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

Presentado por:
Francisco Sánchez Quintero

Grupo:
202337164_3

Tutor:
LUIS FERNANDO ZAMBRANO

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI
Especialización en seguridad informática.
Universidad Nacional Abierta y a Distancia UNAD
mayo de 2025

Resumen

Este informe aborda las capacidades técnicas, legales y de gestión necesarias para los equipos Blue Team y Red Team, mediante la simulación de un entorno de ciberseguridad comprometido en un sistema Windows 7. A través de la explotación de la vulnerabilidad MS17-010 con la herramienta Metasploit, se demuestra un ataque exitoso, seguido de un análisis defensivo detallado por parte del Blue Team. Se revisan leyes colombianas relevantes, estándares internacionales, herramientas especializadas, y se contrastan las funciones del Blue Team con las de un equipo de respuesta a incidentes. El estudio también considera la ética profesional en contextos de ciberseguridad y propone buenas prácticas de hardening, monitoreo y contención de ataques.

Índice

Glosario

Blue Team: Grupo encargado de la defensa proactiva de los sistemas informáticos de una organización.

CIS Benchmarks: Recomendaciones de configuración segura desarrolladas por el Center for Internet Security.

CVE: Common Vulnerabilities and Exposures, lista pública de vulnerabilidades.

Hardening: Proceso de asegurar un sistema mediante la reducción de vulnerabilidades.

Metasploit: Plataforma de código abierto para pruebas de penetración.

MS17-010: Vulnerabilidad crítica del sistema SMBv1 explotada por EternalBlue.

Nmap: Herramienta de escaneo de redes.

Red Team: Equipo que simula ataques reales con el fin de evaluar la efectividad de las defensas existentes.

SIEM: Security Information and Event Management, sistema para la correlación y análisis de eventos de seguridad.

YARA: Herramienta de identificación de malware.

Introducción.

Los equipos Blue Team y Red Team son pilares fundamentales en la estrategia de ciberseguridad organizacional. Mientras los primeros enfocan su labor en prevenir, detectar y contener amenazas, los segundos simulan ataques reales para poner a prueba las defensas. Este trabajo se desarrolla a partir de un entorno simulado donde se explota la vulnerabilidad MS17-010 con el fin de evaluar la reacción técnica del equipo defensor. Además, se abordan los aspectos legales y éticos que rodean la práctica profesional en el área, así como el uso de marcos de referencia y herramientas libres. El propósito general es demostrar cómo una adecuada articulación entre tecnología, normatividad y principios éticos fortalece la postura de seguridad de cualquier organización.

Objetivos

Objetivo General

Analizar y contener un ataque informático simulado en tiempo real dentro de un entorno Windows, aplicando estrategias Blue Team y herramientas de licencia libre, con el fin de mitigar su impacto, proponer mejoras de seguridad y fortalecer la postura defensiva de la organización.

Objetivos Específicos

Identificar las acciones de contención y mitigación que debe ejecutar un equipo de respuesta de incidentes al enfrentar un ataque activo.

Proponer medidas de hardening basadas en estándares reconocidos para prevenir futuras explotaciones.

Explicar el rol del Blue Team en contraste con los equipos Red Team y de respuesta a incidentes.

Aplicar marcos de referencia como los CIS Benchmarks y herramientas como SIEM para fortalecer la defensa informática.

Desarrollo:

Principales características de leyes y decretos existentes dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales:

Constitución Política de Colombia 1991.

Ley Estatutaria 1266 de 2008 " Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

Ley 1273 del 2009 " por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Ley 1581 de 2012. Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

Conpes 3854 del 2016. Política Nacional de Seguridad digital.

Norma ISO/IEC 27001 - Estándar para la seguridad de la información.

Etapas de las pruebas de penetración y ejemplo de una herramienta que se utilice en cada etapa.

Reconocimiento:

Es la primera fase de las pruebas de penetración (Pentest). En esta, los profesionales buscan y reúnen la mayor información posible sobre los sistemas objetivos, esto incluye datos de las topologías de red, sistemas operativos y aplicaciones, cuentas de usuarios, y otros datos relevantes. El objetivo es crear una estrategia efectiva de ataque fundamentada en lo datos encontrados. (Fernandez, 2022)

El reconocimiento se puede clasificar en activo y pasivo dependiendo de los métodos usados para encontrar información. El reconocimiento pasivo junta información de recursos que están abiertos al público mientras que el activo requiere una interacción con el sistema objetivo a fin de obtener información. Normalmente, ambos métodos son necesarios para formar un panorama completo de las vulnerabilidades existentes en el objetivo.

Herramienta activa: Shodan

Herramienta pasiva: Redes sociales

Escaneo.

Una vez que todos los datos relevantes se han reunido en el reconocimiento, se pasa a la fase de escaneo. Aquí, el tester usa varias herramientas para identificar puertos abiertos y revisar el tráfico de red del objetivo. Como los puertos abiertos son potencialmente puntos de entrada para atacantes, los testers necesitan identificar tantos puertos abiertos como sea posible para la siguiente fase.

Este paso puede ser ejecutado fuera las pruebas de penetración; en estos casos, se habla de un escaneo de vulnerabilidades el cual es un proceso automatizado. Sin embargo, hay algunas

acotaciones importantes a realizar escaneos de vulnerabilidades por fuera de un pentest complete: se pueden identificar potenciales amenazas, pero determinar el nivel de acceso que pueden tener los adversarios es imposible. Así que, aunque el escaneo es esencial para la ciberseguridad, necesita la intervención humana (pentest) para alcanzar su máximo potencial. (EC-Council, 2022)

Herramienta: Nmap

Evaluación de Vulnerabilidades.

En esta tercera fase es donde el tester usa toda la información reunida en fases anteriores para identificar las potenciales vulnerabilidades y determinar si pueden ser explotadas. Al igual que el escaneo, la evaluación de vulnerabilidades es útil como herramienta por sí misma pero cuando se combina con las fases del pentesting entrega resultados superiores.

Cuando se determina el riesgo de las vulnerabilidades identificadas, los testers tienen bastantes recursos para consultar como son: National Vulnerability Database (NVD), que es un repositorio de gestión de vulnerabilidades creado y mantenido por los estados unidos al analizar las vulnerabilidades de software publicadas en las bases de datos del Common Vulnerabilities and Exposures (CVE). NVD clasifica las severidades de vulnerabilidades conocidas usando el Common Vulnerability Scoring System (CVSS).

Herramienta: base de datos de common vulnerabilities exposure (CVE).

Exploitation

Una vez que las vulnerabilidades se han identificado, se procede a explotarlas. Es en esta fase donde los penetration testers intentan acceder a los sistemas objetivo y explotar sus

vulnerabilidades, normalmente usando Metasploit, herramienta que permite simular ataques reales.

Esta fase es la más crítica de las pruebas de penetración ya que obtener acceso a un sistema requiere que se salten las restricciones de seguridad. Aunque rara vez se inhabilitan los sistemas en las pruebas de penetración, los testers deben tener especial cuidado para asegurarse de evitar daños importantes o permanentes en los sistemas objetivo. (EC-Council, 2022)

Herramienta: Metasploit.

Reporte

Una vez que la fase de explotación ha culminado, se debe de preparar un reporte que documente los hallazgos. Este reporte es la fase final de toda prueba de penetración y su objetivo es la

mitigación de las vulnerabilidades encontradas en el sistema objetivo y la mejora de las políticas de seguridad de la organización.

Redactar un reporte requiere claridad d al documentar cada vulnerabilidad, poniéndolas en el contexto de la organización para que así se puedan evaluar los riesgos. Los reportes más útiles incluyen secciones para una descripción detallada de las vulnerabilidades, el impacto al negocio, una explicación de la fase de explotación y sus dificultades, un briefing de riesgos técnicos, consejos de remediación, lecciones aprendidas y recomendaciones estratégicas. (Fernandez, 2022)

Definición de herramientas a utilizar:

Metasploit

es una plataforma de código abierto utilizada para el desarrollo y ejecución de exploits contra máquinas remotas. Es ampliamente usada por pentesters y equipos de seguridad para probar vulnerabilidades, ejecutar ataques simulados y desarrollar nuevas técnicas de explotación. Metasploit cuenta con una gran base de datos de exploits conocidos y herramientas auxiliares para escaneo, fuerza bruta, post-explotación, etc. (metasploit, 2025)

Nmap (Network Mapper)

Es una herramienta de código abierto para el escaneo y mapeo de redes. Se usa para descubrir hosts y servicios en una red, identificando puertos abiertos, sistemas operativos, versiones de servicios, etc. Es muy útil en la fase de reconocimiento de un pentest y también para tareas de administración de red. (Nmap, 2025)

OpenVAS (Open Vulnerability Assessment System)

Es un sistema completo de análisis de vulnerabilidades de código abierto. Permite escanear dispositivos en busca de vulnerabilidades conocidas. Incluye un motor de escaneo, un administrador y una base de datos actualizada con miles de vulnerabilidades. Es muy utilizado para auditorías de seguridad y cumplimiento normativo. (OpenVAS, 2025)

Servicios en línea:

