Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Angie Lizbeth Arango Bonilla

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2024

Agradecimientos

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

Dedicatoria

Dedico este trabajo de grado a mi querida madre, quien siempre ha sido mi fuente de apoyo, inspiración y sabiduría. A mi hermano, cuyo constante ánimo y compañía han sido fundamentales en este camino. A todas las personas especiales que han estado a mi lado, brindándome su cariño, comprensión y aliento a lo largo de esta travesía académica. Este logro es un reflejo de su amor y apoyo inquebrantable. Gracias por estar siempre a mi lado.

Resumen

Este informe técnico presenta un análisis integral de los escenarios planteados por CyberFort Technologies, abarcando las acciones del Blue Team, Red Team y aspectos legales de ciberseguridad. En el escenario Blue Team, se implementaron medidas de hardening, como la configuración de cortafuegos, la segmentación de redes y políticas de acceso restringido, fortaleciendo la infraestructura tecnológica y mejorando su resiliencia frente a amenazas internas y externas. Por otro lado, en el escenario Red Team, se simuló un ataque utilizando herramientas como Nmap y Metasploit. Se explotó una vulnerabilidad en el software HFS en un sistema Windows 7, logrando escalamiento de privilegios mediante la creación de un usuario administrador.

El análisis legal abordó la preservación de evidencia digital mediante la creación de copias forenses, asegurando la cadena de custodia para futuros procedimientos legales. También se evaluó el cumplimiento normativo en relación con leyes clave, como la Ley 1273 de 2009 (delitos informáticos), la Ley 1581 de 2012 (protección de datos personales) y el Código Penal Colombiano. Se propusieron políticas alineadas con estos estándares legales para robustecer la gobernanza corporativa y garantizar la conformidad regulatoria de la organización.

El informe concluye con recomendaciones estratégicas que enfatizan la colaboración entre equipos de ciberseguridad, la adopción de herramientas eficaces y el fortalecimiento de políticas legales. Estas acciones, junto con las pruebas de penetración periódicas y las medidas de hardening implementadas, consolidan las competencias técnicas y estratégicas esenciales para proteger la infraestructura tecnológica de CyberFort Technologies frente a desafíos actuales y futuros.

Palabras clave: Ciberseguridad, Evidencia, Hardening, Normatividad, Pentesting.

Abstract

This technical report presents a comprehensive analysis of the scenarios proposed by CyberFort Technologies, covering the actions of the Blue Team, Red Team, and legal aspects of cybersecurity. In the Blue Team scenario, hardening measures such as firewall configuration, network segmentation, and restricted access policies were implemented, strengthening the technological infrastructure and improving its resilience against internal and external threats. Meanwhile, in the Red Team scenario, an attack simulation was conducted using tools like Nmap and Metasploit. A vulnerability in the HFS software on a Windows 7 system was exploited, achieving privilege escalation through the creation of an administrator user.

The legal analysis addressed the preservation of digital evidence through forensic copies, ensuring the chain of custody for future legal proceedings. Regulatory compliance was also evaluated, considering key laws such as Law 1273 of 2009 (cybercrimes), Law 1581 of 2012 (data protection), and the Colombian Penal Code. Policies aligned with these legal standards were proposed to strengthen corporate governance and ensure the organization's regulatory compliance.

The report concludes with strategic recommendations emphasizing collaboration among cybersecurity teams, the adoption of effective tools, and the strengthening of legal policies. These actions, along with regular penetration tests and implemented hardening measures, consolidate the essential technical and strategic skills to protect CyberFort Technologies' technological infrastructure against current and future challenges.

***Keywords*:** Compliance, Cibersecurity, Evidence, Hardening, Pentesting.

Tabla de Contenido

Lista de Figuras

Lista de Apéndices

Introducción

La seguridad cibernética se ha convertido en un pilar fundamental para las organizaciones, dado el aumento constante de las amenazas informáticas que buscan vulnerar sus sistemas. Ante este panorama, CyberFort Technologies planteó una serie de escenarios prácticos para evaluar la capacidad de sus equipos en la identificación, contención y mitigación de riesgos en infraestructuras tecnológicas. Este informe resume el análisis de estas actividades, considerando perspectivas defensivas (Blue Team), ofensivas (Red Team) y legales, destacando estrategias clave para salvaguardar los activos digitales.

En el desarrollo de los escenarios, se aplicaron herramientas de código abierto y técnicas de análisis para abordar problemas en tiempo real, como la contención de ataques y la simulación de vulnerabilidades críticas. Además, se identificaron medidas de hardening para prevenir incidentes futuros, fortaleciendo la infraestructura TI mediante la implementación de controles específicos. Estos ejercicios no solo evaluaron habilidades técnicas, sino también la capacidad de alinear las operaciones con marcos normativos nacionales e internacionales.

El presente informe tiene como objetivo no solo presentar los hallazgos obtenidos, sino también proponer mejoras estratégicas que combinen la colaboración entre equipos de ciberseguridad y el cumplimiento normativo. De este modo, se busca contribuir al fortalecimiento integral de la seguridad en CyberFort Technologies, garantizando un entorno más resiliente frente a las crecientes amenazas cibernéticas.

Justificación

La protección de los activos digitales es crucial en un mundo cada vez más interconectado, donde las amenazas cibernéticas evolucionan en complejidad y frecuencia. La realización de escenarios prácticos en el marco de la evaluación propuesta por CyberFort Technologies permite poner a prueba las capacidades técnicas y estratégicas necesarias para salvaguardar las infraestructuras críticas. Estas actividades son esenciales para desarrollar respuestas efectivas a los desafíos actuales de ciberseguridad.

Por otro lado, la alineación con normativas legales, como la Ley 1273 de 2009, la Ley 1581 de 2012, y otras regulaciones nacionales, es indispensable para garantizar la protección de la información y el cumplimiento de los derechos de los usuarios. Proponer políticas y procesos que incorporen estos estándares legales asegura que las operaciones de la organización no solo sean seguras, sino también éticamente responsables y en cumplimiento con las disposiciones regulatorias.

Finalmente, este informe no solo evidencia las competencias adquiridas durante el análisis de los escenarios, sino que también destaca la importancia de adoptar herramientas efectivas y desarrollar estrategias colaborativas entre equipos de defensa (Blue Team), ofensiva (Red Team) y legales. Este enfoque integral asegura la construcción de un entorno seguro y resiliente frente a las amenazas cibernéticas, posicionando a CyberFort Technologies como una organización preparada para enfrentar los retos del entorno digital.

Objetivos

Objetivos General

Proponer un análisis técnico y estratégico que permita optimizar las prácticas de ciberseguridad en una organización, integrando las estrategias implementadas por equipos Red Team y Blue Team, con un enfoque en el cumplimiento normativo y la implementación de recomendaciones prácticas para fortalecer la seguridad organizacional.

Objetivos Específicos

Evaluar las estrategias utilizadas por los equipos Red Team y Blue Team, identificando las fortalezas y debilidades en su ejecución para plantear mejoras que refuercen la respuesta ante ataques y la protección de la infraestructura tecnológica.

Analizar el marco legal aplicable en ciberseguridad, incluyendo leyes nacionales como la Ley 1273 de 2009, la Ley 1581 de 2012 y otras normativas relacionadas, para garantizar que las estrategias propuestas cumplan con los estándares legales y regulatorios.

Formular recomendaciones específicas para el fortalecimiento de la seguridad organizacional, enfocadas en endurecer las medidas de protección, mejorar la colaboración entre equipos de ciberseguridad y garantizar un entorno resiliente frente a las amenazas actuales.

Desarrollo del Informe

Marco Legal sobre Delitos Informáticos y Protección de Datos en Colombia

El panorama legal en Colombia en materia de delitos informáticos y protección de datos personales se rige por varias leyes y decretos que buscan garantizar la seguridad digital y la privacidad de los ciudadanos. A continuación, se analizan las principales normativas que soportan el desarrollo de estrategias de ciberseguridad en las organizaciones:

Ley 1273 de 2009 - Protección de la Información y los Datos

Esta ley es fundamental en la lucha contra los delitos informáticos. Se introdujo para actualizar el Código Penal y proteger la integridad de los sistemas de información y los datos personales. Entre sus puntos clave está la penalización del acceso abusivo a sistemas informáticos, el daño a datos almacenados, y la creación o distribución de software malicioso. Por ejemplo, una organización podría usar esta ley para denunciar un ataque de ransomware y buscar sanciones contra los responsables.

Ley 1581 de 2012 - Protección de Datos Personales

Establece un marco general para el manejo responsable de datos personales en Colombia. Su importancia radica en que obliga a las organizaciones a implementar medidas de protección y obtener el consentimiento de los titulares antes de procesar su información. Por ejemplo, una empresa financiera que gestiona información de sus clientes debe garantizar que los datos recolectados se utilicen únicamente con los fines indicados al momento de la recolección.

Decreto 1377 de 2013 - Reglamentación de la Ley 1581

Este decreto complementa la Ley 1581 al detallar procedimientos específicos para el cumplimiento de la protección de datos. Refuerza los derechos de los ciudadanos y define mecanismos para la autorización del tratamiento de sus datos. Una organización que recopile

datos en campañas de marketing debe implementar políticas claras de privacidad, asegurando que los usuarios puedan retirar su consentimiento en cualquier momento.

Ley 1928 de 2018 - Delitos Informáticos Transnacionales

Frente al crecimiento de los cibercrímenes internacionales, esta ley facilita la cooperación entre países para combatir delitos como el fraude en línea o el acceso no autorizado a sistemas globales. Por ejemplo, un banco colombiano víctima de un ataque desde el extranjero podría solicitar asistencia internacional para rastrear a los responsables y mitigar el impacto.

Ley 1266 de 2008 - Habeas Data

Regula el manejo de datos crediticios y financieros. Es crucial para las entidades que operan con información personal relacionada con créditos, asegurando que esta sea veraz, actualizada y tratada con autorización. Por ejemplo, un cliente podría solicitar la rectificación de su historial crediticio si se encuentran errores en su información reportada a centrales de riesgo.

Relación con las Estrategias de Ciberseguridad

El cumplimiento de estas leyes es esencial para implementar estrategias de ciberseguridad robustas. Equipos como el Blue Team deben garantizar que las políticas de acceso a sistemas y datos cumplan con la Ley 1273, mientras que los responsables de gestión de datos deben alinearse con las disposiciones de la Ley 1581 y el Decreto 1377. Por otro lado, en un ataque de carácter internacional, el marco de la Ley 1928 podría ser fundamental para coordinar una respuesta efectiva entre países.

Estrategias de Red Team en Pruebas de Penetración

La vulnerabilidad identificada en este escenario es la CVE-2014-6287, que afecta a **Rejetto HTTP File Server**, una aplicación popular para la transferencia de archivos a través de HTTP. Esta vulnerabilidad permite la ejecución remota de código debido a una falta de

validación en las solicitudes HTTP, lo que permite a un atacante ejecutar comandos maliciosos en el servidor afectado. En el caso de la máquina Windows 7 comprometida, esta vulnerabilidad fue clave, ya que facilitó la explotación del sistema y el acceso no autorizado.

