CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOSÉ JULIÁN JARAMILLO MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

SEMINARIO ESPECIALIZADO

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

PASTO

2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOSÉ JULIÁN JARAMILLO MUÑOZ

TUTOR: ALEXANDER LARRAHONDO NUÑEZ

SEMINARIO ESPECIALIZADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

SEMINARIO ESPECIALIZADO

EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

PASTO

2021

TABAL DE CONTENIDO

PAGINA

LISTA DE FIGURAS

PAGINA

INTRODUCCIÓN

En este presente trabajo vamos a realizar un análisis de selección de personal dentro de una entidad prestadora del servicio de seguridad informática y en su contrato se desglosarán todos los apartes con sus respectivos acuerdos, y realizar un análisis de que leyes se pueden vulnerar en este contrato y mirar si las directrices aquí dadas violentan alguna ley y daremos a conocer el dónde y porque de esto.

Vamos a poder escoger y dar a conocer nuestro punto de vista sobre una oferta laboral aquí brindada.

Analizaremos un caso real y podremos dar nuestro punto de vista y dar a conocer las leyes aquí vulneradas.

Vamos a desarrollar un laboratorio donde podremos identificar el uso de herramientas para vulnerar la seguridad de un sistema y hondar un poco más en el tema de la seguridad informática, también se debe desarrollar un entrono real el cual nos permita verificar estas vulnerabilidades desarrolladas en el presente trabajo.

Y se va a definir con argumentos técnicos que se debe indagar en el momento de un ataque, se darán a conocer qué medidas se pueden tomar para el endurecimiento de un sistema y dar la solución para que un ataque a nuestro sistema no se vuelva a presentar se van a explicar las diferencias entre un equipo Blueteam y un equipo de respuesta a ataques informáticos, deberemos explicar si un equipo de Blueteam nos indica trabajar con CIS que beneficios nos traería y del porque trabajaríamos con este, además se darán a conocer las principales características que posee un SIEM y por último se explicaran 3 herramientas para la contención de ataques informáticos.

GLOSARIO

BLUE TEAM: Un equipo azul es un conjunto de personas que realiza un análisis de los sistemas de información para garantizar la seguridad, identificar fallas de seguridad, verificar la efectividad de cada medida de seguridad y asegurarse de que todas las medidas de seguridad continuarán siendo efectivas después de la implementación.

COPNIA: autoridad pública encargada de proteger a la sociedad del inadecuado ejercicio profesional de los ingenieros, profesionales afines y auxiliares, mediante la autorización, inspección, control y vigilancia, que se concreta, de acuerdo con las competencias otorgadas por la Ley, con la inscripción en el Registro Profesional y con la función como Tribunal de Ética Profesional.

CVE: lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.

EXPLOIT DB: archivo definitivo de exploits y software vulnerable. Un gran recurso para probadores de penetración, investigadores de vulnerabilidades y adictos a la seguridad.

HOST: la expresión host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella

METASPLOIT: 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.

NESSUS: programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos.

NMAP: programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma.

OPENVAS: software que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos

OVA: Los Objetos Virtuales de Aprendizaje (OVA) son un conjunto de recursos digitales, auto contenible y reutilizable. Hacen posible el acceso a contenidos educativos, integrando diferentes elementos multimedia para presentar un recurso más didáctico para el estudiante.

PENTESTING: Una prueba de penetración, o pentest, ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos.

REDTEAM: Se nombra como equipo rojo a un grupo independiente que ayuda a una entidad a optimizarse a sí misma. Por intermedio de la realización de ataques a un objetivo, se estudian sus debilidades.

VIRTUAL BOX: software de virtualización para arquitecturas x86/amd64. Actualmente es desarrollado por Oracle Corporation.

VULNERABILIDAD: expresión de ciberseguridad que se refiere a un desperfecto en un sistema que podría dejarlo indefenso ante los atacantes.

OBJETIVOS

OBJETIVO GENERAL:

Identificar las diferencias entre los equipos RedTeam Y BlueTeam y así precisar roles y compromisos a ejecutar dentro de una entidad.

OBJETIVOS ESPECIFICOS:

Identificar las operaciones de los equipos Red Team & Blue Team de una entidad bajo los criterios éticos y legales. Señalar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Expresar habilidades de contención mediante el estudio de riesgos y vulnerabilidades en una infraestructura TI.

1. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

LEGISLACIÓN LEYES Y DECRETOS DENTRO DEL MARGEN LEGAL DE COLOMBIA

Las organizaciones hoy en día, bien sean empresas, grandes o pequeñas, son entes dinámicos que interactúan con el medio ambiente y enfrentan amenazas de diversa índole.

Dichas amenazas comprenden generalmente a un alto grupo de usuarios, eventos, situaciones o actos que pueden ocasionar o ser un peligro para la organización, atacando sus puntos más vulnerables.

Tabla1. Delitos informáticos y artículos de la legislación nacional

No	DELITO	ARTICULOS LEGISLACION
1	**Facilitar el acceso de terceros a información sin la debida autorización**	Ley 1273 de 2009 - Artículo 269ª *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
2	**Uso indebido de la infraestructura tecnológica**	Ley 1273 de 2009 - Artículo 269D *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
3	**Accesos no autorizados**	Ley 1273 de 2009 - Artículo 269ª *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en

No	DELITO	ARTICULOS LEGISLACION
		pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
4	**Suplantación de identidad**	Ley 1273 de 2009 - Artículo 269ª *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
5	**fraude**	Ley 1273 de 2009 - Artículo 269D *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
6	**Robo de hardware**	Ley 1273 de 2009 - Artículo 269D *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
7	**Destrucción de información**	Ley 1273 de 2009 - Artículo 269D *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
8	**Espionaje**	Ley 1273 de 2009 Artículo 269C Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en

No	DELITO	ARTICULOS LEGISLACION
		su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
9	**Virus y malware**	Ley 1273 de 2009 - Artículo 269E *Uso de software malicioso*. 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 1.000 salarios mínimos legales mensuales vigentes.
10	**Violación de datos personales**	Ley 1273 de 2009 - Artículo 269F Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Fuente: www.delitosinformaticos-en Colombia

Autores: *Alberto Caicedo Montenegro, Johana Patricia Manosalva Arteaga, José Julián Jaramillo Muñoz, Mario Andrés Chávez Rosero*

2. En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

ETAPAS DEL PENTESTING

Estas consisten en realizar pruebas de ofensivas contra mecanismos defensivos todo esto para poder identificar y corregir posibles vulnerabilidades:

Fase de recolección de información: En esta etapa debemos recopilar información sobre el sistema que será atacado y en este debemos identificar toda la información posible.

Fase de búsqueda de vulnerabilidades: En esta vamos a analizar toda la información recolectada en la anterior fase y tendremos que identificar las vulnerabilidades

Fase de explotación de vulnerabilidades: En esta fase es donde vamos a conseguir permisos, credenciales o i9nclñuso vulnerar el sistema.

Fase de informe: Esta se da al finalizar todas las demás fases y es donde documentamos y donde se especifica el test de intrusión y las herramientas y técnicas utilizadas.

3. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Herramientas:

- **Metasploit**
- **Nmap**
- **OpenVas**

Servicios en línea:

- **ExploitDB**
- **CVE**

HERRAMIENTAS:

METASPLOIT

Este es un proyecto de código abierto que se usa para la seguridad informática y proporciona información de las vulnerabilidades de seguridad también brinda la posibilidad de visualizar un test de penetración, también otorga un sistema de firmas para la detección de intrusos.

NMAP

Esta es una aplicación de código abierto que se usa para explorar redes y así obtener información acerca de los servicios, sistemas operativos y vulnerabilidades.

OPENVAS

Este se trata de un framework y como principales características sirve para realizar una evaluación de vulnerabilidades y también nos brinda un informe de posibles soluciones.

SERVICIOS EN LÍNEA:

EXPLOITDB

Es utilizado para realizar pruebas de penetración y vulnerabilidades esta se puede definir como un directorio web de vulnerabilidades y en ella se puede observar de cómo sacar provecho de estas.

CVE

En este podemos verificar como un estilo de puntuación del impacto generado de una vulnerabilidad y esta se compone por tres características que son Base, Temporal y Entorno.

4. Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo – Escenario sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo – escenario es lo siguiente:

INSTALACIÓN TERMIANDA DE VIRTUALBOX Y CONFIGURACION DE UNA NUEVA RED

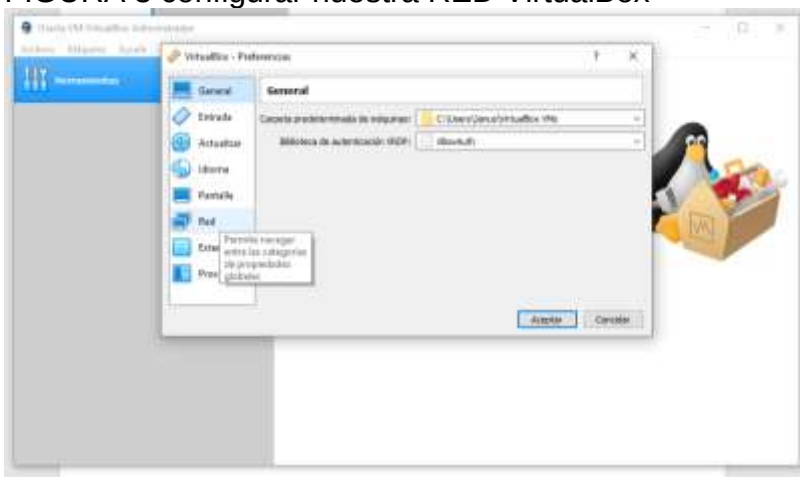
FIGURA 1 configurar nuestra RED VirtualBox

Una vez instalado VirtualBox vamos a configurar nuestra RED

FIGURA 2 configurar nuestra RED VirtualBox

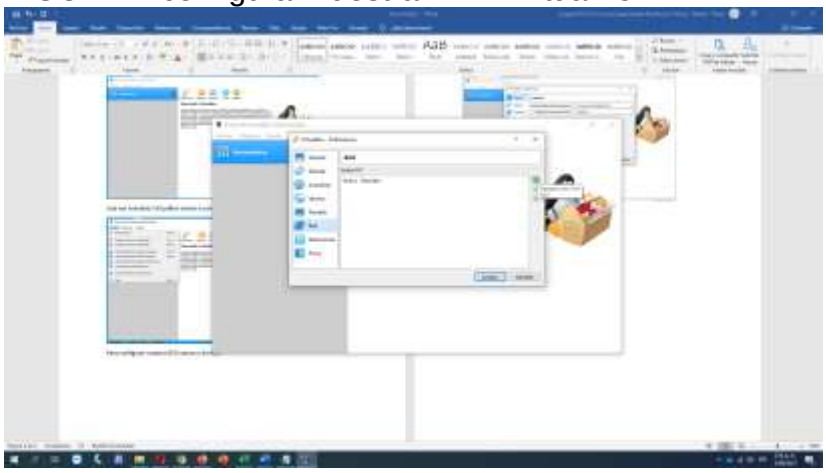
Para configurar nuestra RED vamos a **Archivo**

