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

JESUS DAVID AVILA RODRIGUEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA (UNAD) – JOSE ACEVEDO Y GOMEZ

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

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

BOGOTÁ

2021

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

JESUS DAVID AVILA RODRIGUEZ

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

DIRECTOR:

M. SC. JOHN FREDDY QUINTERO

UNIVERSIDAD ABIERTA Y A DISTANCIA (UNAD) – JOSE ACEVEDO Y GOMEZ

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

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

BOGOTÁ

2021

CONTENIDO

Pág.

LISTA DE GRÁFICOS

Pág.

LISTA DE TABLAS

LISTA DE ANEXOS

pág

RESUMEN

El presente documento comprende el informe final realizado para el Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, tomado como opción de grado para la Especialización en Seguridad Informática, realizado en la Universidad Nacional Abierta y a Distancia UNAD.

El documento está compuesto por diversos aspectos a nivel del desarrollo de la seguridad informática desde la perspectiva del desarrollo de casos de estudio de los equipos de Red Team y Blue Team, en donde desde la simulación de ambientes normales de vida cotidiana en una organización hasta llegar a ambientes en donde se pudieron presentar casos de ataques informáticos o posibles violaciones legales, éticas y morales se pueda tener una perspectiva del correcto comportamiento que se debería tener y como algo tan simple como la ética profesional puede diferenciar a un correcto profesional de una persona que solo busca enriquecerse sin importarle los medios que deba utilizar para conseguirlo.

Para la realización del informe se tienen en cuenta cinco etapas:

1. Concepto de equipos de seguridad.
2. Actuación Ética y legal.
3. Ejecución de pruebas de Pentesting.
4. Contención de ataques informáticos.
5. Socialización del informe técnico.

En cada una de las etapas se realizarán diversos procedimientos para ir ilustrando como cada paso es consecuente para la realización de una validación de seguridad en una organización. Partimos desde las nociones generales de un equipo de seguridad y las herramientas que se requerirán para su ejecución. Continuamos con la propuesta de confidencialidad en donde los profesionales a emplear deben acatar y resguardar la información a la cual van a tener acceso. Proseguimos con la realización de las pruebas y verificación de focos de inseguridad, posibles amenazas y vulnerabilidades a las cuales pueda estar la organización abierta a que sucedan. De acuerdo con los pasos anteriores se plantean de manera generar cuales son las maneras más seguras para contener y en la mayoría de los casos minimizar la sustracción y/o daño de información vital. Por último, tenemos la etapa final donde se verán reflejados todos los pasos recorridos para la realización de las actividades propuestas de la manera más detallada y clara posible.

GLOSARIO

ATAQUE INFORMÁTICO: Forma de acceder ilegalmente a un sistema informático, utilizando las debilidades o fallas que se presentan a nivel software, hardware o el componente humano, con el objetivo de extraer información, producir daños o alterar el funcionamiento de un sistema.

BLUE TEAM: Es el equipo de seguridad que realiza evaluaciones de las distintas amenazas que puedan afectar a las organizaciones, realizar una monitorización de las mismas y establecer planes de remediación para mitigar el riesgo hasta que exista una solución definitiva.

CIBERSEGURIDAD: Se le conoce como un nivel de seguridad para la protección de la información de una organización, garantizando un ambiente de trabajo libre de la mayor cantidad de amenazas informáticas.

COPNIA: (CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA): Organismo Colombiano de carácter público, encargado de controlar, inspeccionar y vigilar el ejercicio de las actividades de ingeniería.

DELITO INFORMÁTICO: son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc

FIREWALL: Son herramientas de software o hardware que se utilizan para realizar una revisión de la información que se está transmitiendo por la red local o externa para determinar e impedir la ejecución de posibles amenazas que afecten al sistema.

PENTESTING: También conocido como test de penetración, son pruebas que se realizan en un sistema de información, de manera que se simula un ataque y con ello se intenta evaluar las posibles vulnerabilidades que tenga el sistema y con ello plantear las probables medidas para evitar ataques externos que las puedan explotar.

RED TEAM: Es un conjunto de profesionales de la seguridad que actúan como amenazas que intentan superar controles de seguridad cibernética. Utilizan todas las técnicas disponibles para encontrar puntos débiles en personas, procesos y tecnología para obtener acceso no autorizado a los activos todo con el fin de generar las recomendaciones pertinentes para fortalecer la seguridad de una organización.

SABOTAJE INFORMATICO: Se define como todas las posibles conductas dirigidas a modificar, eliminar o sustraer datos en un equipo de cómputo, sistema de información o base de datos sin los permisos correspondientes.

VULNERABILIDAD: Son posibles focos, fallas de seguridad, defectos o huecos que puede tener un sistema informático y que está en la capacidad de permitir que un ciberdelincuente las utilice para ingresar en dicho sistema y sustraer, eliminar o modificar la información de dicha organización

JUSTIFICACIÓN

Desde que el mundo paso a ser una comunidad cerrada contenida en los grandes edificios de concreto donde todas las labores de manejo y uso de información se hacían en equipos de cómputo aislados cada uno del otro y donde compartir información eran tareas arduas y complejas donde involucraba demasiadas tareas y trabas generando retrasos en la toma decisiones. Pasamos a un mundo globalizado, donde la información se comparte y usa en segundos y donde las grandes compañías no tienen que sufrir en largos periodos de interconexión entre sus sedes sino con un solo movimiento del ratón pueden tenerlas a todos reunidas y organizándose por medios electrónicos para la toma de decisiones sin perder tiempo.

