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

Integrante No. 1

Ricardo Morales Morales

John Freddy Quintero

Director de Curso

Universidad Nacional Abierta y a Distancia (UNAD)

Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI

Especialización Seguridad Informática

Red Team & Blue Team

CEAD Medellín

04 de Abril del 2021

RESUMEN

La organización WhiteHouse Security, es una compañía de gran prestigio, al ser la responsable de asesorar a múltiples empresas en los diferentes procesos de ciberdefensa y ciberseguridad, por lo tanto, le ha permitido posicionarse como pionera a nivel mundial en servicios de consultoría de seguridad informática. Durante el último tiempo ha tenido un incremento en la demanda de sus servicios, por eso tomó la decisión de reclutar personal, con el propósito de conformar dos equipos, uno de Blue Team y el otro de Red Team.

Para realizar el reclutamiento de sus equipos decidió hacer pruebas técnicas, para el equipo Red Team, su misión es identificar el origen de la fuga de información en los equipos de la organización. Para el equipo Blue Team, su objetivo es contener el ataque y realizar un análisis a nivel técnico y metodologías que permiten estar preparada a la organización para este tipo de eventos.

Para finalizar, se hace entrega de un informe técnico donde se evidencia el desarrollo de los escenarios propuestos, donde se observa el paso a paso de los laboratorios realizados para los equipos Blue Team y Red Team, además de conocer aspectos legales y normativas que un experto en seguridad informática debe conocer.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: Es un hecho, incidente o persona que puede generar daños a un sistema informático, donde puede causar pérdida de información, destrucción de información o problemas funcionales de un sistema o red informática.

ANÁLISIS DE RIESGOS: Utilización sistemática de datos accesibles para reconocer peligros y medir peligros.

ATAQUES INFORMÁTICOS: Es un intento organizado e intencionado causado por una o más personas para ocasionar daños o problemas a un sistema informático o red.

CAUSA: Razón por la que se produce el peligro.

DISPONIBILIDAD: Según la norma ISO/IEC 27002:2013, es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DMZ: Una DMZ o una zona desmilitarizada, es una parte particular del sistema, en la que se encuentran administraciones explícitas de sistemas que están abiertas a sistemas no vinculados, por ejemplo, Internet.

EQUIPO RED TEAM: Es un equipo de expertos en seguridad informática, su misión es simular ataques para encontrar vulnerabilidades en los sistemas de información y aplicaciones que usas las diferentes organizaciones.

EQUIPO BLUE TEAM: Es un equipo de expertos en seguridad informática, su misión es defender y proteger a las organizaciones de los ataques realizados por ciberdelicuentes, también son los responsables de analizar amenazas que pueda sufrir una compañía.

EXPLOITS O PROGRAMAS INTRUSOS: Son códigos diseñados para aprovechar vulnerabilidades de sistemas operativos, programas o aplicaciones con debilidades en su estructura de desarrollo.

FIREWALL: Es un software que identifica y bloquea intentos de intrusión a una red informática.

FRAMEWORK: Es una herramienta de trabajo que permite al especialista realizar sus actividades.

INSEGURIDAD: La inseguridad informática es la falta o poca presencia de seguridad en un sistema operativo, aplicación, red o dispositivo, esto permite su demostración por hackers éticos (sombreros blancos) o su explotación por hackers mal intencionados (sombreros negros).

ISO: (Organización Internacional del Foro de Normalización) es una organización con el propósito de crear estándares internacionales, definidos por diferentes organizaciones nacionales de normalización.

METASPLOIT: Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

PENTESTING: Es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella.

RED DE DATOS: Es la organización de la fundación o correspondencia que ha sido explícitamente destinada a transmitir datos a través del intercambio de información.

RIESGO: Grado de presentación de un beneficio que permite la aparición de un peligro.

SEGURIDAD DE LA INFORMACIÓN: Preservación del secreto, honestidad y accesibilidad de los datos (ISO 27000: 2013).

SERVIDORES: Un servidor es un dispositivo que ejecuta varios procesos para atender las peticiones de un cliente y devolverle una respuesta en concordancia.

SISTEMAS DE INFORMACIÓN: Es un conjunto de datos que interactúan entre sí con un fin común, es importante para los procesos y toma de decisiones de las organizaciones.

SISTEMA OPERATIVO: Es el software principal de un sistema informático facilita administrar los recursos de hardware y suministra servicios a las informáticas.

SOMBREROS BLANCOS: El término se refiere a un hacker ético o experto en seguridad informática, su misión consiste en encontrar vulnerabilidades para mejorar la seguridad del sistema.

SOMBREROS NEGROS: Son expertos de seguridad informática, descubren las vulnerabilidades para conseguir su propio beneficio, son personas que roban datos, contraseñas, tarjetas de crédito, emails, entre otros.

VULNERABILIDAD: Es una debilidad que existe en el sistema de información, que pone en riesgo el activo más valioso de las organizaciones, permitiendo que un atacante afecte la integridad, disponibilidad o confidencialidad de esta.

INTRODUCCIÓN

En la elaboración del siguiente documento, tiene como objetivo entregar un informe técnico realizando pruebas desde el equipo de blue team y red team, el propósito de esta actividad es ilustrar y conocer herramientas utilizadas por los expertos de seguridad informática, además de conocer la leyes y normativas que existen en Colombia con respecto a estos temas.

En la actualidad, los delitos informáticos es una problemática que se presenta a diario, debido a que la información es uno de los activos más importantes que tiene una organización, es importante que los especialistas en seguridad de la información sepan cómo contener ataques y evitar que los daños causados sean mucho más graves.

Para las organizaciones es importante estar preparadas para este tipo de eventualidades, es por ello que deben contar con un modelo de gestión de seguridad informática, para tener una hoja de ruta a seguir y permita tomar decisiones de manera rápida y acertada.

Debido a esta problemática, es importante aprender sobre las diferentes herramientas, métodos, normativas y leyes que utilizan los blue team y red team; aprender a encontrar y simular ataques para saber cómo protegerse de posibles ataques que se puedan presentar.

Objetivos

Objetivo General:

Aprender de diferentes leyes, legislaciones, herramientas y estrategias que pueden ser utilizadas para simular y protegerse de posibles ataques informáticos que se pueden presentar en la organización Whitehouse Security.

Objetivos Específicos:

- Conocer el marco legal sobre protección de datos y personales delitos informáticos en Colombia.
- Definir cada una de las etapas del pentesting.
- Identificar las herramientas de vital importancia en ciberseguridad.
- Investigar sobre marco legal sobre protección de datos y personales delitos informáticos en Colombia.
- Enumerar los artículos que se violan de acuerdo al escenario planteado.
- Leer el código de ética del COPNIA para tomar decisiones sobre el escenario tres.
- Reflejar su opinión sobre casos que hayan ocurrido en la vida real.
- Conocer las herramientas utilizadas para realizar el pentensting.
- Identificar las técnicas utilizadas para evidenciar el fallo del equipo.
- Analizar el ataque realizado con el propósito de reconocer el puerto por el cual se hizo explotación de la vulnerabilidad.
- Investigar sobre el modelo de gestión de incidentes que tiene implementado la compañía para saber cómo proceder para contener el ataque.
- Aprender de medidas de hardenización para que no se presenten futuros ataques.
- Analizar cómo se podría utilizar CIS (Center For Internet Security) dentro de la organización.
- Identificar las características principales y funciones de un SIEM.

DESARROLLO DEL INFORME.

1. MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

El siguiente trabajo documenta algunos de los delitos informáticos en Colombia, entre ellas la ley 1273 de 2009 y la ley 1581 del 2012.

Ley 1273 del 2009:

- **Acceso Abusivo a un Sistema Informático:**

De acuerdo con el artículo 269A, esta violación se presenta cuando una persona ingresa a un sistema sin ser autorizado o se mantenga dentro del mismo sin el consentimiento de los dueños de la información. Este delito podría dar una pena de prisión de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

- **Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación:**

Según el artículo 269B, la incurrencia de esta pena se da cuando una persona sin estar autorizada, impida el correcto funcionamiento de las redes de telecomunicaciones, para este caso, la sanción se podría dar 48 a 96 meses y una multa de 100 a 1000 SMLMV.

- **Interceptación de Datos Informáticos:**

De acuerdo con el artículo 269C: el cual indica que: “El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses”

Basado en dicho artículo, podemos denotar que el atacante o usuario que se vea envuelto en un ataque similar a “MAN IN THE MIDLE” u hombre en el medio. Caso puntual se observó en la famosa “Red de chuzadas ilegales” por parte del DAS quienes interceptaban llamadas, estas como tal no estaban autorizadas por el solo hecho de vulnerar los derechos de las personas a las cuales estaban interceptando.

Según este hecho, se dan aproximadamente en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. Tener presente que este tipo de hechos para el ente público puede ser mayor la penalidad.

- **Daño Informático:**

De acuerdo con el artículo 269D de la ley 1273 de 2009, el daño informático es todo aquel en el que una persona sin autorización daña, borra, altera, suprime o deteriora datos informáticos,

también aquellos componentes de infraestructura tecnológica o de los sistemas de información, las penas van desde 48 hasta los 96 meses y las multas desde 100 a los 1000 salarios mínimos legales vigentes.

Oroboruo es el nickname del hacker colombiano que a sus 27 años ya tenía varios ataques informáticos en su historial de crímenes, como el ataque a la registraduría momentos antes de las votaciones del plebiscito, tuvo la capacidad de vulnerar 3.196 oportunidades a 1.374 dominios en su mayoría del gobierno.

El modo de ataque era la inyección de código malicioso para desconfigurar los sitios web y modificar bases de datos.

De acuerdo con el director general de la policía nacional, general Hernando Nieto Rojas, Oroboruo fue capturado y procesado por delitos como el acceso abusivo a un sistema y daño informáticos.

- **Uso de Software Malicioso:**

De acuerdo con el artículo 269E: “El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.”

Las personas que cometen este delito tienen características muy similares a los White hackers, a comparación de que ellos se dedican a servir a corporaciones delincuenciales, intereses económicos propios. Dentro sus actividades, se dedican al fraude en entidades bancarias.

Hay otro grupo que se dedican a la extorsión, al robo de información de las empresas y exigiendo dinero a sus víctimas.

Existen un sinnúmero de Crackers dedicados a realizar este tipo de modificaciones y se evidencia con frecuencia en software privativo, de alto valor corporativo o en su defecto software que es cotidiano. Al momento de subsanar el obstáculo de licenciamiento, el cracker modifica la integridad del software, en el instante evita el uso de licenciamiento para poder actuar como mediador, pero en sus hechos delictivos se denota un valor agregado por parte del atacante, en su defecto puede ser de modo sustractivo al momento de crear puertas traseras o ser parte de una “botnet” entre otros muchos hechos delictivos que generalmente son parte un ente organizativo.