FIGURA 3 configurar nuestra RED VirtualBox



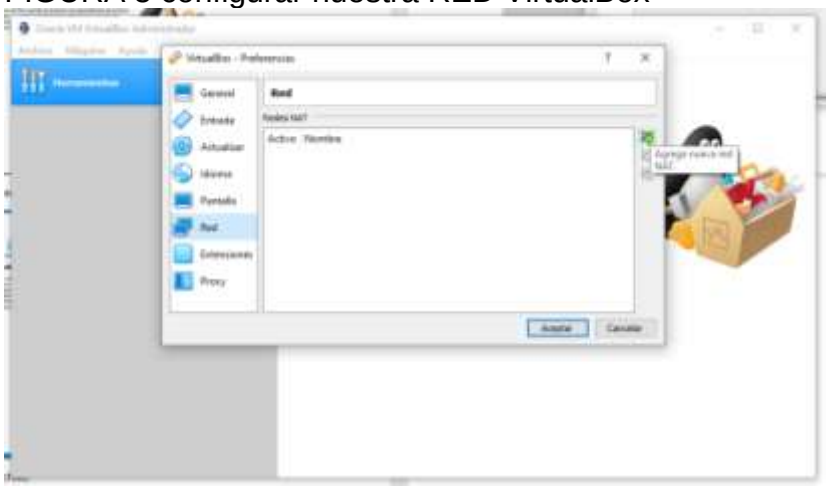
Escogemos la opción **Preferencias**

FIGURA 4 configurar nuestra RED VirtualBox



Escogemos La opción **Red**

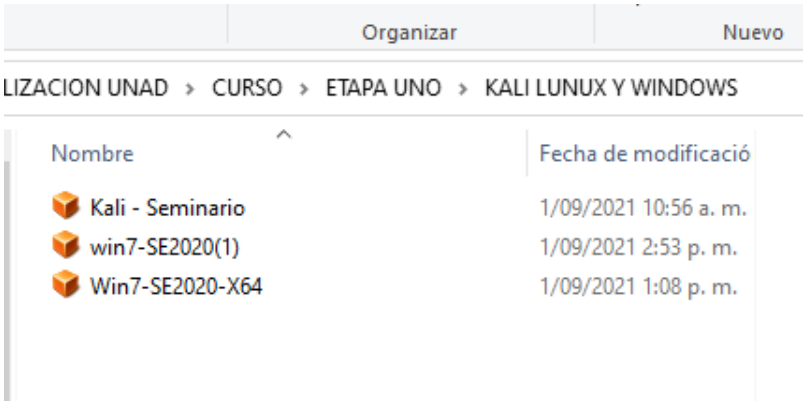
FIGURA 5 configurar nuestra RED VirtualBox



Y por último agregamos una **Nueva Red**

INSTALACIÓN KALI LINUX

FIGURA 6 Instalación KALI Linux VirtualBox



Tenemos nuestras **OVAS** listas para ser instaladas en nuestra máquina virtual y vamos a seguir los siguientes pasos:

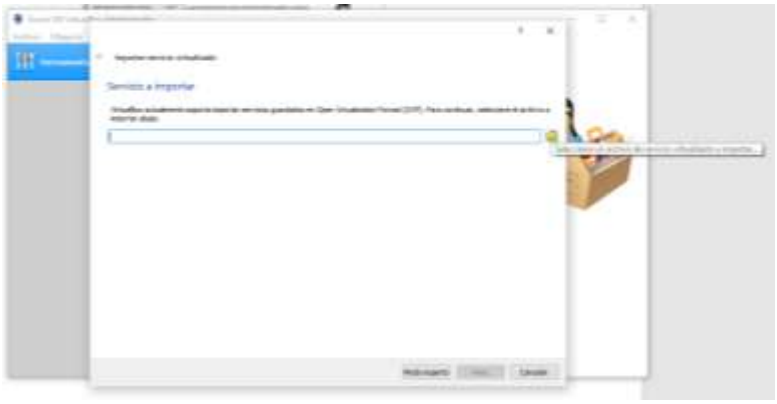
FIGURA 7 Instalación KALI Linux VirtualBox

Tomamos la opción de **Archivo**

FIGURA 8 Instalación KALI Linux VirtualBox

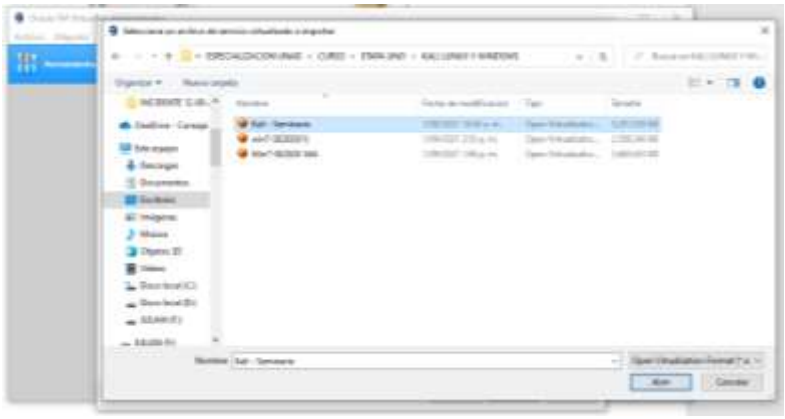
Tomamos la opción de **Importar Servicio Virtualizado**

FIGURA 9 Instalación KALI Linux VirtualBox



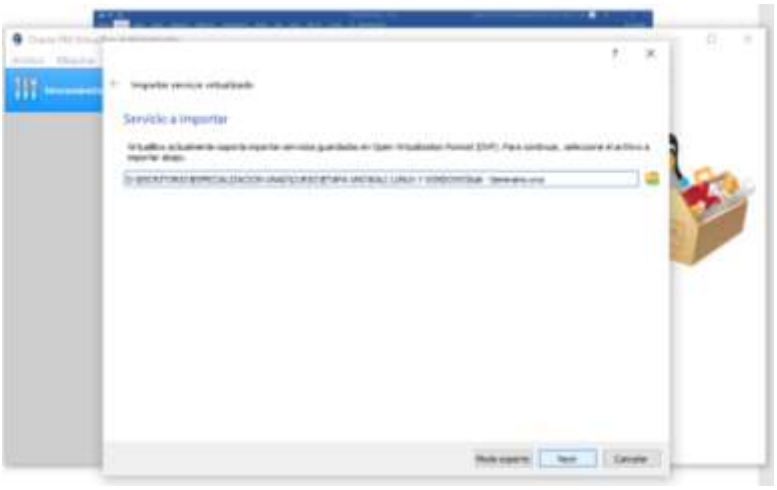
Seleccionamos el archivo en la **ubicación** donde lo tengamos guardado

FIGURA 10 Instalación KALI Linux VirtualBox



Escogemos el **sistema operativo** que corresponda y le damos clic en **Abrir**

FIGURA 11 Instalación KALI Linux VirtualBox

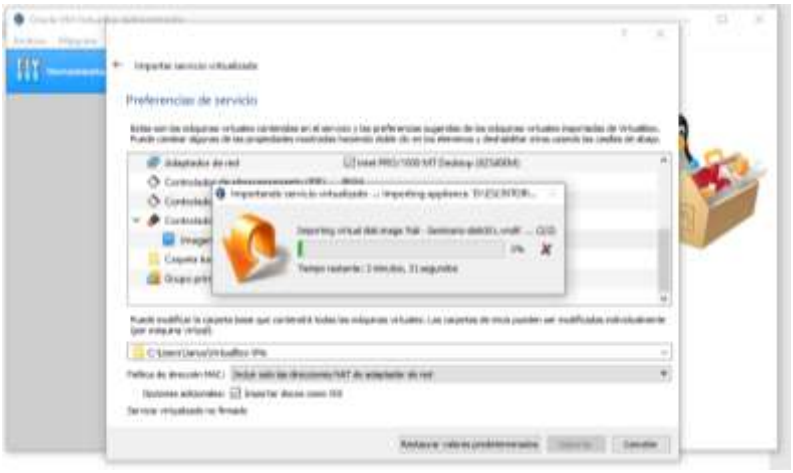


Una vez escogido el sistema operativo le damos clic en la opción **Next**

FIGURA 12 Instalación KALI Linux VirtualBox

Nos dirigimos a la opción **Importar**

FIGURA 13 Instalación KALI Linux VirtualBox



Una vez escogemos la opción importar el empieza con la instalación del sistema operativo

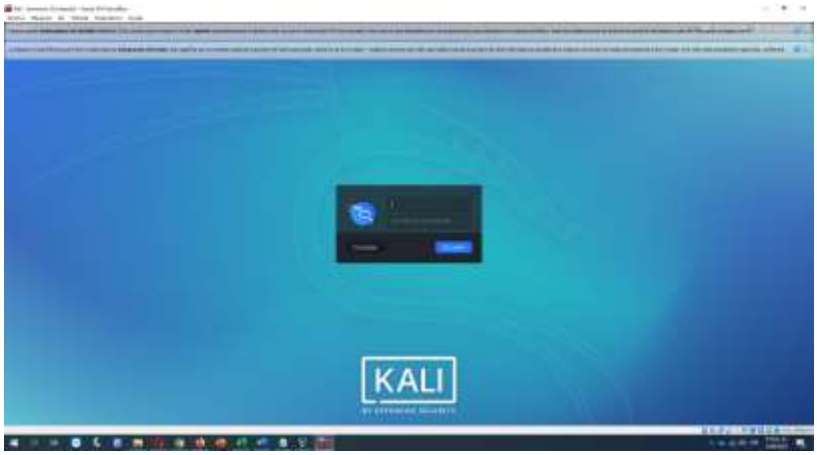
FIGURA 14 Instalación KALI Linux VirtualBox

Aquí observamos que ha terminado con la instalación del sistema operativo

FIGURA 15 Instalación de los Tres Sistemas Operativos

Aquí observamos como están ya instalados los tres sistemas operativos

FIGURA 16 KALI Linux VirtualBox



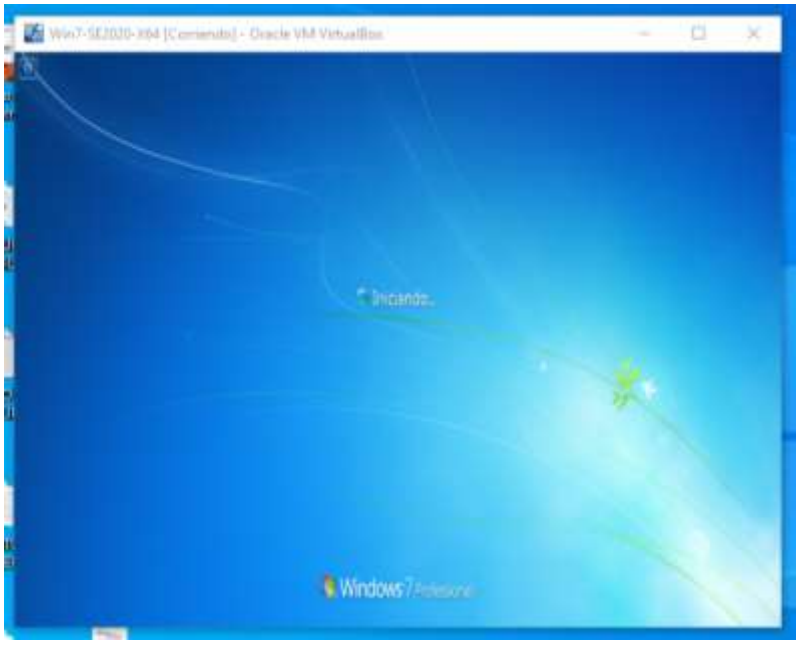
Aquí se observa la pantalla de entrada del sistema operativo Kali Linux, ingresamos usuario y contraseña para dar inicio. Usuario: estudiante Contraseña: unad2020