Lo anterior genero una gran revolución pero a su vez abrió brechas de seguridad que empezaron a ser utilizadas por delincuentes para su propio beneficio. Es por ello que para buscar medidas de seguridad que ayudaran a minimizar la perdida de información y la intrusión no permitida de ciberdelincuentes en una organización, se crearon los equipos de Blue Team & Red Team, quienes prestan diferentes servicios a las organizaciones y les ayudan a corregir sus brechas de seguridad de la manera más óptima y eficaz.

El presente documento se realiza como una manera de presentar como se realiza la gestión, la capacidad técnica y la implementación de las normatividad vigente para los equipos de Blue Team & Red Team de una manera práctica y teniendo en cuenta que sobre estos equipos la ética es un principio de alta importancia y que aunque sus servicios se podrían tomar como de intrusión o de delito, ellos siempre están enfocados a colaborar y solucionar los problemas de seguridad informática que pueden afectar a cualquier organización y como con ello ayudarles que en dado caso de la presencia de un ataque puedan responder de la manera más oportuna y eficaz posible.

METODOLOGÍA

Para el desarrollo del presente informe se tomó la decisión de realizarlo mediante una serie de etapas definidas y ordenadas para con ello tener una mayor apreciación de las circunstancias de los casos de estudio y así proceder de la manera más ordenada y de acuerdo a la situación prescrita.

A continuación se enuncian las cinco etapas realizadas para su realización:

1. Concepto de equipos de seguridad.
2. Actuación Ética y legal.
3. Ejecución de pruebas de Pentesting.
4. Contención de ataques informáticos.
5. Socialización del informe técnico.

En la primera etapa se van a tener en cuenta de manera general los conceptos de las diferentes normatividades bajo las cuales se contemplan los delitos informáticos que se pueden presentar en el país.

En la segunda etapa se va a realizar una verificación a nivel de manejo ético y legal de los aspectos referentes a un acuerdo de confidencialidad y como estos pueden estar en contra de las leyes o decretos informáticos que aplican en nuestro país.

En la tercera etapa se van a realizar las diferentes pruebas enfocadas a un pentesting para así generar los análisis de vulnerabilidades pertinentes y como estos pueden ocasionar inconvenientes en las prestaciones de los servicios de una organización.

En la cuarta etapa de acuerdo a las posibles vulnerabilidades encontradas se definirán que posibles medidas de contención se podrían aplicar y con ello minimizar el impacto que podría tener el ataque a la infraestructura, información o servicios con los que cuente la organización.

En la quinta etapa se reúnen de manera general y ordenada todos los hallazgos y son los que se plasman en el presente documento, junto con las conclusiones y recomendaciones pertinentes.

DEFINICIÓN DEL PROBLEMA

El mundo cibernético es un lugar lleno de gran competencia, nuevos desafíos pero sobretodo de nuevas oportunidades y en este mundo las organizaciones buscan la mejor manera de aprovechar estos recursos para un manejo más efectivo de la información y con ello lograr ventajas competitivas con las demás compañías.

Pero en este mundo ideal también hay grandes peligros y uno de ello que aqueja en gran medida a las compañías son la ciberdelincuencia, aquella que puede ser pagada por terceros, rivales o por incentiva propia y que solo buscan aprovecharse de las debilidades de los sistemas informáticos para irrumpir de manera no permitida y hacer con información de vital importancia para las organizaciones.

Es por ello que la necesidad de personal calificado y especializado en combatir a estos delincuentes se hizo presente los Blue Team & Red Team, son aquellos profesionales que de manera específica combaten de manera directa a las diversas amenazas informáticas que puedan presentarse en un sistema y que por medio de diversas herramientas y capacidades técnicas ayudan a mejorar las condiciones físicas, lógicas y técnicas de una organización dotándola de principios que los ayuden a minimizar tanto la presencia de ataques informáticos como a la perdida de información importante.

Aunque lo anterior no es una medida para estar totalmente seguro, si es una tarea nueva que se debe implementar en cada una de las compañías para tener un estándar básico de seguridad informática y asegurar de una forma práctica y eficaz el resguardo de la información que utilizan de manera diaria y es su insumo más importante.

INTRODUCCIÓN

Cada vez nos encontramos en un mundo más digital, cada vez lo que antes era una rutina diaria de pagar, consumir, comprar o mirar de forma presencial se ha ido eliminando y ha dado paso a un mercado global en donde la adquisición de bienes y servicios se hacen en pocos segundos. Todo esto ha sido un gran avance para la humanidad, pero a su vez ha traído nuevos problemas. Con este mundo digital los delitos y crímenes también se han vuelto digitales y cada vez es más común escuchar que organizaciones han sufrido filtraciones de datos, han sido hackeadas y por ende han comprometido la información personal de sus clientes.

Es por ello que a la par de estos crímenes también se han conformado equipos enfocados en la búsqueda de debilidades de los sistemas informáticos, personas expertas y en algunos casos anteriores delincuentes informáticos para prestar sus servicios a las organizaciones para validar la seguridad de sus sistemas, las debilidades internas y externas y con ello formular las correspondientes recomendaciones que ayuden a mejorar el nivel de ciberseguridad con la que se cuente.

De acuerdo con lo anterior, el seminario especializado: equipos estratégicos en ciberseguridad: red team & blue team nos permite continuar nuestro proceso de formación en el ámbito de la ciberseguridad dándonos las pautas para la realización de análisis de datos, estrategias parala búsqueda de vulnerabilidades utilizando herramientas de pentesting, simular ataques para conocer los alcances de los ataques y por ultimo validar las posibles contenciones que se puedan implementar y ayuden a incrementar la seguridad del sistema. Todo lo anterior haciéndolo siempre en el marco del respeto legal, las normas vigentes y con pleno conocimiento de la entidad donde se realice su aplicación.

