Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Leidi Yojana Brand Ladino

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

A mi esposo, por su paciencia y apoyo incondicional, creer en mí y estar a mi lado brindándome aliento en cada etapa de este proceso formativo, a mi hija por su amor y respaldo incondicional, mi motivación constante en mi formación profesional y personal, a mis compañeros de trabajo por su apoyo, comprensión y colaboración académica por últimos a los docentes por compartir sus conocimientos y hacer de mi una profesional integra, con deseo de superación.

Resumen

Este documento está enfocado en el desarrollo de casos prácticos en la seguridad de la información de la empresa SecureNova Labs, organizado en diferentes etapas desde los aspectos éticos, legales y técnicos de los equipos de seguridad, pruebas de intrusión y prácticas en tiempo real, utilizando técnicas y herramientas de ataque ofensivo, brindado un informe con estrategias sólidas para reducir riesgos y vulnerabilidades y fortalecer la seguridad de los sistemas de información.

***Palabras clave*:** Ataque, ciberseguridad, herramientas, normatividad, vulnerabilidad.

Abstract

This document focuses on the development of practical cases in information security at SecureNova Labs, organized in different stages from the ethical, legal and technical aspects of security teams, penetration tests and real-time practices, using offensive attack techniques and tools, providing a report with solid strategies to reduce risks and vulnerabilities and strengthen the security of information systems.

Keywords: Attack, cybersecurity, tools, regulations, vulnerability.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo responsable de la defensa cibernética de una organización, encargado de detectar y mitigar ataques, intrusiones o incidentes de seguridad informática.

Ciberseguridad:

Métodos, Herramientas y acciones que se usan para proteger sistemas informáticos, redes y datos contra acceso no autorizados o ciberataques.

Mitigación:

Acción implementada para reducir la probabilidad de un incidente o amenaza dentro de una red, equipo o sistema.

Vulnerabilidad:

Debilidad o fallo en un sistema informático, debido a factores maliciosos para comprometer los datos o integridad del equipo.

Introducción

La Ciberseguridad en la empresa es la parte fundamental para resguardar la confidencialidad, integridad, y disponibilidad de la información, brindando una integridad en la protección de datos informáticos. Este documento presenta un análisis detallado de las habilidades tácticas, técnicas y principios éticos y legales de la seguridad digital.

El pentesting y el análisis de sistemas informáticos se han convertido en herramientas indispensables para detectar amenazas o puntos débiles en los sistemas de información y profundizar en incidentes de seguridad, demostrado mediante una práctica realizada en el presente trabajo, aplicando distintas herramientas de ciberseguridad que permiten identificar vulnerabilidades y actuar de manera efectiva frente a ataques o posibles amenazas detectadas.

A lo largo del informe podemos presentar un análisis de distintas técnicas, legales y operativas que permiten construir un enfoque sólido y completo para mejorar la capacidad de respuesta a incidentes.

Justificación

Las amenazas en el entorno cibernético son una problemática que, en la actualidad, tiene un impacto significativo en la protección de datos informáticos. Este proyecto nace de la importancia que tiene las tácticas y técnicas de respuestas a incidentes para resguardar la información.

En Colombia las leyes de protección de datos y delitos informáticos son crucial para cuidar la privacidad de datos personal y evitar robos de información, fraude y uso individuo de la información. Esta investigación busca aportar una reflexión crítica ante los incidentes informáticos con el fin de enriquecer el conocimiento de las organizaciones y aplicar las diferentes normas en post de evitar futuras vulnerabilidades.

Finalmente, este trabajo propone una visión general de ciberseguridad que busca proteger la información bajo las tácticas, técnicas y ética profesional, consolidada y preparada que respondan de manera eficiente a los riesgos digitales.

Objetivos

Objetivo General

Analizar el impacto de las técnicas y tácticas de respuesta para equipos Red Team y Blue Team con el fin de fortalecer la seguridad de la información en las organizaciones para desempeñar funciones de manera efectiva.

Objetivos Específicos

Realizar un diagnóstico técnico y táctico ante respuestas de incidentes de ciberseguridad en tiempo real, utilizando herramientas gratuitas y metodologías de simulación.

Analizar las leyes de protección de datos personales, delitos informáticos en Colombia.

Proponer recomendaciones y estrategias técnicas para que los profesionales en ciberseguridad estén preparados a dar respuesta oportuna ante algún incidente de ciberseguridad.

Describir las actividades practicas realizadas en el curso, mediante herramientas y técnicas para descubrir vulnerabilidades en tiempo real de los sistemas de información.

Desarrollo del Informe

Estrategia Red Team y Blue Team

La estrategia Red Team permite identificar y corregir debilidades en la seguridad de forma proactiva mediante técnicas como pruebas de penetración, evaluación de vulnerabilidades, ingeniería social y simulación de ataques, dando respuesta a incidente reales. (Bardají, 2025; Cilleruelo,2024; UNIR,2020)

- Analiza sistemas para detectar fallos de seguridad mediante ataque controlados para buscar vulnerabilidades en la infraestructura de seguridad.
- Realiza la tarea de recopilar información como datos de los sistemas de la organización, como sistemas operativos, red, puertos abiertos y controles físicos.
- Simulan un ataque real con la mayor discreción posible para no alerta los sistemas ofensivos con la finalidad de descubrir vulnerabilidades.

La estrategia Blue Team tiene como objetivo es monitorear continuamente los sistemas, realizar análisis de vulnerabilidades, implementar controles de seguridad y dar respuesta a incidentes con el fin de proteger a la organización de posibles ataques y en caso de que ocurra una intrusión dar solución lo más pronto posible. (Check Point, s. f, 2025; UNIR,2020)

- Equipo dedicado a la defensa y protección continua de la infraestructura de TI, anticipándose a posibles riesgos.
- Su función es proteger los sistemas, datos y redes de la organización, monitoreando la red para detectar intrusiones.
- Implementa medidas de seguridad mediante parches y herramientas para prevenir vulnerabilidades, accesos no autorizados y ataques cibernéticos.
- Se enfoca en endurecer sistemas y configurar la infraestructura de forma segura.

Análisis Técnico

Las tácticas de Red Team y Blue Team están vinculadas con el marco legal colombiano de manera complementaria, pues las dos deben funcionar dentro de los límites impuestos por las regulaciones en materia de seguridad de la información, protección de datos y crímenes informáticos. Esto se logra a través del cumplimiento normativo y la mejora constante para prevenir el acceso abusivo a un sistema informático, la interceptación de datos o los daños informáticos.

Para identificar el marco legal colombiano debemos tener en cuenta los siguientes fundamentos jurídicos:

Ley 1266 de 2008 – Derecho al Habeas Data

Esta ley regula cómo se manejan los datos que están en bases de datos personales, especialmente la información financiera, crediticia, comercial y de servicios, así como la proveniente del exterior.

También establece las normas generales del derecho al hábeas data y define las reglas que deben seguir tanto entidades públicas como privadas cuando tratan datos personales. Se considera un derecho fundamental para los propietarios de los datos tener acceso a su información, modificarla o solicitar su eliminación. (Secretaría Jurídica Distrital, 2008)

Ley 1581 de 2012 – Protección de Datos Personales

Esta ley tiene como propósito establecer lineamientos y principios generales que aseguren la protección de los datos personales y el respeto por los derechos de sus dueños. En Colombia, esta ley estatutaria establece los principios esenciales de la legalidad, finalidad, veracidad y seguridad en el tratamiento de información y sienta las bases para proteger los datos personales. Asimismo, reconoce el derecho al hábeas data, que permite a todo individuo acceder

a sus datos, modificarlos o corregirlos. La Superintendencia de Industria y Comercio (SIC) es la entidad encargada de implementar estas reglas. (Función Pública, 2012)

Ley 1273 de 2009 – Delitos Informáticos

El propósito de esta ley es establecer un nuevo bien jurídico protegido, que consiste en los datos y la información, mediante la modificación del Código Penal. Su meta fundamental es proteger los sistemas que emplean tecnologías de la información y las comunicaciones.

Clasifica como delitos la manipulación o eliminación de información sin autorización previa, la interceptación de datos y el acceso a sistemas informáticos sin autorización. Asimismo, define castigos particulares para estas acciones, fortaleciendo de esta manera la seguridad digital y la privacidad de la información a través de métodos forenses, documentación detallada y continua, control riguroso de accesos y procedimientos, así como la conformidad con normas técnicas y jurídicas, la gestión apropiada de la evidencia digital satisface los principios de cadena de custodia e integridad.

Esto posibilita que la evidencia digital sea válida desde el punto de vista legal, verificable y confiable. (Ley 1273 de 2009) (Función Pública, 2009)

Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Publica

A través de esta, se establece la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, así como se establecen otras leyes. A pesar de que no se enfoca únicamente en la información personal, esta normativa fomenta el derecho de los ciudadanos a obtener información pública y fortalece la transparencia en la administración del sector público. Define procedimientos transparentes para que cualquier individuo pueda pedir y adquirir datos del Estado, lo que favorecerá una mayor responsabilidad y supervisión ciudadana.