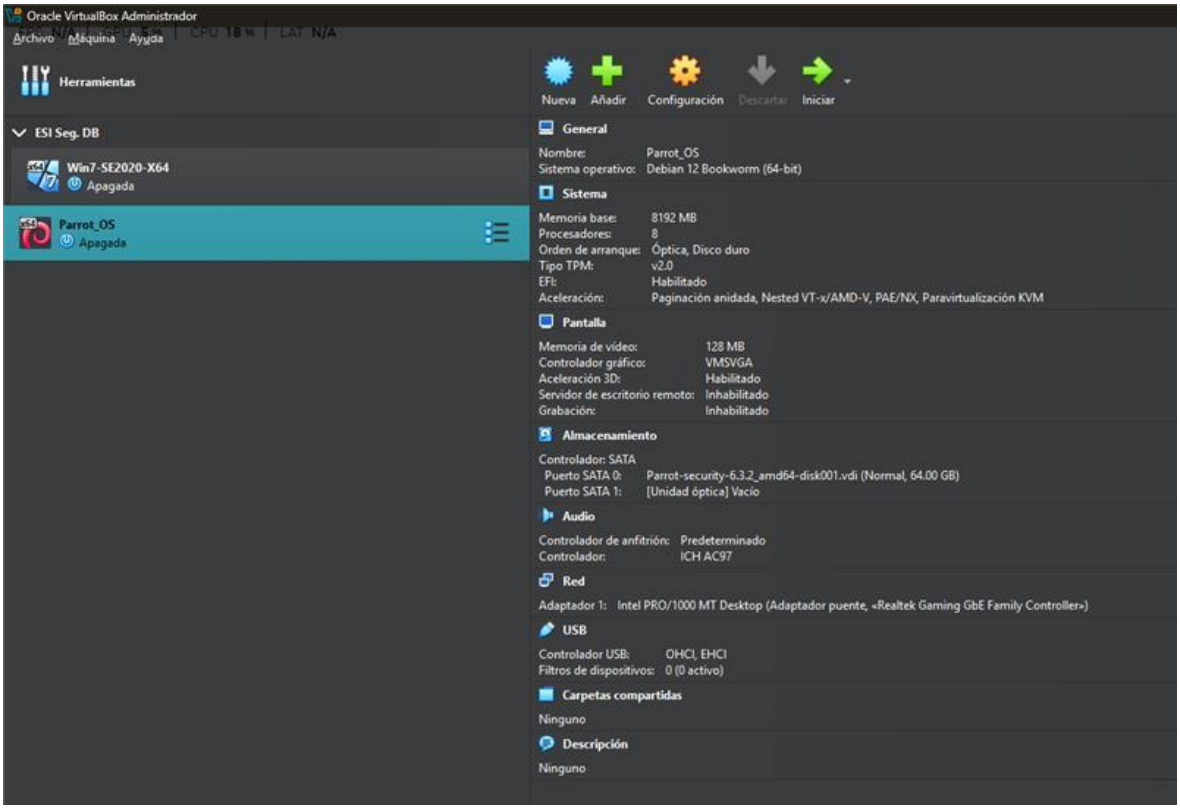
ExploitDB (Exploit Database): es una base de datos pública de exploits conocidos. Es administrada por Offensive Security, este sitio recopila exploits funcionales para vulnerabilidades de software, así como pruebas de concepto (PoC). Es usada por investigadores y pentesters para conocer vulnerabilidades activas en software y sistemas. (Exploit Database, 2025)

CVE (Common Vulnerabilities and Exposures): es un sistema público de referencia para identificar y catalogar vulnerabilidades de software.

Explicación: Cada CVE es un identificador único que describe una vulnerabilidad específica. Es administrado por MITRE Corporation y utilizado por múltiples herramientas y bases de datos de seguridad. Ayuda a estandarizar la forma en que se comunica y rastrea una vulnerabilidad. (CVE, 2025)

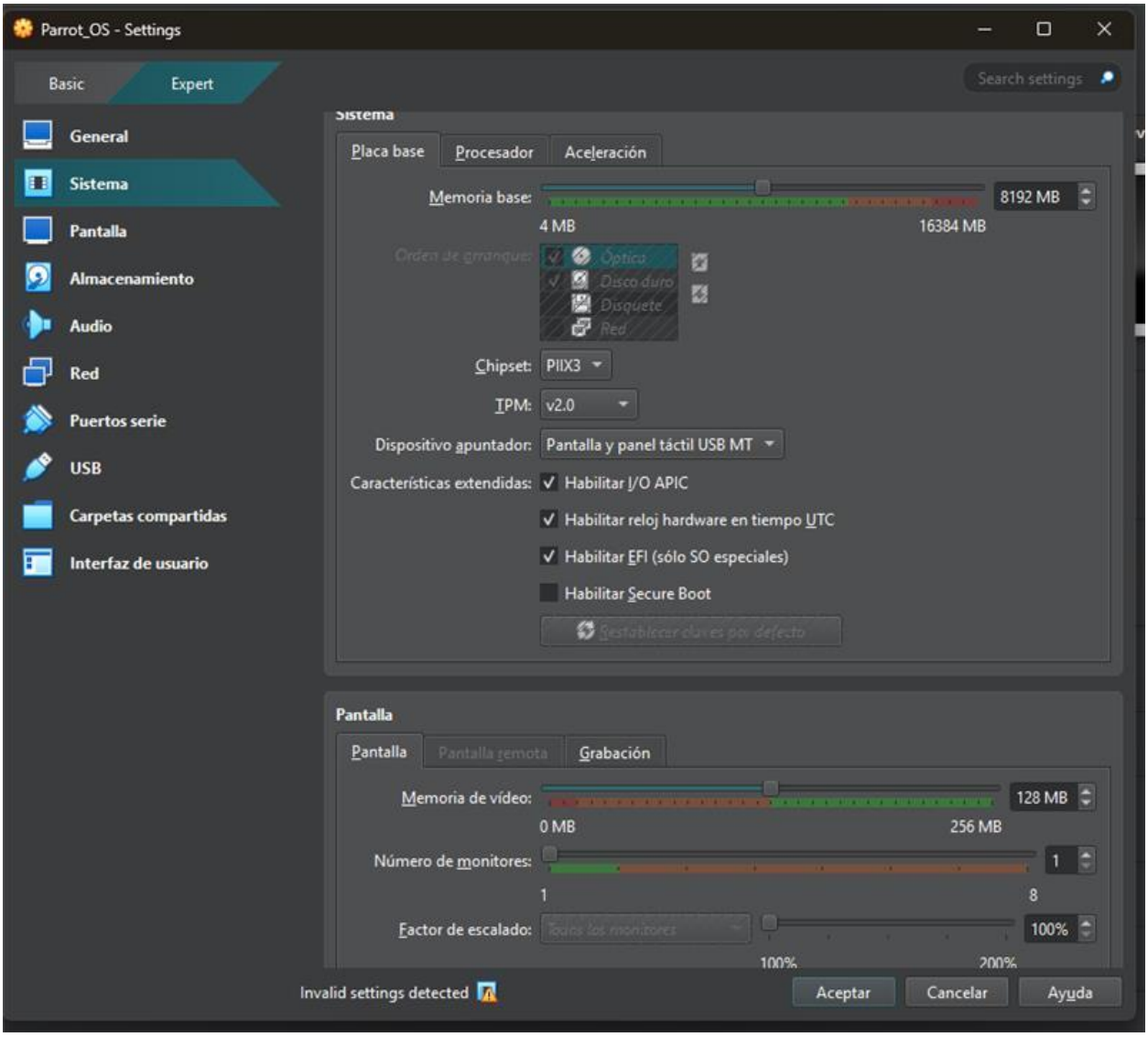
Configuración del banco de trabajo solicitado sobre el cual se realizarán las pruebas de penetración con enfoque Red Team.

Figura 1 - Instalacion de banco de trabajo maquinas parrot - win7



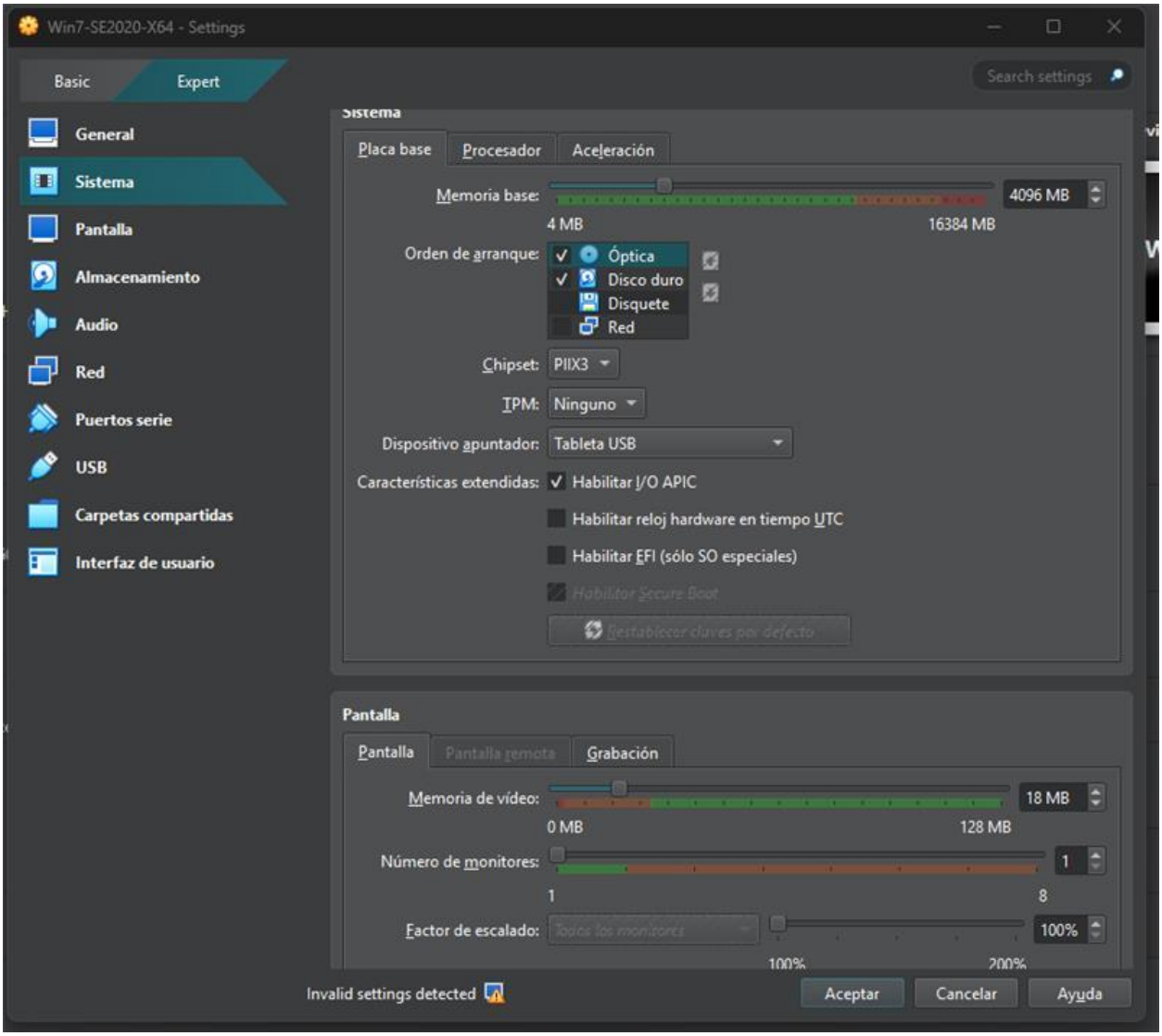
Nota: Las maquinas virtuales fueron descargadas del repositorio de la UNAD e instaladas en VirtualBox.