Es por ello que en el presente documento se presentaran varios escenarios, en los cuales se presentan ciertas temáticas a tratar y explicar para que sirvan de guía e insumo en la realización de estas validaciones de seguridad informática.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Presentar un informe técnico en donde se abarquen cada una de las fases cubiertas por el estudiante en el seminario especializado teniendo en cuenta los requerimientos solicitados por la UNAD.

1.2 OBJETIVOS ESPECIFICOS

- Realizar el análisis de la legislación a nivel de la seguridad y los delitos informáticos que en este momento están vigentes en Colombia.

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

- Encontrar las vulnerabilidades en un sistema informático mediante el uso de herramientas y técnicas específicas.

- Plantear estrategias de contención mediante el análisis de los riesgos y las vulnerabilidades que puedan presentarse en un sistema de información.

- Presentar un informe técnico que contenga cada uno de los procesos realizados en las tareas realizadas como un equipo Red Team & Blue Team de acuerdo con las actividades abarcadas y finalizando con las conclusiones y recomendaciones pertinentes.

2. DESARROLLO DEL INFORME TÉCNICO

2.1 CONCEPTOS EQUIPOS DE SEGURIDAD

2.1.1 Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos, se rigen bajo las siguientes normatividades:

De acuerdo con la investigación realizada sobre que leyes, normas o decretos existen actualmente que abarquen los temas referentes a delitos informáticos u protección de datos tenemos:

1. Artículo 15 de la Constitución Política de Colombia: El artículo nos habla sobre que todas las personas tienen derecho a su intimidad personal, buen nombre, a conocer, actualizar y rectificar la información que se recoja en bancos de datos, archivos públicos, entre otros y el estado está en la obligación de hacerlo cumplir (Constitución Política de Colombia,1991, p. 3)

2. La Ley 1273 del 05 enero de 2009: Dentro de la cual se crearon nuevas disposiciones legales abarcando tanto los delitos informáticos conocidos como la protección de la información y de los datos. Entre los tipos que se crearon encontramos (Ley 1273 del 2009, s.d):

a. Artículo 269A: Acceso Abusivo a un sistema informático: Condena a la persona que con o sin autorización acceda a un sistema informático o permanezca en el sin autorización.
b. Artículo 269B: Obstaculización ilegitima de sistema informático o red de telecomunicaciones: Condena a la persona que impida el ingreso o correcto funcionamiento de un sistema informático.
c. Artículo 269C: Interceptación de datos informáticos: Condena a la persona que intercepte datos informáticos sin la autorización correspondiente.
d. Artículo 269D: Daño Informático: Condena a la persona que dañe, altere o suprima datos informáticos de un sistema de cómputo.
e. Artículo 269E: Uso de Software Malicioso: Condena a la persona que produzca o comercie con software maliciosos.
f. Artículo 269F: Violación de datos personales: Condena a la persona que obtenga, comercie o divulgue datos informáticos obtenidos de diferentes fuentes de información.

g. Artículo 269G: Suplantación de sitios web para captura datos personales: Condena a la persona que comercie con páginas webs maliciosas para la captura de datos de información.
h. Artículo 269H: Circunstancias de agravio punitiva: Consiste en el aumento de las penas de la mitad a tres cuartas partes si el delito se cometiera en unos puntos específicos: Entidades del estado, de parte de un servidor público. aprovechamiento de la confianza del empleador, revelar datos que estén en su poder, obtención de provecho para sí mismo o un tercero, con un fin de terrorismo, utilizar a un tercero para cometer el delito, siendo el administrador de la información.
i. Artículo 269I: Hurto por medios informáticos y semejantes: Condena a quien suplante a un usuario legitimo dentro del sistema de información.
j. Artículo 269J: Transferencia no consentida de activos: Condena a quien obtenga la transferencia no consentida de activos en perjuicio de un tercero.

3. Decreto 1377 de 2013: De acuerdo con la ley 1581 de 2012 donde se establece el marco para la protección de los datos personales. Se establecieron disposiciones para facilitar su implementación y cumplimiento en todas las áreas donde se cuenta con datos informáticos sensibles, de carácter privado o personales (Decreto 1377 del 2013, s.d).

El decreto establece una serie de pautas para tener en cuenta como:

a. El correcto tratamiento de los personales.
b. La autorización para la recolección y tratamiento de datos personales.
c. Las políticas para el tratamiento y privacidad de la información.
d. Los derechos de los titulares para conocer los datos que se almacenan de ellos.
e. La transferencia y/o trasmisión de datos personales.
f. Las responsabilidades sobre el tratamiento de los datos personales.

4. Ley 599 de 2000, Articulo 192. Violación Ilícita de Comunicaciones: Condena a la persona que de manera ilícita intercepte, sustraiga, impida, controle o se entere de una comunicación privada dirigida a otra persona (Ley 599 del 2000, s.d).

5. Ley 679 de 2001, donde se establece el estatuto para la prevención de la explotación sexual, pornografía y turismo con niños menores de edad. Condena a las personas que posean o compartan imágenes, textos, documentos, videos, enlaces que exploten a menores de edad en actividades pornográficas o sexuales (Ley 679 del 2001, s.d).

2.1.2 Concepto y etapas del pentesting

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.