El último informe de Eset security report reveló que el Ramsonware en sus diferentes modalidades sigue siendo la principal causa de incidentes en Latinoamérica y Colombia no está exenta de esta problemática permanente y latente, un cifrado de flujo que usa una clave elegida al azar de una lista de mil claves codificadas en su código binario, de manera que resulta sencillo acceder a ellas.

Este tipo de hecho delictivo generalmente se ha visto en creciente hacia las empresas que cuentan con poca o nula actividad de prevención en hechos de seguridad informática.

- **Violación de Datos Personales:**

De acuerdo con el artículo 269F hace referencia aquellas personas que, sin estar en capacidad, con ayuda de un tercero o por sus propios medios: obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en sistemas de información utilizados en diferentes medios, la persona que cometa este delito tendrá pena de prisión de 48 a 96 meses y una multa de 100 a 1000 SMLMV.

- **Suplantación de Sitios Web para Capturar Datos Personales:**

Según el artículo 269G, aquellas personas que sin tener autorización modifiquen o alteren un sitio de internet, bien sea modificando su interfaz, dominio, dirección IP, correos electrónicos, entre otros; el delito tendrá una pena de prisión de 48 a 96 meses y una multa de 100 a 1000 SMLMV. Esta práctica denomina comúnmente con el nombre de Phishing, donde el atacante modifica las páginas web para capturar usuarios y contraseñas de los usuarios.

- **Circunstancias de Agravación Punitiva:**

Teniendo Presente el artículo 269h: Es de denotar que los servidores públicos tienen mayor responsabilidad y como tal las consecuencias son del mismo calibre, sumándole a la pena interpuesta 3 años e inhabilitándolo de cargos públicos.

El caso puntual actualizado sucedió con el General Guatibonza que en su cargo de nivel público cometió chuzadas, este hecho además de la pena carcelaria interpuesta, le suma 3 años de prisión adicional, la inhabilitación en cualquier cargo público y la cancelación del cargo actual en la entidad que operaba actualmente.

Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes como lo indica dicho artículo, para el caso anterior aplicando el artículo 269c, que van de 36 a 72 meses, más el Articulo 269H quedaría para un total de 54 a 100 meses y una multa dispuesta por el juzgado si así lo amerita.

- **Hurto por Medios Informáticos y Semejantes:**

Según al artículo 269i de la ley 1273 de 2009, el cual hace referencia, “El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.”

Perfil criminológico de quien lo comete, son personas con un alto conocimiento en algoritmos y desarrollo de software, en ocasiones cometen este tipo de delitos por diversión o con el ánimo de lucrarse, entre más difícil sea penetrar las barreras de seguridad, mucho mejor para ellos.

El 07 de noviembre del 2013, cuando el Cuerpo Técnico de Investigación (CTI) de la ciudad de Medellín y miembros de la Unidad de Delitos Informáticos capturaron a miembros de una organización que se dedicaba a este delito de modalidad de transacción abierta, para este fraude utilizaban tarjetas débito, crédito y clonación de tarjetas.

El delito que cometió fue en diciembre 2009, utilizando un cajero automático de una reconocida entidad bancaria en la calle 76 de la ciudad de Medellín, la víctima se encontraba realizando una transacción, es engañado que se encontraba por el sector, logrando que dejara la transacción abierta para luego el delincuente, trasfiriera todo el dinero de esta cuenta.

- **Transferencia no Consentida de Activo:**

De acuerdo con el artículo 269j de la ley 1273 de 2009, el cual dice, “El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.”

Perfil criminológico de quien lo comete, son personas que tienen una inteligencia superior a la de las personas normal, acostumbran de trabajar de noche, son considerados unos genios en la informática, su reto es penetrar sitios inaccesibles y dejar su marca personal en los lugares que han ingresado.

El día 29 de noviembre del 2016 fue capturado Elimeek Quintero Orozco, fue capturado en el corregimiento de Cascará, gracias a las operaciones del grupo Gaula, fue capturado por el delito de Transferencia No Consentida de Activos.

Este hecho fue denunciado por el Gerente del Banco Agrario, de la ciudad de Santa Marta, localizado en el centro, el día 22 de marzo del 2012, quienes aprovecharon hacia mediodía (hora no hábil del banco), realizaron 25 consignaciones electrónicas de manera irregular por valor de 800 mil millones de pesos.

Ley 1581 del 2012:

Esta ley consta de 28 artículos, hace referencia a la ley estatutaria, la cual hacer referencia a la normatividad de protección de datos personales de los colombianos, también es importante resaltar que dicha ley tuvo una reforma a través del decreto 1377 del 2013, donde se reglamentó en parte esta ley, sin embargo, en el año 2014 se hizo entrega del decreto 886 que reglamentó el artículo 25 de esta ley.

Los artículos de esta ley pueden ser aplicados a las personas responsables de realizar el tratamiento de bases de datos de la población colombiana, que contenga información susceptible, puede ocurrir en diferentes tipos de entidades, ya sean de tipo público o privado.

- **Exclusiones de la ley:**

    1. A las bases de datos o documentos mantenidos en un ambiente particular o casero.
    2. A las bases de datos de seguridad y defensa nacional, que son utilizadas para prevención, financiamiento del terrorismo y control del lavado de activos.
    3. A las bases de datos de inteligencia y contrainteligencia.
    4. Sistemas de información periodísticos y otros contenidos digitales.
    5. A los registros reguladas por la Ley 1266 de 2008 (información financiera y crediticia).
    6. Sistemas de información del DANE (Ley 79 de 1993).

- **¿Qué es un dato personal?**

    1. **Ley 1266 de 2008:** Cualquier dato de información perteneciente a una o varias personas explícitas o que puedan relacionarse a un tipo de persona natural o jurídica. La información impersonal no está sujeta al régimen de protección de datos de la presente ley.
    2. **Ley 1581 de 2012:** Cualquier dato de información perteneciente a una o varias personas explícitas.

- **Clasificación de datos personales:**

    1. **Dato Público:** Es un dato que no es calificado como sensible (estado civil, profesión, servidor público y aquellos que pueden compartirse sin ningún inconveniente).
    2. **Dato semiprivado:** Son datos con naturaleza intima, no son públicos y su conocimiento sólo interesa al titular y a cierto grupo de personas (datos financieros y crediticios).
    3. **Dato privado:** Información que solamente es importante para el titular (dirección, teléfono, correo electrónico, archivos multimedia).
    4. **Datos sensibles:** Son datos especiales que corresponde al titular.

- **Sanciones:**

    1. Las para quien incumpla esta ley puede ser 2000 SMLMV.
    2. Las actividades correspondientes a tratamiento de datos serán interrumpidas por un período de seis meses.

3. Se realizaría cierre temporal de las actividades de la entidad.
4. En ciertas ocasiones se podría hacer cierre inmediato y definitivo de las actividades que involucre el tratamiento de datos de personas.

2. ETAPAS DEL PENTESTING

A continuación, se describe las etapas del pentesting en la siguiente matriz:

Tabla 1. Etapas del Pentesting

Proceso Pentesting	Descripción del proceso
Fase de recolección de información:	En esta etapa se realiza un reconocimiento de los sistemas para realizar una auditoría, se debe recolectar toda la información del sistema que se va a atacar, es importante realizar un buen análisis de información para realizar con éxito los pasos posteriores.
Fase de búsqueda de vulnerabilidades:	De acuerdo a la información recolectada anteriormente, en esta etapa se identifica posibles vulnerabilidades, después de este análisis se determina cuáles son las herramientas para realizar los ataques.
Fase de explotación de vulnerabilidades:	En esta etapa se realiza la explotación de las vulnerabilidades, donde se intenta conseguir información o credenciales de la organización, normalmente en esta fase se ejecutan exploit.
Fase Post-explotación:	En este punto, su intención es obtener información relevante sobre la organización o tener permisos de administrador sobre los sistemas de información, a través de diferentes técnicas como el pivoting.
Fase de informe:	Una vez concluidas las etapas anteriores, en este punto es importante documentar los hallazgos encontrados, donde se especifica el proceso realizado, las técnicas utilizadas, herramientas y las vulnerabilidades descubiertas.

Fuente: Propia del autor.

3. HERRAMIENTAS DE CIBERSEGURIDAD

- **Herramientas de Ciberseguridad más utilizadas:**

1. **Metasploit:** Es una herramienta utilizada en seguridad informática en equipos de red team y blue team, que permite explotar vulnerabilidades conocidas, se utiliza a través de módulos que son conocidos como payloads, este suministra los códigos que explotan vulnerabilidades.

   Proporciona otros módulos, entre ellos los encoders, que son códigos cifrados que evaden antivirus o firewall de los sistemas; también dentro de sus beneficios, ofrece la posibilidad de integrarse con herramientas externas.

   Es importante resaltar que es una herramienta libre, aunque también tiene una versión paga, su costo es bastante elevado porque tiene exploits ya desarrollados.

2. **Nmap:** Consiste en un software de código abierto, inicialmente se había creado para sistemas operativo Linux, pero al día de hoy se puede utilizar en diferentes plataformas; su principal función es escanear puertos de una red, su funcionamiento se da mediante el envío de paquetes, luego analiza las respuestas y de esta manera detectar si existen vulnerabilidades sobre dicha red.

3. **Openvas:** Funciona como un escáner open source, su característica principal es que permite la integración con otros servicios y herramientas utilizadas en ciberseguridad, uno de los principales beneficios de esta herramienta es que cuenta con interfaz gráfica, la cual es utilizada para la configuración y planificación de escaneos de los sistemas de información.

- **Servicios en línea:**

1. **ExploitDB:** Es un repositorio web donde un grupo de personas comparte brechas de seguridad y vulnerabilidades de aplicaciones y cómo sacar provecho de ellas, mediante instrucciones específicas.

