que otros pueden requerir una suscripción o pago.

Paso 5: Descargar o Leer el Tutorial

Una vez que accedas al tutorial, puedes descargarlo en tu computadora o leerlo en línea, según las opciones disponibles.

Paso 6: Refinar y Ampliar tu Búsqueda (Opcional)

Si no encuentras el tutorial que estás buscando en los resultados iniciales, puedes modificar tus palabras clave o utilizar comillas para buscar frases específicas. También puedes explorar otras fuentes de información científica relacionadas, como bases de datos especializadas o repositorios académicos.

Paso 7: Guardar y Citar

Si encuentras un tutorial relevante para tu investigación, asegúrate de guardar la referencia bibliográfica y citarla adecuadamente en tu trabajo académico.

Recuerda que la disponibilidad de tutoriales específicos puede variar según el tema y la plataforma CIS que elijas. Si no encuentras tutoriales directamente en el CIS, también puedes buscar en sitios web académicos, blogs especializados y canales de video en línea, donde a menudo se comparten tutoriales y materiales educativos relacionados con la ciencia y la investigación.

CIS es una fuente confiable de información y orientación en el campo de la seguridad cibernética y puede ser una herramienta valiosa para los equipos Blue Team que desean fortalecer sus defensas y proteger sus activos digitales.

7.5 Diferencias entre SIEM y XDR

Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

SIEM (Security Information and Event Management) y XDR (Extended Detection and Response):

Tabla 7 - Tabla diferencias entre SIEM y XDR

Característica	**SIEM (Security Information and Event Management)**	**XDR (Extended Detection and Response)**
Definición	SIEM es una solución de seguridad que recopila, correlaciona y analiza información de eventos y registros de seguridad de múltiples fuentes en una red para detectar amenazas y proporcionar visibilidad.	XDR es una plataforma de seguridad avanzada que combina la detección y respuesta de amenazas en múltiples capas de seguridad para una visión más amplia y una protección más efectiva.
Alcance	Principalmente se centra en la gestión de eventos e información de seguridad (registros) para detectar amenazas y generar alertas.	Ofrece una protección más amplia y unificada que va más allá de la gestión de eventos, incluyendo detección de amenazas en endpoints, redes, correo electrónico y más.
Fuentes de Datos	Recopila datos de eventos y registros de una variedad de fuentes, como firewalls, sistemas de detección de intrusiones (IDS), antivirus y registros de servidores.	Incorpora datos de eventos, registros, endpoints, redes, aplicaciones en la nube y otros puntos de acceso para una visión más completa.
Detección y Respuesta	Detecta amenazas a través del análisis de eventos, correlación de datos y alertas, pero la respuesta generalmente se realiza a través de otras herramientas y sistemas.	Proporciona detección avanzada de amenazas y capacidades de respuesta automatizada o guiada para abordar amenazas en tiempo real.
Contexto	Proporciona contexto sobre eventos y alertas, pero a menudo requiere análisis adicional para comprender completamente las amenazas.	Ofrece un contexto más rico al correlacionar datos de múltiples fuentes y proporciona información sobre la táctica, técnica y procedimiento (TTP) de las amenazas.
Automatización	Puede ofrecer cierto nivel de automatización, pero la respuesta a menudo depende de	Tiene una mayor capacidad de automatización para la detección, análisis y respuesta a amenazas, lo que acelera la mitigación.

	herramientas y procesos adicionales.	
Integración con otras soluciones	Puede integrarse con otras herramientas de seguridad, como firewalls y antivirus, pero la integración puede requerir esfuerzo adicional.	Se integra estrechamente con herramientas de seguridad existentes y a menudo se presenta como una solución unificada con capacidades ampliadas.
Escalabilidad	Puede ser escalable, pero la administración de grandes volúmenes de datos y eventos puede requerir recursos significativos.	Diseñado para ser altamente escalable y manejar grandes flujos de datos y eventos de manera efectiva.
Enfoque en Amenazas Avanzadas	Puede detectar amenazas avanzadas, pero la eficacia puede depender de la configuración y la capacidad de correlación.	Está diseñado específicamente para la detección y respuesta de amenazas avanzadas y la protección contra ataques sofisticados.
Visibilidad	Ofrece visibilidad en eventos y alertas de seguridad, pero a menudo se necesita una capa adicional para la visibilidad de endpoints y redes.	Proporciona una visibilidad completa en toda la infraestructura de seguridad, incluyendo endpoints, redes y aplicaciones en la nube.