Las Pruebas de penetración (Pentesting), es una práctica utilizada en los sistemas de información para la evaluación de vulnerabilidades que pueda tener una organización a nivel de servicios web, servidores internos, servidores externos y bases de datos.

Las etapas que componen las pruebas de penetración (Pentesting) son:

1. Planeación de Pruebas:

   En esta etapa se realiza el alistamiento de los servicios, componentes, aplicativos sobre los cuales se realizarán las diferentes pruebas a ejecutar.

   Se comienza con un inventario de los aplicativos, aplicaciones web, activos tecnológicos a evaluar. Se prosigue con la selección de las herramientas a utilizar dentro de cada una de las pruebas a ejecutar.

   Se genera un documento que contenga el inventario de los servicios a evaluar, donde se especifiquen las aplicaciones, los periodos de pruebas, los posibles riesgos que se puedan presentar, las maneras de mitigación en dado caso de presentarse, el personal requerido para la realización de las pruebas, permisos requeridos, costos de las pruebas y las fechas y tiempos para su ejecución.

2. Ejecución de actividades para pruebas de Pentesting:

   Durante la realización de esta etapa se inicia con la recolección toda la información pertinente de la compañía a evaluar. Para esta parte se pueden utilizar los buscadores web, redes sociales, servicios de video, para encontrar toda la información de la compañía

   Se continúa con la evaluación de los puertos de los hosts que se tengan disponibles, para esta actividad se utiliza la herramienta Nmap, la herramienta permite una diversificación de escaneos por medio del uso de

modificadores que nos ayudan para encontrar los puertos que están disponibles en el host (-sS), los sistemas operativos que se utilizan (-O), los servicios que se están ejecutando en el host (-sV –script=banner). La sintaxis de la sentencia Nmap es:

nmap “Tipo de Sondeo” “objetivo”

Como ejemplo para la utilización de nmap:

- Se realizará la búsqueda de host disponibles en la ip 192.168.20.21
- Se abre nmap desde la ventana de comandos.
- Se configura la sentencia como “ nmap –sS 192.168.20.21” y se ejecuta
- Se evalúan los resultados que se listen.

Posterior se realiza la identificación y análisis de vulnerabilidades utilizando la información que se recopilo en el paso anterior. Para la realización de esta tarea se puede utilizar la aplicación Openvas la cual de una manera efectiva permite la evaluación de vulnerabilidades por medio de su interfaz gráfica.

Como ejemplo se utiliza la aplicación Openvas para la evaluación de vulnerabilidad de un host:

- Se abre la interfaz de Openvas desde un navegador por medio de la url https://localhost:9392
- Se colocan las credenciales configuradas en la aplicación.
- Se configura el escaneo del objetivo a realizar, para ello se inicia un nuevo escaneo.
- Se configura el nombre del escaneo, el host 192.168.20.21 y se crea el objetivo.
- Se crea una nueva tarea, la cual permite la ejecución del análisis. Para ello se configura el escaneo, se selecciona el blanco configurado anteriormente, se crea la tarea.
- Por último, se ejecuta la tarea y de acuerdo a los resultados que se generan, se realiza la evaluación de las vulnerabilidades que hayan sido listadas en el escaneo.
  Continuamos con la realización del plan de explotación, para lo cual utilizando las vulnerabilidades encontradas se evalúa si existen exploits disponibles y en dado caso que los haya se ejecutan utilizando la herramienta Metasploit.

Como ejemplo del uso de Metasploit tenemos:

- De acuerdo con la versión de MetasPloit que se cuenta, se realiza su carga.
- Una vez en la interfaz, se inicia el proceso por medio del comando “run”.
- Cuando termine su carga se usa el comando “use exploit/ubicación del exploit” para ejecutar el exploit.
- Se configura el host a escanear “set rhost 192.168.20.21”
- Por último, se ejecuta el comando exploit y se evalúan los resultados obtenidos.

Por último, se realiza la evaluación de los resultados obtenidos y se presentan en un informe.

3. Entrega y presentación de informes.

   En esta etapa se recopilación de los resultados obtenidos en cada una de las etapas desarrolladas anteriormente. El informe debe contener cada uno de los puntos realizados de manera detallada, los componentes que se evaluaron, los resultados obtenidos y si es el caso las pertinentes recomendaciones que se puedan realizar para la toma de decisiones.

2.1.3 Herramientas de ciberseguridad

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:

2.1.3.1 METASPLOIT: Es una herramienta que se utiliza por profesionales de seguridad informática, hackers éticos y hackers para la búsqueda de vulnerabilidades en los equipos de cómputo de una organización. Para la ejecución de las pruebas se utilizan exploits que previamente fueron seleccionados de acuerdo con el conocimiento que se tenga del sistema a probar como su sistema operativo, servicios de red, puertos habilitados sin protección, entre otros.

Los pasos rápidos de uso de la aplicación son:

- La interfaz de la herramienta Metasploit se carga desde la opción de Servicios del sistema>Metasploit>Community / pro start

- Posteriormente se coloca el comando msfconsole para ingresar a la aplicación.
- Luego se crea un workspace para utilizar en la prueba, para ello se coloca el comando “workspace” si se desea trabajar en nuestro espacio o “workspace -a Win7” si se quiere trabajar en un nuevo espacio.
- Continuamos con la carga de los archivos de la aplicación que se utilizó para la búsqueda de vulnerabilidad como Nesus, el comando de importación es: “db_import”
- Continuamos con el uso de los comandos del Metasploit para la exploración de las vulnerabilidades.