A través de herramientas como Nmap, se identificaron puertos abiertos, particularmente el puerto 80 (HTTP), que es comúnmente utilizado por esta aplicación. Una vez explotada la CVE-2014-6287, el atacante pudo obtener acceso inicial al sistema y proceder con la escalación de privilegios, creando un usuario con derechos de administrador. Esto permitió un control total sobre la máquina afectada, lo que pone en riesgo la integridad y la confidencialidad de los datos almacenados, además de la posible propagación del ataque a otros sistemas en la red. Este incidente resalta la importancia de actualizar y asegurar las aplicaciones instaladas, así como de realizar auditorías regulares para identificar y mitigar vulnerabilidades críticas como la CVE-2014-6287.

A continuación, se detallarán las etapas del pentesting realizadas desde la perspectiva del red team:

Etapas del pentesting

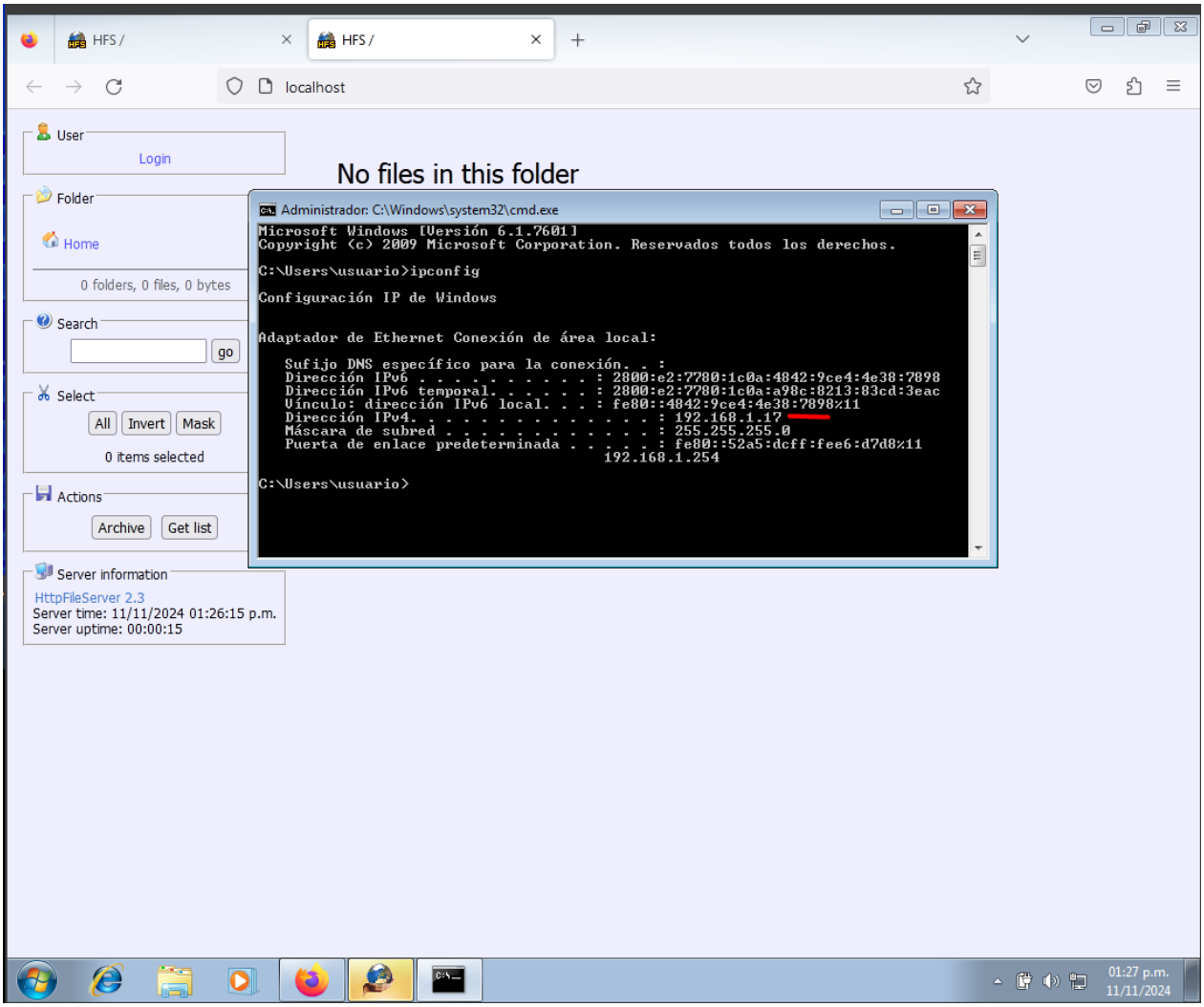
Reconocimiento. Nmap se utiliza en esta fase para obtener información sobre los puertos abiertos, servicios activos y versiones de estos en la máquina objetivo. Esto ayuda a identificar posibles puntos de entrada para la explotación.

Comando ejecutado: *nmap 192.168.1.17.*

Resultado esperado: Un escaneo detallado que muestra los puertos abiertos y los servicios activos en la máquina Windows 7, incluyendo versiones y posibles vulnerabilidades asociadas.

Figura 1

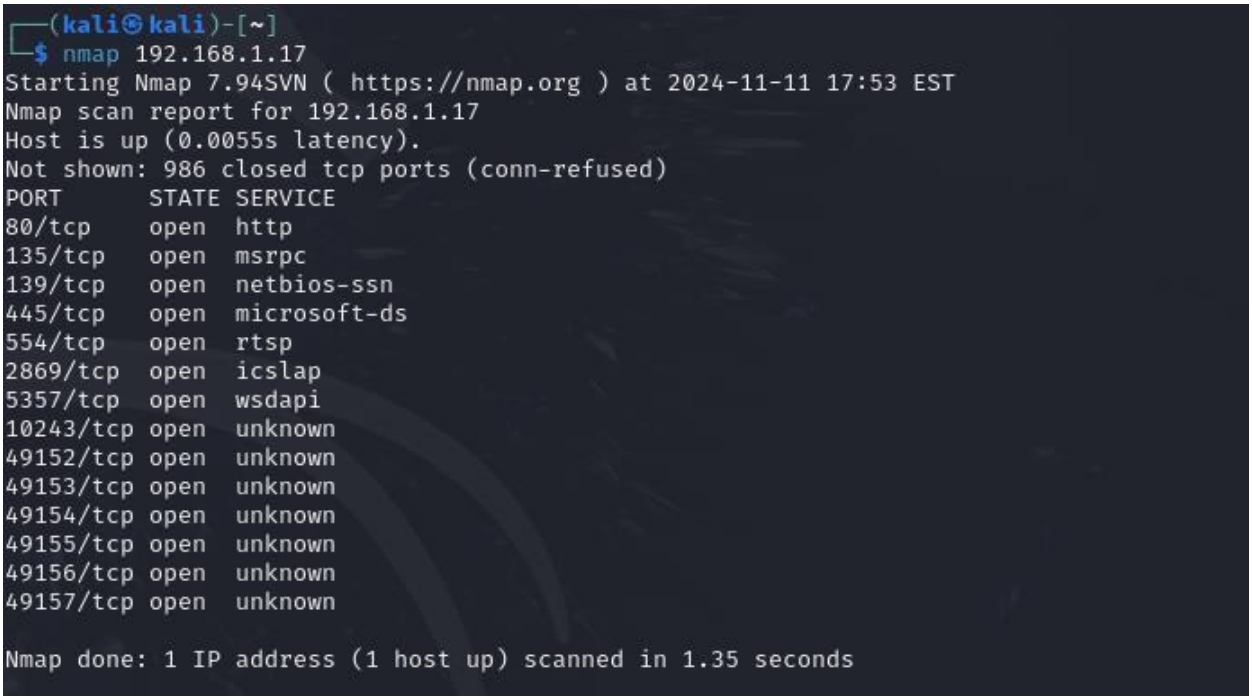
IP del Windows 7



Fuente. Autoría Propia

Figura 2

Resultado Comando Nmap



Fuente. Autoría Propia

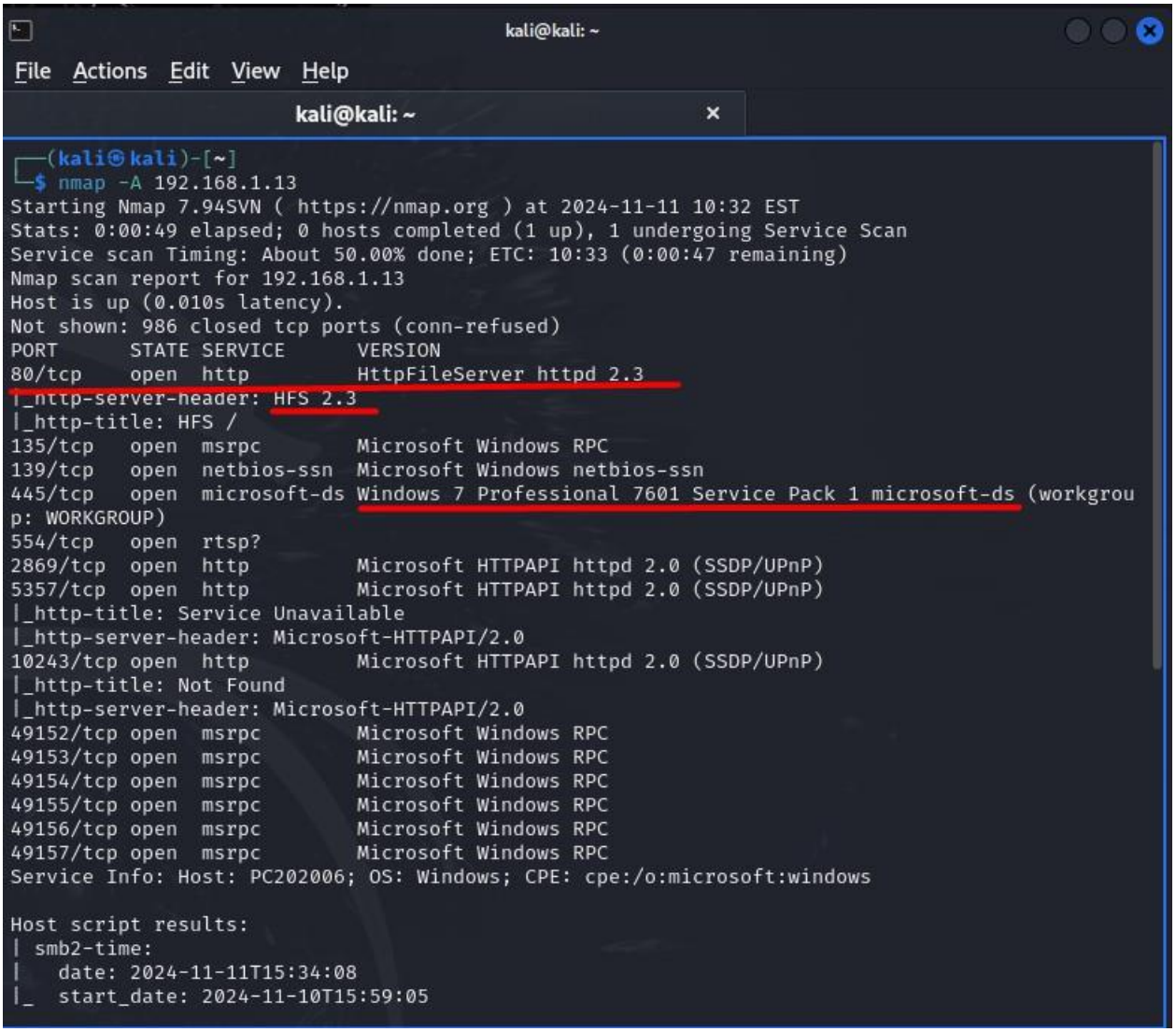
Escaneo. Nmap se emplea para realizar un escaneo profundo que revela detalles sobre los puertos abiertos, el sistema operativo y las posibles vulnerabilidades. En este paso, ya se tiene información más detallada sobre la infraestructura de la máquina Windows 7, lo que permite al pentester identificar los vectores de ataque.