Figura 2 - Recursos asignados a Parrot OS (atacante)



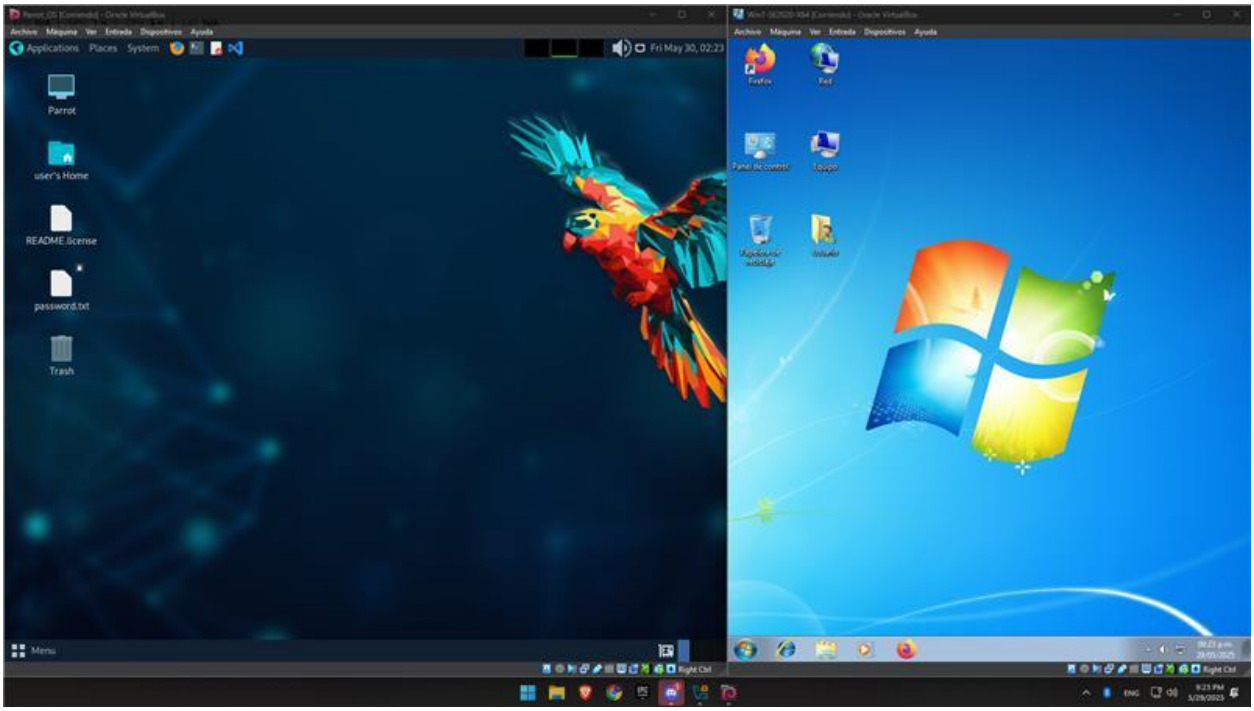
Nota: Parrot Os será utilizada como la maquina atacante.

Figura 3 - Recursos asignados a Win7 (objetivo)



Nota: Windows 7 es la maquina objetivo, a esta se la ha deshabilitado el firewall como medida que permita la explotación de vulnerabilidades con autorización del tutor.

Figura 4 - Escritorios de las maquinas virtuales.



Nota: Estas dos maquinas virtuales componen el banco de trabajo que se utilizará para las pruebas de penetración.

Proceso legal y ético estipulado en acuerdo con CyberFort:

Al leer el acuerdo se encuentra que CyberFort Technologies es plenamente consciente de que adelanta actividades ilegales y conmina a los nuevos empleados a ser cómplices pues les adelanta que desde el primer momento se están obteniendo datos confidenciales por medios abusivos: "*Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal*"

Por otro lado, se evidencia la práctica del espionaje, mal llamado, "datos de chuzadas" que es la interceptación de información por medios tecnológicos: "*Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos,*

nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

CyberFort Technologies, trata de asegurarse de que no se denuncie a la organización por un agente interno pues expresa que "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros*." Y "*Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas*." pues si alguien se atreviera a denunciar, le endilgaría la completa responsabilidad de todo aquello que se le pudiera allanar, esta persona debe "*Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento*."

Otras formas de persuasión al candidato para que no denuncie son "*a la parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de CyberFort Technologies.*" Aunque el uso de la palabra "ilegal" lo hace evidente, para efectos del presente ejercicio se nota un afán de la compañía por blindarse bajo la premisa de conminar a las personas a respetar la confidencialidad de la empresa aun a expensas de sus derechos y deberes penales: "*En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies.*" Pues nadie está obligado a declarar en contra de sí mismo o de algún familiar hasta el cuarto grado de consanguinidad.

Artículos de la ley 1273 que se vulneran en el presente acuerdo:

Teniendo en cuenta que la compañía hace una clara referencia a las “chuzadas” se estaría violando los artículos**:**

269A: *Acceso abusivo a un sistema informático*. *El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes*.

269C: *Interceptación de datos informáticos*. *El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.* (Ley 1273, 2009)

Dado que CyberFort Technologies obtiene información confidencial por medio de los procesos laborales sin previa autorización de los aplicantes, estaría faltando al artículo *269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.* (Ley 1273, 2009)

Los delitos anteriores se verían agravados por abusar del proceso de contratación para hacerse con información a lucro propio, y al contratar a un profesional, valerse de este para

cometer delitos compartiendo o transfiriendo la responsabilidad: Artículo *269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:*

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

5. Obteniendo provecho para sí o para un tercero.

7. Utilizando como instrumento a un tercero de buena fe.

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos. (Ley 1273, 2009)

¿Existiendo procesos poco confiables ¿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?

Tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

No aplicaría a este trabajo y por el contrario denunciaría a la empresa CyberFort Technologies ya que el contrato ofrecido y el código de ética COPNIA van en perfecta contravía. Dejando de lado la parte penal, el riesgo es demasiado alto sabiéndose responsable de los delitos a los que se expone como cómplice y que tomar partido en tan nefasto arreglo puede acarrear la perdida del titulo profesional y la inhabilidad vitalicia para ejercer la profesión. COPNIA es claro en cuanto a los deberes de los profesionales a no ofrecer o aceptar trabajos que van en

contra de las disposiciones legales y a no participar de beneficios ilegales con el objeto de obtener designaciones profesionales o la encomienda de trabajo profesional. (Ley 842, 2003)

Acceso a información sensible de clientes durante auditorías de seguridad y garantías de no explotación indebida de este acceso:

Las empresas, al igual que los usuarios de sistemas tecnológicos deberían de seguir el principio de mínimo privilegio, definido como brindar al profesional, o empresa en este caso, el acceso a información y recursos mínimos para poder llevar a cabo su tarea sin comprometer los resultados ni la ciberseguridad de la compañía (Vaideeswaran, 2025).

Se deben de implementar mecanismos de supervisión y control que garanticen el actuar ético de los profesionales en ciberseguridad, estos mecanismos pueden ser implementados a nivel de software registrando en los logs cada herramienta y aplicativo usado, que usuario fue el que utilizó el recurso, por cuanto tiempo y con qué finalidad. Adicionalmente se deben de implementar protocolos restrictivos en cuanto al uso de dispositivos de uso personal como teléfonos, laptops, memorias, cámaras y documentar, en caso de necesitarse, los 5 que's (quien, cuando, porque, donde y como) va a usar el dispositivo mencionado. Se deben de llevar a cabo capacitaciones que refuercen la ética e implementar auditorías a los procesos en pro de encontrar fortalezas y debilidades, generar acciones de mejora y reportar las lecciones aprendidas.

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

Los gobiernos y organizaciones deben actuar con rapidez, transparencia y firmeza cuando se descubre que una empresa de ciberseguridad contratada ha cometido actos de ciber espionaje. Este tipo de delito y abuso no solo pone en riesgo la seguridad nacional o empresarial, sino que también socava la credibilidad de toda la industria de ciberseguridad.

Se debe de adelantar una auditoría forense independiente que involucre a un tercero confiable e imparcial para analizar el alcance del espionaje, qué datos fueron comprometidos y cómo se realizó.

La colaboración con autoridades judiciales y de inteligencia es vital para determinar si hay implicaciones penales o amenazas a la seguridad nacional.

Proceso judicial: Si se confirma el espionaje, la empresa debe enfrentar cargos penales y civiles.

Los contratos que se encuentren en vigencia deben de ser cancelados inmediatamente se conozca de cualquier delito.

Si el caso es grave, se debe de considerar incluir a la empresa en listas negras y clausurarla temporalmente, se debe de limitar su participación en futuras contrataciones públicas.

La notificación a partes afectadas es una práctica obligatoria en muchos países, entonces de debe de verificar que se informe a clientes, usuarios, empleados u otras entidades comprometidas.

Llevar a cabo una rueda de prensa con comunicado oficial donde se expliquen los hechos, las medidas adoptadas y los pasos a seguir.

Los proveedores actuales deben de pasar por un proceso de auditoria para revisar otros contratos de ciberseguridad con el fin de evitar riesgos similares.

Como lección aprendida y acción de mejora se propone incluir cláusulas más estrictas sobre ética, monitoreo y sanciones en los contratos.

Implementar programas de vigilancia y monitoreo continuo para asegurar que los proveedores cumplan con estándares de seguridad y ética.