Decreto 338 de 2022 – Ciberseguridad – TIC

El objetivo es fortalecer la ciberseguridad en Colombia a través de un marco jurídico que promueva la prevención y reacción frente a incidentes de ciberseguridad.

Definiendo medidas para salvaguardar la información con el propósito de robustecer la gobernanza digital en la nación.

Pentesting o Prueba de Penetración

Se puede entender como un conjunto de métodos que se emplean para analizar el grado de seguridad de una infraestructura tecnológica, un sistema o una red, a través de la simulación controlada de un ataque real.

Mediante las estrategias Blue Team y Red Team, es posible simular un pentesting más exhaustivo, realista y útil. Esto se debe a que representan ataques reales para evaluar la detección y respuesta, el Red Team finge ser un atacante que intenta infiltrarse en el sistema y sostener acceso sin ser detectado, mientras que el Blue Team supervisa, identifica y responde ante los atacantes.

Esta valoración se lleva a cabo en diferentes etapas cada una enfocada en realizar tareas concretas que posibiliten detectar debilidades, corroborar accesos no autorizados y evaluar la robustez de los métodos de protección que se han puesto en marcha en la plataforma evaluada. (Bacudio et al, 2011)

Las siguientes etapas son las más notables:

Planificación: En esta fase se acuerdan los objetivos, se delimita el alcance del ejercicio y se identifican los activos a evaluar.

- Selección de los sistemas y servicios a analizar.
- Obtención de los permisos y acuerdos necesarios para realizar la Prueba.

Reconocimiento: Se busca obtener la mayor cantidad de datos posibles sobre el entorno del objetivo, tanto de Notas abiertas como técnicas.

- Identificación de dominios, rangos IP, puertos abiertos y servicios activos.
- Uso de herramientas como Nmap o Whois para mapear el entorno.

Escaneo: Se examinan los servicios y sistemas detectados para descubrir fallas de seguridad que puedan ser aprovechadas.

- Aplicación de escáneres como Nessus o OpenVAS para detectar puntos débiles.
- Evaluación preliminar del riesgo asociado a cada hallazgo.

Explotación: Se procede a utilizar las vulnerabilidades detectadas con el fin de comprometer los sistemas, de manera controlada.

- Intentos de acceso no autorizado o escalamiento de privilegios.
- Ejecución de exploits con herramientas como Metasploit para verificar impactos.

Post- explotación: Se analiza el alcance real del compromiso y se exploran posibilidades como el movimiento lateral o acceso a información sensible.

- Análisis del entorno comprometido
- Recolección de información critica
- Uso de herramientas como Empire o Wireshark para monitoreo o expansión.

Análisis y Reporte: Se elabora el informe técnico con los hallazgos, impactos potenciales y recomendaciones para mitigar los riesgos.

- Descripción detallada de vulnerabilidades encontradas.
- Propuesta de medidas correctivas.
- Uso de herramientas como Dradis parareporte

Revisión: Tras aplicar las soluciones recomendadas, se realiza una revisión para validar si los riesgos han sido mitigados correctamente

- Ejecución de escaneos posteriores.
- Validación de remediaciones con herramientas como Burp Suite u otras utilidades de análisis de seguridad.

Herramientas y Servicios en Línea

Matasploit

El marco de pruebas de penetración más utilizado del mundo, ayuda a los equipos de seguridad a hacer más que simplemente verificar vulnerabilidades, gestionar evaluaciones de seguridad y mejorar la concienciación en seguridad; empodera y prepara a los defensores para estar siempre un paso (o dos) por delante.

Nmap

Es una herramienta empleada para realizar análisis y auditorías de redes, facilitando la detección de dispositivos activos (hosts), servicios disponibles y puertos abiertos.

Además, permite identificar los sistemas operativos presentes en los equipos conectados, esta herramienta resulta especialmente valiosa durante la etapa de reconocimiento en una prueba de penetración, ya que permite mapear los dispositivos conectados y obtener información detallada sobre la infraestructura de red. (INCIBE, 2023)

OpenVAs (Open Vulnerability Assessment System).

Son herramientas diseñadas para evaluar el estado de seguridad de un sistema, mediante la detección de vulnerabilidades previamente documentadas y posibles fallos en la configuración que puedan representar un riesgo.

Esta herramienta se emplea durante la fase de escaneo en una prueba de penetración, con el propósito de identificar vulnerabilidades presentes en los sistemas evaluados. (INCIBE, 2024)

Exploit

Se trata de una base de datos en línea que centraliza información sobre exploits, pruebas de concepto y vulnerabilidades conocidas.

Representa un recurso esencial para investigadores y profesionales en ciberseguridad, ya que facilita la búsqueda y descarga de exploits específicos según la plataforma o el software objetivo.

CVE (Common Vulnerabilities and Exposures).

Se trata de un sistema estandarizado que permite identificar y catalogar de manera única las vulnerabilidades y exposiciones relacionadas con la seguridad en aplicaciones y sistemas.

Cada registro en la base de datos CVE contiene una descripción detallada de la vulnerabilidad, así como datos relevantes sobre su impacto y posibles métodos de mitigación.

Los especialistas en pruebas de penetración pueden recurrir a ExploitDB como Nota para identificar exploits que se ajusten a las vulnerabilidades detectadas en un sistema. Esto les permite diseñar pruebas más precisas y alineadas con escenarios reales de ataque.

Banco de Trabajo

Análisis e instalación de Banco de trabajo bajo los siguientes pasos.

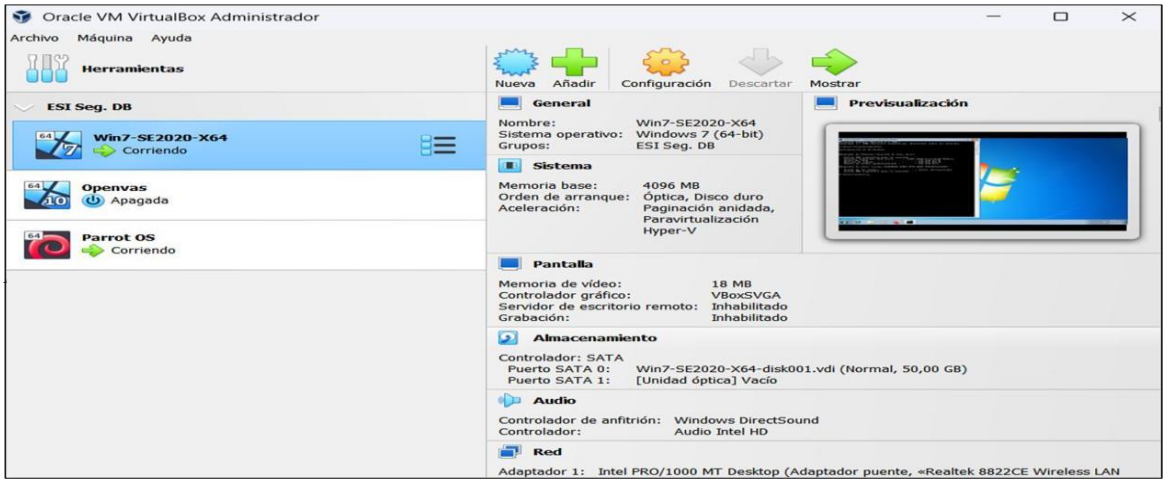
Figura 1

Descarga de Maquina VirtualBox

Nota. Se descarga la herramienta con la cual se va a desarrollar el laboratorio maquina VirtualBox.