FIGURA 17 KALI Linux VirtualBox

Aquí podemos visualizar la pantalla de inicio del sistema operativo Kali Linux

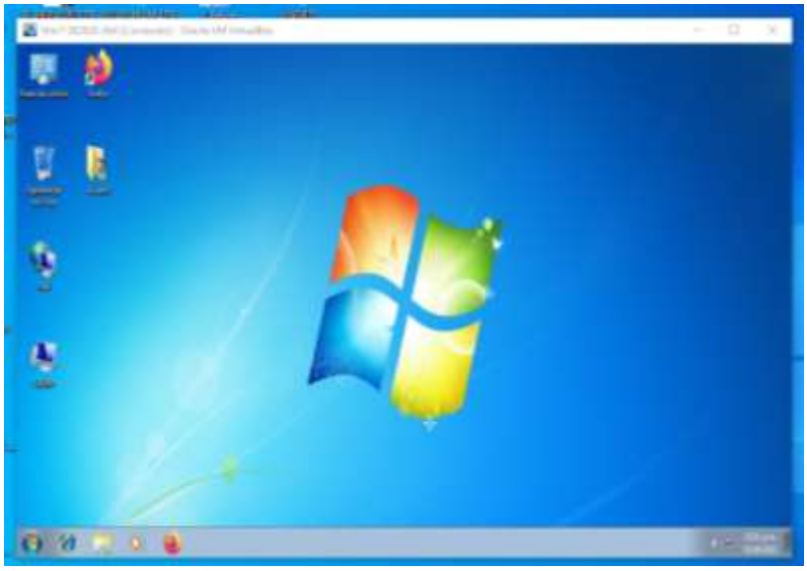
WINDOWS 7 64 BITS

FIGURA 18 WINDOWS 7 64 BITS VirtualBox



Aquí observamos el arranque del sistema operativo Windows de 64 bits

FIGURA 19 WINDOWS 7 64 BITS VirtualBox



Visualizamos el pantallazo de inicio de Windows 7 64 bits

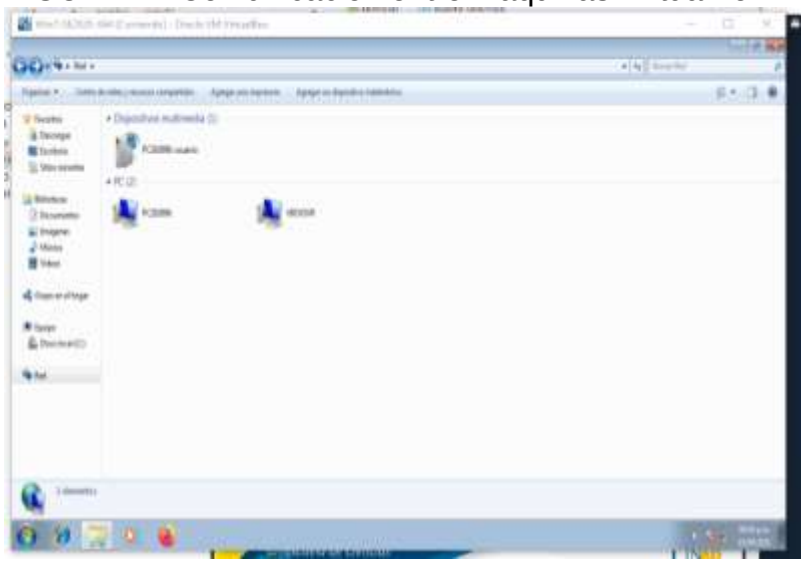
WINDOWS 7 32 BITS

FIGURA 20 WINDOWS 7 32 BITS VirtualBox

Aquí podemos visualizar la pantalla de inicio de Windows 7 32 bits.

VERIFICAR COMUNICACIÓN ENTRE MAQUINAS VIRTUALES

FIGURA 21 Comunicación entre Maquinas VirtualBox

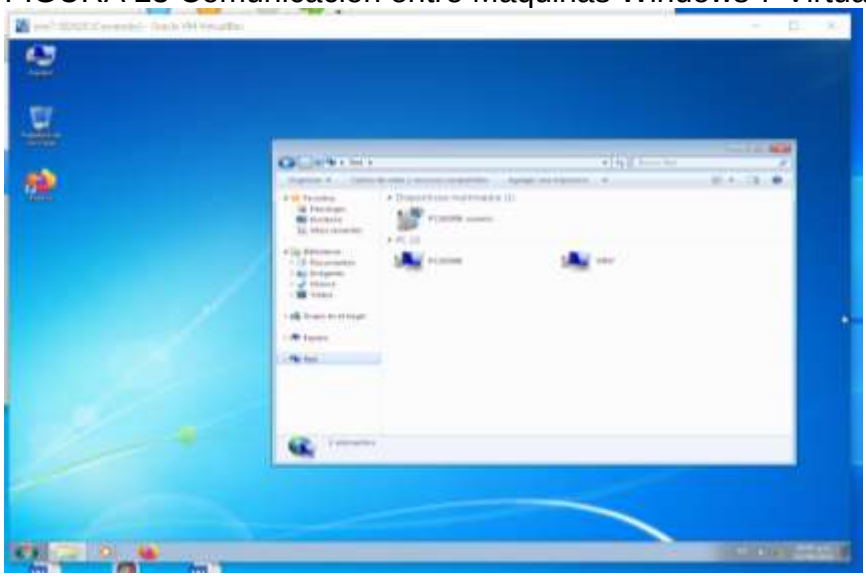


Aquí observamos la comunicación entre **WIDONWS 7 DE 64 BITS Y KALI LINUX**

FIGURA 22 Comunicación entre Maquinas KALI Linux y Windows 7 VirtualBox

Aquí observamos la comunicación entre **KALI LINUX Y WINDOWNS 7 DE 64 BITS**

FIGURA 23 Comunicación entre Maquinas Windows 7 VirtualBox



Aquí observamos la comunicación entre **WINDOWS 7 DE 32 BITS Y WINDOWS 7 DE 64 BITS**

1. **De manera individual usted deberá leer el problema que se encuentra en el anexo 2 – Escenario 2, además deberá leer y analizar el anexo 3 – Acuerdo para generar la solución a las siguientes preguntas orientadoras:**

En el Anexo 2 – Escenario 2 se evidencian una serie de faltas como son:

- Se debe realizar una verificación y análisis exhaustivo del contrato.
- Analizar a fondo los actos ilícitos encontrados.
- Verificar por que fue despedido el abogado.
- Observar la omisión de función realizada por la alta gerencia.

Y en el Anexo 3 encuentro varias irregularidades como son:

Encubrir actos ilícitos o ilegales.

- ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

"Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por ***un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal,*** *por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores".*

Respuesta:

En la parte inicial donde el abogado es despedido por encontrar procesos ilícitos iría en contravía de las siguientes normas:

Se faltaría a la Ley 1778 del 2016 la cual se dictan normas contra actos de corrupción u/o soborno dentro de la empresa.

El siguiente estatuto que se estaría vulnerando es la Ley 1474 del 211 donde se establecen las medidas para la lucha contra la corrupción.

Y por último y no menos importante la Ley 50 de 1990 cuando se presenta un despedido de forma injustificada.

La segunda irregularidad que se encuentra en este texto es la falta de omisión de función por parte de la gerencia la no revisar los contrato con los cuales reclutara al nuevo personal. La cual esta reglamentada por la Ley 1474 del 211.

2. **Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.**

"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 Whitehouse Security no podrán ser divulgados****".*

Respuesta:

En este fragmento señalado iría en contra vía de la ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos.

"2. 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 de información, accesos abusivos a sistemas informáticos"."***

"parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados".

Respuesta:

En este párrafo señalo se puede evidenciar que se está violando la ley 1273 de 2009 más específicamente en los artículos:

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.

Si bien se adquiere un contrato con esta empresa, no es el ente competente y tampoco especifica el cómo se van a realizar estas actividades.

"Tercera. Origen de la información confidencial: ***provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte*** *y sin que requiera advertir su carácter confidencial".*

Respuesta:

En este fragmento señalado iría en contra vía de la ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos. Ya que no especifica o precisa las formas o procedimientos para lograr el objetivo.

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

Respuesta:

En este fragmento señalado iría en contra vía de la ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos, además iría en contra de la moral y ética profesional al encubrir actos ilegales que vulneren derechos de terceros.

4. **"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas".**

Respuesta:

En este fragmento señalado iría en contra vía de la ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos, además iría en contra del control que se debe hacer o realizar de la información que involucre actos ilícitos, dificultando así el trabajo de control de los entes competentes.

9. *"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 Whitehouse Security".

Respuesta:

En este fragmento señalado iría en contra vía de la ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos, además no puede ser la entidad la responsable de investigar y juzgar al mismo tiempo ya que para eso hay entes de control dictaminados por la ley.

"Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. **En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security".**

Respuesta:

Aquí debe existir una responsabilidad compartida y la entidad también está en la obligación de presentar sus sustentos legales y no solo recaer la responsabilidad sobre el receptor.

3. **¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted cómo experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de 1 $15.000.000 de pesos colombianos mensuales y contrato vitalicio? e argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.**

Respuesta:

No aceptaría, toda vez, que si bien el contrato es con un muy buen beneficio monetario, va en contra de todas las normas legales y leyes existentes en Colombia, además estaría en contra vía de mi ética personal y profesional ya que en este contrato se estipulan muchas violaciones tanto a los derechos de la privacidad con de terceros dando mucha libertad a la entidad para la libre manipulación de esta información.

Y además se iría en contra vía del código del COPNIA en los siguientes artículos:

- ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES.

- ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.

- ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.
- ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL".

4. **Deberá buscar la noticia del caso "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.**

En este caso podemos observar una complejidad en el desarrollo de esta ya que si bien el Ejercito Nacional acredita dicha creación de la facha en un marco legal no se responsabiliza de sus operadores que son adscritos a la institución dejando así de lado la obligación compartida que tenían estos con sus operarios o subalternos, se puede observar una vulneración de los derechos en cuanto se manipula a los participantes en estas actividades con engaños y ocultación del porque se realizan dichas actividades en ese sitio y con qué fines se utilizaría esa información hay obtenida, si bien se dice que era con fines de conocimiento y aprendizaje podemos ver como los participantes nunca se les menciona o se les informa quien es el operador o benefactor de esta entidad, vulnerado así la buena fe de los aquí participantes dado que una vez a ellos se les explica quiénes son los benefactores de dicho proyecto los aquí partícipes se encuentran renuentes y dan a entender su inconformidad de lo hay sucedido, para mi aquí se violentan las siguientes leyes:

- Ley 1273 de 2009 ya que se vulneraria la seguridad de la información y se materializaría en hurtos y fraudes tecnológicos.

- Artículo 83, Constitución Política Colombiana - Principio de la buena fe.

- LEY 599 DE 2000 del código penal, engaño con fines de explotación.

- LEY 599 DE 2000 del código penal, reclutamiento ilegal.

ANEXO 4 – ESCENARIO 3

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos red team.

Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v.

2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

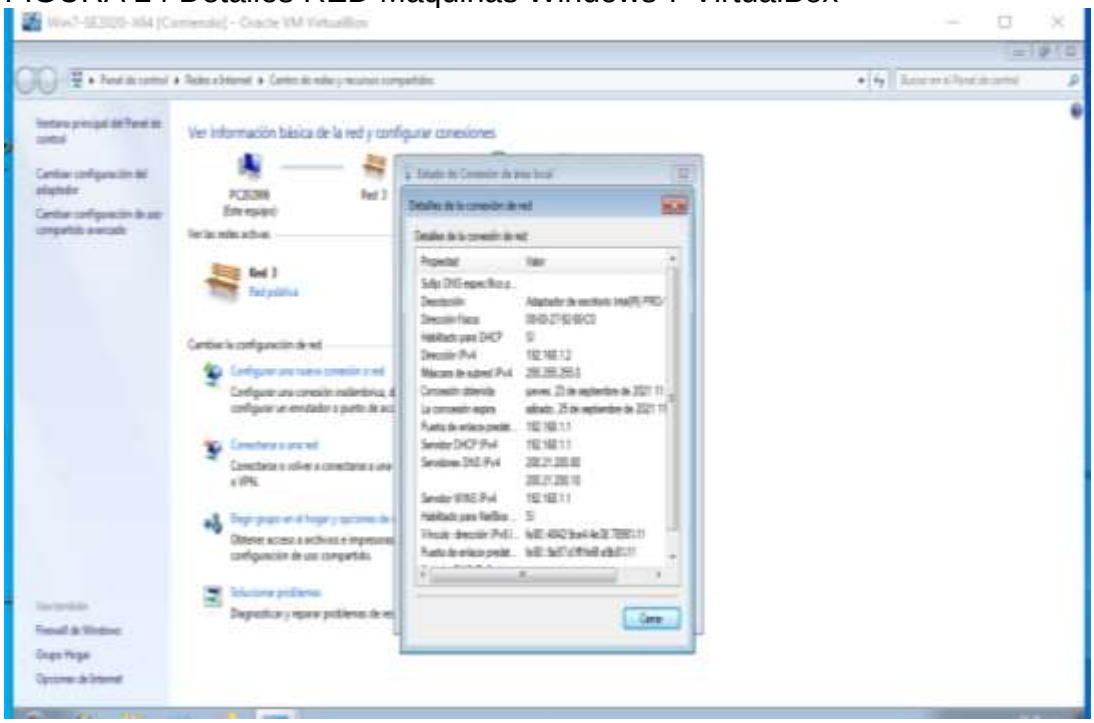
El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

1. **Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.**

- NMAP: esta herramienta multiplataforma utilizada para la exploración de redes se utiliza para poder identificar los puertos abiertos, los servicios que produce, sistema operativo y vulnerabilidades además tenemos que tener en cuenta como se comentó en un anterior trabajo que esta es una aplicación de código abierto.