Fuente: Realizada por Autor

Es importante destacar que tanto SIEM como XDR son componentes esenciales en la ciberseguridad moderna, y la elección entre ellos dependerá de las necesidades específicas de seguridad de una organización y su presupuesto. Algunas organizaciones optan por implementar ambas soluciones para obtener una defensa integral contra las amenazas cibernéticas.

7.6 Herramientas de detección de ataque información con licencia GPL

Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

- Snort :
  Licencia : GPL (Licencia Pública General GNU)
  Descripción : Snort es uno de los sistemas de detección de intrusiones de red (NIDS) más populares y ampliamente utilizados. Utiliza reglas personalizables para analizar el tráfico de red en busca de patrones y firmas conocidas de ataques y actividad maliciosa. Snort también es altamente extensible y se puede integrar con otros sistemas y herramientas de seguridad.

- Suricata :
  Licencia : GPL (Licencia Pública General GNU)

Descripción : Suricata es otro NIDS de código abierto que se centra en el rendimiento y la capacidad de procesamiento de alta velocidad. Ofrece detección de amenazas en tiempo real, análisis de protocolos y soporte para reglas de Snort, lo que lo hace compatible con muchas de las reglas existentes de Snort.

- OSSEC :
  Licencia : GPL (Licencia Pública General GNU)
  Descripción : OSSEC es un sistema de detección de intrusos de host (HIDS) de código abierto. Se instala en sistemas individuales y monitoriza eventos y cambios de archivos en busca de actividad sospechosa. OSSEC proporciona alertas en tiempo real y se integra con otros sistemas de seguridad, como firewalls y sistemas de detección de intrusos de red.

Estas herramientas son ejemplos de software de seguridad de código abierto que pueden ayudar en la detección de ataques informáticos y en la mejora de la seguridad de los sistemas y redes. Su licencia GPL permite su uso y modificación gratuita, lo que los hace accesibles para una amplia variedad de organizaciones y profesionales de seguridad.

8 Integración de la estrategia de RedTeam, BlueTeam & Purple Team

8.1 Estrategias de RedTeam & BlueTeam

El enfoque de Red Team y Blue Team es fundamental para mejorar la seguridad cibernética de una organización. El equipo Red Team simula ataques cibernéticos, mientras que el equipo Blue Team defiende y protege los sistemas, a continuación, menciono algunas estrategias recomendadas para ambos equipos:

8.1.1 Estrategias para el Red Team:

- Conocimiento profundo: Investiga y comprende a fondo los sistemas y la infraestructura de la organización, incluyendo las vulnerabilidades conocidas y las amenazas actuales.

- Evaluación de riesgos: Identifica y prioriza los activos críticos y las vulnerabilidades más importantes para dirigir tus esfuerzos de manera efectiva.

- Pensamiento creativo: Piensa fuera de la caja y desarrolla tácticas y técnicas innovadoras para eludir las defensas de Blue Team y simular ataques realistas.

- Reconocimiento constante: Mantén la vigilancia y realiza una recopilación continua de información sobre la organización, ya que las configuraciones y amenazas pueden cambiar con el tiempo.

- Documentación: Registra tus actividades y resultados de pruebas de manera exhaustiva para ayudar a Blue Team a comprender y remediar las debilidades encontradas.

8.1.2 Estrategias para el Blue Team:

- Defensa en capas: Implementa múltiples capas de seguridad, incluyendo firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), antivirus y otras soluciones de seguridad.

- Monitoreo continuo: Establece una capacidad de monitoreo constante de la red y los sistemas para detectar actividad sospechosa y responder rápidamente.

- Respuesta a incidentes: Desarrolla un plan de respuesta a incidentes eficiente que incluya pasos claros para identificar, contener y mitigar las amenazas.