Figura 2

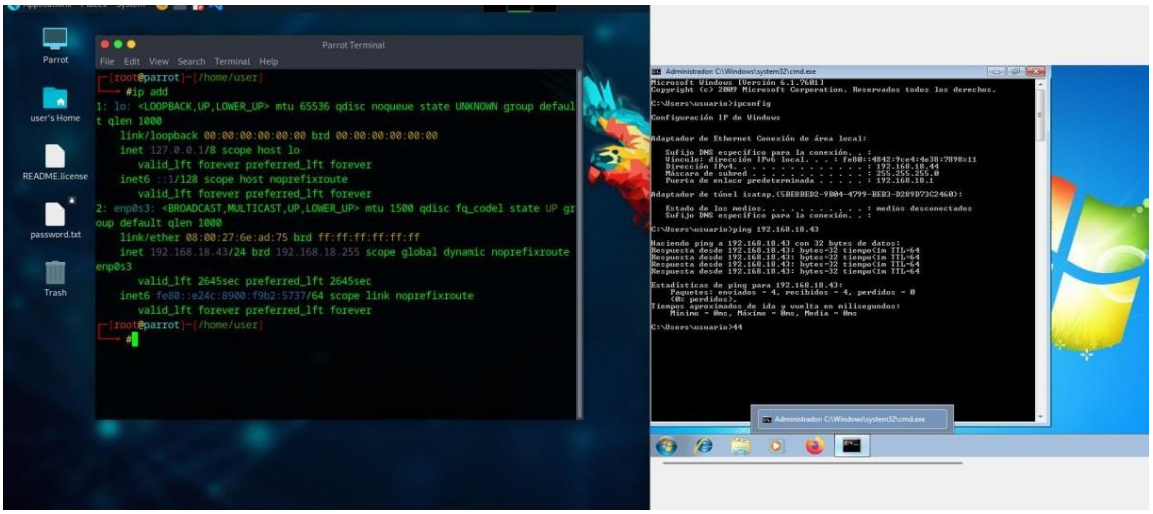
Instalación de Maquina Parrot y Windows 7



Nota. Se instalan las máquinas virtuales para continuar con el laboratorio

Figura 3

Comunicación Entre las Maquinas



Nota. Se evidencia comunicación entre las maquinas mediante un ping

Anexo 2 – Escenario Dos y Tres

Desde mi punto de vista evidencio algunos aspectos que no encajan desde el punto de vista legal ni ético, la alta gerencia no revisó los contratos antes de entregarlos al nuevo personal aspirante a laborar en la empresa, los contratos fueron elaborados por un abogado que ya no está laborando en la empresa, porque al parecer estuvo comprometido con algunas irregularidades en la organización.

Los documentos sin previa revisión es una falta de atención por parte de los responsables de contratación, esto es preocupante, porque un contrato mal hecho puede incluir cláusulas injustas o incluso ilegales y al final eso termina afectando tanto a los trabajadores como a la empresa.

Lo primero que hay que hacer es revisar muy bien la documentación contractual de la empresa, no solo lo que dejó ese abogado, sino también los que se use de ahora en adelante, lo ideal sería asegurarse de que todo esté claro los derechos y obligaciones de los empleados, las condiciones de trabajo y las funciones.

El documento indica "***La gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal"***, y evidentemente no están revisando esos documentos como deberían. Si no se chequean bien o no cumplen con las normativas, podrían poner en riesgo la seguridad de la información de la empresa y la privacidad de los empleados.

Vulneración Ley 1273 de 2009

Es la ley que actualiza el código penal de delitos informáticos, se enfoca en temas como la protección de datos e información.

Su propósito se centra en tres aspectos fundamentales: salvaguardar la información y los sistemas frente a ataques o delitos informáticos, imponer sanciones a quienes cometan actos como el acceso no autorizado a sistemas, el robo de datos o la distribución de software malicioso, y regular la ciberseguridad y la protección de datos personales en Colombia.

Además, existen varios aspectos relevantes a considerar:

Artículo 269A - Acceso Abusivo a un Sistema Informático

El documento especifica que la parte que recibe la información no debe denunciar actividades como espionaje o cualquier intento de quedarse con datos de terceros, esta cláusula del acuerdo podría estar yendo en contra de la ley, porque básicamente está restringiendo la obligación de reportar accesos no autorizados o usos indebidos de sistemas informáticos.

Artículo 269B - Obstaculización Ilegítima de Sistema Informático

El documento limita la posibilidad de responder o defenderse ante interferencias o ciberataques, básicamente está dejando a la empresa con las manos atadas. Esto no solo dificultaría protegerse, sino que podría debilitar su capacidad de reaccionar rápido y mantener sus sistemas a salvo.

Artículo 269C - Prohíbe la Interceptación de Datos Informáticos Sin Orden Judicial.

El acuerdo tiene algunos términos que podrían dar a entender que no hay obligación de denunciar prácticas como la interceptación de información, esto es un problema, porque va en contra del artículo que prohíbe y castiga la interceptación no autorizada de datos. Si el acuerdo limita la intervención de las autoridades, está facilitando directamente que se viole la ley.

Artículo 269D - Daño Informático

El acuerdo prohíbe a la parte receptora denunciar actividades sospechosas o de espionaje y eso puede ocasionar graves problemas, por que donde se descubre un daño o una alteración en

la información de los sistemas informáticos, se debe reportar de lo contrario estaremos incumpliendo con la Ley.

Artículo 269F – Penado por la Violación de Datos Personales.

En el acuerdo se limita la posibilidad de denunciar incidentes relacionados con la violación de datos personales. porque al limitar el reporte se facilita que alguien haga un mal uso de esa información si no se puede reaccionar rápido ante accesos no autorizados o usos indebidos.

Propuesta Laboral

Como profesional en ciberseguridad estudiaría detenidamente la oferta, restringiéndome a los términos del acuerdo de confidencialidad que se debe firmar y al código ético profesional; tras un análisis exhaustivo y con mi ética profesional como guía, no aceptaría la oferta, ya que el Anexo 3 limita la oportunidad de reportar acciones sospechosas o incluso ilegales, lo cual contradice mis principios y lo que yo defino como buenas prácticas en ciberseguridad.

La transparencia y la confidencialidad, para mí, son los fundamentos que me distinguen como responsable de la seguridad informática. Si detecto procesos o actividades ilegales en el interior de la compañía, no tengo intención de poner en peligro su integridad ni la de los clientes no puedo denunciarlos porque podría tener problemas legales. Esto también puede perjudicar el cumplimiento de las leyes de seguridad de la información, particularmente en lo que respecta a los delitos informáticos. Me gusta trabajar en un sitio donde tenga la posibilidad de realizar mi trabajo con ética, resguardar los datos y no tener que angustiarme por encubrir acciones que contradicen mi ética profesional o lo legal.

Caso problema "Ciberespionaje y Ética en SecureNova Labs."

El caso problema, en particular debido a sus consecuencias para el gobierno y la confianza que tenemos en las empresas que gestionan datos sensibles, se enfrenta a un dilema serio relacionado con las compañías de ciberseguridad. Nos cuestionamos: ¿Qué sucede cuando una empresa, que debería proteger información crítica y sensible con máxima responsabilidad, admite que esta información ha sido filtrada?

La compañía emplea de forma inapropiada su acceso para recopilar y comercializar información confidencial sin autorización. Esto no solo infringe la ética profesional y la confianza de sus clientes, sino que además socava la reputación de toda la industria y de esta empresa.

Los clientes tienen la expectativa de que las compañías de ciberseguridad respeten su principio de salvaguardar la información confidencial, integra y accesible cuando se necesite acceder a ella, en mi opinión legal, las actividades de algunos trabajadores podrían considerarse como violaciones de privacidad o ciber espionaje, lo que va en contra de las leyes de protección de datos. Asimismo, la venta de información sin autorización podría tener graves consecuencias, como el espionaje corporativo o el uso indebido de datos confidenciales. Esto podría poner en problemas no solo a ellos, sino también a la empresa si se inician acciones legales.

Pregunta 1- Limite de Acceso a la Información por Parte de Terceros o Contratistas.

Es necesario determinar el alcance de los accesos requeridos, lo que significa que las empresas de ciberseguridad solo deben acceder a la información necesaria para las auditorías, evitando exceder sus funciones o acceder a datos sin autorización. Por este motivo, es crucial definir con exactitud el alcance, la naturaleza de la información y las restricciones pertinentes a los datos y sistemas informáticos para evitar el uso indebido de accesos no autorizados. También

es importante contar con políticas de seguridad bien definidas y claras que permitan supervisar y documentar las acciones realizadas por los usuarios durante las auditorías. Esto requiere ajustar los permisos de usuario según su rol y responsabilidades en cada puesto, tanto en auditorías internas como externas, asegurando así el cumplimiento de las normativas internas.

Pregunta 2- Mecanismos de Supervisión y Control en las Empresas de Ciberseguridad.

Es crucial tener políticas de control y supervisión que regulen su implementación de acuerdo a los niveles autorizados, como la definición precisa de roles, la realización continua de supervisiones internas y externas, así como el establecimiento de normas que fomenten la ética profesional.

Pregunta 3- Respuestas de los Gobiernos y Organizaciones

Es necesario llevar a cabo auditorías externas y pesquisas internas de carácter legal para establecer la magnitud de eventuales infracciones de seguridad y las obligaciones de los participantes en cada incidente. Asimismo, cooperar con las entidades judiciales, las agencias de inteligencia y los organismos reguladores para definir responsabilidades y establecer precedentes en el caso.

De acuerdo con los resultados adquiridos en el proceso, se determinan sanciones económicas o limitaciones contractuales si es necesario. También se establecen criterios más estrictos para elegir proveedores, considerando su historial ético, su reputación y sus capacidades técnicas.

Ejecución Pruebas de Intrusión

Pasos de un Pentesting

Las estrategias Red Team y Blue Team permiten simular un pentesting más exhaustivo, ya que representan ataques verdaderos. El Red Team se comporta como un atacante que intenta

acceder al sistema y mantener el acceso; busca explotar debilidades y aplica técnicas como el escaneo de puertos o la explotación de fallas.

