Etapa 5 – Capacidades Técnicas, Legales y de Gestión para Equipos Red Team y Blue Team

Sandra Patricia Carrillo Velosa

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

Diciembre 2024

Etapa 5 – Capacidades técnicas legales y de gestión para Equipos de Red Team & Blue Team

Sandra Patricia Carrillo Velosa

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

Diciembre 2024

Resumen

Durante el seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”, se ejecutaron diversas actividades centradas en el reconocimiento y la aplicación de las metodologías y procedimientos utilizados por los equipos Red Team y Blue Team. Estas acciones permitieron la individualización de grietas de seguridad dentro de las organizaciones. La institución educativa suministró una cadena de escenas que fueron explorados en cada etapa del seminario. Además, se contó con bancos de trabajo y guías de configuración que facilitaron la ejecución de las tareas asignadas. Este pliego presenta un resumen de las principales etapas del seminario, destacando las características de cada fase y proporcionando una visión general de las actividades realizadas. Estas actividades contribuyeron al aprendizaje sobre la representación, funcionamiento y diferencias entre los equipos Red Team y Blue Team. En términos de las actividades ejecutadas, la primera fase estuvo enfocada en reforzar los conocimientos sobre las leyes colombianas relacionadas con la seguridad informática y la protección de la información. Asimismo, se configuraron entornos de trabajo en diversas versiones, los cuales fueron utilizados para realizar pruebas de seguridad. En la segunda fase, se identificaron vulnerabilidades en los acuerdos de confidencialidad firmados por las empresas, así como los riesgos asociados al abuso de esta información. Durante la tercera fase, se llevaron a cabo ataques simulados a los equipos previamente configurados para identificar brechas de seguridad, empleando diversas herramientas de escaneo. Finalmente, en la cuarta fase, se implementaron controles sobre las vulnerabilidades detectadas y se establecieron los pasos a seguir tras un ataque exitoso. Al finalizar el seminario, se presentarán las conclusiones más relevantes de cada fase, con el objetivo de generar recomendaciones prácticas que sean comprensibles para los lectores.

Palabras clave: Herramientas, Protección de Información, Seguridad Informática.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario

Amenaza: Potencial peligro o evento que puede causar daño a la infraestructura TI, como un ataque cibernético, fallo de hardware, desastres naturales, entre otros.

Análisis de Riesgos: Proceso que implica identificar, evaluar y priorizar los riesgos asociados con la infraestructura TI, con el fin de implementar medidas que mitiguen las amenazas y minimicen el impacto en la organización.

Ciberseguridad: Disciplina dedicada a la protección de los sistemas informáticos, redes y datos contra amenazas cibernéticas, como los ataques maliciosos, robos de información, o alteraciones de la infraestructura tecnológica.

Contención: Estrategias o medidas implementadas para limitar el impacto de una amenaza o vulnerabilidad una vez que ha sido identificada, impidiendo su propagación o exacerbación.

Controles de Seguridad: Medidas preventivas, detectivas o correctivas implementadas para proteger la infraestructura TI contra riesgos y vulnerabilidades, tales como firewalls, autenticación multifactor, encriptación, etc.

Evaluación de Impacto en el Negocio (BIA): Análisis que evalúa los efectos potenciales de una interrupción en las operaciones de negocio, identificando funciones críticas que requieren protección prioritaria durante una crisis.

Evaluación de Vulnerabilidades: Proceso de escanear y analizar sistemas y redes en busca de debilidades que puedan ser explotadas por atacantes para obtener acceso no autorizado o causar daño.

Explotación de Vulnerabilidades: Acto de aprovechar una debilidad o falla en un sistema con el fin de obtener acceso no autorizado o realizar una acción maliciosa.

Firewall (Cortafuegos): Dispositivo o software que controla el tráfico de red entre sistemas o redes, permitiendo o bloqueando comunicaciones según reglas de seguridad preestablecidas.

Gestión de Riesgos: El enfoque sistemático para identificar, evaluar, mitigar y monitorear los riesgos asociados a los sistemas y activos tecnológicos de una organización.

Impacto: Consecuencia de un evento de seguridad o incidente, que puede incluir pérdidas económicas, daños a la reputación, interrupciones operativas, entre otros efectos adversos.

Infraestructura TI: El conjunto de componentes tecnológicos, como hardware, software, redes, sistemas operativos y otros recursos, que permiten el funcionamiento de las operaciones informáticas dentro de una organización.

Mitigación: Conjunto de acciones que se toman para reducir o eliminar el riesgo o el impacto de una amenaza en la infraestructura TI.

Plan de Contingencia: Conjunto de procedimientos que una organización sigue para responder a eventos imprevistos que puedan afectar su infraestructura TI, buscando minimizar el impacto y asegurar la continuidad operativa.

Plan de Respuesta ante Desastres (DRP): Estrategia diseñada para recuperar la infraestructura TI y los servicios críticos después de un desastre, minimizando el tiempo de inactividad y protegiendo los datos esenciales.

Pruebas de Penetración (Pentesting): Simulación de ataques informáticos para identificar vulnerabilidades en una infraestructura TI, ayudando a evaluar su seguridad antes de que un atacante realice un ataque real.

Respuesta ante Incidentes: Proceso de identificación, manejo y resolución de incidentes de seguridad informática, con el objetivo de minimizar el impacto y restaurar la operatividad normal lo más rápido posible.

Riesgo: La probabilidad de que una amenaza explote una vulnerabilidad y cause un daño a los activos de una organización, generalmente medido en términos de impacto y probabilidad.

Simulación de Ataques: Ejercicio realizado con el fin de poner a prueba las defensas de un sistema informático a través de la simulación de diferentes tipos de ciberataques.

Vulnerabilidad: Cualquier debilidad en un sistema, red o infraestructura que pueda ser explotada por una amenaza para comprometer la seguridad o la integridad de la infraestructura TI.