- Actualizaciones y parches: Mantén todos los sistemas y software actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

- Formación y concienciación: Proporciona capacitación en seguridad a empleados y usuarios finales para que estén al tanto de las mejores prácticas y sean conscientes de las amenazas.

- Comunicación efectiva: Establece canales de comunicación sólidos con el equipo Red Team para comprender las tácticas y técnicas utilizadas y mejorar las defensas en consecuencia.

- Evaluación continua: Realiza evaluaciones regulares de la postura de seguridad de la organización y ajusta las políticas y configuraciones en función de las lecciones aprendidas.

- Colaboración interinstitucional: Fomenta la colaboración entre diferentes departamentos, como TI y seguridad, para garantizar una implementación efectiva de la seguridad.

Es importante destacar que la colaboración y la retroalimentación entre el Red Team y el Blue Team son esenciales para el éxito en la mejora de la postura de seguridad de una organización. Ambos equipos deben trabajar juntos para identificar, abordar y mitigar las amenazas cibernéticas de manera proactiva.

8.2 Política integración en ciberseguridad equipos de Blue Team, Red Team y Purple Team

La integración de equipos Blue Team, Red Team y Purple Team en una organización puede ser altamente beneficiosa para mejorar la postura de seguridad cibernética. Cada uno de estos equipos desempeña un papel importante en la protección de los activos digitales de la organización y en la detección de vulnerabilidades y amenazas. Aquí se explica cómo pueden colaborar de manera efectiva:

8.2.1 Blue Team:

Responsabilidades: El Blue Team se enfoca en la defensa activa de los sistemas y datos de la organización, implementando medidas de seguridad, monitoreando la red y respondiendo a incidentes.

Colaboración: El Blue Team puede beneficiarse al trabajar en estrecha colaboración con el Red Team y el Purple Team para comprender las tácticas y técnicas utilizadas por los atacantes y fortalecer las defensas.

8.2.2 Red Team:

Responsabilidades: El Red Team simula ataques cibernéticos para identificar vulnerabilidades y debilidades en la infraestructura y las políticas de seguridad de la organización.

Colaboración: El Red Team puede compartir sus hallazgos y tácticas con el Blue Team y el Purple Team para que puedan abordar las vulnerabilidades descubiertas de manera más efectiva.

8.2.3 Purple Team:

Responsabilidades: El Purple Team actúa como un puente entre el Red Team y el Blue Team, facilitando la comunicación y la colaboración entre ambos.

Colaboración: El Purple Team puede organizar ejercicios conjuntos en los que el Red Team realiza un ataque simulado y el Blue Team defiende contra él en tiempo real. Esto permite una retroalimentación inmediata y una mejora continua de las defensas.

La política de seguridad en la integración de equipos de Blue Team, Red Team y Purple Team es fundamental para garantizar la efectividad de las operaciones de ciberseguridad en una organización. Estos equipos desempeñan roles críticos en la defensa y evaluación de la seguridad de la infraestructura de TI y deben colaborar de manera coordinada para lograr los mejores resultados. A continuación, se presentan algunas pautas que podrían formar parte de una política de seguridad para la integración de estos equipos:

8.2.4 Definición de Roles y Responsabilidades:

Especificar claramente las responsabilidades y roles de los equipos Blue Team, Red Team y Purple Team.

Establecer límites claros entre las operaciones de cada equipo para evitar conflictos y confusiones.

- Colaboración y Comunicación: Fomentar la comunicación fluida y la colaboración entre los equipos. Programar reuniones regulares para discutir hallazgos, estrategias y tácticas. Facilitar el intercambio de información relevante para mejorar la defensa y las pruebas de seguridad.

- Planificación y Coordinación: Desarrollar planes de acción conjuntos que incluyan la respuesta a incidentes. Coordinar simulacros de incidentes para evaluar la capacidad de respuesta de la organización. Planificar y coordinar evaluaciones de seguridad regulares (pruebas de penetración, evaluaciones de vulnerabilidades, etc.).