El Blue Team, por su parte, utiliza herramientas como SIEM, IDS/IPS y firewalls para supervisar, identificar y reaccionar ante el atacante.

Se ha definido un marco de trabajo con los siguientes pasos y procedimientos para que pueda llevarse a cabo de manera efectiva y segura una prueba de Pentesting (Qualysec, 2024).

Interacciones Previas: En esta etapa se crea tanto la planificación como la definición del alcance de la prueba de penetración. Estableciendo los objetivos, las reglas y los límites que va a tener la prueba.

Recopilación de Información: En esta etapa se realiza la recopilación de información sobre el objetivo incluye datos sobre la infraestructura, los sistemas, las aplicaciones y los empleados.

Modelado de Amenazas: En esta etapa se plantean y analizan las posibles amenazas que podrían afectar al objetivo definido. Se evalúan los riesgos y se priorizan las vulnerabilidades.

Análisis de Vulnerabilidades: Dentro de esta etapa se realiza la búsqueda y el análisis de todas las vulnerabilidades en el sistema. Se utilizan herramientas para el escaneo y detección de fallos de seguridad y se organiza la viabilidad de explotación de las vulnerabilidades encontradas.

Explotación: Una vez identificadas las vulnerabilidades, se realiza la explotación para comprobar si realmente pueden ser utilizadas para comprometer el sistema y comprobar su nivel de alcance.

Post-Explotación: Después de explotar las vulnerabilidades, se evalúa el impacto en línea con el objetivo planteado y se intenta asegurar el acceso al sistema comprometido. Se

recopila información que pueda obtener la fase anterior y establecer el cómo se puede llegar a utilizar.

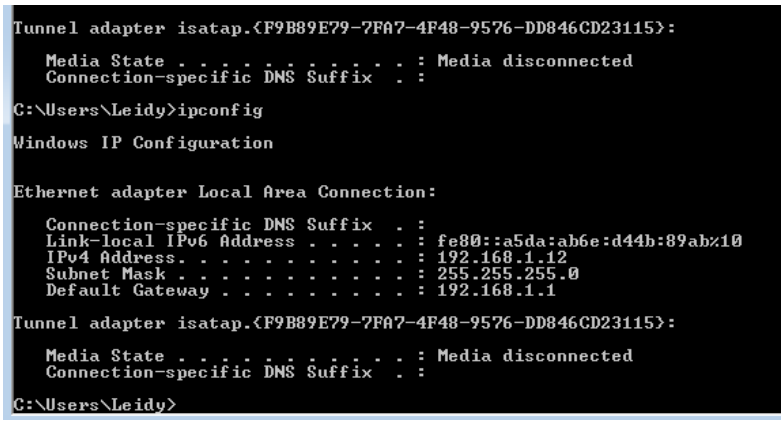
Reportes: Finalmente, se documentan todos los hallazgos y se elabora un informe de manera detallado el cual incluya todas las vulnerabilidades encontradas, las técnicas que se utilizaron y todas las recomendaciones para mitigar los riesgos encontrados.

Recolección de Información

Se identifica el equipo sobre el cual se realizará el ejercicio de escaneo, se trata de un equipo con sistema operativo Microsoft Windows 7 SP1, arquitectura x64, y con el este equipo no cuenta con usuario configurado, sin contraseña de acceso, con la dirección IP 192.168.1.12

Figura 4

Información de la Maquina Objeto

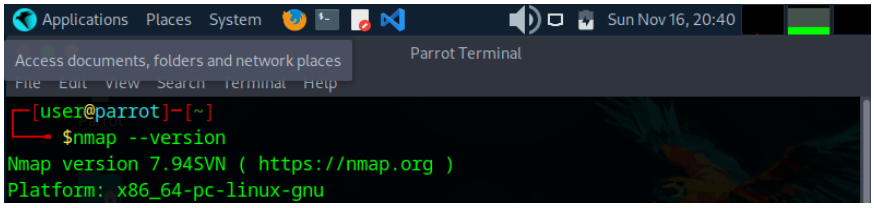


Nota. Se identifica la máquina objeto.

Nmap: Es una herramienta gratuita y de código abierto que se usa para explorar redes y revisar su seguridad. Con ella, puedes escanear a fondo los puertos y servicios de un sistema o red, el objetivo es ejecutar comandos que permitan identificar las direcciones IP asociadas al dispositivo a evaluar. El software empleado es **Nmap**, versión **7.94SVN**.

Figura 5

Validación de la Versión Nmap



Nota. Mediante el comando Nmap se valida la versión que se va a utilizar para el escaneo.

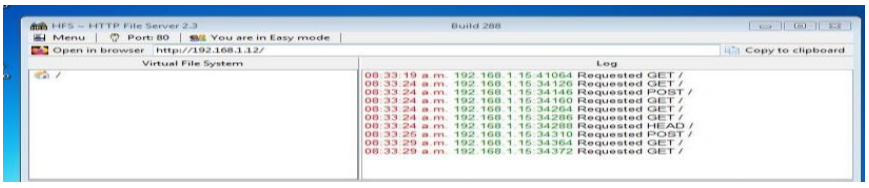
Búsqueda de Vulnerabilidades

Es fundamental la identificación de los medios a través de los cuales se está generando la fuga de información desde la máquina comprometida tales como:

- **Configuración Insegura de Usuario**: El equipo no cuenta con un usuario ni contraseña de acceso, lo que representa una vulnerabilidad crítica en cuanto a controles de autenticación y protección del sistema.
- **Sistema Operativo Obsoleto**: El equipo tiene Windows 7, un sistema que ya no está en uso y que Microsoft ha dejado de respaldar oficialmente. Esto significa que no se pueden realizar actualizaciones de seguridad, por lo tanto, no es posible implementar parches para las vulnerabilidades identificadas.
- **Presencia de Software Vulnerable**: Durante el análisis se identificó el software **Rejetto File Server**, versión **2.3**, la cual no se encuentra actualizada, la última versión disponible es la **2.4.0 RC7**, lo que sugiere la existencia de posibles vulnerabilidades explotables en la versión instalada.

Figura 6

Validación de Rejjetto



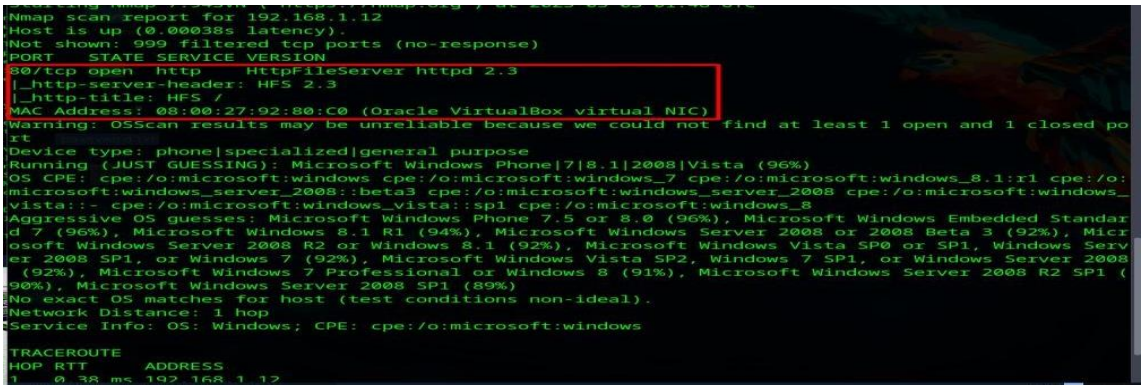
Nota. Se valida el Rejetto en la maquina objeto.

Explotación de Vulnerabilidades

En este punto, con las máquinas virtuales ya encendidas, se llevan a cabo acciones desde la consola de Parrot hacia el equipo objetivo, que es una computadora con Windows 7 SP1 que tiene en funcionamiento el programa Rejetto File Server versión 2.3.

Figura 7

Escaneo con Nmap e Identificación de la Vulnerabilidad



Nota. Se realiza el escaneo y se evidencia la vulnerabilidad en el equipo objeto

Para detectar vulnerabilidades, se ejecuta un escaneo utilizando NMAP con el comando nmap -sS -A 192.168.1.12 en la computadora que tiene instalado Windows 7 y cuya dirección IP es 192.168.1.12, desde la máquina que opera con la distribución de Linux Parrot; esto arroja resultados de vulnerabilidades en el puerto 80 HttpFileServer. (Haran,2020)

Se puede notar que la vulnerabilidad de Rejetto FileServer 2.3 posibilita un ataque de ejecución remota de Código (RCE), por medio del cual se pueden correr comandos del sistema a través de una shell. Esto da la posibilidad, por ejemplo, de usar el comando NET USER para crear usuarios nuevos y darles privilegios administrativos.