Introducción

En el entorno actual de la tecnología, las infraestructuras de TI (Tecnologías de la Información) se han convertido en el núcleo fundamental de las operaciones empresariales. Sin embargo, a medida que las amenazas cibernéticas evolucionan y se diversifican, las organizaciones enfrentan una creciente presión para proteger sus activos digitales y garantizar la continuidad de sus servicios. En este contexto, la formulación de estrategias de contención se vuelve esencial para mitigar riesgos y vulnerabilidades que puedan poner en peligro la seguridad de la infraestructura tecnológica.

Este trabajo tiene como objetivo desarrollar estrategias efectivas de contención, basadas en un análisis exhaustivo de los riesgos y las vulnerabilidades presentes en una infraestructura de TI. A través de un enfoque sistemático, se identificarán los principales riesgos que podrían comprometer la seguridad, se evaluarán las vulnerabilidades específicas de los sistemas y se propondrán soluciones adecuadas para cada situación. El análisis se centrará en las metodologías y herramientas utilizadas para identificar, evaluar y gestionar estos riesgos, con el fin de fortalecer las defensas y minimizar las posibilidades de un ataque exitoso.

La correcta formulación de estrategias de contención no solo permite a las organizaciones proteger sus activos más valiosos, sino que también promueve una cultura organizacional resiliente frente a incidentes de seguridad. Este trabajo busca proporcionar un marco de acción claro y detallado que permita a los responsables de la infraestructura tecnológica tomar decisiones informadas para mejorar la seguridad cibernética en su entorno.

Objetivos

Objetivo general

Elaborar un informe técnico que resuma los aspectos más relevantes del desarrollo de las actividades, con el fin de presentar recomendaciones y conclusiones.

Objetivo específico

Desarrollar estrategias de contención a través del análisis de riesgos y vulnerabilidades.

Analizar casos prácticos donde la implementación de equipos de seguridad ha sido clave para prevenir o mitigar ataques cibernéticos, resaltando su impacto en la seguridad de la información.

Proponer recomendaciones sobre buenas prácticas en el uso y mantenimiento de equipos de seguridad, asegurando su efectividad en entornos corporativos o personales.

4 Desarrollo del Informe

4.1 Etapa 1 – Conceptos Equipos de Seguridad

4.1.1 Marco Jurídico de los Delitos Informáticos: Decretos Vigentes

En Colombia, los delitos informáticos y la protección de datos personales están regulados por diversas leyes que establecen el marco legal para prevenir, sancionar y regular el uso adecuado de la información digital y los datos personales. A continuación, se destacan las principales leyes y decretos en estos ámbitos:

Ley 1273 de 2009 - Delitos Informáticos

Esta ley modifica el Código Penal para incluir y sancionar los delitos informáticos. Su objetivo es proteger los bienes jurídicos afectados por las conductas que afectan los sistemas de información y datos. Las principales características de esta ley son:

Tabla 1

Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos

Artículo	Delito
269A	Acceso abusivo a un sistema informático.
269B	Obstaculización o interceptación de comunicaciones electrónicas.
269E	Uso indebido de software malicioso (malware).
269I	Violación de medidas de seguridad.
269J	Delitos informáticos financieros: Phishing, clonación de tarjetas y otras modalidades de fraude electrónico.

Nota: Es de anotar que las penas previstas para la vulneración de esta Ley oscilan entre 36 meses a 120 meses con privación de la libertad en establecimiento carcelario.

Ley 1581 de 2012 - Protección de Datos Personales

Conocida como la "Ley de Protección de Datos Personales", esta norma regula el tratamiento de datos personales por parte de personas naturales y jurídicas, tanto públicas

como privadas. Busca garantizar el derecho constitucional a la protección de los datos personales.

Sanciones: La Superintendencia de Industria y Comercio (SIC) es la autoridad encargada de vigilar el cumplimiento de esta ley, con la potestad de imponer multas o sanciones por incumplimiento. (Congreso de Colombia 2012)

En Colombia, la legislación sobre delitos informáticos y protección de datos personales incluye un marco integral que busca tanto sancionar delitos relacionados con la tecnología y la información, como proteger la privacidad de los ciudadanos. Las leyes más importantes, como la Ley 1273 de 2009 (Delitos Informáticos) y la Ley 1581 de 2012 (Protección de Datos Personales), ofrecen mecanismos legales para proteger la confidencialidad, integridad y uso adecuado de la información digital, con la Superintendencia de Industria y Comercio como autoridad principal para garantizar su cumplimiento

4.1.2 Metodología Del Pentesting: Etapas Fundamentales

El pentesting, o pruebas de penetración, es un proceso estructurado que busca identificar y explotar vulnerabilidades en sistemas o redes de una organización, con el fin de evaluar su seguridad. Se sigue un conjunto de etapas claramente definidas para garantizar un enfoque sistemático. (Skoudis 2016). A continuación, se describen las etapas del pentesting y se menciona una herramienta para cada fase:

Tabla 2

Etapas del Pentesting

Etapas	Herramienta
Reconocimiento: recopilar información sobre el objetivo sin interactuar directamente con el sistema o red	Maltego permite realizar un reconocimiento pasivo al mapear relaciones entre personas, dominios, direcciones IP, entre otros, lo que facilita la identificación de activos y posibles puntos de entrada
Escaneo interactúa más directamente con el sistema para identificar puertos abiertos,	Nmap es una herramienta popular para realizar escaneos de red y servicios

servicios en ejecución y versiones del software utilizado	
Enumeración el atacante trata de profundizar en los detalles de los sistemas descubiertos información especifica	Netcat es una herramienta útil para interactuar con puertos abiertos y enumerar servicios manualmente
Explotación aprovechar las vulnerabilidades descubiertas en las fases anteriores	Metasploit es una plataforma de pruebas de penetración que permite ejecutar exploits en sistemas vulnerables
Mantenimiento del Acceso obtener más privilegios o extraer información de manera continua	Empire es una herramienta que proporciona un framework para ejecutar agentes en el sistema comprometido
Escalada de Privilegios obtener mayores permisos dentro del sistema comprometido	Linux Exploit Suggester analiza un sistema Linux para determinar posibles vulnerabilidades locales
Cobertura de Rastros eliminar o modificar registros y rastros de sus acciones para evitar ser detectado	ClearLogs es una herramienta utilizada para eliminar entradas de registro en sistemas Windows, lo que ayuda a ocultar la presencia del atacante
Generación de Reportes creación de un informe que documente todas las actividades realizadas durante la prueba de penetración	Dradis es una herramienta colaborativa que permite organizar y documentar la información obtenida durante un Pentesting