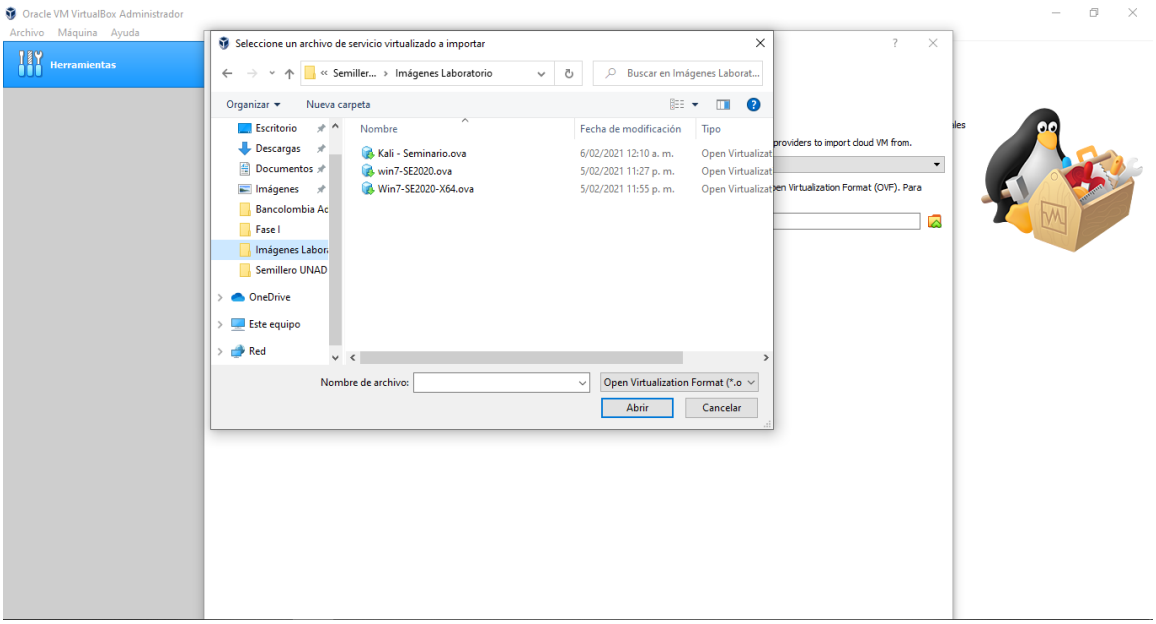
2. **CVE:** Sus siglas hacen referencia a vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures), es una lista de información donde se registran vulnerabilidades seguras conocidas y cada una tiene su número de identificación, en esta lista se encuentran la descripción, versiones de software que son afectadas y posible solución, esta lista es definida y mantenida por Mitre Corporation.

4. INSTALACIÓN DE MÁQUINAS VIRTUALES

A continuación, se procederá a realizar la instalación de tres máquinas virtuales: Dos con Windows 7 de 32 y 64 bits y una con Kali Linux.

1. Descargar virtualbox de la siguiente página: [Downloads – Oracle VM VirtualBox]
2. Una vez se haya descargado e instalado el programa, procederemos a instalar las imágenes compartidas por el docente.

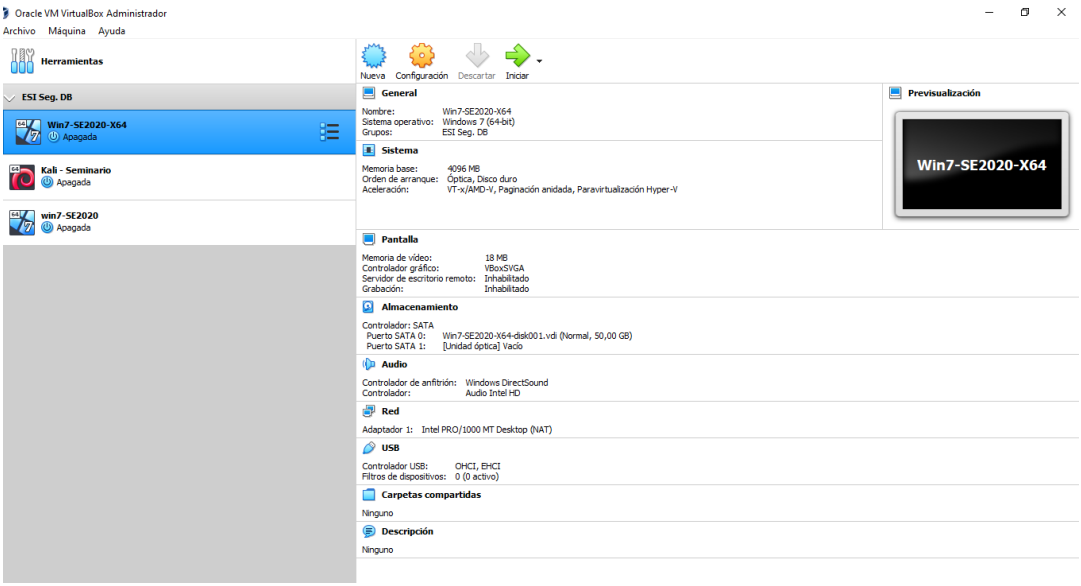
Ilustración 1. Instalación de imágenes compartidas por el docente.



Fuente: Propia del autor.

3. Una vez instaladas las imágenes se van a apreciar de tal manera:

Ilustración 2 Vista de las máquinas virtuales ya instaladas.

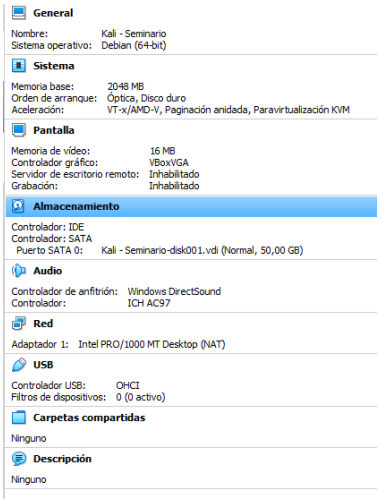


Fuente: Propia del autor.

A continuación, vamos a describir las características técnicas de cada uno de los equipos:

- **Máquina Kali Linux:**
  - ✓ Nombre: Kali –Seminario
  - ✓ Sistema Operativo: Debian (64 bits)
  - ✓ Memoria RAM: 2 gb
  - ✓ Disco Duro: 50 gb

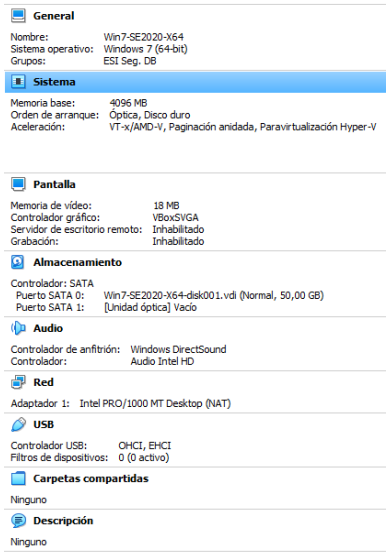
Ilustración 3 Características de la máquina virtual de KaliLinux



Fuente: Propia del autor.

- **Windows 7 64 bits:**
  - ✓ Nombre: Win7-SE2020-X64
  - ✓ Sistema Operativo: Windows 7 (64 bits)
  - ✓ Memoria RAM: 4 gb
  - ✓ Disco Duro: 50 gb

Ilustración 4 Características de la máquina virtual de Windws 7 64 bits.



Fuente: Propia del autor.

- **Windows 7 32 bits:**
  - ✓ Nombre: Win7-SE2020
  - ✓ Sistema Operativo: Windows 7 (64 bits)
  - ✓ Memoria RAM: 4 gb
  - ✓ Disco Duro: 50 gb

Ilustración 5 Características de la máquina virtual de Windws 7 64 bits.

Fuente: Propia del autor.

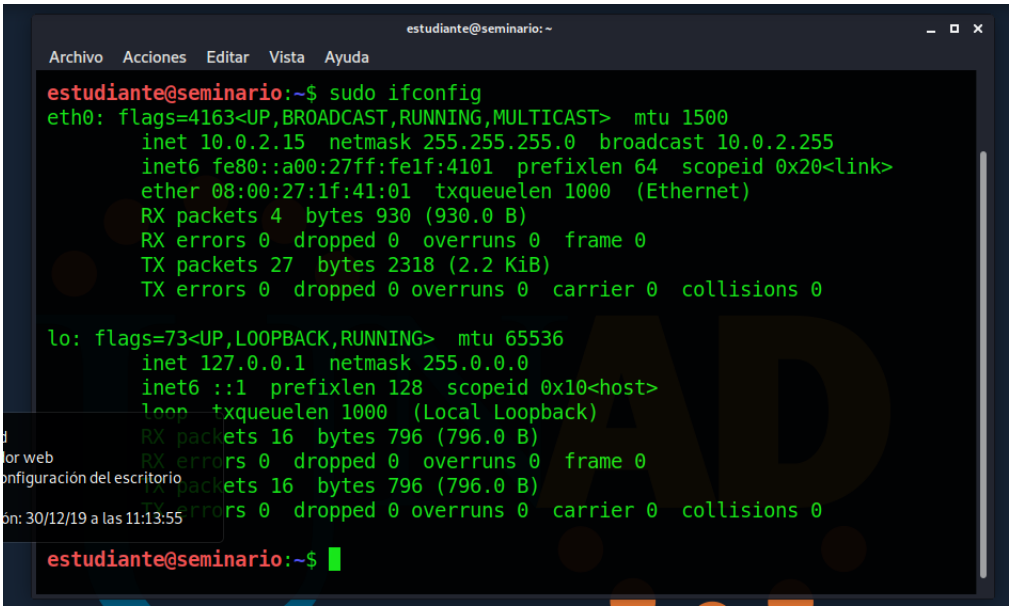
4. Comprobación de comunicación entre máquinas Windows y Kali Linux:

Ilustración 6 Inicio en virtualbox de la máquina virtual de KaliLinux.

Fuente: Propia del autor.

Utilizamos el comando sudo ifconfig para conocer la dirección IP de la máquina de Kali Linux:

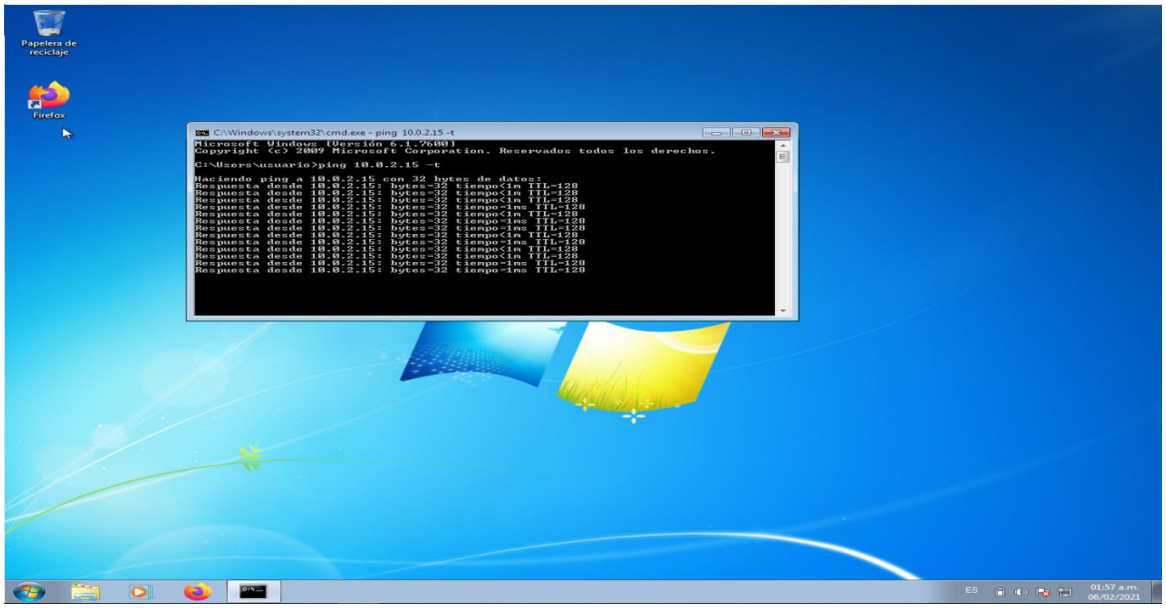
Ilustración 7 Comprobación de dirección de ip de la máquina Kali Linux.