Así, un atacante puede lograr que el equipo comprometido esté permanentemente a su

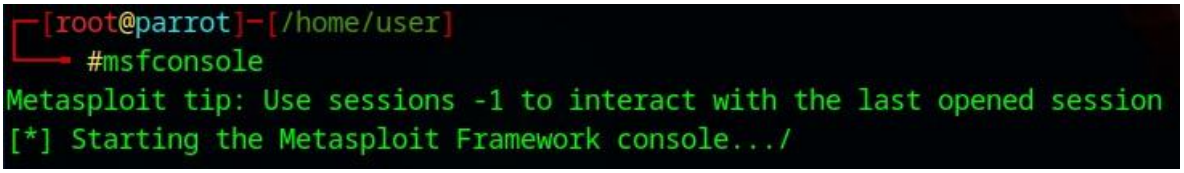
disposición y llevar a cabo una variedad de acciones que impactan al sistema, la red, los usuarios y los datos, poniendo en riesgo la disponibilidad, integridad y confidencialidad de la información. Este laboratorio permite entender cómo un exploit que utiliza una vulnerabilidad como el Rejetto FileServer 2.3 y toma el control en la máquina víctima para que el ataque funcione y se logre el control absoluto del sistema.

Post Explotación

Luego de identificar las posibles vulnerabilidades y accesos disponibles en el equipo víctima, se procede de manera controlada a realizar diferentes pruebas con herramientas como MSF6, junto con exploits, payloads y ejecuciones tipo shell, con el objetivo de obtener acceso y control remoto sobre el equipo Windows 7, cuya dirección IP es 192.168.1.12

Figura 8

Comando msfconsole para ejecutar interfaz de metasploit

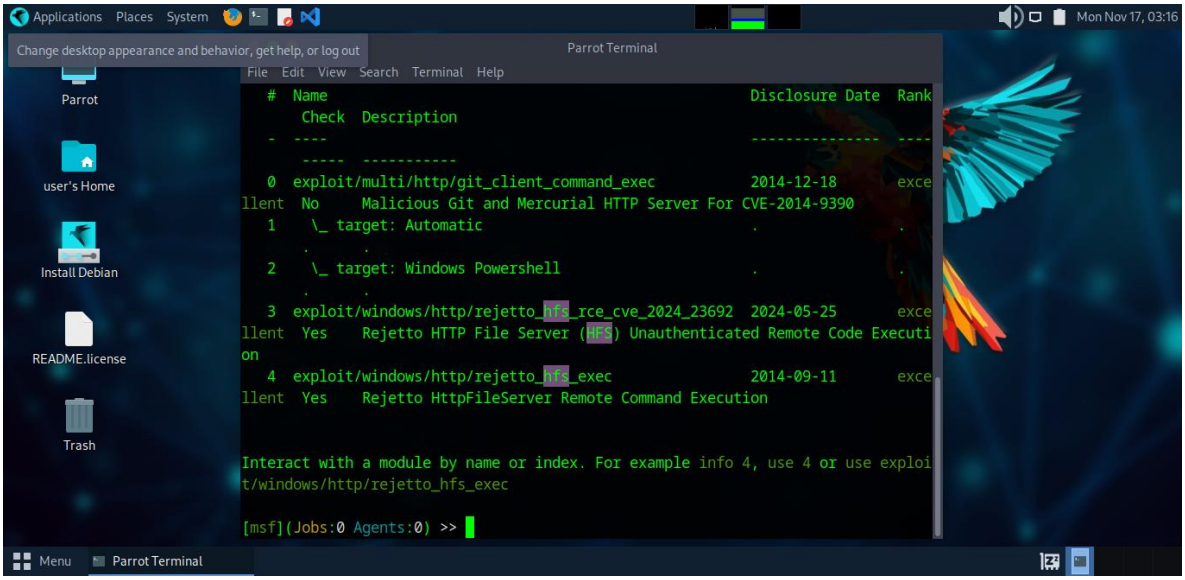


Nota. Se ingresa a la consola para ejecutar el comando metasploit y lanzar ataques contra el sistema remoto Windows 7 aprovechando que es un sistema vulnerable, donde se puede evidenciar la vulnerabilidad Rejetto HTTP.

Payloads: Código malicioso que se activa tras explotar una vulnerabilidad, diseñado para ejecutar acciones específicas en un sistema comprometido, como establecer conexiones remotas (shell inversos), ejecutar comandos con privilegios elevados o instalar malware persistente (rootkits). Su complejidad varía desde funciones básicas hasta técnicas avanzadas de evasión.

Figura 9

Comando Search para Búsqueda de Exploits y Payloads



Nota. Se identifican la vulnerabilidad Rejetto HTTP mediante los exploits

Informe

Las pruebas de intrusión que se hicieron en el escenario 3 comprobaron que el sistema operativo Windows 7 no tenía actualizaciones recientes.

Se observó que Windows 7 tiene muchas debilidades debido a que se trata de una plataforma descontinuada y sin soporte oficial de Microsoft desde hace años, durante el proceso de detección de vulnerabilidades. Este informe permitió enfocar el análisis en la búsqueda de *exploits* específicos tanto para esta aplicación como para el sistema operativo. La combinación de ambos factores sugería la posibilidad de ejecutar código remoto, abrir una shell y escalar privilegios dentro del sistema.

Se notaron intentos de salida inusuales que no coincidían con el comportamiento esperado del equipo o de la aplicación instalada. Este patrón fue un indicador claro de actividad anómala y

fortaleció la hipótesis sobre la fuga de información a través del servicio vulnerable.

Entre las vulnerabilidades halladas se encuentra la aplicación Rejetto v2.3, famosa por tener errores de seguridad graves.

Sobresale la presentación de servicios y puertos abiertos que habilitan conexiones remotas sin autorización, además de la desactivación del cortafuegos, lo cual simplifica en gran medida el trabajo de los atacantes cuando intentan detectar y aprovechar vulnerabilidades de seguridad.

Además, se realizó un análisis de los registros de eventos del sistema operativo. Estos registros fueron útiles para detectar eventos que levantaran sospechas en relación con la creación de usuarios nuevos y acciones potenciales para aumentar privilegios, el acceso remoto no autorizado fue posible gracias a las condiciones del sistema.

Fallo de Seguridad Especifico en Maquina Windows 1

Al examinar los puertos activos y las conexiones de red, se detectaron intentos de salida extraños que no correspondían al comportamiento esperado del equipo o la aplicación instalada. En lo que respecta a la detección de vulnerabilidades en el sistema operativo Windows 7 (Service Pack 1), como lo es Rejetto v2.3 se verificó que este presenta numerosas debilidades dado que es una plataforma sin soporte oficial por parte de Microsoft desde hace varios años. Entre estos elementos sobresale la presentación de servicios y puertos abiertos que habilitan conexiones remotas no permitidas, además de la desactivación del firewall, lo cual simplifica notablemente el trabajo para potenciales atacantes cuando se trata de identificar y aprovechar vulnerabilidades de seguridad.

Identificación de Fallo de Seguridad

Al ser un sistema informático y no tener una configuración apropiada de las reglas del

firewall, el entorno del sistema queda expuesto, lo que disminuye significativamente su capacidad de defensa en tiempo real.

Una de las amenazas reconocidas fue la oportunidad de llevar a cabo comandos de manera remota, lo cual era posible gracias a una aplicación con una versión anticuada del software Rejetto (v2.3). Esta aplicación se puede acceder por medio del puerto 80 y es famosa porque posibilita la explotación de vulnerabilidades, lo cual permite que se reconozcan los servicios activos, que se escalen privilegios, que se creen cuentas ilegítimas, que se alteren o eliminen archivos e incluso que se instalen programas dañinos.

Afectación del Ataque a la Maquina

La falta de una configuración apropiada de las reglas del firewall deja vulnerable el entorno del sistema, disminuyendo su capacidad defensiva. Esto ocurre cuando hay una posibilidad de ejecutar comandos de manera remota a través de una aplicación con una versión desactualizada del software. En consecuencia, se pueden llevar a cabo acciones como la identificación de servicios activos, la elevación de privilegios, la creación de cuentas ilegítimas, la modificación o eliminación de archivos y hasta la instalación de programas dañinos. El equipo queda expuesto a que se recolecte información sensible, se transfieran datos a lugares externos y se use el sistema comprometido para fines ilegales o destructivos.