Nota: Elegir las Herramientas Adecuadas para Cada Etapa del Pentesting

4.1.3 Herramientas de Ciberseguridad

Metasploit: Esta herramienta permite identificar vulnerabilidades de seguridad y generar información clave para evaluar posibles puntos de acceso. Se trata de un proyecto de código abierto diseñado para desarrollar y ejecutar exploits dirigidos contra máquinas remotas.(Frias 2021)

Nmap: Este programa, de código abierto, está diseñado para realizar el rastreo de puertos, lo que permite evaluar la seguridad de los sistemas informáticos. Además, puede identificar servidores y servicios activos en redes, facilitando el análisis y la detección de posibles vulnerabilidades. (P. Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2013)

OpenVAS: A diferencia de las dos herramientas mencionadas anteriormente, esta actúa como una suite de software que integra múltiples servicios y herramientas

especializadas en la detección de brechas de seguridad en sistemas informáticos. Además, se trata de un producto de software libre, lo que facilita su acceso y personalización (NVT, Network Vulnerability Tests).

ExploitDB: Es un recurso diseñado para identificar diversas vulnerabilidades en redes, permitiendo mantenerse actualizado sobre los posibles ataques que podrían ocurrir en otros entornos. ExploitDB facilita el acceso a un conocimiento más profundo sobre los métodos utilizados por los ciberdelincuentes, lo que contribuye a fortalecer la seguridad de nuestros sistemas. (Exploit Database 2023)

CVE (Common Vulnerabilities and Exposures): Referencia ampliamente utilizado en ciberseguridad que proporciona identificadores únicos para vulnerabilidades conocidas en software y hardware. Su meta es proporcionar el cambio de información sobre vulnerabilidades y exposiciones, permitiendo a los investigadores, desarrolladores y profesionales de la seguridad acceder a datos consistentes y estandarizados. (CVE - Common Vulnerabilities and Exposures 2023)

4.2 Etapa 2 – Actuación Ética y Legal

4.2.1 Procesos Ilegales o no Éticos de los anexos

Los documentos proporcionados subrayan la importancia de una lectura detallada y comprensiva de los contratos, cláusulas o acuerdos que se firman con organizaciones, empresas e incluso individuos en el ámbito cotidiano. Una vez revisadas a fondo las cláusulas de los anexos, se evidencian diversas irregularidades que apuntan a prácticas ilegales y no éticas dentro de las operaciones de CyberFort Technologies.

En primer lugar, en el escenario 2, se señala una omisión en las medidas de seguridad en el proceso de contratación de personal. El contrato que se va a firmar fue redactado por un

abogado que ya no trabaja en la empresa, quien fue despedido tras ser señalado por involucrarse en procesos ilícitos. Además, no hubo un segundo filtro de revisión que permitiera validar el contrato ni aplicar los cambios necesarios en función de la evaluación de la empresa, sus procesos y la información pertinente.

Por otro lado, las cláusulas del acuerdo contienen información completamente fuera de los parámetros éticos y legales, destacándose algunos fragmentos ilegales y moralmente cuestionables, como los siguientes:

- Se proporciona información obtenida de actividades internas para los procesos de selección, entregando datos sensibles a personal ajeno a la empresa.
- La cláusula establece que la información confidencial sobre procesos ilegales dentro de CyberFort Technologies no podrá ser divulgada.
- Se considera como "datos privados" los relacionados con "chuzadas", interceptación de información y accesos indebidos a sistemas informáticos.
- Se prohíbe denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro acto relacionado con la apropiación de información de terceros.
- Los empleados deben abstenerse de denunciar o divulgar cualquier información confidencial o ilegal que conozcan, reciban o intercambien durante las reuniones, bajo la premisa de que podrían estar compartiendo información privada.
- En caso de que la información se encuentre en poder de un trabajador durante un allanamiento, él será el responsable ante las autoridades competentes, incluso si dicha información fue suministrada por la empresa en el marco de su labor.

- La parte receptora se compromete a no divulgar, comunicar ni revelar total o parcialmente la información confidencial o ilegal sin el previo consentimiento por escrito de CyberFort Technologies. Aunque la cláusula en general es adecuada, se refiere a la prohibición de divulgar o denunciar información obtenida de manera ilegal o que sea ilegal en sí misma.
- Si la información ilegal o confidencial es encontrada en manos del receptor, este deberá consultar a un abogado privado y eximir de cualquier responsabilidad legal o penal a CyberFort Technologies.

4.2.2 Incumplimientos al Acuerdo 1273 de 2009

Protección de la Información y los Datos Personales

En 2009, Colombia promulgó la Ley 1273 con el objetivo de proteger la información y los datos personales, estableciendo un marco legal para los delitos informáticos. Esta ley se divide en dos grandes bloques:

- Atentados contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Atentados informáticos y otras infracciones.

Cada una de estas secciones establece penas legales que varían entre 36 y 120 meses de prisión, además de multas que van de 100 a 1.000 salarios mínimos mensuales legales vigentes.