- Compartir Resultados de Pruebas: Compartir de manera transparente los resultados de las pruebas realizadas por el equipo Red Team con el equipo Blue Team. Utilizar los resultados para mejorar las defensas y corregir las vulnerabilidades identificadas.

- Equipo Purple Team: Designar un líder o coordinador para el equipo Purple Team. Establecer protocolos para la ejecución de ejercicios de Purple Team. Asegurarse de

que el Purple Team tenga acceso a la información y herramientas necesarias para desempeñar su función de manera efectiva.

- Seguimiento y Métricas: Establecer métricas de desempeño para evaluar la efectividad de los equipos y las mejoras en la seguridad. Realizar revisiones periódicas de incidentes y pruebas para identificar áreas de mejora.

- Formación Continua: Fomentar la formación continua de los miembros de los equipos para mantenerse al día con las amenazas y las técnicas de ataque más recientes.

- Políticas de Confidencialidad: Establecer políticas claras de confidencialidad para proteger la información sensible que manejan los equipos. Definir los procedimientos para el manejo y la protección de datos sensibles.

- Cumplimiento Normativo: Asegurarse de que la integración de equipos cumpla con las normativas y estándares de seguridad aplicables en la industria y la jurisdicción en la que opera la organización.

- Revisión y Actualización: Periódicamente revisar y actualizar la política de seguridad en función de cambios en la organización, en la tecnología y en las amenazas.

La política de seguridad para la integración de equipos de Blue Team, Red Team y Purple Team debe ser un documento vivo que evolucione con las necesidades de la organización y las amenazas emergentes. La colaboración efectiva entre estos equipos es esencial para mantener la ciberseguridad de la organización en un nivel óptimo y mejorar la capacidad de respuesta ante incidentes de seguridad.

8.3 Beneficios de la integración de equipos Blue, Red y Purple:

La integración de equipos Blue Team, Red Team y Purple Team ofrece varios beneficios para una organización en términos de fortalecimiento de la ciberseguridad y mejora de la capacidad de respuesta ante amenazas. Aquí tienes algunos de los beneficios clave:

- Mejora de la Resiliencia de Seguridad: La colaboración entre equipos permite una evaluación más exhaustiva de la seguridad de la organización. Los hallazgos y recomendaciones del equipo Purple Team pueden ser implementados por el Blue Team para mejorar las defensas y reducir vulnerabilidades.

- Identificación Temprana de Vulnerabilidades: Los equipos Red Team pueden identificar y explotar vulnerabilidades en el entorno de TI antes de que los actores maliciosos lo hagan, lo que permite a la organización parchear o corregir estas debilidades de seguridad antes de que sean aprovechadas.

- Evaluación Holística de la Seguridad: La integración de los equipos permite una evaluación más completa y holística de la seguridad, considerando tanto las defensas (Blue Team) como las amenazas (Red Team). El equipo Purple Team actúa como

intermediario, garantizando que los resultados se compartan y se utilicen eficazmente.

- Mejora de la Preparación ante Incidentes: Los ejercicios de Purple Team ayudan a evaluar la capacidad de respuesta a incidentes de la organización, lo que mejora la preparación para enfrentar amenazas reales.

- Reducción de Brechas de Seguridad: La retroalimentación continua de los equipos Red Team y Purple Team ayuda a cerrar brechas de seguridad y a perfeccionar las defensas, lo que disminuye el riesgo de violaciones de seguridad.

- Optimización de Recursos: La colaboración entre equipos evita la duplicación de esfuerzos y recursos al llevar a cabo evaluaciones de seguridad. Se maximiza el uso de los recursos disponibles para fortalecer la seguridad.

- Mayor Conciencia de Seguridad: La interacción constante entre los equipos aumenta la conciencia de seguridad en toda la organización, desde los equipos técnicos hasta la alta dirección. Los empleados tienden a estar más alerta y conscientes de las amenazas de seguridad.

- Aprendizaje Continuo: Los equipos Red Team y Purple Team están en constante evolución y aprendizaje, lo que los hace más efectivos en la identificación de nuevas amenazas y tácticas.