Crear programas de capacitación y concientización en toda la cadena organizacional sobre estándares de seguridad y ética.

Por último, se debe de sancionar comercialmente con multas y, de haber afectación estatal extranjera, se deben de aplicar sanciones diplomáticas.

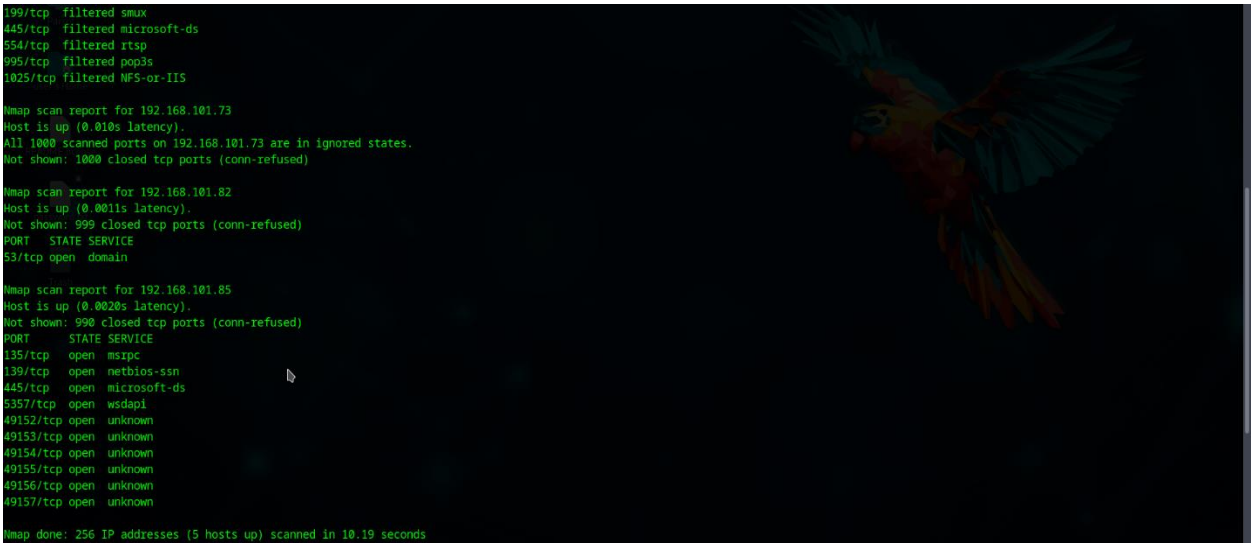
Descripción específica de las herramientas (software) utilizadas para llevar a cabo las pruebas de penetración con rnfoque Red team:

Para la fase de escaneo se utiliza la herramienta Nmap:

Procedemos a escanear la red local con Nmap, esto se hace para descubrir a la víctima que será atacada, para esto ejecutamos el comando `Nmap 192.168.101.*` el cual descubrirá todos los equipos desprotegidos entre las direcciones IP 192.168.101.1 y 192.168.101.254. (Lyon, 2022)

*Figura 5 - salida del comando nmap 192.168.101.**

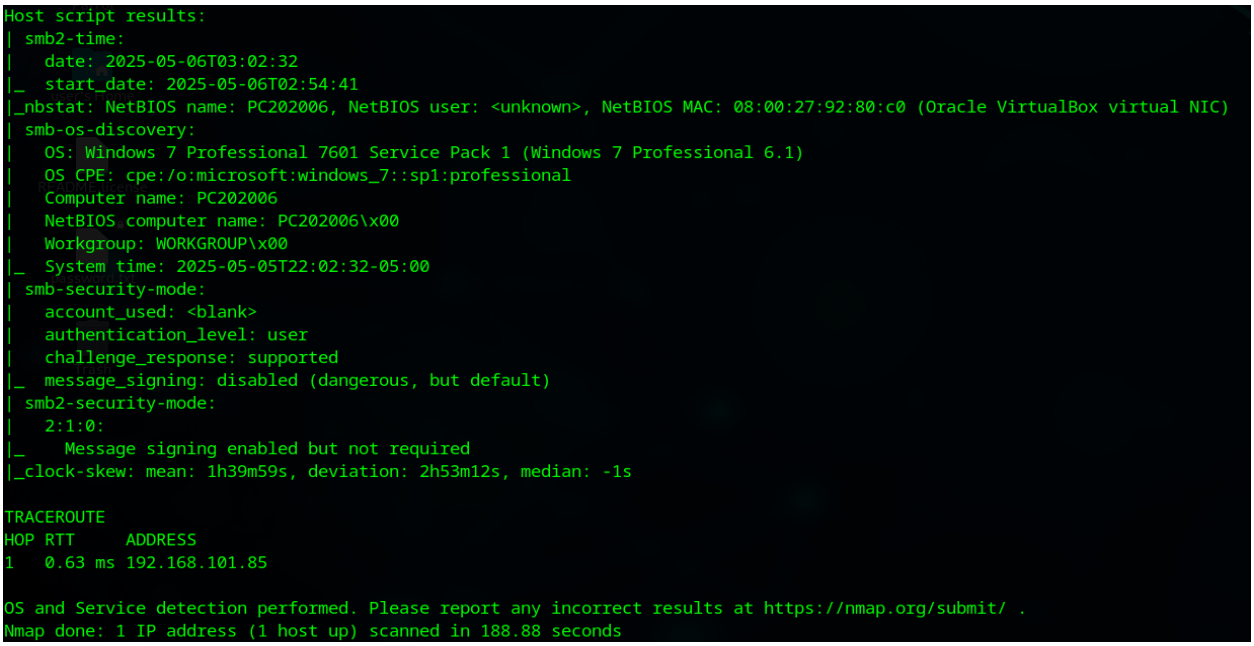
Figura 6 - Reconocimiento de la maquina objetivo en 192.168.101.85



Encontramos asi que en la direccion 192.168.101.85 hay una maquina cuyo puerto 445 tiene alojado el servicio de microsoft-ds, lo cual es congruente con los datos suministrados para el Pentest; asi que procedemos a hacer un escaneo mas agresivo y enfocado usando el comando `Nmap 192.168.101.85 -sV -A -O -T4` (sV: para conocer la version del servicio, A: permite detectar el sistema operativo, version, traceroute y el escaneo de scripts, O: para detectar el SO, T4: para que el escaneo sea mas agresivo y rapido). (Lyon, 2022)

Figura 7 - Salida del comando nmap 192.168.101.85 -sV –A –O –T4

Figura 8 - Version de OS de la maquina objetivo



Habiendo identificado los puertos abiertos del sistema Microsoft Windows 7 / 2008 / 8.1 y sus versiones, pasamos a la siguiente fase. Salta a la vista que el smb-security-mode tiene configuraciones (dangerous, but default)

Para la fase de enumeración se utiliza el CVE de MITRE y la página del propietario para conocer las posibles vulnerabilidades.

Figura 9 - Pagina del CVE de MITRE: vulnerabilidades de windows 7 (The MITRE Corporation, 2025)

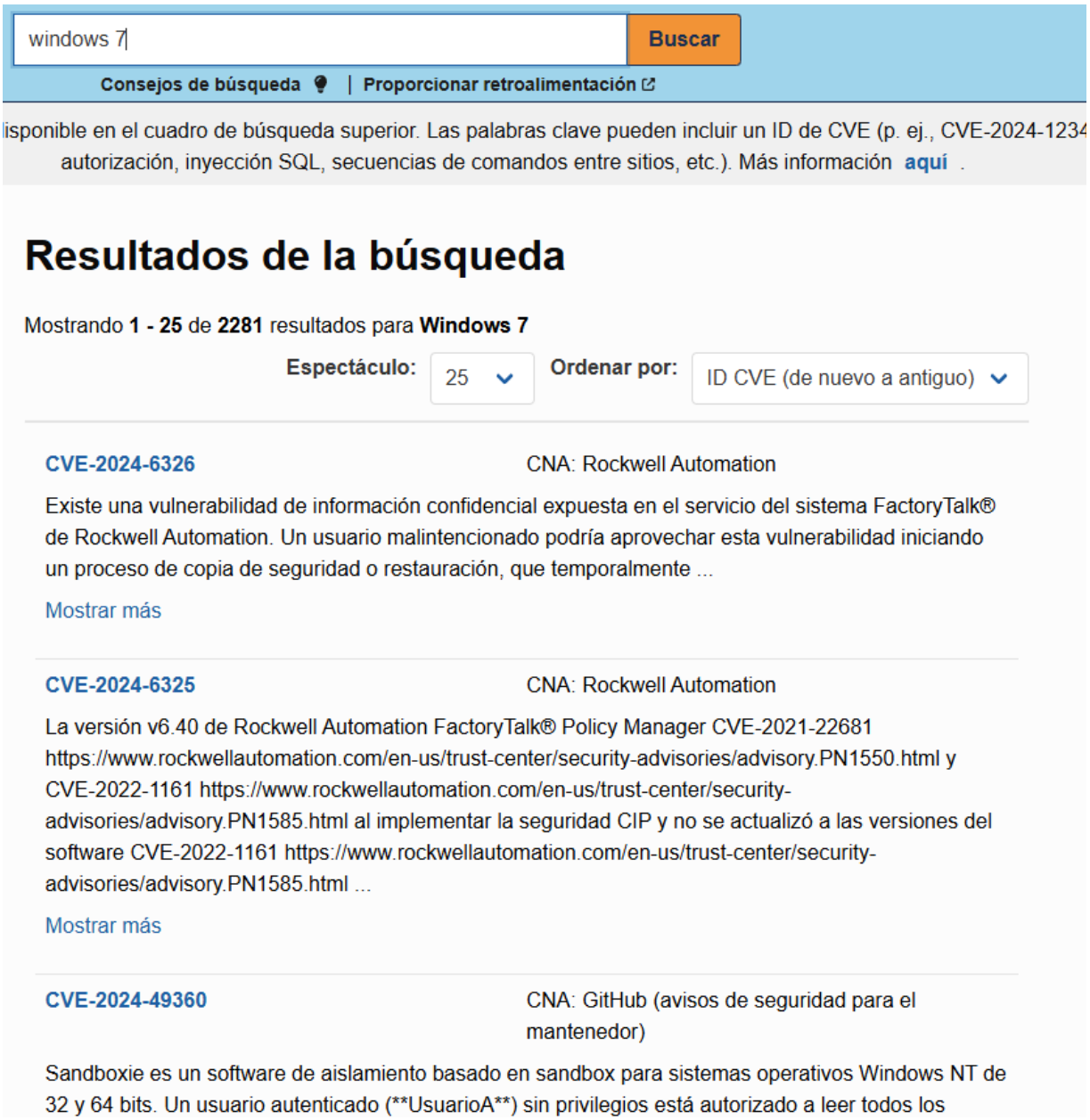
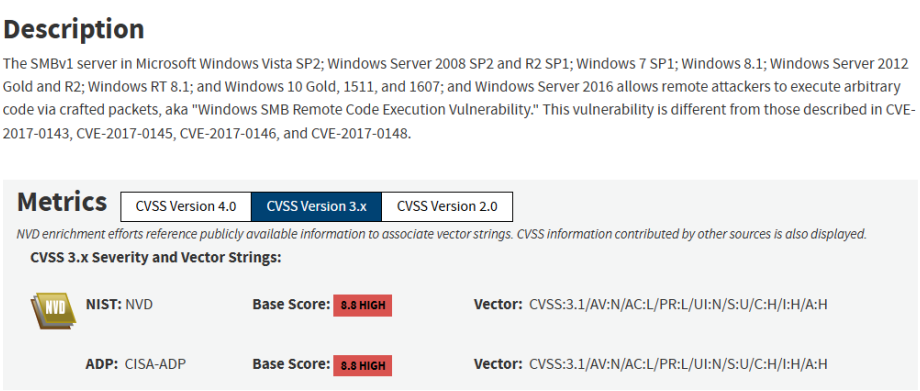