Figura 10

Grafica del Proceso de Ataque a la Maquina Objeto

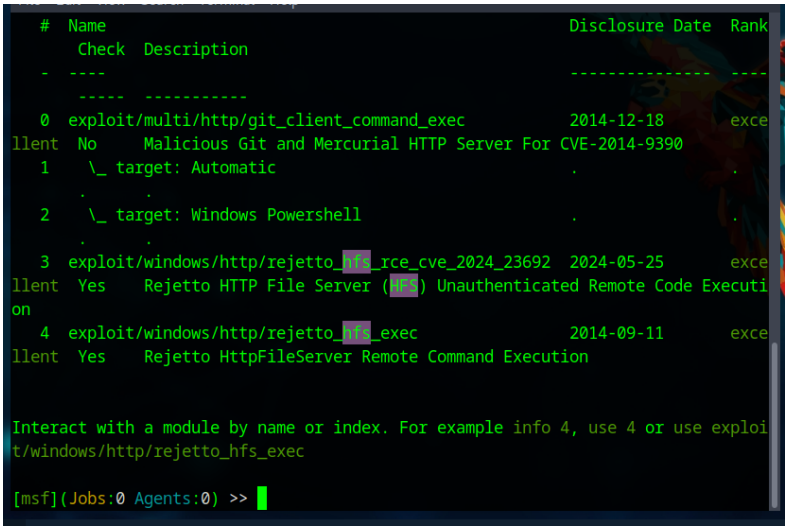
Nota. Se visualiza la recolección de información de la maquina objeto, se realiza el escaneo de vulnerabilidades mediante el comando Nmap, la explotación de los exploits mediante la consola msfconsole, y se presenta informe detallado de la prueba de intrusión.

Pasos de Explotación de Vulnerabilidades

Para la fase de explotación del equipo objetivo con Windows 7 Pro SP1, con dirección IP 192.168.1.12, Sin parches de actualizaciones de seguridad y versiones obsoletas de software como rejetto v2.3, la cual cuenta con vulnerabilidades y métodos de explotación desde Metasploit en su versión 6.4.58-dev.

Figura 11

Búsqueda de los Exploit Asociados a Rejetto



Nota. Mediante el comando Search hfs se realiza la búsqueda de los exploits asociados a rejetto.

Una vez en nuestra maquina parrot iniciamos terminal y escribimos el comando **msfconsole** para iniciar metaexploit, ya en la consola de metaexploit procedemos a seleccionar el exploit que permite explotar una vulnerabilidad conocida en el servidor web Rejetto V2.3 HFS (HTTP File Server) obteniendo acceso mediante la ejecución remota de código. Mediante el

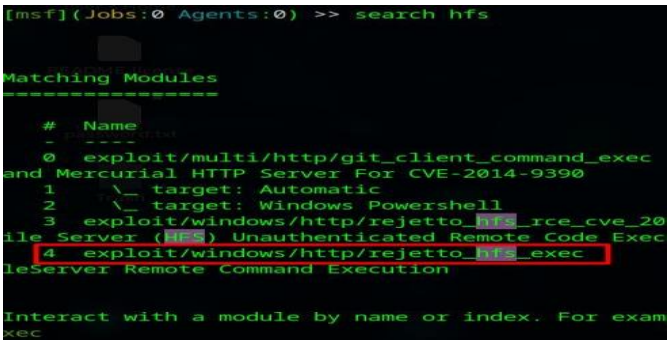
comando: **use exploit/windows/http/rejetto_hfs_exec**

Una vez en nuestra maquina parrot iniciamos terminal y escribimos el comando **msfconsole** para iniciar metaexploit, ya en la consola de metaexploit procedemos a seleccionar el exploit que permite explotar una vulnerabilidad conocida en el servidor web Rejetto (HTTP File Server).

Mediante la ejecución remota del código **Use xploit/windows/http/rejetto_hfs_exec** Indicamos que vamos a emplear este exploit, Luego empleamos **set payload windows/x64/meterpreter/reverse_tcp**

Figura 12

Búsqueda de Exploit



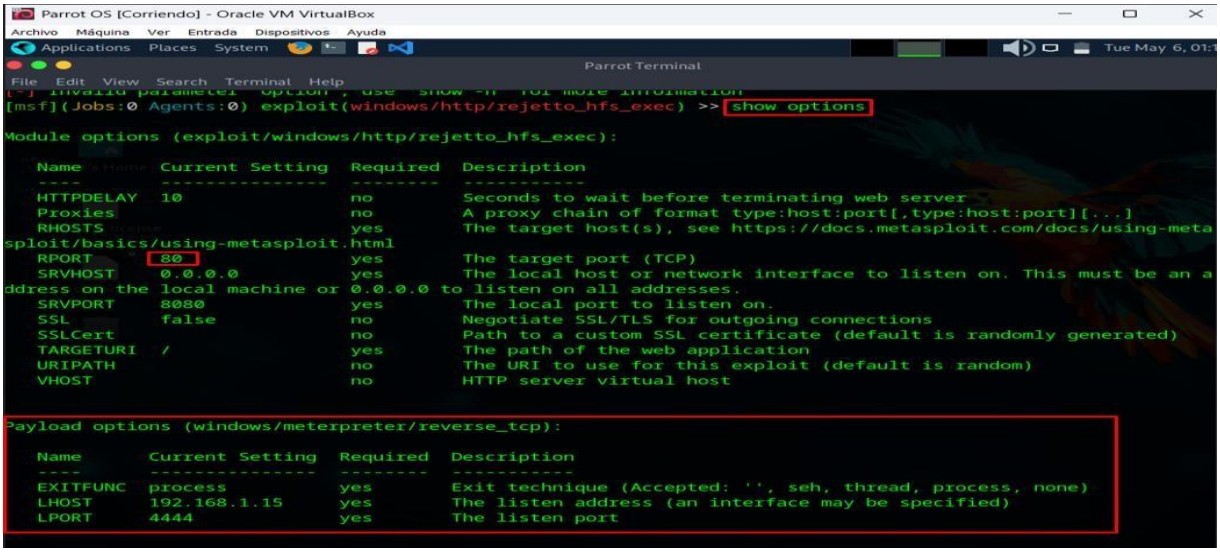
Nota. Se puede evidenciar la búsqueda de la explotación.

Para elegir el payload que se ejecutará tras una explotación exitosa de la vulnerabilidad, se configura una conexión inversa mediante TCP. Esta conexión permite que la máquina objetivo otorgue acceso remoto al atacante.

Utilizamos el comando **show options** que permite ver la configuración del exploit seleccionado.

Figura 13

Contenido de Exploit

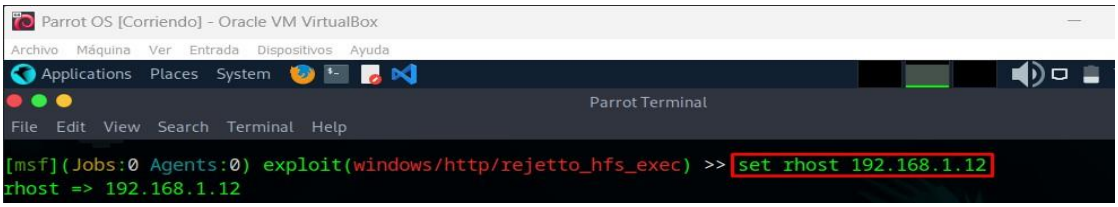


Nota. Configuración del exploit seleccionado.

Comando: **set rhost 192.168.1.12,** Con el cual se indica la dirección IP de la maquina objetivo.

Figura 14

Direccionamiento del Exploit

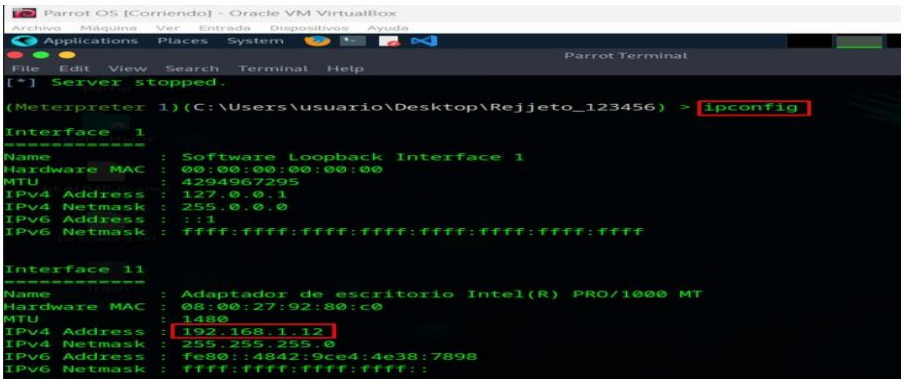


Nota. Tras la ejecución exitosa del exploit, se logra establecer una conexión remota con el sistema comprometido.

Una vez establecida la conexión se procede a ejecutar comandos como **Ipconfig,**

Figura 15

Ejecución Comando Ipconfig

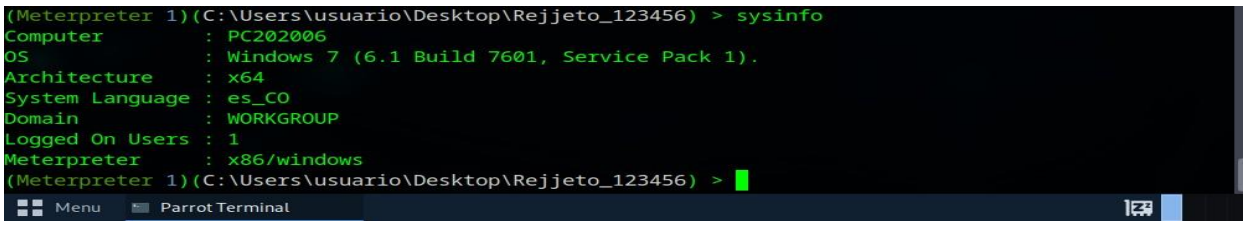


Nota. Se valida la dirección IP del equipo objet

Para validar la dirección IP del equipo objetivo, obteniendo el direccionamiento.