- METASPLOIT: como ya lo di a conocer en un trabajo anterior este es un proyecto de código abierto que se usa para la seguridad informática y proporciona información de las vulnerabilidades de seguridad también brinda la posibilidad de visualizar un test de penetración, también otorga un sistema de firmas para la detección de intrusos.

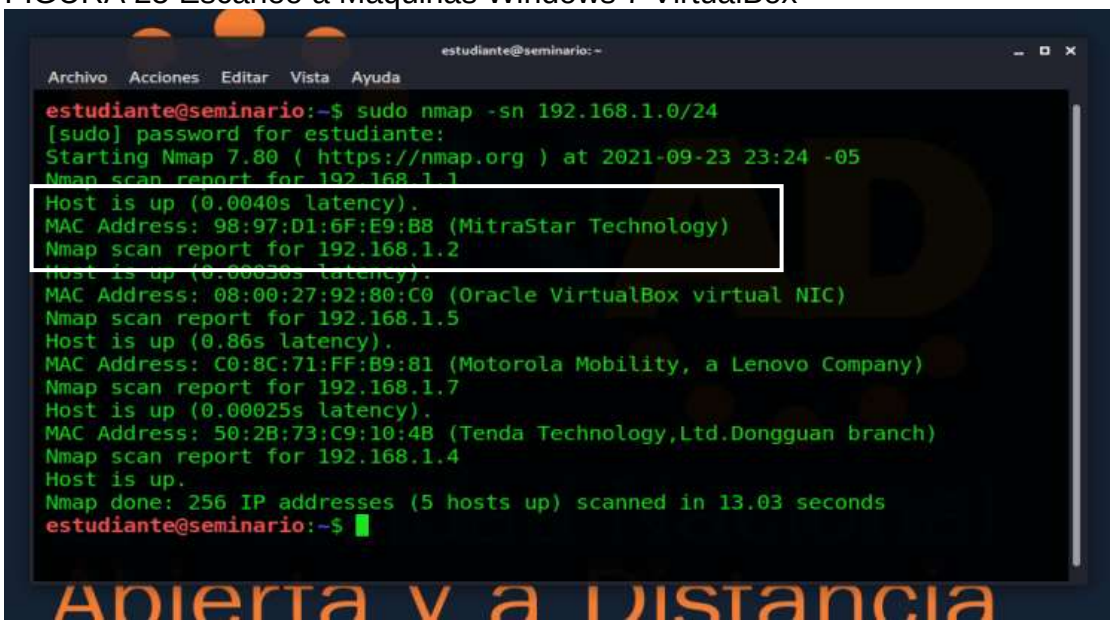
FIGURA 24 Detalles RED Maquinas Windows 7 VirtualBox



Fuente: Autor

Primero iniciamos verificando la dirección IP para que así `puedan observar más adelante que todas estas pruebas son reales y así puedan verificar cada paso a paso.

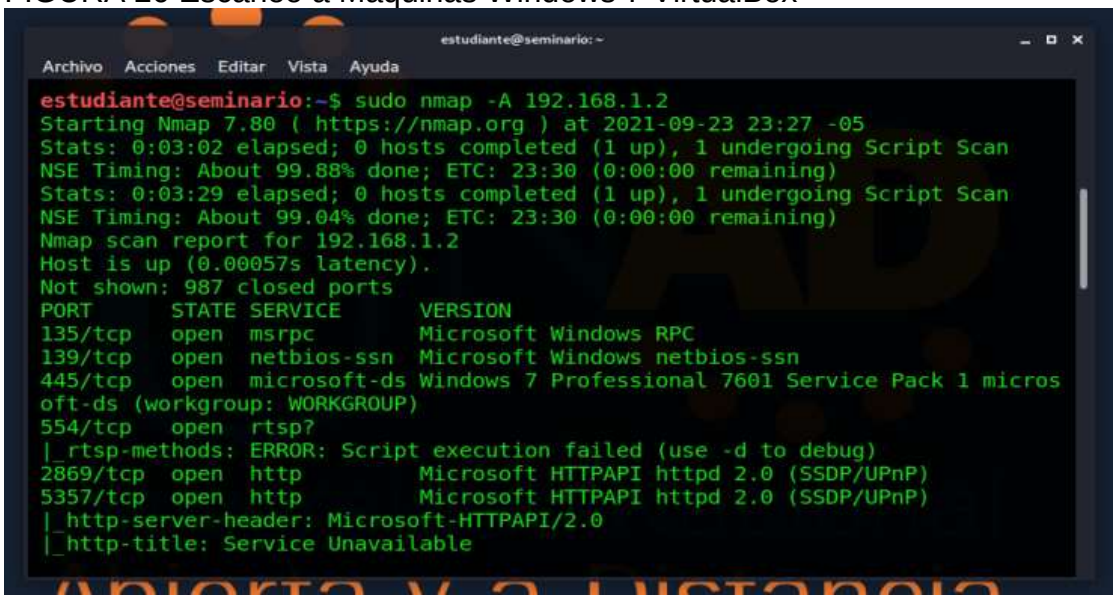
FIGURA 25 Escaneo a Maquinas Windows 7 VirtualBox



Fuente: Autor

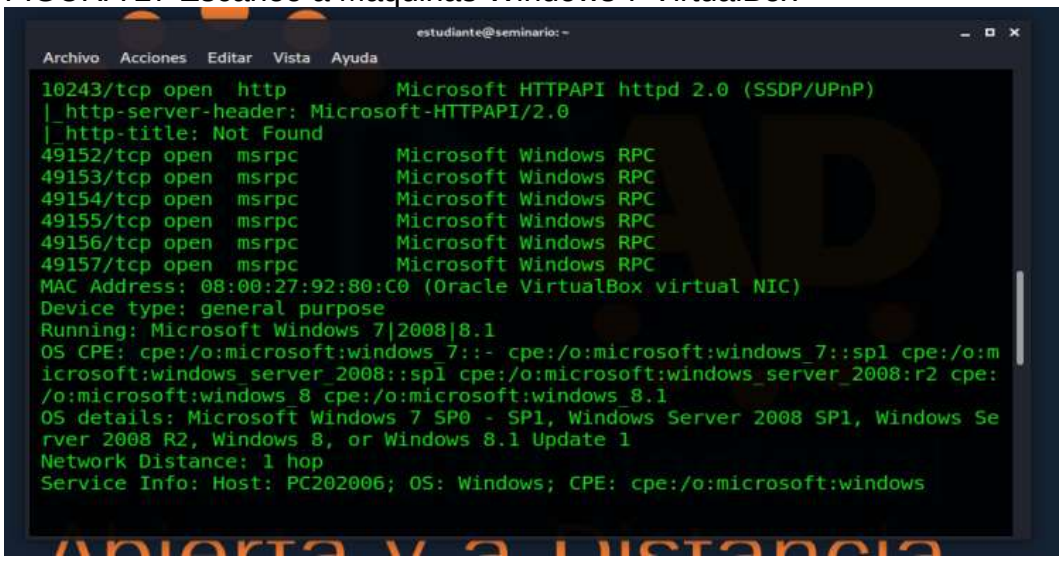
Aquí nos dirigimos a nuestro sistema operativo Kali Linux y por medio de una terminal vamos a realizar un escaneo con la herramienta NMAP aquí introducimos el comando sudo nmap -sn el cual nos dará como resultado los dispositivos conectados a la red.

FIGURA 26 Escaneo a Maquinas Windows 7 VirtualBox



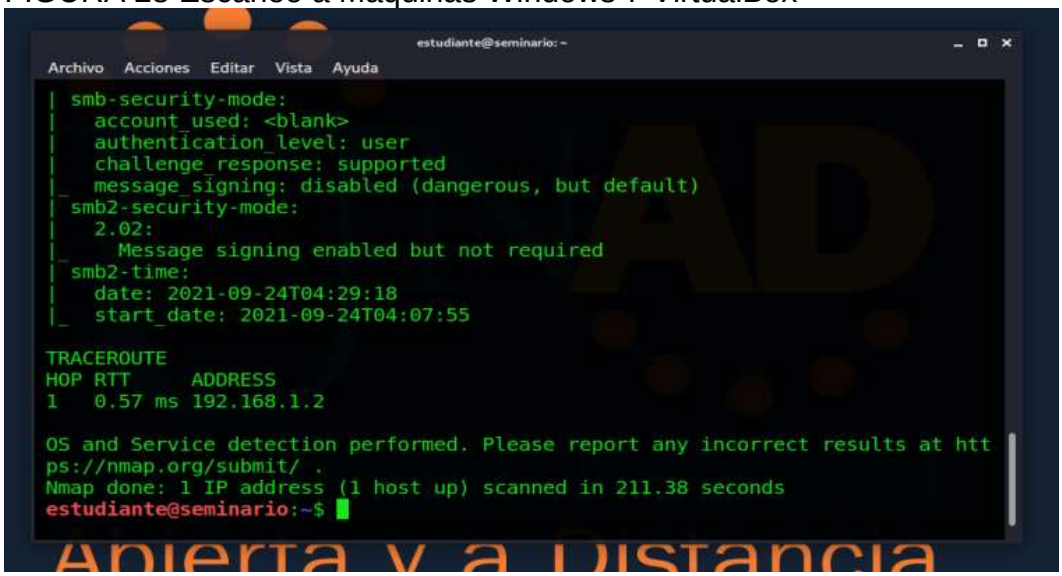
Fuente: Autor

FIGURA 27 Escaneo a Maquinas Windows 7 VirtualBox



Fuente: Autor

FIGURA 28 Escaneo a Maquinas Windows 7 VirtualBox



Fuente: Autor

En este punto vamos a verificar el sistema operativo y servicios por medio del comando sudo nmap -A

FASE DE INFORME

Aquí podemos observar que has posibles vulnerabilidades las cuales se pueden explotar por personal interno o externo a la entidad y que los hallazgos aquí encontrados nos sirven para decir que no se están cumpliendo con todas las medidas de seguridad requeridas y que estos fallos o vulnerabilidades son muestra que falta de actualización o mejora por parte del proveedor.

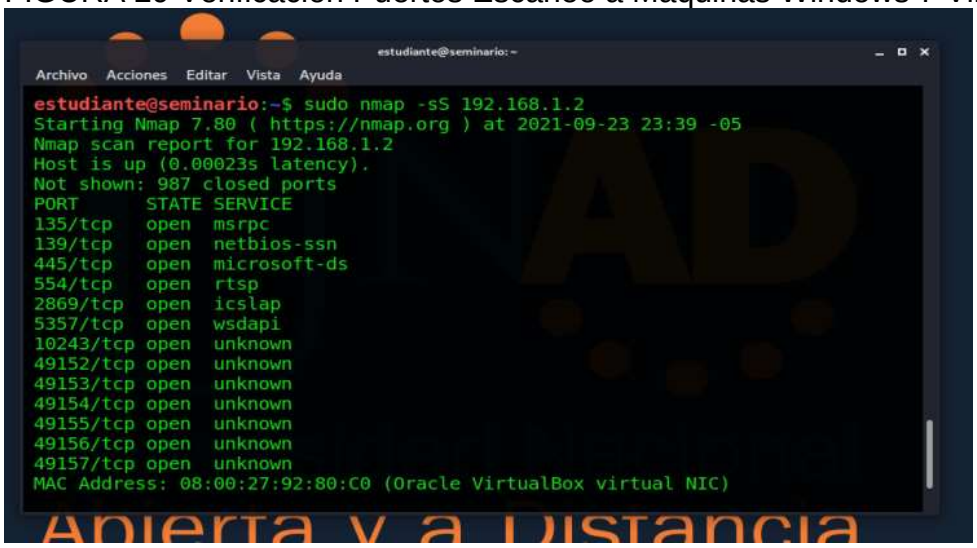
Le doy a conocer también al cliente como los equipos que se encuentran al servicio de la entidad están en un estado de vulnerabilidad el cual si no se realizan las correcciones adecuadas se seguirá estando en un estado de fácil ataque por personal tanto interno como externo a la entidad dando así una sensación de inseguridad en el manejo de su información.