A continuación, se presentan algunos de los posibles delitos que podrían involucrar a la empresa CyberFort Technologies:

- Incumplimiento del artículo 269A: Debido a las cláusulas que prohíben divulgar información obtenida a través de accesos abusivos a sistemas informáticos.
- Incumplimiento del artículo 269C: Relacionado con actividades de interceptación de información y accesos no autorizados a sistemas informáticos.
- Incumplimiento del artículo 269J: En relación con la obligación de los empleados de no divulgar o publicar información proveniente del intercambio de datos privados.
- Incumplimiento del artículo 269F: Por el acceso no autorizado a datos privados mediante interceptaciones o cualquier otro método ilegal utilizado por CyberFort Technologies para obtener información.
- Incumplimiento del artículo 269H: Por el uso de un tercero de buena fe como instrumento para llevar a cabo actividades ilícitas.

4.3 Herramientas y Software para el desarrollo de la actividad

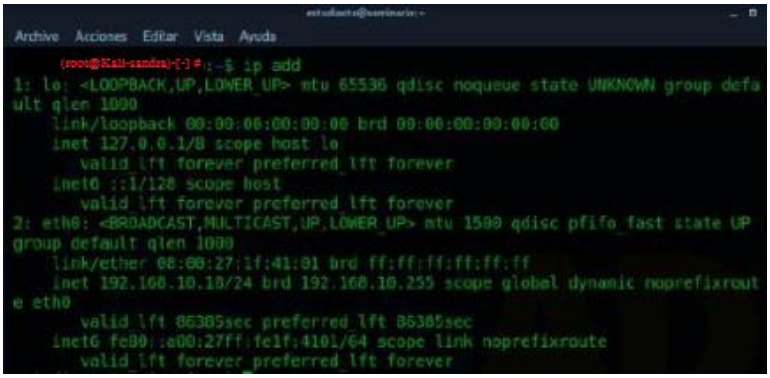
4.3.1 Herramientas utilizadas y comandos

Considerando la actividad a realizar como parte del equipo de Red Team, se emplearon las siguientes herramientas para ejecutar las pruebas:

Kali Linux: Esta herramienta facilitó la identificación de la dirección IP de la red conectada. Para ello, se utilizó el comando ***ip add***, como se muestra en la figura 1,