Fuente: Propia del autor.

✓ Ahora desde la máquina virtual de Windows 32 bits, enviamos un ping a la dirección ip 10.0.2.15:

Ilustración 8 Envío de ping desde la máquina virtual de Windows 7 32 bits hacia la máquina de KaliLinux.

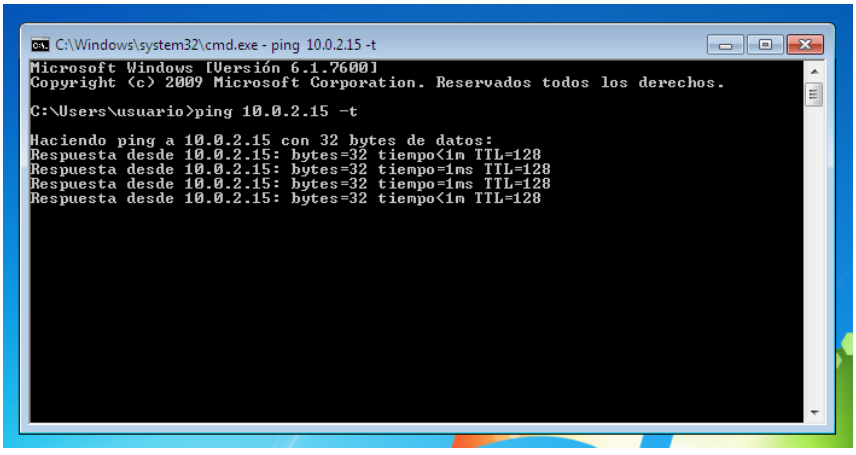


Fuente: Propia del autor.

✓ Se puede evidenciar que responde de manera exitosa todos los paquetes que fueron enviados.

✓ Luego vamos a verificar la conexión desde la máquina que tiene Windows 7 64 bits.

Ilustración 9 Envío de ping desde la máquina virtual de Windows 7 32 bits hacia la máquina de KaliLinux.



Fuente: Propia del autor.

- ✓ Como se puede apreciar en la imagen anterior, la máquina responde a los paquetes enviados.

5. EVIDENCIA SOBRE ANEXO 2 Y ANEXO 3.

Para los escenarios propuestos, fue solicitado un análisis legal sobre el contrato de reclutamiento que utiliza la empresa WhiteHouse Security, con el propósito de armar sus equipos de Blue Team y Red Team.

En los contratos realizados entre empresas y colaboradores, existen acuerdos de confidencialidad que son utilizados con el propósito de proteger la información de la empresa; su principal objetivo es guardar la información y no revelar información a terceros. Esto indica que el acuerdo de confidencialidad se argumenta en el principio de la buena fe. En la investigación que se realizó, se encontró que estos contratos se utilizan para proteger el deber precontractual de confidencialidad, que está relacionado con el carácter secreto de la información y la obligación de guardar confidencialidad.

También es importante decir que en la legislación colombiana no se ha desarrollado referente tema, una ley o artículo que se pueda aplicar a los contratos y obligaciones, debido a que se considera que con el contrato de reclutamiento es claro y suficiente por parte del trabajador.

6. ARTÍCULOS QUE SE ESTÁN VIOLANDO EN EL ANEXO 3.

Una vez leído el anexo tres de la correspondiente actividad, se logró identificar aspectos ilegales y no éticos, que de acuerdo a la legislación colombiana se pueden enumerar de la siguiente manera:

- En la primera cláusula del contrato, la parte receptora es obligada a no divulgar directa o indirectamente procesos ilegales que se realizan dentro de la organización, son involucrados en procesos legales que van en contra de la ley.

- En la segunda cláusula, hacen que la parte receptora realicen delitos, a través de vulneraciones a información confidencial, interceptación de datos, acceder de manera ilegal a los sistemas informáticos, entre otros.

- En la cuarta cláusula, la parte receptora es obligada a no denunciar actos ilícitos y no éticos que se presentan en la organización, también se evidencia que la parte receptora debe responder por el mal uso de la información confidencial de los representantes, y responder por sus actos delictivos dado el caso que sean acusados por estos hechos.

- En la cláusula octava, la empresa hace responsable de todos actos delictivos y procesos ilícitos a la parte receptora, haciéndose exenta de cualquier responsabilidad penal y legal a la organización.

Finalmente, aquí se puede apreciar que se violan los artículos 269A, 269C, 269D, 269F, 269H y 269I de la ley 1273 del 2009.

7. FIRMARÍA EL CONTRATO DEL ANEXO 3.

Una vez realizada la lectura del código de ética del COPNIA, mi decisión de firmar el contrato es negativa por los siguientes motivos:

El código de ética del COPNIA está fundamentado en la ley 843 del 2003, su propósito principal es que los profesionales actúen con compromiso y honestidad, haciendo un ejercicio ético de su profesión, también hay que recalcar que sobre esta ley existen deberes, como bien lo especifica el artículo 31, “es deber del profesional custodiar y cuidar los bienes, valores, documentación e información…”.

En el artículo 40, hace referencia que los profesionales en Ingeniería no pueden aceptar para su beneficio o el de terceros, algún tipo de regalías por la ejecución de trabajos que vayan en contra de la normatividad y principios éticos del profesional.

Además al firmar este contrato, incurriría en una falta gravísima, que de acuerdo al artículo 45, puede realizarse la cancelación de su tarjeta profesional de manera permanente, sin derecho a ejercer más como Ingeniero en cualquiera de sus áreas.

8. OPINIÓN SOBRE LA OPERACIÓN ANDROMEDA

En el artículo publicado en la página del tiempo con respecto a la operación a la fachada Andrómeda, hace referencia a la incautación que hizo en el año 2015, debido a la estrecha relación que existía entre esta conspiración y el caso del hacker Andrés Sepúlveda.

Sin embargo, en la investigación realizada en enero del año 2015 por parte del CTI, se logró identificar que las actividades realizadas en este lugar no eran ilegales, a pesar de la falta de control sobre los ambientes de trabajo, la falta de supervisión del equipo y los contratos de confidencialidad, permitieron fuga de información y el uso de malas prácticas por parte del personal especializado que se encontraba en este lugar.

Este tipo de iniciativas son buenas cuando se tienen ambientes controlados y permite la capacitación y fortalecer conocimientos para personal especializado, pero en este

acontecimiento particular, es un claro ejemplo de una realidad que se vive en diferentes organizaciones del país, bien sean de tipo público o privado, la falta de personal capacitado y la imposición de controles que son recomendados por la norma ISO27001, hace que se genere este tipo de situaciones, donde se conforman equipos de Blue Team y Red Team, pero no existen límites de sus acciones, ni acuerdos de confidencialidad, donde el personal especializado pueden incurrir en la violación de varios artículos que están establecidos en la ley 1273 y en la ley 843.

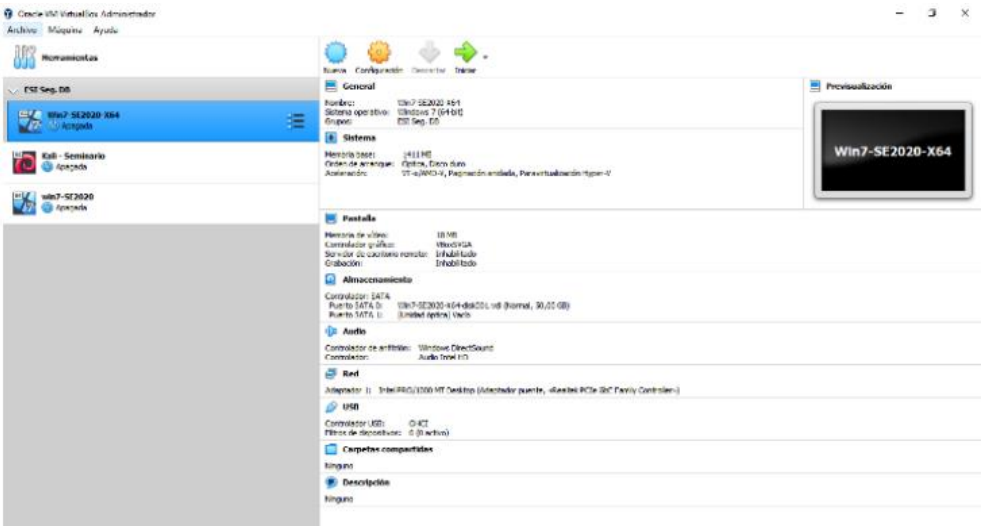
Estamos en una era, donde la información es el activo más preciado que tienen las organizaciones, pero la falta de especialistas de seguridad de la información en las empresas, permite que falte gran cantidad de controles y la fuga de información se realice fácilmente para realizar actos delictivos.

9. DESCRIPCIÓN DE SOFTWARE UTILIZADO EN EL ANEXO 4.

A continuación, se va a realizar un paso a paso la recreación del ataque realizado, donde se evidencia las herramientas utilizadas para hacer el pentesting.

- Instalar las imágenes con Windows 7 x 64 y Kali Linux en VirtualBox:

Ilustración 10 Instalación de máquinas virtuales en virtualbox.



Fuente: Propia del autor.

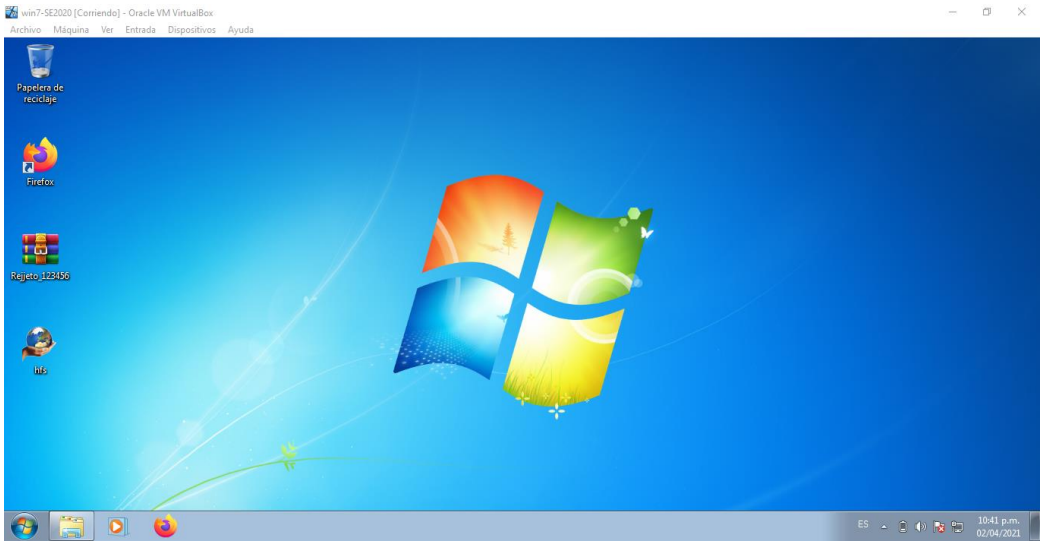
- Se inicia la máquina con Kali Linux:

Ilustración 11. Inicio de máquina virtual KaliLinux.