Comando ejecutado: nmap -A 192.168.1.17.

Resultado esperado: Un análisis exhaustivo y detallado de los servicios y puertos abiertos, permitiendo que el atacante se enfoque en posibles vulnerabilidades críticas.

Figura 3

Escaneo con Nmap



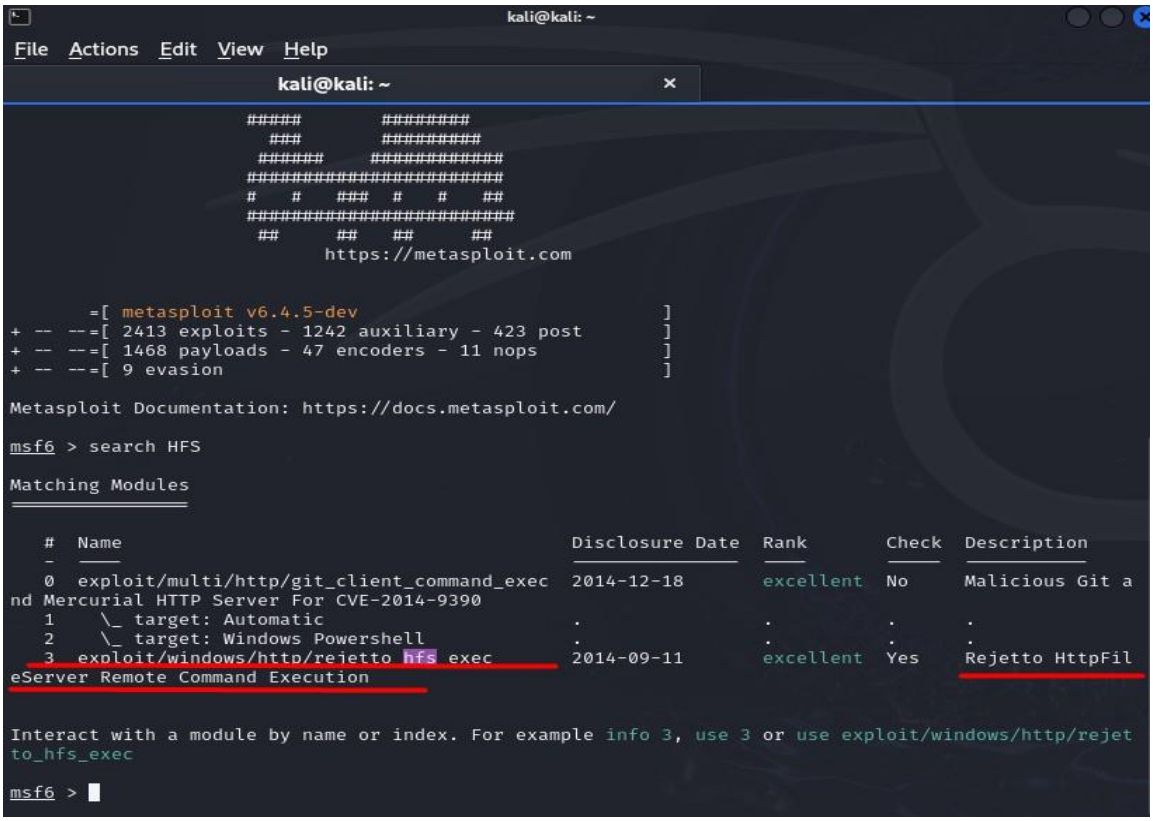
Fuente. Autoría Propia

Obtención de Acceso. Metasploit es utilizado para explotar una vulnerabilidad en la máquina Windows 7. A través de un exploit relacionado con la aplicación HFS (HTTP File Server), el pentester puede obtener acceso remoto a la máquina víctima.

Resultado Esperado. Ejecución exitosa del exploit que permite el acceso a la máquina comprometida, normalmente mostrando una sesión abierta en Meterpreter.

Figura 4

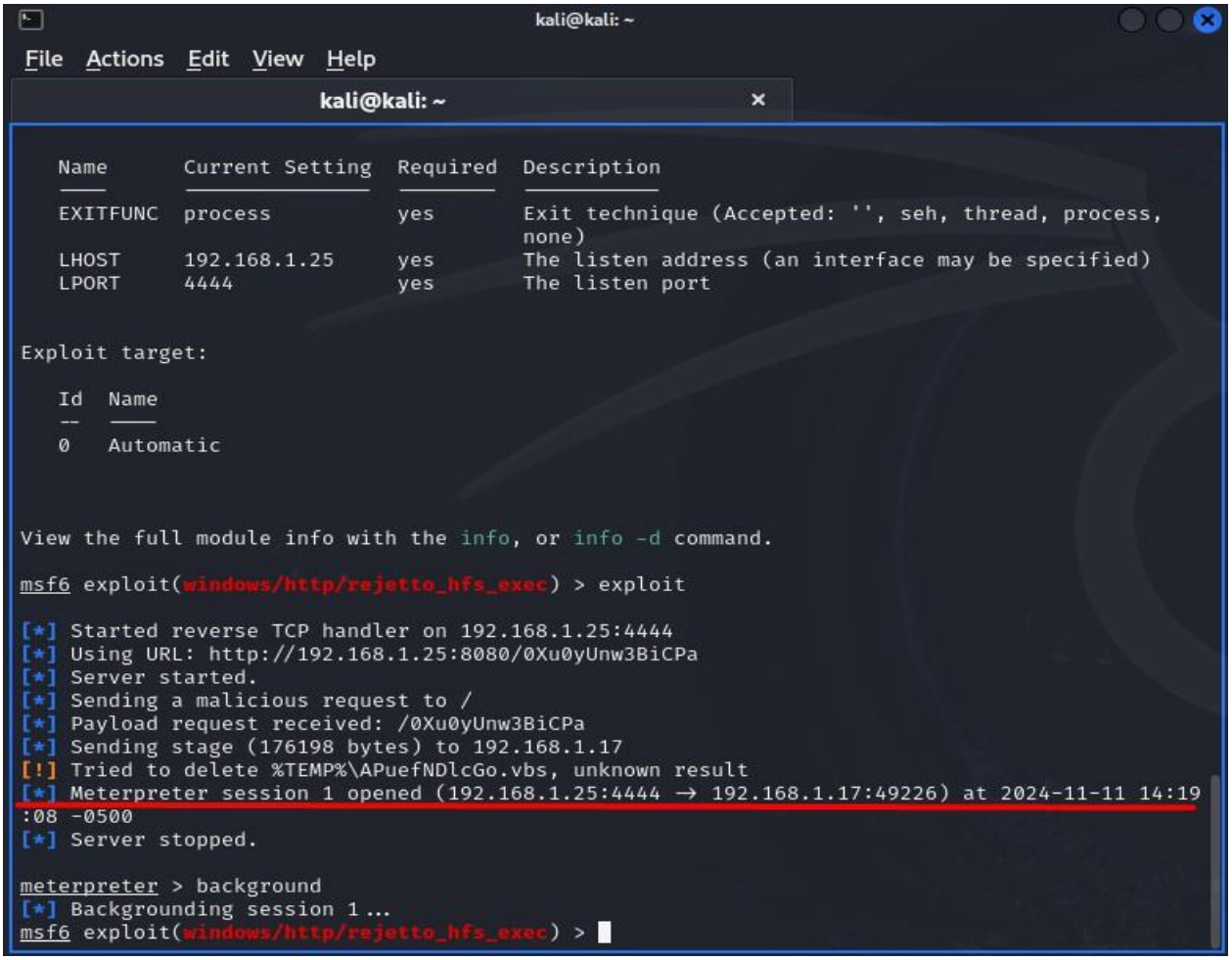
Ingreso a la Consola De Metasploit Y Búsqueda Del Servicio HFS



Fuente. Autoría Propia

Figura 5

Sesión Iniciada con Meterpreter



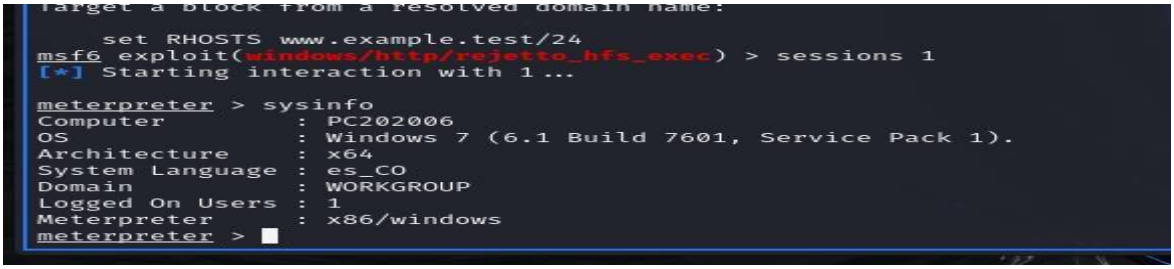
Fuente. Autoría Propia

Escalación de Privilegios. Una vez obtenida la conexión con Meterpreter, el atacante puede comprobar los privilegios actuales y escalarlos para obtener control total de la máquina.

Resultado Esperado: Confirmación de los privilegios actuales en la máquina Windows. El comando getprivs muestra los privilegios disponibles, permitiendo que el atacante determine si puede escalar sus permisos.