Figura 1

Comando para identificar la IP

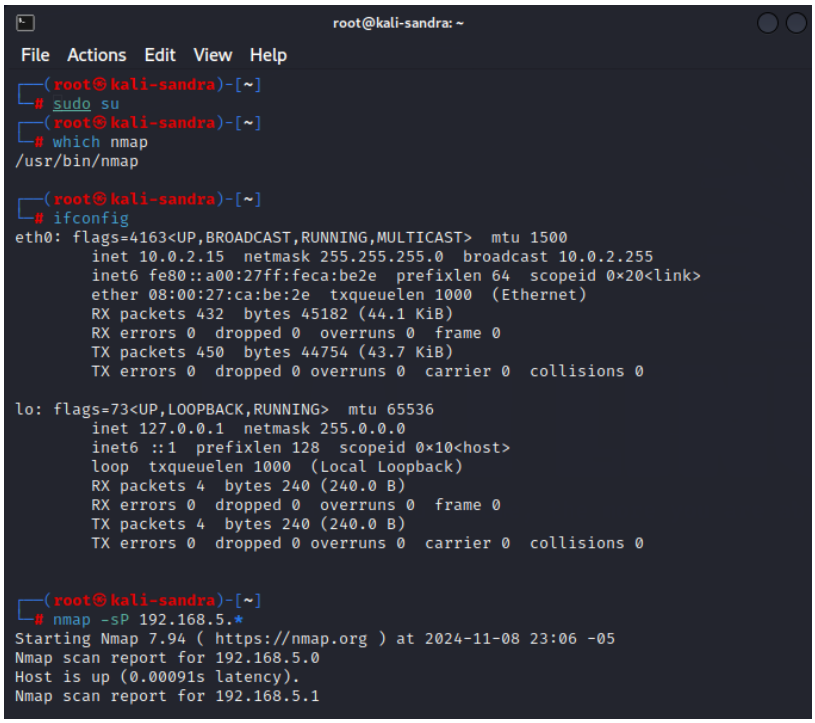


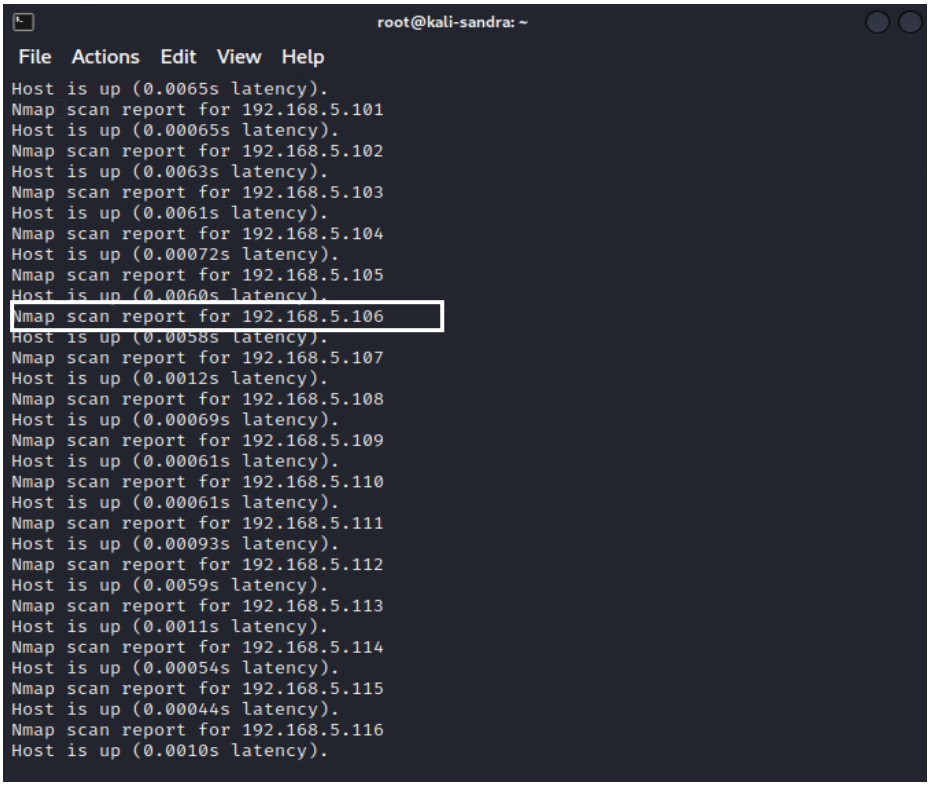
Fuente propia

Nmap: Es una herramienta que permite realizar un rastreo de puertos, así como detectar equipos, servicios y sistemas operativos. En este caso, Nmap está preinstalado en Kali Linux y se utilizará, como se mencionó anteriormente, para realizar un escaneo de los puertos de red mediante el siguiente comando: ***sudo su,*** con el fin de establecer todos los privilegios; luego se digita el comando ***which nmap,*** posteriormente el comando ***ifconfig*** para observar la IP: luego usando las ventajas de nmap usamos el comando ***namp -sP 192.168.5.****.*; como se observa en la Figura 2,

Figura 2

Comando para observar IP



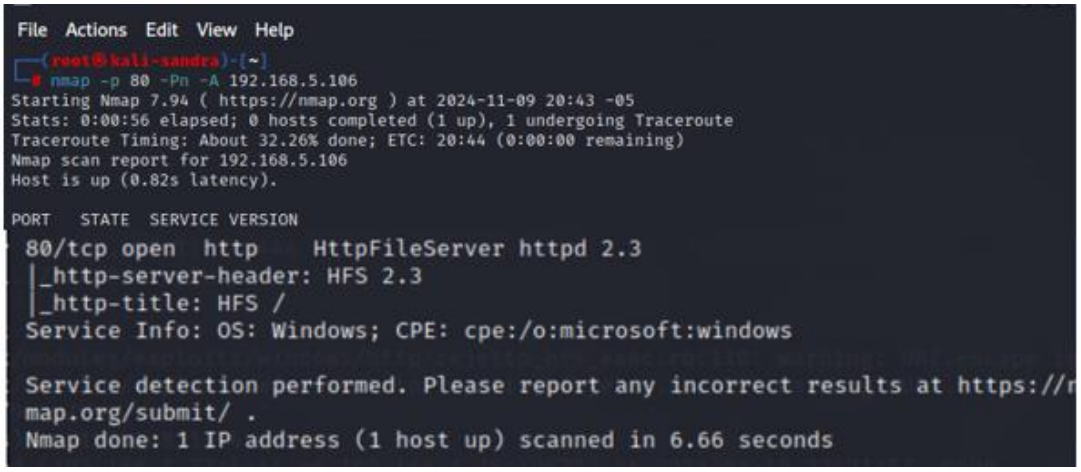


Fuente propia

Se sabe que la empresa emplea Rejetto en su versión 2.3b, la cual presenta una vulnerabilidad importante. Esta aplicación funciona de manera predeterminada en el puerto 80. En esta etapa, se utilizará Nmap para verificar si el puerto está abierto o si está filtrado por algún firewall, Figura 3,

Figura 3

Escaneo de puertos en la máquina vulnerable



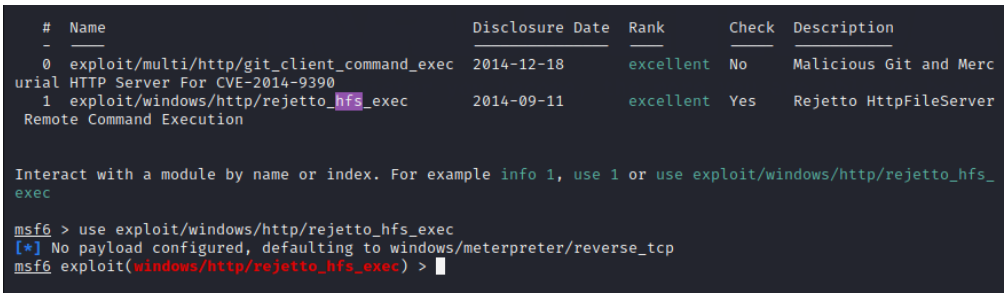
Fuente propia

Al ejecutar Nmap con el parámetro *nmap -p 80 -Pn -A 192.168.5.105-106* para filtrar por la aplicación vulnerable conocida, se observa que el puerto 80 está abierto y que la aplicación HFS 2.3 está en funcionamiento en el momento del escaneo. Esta información es crucial para poder explotar la vulnerabilidad.

Metasploit Framework: Esta herramienta es fundamental para obtener información sobre las vulnerabilidades de seguridad, convirtiéndola en un aliado clave durante las pruebas de penetración (Pentesting). Permite desarrollar y ejecutar exploits contra una máquina remota. Una vez abierta la herramienta, se utiliza el comando **use exploit/Windows/http/rejetto_hfs_exec** para seleccionar el exploit correspondiente, ver Figura 4,

Figura 4

Carga del exploit

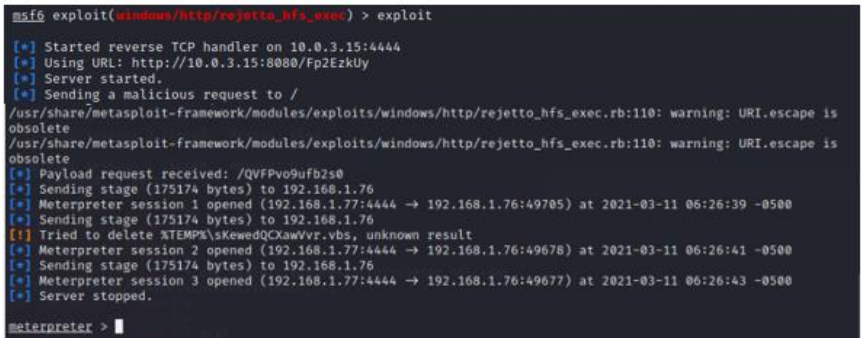


Fuente propia

Una vez configurados todos los parámetros del exploit, procedemos a ejecutarlo mediante el comando *exploit*, que establece una conexión con el equipo objetivo y abre una sesión de Meterpreter. Esto nos permite interactuar con la máquina objetivo a través de una línea de comandos, Figura 5