2.1.3.1 NMAP: Es una aplicación que permite visualizar por medio de una serie de comandos los equipos que están activos en una red. Igualmente permite buscar información sobre puertos abiertos, aplicaciones en ejecución, sistema operativo, servidores entre otros.

Los pasos rápidos de uso de la aplicación son:

- Se ingresa a la interfaz de Nmap, para ello se carga una ventana de comandos.
- En la ventana se coloca el comando “nmap -sn 192.168.20.0/24” donde (-sn) son los tipos de sondeo a realizar y (192.168.20.0/24) es la dirección ip o el segmento de red que se desea escanear. Se puede validar las diferentes opciones de tipos de sondeos a disposición de la aplicación.
- Una vez la aplicación genere los resultados, únicamente queda por analizarlos y según corresponda utilizarlos para las siguientes fases de pruebas.

2.1.3.2 OPENVAS: Es una herramienta que se utiliza para el análisis y verificación de vulnerabilidades en los sistemas de información. Entre las aplicaciones de este tipo permite manejar los dos ambientes de trabajo, tanto en línea de comandos como en modo interfaz gráfica. Cuenta con una gran cantidad de documentación y una comunidad que ayuda a mejorarlo y a resolver dudas que se tenga.

Los pasos rápidos de uso de la aplicación son:

- Para el ingreso a la aplicación primero se configura la herramienta utilizando el script openvas-setup. El archivo se ubica en la ubicación Vulnerability Analysis>Openvas>openvas-setup
- Luego desde el navegador se abre la Url: https://localhost:9392
- Se loguea con las credenciales configuradas anteriormente.
- Primero se configura el gestor de escaneo para ello se ingresa a la opción “scan management”. Donde se configura primero el objetivo a analizar, luego se configura la tarea a ejecutar y por último se ejecuta la tarea.
- Posteriormente se evalúa los resultados que se generaron, la aplicación las ordena por su prioridad de impacto.

2.1.3.3 EXPLOITDB: Es un archivo que contiene compilaciones de exploits que se han publicado y elaborados por la comunidad informática para utilizarse en la evaluación de vulnerabilidades de red en un sistema de información.

2.1.3.4 CVE: Son las siglas de Common Vulnerabilities and Exposures, es decir las vulnerabilidades más recurrentes que se puedan presentar en un sistema informático y que por medio del uso de exploits se pueden verificar si el sistema a probar puede estar expuesto a ellas. En la red se encuentran listas registradas con las vulnerabilidades conocidas, cada una codificada con un identificador para su consulta y una valoración de su posible impacto en un sistema de información.

2.1.4 Configuración del banco de trabajo

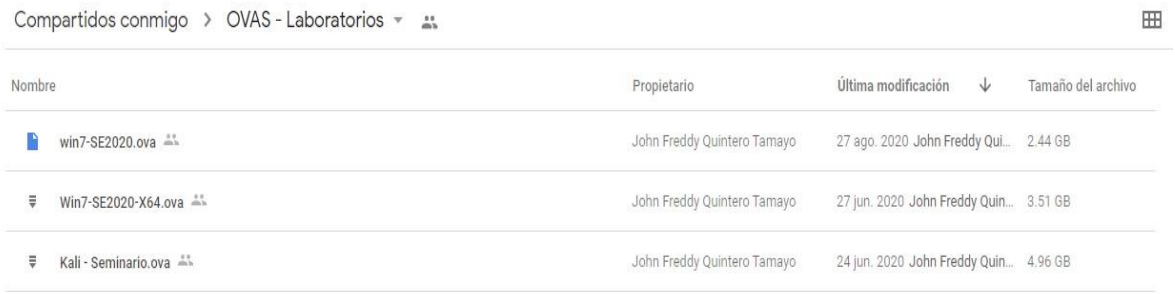
De acuerdo con la solicitud de la organización se realiza el montaje del banco de trabajo, el cual consta de 3 máquinas virtuales: 2 de ellas con Sistema Operativo Windows y 1 de ellas con el Sistema Operativo Kali. Las Ovas son proporcionadas directamente por la organización. Para el montaje de estas, se utiliza la herramienta VirtualBox. Posteriormente estas serán las herramientas que se utilizarán según se solicite para el análisis de los diferentes escenarios que la organización The WhiteHouse Company defina para su estudio.

Paso A: Se descarga la Herramienta VirtualBox para la realización del montaje de las OVAS. Ver Gráfica 1.

Gráfico 1. Herramienta VirtualBox.

Paso B: Se descargan las OVAS que vienen preconfiguradas para la realización de las actividades propuestas. Las 3 imágenes constan de: Windows 7-X86, Windows 7-X64 y Kali Linux. Ver Gráfica 2.

Gráfico 2. Ovas preconfiguradas.



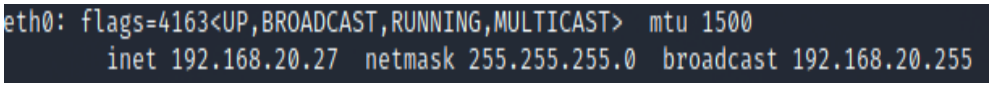
Paso C: Verificación de la comunicación entre máquinas y especificación técnica de las maquinas.

1.4.1 Paso C. Se realiza la validación de comunicación entre cada una de las maquinas:

a. Se realiza la validación de comunicación entre la máquina de Windows X64 con la máquina de Kali.

b. Para realizar esta validación se verifica que dirección IP tiene cada una de las máquinas y si están en el mismo segmento de red.
Se encuentra que la IP es la 192.168.20.27 en la maquina Kali. Ver Gráfica 3.