Figura 6

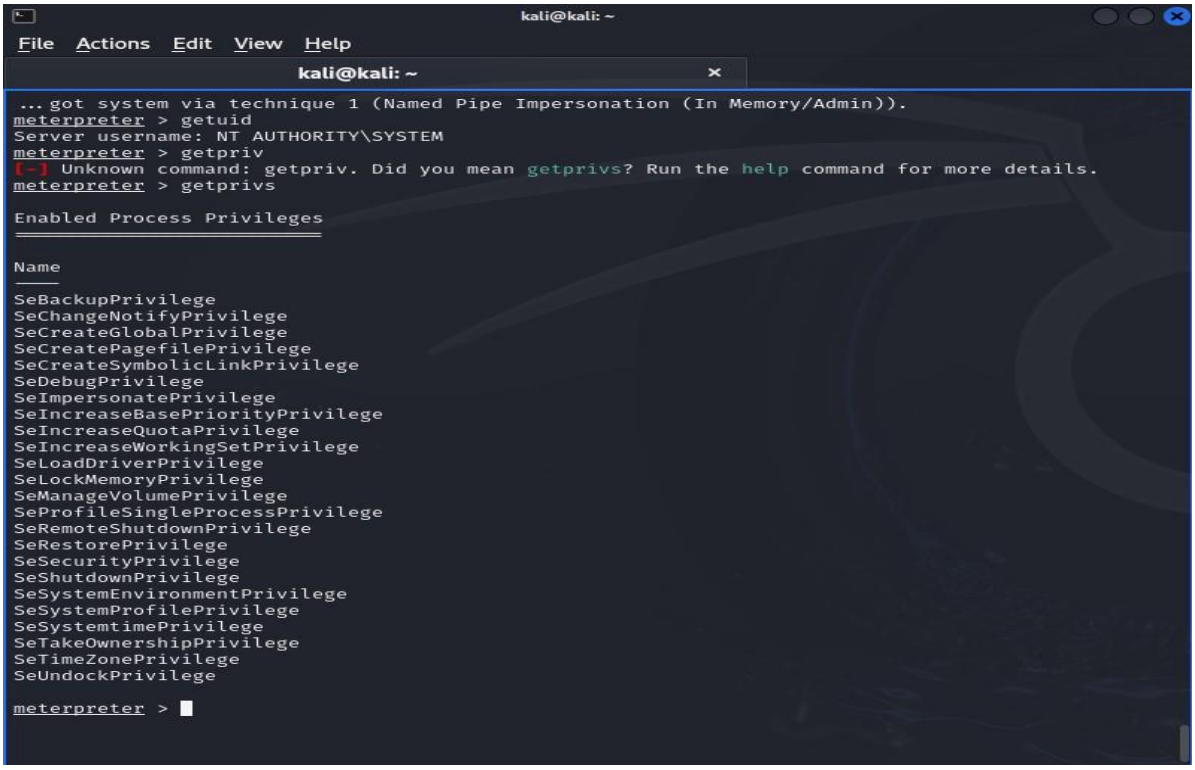
Información del Sistema de la Maquina Victim



Fuente: Autoría Propia

Figura 7

Comando para Visualizar los Privilegios de los Usuarios de la Maquina



Fuente. Autoría Propia

Resultado Esperado. Creación de un usuario con privilegios de administrador, proporcionando al atacante el control total sobre el sistema.

Figura 8

Ejecución de comando para crear usuario desde powershell

Fuente: Autoría Propia

Mantenimiento del Acceso. Con el objetivo de mantener el acceso a la máquina comprometida, se crea un nuevo usuario con privilegios de administrador y se confirma que se ha añadido al sistema con éxito. Esto permite al atacante volver a acceder a la máquina en el futuro si es necesario.

Resultado Esperado: Confirmación de que el nuevo usuario ha sido creado correctamente y tiene privilegios de administrador.

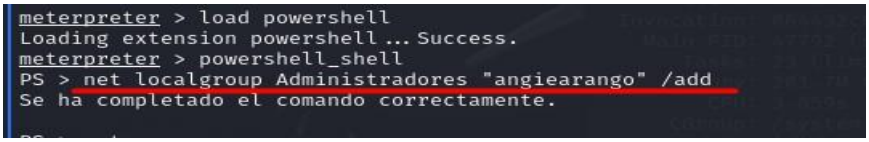
Figura 9

Ejecución de Comando para Crear Usuario Desde Powershell

Fuente. Autoría Propia

Figura 10

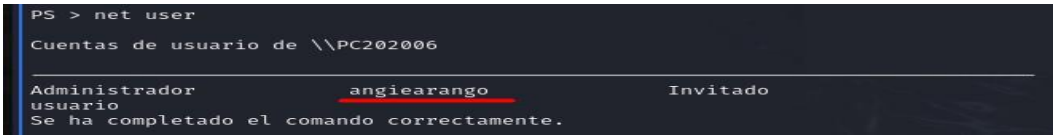
Asignación de Grupo Administrador al Usuario Creado



Fuente. Autoría Propia

Figura 11

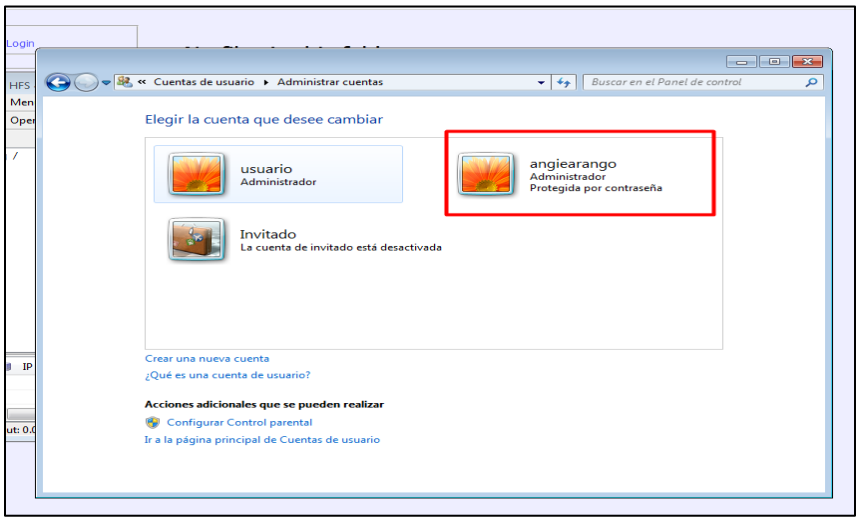
Visualización de los Usuarios en la Maquina Windows 7



Fuente. Autoría Propia

Figura 12

Visualización de Usuario Creado Desde la Maquina Windows 7



Fuente. Autoría Propia

Análisis Post-Explotación. Después de obtener privilegios elevados, el atacante puede continuar con otras tareas, como explorar la máquina comprometida y asegurarse de que el acceso persistente se mantenga, por ejemplo, a través de una sesión persistente o el uso de herramientas adicionales.

Resultado Esperado. Continuación de la sesión en segundo plano para realizar más tareas en la máquina comprometida, como ejecutar scripts adicionales o explorar más recursos.

En este análisis, se utilizaron varias herramientas de Kali Linux y Metasploit para llevar a cabo cada una de las fases de un pentesting. El uso de Nmap para el escaneo de puertos, Metasploit para la explotación de vulnerabilidades, Meterpreter para interactuar con la máquina comprometida y PowerShell para crear un usuario con privilegios de administrador, permitió demostrar un ataque completo y escalado en un entorno controlado.

Información Escenario

Sistema Operativo Afectado (Windows 7): La información de que la máquina comprometida ejecuta Windows 7 fue crucial, ya que este sistema operativo es conocido por tener múltiples vulnerabilidades de seguridad, especialmente si no se encuentra actualizado. Esto orientó la investigación hacia las vulnerabilidades comunes en versiones antiguas de Windows, incluidas aquellas relacionadas con servicios no parchados o aplicaciones inseguras.

Aplicación Vulnerable Instalada: Se identificó que una aplicación vulnerable estaba instalada en el sistema. Esta aplicación fue el punto de partida para la investigación, ya que se sospechaba que pudiera tener un exploit asociado que facilitara el acceso no autorizado. Esto llevó a un análisis más profundo de la aplicación en busca de posibles fallas, configuraciones incorrectas o problemas de seguridad.

Exploit Conocido Asociado A La Aplicación. La sospecha de que la aplicación vulnerable tenía un exploit conocido fue fundamental para el análisis. Al tener este conocimiento, se pudo enfocar la investigación en la explotación de dicha vulnerabilidad, lo que permitió realizar pruebas de intrusión específicas para ver si realmente era posible acceder al sistema y escalar privilegios.

Escalación De Privilegios Mediante Creación De Un Usuario Administrador. La información de que el ataque incluía la creación de un usuario con privilegios de administrador fue un dato importante. Este objetivo específico ayudó a guiar el enfoque hacia técnicas de escalación de privilegios, particularmente buscando maneras de ganar acceso elevado mediante la explotación de la vulnerabilidad de la aplicación.

Copia forense del Servidor. La entrega de una copia forense del servidor afectado fue una pieza clave, ya que permitió realizar un análisis detallado del sistema sin comprometer la integridad del sistema original. Esto permitió explorar posibles trazas de la vulnerabilidad, revisar archivos de configuración, logs y demás elementos del sistema que podrían haber facilitado la explotación.

Datos Sobre Puertos Y Servicios Abiertos. Aunque no se menciona explícitamente en el escenario 3, la información sobre puertos abiertos en la máquina (como el 135, 80, 139 y 10243) fue crucial en la identificación de posibles vectores de ataque adicionales. Estos puertos revelaron servicios que podrían ser explotados o utilizados como puntos de entrada para realizar el ataque.

Fuga de Información Interna. El dato sobre la fuga de información fue clave para el análisis, ya que proporcionó el contexto de la amenaza. Esto permitió enfocar la investigación en la identificación de posibles puntos de acceso a los que se pudiera estar extrayendo información

confidencial, facilitando así la detección de las vulnerabilidades que podrían ser explotadas por un atacante.

Herramientas Utilizadas y Puertos

Para identificar los fallos de seguridad en la máquina Windows, utilicé Kali Linux como entorno de pruebas. Esta plataforma es ampliamente utilizada en pruebas de penetración debido a sus poderosas herramientas de seguridad. Dentro de Kali Linux, empleé Nmap, una herramienta esencial para escanear redes y sistemas en busca de puertos abiertos y servicios vulnerables. Realicé un escaneo de vulnerabilidades hacia la dirección IP 192.168.1.17, que corresponde a la máquina Windows 7 en el escenario. Este escaneo me permitió identificar servicios activos, puertos abiertos y posibles puntos de entrada a través de los cuales un atacante podría explotar vulnerabilidades en el sistema.

A través del escaneo con Nmap, se detectaron varios puertos abiertos en la máquina Windows 7, entre los cuales se incluyen puertos como 135, 80, 139 y 10243. Estos puertos corresponden a servicios comunes en Windows, como el MS RPC (puerto 135), HTTP (puerto 80), y NetBIOS (puertos 139 y 10243). En particular, la aplicación vulnerable asociada en este escenario podría estar utilizando uno de estos puertos, especialmente el puerto 80 (HTTP), que es comúnmente aprovechado por aplicaciones web vulnerables. Estos puertos abiertos representan vectores de ataque potenciales que un atacante podría explotar para acceder a la máquina Windows y comprometer la seguridad del sistema.