Figura 10 - CVE 2017 - 0144 (The MITRE Corporation, 2025)



Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

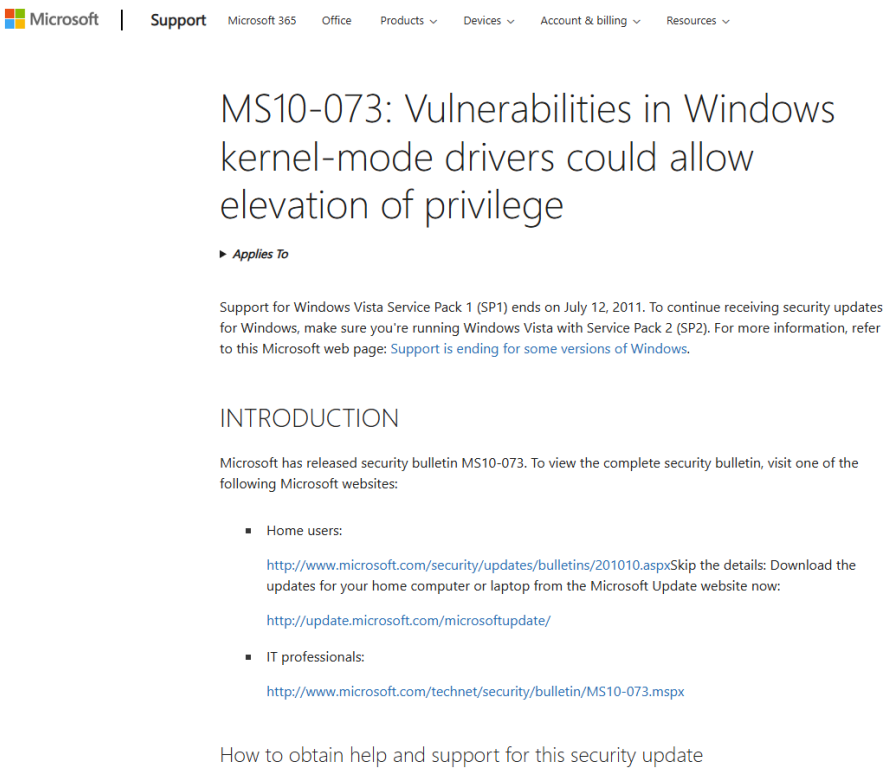
CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
ADP: CISA-ADP	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on

Figura 11 - Support site de Microsoft: MS10-073 vulnerabilities report.



Microsoft | Support Microsoft 365 Office Products Devices Account & billing Resources

MS10-073: Vulnerabilities in Windows kernel-mode drivers could allow elevation of privilege

▸ *Applies To*

Support for Windows Vista Service Pack 1 (SP1) ends on July 12, 2011. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, refer to this Microsoft web page: Support is ending for some versions of Windows.

INTRODUCTION

Microsoft has released security bulletin MS10-073. To view the complete security bulletin, visit one of the following Microsoft websites:

- Home users:

  http://www.microsoft.com/security/updates/bulletins/201010.aspxSkip the details: Download the updates for your home computer or laptop from the Microsoft Update website now:

  http://update.microsoft.com/microsoftupdate/

- IT professionals:

  http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx

How to obtain help and support for this security update

Figura 12 - Boletín de seguridad de Microsoft para la vulnerabilidad MS17-010 (Micorsoft, 2025)

Figura 13 - Versiones de Windows 7 vulnerables a MS17-010 (Microsoft, 2025)

Windows 7							
Windows 7 for 32-bit Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for 32-bit Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646
Windows 7 for x64-based Systems Service Pack 1 (4012212) Security Only[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	None
Windows 7 for x64-based Systems Service Pack 1 (4012215) Monthly Rollup[1]	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3212646

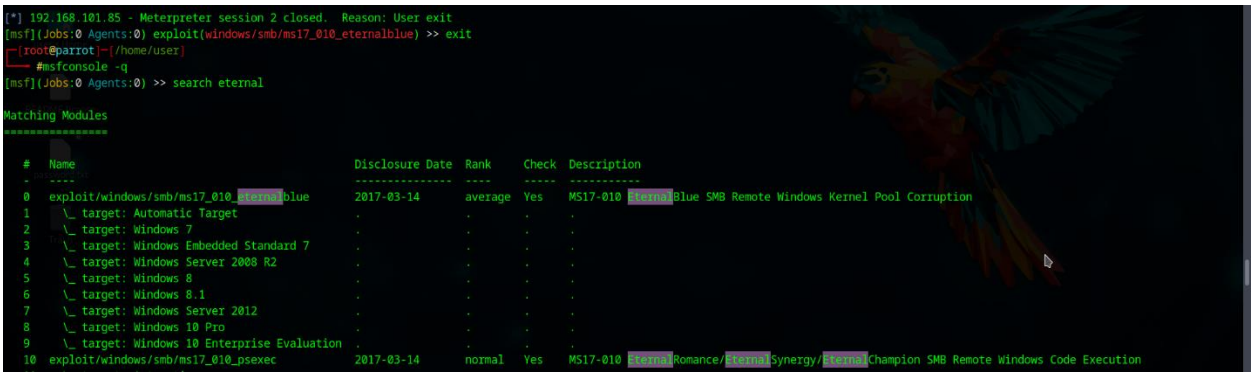
Al identificar las vulnerabilidades posibles se pasa a la siguiente fase, la explotación.

Para esta fase se usará la herramienta Metasploit, y se verifica que la herramienta cuente con el exploit a las vulnerabilidades enumeradas en la fase anterior y se encuentra que MS17-010 es explotable:

Accedemos a la herramienta Metasploit usando el comando msfconsole “MSF= MetaSploit Framework”.

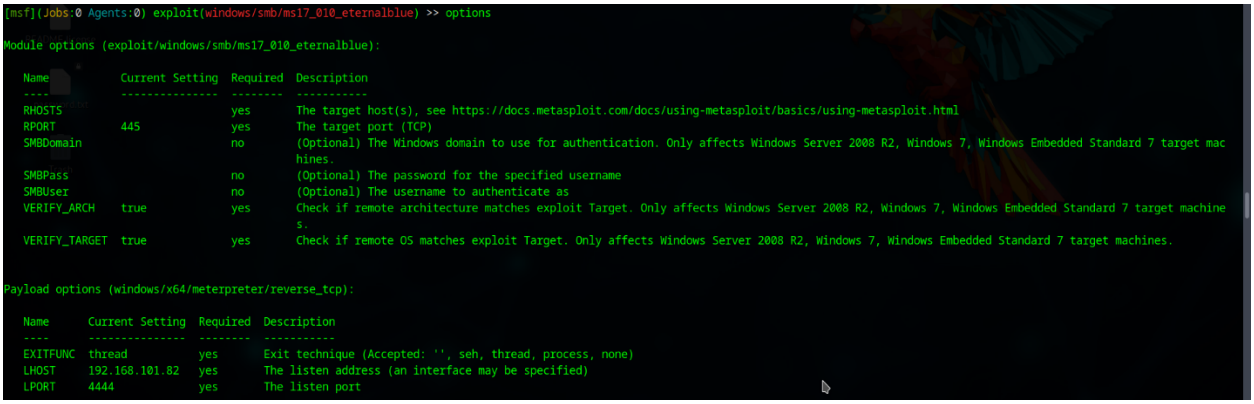
Buscamos la vulnerabilidad usando el comando `search eternal blue o search MS17-010.` Se define entonces realizar el proceso de hacking automático (usando scripts):

Figura 14 - msfconsole search Eternal Blue (MS17-010)



Se hace un listado de las opciones que tiene el exploit elegido y se contrasta con la información recolectada en fases anteriores: RHOST, RPORT y payload según el CVE/Microsoft.