Fuente: Propia del autor.

- También se inicia la máquina con Windows 7 de 64 bits

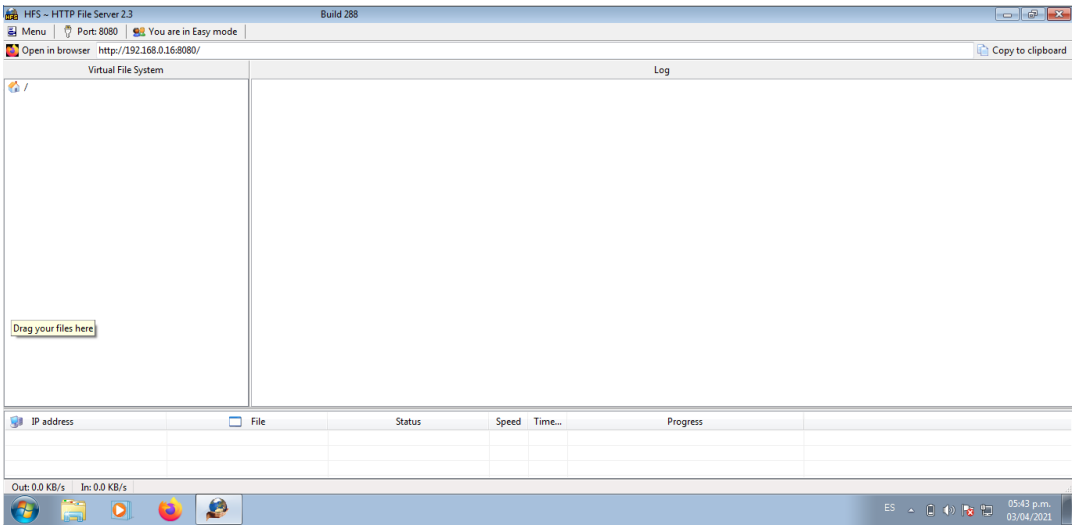
Ilustración 12 Inicio de máquina virtual Windows 7 64 bits.



Fuente: Propia del autor.

- Ejecutar la aplicación de rejetto en la máquina virtual de Windows, aquí se puede apreciar la dirección ip y puerto por el cual se puede ingresar al equipo, para este caso se da mediante la dirección 192.168.0.16:8080

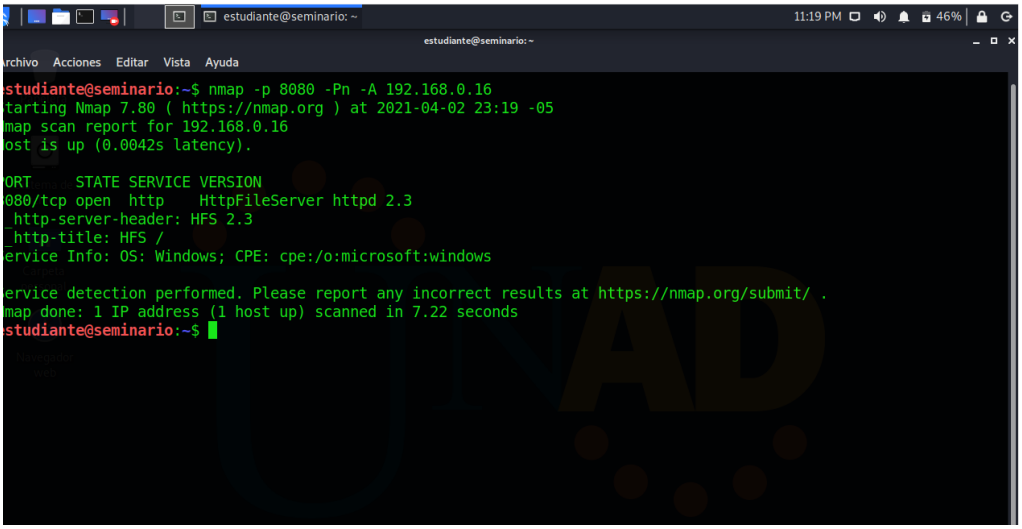
Ilustración 13 Inicio de la aplicación Rejetto en Windows 7 64 bits



Fuente: Propia del autor.

- En la máquina de Kali Linux, abrimos una consola de comandos y usamos nmap para el escaneo de vulnerabilidades.

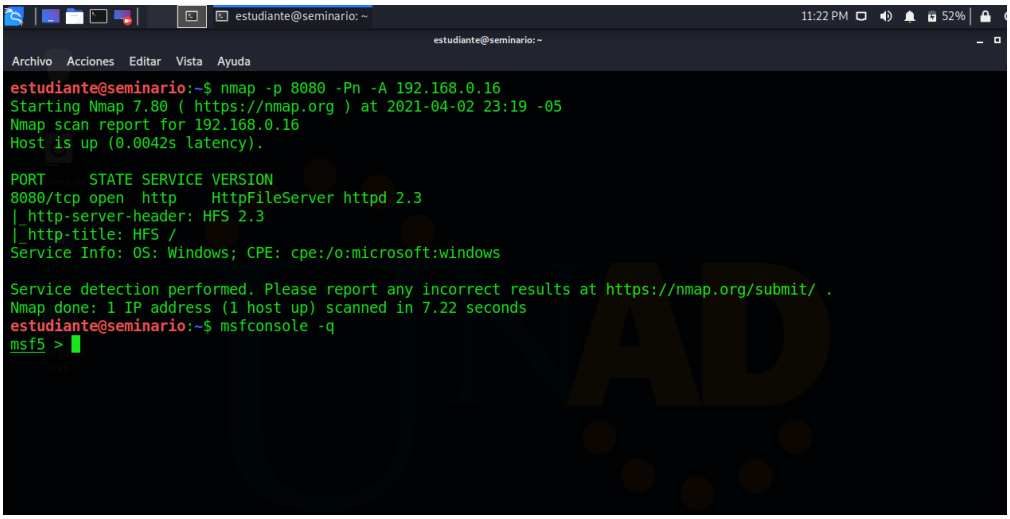
Ilustración 14 Escaneo de puertos abiertos mediante nmap.



Fuente: Propia del autor.

- Desde la misma consola de comandos se utiliza el comando msfconsole –q para usar la consola de comandos y explotar la vulnerabilidad en rejetto.

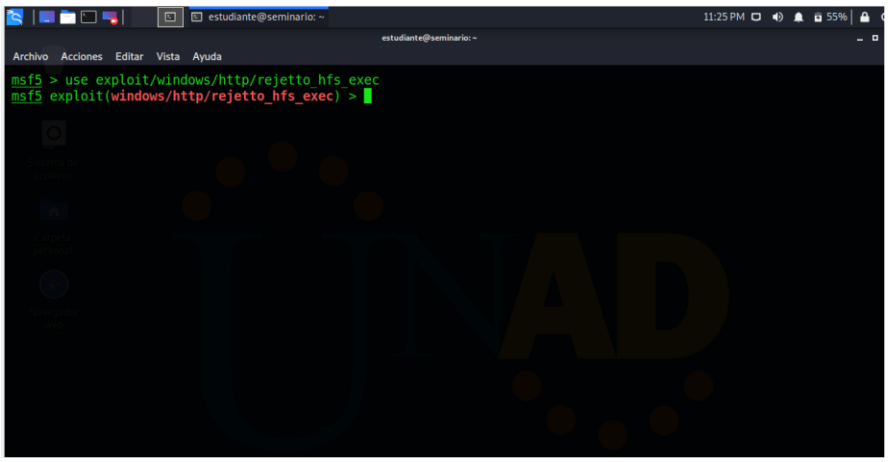
Ilustración 15 Ingresar a la consola de comandos metasploit.



Fuente: Propia del autor.

- Escogemos el tipo de exploit que vamos a realizar, para esta ocasión se va a realizar mediante rejetto.

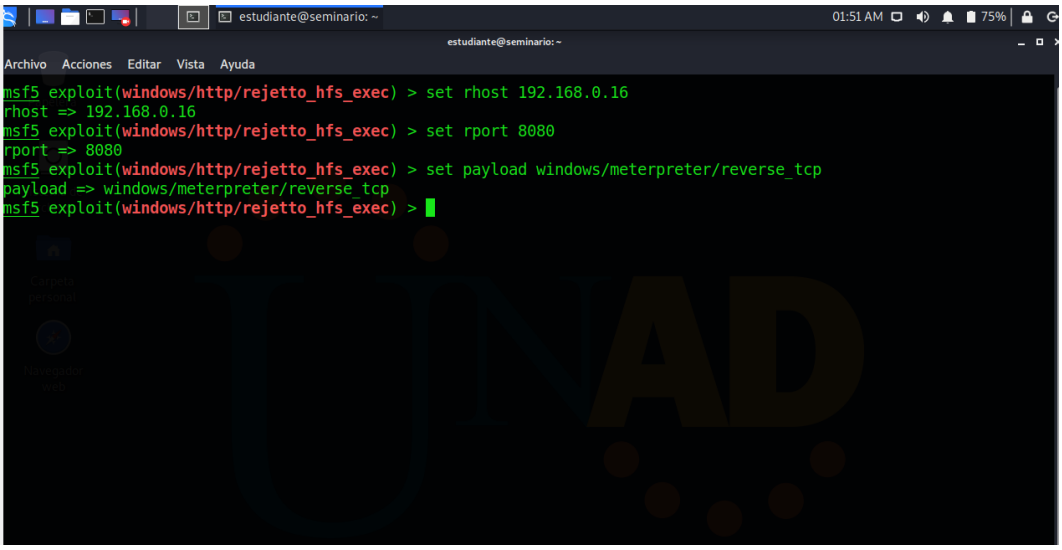
Ilustración 16 Se escoge el tipo de exploit que se desea utilizar.



Fuente: Propia del autor.

- Luego se asignan las variables para realizar el ataque, dentro de las cuales se encuentran: rhost, rport, y payload.