Figura 16

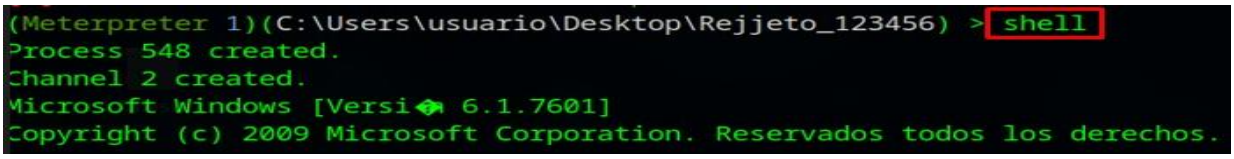
Comando Sysinfo



Nota. validamos la información de la maquina Objetivo.

Figura 17

Comando Shell



Nota. Ahora empleamos el comando **Shell,** para la ejecución de comandos en la maquina

Ingresamos los siguientes comandos para crear un usuario nuevo con cuenta de administrador **net user LeidiBrand /add,** para crear el usuario.

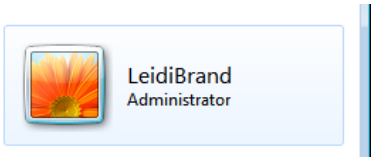
Elevamos los privilegios del usuario creado como administrador con el comando: **localgroup administradores LeidiBrand /add.**

Ejecutamos el comando: net user, para corroborar los usuarios creados actualmente en la maquina con sus roles respectivos**.**

Se procede a validar en la maquina victima el usuario creado mediante comandos desde parrot y que este usuario pertenezca al grupo de administradores.

Figura 18

Validación de Usuario Como Administrador



Nota. Se valida el usuario creado en la maquina objeto

Ataque en Tiempo Real

Para verificar la presencia de una intrusión activa en la máquina afectada, es necesario examinar las conexiones de red activas. Esto posibilitará detectar conexiones inusuales hacia IPs externas o desde estaciones que no son estándar o que no se emplean. Es necesario validar el número de conexiones cuando se detectan estas conexiones inusuales, porque un volumen excesivo de conexiones desde o hacia la misma dirección IP puede ser una señal de que está ocurriendo una exfiltración o escaneo de datos.

En el caso del equipo comprometido, se puede analizar el comportamiento y el tráfico del puerto 80 el cual es el puerto utilizado por la aplicación Rejjeto HFS, La evaluación de los

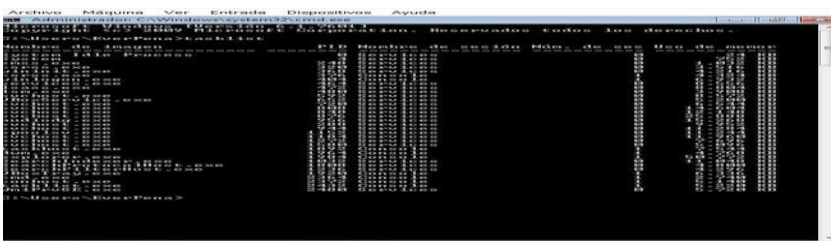
procesos que se están llevando a cabo, también es crucial para detectar un ataque en tiempo real. Además de tener en cuenta el rendimiento de la máquina, como la CPU o la memoria, ya que estos pueden generar picos altos cuando se llevan a cabo procesos no legítimos o maliciosos, es posible detectar algunos procedimientos, como los utilizados por Powershell o aquellos que incluyan archivos temporales en la carpeta del Rejjeto o procesos anómalos de HFS.exe.

Las primeras medidas a tomar cuando se está sufriendo un ciberataque en tiempo real deben ser las de contener la situación, mantener la evidencia y prevenir que el peligro se propague. Para conseguirlo, es fundamental seguir una serie de pasos claramente establecidos:

- **Aislar de inmediato el equipo comprometido***:* Se desconecta el equipo de la red tanto a nivel físico como virtual, para evitar la propagación del ataque, sí es posible, redirigir el tráfico de red para minimizar el impacto.
- **Desconectar accesos remotos y cambiar contraseñas***:* Debemos restringir cualquier acceso al equipo no autorizado y restablecer contraseñas para evitar accesos mal intencionados.
- **Detección de actividad sospechosa:** Reconocer procesos y servicios que puedan estar vinculados con el ataque, empleando herramientas como tasklist o el administrador de tareas de Windows que permiten revisar los activos y detectar comportamientos inusuales.

Figura 19

Ejecución de Comando Tasklist

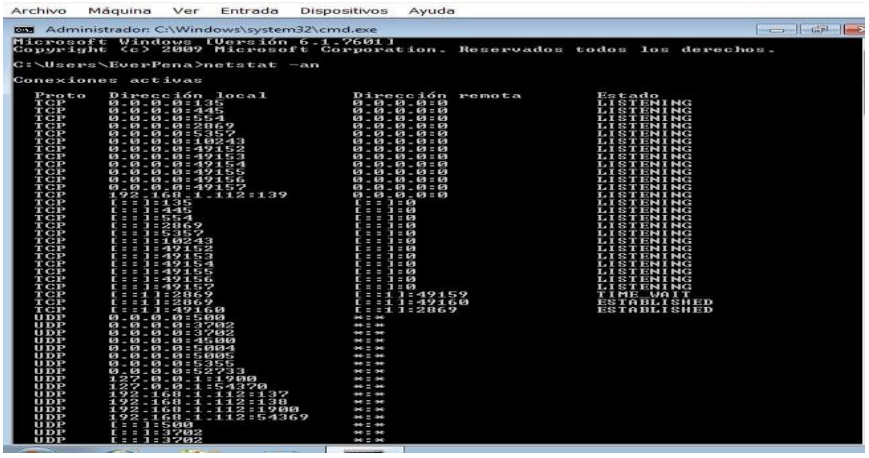


Nota. Se verifica procesos y servicios que puedan estar vinculados con el ataque.

- **Revisión de los registros del sistema:** Se debe verificar los eventos recientes a través del visor de eventos de Windows, hay que prestar atención a intentos fallidos o exitosos de inicio de sección, cambien configuraciones y la aparición de errores o advertencias inusuales.

Figura 20

Ejecución de Comando Netstat - an



Nota. Verificación de túneles de comunicación.

- **Elaboración de informes y comunicación con el equipo de seguridad:** Es fundamental coordinar de manera efectiva las medidas de contención y recuperación del equipo afectado, además de facilitar la evaluación de posibles impactos adicionales dentro de la red.

Medidas de Hardenizaciòn

Es esencial, para robustecer los sistemas de información, implementar un conjunto de medidas técnicas y organizativas. En este contexto, la estrategia Blue Team juega un rol relevante; como equipo defensor cuya responsabilidad es prevenir, identificar y reaccionar ante ataques mediante la ejecución de medidas de hardenización. su finalidad es salvaguardar,

detectar y reducir los ataques eficazmente. Se pueden estructurar estas acciones en diversos ámbitos.

Para el equipo comprometido, es posible examinar la actividad y el tráfico del puerto 80, que es el que emplea la aplicación Rejjeto HFS.

Reemplazar o Eliminar el Software Vulnerable

Desinstalar la aplicación HFS 2.3 previamente identificada como brecha de seguridad, se debe actualizar a la versión más reciente sin vulnerabilidades conocidas, sin embargo, sería más conveniente reemplazar HFS por un servidor web más seguro.

Restringir la Exposición del Servicio

Limitar accesos a través de controles de seguridad Configurando el servidor HFS para que escuche únicamente en la dirección IP local o en una sub red específica.

Configurar el firewall para que por defecto solo permita el acceso de IP internas autorizadas y bloquear accesos externos.

Configuración Del Firewall En Windows 7

Crear reglas para bloquear el puerto del servidor (por defecto el puerto 80) desde direcciones externas, cerrar todos los puertos innecesarios y mantener un enfoque de denegación, además de asegurarse de que solo los servicios requeridos estén accesibles desde la red. (Haran,2020).

Diferencia entre Blue Team y Equipo Respuesta Incidentes

Tabla 1

Diferencias entre Blue Team y Equipo de Respuesta Incidentes Informáticos.