Figura 15 - Salida del comando "options" para el exploit MS17-010



Como el puerto 445 está predeterminado en el exploit, iniciamos por hacer un pentest a este puerto/protocolo especifico luego de verificar que efectivamente está abierto en la maquina victima:

Figura 16 - configuracion de las opciones RHOST y payload de MS17-010

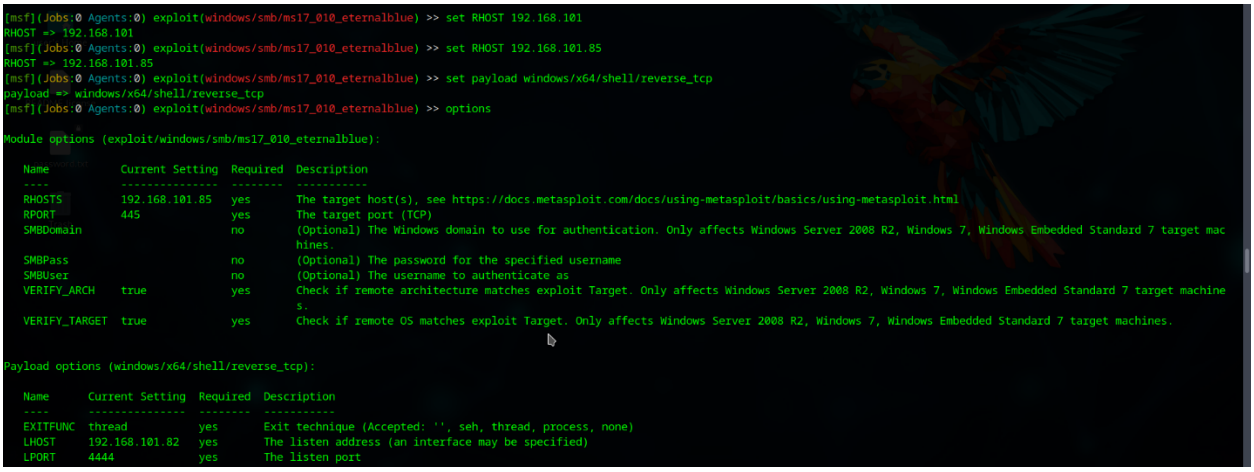
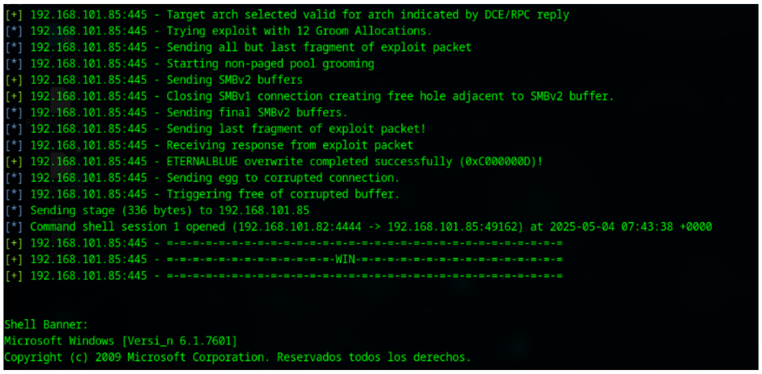


Figura 17 - Ejecución exitosa del exploit



Al ejecutar el exploit obtenemos un resultado favorable a este ataque observando el banner "=-=-WIN-=-="

En este punto se tiene control de la maquina víctima y podemos reunir mucha más información que nos permita elevar privilegios o realizar un ataque persistente o backdoor:

Figura 18 - creación de un directorio en la maquina objetivo.

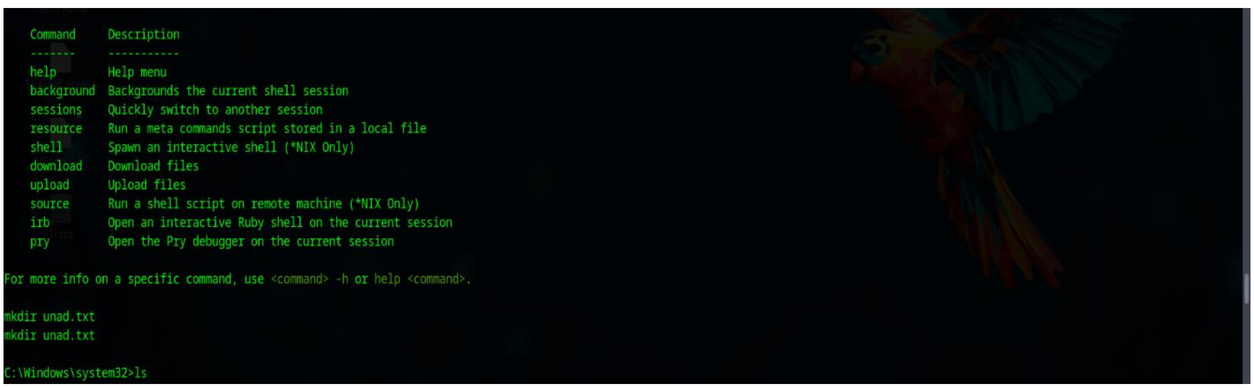


Figura 19 - Verificación de creación de directorio.

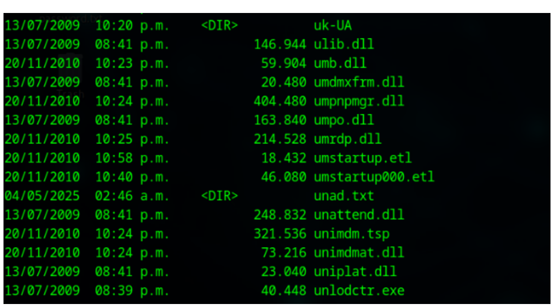


Figura 20 - Reconocimiento del "path".

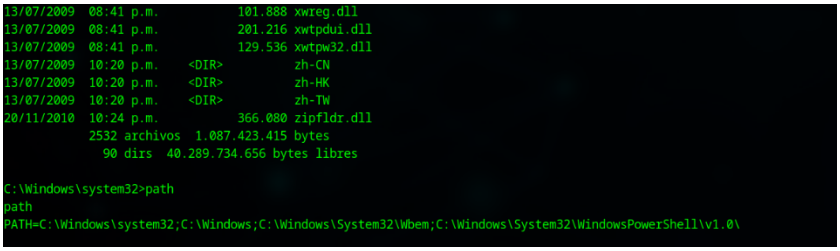


Figura 21 - Verificación de acceso exitoso.

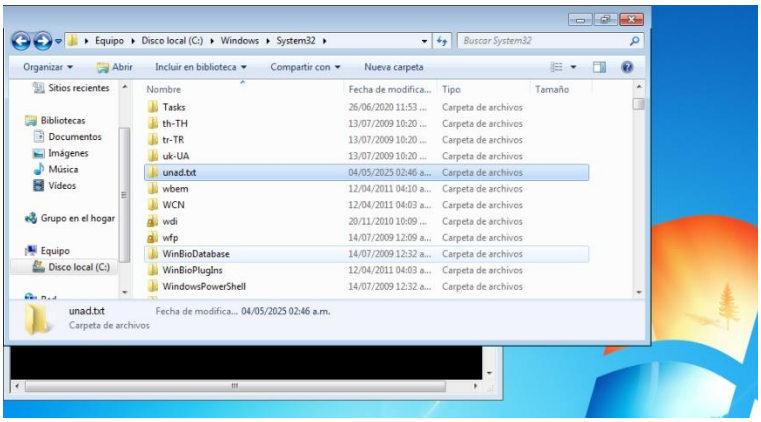
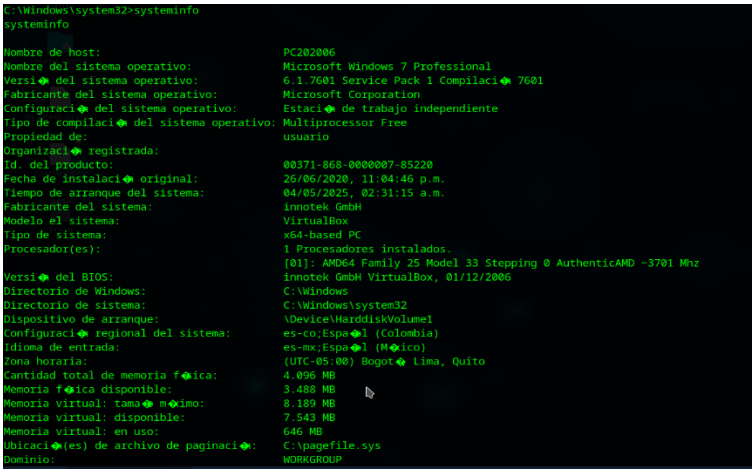


Figura 22 - Salida del commando systeminfo



Se procede a crear un usuario y asignarle privilegios de administrador como parte de la investigación del caso forense “escenario 3” para confirmar la hipótesis inicial:

Figura 23 - comando net user francisco_sanchez /add correcto

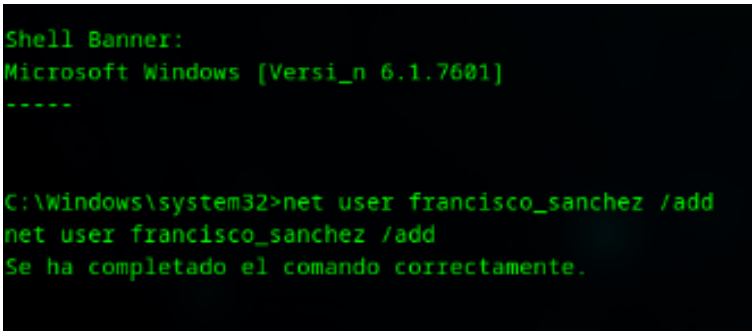
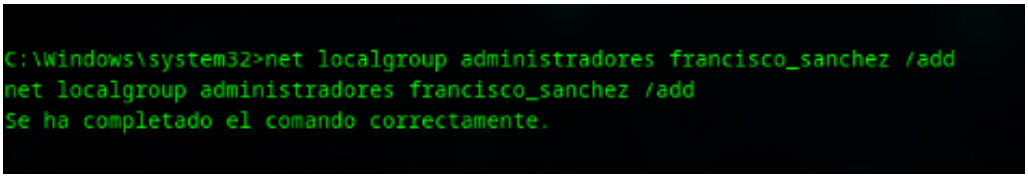
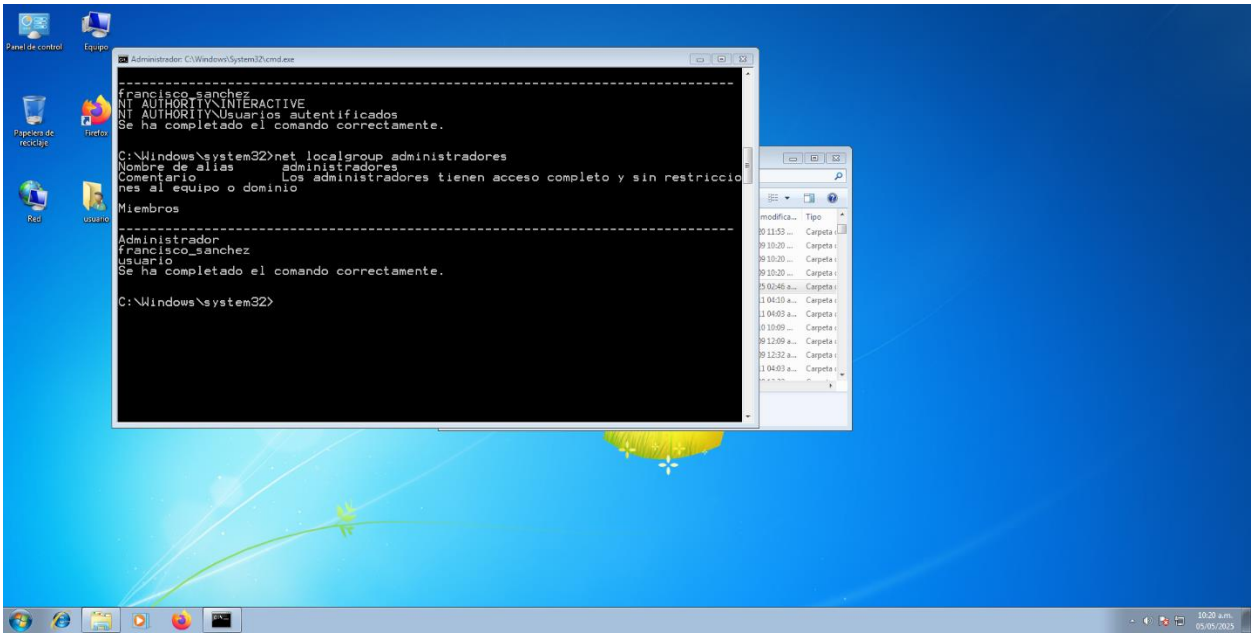


Figura 24 - comando net localgroup administradores francisco_sanchez /add correcto



Se verifica entonces en la maquina objetivo que las configuraciones externas se hayan hecho correctamente según la hipótesis inicial y se evidencia que el pentest fue exitoso:

Figura 25 - Exploit y elevación de privilegios exitosos.



Descripción de datos e información del anexo que fueron de ayuda para identificar el fallo de seguridad específico vulnerado en la máquina Windows:

Que es un ataque con fuga de información, esto ayudó a reducir los posibles protocolos usados a unos cuantos, como ftp, ssh, tcp, smb, etc.

Que la maquina víctima es Windows, es un dato vital para saber qué se está buscando al escanear las redes.

Que tiene asociado un exploit que puede terminar en un acceso a través de Shell, reduciendo aún más los protocolos y puertos esperados en el ataque. Incluso este dato fue determinante al elegir el exploit a ejecutar.

escalación de privilegios: Saber que el ataque puede generar una escalación de privilegios permite saber que vulnerabilidad se está explotando y que técnica se está usando para este fin.

creación de un usuario tipo administrador: El objetivo del pentest fue determinado por este dato, al ser capaz de recrear este punto, se da por terminado el pentest pues el ataque y los vectores fueron eficaces.

Herramientas utilizadas para la identificación de los fallos de seguridad de la "máquina Windows" y el puerto que abre la aplicación específica en el anexo:

Se utilizo la herramienta NMAP en la identificación de protocolos, puertos y sistemas operativos.

Se contrastó la información con el CVE de MITRE y los boletines de seguridad de Microsoft para conocer las vulnerabilidades asociadas.

Se usó Metasploit para verificar si la maquina era vulnerable y se ejecutó el pentest siguiendo estos hallazgos.

El puerto que abre la aplicación específica del anexo es el puerto 445: SMB.

el ataque afecta a la máquina (Windows) de la siguiente manera:

Se escanea el puerto 445 y el atacante identifica que este puerto (usado por el protocolo SMB) está abierto en la máquina Windows 7.

Se realiza el envío de un script malicioso especialmente diseñado que explota la forma en que Windows maneja los mensajes del protocolo SMB (prácticamente desborda el búfer en el kernel). Esto lo logra al manipular la memoria del kernel y así sobrescribir partes de la misma, lo anterior permite ejecutar código a nivel del sistema operativo.

Sin necesidad de que usuario interactúe, el atacante puede ejecutar comandos remotamente como net localgroup admin /add, otorgando privilegios a usuarios fraudulentos en Windows. (Microsoft, 2025)

Análisis Blue team para la contención de ataques informáticos.

Ante un ataque en tiempo real en un sistema operativo Windows, bajo las condiciones establecidas por CyberFort Technologies y haciendo uso exclusivo de herramientas con licencia GPL o gratuitas, como integrante del Blue Team se deben seguir pasos técnicos rigurosos para contener el ataque, investigar su naturaleza y minimizar el impacto sobre la organización. A continuación, se describe una estrategia operativa dividida en fases con enfoque técnico, a nivel de sistema operativo y de red:

Se simuló un ataque en tiempo real contra un equipo que ejecutaba el sistema operativo Windows 7. El ataque fue posible mediante la explotación de una vulnerabilidad crítica conocida como MS17-010, más comúnmente asociada con el exploit EternalBlue, este fue desarrollado por la NSA y filtrado públicamente en 2017. Esta vulnerabilidad permite que un atacante tome control del sistema de forma remota, sin necesidad de autenticación, mediante el protocolo de red SMBv1.

Durante el análisis del simulacro se identificaron los siguientes indicadores:

- Conexiones inusuales desde IPs externas al puerto 445/TCP.
- Procesos ejecutados sin interacción del usuario.
- Actividad sospechosa en memoria y cambios en usuarios y privilegios.

Herramientas a utilizar para contener el ataque: Wireshark; para escaneo de redes e identificación de conexiones sospechosas, Firewall de Windows; es una herramienta nativa del sistema operativo Windows que deshabilita puertos vulnerables como el 445 en este caso, Nmap; para escanear otras maquinas vulnerables y acortar la superficie del ataque, YARA; Identifica si

el exploit ha cargado payloads persistentes para eliminar archivos maliciosos detectados o reportarlos para análisis,

Indagación primaria y reacción ante un ataque en tiempo real.

Lo primero que se indagaría en caso de encontrar un ataque en tiempo real sería: confirmar la legitimidad del ataque (Detección y Validación) con el objetivo de evitar falsos positivos y enfocar los recursos correctamente. Esto lo llevaría a cabo mediante la verificación de alertas generadas por el SIEM, contrastando la información con los Logs de los endpoints, firewalls, EDR, WAF, entre otras herramientas que se tuvieran a disposición.

En caso de que esta información ya se tenga disponible, lo primero que se llevaría a cabo sería la contención inmediata del ataque, detener la propagación sin afectar gravemente la operación es la principal motivación de esta decisión. Por lo anterior se debe de aislar el host comprometido de la red mediante el EDR o los switches. Cortando conexiones salientes sospechosas con el firewall. Adicionalmente se deben de suspender credenciales comprometidas o sesiones activas complementando esto con la detención de procesos maliciosos identificados.

Medidas de hardenización para evitar que el ataque no se repita teniendo en cuenta el ataque simulado desde el ejercicio de Red team.

Lo primero que se haría es revisar los boletines de seguridad de Microsoft y CVE-Mitre para implementar los “upgrades”, parches o actualizaciones que mitiguen la vulnerabilidad. Para el caso de la vulnerabilidad explotada, Microsoft propone en su boletín:

Actualización de seguridad para Microsoft Windows SMB Server (4013389)

Publicado: 14 de marzo de 2017

Versión: 1.0

Resumen ejecutivo

Esta actualización de seguridad resuelve vulnerabilidades en Microsoft Windows. La más grave de las vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Bloque de mensajes de Microsoft Server 1.0 (SMBv1).

Esta actualización de seguridad es crítica para todas las versiones compatibles de Microsoft Windows. Para obtener más información, consulte la sección Clasificación de gravedad de vulnerabilidad y software afectado.

La actualización de seguridad aborda las vulnerabilidades mediante la corrección del modo en que SMBv1 controla las solicitudes especialmente diseñadas. (Microsoft, 2017)

Adicionalmente a lo anterior el firewall nativo de Windows demostró ser de gran importancia por lo que contar con esta herramienta configurada, actualizada y activa es una medida que contribuye a que el ataque en mención no se repita.

Diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos

Un equipo Blue team es un conjunto de profesionales que evalúan la seguridad de una organización de manera proactiva (seguridad defensiva) esto se hace generalmente de la mano de equipos estratégicos Red team (seguridad ofensiva) que se encargan de buscar activamente vulnerabilidades explotables y riesgos latentes que son informados al Blue team para que estos busquen la manera de mitigar o reducir el riesgo de exposición, otras funciones son las de monitorear redes y eventos de seguridad, fortalecimiento de infraestructuras (hardening), gestión de vulnerabilidades (parcheo de softwares), desarrollo de alertas y reglas de detección y

respuesta automática, simulación de ataques internos; llamado purple teaming junto al Red team, Capacitación de funcionarios.