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 7 X64.**

De primera mano se tiene que existe una falla o vulnerabilidad dentro de la entidad, se puede observar que según el análisis realizado que la aplicación Rejjetto es la que genera esta vulnerabilidad y esta esta asociada con un exploit.

Esto se pudo generar por una incorrecta configuración del firewall o una práctica errónea la cual es tener los puertos abierto todas estas malas políticas y falta de controles permite las vulnerabilidades en la información.

FIGURA 29 Verificación Puertos Escaneo a Maquinas Windows 7 VirtualBox

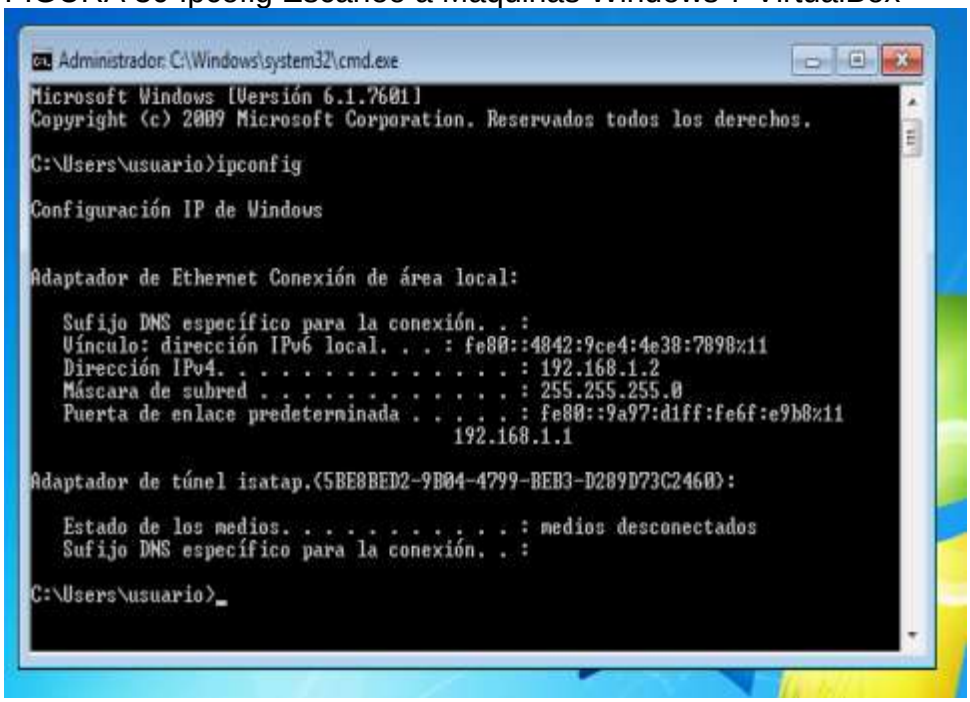


Fuente: Autor

Por medio del comando **nmap -sS** vamos a comprar si el puerto objetivo está abierto.

3. **¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"? ¿Qué puerto abre la aplicación específica en el anexo?**

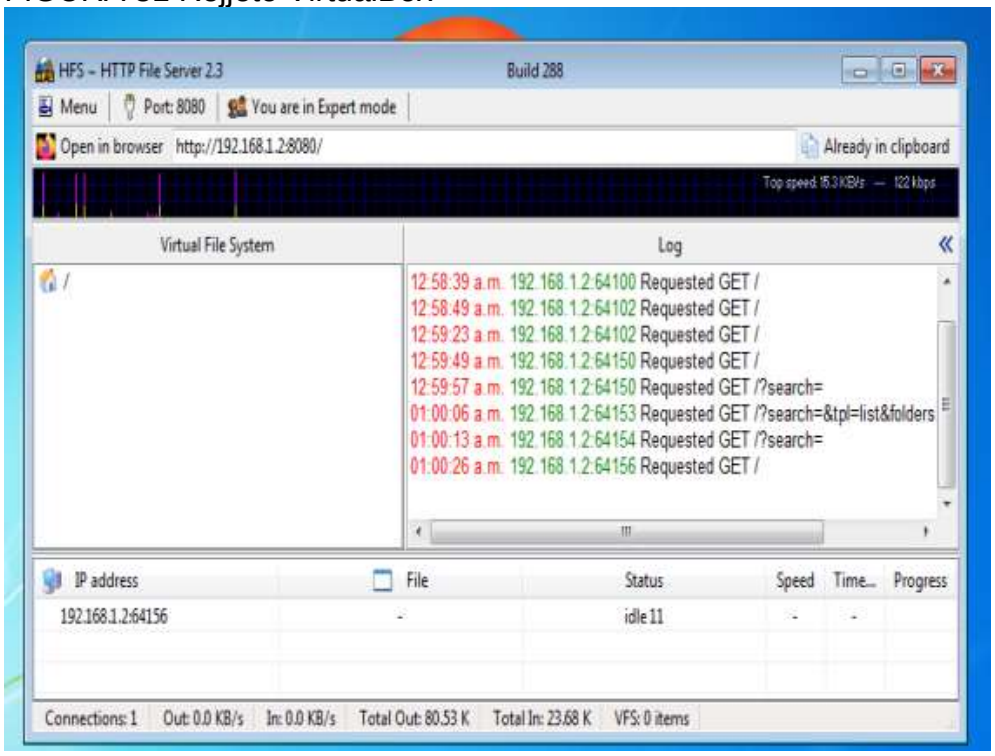
FIGURA 30 Ipcofig Escaneo a Maquinas Windows 7 VirtualBox



Fuente: Autor

Vamos a utilizar el comando **ipconfig** en el equipo con sistema operativo Windows 7 de 64 bits donde podemos observar que se tiene configurada la dirección ip 192.168.1.2

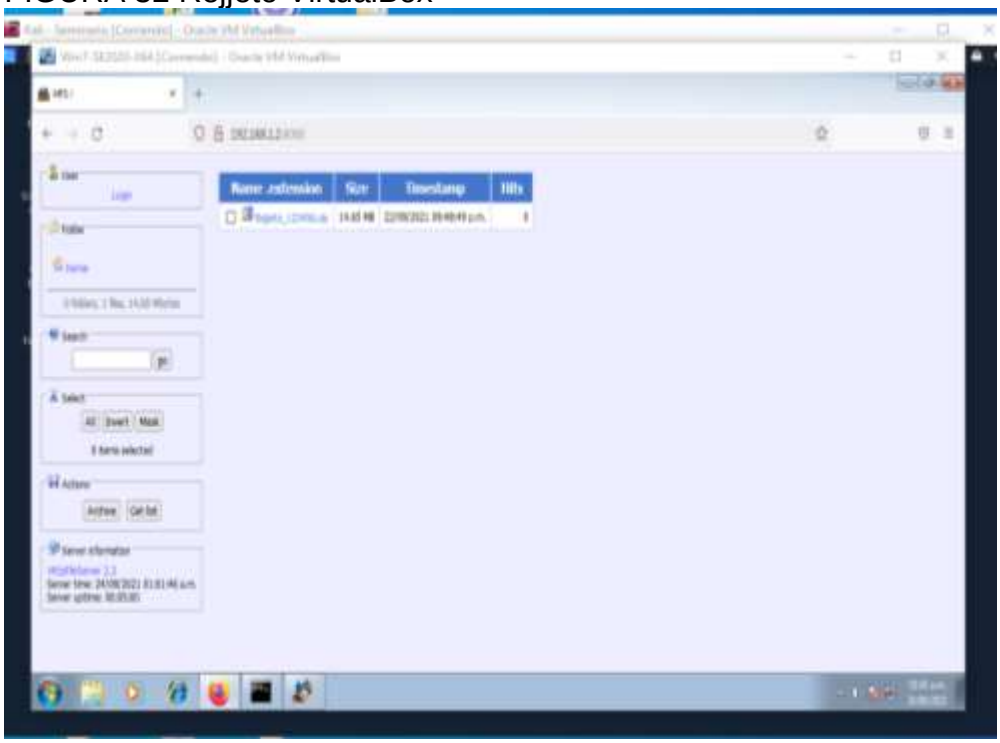
FIGURA 31 Rejjeto VirtualBox



Fuente: Autor

En esta imagen podemos observar cómo al ejecutar el programa Rejetto se abre el puerto 8080

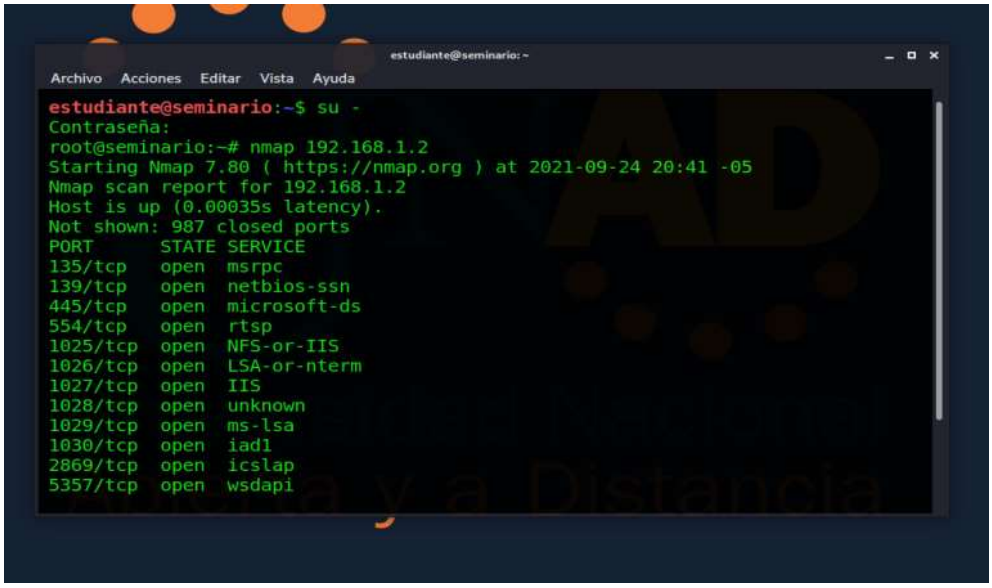
FIGURA 32 Rejjeto VirtualBox



Fuente: Autor

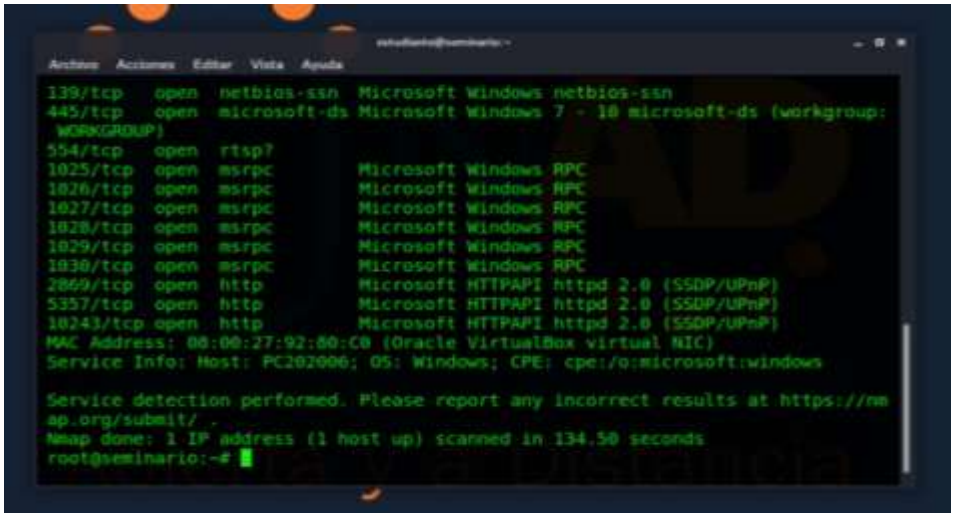
Aquí esta ejecutado el programa Rejetto y miramos como se tiene acceso a los archivos que se encuentran en el equipo con sistema operativo Windows 7 de 64 bits.