Explicación del Impacto del Ataque en la Máquina Windows

El ataque dirigido a la máquina Windows 7 se basa en la explotación de una vulnerabilidad en una aplicación específica instalada en el sistema, que permite el acceso no autorizado al dispositivo. Utilizando Kali Linux y herramientas como Nmap, se identificaron

varios puertos abiertos en el sistema de la máquina Windows 7, lo que permitió determinar puntos de entrada a través de los cuales un atacante podría infiltrarse. El ataque en cuestión se aprovechó de una vulnerabilidad que podría haber estado relacionada con un servicio que escucha en el puerto 80 (HTTP), permitiendo así la ejecución remota de código malicioso.

Una vez que el atacante accede a la máquina, la explotación de la vulnerabilidad puede dar paso a la ejecución de un exploit, que en este caso permitió ganar acceso al sistema. Con ese acceso inicial, el atacante puede escalar privilegios en la máquina, creando un usuario con privilegios de administrador (utilizando “angiearango”), lo que permite un control total del sistema afectado. Este tipo de ataque tiene un impacto significativo, ya que el atacante obtiene control completo sobre el sistema, lo que permite no solo robar o modificar información sensible, sino también potencialmente comprometer la red y otros sistemas conectados.

A continuación, se presenta un gráfico que ilustra cómo se lleva a cabo este ataque:

Escaneo de Vulnerabilidades. El atacante utiliza herramientas como Nmap para identificar puertos abiertos en la máquina Windows. En este caso, se detectaron puertos como 135, 80, 139 y 10243, que son servicios comunes en Windows y que pueden estar asociados a vulnerabilidades explotables.

Explotación de la Vulnerabilidad. A través de un exploit en la aplicación vulnerable (posiblemente asociada al puerto 80 o 135), el atacante puede ejecutar comandos remotamente, obteniendo acceso al sistema afectado.

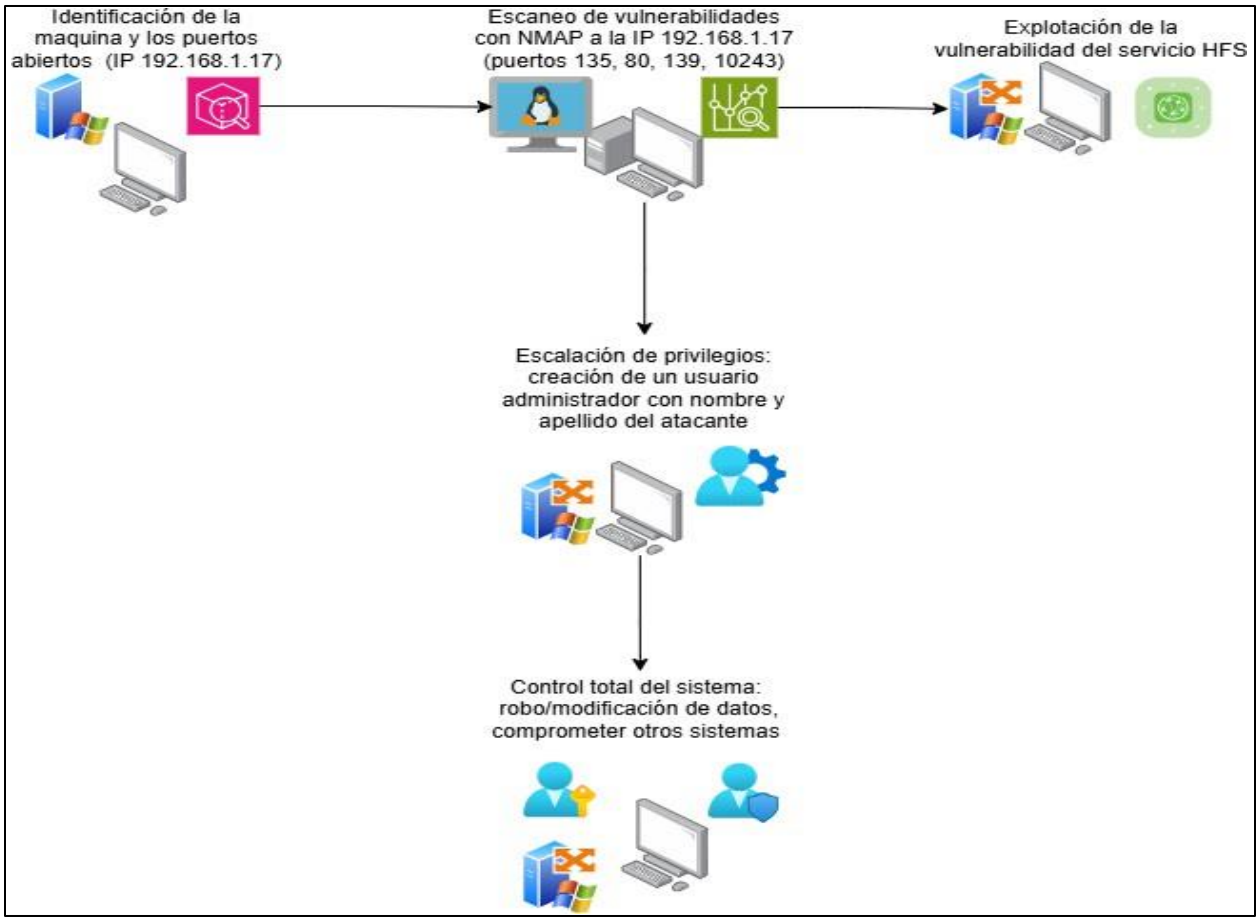
Escalación de Privilegios. Una vez dentro del sistema, el atacante puede elevar sus privilegios a nivel de administrador, creando un nuevo usuario con privilegios de administrador (utilizando “angiearango”). Esto le permite tener un control completo sobre el sistema, lo que incluye la capacidad de robar o modificar información sensible

Impacto Final. El atacante ahora tiene acceso completo al sistema, lo que le permite robar información, modificar configuraciones o incluso comprometer otras máquinas conectadas a la misma red. Esta situación presenta un grave riesgo de fuga de datos y daño a la integridad de los sistemas.

Este tipo de ataque subraya la importancia de mantener los sistemas actualizados y realizar auditorías de seguridad de manera regular para prevenir este tipo de brechas.

Figura 13

Explicación del Ataque



Fuente. Autoría Propia

Defensa Cibernética: Estrategias del Blue Team

Argumento Técnico

Al enfrentarse a un ataque en tiempo real, lo primero que se debe hacer es priorizar la contención y el análisis inicial para minimizar el daño y entender el alcance del ataque, , detallo un enfoque basado en las mejores prácticas técnicas:

Identificación del Ataque

Acciones: Confirmar la existencia del ataque analizando alertas del sistema (logs, IDS/IPS, firewall).

Identificar los síntomas:

- Tráfico inusual en la real.
- Alta utilización de recursos.
- Procesos sospechosos.

Argumento Técnico: Confirmar la existencia del ataque es esencial para distinguir entre un incidente legítimo y un falso positivo. Esto implica analizar registros del sistema, alertas de herramientas como IDS/IPS, y datos de firewalls. Los síntomas, como tráfico inusual en la red, consumo excesivo de recursos o procesos desconocidos en ejecución, son indicadores clave. Herramientas como Wireshark pueden analizar paquetes sospechosos en la red, mientras que los registros del sistema operativo ayudan a detectar patrones anómalos que indiquen actividad maliciosa.

Aislamiento del Sistema Afectado

Acciones: Desconectar la máquina comprometida de la red para evitar la propagación del ataque.

Aplicar reglas en el firewall para bloquear direcciones IP sospechosas.

Argumento Técnico: Aislar el equipo comprometido de la red evita que el atacante propague el ataque o acceda a otros recursos. Esto se logra desconectando físicamente el sistema o configurando reglas específicas en el firewall para bloquear direcciones IP maliciosas. La segmentación de la red y la suspensión de servicios comprometidos son medidas críticas. Este paso protege la infraestructura restante mientras se trabaja en la contención.

Análisis Rápido

Acciones

- Revisar procesos activos con herramientas GPL como Process Hacker o Sysinternals Suite.
- Identificar conexiones activas con comandos como “netstat -ano”.
- Inspeccionar logs relevantes, como el Visor de Eventos de Windows, para detectar patrones sospechosos.

Argumento Técnico: Realizar un análisis inicial ayuda a identificar el vector de ataque y el alcance del daño. Herramientas como Process Hacker o el Visor de Eventos de Windows permiten detectar procesos maliciosos o conexiones sospechosas. El uso del comando netstat - ano ayuda a identificar conexiones activas y posibles IPs involucradas en el ataque. Este análisis preliminar da una visión general del ataque y prioriza las acciones de mitigación necesarias.

Captura de Evidencia

Acciones

- Generar un volcado de memoria usando herramientas como DumpIt o Volatility Framework.
- Copiar logs y configuraciones relevantes.

Argumento Técnico: Es fundamental preservar datos del sistema afectado para la investigación forense. Esto incluye generar volcados de memoria con herramientas como Volatility Framework, copiar registros críticos del sistema y capturar configuraciones de red. Estos datos deben almacenarse en un entorno seguro para evitar alteraciones. La evidencia recopilada es clave para determinar cómo ocurrió el ataque y preparar un informe técnico detallado.

Contención

Acciones:

- Detener servicios o procesos maliciosos identificados.
- Revocar credenciales comprometidas y cambiar contraseñas críticas.

Argumento Técnico: Detener el ataque implica cerrar procesos maliciosos, desactivar servicios comprometidos y revocar credenciales afectadas. Cambiar contraseñas y fortalecer políticas de acceso mitiga la posibilidad de reingreso del atacante. Este paso no solo detiene el daño inmediato, sino que asegura que el sistema pueda ser estabilizado para su posterior análisis y recuperación.

Notificación Interna

Acciones:

- Informar al equipo de ciberseguridad y liderazgo interno.
- Activar el plan de respuesta a incidentes.

Argumento Técnico: Es fundamental informar al equipo de ciberseguridad y a los líderes de la organización sobre el ataque para activar el plan de respuesta a incidentes. La comunicación oportuna asegura que todos los involucrados estén alineados y puedan tomar decisiones rápidas, como reforzar controles de acceso o preparar acciones legales. Además,

permite coordinar recursos, como personal y herramientas, para contener el ataque y gestionar sus efectos. La transparencia interna también es clave para evaluar el impacto operativo del incidente.

Estas son algunas de las herramientas recomendadas (licencia GPL), para realizar un proceso de identificación, aislamiento, captura de evidencia, etc.:

- Wireshark: Para analizar tráfico de red.
- ClamAV: Para escaneo y eliminación de malware.
- Volatility Framework: Para análisis forense de memoria.
- OSSEC: Para monitoreo de logs y detección de intrusos.

Hardenización

Para prevenir que un ataque como el ejecutado en el ejercicio de Red Team se repita, es fundamental implementar medidas de hardening en los sistemas y la red. Estas medidas deben abordar las vulnerabilidades explotadas y fortalecer la seguridad general.