- Cumplimiento Regulatorio: La integración de equipos de seguridad puede ayudar a cumplir con requisitos regulatorios al demostrar un enfoque proactivo hacia la ciberseguridad.

- Mejora de la Confianza del Cliente: Al mostrar un compromiso sólido con la seguridad, las organizaciones pueden ganar la confianza de sus clientes y socios comerciales, lo que puede ser beneficioso para la reputación y las relaciones comerciales.

En resumen, la integración de equipos Blue Team, Red Team y Purple Team contribuye significativamente a fortalecer la postura de seguridad de una organización, mejorar la preparación para incidentes y reducir los riesgos de seguridad cibernética. Esta colaboración efectiva es esencial en un entorno en constante evolución de amenazas cibernéticas.

8.3.1 Beneficios de implementar Ciberseguridad en la organización

La implementación de ciberseguridad en una organización ofrece una serie de beneficios cruciales para proteger sus activos digitales, datos y operaciones. A continuación, se enumeran algunos de los beneficios clave de implementar una sólida estrategia de ciberseguridad:

- Protección de Datos Sensibles: La ciberseguridad protege la confidencialidad, integridad y disponibilidad de los datos sensibles de la organización, como información financiera, datos de clientes y propiedad intelectual.

- Reducción de Riesgos y Amenazas: Una estrategia de ciberseguridad efectiva reduce los riesgos asociados con amenazas cibernéticas, como malware, ransomware, phishing y ataques de ingeniería social.

- Cumplimiento Normativo: Ayuda a cumplir con requisitos regulatorios específicos relacionados con la seguridad de datos, privacidad y ciberseguridad, evitando sanciones y multas.

- Continuidad de Negocio: La ciberseguridad protege las operaciones críticas de la organización, lo que garantiza la continuidad del negocio incluso en caso de incidentes cibernéticos.

- Protección de la Reputación: Evita brechas de seguridad que pueden dañar la reputación de la organización y la confianza de los clientes.

- Aumento de la Confianza del Cliente: La inversión en ciberseguridad demuestra el compromiso de la organización con la protección de los datos de sus clientes, lo que puede mejorar la confianza y la lealtad del cliente.

- Eficiencia Operativa: La ciberseguridad reduce el tiempo de inactividad causado por ataques y problemas de seguridad, lo que mejora la eficiencia operativa.

- Protección de Activos Digitales: Protege los activos digitales de la organización, incluidos sistemas críticos, aplicaciones y la infraestructura de TI.

- Detección Temprana de Amenazas: Permite la detección temprana de actividades maliciosas y amenazas, lo que facilita una respuesta más rápida y eficaz.

- Mejora de la Educación en Seguridad: Fomenta una cultura de seguridad en toda la organización, aumentando la conciencia de seguridad entre los empleados.

- Reducción de Costos: Aunque la inversión en ciberseguridad puede parecer costosa, puede ahorrar dinero a largo plazo al prevenir incidentes costosos y tiempo de inactividad.

- Adaptación a las Tendencias Tecnológicas: Ayuda a la organización a adoptar nuevas tecnologías, como la nube y la movilidad, de manera segura.

- Protección contra el Robo de Identidad: Mitiga el riesgo de robo de identidad de empleados y clientes, lo que podría tener graves repercusiones legales y financieras.

- Preparación para el Futuro: Prepara a la organización para enfrentar amenazas emergentes y cambios en el panorama de la ciberseguridad.

8.3.2 Evaluación de Riesgos y Amenazas:

En la etapa inicial del seminario, se identificaron y evaluaron los riesgos y amenazas cibernéticas que enfrenta la organización. Esto incluye amenazas internas y externas, así como vulnerabilidades en la infraestructura de TI y las políticas de seguridad.

- Impacto Potencial: El posible impacto de un ciberataque en una organización, incluyendo la pérdida de datos, el tiempo de inactividad, la reputación dañada y las posibles sanciones regulatorias. Estos impactos pueden ser costosos y perjudiciales para la continuidad del negocio.