Gráfico 3. Dirección IP Linux.

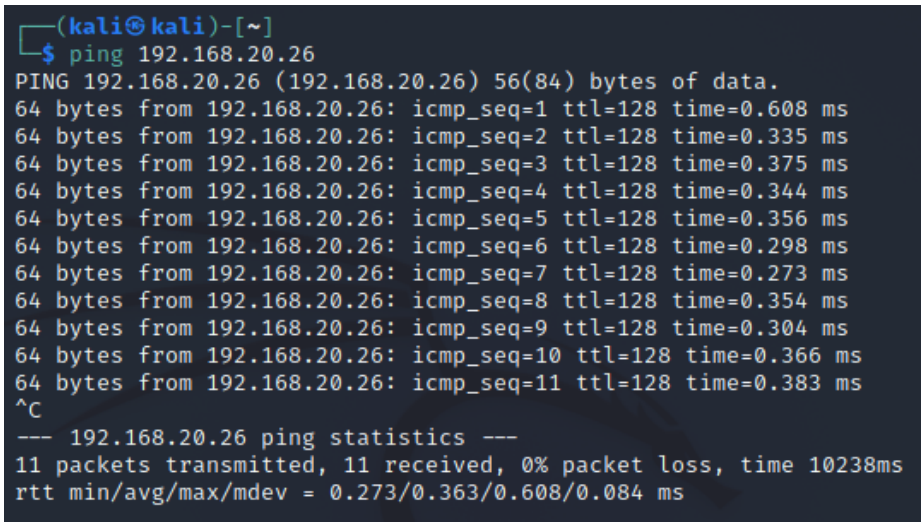


Para la maquina Windows la IP es la 192.168.20.26. Ver Gráfica 4.

Gráfico 4. Dirección IP Windows X86.

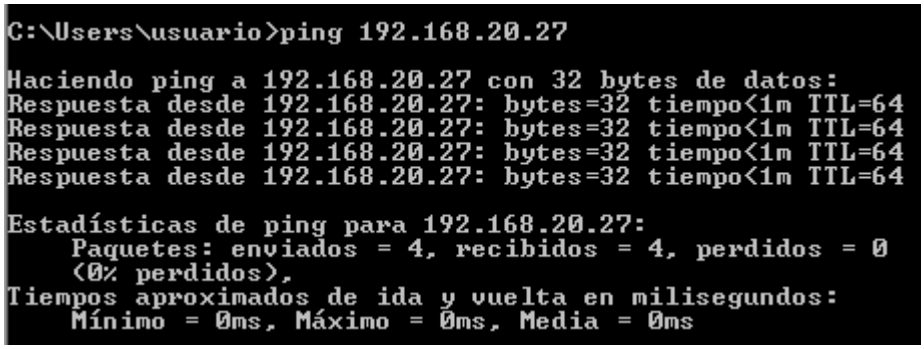
c. Se realiza un ping desde la maquina Kali a la maquina Windows y se observa que hay respuesta. Ver Gráfica 5.

Gráfico 5. Ping Maquina Linux a Windows.



d. Se realiza un ping desde la maquina Windows a la maquina Kali y se observa que hay respuesta. Ver Gráfica 6.

Gráfico 6. Ping Maquina Windows a Linux.

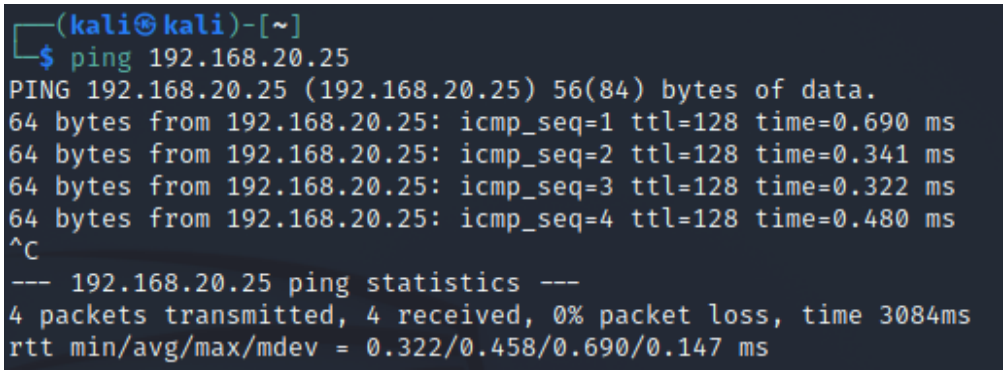


e. Se realiza el mismo proceso para la otra máquina de Windows. La dirección Ip que tienes es la 192.168.20.25. Ver Gráfica 7.

Gráfico 7. Dirección IP Windows 7.

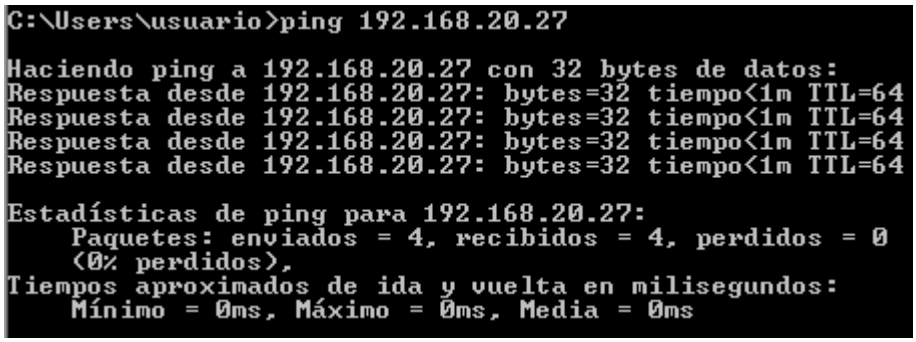
f. Se realiza el ping desde la maquina Kali a la maquina Windows y se verifica respuesta. Ver Gráfica 8.