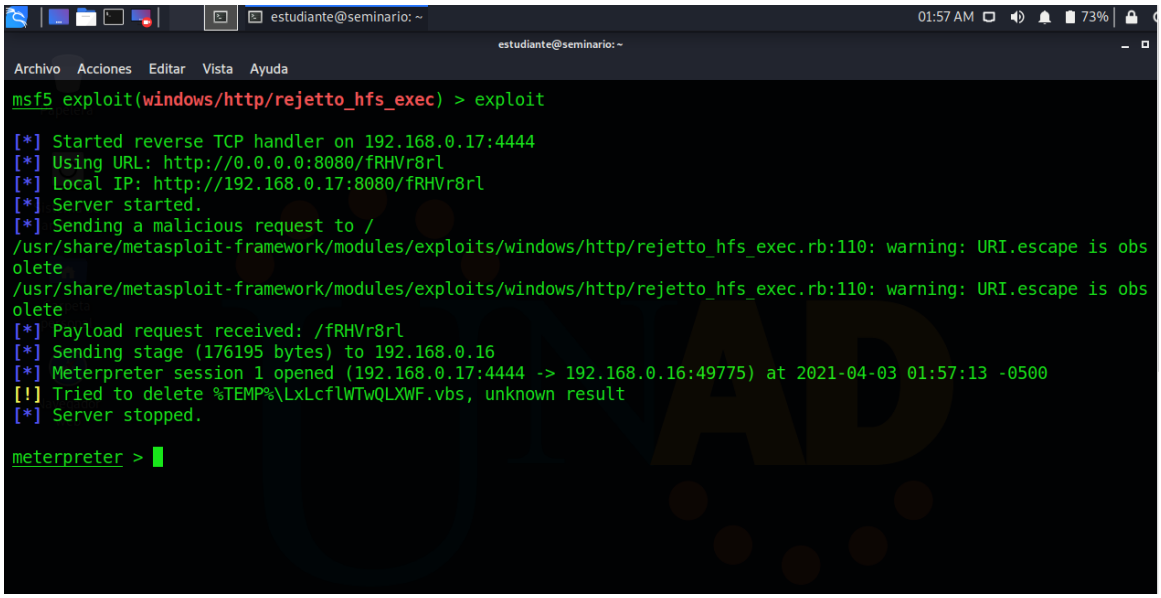
Ilustración 17 Se asignan valores a las variables para realizar el ataque.



Fuente: Propia del autor.

Luego, se realiza el exploit, si la conexión se realiza de manera exitosa con la máquina que se desea atacar, se verá una imagen como la siguiente:

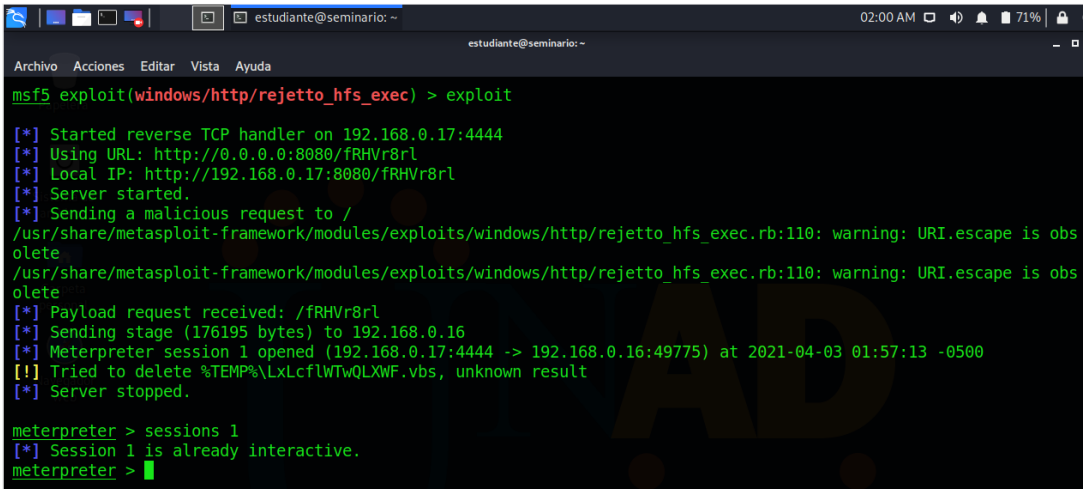
Ilustración 18 Se ejecuta el exploit para iniciar con el ataque.



Fuente: Propia del autor.

Ahora se procede a entrar a esa sesión como se aprecia en la siguiente imagen:

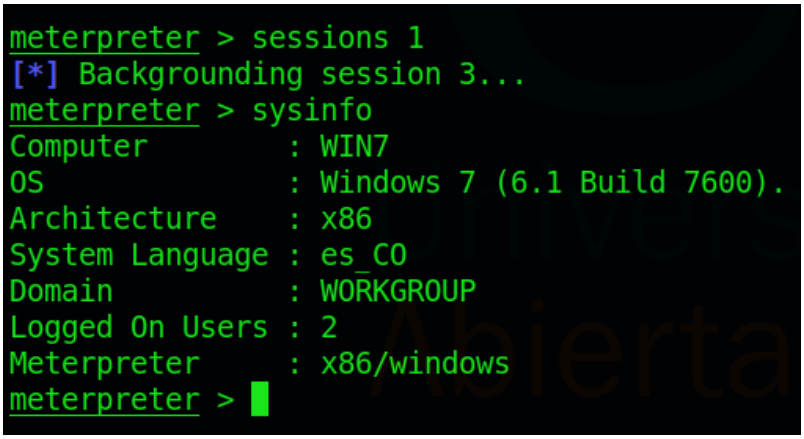
Ilustración 19 Se logra el acceso a la máquina que se va a atacar .



Fuente: Propia del autor.

- Mediante el comando de sysinfo, permite conocer las características del equipo al que se pudo acceder como se aprecia en la siguiente imagen:

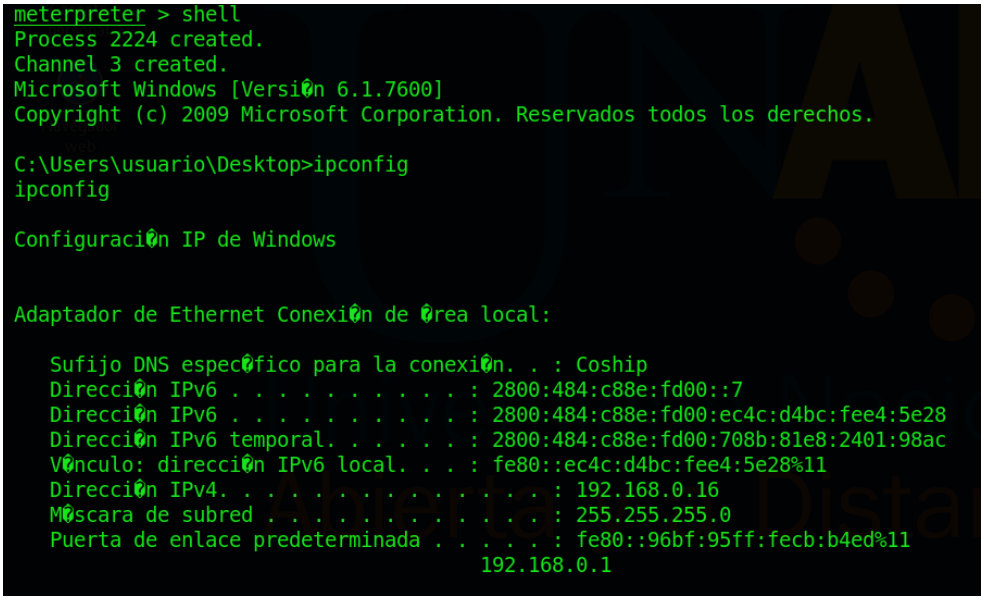
Ilustración 20 Se ejecuta el comando sysinfo para obtener información del máquina atacada .



Fuente: Propia del autor.

- Con el comando Shell, se genera una consola de comandos, la cual permite conocer la dirección ip del equipo que fue atacado

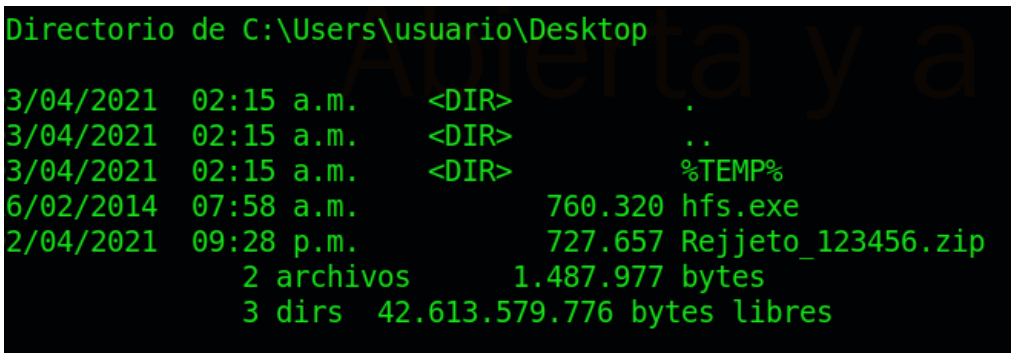
Ilustración 21 Se abre una consola shell para conocer la dirección ip de la máquina atacada .



Fuente: Propia del autor.

- Finalmente, se con el comando ver, permite visualizar los archivos que se encuentran en el escritorio del equipo que fue atacado.

Ilustración 22 Se ejecuta el comando dir para conocer los archivos que existen en el equipo .



Fuente: Propia del autor.

10. LISTA Y DESCRIPCIÓN DE DATOS UTILIZADAS EN EL ANEXO 4.

La información relevante para realizar la simulación de ataque en el anexo, fue la siguiente:

- Los sistemas operativos que utilizaron para realizar el ataque.
- El nombre de la aplicación instalada, para este escenario fue rejetto.
- El tipo de permisos y configuración que tienen configurado la máquina que fue atacada.
- La detención del firewall de Windows para realizar el ataque de manera exitosa.
- El tipo de exploit que fue utilizado para recrear el escenario.

11. HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR LA FALLA DE SEGURIDAD DEL ANEXO 4.

Para la práctica anteriormente realizada, fueron utilizadas varias herramientas las cuales se van a mencionar a continuación:

- **VirtualBox:** Es un software utilizado para la creación de máquinas virtuales, en esta ocasión fue utilizado para simular la práctica de pentesting a través de sistemas operativos Windows 7 y Kali Linux.
- **Nmap:** Consiste en un software de código abierto, inicialmente se había creado para sistemas operativo Linux, pero al día de hoy se puede utilizar en diferentes plataformas; su principal función es escanear puertos de una red, su funcionamiento se da mediante el envío de paquetes, luego analiza las respuestas y de esta manera detectar si existen vulnerabilidades sobre dicha red.

- **Metasploit Framework:** Es una herramienta utilizada en seguridad informática en equipos de red team y blue team, que permite explotar vulnerabilidades conocidas, se utiliza a través de módulos que son conocidos como payloads, este suministra los códigos que explotan vulnerabilidades.

  Proporciona otros módulos, entre ellos los encoders, que son códigos cifrados que evaden antivirus o firewall de los sistemas; también dentro de sus beneficios, ofrece la posibilidad de integrarse con herramientas externas.

  Es importante resaltar que es una herramienta libre, aunque también tiene una versión paga, su costo es bastante elevado porque tiene exploits ya desarrollados.