Actualización y Parcheo del Sistema Operativo

Mantener el sistema operativo actualizado es crucial para protegerlo contra vulnerabilidades conocidas, como la explotada en la máquina Windows 7. Aplicar parches de seguridad de manera regular y planificar una migración a versiones más modernas, como Windows 10 o 11, elimina riesgos asociados con sistemas sin soporte técnico.

Eliminación de Aplicaciones Inseguras

Retirar o reemplazar aplicaciones obsoletas o vulnerables, como el HTTP File Server (HFS) mencionado, minimiza posibles vectores de ataque. Si no es posible eliminarlas, se deben implementar medidas como configurar entornos aislados mediante virtualización o contenedores para ejecutar estas aplicaciones de forma más segura.

Configuración de Roles y Privilegios

Restringir los permisos de usuario minimiza el impacto de escalaciones de privilegios. Implementar el principio de mínimo privilegio garantiza que solo los usuarios autorizados puedan realizar tareas administrativas. Además, las cuentas con privilegios elevados deben monitorearse de manera continua, registrando su uso y revisándolas periódicamente.

Monitoreo y Detección de Intrusiones

Instalar herramientas GPL como *OSSEC* para detectar actividades sospechosas, como intentos de escalación de privilegios o cambios en usuarios del sistema. También es recomendable habilitar registros detallados en el sistema operativo y configurarlos para que se envíen a un servidor centralizado, evitando su manipulación por atacantes.

Restricción de Puertos y Servicios

Deshabilitar puertos no utilizados y restringir el acceso a servicios críticos reduce la superficie de ataque. En el caso específico del ejercicio, puertos como el 135, 80, 139 y 10243 deben configurarse para aceptar conexiones únicamente desde direcciones IP confiables. El uso de un firewall de host puede reforzar estas restricciones.

Implementación de Políticas de Contraseñas Fuertes

Reforzar las políticas de contraseñas asegura que los usuarios no creen credenciales fáciles de adivinar. Esto incluye exigir contraseñas largas, complejas y únicas, además de implementar autenticación multifactor (MFA) para cuentas críticas.

Segmentación de la Red

Dividir la red en segmentos protegidos asegura que incluso si un atacante compromete un sistema, su acceso no se propague a otros recursos. Además, es recomendable usar VLANs y controles de acceso específicos para limitar el tráfico entre diferentes partes de la red.

Escaneos de Vulnerabilidades Regulares

Implementar herramientas como *OpenVAS* o *Nessus* en su versión GPL para realizar análisis periódicos de vulnerabilidades en los sistemas y aplicaciones. Esto permite identificar y corregir posibles puntos débiles antes de que puedan ser explotados.

Diferencia entre Blue Team y Equipo de Respuesta A Incidentes Informáticos

Enfoque y Propósito Principal

El Blue Team es un equipo dedicado a fortalecer la seguridad de la organización. Su enfoque está en la defensa proactiva, como la implementación de controles de seguridad, monitoreo continuo y gestión de vulnerabilidades. Trabajan para prevenir incidentes antes de que ocurran.

El IR Team, por otro lado, es responsable de responder y gestionar incidentes de seguridad cuando ocurren. Su objetivo es contener, investigar, mitigar y recuperar los sistemas afectados tras un ataque. Este equipo trabaja principalmente de manera reactiva.

Actividades realizadas

El Blue Team realiza tareas como análisis de tráfico de red, auditorías de seguridad, configuración de sistemas y revisión de registros para detectar actividades sospechosas.

El IR Team se especializa en análisis forense, restauración de sistemas, manejo de evidencias y comunicación con partes interesadas durante un incidente.

Metodologías

El Blue Team utiliza herramientas como SIEM (Gestión de Eventos e Información de Seguridad), IDS/IPS (Sistemas de Detección/Prevención de Intrusos) y soluciones de monitoreo.

El IR Team sigue un plan de respuesta a incidentes que incluye identificación, contención, erradicación, recuperación y lecciones aprendidas.

Ejemplo Práctico

Imaginemos que una organización detecta un tráfico inusual hacia un puerto no estándar.

El Blue Team utiliza herramientas como Wireshark para analizar el tráfico y ajustar el firewall, bloqueando el acceso al puerto comprometido.

Si el tráfico resulta ser parte de un ataque ya en curso, el IR Team toma el control, desconecta el sistema afectado, recopila evidencia forense e inicia la recuperación del servicio.

Ventajas de Cada Equipo

Blue Team

Previene incidentes antes de que ocurran mediante un enfoque proactivo.

Reduce la superficie de ataque al implementar medidas de seguridad robustas.

Ofrece monitoreo continuo, detectando amenazas en etapas tempranas.

IR Team

Minimiza el impacto de los incidentes al responder rápidamente.

Recupera los sistemas de forma organizada y con enfoque en la continuidad del negocio.

Proporciona análisis forense, permitiendo identificar las causas raíz y evitar incidentes futuros.

Respuesta CIS

El CIS proporciona directrices, controles y herramientas diseñadas para fortalecer la seguridad de sistemas y redes.

Dentro de un equipo Blue Team, se utilizaría principalmente para:

Implementar Controles De Seguridad Estandarizados

Los CIS Controls son un conjunto de mejores prácticas diseñadas para priorizar las acciones de seguridad más efectivas contra amenazas comunes. El Blue Team puede utilizarlos para fortalecer la seguridad organizacional, enfocándose en áreas clave como la gestión de activos, control de acceso y monitoreo continuo. Esto permite establecer un marco estructurado que prioriza medidas con alto impacto en la reducción de riesgos.

Asegurar Configuraciones De Sistemas Y Aplicaciones

Los benchmarks de CIS ofrecen guías detalladas para configurar sistemas operativos, aplicaciones y dispositivos con un enfoque seguro. Estas configuraciones minimizan vulnerabilidades derivadas de valores predeterminados inseguros o configuraciones incorrectas. Al aplicar estas guías, el Blue Team asegura que la infraestructura sea más resistente frente a ataques cibernéticos, especialmente aquellos que explotan configuraciones mal aseguradas.

Auditoría y Monitoreo Continuo

Las recomendaciones de CIS sirven como estándares para auditar la seguridad de los sistemas, ayudando al equipo a identificar desviaciones en las configuraciones implementadas. Estas auditorías aseguran que los sistemas cumplan con las políticas internas y los estándares de la industria. Además, fomentan un monitoreo continuo para detectar y corregir rápidamente posibles configuraciones inseguras antes de que puedan ser explotadas.

Ejemplo

Supongamos que una organización utiliza servidores Windows para alojar aplicaciones críticas. El Blue Team identifica que los servidores no tienen configuraciones optimizadas para seguridad. Usando los benchmarks de CIS para Windows Server, pueden implementar configuraciones seguras como:

- Desactivar servicios no esenciales.
- Forzar políticas de contraseñas fuertes.
- Habilitar cifrado de datos en tránsito y en reposo.

En resumen, aplicar estas guías no solo reduce la probabilidad de explotación de vulnerabilidades conocidas, sino que también asegura que los servidores cumplan con estándares de la industria. Esto mejora la postura de seguridad de manera proactiva, alineando las operaciones del equipo Blue Team con prácticas reconocidas internacionalmente.

SIEM

Un SIEM (Security Information and Event Management) es una solución de software que centraliza, analiza y correlaciona datos de eventos de seguridad provenientes de múltiples fuentes en una red. Es fundamental para la detección temprana de amenazas, cumplimiento normativo y respuesta a incidentes. Sus funciones y características principales son:

Recolección Centralizada de Logs

Un SIEM recopila registros de eventos de diversas fuentes, como firewalls, sistemas operativos, aplicaciones, IDS/IPS, y bases de datos. Esta capacidad centraliza la información, facilitando su análisis y reduciendo la complejidad de gestionar múltiples sistemas. Esto asegura que el equipo de seguridad tenga visibilidad completa de la infraestructura.

Correlación y Análisis de Eventos

El SIEM utiliza reglas, algoritmos y análisis avanzado para correlacionar eventos de distintas fuentes. Esto permite identificar patrones que podrían indicar un ataque o actividad sospechosa, como intentos de inicio de sesión fallidos en múltiples sistemas. Esta característica

transforma grandes volúmenes de datos en información accionable para los equipos de seguridad.

Monitoreo en Tiempo Real

Un SIEM proporciona alertas en tiempo real sobre eventos críticos que puedan indicar una amenaza. Por ejemplo, si detecta un aumento repentino en el tráfico hacia un puerto inusual o una escalación de privilegios no autorizada. Esta capacidad permite a los equipos de seguridad responder de manera inmediata para contener incidentes.

Gestión de Incidentes

Ofrece herramientas para rastrear, documentar y gestionar incidentes de seguridad desde su detección hasta su resolución. Esto incluye la generación de informes sobre las acciones tomadas y las lecciones aprendidas. Esta función facilita el cumplimiento normativo al demostrar que los incidentes se manejaron adecuadamente.

Informes y Cumplimiento Normativo

El SIEM genera informes personalizados que ayudan a las organizaciones a cumplir con regulaciones como GDPR, ISO 27001, o PCI DSS. Estos informes incluyen detalles sobre eventos de seguridad, auditorías y métricas clave, demostrando la eficacia de las medidas de seguridad implementadas.

Características Adicionales

- Escalabilidad: Puede manejar grandes volúmenes de datos en organizaciones de cualquier tamaño.
- Integración: Se conecta con múltiples tecnologías de seguridad, como EDR (Endpoint Detection and Response) o soluciones de firewall.

- Automatización: Incorpora respuestas automáticas a incidentes, como bloquear direcciones IP sospechosas o aislar endpoints comprometidos.

Ejemplos de Herramientas SIEM Populares

Splunk Enterprise Security

- Splunk es una de las soluciones más robustas y completas del mercado, conocida por su capacidad de manejar grandes volúmenes de datos y ofrecer análisis avanzado.
- Características clave: Correlación en tiempo real, paneles personalizables y automatización de respuesta a incidentes (SOAR).
- Usos: Ideal para organizaciones que necesitan capacidades avanzadas de búsqueda y análisis de datos.

IBM QRadar

- Descripción: Ofrece una integración avanzada con otras soluciones de IBM y es ampliamente utilizado en grandes empresas.
- Características clave: Detección de amenazas con inteligencia artificial, gestión automatizada de incidentes y fácil escalabilidad.
- Usos: Excelente para empresas que necesitan integrar su SIEM con sistemas de inteligencia de amenazas.

ArcSight (Micro Focus)

- Descripción: Este SIEM es conocido por su enfoque en la correlación avanzada de eventos y es una de las soluciones más antiguas del mercado.
- Características clave: Análisis de datos en tiempo real, soporte para grandes volúmenes de datos y robustas capacidades de integración.

- Usos: Adecuado para redes corporativas complejas con necesidades avanzadas de correlación de eventos.

AlienVault (AT&T Cybersecurity)

- Descripción: Una solución más accesible para empresas medianas y pequeñas. Integra capacidades SIEM con gestión de vulnerabilidades y análisis de amenazas.
- Características clave: Análisis de amenazas basado en la comunidad (OTX), escaneo de vulnerabilidades y detección de intrusos.
- Usos: Perfecto para organizaciones que buscan una solución todo-en-uno sin altos costos.