FIGURA 33 Uso Comando NMAP VirtualBox



Fuente: Autor

FIGURA 34 Uso Comando NMAP VirtualBox



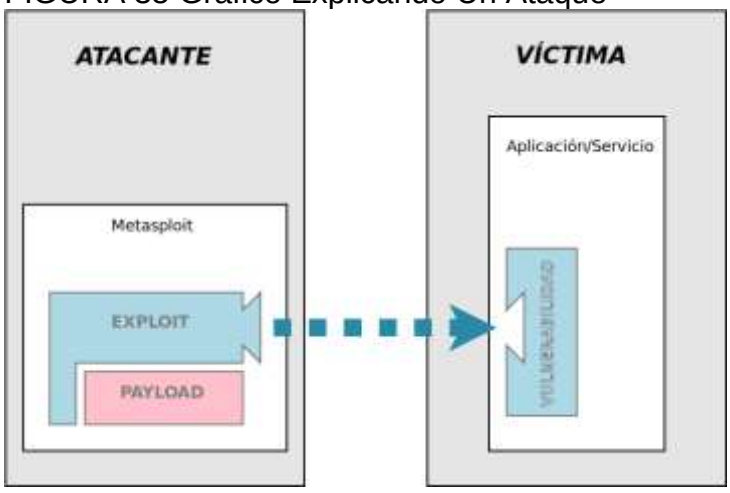
Fuente: Autor

Aquí podemos observar por medio del comando nmap un escaneo del sistema operativo y servicios.

4. **Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.**

Mediante las pruebas realizadas se pudo observar he identificar todas las falencias encontradas en la maquina en mención se puede decir que fue fácil de lograr gracias al exploit encontrado en el programa Rejjeto, para el ataque se utilizó la herramienta Metasploit, una vez identificamos las vulnerabilidades se procede a lanzar un ataque y poder aprovechar y comprometer el sistema.

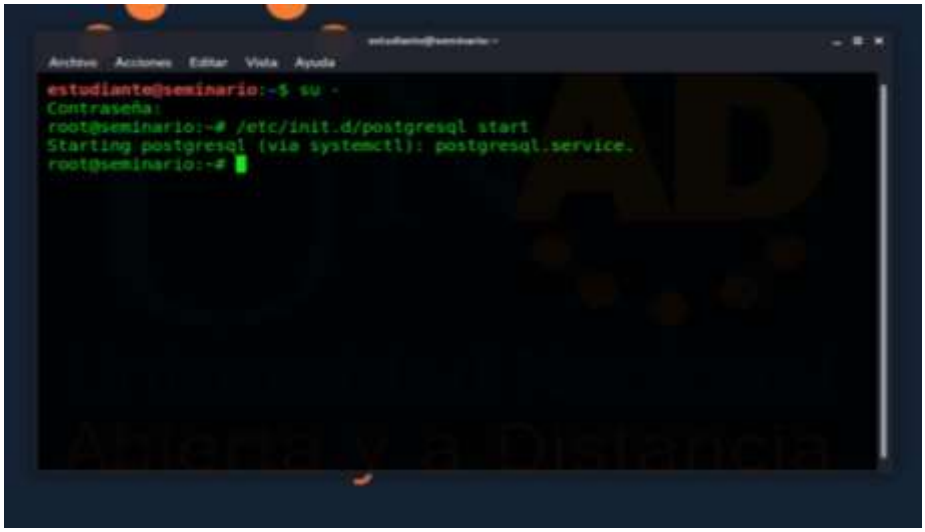
FIGURA 35 Grafico Explicando Un Ataque



Fuente: https://ccia.esei.uvigo.es/docencia/SSI/1819/practicas/ejercicio-metasploit/

5. **Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.**

FIGURA 36 Uso Comando SU- VirtualBox



Fuente: Autor

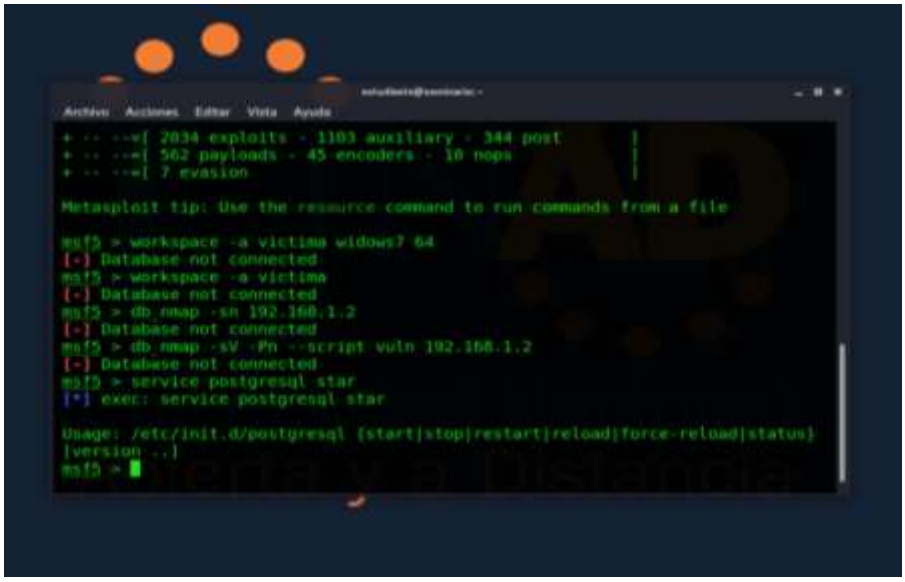
Primero vamos a ingresar como root mediante el comando su –

FIGURA 37 Uso Comando MSFCONSOLE VirtualBox

Fuente: Autor

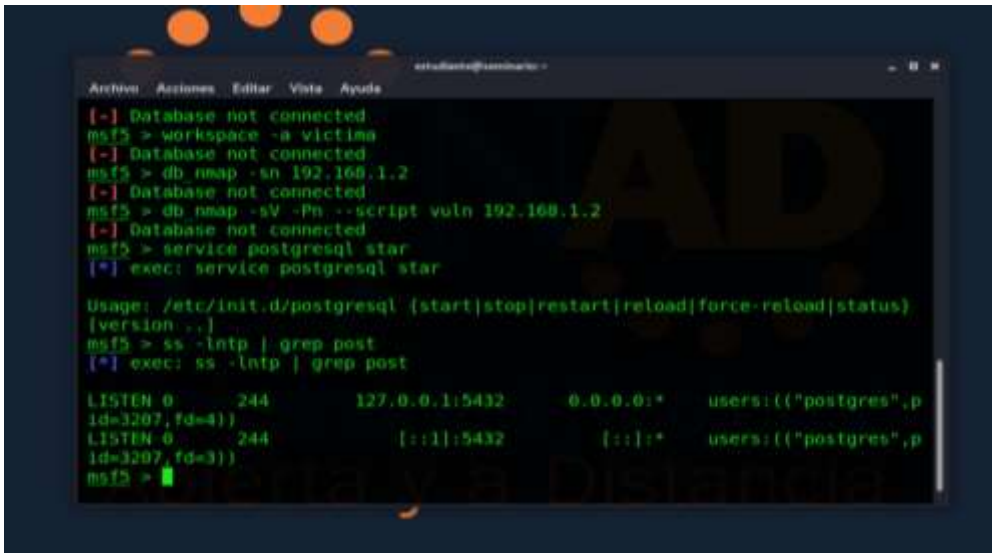
Ejecutamos el comando msfconsole

FIGURA 38 MSFCONSOLE VirtualBox



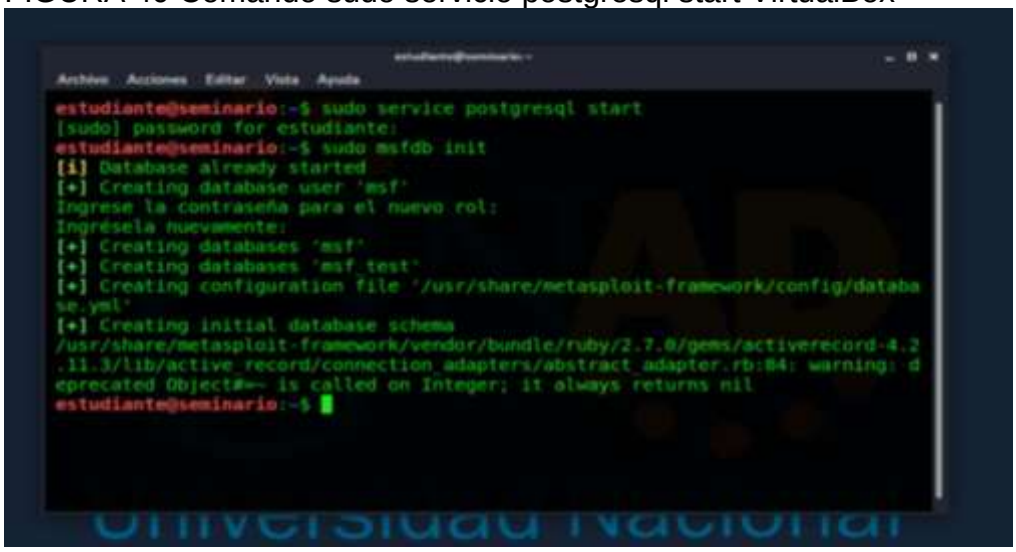
Fuente: Autor

FIGURA 39 MSFCONSOLE VirtualBox



Fuente: Autor

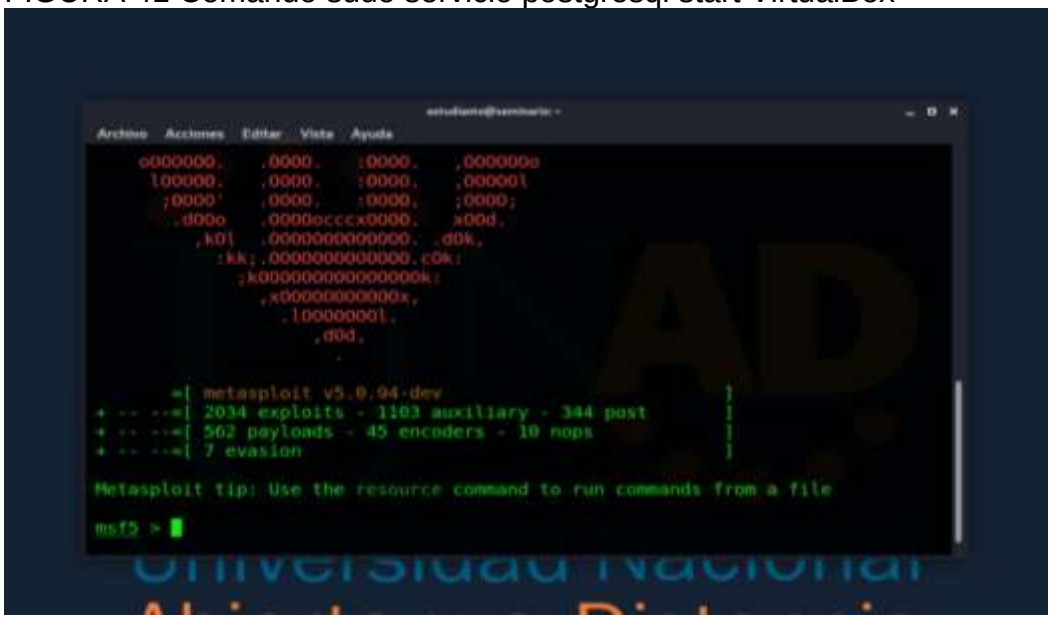
FIGURA 40 Comando sudo servicio postgresql start VirtualBox



Fuente: Autor

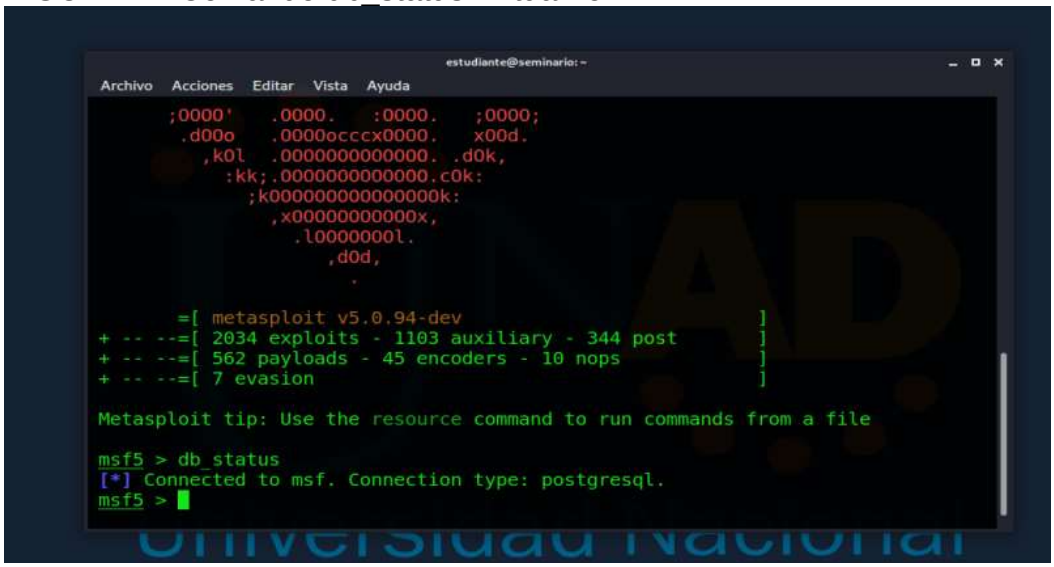
Ejecutamos el comando sudo servicio postgresql start para arrancar el servicio antes que todo.