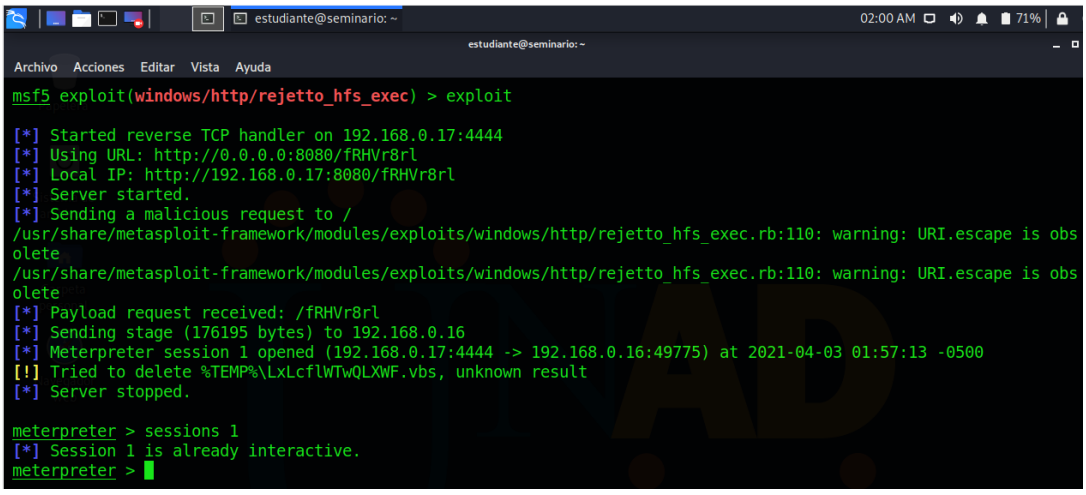
- **Rejetto:** Es un software fileserver, que es utilizado para el envío y recibimiento de archivos que se encuentran alojados en un equipo.

Finalmente es importante nombrar, que el puerto utilizado para realizar el ataque es el 8080, fue el que se logró identificar cuando se realizó el escaneo con nmap, que una vez finalizado, en el resultado se pudo identificar que estaba abierto.

12. EXPLICACIÓN DE CÓMO AFECTA EL ATAQUE.

Una vez realizada la simulación del ataque, donde finalmente se evidencia que se logra tener un acceso a la máquina del atacante, como se evidencia en la siguiente gráfica:

Ilustración 23 Evidencia de afectación del ataque



Fuente: Propia del autor.

Se logra identificar que por medio de este tipo de ataque se puede presentar fuga de información propiamente de la empresa, como especialistas de seguridad informática, se debe velar que el activo más importante de las organizaciones, se encuentre seguro y protegido.

Se plantea el siguiente escenario, para entender lo delicado de este tipo de situaciones, suponiendo que el equipo atacado pueda ser de una persona que sea la responsable de recursos humanos; y la información que se puede obtener mediante este tipo de ataques sea información sensible de todos los colaboradores de la información, podría quedar expuesta información íntima como direcciones, salarios, cuentas de nómina, caja de compensación, entre otra información relevante; lo cual podría causar problemas tanto a la organización por no tener implementado un buen sistema de seguridad informático y a los dueños de la información que acaba de ser hurtada.

13. INDAGACIÓN Y ATAQUE EN TIEMPO REAL.

En una organización cuando se presenta este tipo de situaciones es importante estar preparado, sin embargo, en mi rol como especialista de seguridad de la información, debo acudir al documento de Modelo de Gestión de Incidentes, esto con el propósito de encontrar estrategias y actuar de manera oportuna. Esto se realiza con el propósito de evitar que el ataque se propague hacia otros equipos y reducir los daños a la organización, para ello se debe tener en cuenta los pilares de la seguridad de la información, que son confidencialidad, integridad y disponibilidad de la información.

Es importante mencionar que el Modelo de Gestión de Incidentes está conformado de cuatro fases, los cuales se describen a continuación:

- **Preparación:** En esta fase se definen las políticas de seguridad de la información, para ello pueden basarse en la normatividad de la ISO27001:2013, se debe recolectar la mayor cantidad de información posible, con el propósito de definir roles, planes y estrategias en caso de que se presente una eventualidad.
- **Detección y Análisis:** En este punto se hace recolección de la información sobre la situación presentada, normalmente aquí existen sistemas de monitoreo que permiten al especialista analizar y agilizar la toma de decisiones.
- **Contención, Erradicación y Recuperación:** El objetivo de esta actividad es evitar que el ataque se propague y genere el menor daño posible, en este punto se debe tomar decisiones importantes, puede ser como: apagar el sistema, deshabilitar la red, apagar servicios, entre otros.

Una vez realizada la acción de contención, debe realizarse un escaneo del equipo para eliminar los malware, hacer actualización del sistema operativo y antivirus para eliminar el código malicioso que se encontraba, dado el caso de que se presente pérdida de información, la compañía debe contar con políticas de generación de back ups para recuperar la información.

- **Actividades Post-Incidente:** En la fase final, deben aplicarse nuevas políticas sobre las lecciones aprendidas, para el caso particular del ataque realizado con rejetto, el especialista de seguridad de información debería tomar las siguientes acciones:

  - ✓ Implementar un firewall que evite la presencia de intrusos.
  - ✓ Mantener los sistemas operativos de los equipos de la organización actualizados.
  - ✓ Mantener la consola de antivirus actualizadas para detectar la presencia de intrusos y malwares sobre los computadores.
  - ✓

14. MEDIDAS DE HARDENIZACIÓN PARA EL ANEXO 5.

En seguridad informática el proceso de hardenización se conoce como el conjunto de técnicas que se pueden utilizar para asegurar un sistema, con el propósito de reducir vulnerabilidades. Para este caso particular, el especialista de seguridad de la información podría considerar tomar las siguientes medidas sobre el equipo que fue víctima del ataque:

- ✓ Instalar los parches de actualización del sistema operativo.
- ✓ Instalar y mantener actualizado el sistema de antivirus sobre el equipo.
- ✓ Activar el firewall de equipo.
- ✓ Bloquear los puertos de red por los cuales los intrusos podrían realizar un ataque.
- ✓ Quitar permisos de administrador sobre el equipo mediante la implementación de un servidor que maneje directorio activo.

15. DIFERENCIAS ENTRE EQUIPO DE RESPUESTA DE INCIDENTES INFORMÁTCIOS Y BLUE TEAM

En la siguiente tabla, se explica la diferencia que existe entre el equipo blue team y el equipo de respuesta de incidentes informáticos:

Tabla 2. Diferencias entre el blue tea y equipo de respuesta de incidentes informáticos

Blue Team	Respuesta de Incidentes Informáticos
Es un equipo de seguridad informática encargado de las defensivas, su función principal es proteger los activos críticos de la organización de cualquier ataque o amenaza.	El equipo de respuesta de incidentes informáticos son los responsables en dar soluciones a eventos o situaciones presentadas en la organización.
Dentro de sus responsabilidades deben identificar vulnerabilidades, recomendar planes de mitigación, establecer medidas defensivas para proteger los sistemas informáticos de la organización.	Son los responsables de realizar la contención, erradicación y recuperación cuando se presenta un incidente, su misión es estar preparados para cuando se presente alguna eventualidad.

Fuente: Propia del autor.

En conclusión, el equipo de blue team son los encargados de realizar la planeación y estrategias para los posibles ataques informáticos que se puedan presentar, sin embargo, como los sistemas de seguridad no son completamente seguros, el equipo de respuesta de incidentes informáticos son los responsables de contener los ataques cuando son presentados.

16. ¿CON CUÁL PROPÓSITO UTILIZARÍA CIS EN UN EQUIPO BLUE TEAM?

CIS (Center for Internet Security) es una organización sin ánimo de lucro que ayuda a organizaciones tanto públicas como privadas a estar protegidas de ataques y amenazas cibernéticas.

Su principal propósito es identificar, validar, promover y sostener soluciones prácticas en defensa de sistemas informáticos, con el fin de generar un entorno de seguridad y confianza a los sistemas de información que existen en diferentes organizaciones.

El CIS lo utilizaría dentro del equipo de blue team con el propósito de revisar, identificar y evaluar posibles vulnerabilidades, también para monitorear y revisar el comportamiento de las redes en la organización.

17. FUNCIONES Y CARACTERÍSTICAS ESPECIALES DE SIEM

SIEM (Security Information and Event Management), es una categoría de software, que su principal propósito es brindar a las empresas públicas y privadas información útil de vulnerabilidades y amenazas más potentes que se pueden presentar en las redes de las organizaciones, esto se realiza a través de información y categorización de las amenazas.

El funcionamiento de este componente está dado por un repositorio, que brinda información de seguridad, antivirus, firewall y soluciones de prevención en las intrusiones.

Las funciones y características especiales de SIEM son:

- ✓ Identificar amenazas que requieren soporte inmediato.
- ✓ Escalar inconvenientes al grupo de respuesta de incidentes informáticos para que solucionen en el menor tiempo posible.
- ✓ Utilizar un formato de reporte para cumplir con las regulaciones de la industria.
- ✓ Dar contexto de los eventos de seguridad para brindar optimas soluciones.
- ✓ Registrar las evidencias de auditoria, eventos detectados y la solución de los mismos.

18. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS

De acuerdo a las lecciones aprendidas del ataque presentado a la empresa WhiteHouse Security, se recomienda utilizar las siguientes herramientas para contener los ataques informáticos en la organización:

- ✓ **Software de antivirus:** Es recomendable que los equipos que hacen parte de una organización deben contar con antivirus gratuito y confiable, este tipo de software brinda tranquilidad de que los equipos puedan ser atacados por un malware, sin embargo, es importante que siempre mantenga actualizado para evitar ser víctima de ataques informáticos.

- ✓ **Firewall Perimetral:** Es la herramienta más recomendada que existe en temas de ciberseguridad, es la responsable de escanear el tráfico en la red, permitiendo el paso o haciendo bloqueo de acuerdo a las reglas definidas por el administrador. También permite bloquear el acceso a páginas de internet no autorizadas, con el propósito de que los usuarios no ingresen y descarguen algún tipo de malware que pueda afectar los sistemas de información de la organización.

- ✓ **Actualizaciones de Seguridad:** Las actualizaciones de los sistemas operativos son importantes que se realicen a nivel de toda la infraestructura de la organización, con el propósito de instalar los parches que evitan que existan vulnerabilidades y huecos de seguridad, en este punto es recomendable establecer una política de rutinas de cada cuánto se deben actualizar los equipos cómputo, servidores, sistemas de enrutamiento y firewall de la organización.

- ✓ **Bloqueo de puertos para el uso de dispositivos de almacenamientos:** Al bloquear los puertos usb de los equipos computo de la organización, evita que exista fuga de información, también de que se pueda instalar algún tipo de malware, dado que en muchas ocasiones el principal actor de incidentes informáticos son los trabajadores de la organización.