- Tendencias Actuales en Ciberseguridad: Las tendencias actuales en ciberseguridad, el aumento de ataques de ransomware, phishing, y la sofisticación de los atacantes, demuestra que las amenazas cibernéticas están en constante evolución y se vuelven más peligrosas.

- Vulnerabilidades Identificadas: Se destacaron las vulnerabilidades específicas que se encontraron durante las pruebas de seguridad y evaluaciones. Estas vulnerabilidades son puertas de entrada potenciales para los atacantes y requieren una acción inmediata.

- Cumplimiento Normativo: Es importante el cumplimiento normativo en ciberseguridad, El incumplimiento puede resultar en multas sustanciales.

8.3.3 Riesgo Financiero:

El riesgo financiero potencial en caso de un ciberataque incluye costos de recuperación, pérdida de ingresos y daño a la reputación, que pueden ser significativos.

Reputación de la Marca: La reputación de la marca y cómo un ciberataque exitoso puede erosionar la confianza de los clientes y afectar negativamente la imagen de la organización.

Beneficios de la Inversión: Invertir en ciberseguridad, reduce riesgos, la protección de datos, la mejora de la continuidad del negocio y la mejora de la confianza de los clientes.

Plan de Acción: Desarrollar un plan de acción detallado que incluye la implementación de medidas de seguridad específicas, capacitación de empleados, y la mejora de políticas y procedimientos.

Retorno de la Inversión (ROI): Calcular el ROI esperado de la inversión en ciberseguridad, mostrando cómo los costos de prevención son mucho menores que los costos de recuperación después de un ciberataque.

9 Conclusiones

La implementación de equipos de Red Teams, Blue Teams y Purple Teams en una organización es una estrategia integral para fortalecer la ciberseguridad y garantizar una respuesta efectiva a las amenazas cibernéticas. A continuación, se presentan algunas conclusiones clave sobre la implementación de estos equipos:

Identificación de Vulnerabilidades Proactiva: Los equipos de Red Team desempeñan un papel fundamental al exponer debilidades y vulnerabilidades en la infraestructura y las políticas de seguridad antes de que los actores maliciosos las exploren. Esta identificación proactiva permite a la organización tomar medidas preventivas para mitigar riesgos.

Respuesta Rápida a Incidentes: Los equipos de Blue Team se centran en la detección y respuesta a incidentes en tiempo real. Su capacitación y preparación continuas les permiten tomar medidas inmediatas para limitar el daño en caso de una amenaza cibernética.

Mejora Continua de la Ciberseguridad: La colaboración entre Red Teams y Blue Teams, facilitada por los Purple Teams, impulsa la mejora continua de las defensas cibernéticas. Esto incluye la optimización de políticas, procedimientos y tecnologías de seguridad.

Evaluación Holística de Seguridad: La implementación de estos equipos permite una evaluación más completa y holística de la seguridad cibernética de la organización. Esto no solo abarca la tecnología, sino también la cultura de seguridad y la conciencia de los empleados.

Cultura de Seguridad Fortalecida: La educación y la concienciación en seguridad se fomentan en toda la organización. La seguridad se convierte en una responsabilidad compartida, desde la alta dirección hasta el personal de nivel operativo.

Preparación para Amenazas Futuras: La práctica regular y la colaboración entre equipos ayudan a la organización a estar mejor preparada para enfrentar las amenazas cibernéticas en constante evolución. Esto incluye amenazas emergentes y nuevas tácticas de ataque.

Cumplimiento Normativo y Reputación Empresarial: La implementación de estos equipos ayuda a la organización a cumplir con los requisitos normativos de seguridad de datos, lo que puede proteger su reputación y evitar sanciones.

Alineación con Objetivos de Negocio: La ciberseguridad se integra en la estrategia de negocio, lo que garantiza la continuidad de las operaciones y protege la inversión en tecnología y datos.

En resumen, la implementación de equipos de Red Teams, Blue Teams y Purple Teams no solo es esencial para fortalecer la seguridad cibernética de una organización, sino que también promueve una cultura de seguridad, la adaptación a las amenazas cambiantes y la protección de la reputación empresarial. Estos equipos son una parte crítica de la defensa contra las amenazas cibernéticas en un mundo digitalmente conectado.