FIGURA 41 Comando sudo servicio postgresql start VirtualBox



Fuente: Autor

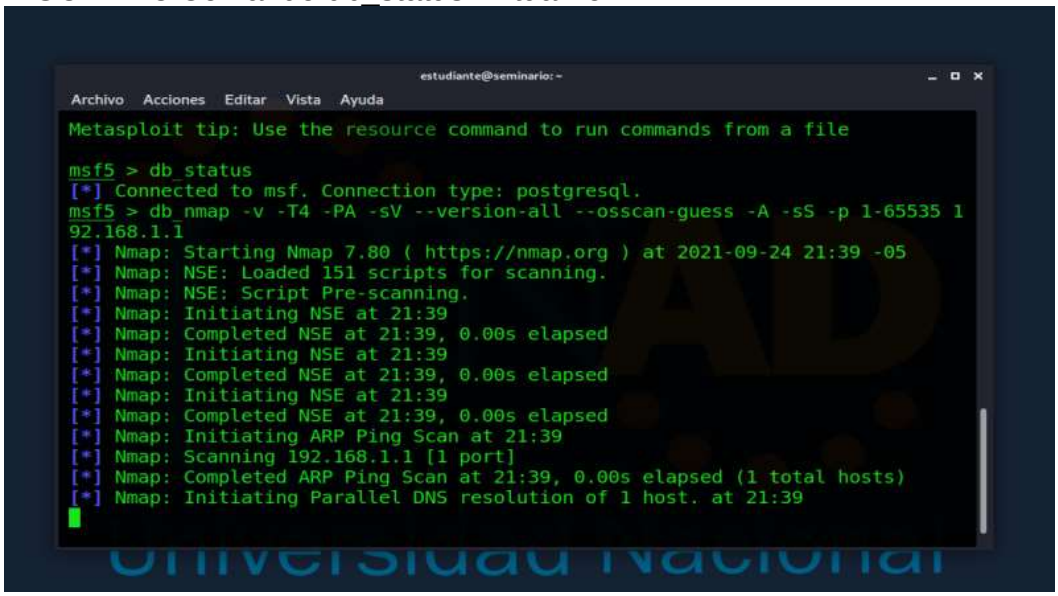
FIGURA 42 Comando db_status VirtualBox



Fuente: Autor

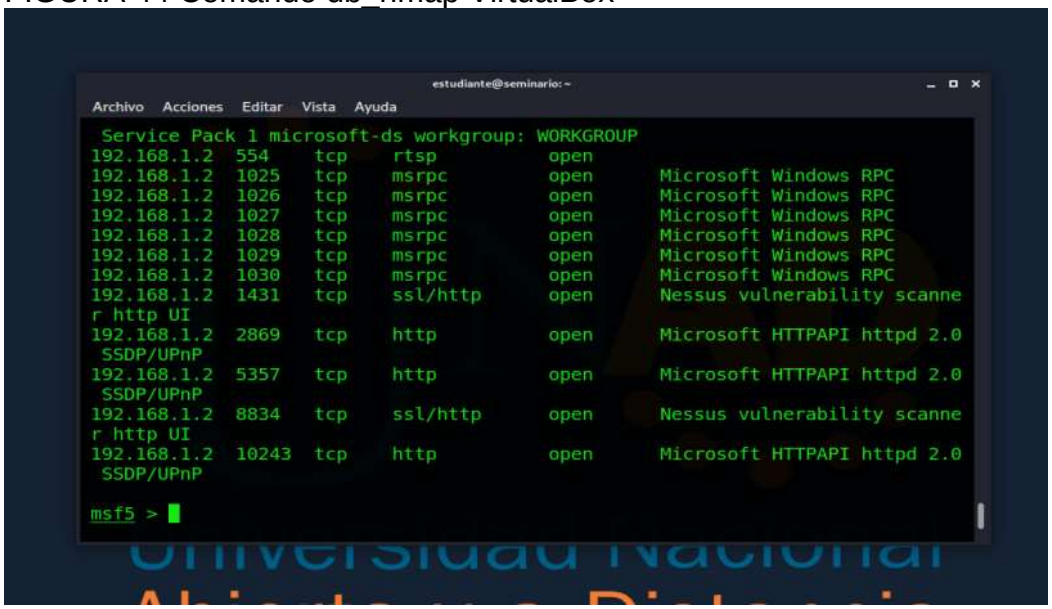
Ejecutamos le comando db_status para verificar la base de datos y que todo funcione de forma correcta

FIGURA 43 Comando db_status VirtualBox



Fuente: Autor

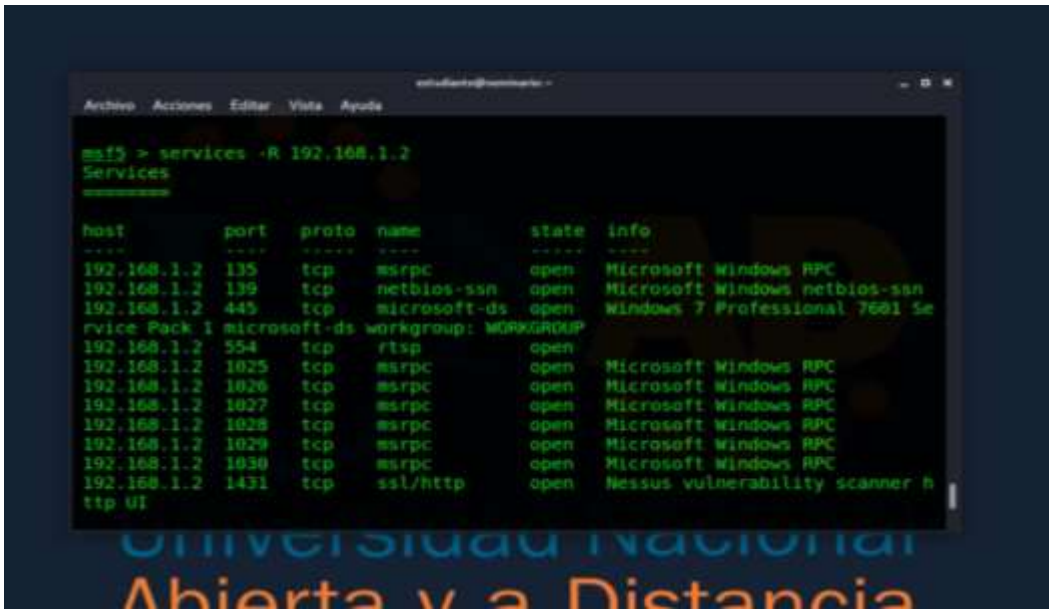
FIGURA 44 Comando db_nmap VirtualBox



Fuente: Autor

Ejecutamos el comando db_nmap -v -T4 -PA -sV --version-all --osscan-guess -A -sS -p 1-65535 192.168.1.2 el cual nos da la opción para realizar un escaneo extenso.

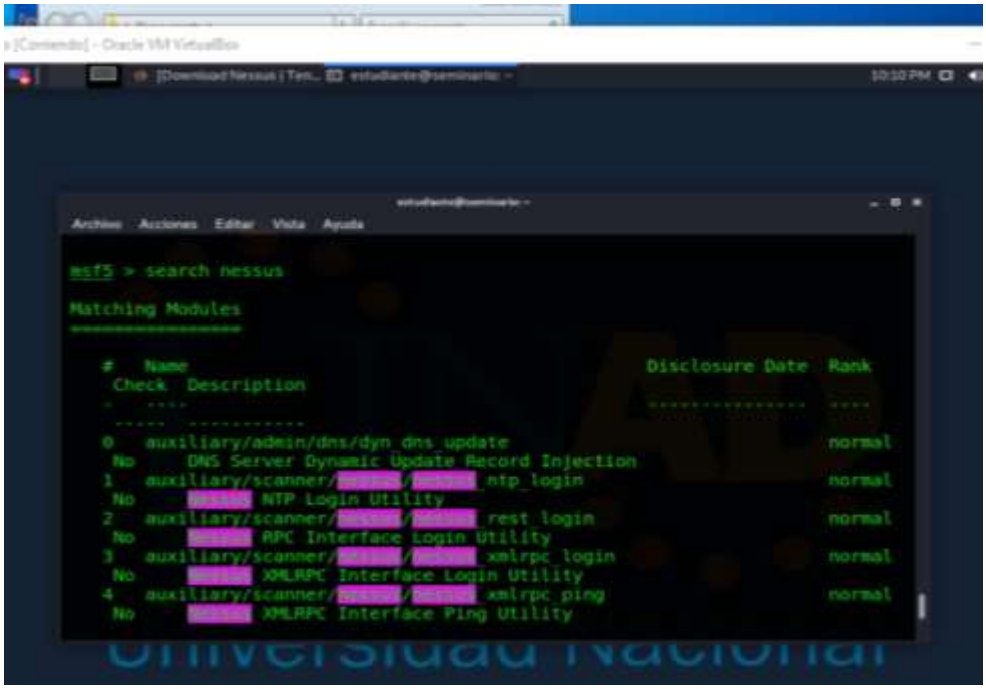
FIGURA 45 Comando services -R VirtualBox



Fuente: Autor

Ejecutamos el comando services -R para poder observar los servicios.

FIGURA 46 Comando search VirtualBox



Fuente: Autor

Ejecutamos el comando search para poder realizar una descripción del servicio al cual se le puede realizar algún tipo de ataque.

Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

1. **¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.**

Si bien hoy por hoy es casi imposible crear un entorno libre de ataques informáticos si se puede crear un espacio preventivo, las medidas que tomaría son las siguientes:

Prevención:

Es aquí cuando tenemos la oportunidad de generar políticas preventivas y de buenas prácticas en el manejo de la información.

- Generar dentro de la entidad políticas para la buena gestión de la información.
- Crear políticas de seguridad para el manejo de la información y sus ciclos.
- Crear un sistema de gestión.
- Generar roles de acceso a la información.
- Crear sistemas de control de acceso a la entidad.
- Control de dispositivos extraíbles.
- Crear copias de seguridad de la información.

Detección:

En este momento crítico para la entidad es cuando se identifica una falla o salida de información y la buena gestión que se de en este momento disminuirá el impacto del ataque.

- Medidas de detección internas: Aquí entran a jugar las políticas creadas por la entidad para controlar el incidente o ataque, en este punto deben participar personal capacitado para poder decidir, gestionar y coordinar con la finalidad de controlar y evitar efectos adicionales.
- Medidas técnicas: dar un continuo monitoreo a los sistemas y que esto nos permita detectar cualquier entrada sospechosa.
- Medidas legales: Se aplica las normas o leyes actuales para la protección de datos, aquí debemos registrar el incidente o el fallo de seguridad y dejar constancia de el tipo, momento, efectos de la incidencia y medidas correctivas.