Gráfico 8. Ping Maquina Linux a Windows.



g. Se realiza el ping desde la maquina Windows a la maquina Kali y se verifica respuesta. Ver Gráfica 9.

Gráfico 9. Ping Maquina Windows a Linux.

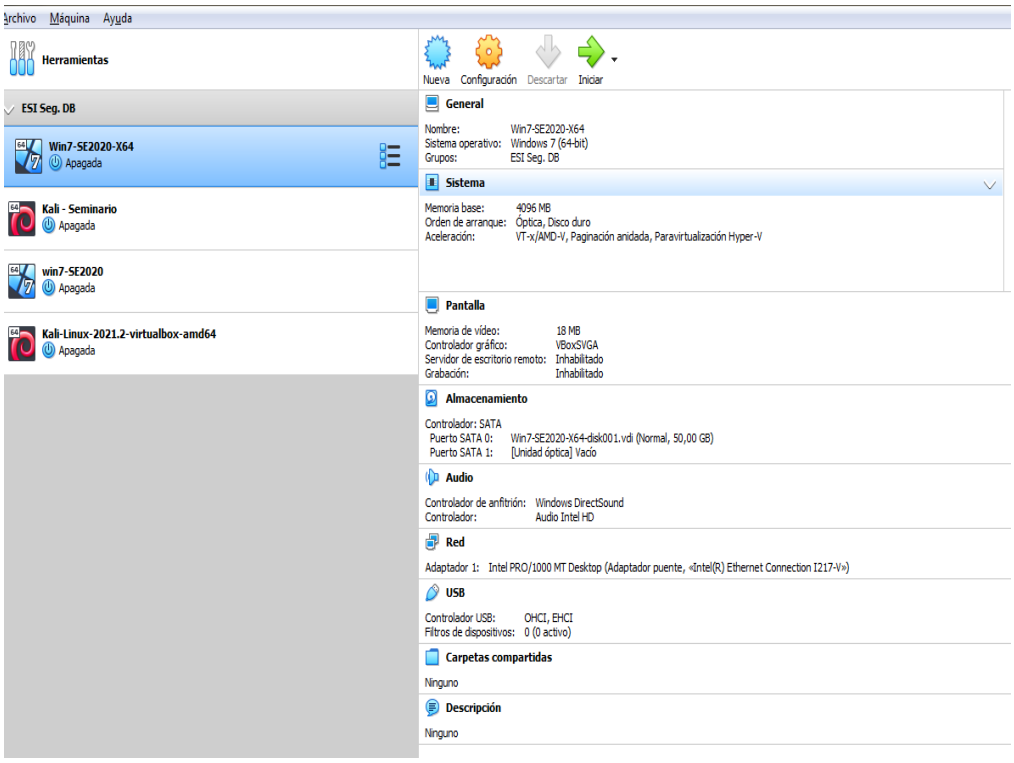


Paso D. Se Muestra el Banco de trabajo a utilizar, se especifica el tipo de Windows que se tiene, las características del sistema, los adaptadores con los que cuenta, entre otros:

a. En primer lugar, se muestra la configuración de la máquina de Windows 7 X64 (Ver Gráfica 10):

- Cuenta con un Sistema Windows 7 de 64 Bit.
- Memoria RAM de 4096 MB
- Memoria de Video de 18 MB
- Almacenamiento variable dependiendo del crecimiento de la máquina virtual.
- EL adaptador de Red que se usa es un Adaptador Puente, para la generación de la IP.
- Controlador USB para la conexión.

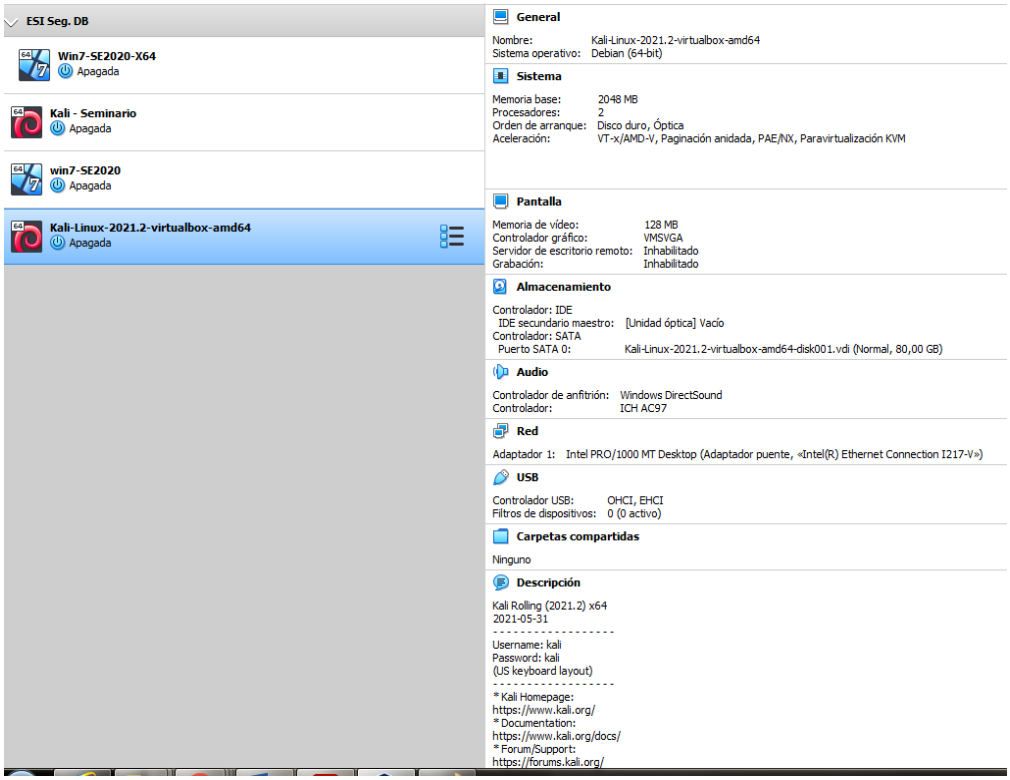
Gráfico 10. Especificaciones técnicas Win 7 X64.