10 Recomendaciones

La implementación efectiva de prácticas de Red Teams, Blue Teams y Purple Teams en una organización requiere una planificación cuidadosa y una estrategia sólida. Aquí tienes algunas recomendaciones para poner en práctica estos equipos de manera exitosa:

Red Teams: Definir Objetivos Claros: Antes de comenzar las pruebas, establece objetivos claros y realistas para el equipo Red Team. ¿Qué debilidades o amenazas específicas deseas que evalúen?

Mantener la Independencia: El equipo Red Team debe operar de manera independiente para simular de manera efectiva las tácticas de un atacante real. Limita su acceso a información detallada para mantener la sorpresa.

Documentar Hallazgos: Registra de manera exhaustiva todos los hallazgos, vulnerabilidades y puntos débiles identificados durante las pruebas. Proporciona informes detallados para su revisión.

Blue Teams: Configuración de Herramientas de Detección: Asegúrate de que las herramientas de detección y prevención de amenazas estén configuradas adecuadamente y actualizadas.

Capacitación Continua: Proporciona capacitación continua al equipo Blue Team para mantenerlos al tanto de las últimas amenazas y tácticas de ataque.

Comunicación Efectiva: Establece canales de comunicación claros y rápidos entre el Blue Team y otros equipos de la organización, como el equipo de respuesta a incidentes y la alta dirección.

Purple Teams: Definir Roles y Responsabilidades: Asegúrate de que los roles y responsabilidades del equipo Purple Team estén claramente definidos y que tengan acceso a la información y herramientas necesarias.

Ejercicios de Purple Team Regulares: Planifica y ejecuta ejercicios regulares de Purple Team en los que el Red Team y el Blue Team colaboren para mejorar la seguridad y la respuesta a incidentes.

Facilitar la Retroalimentación: Fomenta una cultura de retroalimentación constructiva entre el Red Team y el Blue Team. Ambos equipos deben compartir conocimientos y experiencias para aprender de manera continua.

Consideraciones Generales:

Apoyo de la Alta Dirección: Obtén el apoyo de la alta dirección de la organización para garantizar que los equipos Red, Blue y Purple tengan los recursos y la autoridad necesarios.
Mejora Continua: Utiliza los resultados de las pruebas y ejercicios para mejorar continuamente las políticas de seguridad, los procesos y las tecnologías.

Mantener la Confidencialidad: Asegura que los hallazgos de las pruebas se manejen de manera confidencial y solo se compartan con las partes relevantes de la organización.

Cumplimiento Regulatorio: Asegúrate de que las prácticas de Red Teams, Blue Teams y Purple Teams cumplan con los requisitos regulatorios aplicables.
Educación y Sensibilización: Fomenta la educación y la sensibilización sobre la ciberseguridad en toda la organización, no solo entre los equipos de seguridad.

Revisión y Ajuste: Regularmente revisa y ajusta las estrategias y prácticas de estos equipos en función de las cambiantes amenazas y necesidades de la organización.

La colaboración efectiva entre Red Teams, Blue Teams y Purple Teams es esencial para fortalecer la ciberseguridad y preparar a la organización contra las amenazas cibernéticas. Al seguir estas recomendaciones, puedes optimizar la efectividad de estos equipos en tu organización.

11 Referencias bibliográficas

1. "Advanced Penetration Testing: Hacking the World's Most Secure Networks"

2. "Gray Hat Hacking: The Ethical Hacker's Handbook". Autores: Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, and Michael Baucom. Editorial: McGraw-Hill Education. Año: 2021

3. "Hacking: The Art of Exploitation". Autor: Jon Erickson. Editorial: No Starch Press. Año: 2021

4. "Kali Linux Revealed: Mastering the Penetration Testing Distribution". Autores: Raphaël Hertzog, Jim O'Gorman, y Mati Aharoni. Editorial: Offsec Press. Año: 2017

5. "Metasploit for Beginners". Autor: Sagar Rahalkar. Editorial: Packt Publishing. Año: 2018