Figura 5

Iniciando la ejecución del Exploit



Fuente propia

4.3.2 Que permitió identificar el Fallo de Seguridad

Con base en la información obtenida en el Anexo 4, se pudo determinar que es posible obtener una Shell reversa y una sesión Meterpreter. Además, se logró identificar información relevante, como el nombre de la aplicación 'Rejjeto' y el tipo de sistema operativo de la máquina.

Es importante destacar que, debido al desconocimiento inicial del concepto de Meterpreter, se llevó a cabo una investigación para comprender mejor las características de esta herramienta. Se identificó que Meterpreter permite el control remoto de computadoras infectadas. Este programa malicioso, de tipo troyano, se ejecuta completamente en memoria.

4.3.3 Herramientas utilizadas para Identificar las Fallas de Seguridad

De acuerdo con los parámetros establecidos para la actividad y la información proporcionada en los anexos, se utilizaron los siguientes sistemas, herramientas y métodos alternativos para identificar las fallas de seguridad en la máquina con Windows 7:

- Kali Linux
- Nmap
- Metasploit Framework

- Google, para la consulta de información adicional

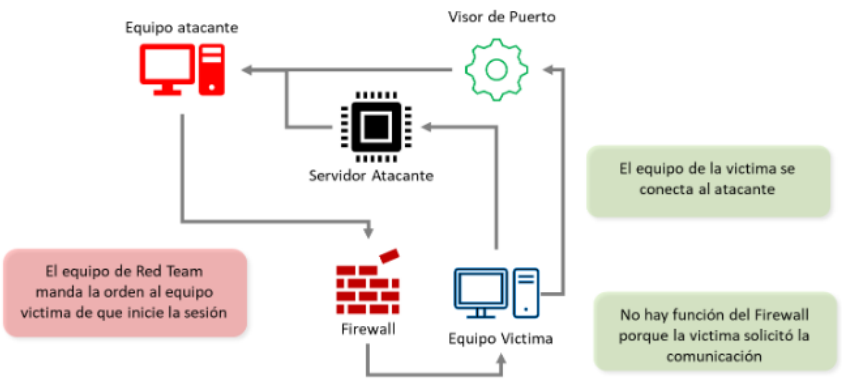
Utilizando las herramientas mencionadas, especialmente Nmap y sus comandos, se determinó que el puerto 80 estaba abierto y accesible, lo que permitió iniciar el ataque.

4.3.4 Como afecta el Ataque a la Máquina

Este tipo de ataque permite al ciberdelincuente crear un usuario administrador en el sistema, otorgándole acceso a información privilegiada. Esto ocurre porque el sistema operativo de la víctima establece una conexión con el equipo atacante, lo que facilita la activación de una Shell para ejecutar comandos de forma remota, figura 6,

Figura 6

Diagrama del ataque



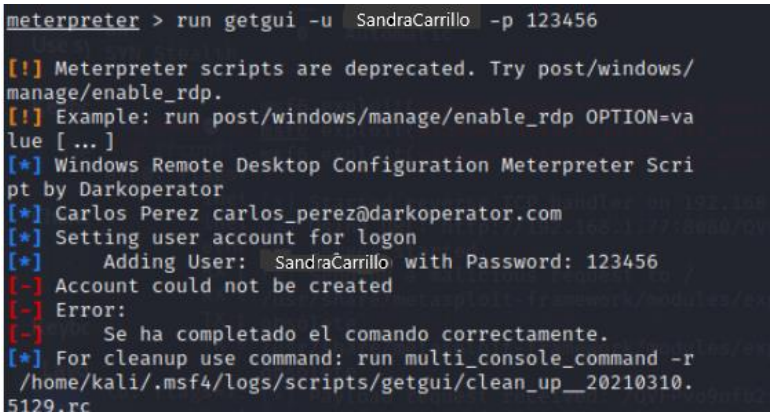
Fuente propia

4.3.5 Evidencias de Explotación de las Vulnerabilidades

Ahora contamos con acceso completo. Para verificarlo, crearemos un usuario con privilegios de administrador en Windows 7, lo que evidenciará el control total sobre la máquina. Para ello, utilizaremos el comando *run getgui*.

Figura 7

Usuario con privilegios de administrador



Fuente propia

A continuación, otorgaremos permisos de administrador al usuario. Para esto, utilizaremos el comando *use incognito*, que permite crear usuarios en Windows y asignarlos a grupos específicos. (Nmap s.f.)

Procedemos a cargar la aplicación Incognito.

Figura 8

Carga de la aplicación Incognito para asociar grupos de usuarios

Fuente propia

Usando el comando *list_tokens -g*, es posible visualizar la lista de tokens del sistema, los cuales funcionan como grupos. Dentro de estos tokens, se puede identificar el de administrador.

Figura 9

Comprobación de los roles disponibles

```
meterpreter > list_tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
\
\INICIO DE SESIÓN EN LA CONSOLA
\Todos
BUILTIN\Administradores
BUILTIN\Usuarios
NT AUTHORITY\Autenticación NTLM
NT AUTHORITY\Esta compañía
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\SERVICIO
NT AUTHORITY\Usuarios autentificados
NT SERVICE\AudioEndpointBuilder
NT SERVICE\CscService
NT SERVICE\IKEEXT
NT SERVICE\iphlpsvc
NT SERVICE\LanmanServer
NT SERVICE\MMCSS
NT SERVICE\Netman
NT SERVICE\PcaSvc
```

Fuente propia

Usaremos el comando *add_localgroup_user* para agregar al usuario SandraCarrillo al conjunto de administradores.