Recuperación:

En esta etapa vamos a restablecer el sistema a como estaba antes del ataque informático.

- Backup del sistema o Copias de seguridad: Esta copia o respaldo del sistema nos permite restablecer el sistema o la información a un punto anterior al ataque, estas copias deben tomarse de forma periódica y deben estar contempladas en las políticas internas de la entidad.

Respuesta:

En este momento de sebe informar a todas las partes interesadas de la fuga de información o falla de seguridad presentada y se debe buscar la forma de minimizar la propagación de la información sustraída, para esto se deben

buscar los canales más adecuados y ser concretos atendiendo a todas las partes afectadas y así poder dar respuesta a todas las dudas o inquietudes que se presenten. También en este punto se debe estar dispuesto y es obligatorio presentar la denuncia correspondiente ante las autoridades competentes.

2. **¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?**

Por hardenización o endurecimiento de un sistema de información se entiende que es el proceso donde se buscara disminuir al máximo la afectación de un ataque, todo esto se logra a través de una serie de actividades que son:

- Configuración del firmware, creación de contraseñas, deshabilitar el inicio del sistema de cualquier unidad que no sea el disco duro, deshabilitar dispositivos ópticos para evitar accesos de malware desde un dispositivo externo.
- Instalación segura del sistema operativo creando dos particiones, una para el sistema y otra para datos, evitar la instalación de cualquier componente que no sea necesario para el funcionamiento del sistema.
- Configuración y activación adecuada de servicios asegurándose de que los equipos posean todos los parches de seguridad he instalar también un servidor de actualizaciones para la entidad.
- Instalación y configuración con políticas bien definidas por la entidad de programas de seguridad como lo son los antivirus, antimalware entre otros.
- Políticas de seguridad desarrolladas por la entidad acoplándose de acuerdo a la necesidad que se presente en el entorno del sistema.
- Configuración de rutas de acceso compartido y opciones de red tratando de limitar al mínimo los privilegios de los usuarios activos.
- Restricción de software aplicando políticas de software permitido.
- Creación de auditorias internas esto nos ayudara a tener un registro de todas las actividades que se generen en la entidad.
- Configurar servicios del sistema de tal forma que solo queden en funcionamiento los necesarios para el funcionamiento del sistema los demás deberán ser deshabilitados.
- Configurar los protocolos de red deshabilitando todos aquellos innecesarios en el sistema y usar un sistema de traducción de dirección es NAT, esto para direccionar los equipos de la entidad.
- Configurar el acceso remoto este debe ser dejado en funcionamiento si es estrictamente necesario de lo contrario deshabilitar esta función.
- Realizar copias de seguridad o respaldo de forma frecuente de la información.

Si bien las actividades a realizar en este punto son muchas y variadas se debe tratar en la medida de lo posible dejar al sistema lo más restringido y no nos podemos olvidar que esto también nos ayudara a la administración del mismo.

3. **¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?**

Equipo de Blueteam: Este se encarga principalmente de ejecutar estudios de seguridad que garanticen controles efectivos de seguridad creados en una entidad. Aquí se evalúan las diferentes amenazas que afecten a un sistema y se realiza una monitorización de la misma y se establecen planes para mitigar los riesgos hasta encontrar una solución final. Estos son grupos de expertos en ciberseguridad especializados en examinar el proceder de un sistema dentro de una entidad, se estudian los comportamientos de sus usuarios para poder descubrir de forma rápida cualquier inconveniente que pueda pasar inadvertido.

Para esto se observa el trafico de datos, el comportamiento de sus sistemas, el origen y empleo de sus conexiones y el operar de sus usuarios de forma cotidiana. Desde este punto el equipo de Blueteam se mantiene alerta para identificar de forma inmediata cualquier comportamiento malicioso de este modo se identifica cualquier incidente con la suficiente rapidez para impedir el hurto o perdida de datos.

Equipo de respuesta a incidentes informáticos: Este se encarga de verificar que incidente se ha producido de mantener y restaurar el buen funcionar del sistema aquí se facultan de reducir el impacto de un incidente se determina en que forma el ataque se convirtió en un incidente, se previenen futuros ataques y se mejora la seguridad y respuesta de un incidente, se persiguen las actuaciones ilegales y se mantiene informado sobre la gestión de la situación y su respuesta. Estos servicios se activan ante un evento o pedido de un informe o se visualice el momento en que se encuentra comprometido o se observa algo malicioso en el sistema, estos servicios son reactivos y proactivos por lo general estos son contratados por entidades gubernamentales, empresas de gran tamaño o universidades.

4. **¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?**

Si se me indicara trabajar con CIS lo utilizaría para el desarrollo de buenas prácticas y soluciones en ciberseguridad ya que aquí podemos encontrar controles críticos identificados además obtenemos diversidad de herramientas, versiones del control con su respectiva descripción y variedad de material relacionado , con esta práctica podemos mejorar estándares de seguridad que nos ayudara a comprender las amenazas, con estas actividades nos aseguramos que los controles sean un conjunto de acciones

implementables, utilizables, escalables y compatibles con las diferentes exigencia en seguridad y ya que estos controles son abastecidos de ataques reales con una defensa positiva me brindarían una base efectiva para defender de los ciberataques a la entidad. Por ultimo con lo aportado en la CIS puedo crear una estructura para el programa de seguridad, tener un enfoque comprobado de riesgos para la seguridad informática con un conjunto más efectivo y específico de medidas técnicas para la defensa de la entidad y por ultimo me ayudaría a ajustarme a otras normas y regulaciones.

5. **Explique y redacte las funciones y características principales de lo que es un SIEM.**

Un SIEM (información de seguridad y gestión de eventos) es capaz de detectar de forma eficaz para responder y así neutralizar amenazas informáticas el objetivo de esta es ofrecer una visión global de tecnología en la información. Esta nace pro la combinación de dos categorías que son:

SEM: la cual centraliza el almacenamiento y nos permite realizar un análisis casi en tiempo real, de lo que esta sucediendo en la administración de seguridad.

SIM: aquí se recopila datos a nivel central para luego ser analizados y así nos proporciona informes automatizados.

Y estas funciones combinadas nos permiten actuar de forma más eficaz sobre los ataques ya que nos ofrece más visibilidad y nos permite utilizar los datos para su análisis en tiempo real las principales características son:

- Identificar amenazas reales.
- Monitorizar de forma centralizada amenazas potenciales.
- Dirigir al personal calificado las amenazas para resolverlas.
- Aportar conocimiento sobre incidentes y así facilitar su solución.
- Documenta todo el proceso de detección, actuación y solución.
- Dar cumplimento a todas a las normas y legislaciones vigentes.

En conclusión, se podrá monitorizar y recopilar la información para así poder detectar comportamientos sospechosos en tiempo real, y así dar una respuesta eficaz y minimizar las consecuencias o daños.

6. **Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.**

FIGURA 47 SNORT

- Snort: Es un sistema de detección de intrusos en red, este es un sistema libre y gratuito, nos ofrece capacidad de almacenamiento de bitácoras de en archivos de texto y en base de datos abiertas como MySQL. Estos paquetes son analizados y con esto es posible determinar qué acciones se podrán llevar a cabo, los usuarios crear firmas basadas en las características de los ataques de red y enviarlas a la lista de correos de firmas de Snort.

FIGURA 48 OSSEC

- OSSEC (HIDS): Es un sistema de detección de intrusos el cual también opera como un SIM, OSSEC es un sistema de código abierto y gratuito, es un software altamente adaptable a las necesidades de seguridad a través de sus opciones de configuración, adición de reglas de alertas personalizada y escritura de reglas en respuesta las alertas de seguridad. Permite a los clientes crear un sistema integral de detección de intrusos basados en la supervisión del host con políticas específicas de aplicación en el lado del servidor, ofrece una gestión centralizada simplificada para la gestión de políticas en varios sistemas operativos.

FIGURA 49 OPENNAC

- OpenNAC: Esta herramienta se utiliza para el control de accesos de redes se tiene visibilidad, control y previene los riesgos de todos los

dispositivos conectados a la red, es una herramienta adaptable a las necesidades de la entidad, segmenta de forma automática las redes determinando el tramo de red al cual se le asignara a cada dispositivo, a cada usuario se le asigna una VLAN de forma dinámica y automática, además articula diferentes componentes de la red y así incrementar las acciones de autenticación y autorización también detecta amenazas aislando el dispositivo y responde ante el incidente informando sobre el impacto y su evolución.

CONCLUSIONES

En el presente trabajo aprendimos sobre las leyes que rigen en Colombia sobre los delitos informáticos y sus implicaciones, también encontramos un proceso de selección de personal con sus respectivas directrices o acuerdos y como deben ser abordados y analizados de forma concienzuda y no caer en engaños que luego incurran en la violación de derechos, además de poder conocer más sobre la ética profesional que nos rige a nosotros los ingenieros y pudimos analizar un caso en concreto y desglosar así un estudio de este y poder determinar que leyes se violentaron en este caso en mención.

Identificamos vulnerabilidades en un equipo con sistema operativo Windows 7 de 64 bits, a lo cual nos llevó a un paso siguiente y es saber explotar estas vulnerabilidades encontradas también nos da una guía de cómo debemos manejar y mejorar estos inconvenientes encontrados y así poder una idea más clara de este tema.

También nos brindó un espectro más amplio de cómo se deben manejar políticas internar y saber interpretar y conocer más sobre este tema.

Y por último aprendimos más sobre el proceder de un ataque en tiempo real y dar respuesta con argumentos técnicos de nuestro actuar y así especificar que se indagaría primero en estos casos, también se propuso que medidas de endurecimiento del sistema se tomarían para que un ataque no se repita, explicamos y aprendimos las ventajas de trabajar con CIS y como este nos ayuda a fortalecer las políticas y buenas prácticas dentro de la entidad, además describimos con nuestras palabras que es un equipo Blueteam y que es un equipo de respuesta a incidentes informáticos, además explicamos las diferentes características de un SIEM y por último se definieron y se explicaron 3 herramientas para la contención de ataques informáticos.

BIBLIOGRAFÍA

COLOMBIA. CODIGO PENAL. Ley 1273. (5, enero, 2009). “Por la cual se crea un nuevo bien jurídico tutelado - denominado “De la protección de la información y de los datos” Y se preservan integralmente de los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones.

COPNIA. (2020). Código de ética | Copnia. (https://www.copnia.gov.co/tribunaldeetica/codigo-de-etica)

COPNIA (2003). Ley 842 de 2003. | Copnia. (https://www.copnia.gov.co/nuestraentidad/normatividad/ley-842-de-2003)

EL ESPECTADOR (2018). Caso Andrómeda y sus interrogantes [En línea]. (https://www.elespectador.com/noticias/judicial/casoandromeda-y-sus-interrogantes/)

ECURED “OpenVas”. Internet: (https://www.ecured.cu/OpenVas)

GFI LANGUARD 12 “Vulnerabilidades y exposiciones comunes (CVE)”. Internet: (https://manuals.gfi.com/es/languard/content/acm/topics/appendix/common_vulnerabilities_and_exposures__cve_.htm)

NESSUS “Instalación en Kali Linux” Internet video YouTube: (https://www.youtube.com/watch?v=6erDDE5evIQ&feature=youtu.be)

OPENWEBINARS “Qué es metasploit framework”. Internet: (https://openwebinars.net/blog/que-es-metasploit/)

PCHARDWAREPRO “¿Qué es mestasploit y cómo utilizarlo correctamente”? Internet: (https://www.pchardwarepro.com/que-es-metasploit-y-como-utilizarlo-correctamente)

REVISTA HACKING ÉTICO “Fases del pentesting, aprende como hacer auditoria de hacking a empresas”. Internet: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-comohacer.html)

Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution.2014. (https://www.kb.cert.org/vuls/id/251276)

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-20146287). 2014. (https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287)

ANEXOS

URL video presentación trabajo final:

https://youtu.be/-XiIce6FghQ