Graylog

- Descripción: Es una opción de código abierto, ideal para empresas con presupuestos limitados que buscan personalización.
- Características clave: Gestión eficiente de logs, visualización de datos y fácil integración con otros sistemas.
- Usos: Pequeñas empresas o entornos donde se necesite adaptar la herramienta a necesidades específicas.

Herramientas de Contención De Ataques Informáticos

Las herramientas de contención son aquellas diseñadas para mitigar y limitar el impacto de un ataque en tiempo real, evitando su propagación y protegiendo los activos críticos. A continuación, se describen tres herramientas clave:

Firewalls de Próxima Generación (NGFW)

Son dispositivos o software que supervisan, filtran y bloquean el tráfico de red basado en reglas predefinidas y en análisis avanzados. Además de las capacidades tradicionales de los firewalls, incluyen inspección profunda de paquetes, control de aplicaciones y detección de malware.

- Uso en Contención:
  - Permiten bloquear tráfico malicioso identificado durante un ataque.
  - Pueden contener un ataque como una intrusión o un intento de exfiltración de datos al cortar la conexión a direcciones IP específicas.
- Ejemplo: Palo Alto Networks NGFW, Fortinet Fortigate o Cisco Firepower.

Sistemas de Prevención de Intrusos (IPS)

Son sistemas diseñados para monitorear el tráfico de red y detener actividades maliciosas en tiempo real mediante la aplicación de políticas de bloqueo. A diferencia de los IDS, que solo detectan, los IPS toman acciones inmediatas para mitigar ataques.

- Uso en Contención:
  - Bloquean conexiones sospechosas o tráfico relacionado con exploits conocidos.
  - Actúan como una barrera que impide que un atacante acceda a servicios vulnerables o propague malware.
- Ejemplo: Snort (software GPL) o Suricata.

Software de Control de Acceso a Aplicaciones (WAF)

Un WAF (Web Application Firewall) protege aplicaciones web al filtrar y monitorear tráfico HTTP, deteniendo solicitudes maliciosas que buscan explotar vulnerabilidades en aplicaciones web.

- Uso en Contención:
  - Bloquea intentos de inyección SQL, Cross-Site Scripting (XSS) y otros ataques web.
  - Impide que el tráfico malicioso llegue a la aplicación objetivo, conteniendo la amenaza antes de que cause daño.
- Ejemplo: ModSecurity, Fortinet FortiWeb o AWS WAF.

Mientras que los firewalls y los IPS actúan a nivel de red para contener amenazas generalizadas, los WAFs se enfocan en proteger aplicaciones críticas específicas. Estas herramientas son fundamentales para una estrategia integral de respuesta a incidentes, ya que limitan el impacto de un ataque antes de que pueda comprometer la infraestructura.

Ejemplos:

Firewall Fortinet (FortiGate): Contención de un Ataque de Ransomware

- Escenario: Una organización detecta un aumento repentino de tráfico saliente desde varios equipos hacia direcciones IP desconocidas. Esto es un comportamiento típico de un ransomware en su etapa de exfiltración de datos.
- Acción de Contención: El FortiGate NGFW detecta patrones anómalos en el tráfico y, basado en su análisis profundo de paquetes, bloquea automáticamente las conexiones hacia las IP sospechosas. Además, aísla la red de los equipos afectados mediante la segmentación dinámica, impidiendo que el ransomware se propague dentro de la infraestructura.
- Resultado: El ataque es contenido rápidamente, limitando su impacto y evitando la fuga de datos críticos.

IPS Check Point: Contención de un Exploit de Día Cero

- Escenario: Un atacante intenta explotar una vulnerabilidad desconocida en el sistema operativo de un servidor corporativo, utilizando un exploit de día cero.
- Acción de Contención: El IPS Check Point Intrusion Prevention System, gracias a su integración con inteligencia de amenazas en tiempo real, identifica el tráfico como malicioso por su comportamiento. Actúa bloqueando automáticamente las solicitudes entrantes al puerto comprometido del servidor y genera una alerta al equipo de seguridad para tomar medidas adicionales.
- Resultado: El servidor queda protegido antes de que el atacante pueda completar la explotación, asegurando la continuidad del servicio.

WAF Fortinet (FortiWeb): Contención de un Ataque de Inyección SQL

- Escenario: Una aplicación web de comercio electrónico está siendo atacada con inyecciones SQL para extraer datos sensibles de la base de datos, como información de clientes y transacciones.
- Acción de Contención: FortiWeb detecta las solicitudes maliciosas analizando patrones en el tráfico HTTP/HTTPS. Bloquea automáticamente las peticiones sospechosas y coloca en una lista negra temporal las direcciones IP que realizan el ataque. También genera un informe detallado sobre las actividades bloqueadas para análisis posterior.
- Resultado: Los datos sensibles de los clientes no son expuestos, y la aplicación sigue operando sin interrupciones para los usuarios legítimos.

Firewall IPtables (Linux): Contención de un Ataque DDoS

- Escenario: Un servidor web experimenta un tráfico anómalo proveniente de miles de IPs, lo que ralentiza el servicio (ataque DDoS).

- Acción de Contención: El administrador configura IPtables, un firewall gratuito integrado en Linux, para limitar el número de conexiones por dirección IP mediante reglas como:

iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 10 -j DROP

Esto limita las conexiones simultáneas por IP, mitigando el ataque y priorizando usuarios legítimos.

Snort: Contención de un Escaneo de Puertos Malicioso

- Escenario: Una organización detecta múltiples intentos de escaneo de puertos en su red corporativa, una técnica utilizada para identificar servicios vulnerables.
- Acción de Contención: El administrador de red utiliza Snort, un sistema de prevención/detección de intrusos gratuito, configurando una regla personalizada para identificar y bloquear los escaneos:

alert tcp any any -> any any (msg:"Port Scan Detected"; flags:S; threshold:type both, track by_src, count 10, seconds 5; sid:1000001;)

Cuando Snort detecta más de 10 conexiones en 5 segundos desde la misma IP, genera una alerta y puede integrarse con herramientas de firewall (como IPtables) para bloquear automáticamente la IP atacante.

- Resultado: El ataque es contenido, y el atacante no puede continuar explorando la red para identificar vulnerabilidades.

AWS WAF: Contención de un Ataque de Inyección SQL

- Escenario: Una aplicación web alojada en AWS está siendo atacada con inyecciones SQL para extraer información sensible de una base de datos.
- Acción de Contención: El administrador configura AWS WAF, el firewall de aplicaciones web de Amazon, para identificar y bloquear patrones de inyección SQL. Usando las

reglas administradas de AWS, se activa un filtro para bloquear solicitudes con cadenas sospechosas como SELECT, DROP, o -- en los parámetros HTTP.

- Ejemplo de regla administrada: Activa AWS Managed Ruleset "SQL Injection Protection" para bloquear automáticamente solicitudes maliciosas.
    - El WAF también genera un informe detallado de las solicitudes bloqueadas, permitiendo al equipo de seguridad investigar el origen del ataque.
- Resultado: El atacante no logra acceder a la base de datos, y la aplicación web continúa operando sin interrupciones.

Conclusiones

En conclusión, el análisis de la vulnerabilidad CVE-2014-6287 en el contexto del pentesting y las pruebas de seguridad realizadas revela la importancia de una defensa integral frente a los ataques. El Red Team, al aprovechar las vulnerabilidades conocidas y las configuraciones inseguras de los sistemas, puede simular ataques avanzados que evidencian fallos críticos en las políticas de seguridad de la organización. La explotación de vulnerabilidades como el HTTP File Server (HFS) subraya la necesidad de mantener sistemas y aplicaciones actualizados, así como de aplicar medidas de hardening que eliminen posibles vectores de ataque antes de que sean aprovechados por los atacantes.

Por su parte, el Blue Team debe implementar un enfoque proactivo en la identificación y mitigación de riesgos, centrando sus esfuerzos en la detección temprana, la contención rápida y la protección de los sistemas. El monitoreo en tiempo real, el aislamiento efectivo de los sistemas comprometidos y la correcta aplicación de políticas de seguridad como la segmentación de redes y la gestión de privilegios son elementos clave para reducir el impacto de un ataque. Además, la preservación de evidencia forense y la revisión detallada de los logs y registros son fundamentales para analizar la raíz del ataque y mejorar las estrategias de defensa.

El trabajo conjunto entre el Red Team y el Blue Team permite una visión más completa de la seguridad organizacional, ya que mientras el primero identifica las brechas y puntos vulnerables, el segundo puede implementar las medidas correctivas y preventivas necesarias. Ambos equipos deben colaborar estrechamente para garantizar que las lecciones aprendidas de cada simulación de ataque sean aplicadas para mejorar la seguridad en tiempo real. La mejora continua de las políticas de seguridad y la capacitación constante del personal son elementos fundamentales para fortalecer la postura de ciberseguridad de la organización.

Finalmente, la integración de buenas prácticas de seguridad, como el uso de herramientas GPL de monitoreo y escaneo, la implementación de políticas de contraseñas fuertes y la planificación de actualizaciones periódicas, es crucial para proteger los sistemas ante amenazas cada vez más sofisticadas. A través de una cultura de seguridad y la adopción de tecnologías avanzadas de protección, las organizaciones pueden reducir significativamente los riesgos y asegurar la integridad de sus sistemas e información ante ataques internos y externos.

Recomendaciones

Leyes

A continuación, se presentan algunas recomendaciones clave que podrían mejorar las prácticas de CyberFort Technologies y asegurar que cumplan con las normativas legales y éticas aplicables en Colombia, especialmente en relación con la ciberseguridad y la protección de la información:

Cumplir con las Normas Legales Colombianas

La empresa debe revisar y adecuar sus acuerdos a la legislación vigente en Colombia, particularmente en lo que respecta a la Ley 1273 de 2009 (ley contra los delitos informáticos) y el Código Penal Colombiano. La obligación de no denunciar actividades ilegales, como se menciona en el acuerdo de confidencialidad, va en contra de varias leyes que sancionan la omisión de denuncia de hechos delictivos y la protección de datos personales.

Recomendación: Eliminar las cláusulas que impiden la denuncia de actividades ilegales. En su lugar, la empresa debe promover un ambiente que fomente la transparencia y el cumplimiento de la ley. Establecer un protocolo claro de actuación frente a actividades sospechosas y ofrecer canales seguros para que los empleados puedan reportar incidentes, en línea con las normativas colombianas.

Promover una Cultura Ética en Ciberseguridad

El acuerdo de confidencialidad actual parece justificar la protección de actividades ilegales, como la interceptación de datos sin autorización o el acceso abusivo a sistemas informáticos. Esto va en contra de los principios éticos fundamentales para los profesionales de ciberseguridad, como lo establece el Código de Ética del COPNIA.