Figura 10

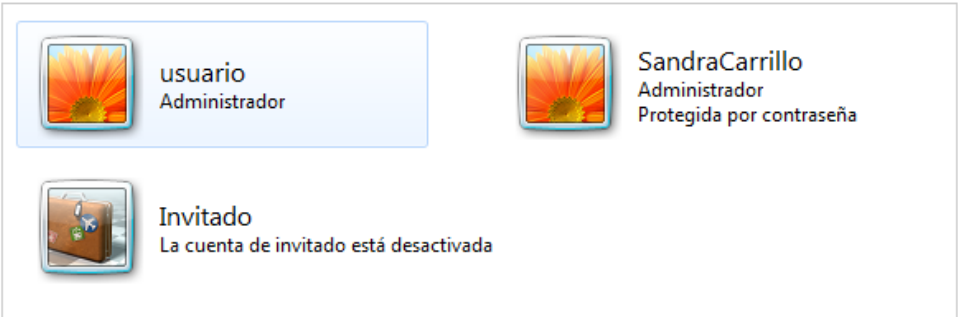
Agregando el usuario al grupo de administradores

```
meterpreter > add_localgroup_user "Administradores" "SandraCarrillo"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user JohnSalcedo to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

Fuente propia

Al acceder ahora a la máquina con Windows, podemos ver que el usuario tiene privilegios de administrador del sistema.

Figura 11 Evidencia del usuario creado con privilegios de administrador



Fuente propia

4.4 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

No obstante, la detección de ataques en tiempo real es extremadamente difícil, ya que la mayoría se identifican solo después de haber comprometido parte o toda la información, la primera acción a tomar, si se detecta un ataque, es cortar la conexión a la red. Esto es esencial, ya que estos ataques generalmente se ejecutan a través de esta vía. Una vez mitigado el riesgo al desconectar la red, es fundamental identificar el tipo de ataque y su objetivo, ya que esta información será crucial para mitigar los riesgos y cerrar posibles brechas de seguridad. Las acciones a seguir dependerán del objetivo, el método y el medio utilizados en el ataque.

En el caso desarrollado en la fase anterior, se propone que, en primer lugar, se identifique la brecha de seguridad. Para ello, se deben analizar los puertos para verificar si alguno permanece abierto en el servidor. Existen diversas metodologías y herramientas para realizar esta tarea, pero personalmente recomendaría usar NMAP, ya que permite rastrear los puertos por donde el ataque pudo haber accedido al sistema. Si se detectan puertos abiertos, lo primero es cerrar esos puertos y actualizar los sistemas afectados. Además, es crucial identificar cualquier usuario no autorizado que haya sido creado, especialmente aquellos administrados por los atacantes. Estos usuarios deben ser eliminados inmediatamente.

4.4.1 Medidas de Hardenización propuestas para evitar futuros ataques

Indispensable formarse de las faltas cometidas, lo cual implica cerrar las brechas de seguridad identificadas durante el ataque. Después de esto, se deben implementar las siguientes acciones:

- Actualizar o adquirir antivirus que permitan escanear los sistemas en tiempo real y generar alertas sobre posibles amenazas.
- Establecer políticas de instalación de software en los equipos de la empresa o en aquellos que se conectan a la red corporativa. Además, se debe proceder a desinstalar programas no utilizados o potencialmente peligrosos.
- Actualizar los equipos y sistemas operativos de la empresa para asegurar que se utilicen las versiones más recientes y seguras.
- Permitir el acceso remoto únicamente a través de VPN, y bajo autorización previa del departamento de TI.
- Instalar firewalls de Windows si no están presentes en los equipos.
- Restringir el uso de cuentas con privilegios de administrador a personal exclusivo del área de informática.
- Realizar pruebas de vulnerabilidad de manera periódica para identificar posibles riesgos y fortalecer la seguridad.

4.4.2 Diferencia entre Blue Team y un equipo de Respuesta a Incidentes Informáticos

En ocasiones puede resultar difícil distinguir las funciones de un equipo de Red Team y un Equipo de Respuesta a Incidentes Informáticos, a continuación, se destacan algunas de las principales características de cada uno.

Los Equipos de Respuesta a Incidentes Informáticos (también conocidos como CSIRT, por sus siglas en inglés) son responsables de recibir, analizar y responder ante incidentes de seguridad. Estos pueden ser reportados a través de diversas plataformas de colaboración, como otros CSIRT, empresas o usuarios. La labor de los CSIRT es

principalmente reactiva, ya que actúan únicamente después de que un incidente se ha producido, lo que los hace más enfocados en la resolución que en la prevención.

En cambio, el Blue Team adopta un enfoque más preventivo. Su función principal es desarrollar y aplicar medidas de seguridad, así como crear herramientas para prevenir ataques y mitigar los riesgos de vulnerabilidades, reduciendo al mínimo las posibilidades de que se abran brechas de seguridad.

5 Aspectos que aporten al desarrollo de estrategias de Red Team y Blue Team

Dado que se trata de equipos de trabajo, en los cuales intervienen varios individuos en el desarrollo de funciones, es fundamental establecer reglas claras, especialmente en el caso del equipo azul, encargado de la defensa de los sistemas. El equipo rojo, por otro lado, no debería tener reglas ni parámetros en sus ataques, ya que su objetivo es emular las tácticas de los delincuentes, quienes usualmente no siguen principios éticos en sus operaciones.

La documentación de los procesos es una etapa crucial que no debe pasarse por alto. Es esencial conservar un registro detallado de los procedimientos utilizados en cada tarea. Se recomienda que esta información describa paso a paso el proceso, para que pueda ser estudiada por personal nuevo o actualizada con el tiempo. Esto es especialmente relevante en pruebas realizadas en la red de la organización, donde no siempre existen entornos de prueba.

El mayor aporte que pueden ofrecer los equipos de Red Team y Blue Team a la organización es el conocimiento. Por lo tanto, ambos deben mantenerse en un proceso constante de aprendizaje, buscando nuevas maneras de proteger los sistemas y de identificar posibles vulnerabilidades. No basta con los conocimientos adquiridos en el pasado, ya que la tecnología y las tácticas de los ciberdelincuentes avanzan a un ritmo acelerado.