Equipo Blue – Team	Equipo de respuesta a incidentes
Equipo dedicado a la defensa y protección continua de la infraestructura de TI, anticipándose a posibles riesgos.	Grupo de profesionales capacitados que actúan durante y después de un incidente de seguridad, con el objetivo de controlar la situación, mitigar el impacto y restaurar la normalidad en los sistemas afectados.
Su función es proteger los sistemas, datos y redes de la organización, monitoreando la red para detectar intrusiones.	Su principal objetivo es monitorear sistemas de información con la finalidad de identificar amenazas y eliminar el ataque del sistema.
Implementa medidas de seguridad mediante parches y herramientas para prevenir vulnerabilidades, accesos no autorizados y ataques cibernéticos.	Su función es restaurar el sistema para volver a la normalidad operativa lo más rápido posible.
Se enfoca en endurecer sistemas y configurar la infraestructura de forma segura.	Realiza investigaciones y análisis forenses después del incidente.
Implementa herramientas de seguridad como firewalls, IDS/IPS y sistemas SIEM.	Restaura servicios afectados y elimina las amenazas detectadas.
Capacita a los empleados en buenas prácticas de ciberseguridad.	Elabora informes detallados que documentan el incidente y sus causas.

Nota. Diferentes características entre equipo Blue Team y equipo de respuesta a incidentes.

(Check Point, s. f, 2025; UNIR, 2020)

CIS “Center For Internet Security”

Los Controles CIS son una herramienta fundamental para el Blue Team, ayudan a fortalecer sus defensas y a cumplir con estándares de seguridad establecidos, proporciona recursos completos como guías de configuración de seguridad, herramientas y controles para fortalecer la ciberseguridad, dentro de un equipo Blue Team, estas herramientas y lineamientos pueden ser aprovechados con distintos fines, tales como (Center for Internet Security [CIS], 2024).

- Implementar los **CIS Benchmarks** para establecer configuraciones seguras y recomendadas en diferentes tecnologías.
- Realizar evaluaciones y endurecimiento (hardenización) de sistemas para reducir vulnerabilidades.
- Llevar a cabo auditorías y verificar el cumplimiento con estándares de seguridad.
- Monitorizar de forma continua utilizando los **CIS Controls**, un conjunto de mejores prácticas para la ciberseguridad.
- Aprovechar las herramientas gratuitas que proporciona CIS para facilitar la protección y gestión de los sistemas.
- Desarrollar planes de respuesta ante incidentes y recuperación para minimizar impactos en caso de ataques.
- Capacitar y sensibilizar al equipo de seguridad para mantenerlos actualizados y preparados ante amenazas.

SIEM: Gestión de Eventos e Información de Seguridad

Su función principal es reunir y analizar datos de seguridad en tiempo real, combinando dos enfoques, la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM). (SentinelOne, 2024)

Utiliza análisis avanzado como la inteligencia artificial identificando anomalías en tiempo real, permitiendo responder a los ataques antes de que causen daño.

Tabla 2

Gestión de Eventos e Información de Seguridad

Componentes y Función	Descripción
Administración de registros	Analizan registro de toda la organización con el fin de encontrar anomalías que indiquen una amenaza, utilizan inteligencia artificial con el objetivo de bloquear lo más pronto posible un ciber ataque.
Correlación de eventos	Se recopila información de múltiples sistemas de una empresa, con la finalidad de detectar actividades benignas en diferentes eventos.
Respuestas a incidentes	Se realiza mediante el monitoreo continuo a los sistemas digitales y locales con el fin de enviar alerta a los analistas de seguridad, en algunos casos se puede tomar

Componentes y Función	Descripción
	medidas automáticamente según reglas definidas con casos más complejos.
Recolección de información	Centraliza y organiza los registros de actividad provenientes de distintas Notas, como servidores, aplicaciones o dispositivos de red.
Correlación de eventos	Conecta distintos eventos que por sí solos parecen inofensivos, pero que en conjunto pueden revelar comportamientos sospechosos.
Supervisión en tiempo real	Vigila continuamente el entorno digital para identificar rápidamente cualquier señal de amenaza o comportamiento anómalo.

Nota. Eventos a realizar mediante identificación de amenazas.

Herramientas de Contención de Ataques

Tabla 3

Herramientas de Contención de Ataques

Herramientas	Descripción	Función
pfSense	Firewall de código abierto altamente configurable, ideal para la protección perimetral de redes	Filtra el tráfico entrante y saliente de la red tanto interna como externa.
Snort	Sistema de detección y prevención de intrusiones que examina el tráfico de red en busca de amenazas.	Busca inspeccionar el tráfico en tiempo real en busca de actividades maliciosas o mal intencionadas.
Wazuh	Plataforma open source centrada en el monitoreo y respuesta ante amenazas en dispositivos finales (endpoints).	Registra eventos sospechosos en tiempo real, detecta comportamientos maliciosos en estaciones de trabajo y servidores.

Nota. Diferentes herramientas para contener un ciber ataque.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/gBac5ec6dH0

Conclusiones

En conclusión, la importancia de las leyes de protección de datos personales y el proceso legal ante los delitos informáticos es el deber y la responsabilidad que tenemos como profesionales a enfrentar situaciones relacionadas con la seguridad informática mediante normativas que generan confianza en la protección de datos informáticos de las diferentes organizaciones.

En la práctica simulada aplique diferentes herramientas técnicas y tácticas que me brindaron la posibilidad de explotar vulnerabilidades o ataques en tiempo real para tener una perspectiva más clara ante incidentes de seguridad y brindar solución oportuna y concreta ante un incidente de ciberseguridad.

Aplicamos pruebas de intrusión mediante herramientas gratuitas con el fin de mitigar el riesgo y proteger los sistemas de información de ataques o vulnerabilidades, brindando respuestas oportuna y eficaz ante un ataque a un sistema vulnerable.

Recomendaciones

Conocer con claridad las diferentes leyes de seguridad de la información con el objetivo de garantizar un cumplimiento normativo ante cualquier incidente de ciberseguridad.

En el análisis de la práctica realizada puedo evidenciar la importancia del enfoque Red Team y Blue Team como monitoreo continuo para la identificación de la vulnerabilidad en el equipo expuesto, permitiendo una respuesta oportuna e identificación de puntos débiles y fortalecer la seguridad del sistema.

Se debe implementar controles de acceso solo a usuarios autorizados, aplicando mecanismos robustos de autenticación para garantizar la confidencialidad, integridad y disponibilidad de la información.

Establecer políticas claras en el manejo y gestión de vulnerabilidades, control de accesos, respuesta a incidentes y mejores prácticas de seguridad, estas deben estar alineadas con estándares internacionales y política organizativa.

Referencias Bibliográficas

Bacudio, A. G., et al. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications. https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing

Bardají, E. (2025). Red team vs. blue team: Simulaciones de ciberataques para fortalecer la seguridad empresarial. ESEDsl. https://www.esedsl.com/blog/red-team-vs-blue-team-simulaciones-de-ciberataques-para-fortalecer-la-seguridad-empresarial

Check Point Software. (2025). Red Team vs. Blue Team. https://www.checkpoint.com/cyber-hub/cyber-security/red-team-vs-blue-team/

Cilleruelo, C. (2024). El Red Team y las simulaciones de ataques. KeepCoding. https://keepcoding.io/ciberseguridad/el-red-team-y-las-simulaciones-de-ataques/

CIS. (2024). Creating confidence in the connected world. https://www.cisecurity.org/

Haran, J. M. (2020). Advierten sobre los riesgos de seguridad que supone seguir utilizando Windows 7. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

INCIBE. (2023). Pentesting. https://www.incibe.es/aprendeciberseguridad/pentesting

INCIBE. (2024). Múltiples vulnerabilidades en HTTP File Server de Rejetto. https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-http-file-server-de-rejetto

Función Pública. (2012). Ley Estatutaria 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981 3

Función Pública. (2009). Ley 1273 de 2009.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1273 de 2009. (2009). Por medio de la cual se modifica el Código Penal colombiano. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Qualysec. (2024). Penetration testing execution standard (PTES): What is. https://qualysec.com/penetration-testing-execution-standard/

SentinelOne. (2024). Red team exercises in cybersecurity: Benefits & examples. https://www.sentinelone.com/cybersecurity-101/services/red-team-exercise-in-cybersecurity/

Secretaría Jurídica Distrital. (2008). Ley 1266 de 2008 - Congreso de la República de Colombia. https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34488

UNIR. (2020). Red team, blue team y purple team: Funciones y diferencias. UNIR Revista. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Apéndices

Apéndice A

Resultado de Revisión en Turnitin

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	LEIDI YOJANA BRAND LADINO
Título del ejercicio:	ECBTI - Draftbank 4 Sección 1 (Moodle TT)
Título de la entrega:	Seminario
Nombre del archivo:	1218848_LEIDI_YOJANA_BRAND_LADINO_Seminario_1234_412...
Tamaño del archivo:	4.78M
Total páginas:	57
Total de palabras:	7,857
Total de caracteres:	47,387
Fecha de entrega:	08-dic-2025 03:47p. m. (UTC-0500)
Identificador de la entrega:	2840295347

Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Leidi Yojana Brand Ladino

Asesor

Edwin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Nota. Informe del turnitin