Recomendación: Revisar y ajustar la política ética de la empresa para alinearla con los estándares internacionales y nacionales de ciberseguridad. La empresa debe crear una cultura ética sólida, en la que se valore la integridad profesional, la protección de la privacidad y el respeto por la ley.

Fomentar la educación continua en principios éticos de ciberseguridad para todos los empleados, asegurándose de que comprendan y adopten prácticas de seguridad responsables.

Asegurar la Protección de Datos Personales

Las cláusulas que protegen prácticas ilegales, como la apropiación de información de terceros, están en conflicto con la Ley 1581 de 2012, que regula la protección de datos personales en Colombia. La ley establece responsabilidades claras para quienes manejan información personal, y cualquier acción que viole estos principios podría acarrear sanciones graves.

Recomendación: Actualizar las políticas de privacidad y manejo de datos para asegurar que los empleados comprendan las implicaciones legales de manejar datos personales y cómo deben protegerlos. Los contratos deben reflejar el compromiso de la empresa con la transparencia en el uso de datos personales y su protección.

Implementar medidas de seguridad tecnológica adecuadas para proteger la información confidencial y personal, siguiendo las mejores prácticas de la industria y la legislación vigente.

Revisión y Modificación de los Acuerdos de Confidencialidad

El actual acuerdo de confidencialidad debe ser revisado para asegurarse de que no incluya cláusulas que puedan interpretarse como un encubrimiento de actividades ilegales. Las cláusulas que eximen de responsabilidad a la empresa en caso de prácticas ilegales deben ser eliminadas, ya que son legales y éticamente cuestionables.

Recomendación: Modificar el acuerdo de confidencialidad para incluir garantías claras sobre el cumplimiento de la ley, la no participación en actividades ilegales y la responsabilidad compartida en caso de violaciones. Las cláusulas deben enfocarse en la protección de la información, pero sin encubrir actividades ilegales.

Establecer un Comité de Cumplimiento Normativo

Dado que las leyes relacionadas con la ciberseguridad y la protección de datos están en constante evolución, es fundamental que la empresa implemente un comité de cumplimiento normativo o comité de ética, compuesto por expertos legales y en ciberseguridad. Este comité debe revisar de forma periódica todas las políticas y procedimientos de la empresa para asegurar que estén alineados con las leyes nacionales e internacionales.

Recomendación: Crear un comité de cumplimiento para revisar periódicamente los contratos, políticas de seguridad y acuerdos de confidencialidad, asegurando que todos estén en conformidad con las leyes y regulaciones aplicables. Además, este comité debe tener la capacidad de implementar medidas correctivas cuando se identifiquen violaciones de las normas legales o éticas.

Establecer Canales Seguros para Denunciar Incidentes

Una de las principales preocupaciones éticas y legales del acuerdo actual es la imposición de la no denuncia de actividades ilegales. Es fundamental que la empresa cree mecanismos adecuados para la denuncia de incidentes, permitiendo que los empleados puedan reportar cualquier actividad sospechosa de forma segura y confidencial.

Recomendación: Implementar canales seguros y confidenciales donde los empleados puedan reportar actividades ilegales sin temor a represalias. Esto podría incluir sistemas de

denuncia anónima, líneas directas con el equipo de cumplimiento y una política de no represalias frente a denuncias legítimas.

Red Team (Simulación de ataque):

Simulación de ataques a sistemas obsoletos: Realizar pruebas regulares en sistemas antiguos y aplicaciones desactualizadas, como el HTTP File Server (CVE-2014-6287), para identificar posibles vectores de ataque antes de que los atacantes reales los exploten.

Explotación de configuraciones incorrectas: Asegurarse de que el equipo de Red Team evalúe las configuraciones de seguridad, especialmente en los servicios activos, puertos abiertos y roles de privilegios, para identificar posibles fallos en las políticas de seguridad.

Escalación de privilegios mediante la explotación de vulnerabilidades: Aprovechar vulnerabilidades conocidas y configuraciones inseguras para obtener privilegios elevados y demostrar los riesgos de no seguir el principio de mínimo privilegio en el sistema.

Simulación de evasión de herramientas de detección: Evaluar la efectividad de las herramientas de detección como IDS/IPS, analizando cómo los atacantes podrían evadir su monitoreo mediante técnicas de cifrado de tráfico o explotación de sistemas mal configurados.

Pruebas de propagación lateral: Realizar pruebas de propagación lateral dentro de la red para verificar cómo un atacante podría moverse de un sistema comprometido a otros sistemas conectados, utilizando herramientas como Metasploit y técnicas avanzadas de explotación de vulnerabilidades.

Blue Team (Defensa y protección):

Monitoreo de tráfico de red: Implementar herramientas de monitoreo en tiempo real, como Wireshark y OSSEC, para identificar comportamientos anómalos en la red, como tráfico inusual y la actividad de procesos desconocidos, ayudando a detectar ataques de manera temprana.

Parcheo y actualización constante: Mantener los sistemas actualizados, especialmente los sistemas operativos antiguos, para evitar que los atacantes exploten vulnerabilidades conocidas, como CVE-2014-6287. Planificar migraciones a versiones más seguras y recientes.

Segmentación de la red y control de acceso: Implementar segmentación de la red utilizando VLANs y firewalls internos para limitar el movimiento lateral de los atacantes dentro de la infraestructura. Solo permitir conexiones de puertos críticos desde IPs confiables.

Revisión y auditoría de privilegios: Restringir los privilegios de los usuarios, asegurándose de aplicar el principio de mínimo privilegio y monitorear el uso de cuentas con privilegios elevados. Auditar regularmente las configuraciones de privilegios para detectar posibles escalaciones.

Simulación de ataques internos: Realizar simulaciones de ataques internos para evaluar cómo los atacantes pueden aprovechar vulnerabilidades en configuraciones, credenciales comprometidas o aplicaciones inseguras, y así mejorar la capacidad de respuesta ante incidentes.

Referencias Bibliográficas

Amazon.com. (s. f.). AWS WAF. Recuperado 24 de noviembre de 2024, de https://aws.amazon.com/waf

C., D., C., D., D., M., J., S., & N., R. (2023). Red Team Ethical Physical Penetration Testing Simulations using Open Source Intelligence. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023Pages 572 - 5782023 13th IEEE Annual Computing and Communication Workshop and Conference, CCWC 2023.

Cilleruelo, C. (2022a, junio 29). Fases de un pentest. KeepCoding Bootcamps. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

Cilleruelo, C. (2022b, julio 4). ¿Qué es Metasploit? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-metasploit-ciberseguridad/

Cilleruelo, C. (2022c, octubre 4). ¿Qué es ExploitDB? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/

CIS; Center for Internet Security. (s. f.). CIS Center for Internet Security. Recuperado 24 de noviembre de 2024, de https://www.cisecurity.org/

Center for Internet Security (CIS) benchmarks. (s. f.). Microsoft.com. Recuperado 24 de noviembre de 2024, de https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

Coppola, M. (2023, mayo 23). Auditoría de seguridad informática: qué es, ventajas, tipos y fases. Hubspot.es. https://blog.hubspot.es/website/auditoria-de-seguridad

El, A., de Noviembre, D. E., & Budapest., E. N. (s. f.). Visto el texto del "Convenio sobre la Ciberdelincuencia". Gov.co. Recuperado 12 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

El concepto de CVE. (s. f.). Redhat.com. Recuperado 12 de octubre de 2024, de https://www.redhat.com/es/topics/security/what-is-cve

Equipo rojo contra equipo azul. (2023, agosto 16). Check Point Software. https://www.checkpoint.com/es/cyber-hub/cyber-security/red-team-vs-blue-team/

Gómez, J. A. (2023, julio 4). Auditoría de seguridad informática: Tipos, fases y ventajas. Deltaprotect.com; Delta Protect. https://www.deltaprotect.com/blog/auditoria-de-seguridad-informatica

Guía de referencia de Nmap (Página de manual). (s. f.). Nmap.org. Recuperado 12 de octubre de 2024, de https://nmap.org/man/es/index.html

Hernández, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Institute of Electrical and Electronics Engineers Inc. (2023). Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges. Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 20232023 1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, ICoCICs 2023Hybrid, Bogor22.

Ley 1266 de 2008 - Gestor Normativo. (s. f.). Gov.co. Recuperado 12 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1273 de 2009 - Gestor Normativo. (s. f.). Gov.co. Recuperado 12 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 12 de octubre de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 842 de 2003. (s. f.). Gov.co. Recuperado 24 de octubre de 2024, de https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Londoño, I. (2020, octubre 28). 5 buenas prácticas de ciberseguridad que debes conocer. Piranirisk.com. https://www.piranirisk.com/es/blog/5-buenas-practicas-de-ciberseguridad-que-debe-conocer

Lozano, P. A. (2023, septiembre 29). Fases del pentesting: Pasos para asegurar tus sistemas. Openwebinars.net. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Mendoza, M. Á. (s. f.). El principio de la mínima exposición como estrategia de seguridad. Welivesecurity.com. Recuperado 24 de octubre de 2024, de https://www.welivesecurity.com/la-es/2018/07/02/principio-minima-exposicion-estrategia-seguridad/

Metasploit. (s. f.). Metasploit. Recuperado 24 de noviembre de 2024, de https://www.metasploit.com/

Microsoft.com. (2024, julio 18). ¿Qué es SIEM? https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

Nmap: The network mapper - Free Security Scanner. (s. f.). Nmap.org. Recuperado 24 de noviembre de 2024, de https://nmap.org/

OpenVAS - Open Vulnerability Assessment Scanner. (s. f.). Openvas.org. Recuperado 24 de noviembre de 2024, de https://www.openvas.org/

Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. (s. f.). Incibe.es. Recuperado 24 de noviembre de 2024, de https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. (2021, enero 26). Intelequia. https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Snort - network intrusion detection & prevention system. (s. f.). Snort.org. Recuperado 24 de noviembre de 2024, de https://www.snort.org/

Wireshark · go deep. (s. f.). Wireshark. Recuperado 24 de noviembre de 2024, de https://www.wireshark.org/

Solar, C. (2022). Cybersecurity Governance in Latin America: States, Threats, and Alliances. Piraí: SUNY Press. (SUNY Series in Ethics and the Challenges of Contemporary Warfare Ser). https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=e000xww&AN=3300847&lang=es&site=eds-live&scope=site

¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas. (s. f.). Fortinet. Recuperado 12 de octubre de 2024, de https://www.fortinet.com/lat/resources/cyberglossary/cve

¿Qué es NMAP? (2023, enero 16). Genuino Cloud | Correo electrónico corporativo; GenuinoCloud. https://genuinocloud.com/blog/que-es-nmap/

¿Qué es SIEM? (2024, julio 18). Ibm.com. https://www.ibm.com/mx-es/topics/siem

Apéndices

Apéndice A

Sustentación del informe técnico

- Stream - Sustentación_ Capacidades técnicas, legales y de gestión para equipos blue team y red team - Angie L. Arango-20241203_165907-Grabación de la reunión.mp4
- Youtube - https://youtu.be/YBjG_iQ8JGQ