Conclusiones

Toda organización que desee proteger sus sistemas de información y operaciones debe contar con un experto en seguridad informática, ya que el conocimiento técnico y legal es fundamental en las estrategias de prevención que deben implementarse.

En el marco de las diversas medidas de seguridad, existen herramientas que facilitan la realización de pruebas preventivas y de penetración, las cuales deben aplicarse de manera periódica. Estas pruebas son esenciales para identificar vulnerabilidades y aplicar controles correctivos de forma oportuna.

Es crucial destacar que el incumplimiento de cualquier artículo de la Ley 1273 conlleva sanciones legales y reputacionales, lo que puede afectar gravemente los principios profesionales del responsable.

Los equipos de Red Team y Blue Team son fundamentales para fortalecer la seguridad en las organizaciones. Estos equipos, compuestos por profesionales especializados en defensa y ataque de sistemas operativos, redes y recursos empresariales, simulan ataques reales para evaluar la capacidad de respuesta de la empresa ante amenazas digitales, permitiendo así medir el nivel de protección y contención existente.

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

Según lo mencionado previamente, lo fundamental de las estrategias de mejora es aprender tanto de los errores propios como de los ajenos. Para ello, es esencial mantenerse actualizado sobre las operaciones realizadas en distintas organizaciones, analizando cómo se ejecutaron, cómo se controlaron y cómo se mitigaron los posibles riesgos.

En este sentido, las empresas deben comprender la importancia de actualizar sus equipos, adquirir antivirus, establecer políticas de seguridad, gestionar los accesos y controlar a los usuarios, entre otras acciones. Cuando se implementan de manera conjunta, estas medidas refuerzan significativamente la seguridad organizacional.

Además, no se puede subestimar el factor humano, ya que sigue siendo una de las principales brechas de seguridad, especialmente en lo que respecta al acceso no autorizado a sistemas e información. La capacitación continua y la sensibilización sobre las normas de seguridad y sus posibles consecuencias deben ser consideradas una obligación.

Finalmente, es crucial que las empresas sean sometidas a un monitoreo constante, asegurando el cumplimiento de las políticas de seguridad informática y de la información. También deben realizarse auditorías periódicas en las diferentes áreas y aplicar controles efectivos frente a las inconformidades detectadas.

Anexos

Sustentación – Link video

SUSTENTACION_INFORME

Bibliografía

Congreso de Colombia. *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crean nuevos tipos penales relacionados con los delitos informáticos.* 2009. https://www.suin-juriscol.gov.co (último acceso: 10 de 12 de 2024).

—. *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.* 2012. https://www.sic.gov.co (último acceso: 10 de 10 de 2024).

—. *Ley 1712 de 2014, por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.* 2014. https://www.suin-juriscol.gov.co (último acceso: 11 de 10 de 2024).

—. *Ley 1928 de 2018, por medio de la cual se aprueba el Convenio sobre Ciberdelito del Consejo de Europa.* 2018. https://www.suin-juriscol.gov.co (último acceso: 11 de 10 de 2024).

CVE - Common Vulnerabilities and Exposures. *CVE Official Website.* 2023. https://cve.mitre.org (último acceso: 9 de 10 de 2024).

Engebretson, P. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress, 2013.

—. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress, 2013.

Engebretson, P. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress, 2013.

Exploit Database. *Exploit Database - Search the database.* 2023. https://www.exploit-db.com (último acceso: 10 de 10 de 2024).

Frias, M. *Fundamentos de Metasploit Framework | OpenWebinars. OpenWebinars.net.* 18 de 10 de 2021. https://openwebinars.net/blog/fundamentos-de-metasploit-framework/#:~:text=Comandos%20b%C3%A1sicos%20Metasploit%20Framework,-

Seguidamente,%20debemos%20tener&text=search:%20Destinado%20a%20buscar%20m%C3%B3dulos,exploits:%20Mostrar%C3%A1%20todos%20los%2 (último acceso: 10 de 10 de 2024).

Kali Linux Documentation. *Kali Tools Documentation.* https://www.kali.org/tools/, 2023.

Mitropoulos, D. *Penetration Testing Tools and Techniques.* Packt Publishing, 2014.

Networks, Greenbone. *OpenVAS Documentation.* 2023. https://www.greenbone.net (último acceso: 10 de 10 de 2024).

Oracle Corporation. *Virtual Box Download.* 2023. https://www.virtualbox.org/wiki/Downloads (último acceso: 20 de 09 de 2023).

Presidencia de la República. *Decreto 090 de 2018, por el cual se establecen disposiciones relacionadas con la seguridad informática y la prevención de delitos informáticos.* 2018. https://www.suin-juriscol.gov.co (último acceso: 11 de 10 de 2024).

—. *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.* 2013. https://www.suin-juriscol.gov.co (último acceso: 11 de 10 de 2024).

SANS Institute. *Penetration Testing: Planning and Scoping.* SANS Whitepaper, 2020.

Skoudis, E., & Liston, T. *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Prentice Hall, 2016.

Unad. *Seminarios Especializados RedTeam & BlueTeam2024.* 2024. https://unadvirtualedu-my.sharepoint.com/personal/luis_zambrano_unad_edu_co/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fluis%5Fzambrano%5Funad%5Fedu%5Fco%2FDocuments%2FLaboratorios%20Controlados%2FSeminario%20Especializado%2FRedTeam%26BlueTeam2024&ga=1 (último acceso: 10 de 2024).