- ✓ **Implementación de políticas de copias de seguridad de la información:** En este punto, se considera importante optar por una política de generación de back up a todos los sistemas de información de la compañía, bien sea a motores de base de datos, archivos, documentos, entre otros; esto con el propósito de que, si llegan a ser víctimas de un ataque o secuestro informático, se pueda contar con un respaldo.

CONCLUSIONES

- A partir de la investigación realizada, permitió conocer las leyes y artículos que existen en Colombia con respecto a seguridad de la información y la ley de tratamiento de datos.

- De acuerdo al análisis realizado, se pudo conocer cada una de las etapas que son utilizadas en el pentesting y que se realiza en cada una de ellas.

- Se identificaron las herramientas más utilizadas open source que son utilizadas para conocer vulnerabilidades y hacer exploits de diferentes sistemas.

- Se hizo la instalación de las máquinas virtuales, conociendo las características de cada una de ellas y verificando su conexión entre ellas. A partir de la investigación realizada, permitió tomar decisiones en base a las leyes y artículos que existen en Colombia con respecto a seguridad de la información y la ley de tratamiento de datos.

- De acuerdo al análisis realizado, se identificar los procesos ilegales relacionados en el anexo 3.

- Se identificaron los artículos del código de ética del COPNIA que fueron violados en el planteamiento del escenario.

- Se hizo un análisis con respecto al caso que se presentó hace algunos años de la fachada Andrómeda.
- Se realiza la instalación y configuración de las máquinas virtuales, montando sus respectivos sistemas operativos para simular el ataque.

- A partir del laboratorio realizado, permitió conocer cómo explotar vulnerabilidades mediante diferentes herramientas que son utilizadas en Ethical Hacking.

- Es importante mantener los equipos con antivirus y firewall actualizados para evitar este tipo de ataques.

- Se hizo la instalación de las máquinas virtuales, conociendo las características de cada una de ellas y verificando su conexión entre ellas.
- Es importante que las empresas cuenten con un Sistema de Gestión de Seguridad de la Información para estar preparados ante cualquier tipo de ataque.

- Una vez realizado el análisis de cómo se pudo haber evitado el ataque presentado en la organización, permitió conocer técnicas hardenización para evitar que vuelva a ocurrir.

- Al realizar esta investigación permitió diferencias las responsabilidades que existen entre el blue team y el equipo de incidentes informáticos.

- Con la búsqueda realizada se identificó que es recomendable utilizar CIS para el equipo blue team, con el objetivo de hacer planeación y estrategias de posibles ataques que puedan dar.

- Se conocieron las principales funciones y características del SIEM, también su relevancia en el blue team y la organización.

- Permitió conocer diferentes herramientas de uso libre, que realizan contención sobre los ataques que se puedan presentar en la compañía.

19. ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS

En los equipos de Blue Team y Red Team, es recomendable que los expertos en seguridad informática estén en constante investigación y aprendizaje, dado que a diario surgen nuevas técnicas o ataques que realizan a diferentes organizaciones, donde surgen lecciones aprendidas y permite que las otras organizaciones se puedan preparar para que no les ocurra lo mismo.

En la actualidad existen todo tipo de certificaciones para el campo de seguridad informática, por lo que es recomendable que los especialistas de esta área se formen y certifiquen en ramas específicas, para que sean expertos técnicos de temas específicos y les permita tomar decisiones ágiles y estar preparados ante cualquier eventualidad que se pueda presentar.

20. RECOMENDACIONES

De acuerdo al informe técnico realizado, se recomienda realizar las siguientes medidas para evitar ser víctimas de un ataque informático y que se genere fuga de información técnica de la organización:

- ✓ Firmar un acuerdo de confidencialidad con los trabajadores de la compañía, esto con el propósito de que las personas conozcan que, si utilizan la información de la organización con fines lucrativos, están faltando a norma grave del reglamento interno de trabajo.

- ✓ Capacitaciones constantes a los usuarios, muchos de los ataques informáticos se generan porque los usuarios desconocen buenas prácticas y políticas que existen en la organización, en diversas ocasiones los usuarios son los principales responsables de que se generen los ciberataques.

- ✓ Actualización de firmwares a dispositivos de la organización. Las actualizaciones de los sistemas operativos son importantes que se realicen a nivel de toda la infraestructura de la organización, con el propósito de instalar los parches que evitan que existan vulnerabilidades y huecos de seguridad, en este punto es recomendable establecer una política de rutinas de cada cuánto se deben actualizar los equipos cómputo, servidores, sistemas de enrutamiento y firewall de la organización.

- ✓ Instalar una consola de antivirus para evitar la instalación de malwares, es recomendable que los equipos que hacen parte de una organización deben contar con antivirus gratuito y confiable, este tipo de software brinda tranquilidad de que los equipos puedan ser atacados por un malware, sin embargo, es importante que siempre mantenga actualizado para evitar ser víctima de ataques informáticos

- ✓ Implementar un firewall para que no permita el ingreso a intrusos, es la herramienta más recomendada que existe en temas de ciberseguridad, es la responsable de escanear el tráfico en la red, permitiendo el paso o haciendo bloqueo de acuerdo a las reglas definidas por el administrador.

  También permite bloquear el acceso a páginas de internet no autorizadas, con el propósito de que los usuarios no ingresen y descarguen algún tipo de malware que pueda afectar los sistemas de información de la organización.

- ✓ Bloquear los puertos usb de los equipos computo de la organización, Al bloquear los puertos usb de los equipos computo de la organización, evita que exista fuga de información, también de que se pueda instalar algún tipo de malware, dado que en muchas ocasiones el principal actor de incidentes informáticos son los trabajadores de la organización.

- ✓ Partición de discos duros de los equipos computo de la organización, se sugiere realizar esta operación para almacenar la información de esta manera: la partición principal para programas y sistema operativo, otra para información confidencial de la organización y una para almacenar información confidencial de los trabajadores.

- ✓ Implementar un servidor para la configuración de directorio activo y dns de la organización, es una buena práctica porque permite mayor seguridad para autenticarse en los equipos computo, además que permite ocultar la dirección ip pública y administrar las direcciones ip de los equipos computo de la organización.

- ✓ Establecer políticas y buenas prácticas del uso de los computadores de la organización, para este punto se recomienda establecer los ítems del reglamento de acuerdo a la normatividad ISO27001:2013.

- ✓ Quitar privilegios de administrador sobre los equipos computo, esta recomendación se hace con el propósito de que los usuarios no puedan realizar instalación de software que no esté aprobado por la organización para su uso.

- ✓ Realizar auditorías internas, es importante realizar auditorías a los usuarios de la organización, para saber si están incurriendo en alguna falta de las políticas implementadas y tomar acciones tempranas, antes de que a cusa de ellas se pueda generar un ataque informático.

BIBLIOGRAFIA

- Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

- R. E. Tiempo, «'Oroboruo', el paisa de los más de 3.000 ataques a dominios del gobierno,» La historia detrás de cinco 'hackers' colombianos y sus delitos, 6 10 2016. [En línea]. Available: https://www.eltiempo.com/justicia/cortes/delitos-de-hackers-en-colombia-52232

- El Tiempo, «El ciberdelincuente que viajó por el mundo con millas de los famosos,» 25 6 2015. [En línea]. Available: https://www.eltiempo.com/archivo/documento/CMS-16006809

- El Tiempo, « Ciberataque 'amateur' no protege sus propias claves,» 01 10 2018. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-amateur-no-protege-sus-propias-claves-275584.

- SHAHRIAR HOSSAIN, Zulkemine Mohammad. (2011). Information Source-based Classification of Automatic Phishing Website Detectors. School of Computing. Queen's University, Kingston, Canada

- El Heraldo, «Capturan en Bogotá y Santa Marta a idcados en hurtos informáticos,» [En línea]. Available: https://www.elheraldo.co/nacional/capturan-en-bogota-y-santa-marta-indiciados-en-hurtos-informaticos-131337

- El Ejercito, «Por el delito de Transferencia No Consentida de Activos, fue capturado un sujeto en Agustín Codazzi, Cesar,» [En línea]. Available: https://www.ejercito.mil.co/?idcategoria=406121

- Openwebinars, «¿Qué es Metasploit framework? Rizaldos, Hector,» [En línea]. Available: https://openwebinars.net/blog/que-es-metasploit/
- Ochobitshacenunbyte, «Principales usos de nmap, Ochobits, David,» [En línea]. Available: https://www.ochobitshacenunbyte.com/2020/04/22/principales-usos-de-nmap/
- Incibe-cert, «Testeando la seguridad en redes industriales, INCIBE,» [En línea]. Available: https://www.incibe-cert.es/blog/nvt-testeando-seguridad-redes-industriales#:~:text=OpenVAS%20(Open%20Vulnerability%20Assessment%20System,escaneo%20y%20gesti%C3%B3n%20de%20vulnerabilidades.
- Exploit Database, «About the Exploit Database, Exploit-db,» [En línea]. Available: https://www.exploit-db.com/about-exploit-db
- Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf
- PTES Standart (2018). PTES Technical Guidelines. Obtenido de: http://www.penteststandard.org/index.php/PTES_Technical_Guidelines.
- Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf
- Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291
- Mintic. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
- Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

- OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26) Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

- El Tiempo (2015). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. Recuperado de: Informe militar sobre el caso Andrómeda - Archivo Digital de Noticias de Colombia y el Mundo desde 1.990 - eltiempo.com

- Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

- Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: https://www.incibe-cert.es/blog/owasp-4

- KOTENKO, I. POLUBELOVA, O. SAENKO, I. (2012). The Ontological Approach for SIEM Data Repository Implementation. Lab. of Comput. Security Problems, St. Petersburg Inst. for Inf. & Autom. (SPIIRAS), St. Petersburg, Russia

- Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

- PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

- Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. Recuperado de: https://metasploit.help.rapid7.com/docs/metasploitable-2

- Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

- Openwebinars, «¿Qué es Metasploit framework? Rizaldos, Hector,» [En línea]. Available: https://openwebinars.net/blog/que-es-metasploit/

- Ochobitshacenunbyte, «Principales usos de nmap, Ochobits, David,» [En línea]. Available: https://www.ochobitshacenunbyte.com/2020/04/22/principales-usos-de-nmap/
- Incibe-cert, «Testeando la seguridad en redes industriales, INCIBE,» [En línea]. Available: https://www.incibe-cert.es/blog/nvt-testeando-seguridad-redes-industriales#:~:text=OpenVAS%20(Open%20Vulnerability%20Assessment%20System,escaneo%20y%20gesti%C3%B3n%20de%20vulnerabilidades.

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

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

- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

- Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

- Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

- Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Anexo A Vídeo Sustentación

A continuación, se encuentra el enlace del vídeo en YouTube, donde se evidencia la sustentación del seminario realizado:

- ✓ https://youtu.be/Rxa6Szk431o

Anexo B Resultado Turnitin

El resultado de las coincidencias del escaneo del documento realizado por turnitin es el siguiente, donde se evidencia que cuenta con el 15% en coincidencias:

Fuente: Propia del autor.