6. "Metasploit: The Penetration Tester's Guide". Autor: David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni . Editorial: No Starch Press. Año: 2011

7. "Penetration Testing: A Hands-On Introduction to Hacking". Autor: Georgia Weidman. Editorial: No Starch Press. Año: 2014

8. "Penetration Testing: Procedures & Methodologies". Autor: EC-Council. Editorial: Cengage Learning. Año: 2019

9. "Red Team Field Manual". Autor: Ben Clark. Editorial: CreateSpace Independent Publishing Platform. Año: 2017

10. "The Hacker Playbook: Practical Guide to Penetration Testing". Autor: Peter Kim. Editorial: CreateSpace Independent Publishing Platform. Año: 2014

11. "The Mobile Application Hacker's Handbook". Autores: Dominic Chell, Tyrone Erasmus, Shaun Colley, y Ollie Whitehouse. Editorial: Wiley. Año: 2015

12. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws". Autores: Dafydd Stuttard y Marcus Pinto. Editorial: Wiley. Año: 2020

13. "Web Penetration Testing with Kali Linux". Autor: Joseph Muniz y Aamir Lakhani Editorial: Packt Publishing. Año: 2018

14. Albert Cuesta, Alejandro Ramos. Título: "Hacking ético. La guía definitiva para convertirse en hacker y saber cómo te pueden hackear a ti." Año: 2017

15. Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

16. Alejandro Ramos Título: "Guía de hacking y seguridad para principiantes: Lecciones prácticas y ejercicios" Año: 2020

17. Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

18. Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

19. Anderson, R. Título: "Security Engineering: A Guide to Building Dependable Distributed Systems."Año: 2020.

20. Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad.. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

21. Barría Huidobro, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Editorial ebooks Patagonia - Ediciones UM. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

22. Carrascosa, J.Título: "Auditoría Informática en Seguridad y Tecnologías de la Información."Año: 2006.

23. CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). 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

24. CERTIFICADO. (2020). Guía de respuesta a incidentes de seguridad cibernética. Recuperado de https://www.cert.org/guia-de-respuesta-a-incidentes-ciberneticos.

25. Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

26. Daniel Barrientos. Título: "Hacking con Raspberry Pi: Una guía completa para iniciarse en el mundo de la ciberseguridad con Raspberry Pi" Año: 2018

27. Daniel Solís Título: "Hacker Épico. Guía definitiva para convertirse en hacker" Año: 2020

28. Dhillon, G., & Backhouse, J. Título: "Information System Security Management in the New Millennium.". Año (2000)

29. Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61).

30. Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp.18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

31. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

32. Hernández, R., & Hernández.Título: "Manual de Seguridad Informática." Año: 2017.

33. ICONTEC. NTC 1486: Gestión de la calidad y aseguramiento de la calidad - Vocabulario. Instituto Colombiano de Normas Técnicas y Certificación. Año (2018).

34. ICONTEC. NTC 6166: Clasificación y codificación de productos para el comercio internacional. Instituto Colombiano de Normas Técnicas y Certificación. Año (2011).

35. Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

36. Javier Andrés Alonso, Julio Cesar Fort. Título: "Red Team: Cómo la CIA simula guerras" 2018.

37. Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech.. Dykinson. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/118410

38. Martínez, M.Título: "Seguridad de la Información en la Empresa." Año: 2018.

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

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

41. 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

42. OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

43. PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

44. Pfleeger, C. P., & Pfleeger, S. L. Título: "Security in Computing."Año: 2015.

45. Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. https://repository.unad.edu.co/handle/10596/35497

46. Ramos, L.Título: "Gestión de riesgos en sistemas de información." Año: 2013.

47. Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

48. Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

49. Shostack, A. Título: "Threat Modeling: Designing for Security."Año: 2014.

50. Urquhart, J. L.Título: "Gestión de riesgos informáticos."Año: 2004.

51. Whitman, M. E., & Mattord, H. J. Título: "Management of Information Security."Año: 2018.

12 Link de la Socialización

Ilustración 33 - Visualización link presentación sustentación

Link: https://youtu.be/ymjredPLrUk

Fuente: Realizada por el Autor