Mientras que un ERI (equipo de respuesta de incidentes) es un conjunto multidisciplinario de profesionales con conocimientos técnicos especializados cuyo principal cometido es la gestión de incidentes de seguridad, el enfoque es mayoritariamente reactivo,

aunque se han venido definiendo etapas proactivas como: planificación, valoración de activos y riesgos, lecciones aprendidas y métricas e indicadores. (Garcia, 2022, págs. 68-70)

Tabla 1 - Diferencias Blue Team vs ERI

Característica	Blue Team	Equipo de Respuesta a Incidentes
Enfoque	Proactivo (prevención y defensa)	Reactivo (respuesta y contención)
Momento de actuación	Antes/durante un ataque	Durante/después de un ataque
Actividades principales	Monitoreo, hardening, detección	Análisis, contención, recuperación
Herramientas comunes	SIEM, EDR, firewalls, escáneres	Forense, análisis de red, Autopsy, Volatility.
Perfil del equipo	Analistas SOC, ingenieros en ciberseguridad, administradores	Analistas forenses, multidisciplinar, Sistema comando de incidentes

Nota: Esta tabla muestra las principales diferencias entre los equipos Blue Team y ERI Fuente: Propia

Uso de CIS "Center For Internet Security" dentro de un equipo Blue team.

Si dentro de un equipo Blue Team se indica la necesidad de trabajar con CIS (Center for Internet Security), la implementación de los controles de seguridad estandarizados y buenas prácticas de defensa informática en los sistemas y redes de la organización sería un buen primer objetivo.

Los “CIS Controls” son un conjunto de 18 controles de alta prioridad, son prácticos tienen el objetivo de ayudar a defenderse contra las amenazas más comunes. Estos son usados para: Establecer una línea base de seguridad, priorizar acciones defensivas, auditar el estado de la seguridad actual, guiar el hardening de sistemas.

Por ejemplo: implementar el CIS Control 4 (que trata sobre la gestión de configuraciones seguras) asegura que los sistemas operativos y aplicaciones se configuren correctamente, reduciendo posibles vectores de ataque. (Center for Internet Security, 2025)

Lo anterior es importante porque atiende varios puntos clave: permite cumplir con las normativas legales locales e internacionales, estos controles están priorizados y son fáciles de entender; además de tener un costo-beneficio importante para las MiPymes, permitiendo que estas demuestren tener ciertos estándares de seguridad importantes en el mercado. Los “*CIS 18*” son una buena base para empezar a construir el programa de ciberseguridad de la organización.

Funciones y características principales de lo que es un SIEM.

Los SIEM son sistemas que tienen las siguientes funciones como mínimo:

Agregar información: Consolida la información de múltiples fuentes en un intento por evitar que se pierdan eventos importantes. Algunas fuentes de información pueden ser: dispositivos de red, servidores, bases de datos, logs, etc.

Correlación de eventos: Enlaza entre si eventos que comparten atributos comunes y que se extraen de diferentes fuentes de información para convertirlos en información valiosa.

Generar alertas: Es la notificación a un conjunto de interesados sobre los sucesos emergentes. La notificación se puede realizar por correos, trap hosts o desde un panel de control (dashboard).

Tener un *Dashboard*: Los SIEM permiten procesar datos y representarlos gráficamente facilitando el análisis de patrones y desvíos con los estándares de utilización establecidos.

Aportar al *Compliance*: automatizan el proceso de recolección de datos para generar informes que serán entregados al gobierno TI o a la auditoria.

Retención: El almacenamiento de datos por largos periodos de tiempo es pilar fundamental del cumplimiento normativo y de los procesos de análisis forense.

Análisis forense: Permite realizar búsquedas centralizadas a través de logs de diferentes nodos según criterios establecidos por el ERI evitando procesos manuales que consumen tiempo. (Garcia, 2022, pág. 109)

Figura 26 - Dashboard SIEM Splunk en Microsoft 365.

Nota: Se presenta a modo de ejemplo el dashboard del SIEM Splunk en Windows 365. Fuente: https://www.splunk.com/en_us/blog/platform/dashboard-studio-level-up-your-app-with-dashboard-studio.html

Definición de herramientas de contención de ataques informáticos “hardware o software”.

Endpoint Detection and Response (EDR), herramientas: Microsoft Defender for Endpoint, CrowdStrike Falcon

Incluyen capacidades de detección, pero los EDR son también herramientas de contención efectivas. Permiten aislar, de manera remota, un equipo infectado de la red, detener procesos maliciosos activos, eliminar archivos sospechosos y bloquear conexiones. Esta última siendo clave para evitar que una amenaza se propague a través de la red interna. Los EDR también soportan scripts que ejecutan acciones defensivas inmediatas. (Micorsoft, 2025)

Next Generation Firewalls (NGFW), herramientas: Palo Alto, Fortinet, Check Point

Un NGFW se configura para bloquear tráfico entrante o saliente específico, terminar sesiones activas y limitar el acceso a determinados servicios, puertos o direcciones IP en tiempo real. En caso de un ataque, el firewall puede aplicar reglas dinámicas para detener la comunicación, evitando así que el atacante mantenga el control del sistema o exfiltre información. (Check point, 2025)

Network Access Control (NAC), herramientas: Cisco ISE, Aruba ClearPass

Permiten controlar los accesos a la red, basándose en políticas definidas. Al detectar un comportamiento anómalo, el NAC puede mover el host comprometido a una red para "cuarentena", denegar el acceso a recursos críticos o simplemente desconectarlo por completo. Esta contención, física o lógica, evita que una amenaza escale lateralmente dentro de la infraestructura protegida. (Cisco Systems, Inc., 2025)

Estas herramientas pueden actuar en distintas capas y se aconseja su combinación como medida clave para una estrategia de defensa efectiva frente a ataques informáticos.

Conclusiones.

La respuesta efectiva ante un ataque en tiempo real depende en gran medida de la preparación y reacción técnica inmediata del ERI. La correcta identificación del vector de ataque, junto con acciones como el aislamiento del sistema afectado, el análisis de tráfico y el bloqueo de servicios vulnerables, permite mitigar rápidamente el impacto del incidente y evitar su propagación en la red corporativa.

El uso de herramientas de código abierto con licencias GPL permite realizar acciones de contención, análisis forense y endurecimiento de sistemas sin necesidad de inversiones económicas altas. Herramientas como Wireshark, Nmap, Windows firewall y YARA pueden ser utilizadas en la detección actividad maliciosa, bloqueo de vectores de ataque y reducción de la superficie de ataque, destacando su usabilidad en entornos con recursos limitados.

El fortalecimiento de la seguridad organizacional no solo requiere herramientas, sino también el uso de estándares y marcos de referencia como son los CIS Benchmarks y la correcta implementación de soluciones como SIEMs. Además, comprender la diferencia entre los roles del Blue Team, Red Team y el equipo de respuesta a incidentes permite establecer flujos de trabajo eficientes para la defensa, análisis y recuperación ante amenazas informáticas.

Recomendaciones

Implementar programas de capacitación constantes en ciberseguridad ofensiva y defensiva, adaptados a los diferentes roles dentro del equipo de TI de las organizaciones.

Establecer estrategias de defensa en profundidad combinando herramientas EDR, firewalls, NAC y soluciones SIEM, entre otras según las necesidades particulares identificadas.

Asegurar el cumplimiento de marcos legales y estándares como ISO 27001 y CIS Controls para garantizar una protección integral, la elección de cada marco de trabajo debe de hacerse al evaluar cuidadosamente los objetivos y las necesidades identificadas por el gobierno TI.

Fortalecer la colaboración entre Red Team y Blue Team a través de ejercicios de Purple Teaming en un ciclo continuo que permita la identificación de vulnerabilidades de manera proactiva y eficiente.

Incluir cláusulas éticas y de responsabilidad en los contratos con proveedores de ciberseguridad para prevenir posibles abusos o espionaje, así como el fortalecimiento del actuar ético de empleados y organizaciones.

Bibliografía

Center for Internet Security. (2025, 05 15). *cisecurity.org*. Retrieved from Center for Internet Security web site: https://www.cisecurity.org/controls

Check point. (2025). *Check point.* Retrieved from Check point web site: https://checkpoint.com/es/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/

Cisco Systems, Inc. (2025). *Cisco Systems, Inc.* Retrieved from Cisco web site: https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html

Congreso de Colombia. (2003, 03 de octubre). *Ley 842.* Diario Oficial 45.340. Retrieved from https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Congreso de Colombia. (2009, 05 de enero). *LEY 1273 DE 2009.* Codigo penal. Retrieved from https://www.ins.gov.co/Transparencia/Docs/Ley-1273-de-2009.pdf

CVE. (2025). *About us: CVE*. Retrieved from CVE Web site: https://www.cve.org/About/Overview

EC-Council. (2022, 03 28). *EC-Council*. Retrieved from EC-Council web site: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/

Exploit Database. (2025). *About the Exploit Database*. Retrieved from Exploit-db web site: https://www.exploit-db.com/about-exploit-db

Fernandez, R. (2022, 10 23). *eSecurity Planet*. Retrieved from eSecurity Plantet website: www.esecurityplanet.com/networks/penetration-testing-phases/

Garcia, M. M. (2022). *Gestión de incidentes de ciberseguridad.* Madrid: Ra-Ma editorial.

Lyon, G. “. (2022). *Nmap Network Scanning.* Nmap Software LLC.

metasploit. (2025, 05 28). *Rapid 7 metasploit*. Retrieved from Rapid 7 metasploit website: https://www.metasploit.com/

Micorsoft. (2025). *Microsoft.* Retrieved from Seguridad de Microsoft: https://www.microsoft.com/es-es/security/business/security-101/what-is-edr-endpoint-detection-response?msockid=15cce03f362867bf2ee7f5ea3787663a

Microsoft. (2017). *Microsoft*. Retrieved from Microsoft support web site: https://support.microsoft.com/

Microsoft. (2025). *Microsoft*. Retrieved from Microsoft support web site: https://support.microsoft.com/

Nmap. (2025). *NMAP.ORG*. Retrieved from NMAP web site: https://nmap.org/

OpenVAS. (2025). *Greenbone OpenVAS*. Retrieved from Greenbone OpenVAS website: https://openvas.org/

The MITRE Corporation. (2025). *CVE*. Retrieved from MITRE CVE website: www.cve.mitre.org

Vaideeswaran, N. (2025, 01 08). *Crowdstrike*. Retrieved from Crowdstrike website: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/principle-of-least-privilege-polp/

Adjuntos.

Link: https://youtu.be/kZIVntAYfBM