b. En Segundo lugar, se muestra la configuración de la máquina Kali (Ver Gráfica 11):

- Cuenta con un Sistema Debian, Kali-Linux 2021 de 64 bit.
- Cuenta con 2 Procesadores.
- Memoria RAM de 2048 MB
- Memoria de Video de 128 MB
- Almacenamiento variable dependiendo del crecimiento de la máquina virtual.
- EL adaptador de Red que se usa es un Adaptador Puente, para la generación de la IP.
- Controlador USB para la conexión.

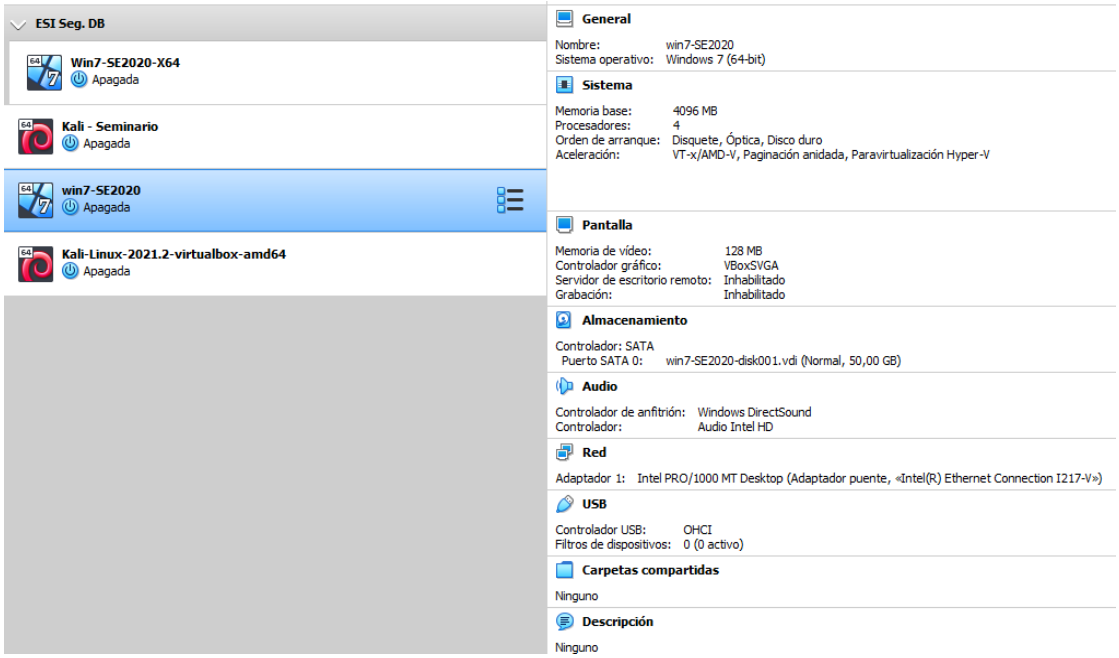
Gráfico 11. Especificaciones técnicas Kali Linux.



c. En Tercer lugar, se muestra la configuración de la máquina Windows 7(Ver Gráfica 12):

- Cuenta con un Sistema Windows 7 de 64 bit.
- Cuenta con 4 Procesadores.
- Memoria RAM de 4096 MB
- Memoria de Video de 128 MB
- Almacenamiento variable dependiendo del crecimiento de la máquina virtual.
- EL adaptador de Red que se usa es un Adaptador Puente, para la generación de la IP.
- Controlador USB para la conexión.

Gráfico 12. Especificaciones técnicas Win 7.



2.2 ACTUACIÓN ÉTICA Y LEGAL

2.2.1 Verificación de procesos ilegales o no éticos en el acuerdo

Una vez realizada la verificación del acuerdo en cada uno de sus puntos, se encuentra de manera evidente la presencia de procesos ilegales y situaciones no éticas que comprometen la imagen y buena fe de la compañía y predisponen al profesional y/o estudiante que decida firmarlo a incurrir en actos delictivos que a la larga y por compromiso del acuerdo libera a la compañía de toda responsabilidad y su vez esta persona asume toda culpa por la posesión, conocimiento y uso de esa información.

A continuación, se enumerarán los hallazgos que se evidenciaron en el acuerdo y que deberían analizarse porque incurren en delitos según las leyes colombianas:

1. En la definición del objeto, se enuncia lo siguiente: “la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.” Lo anterior demuestra que desde el inicio que parte del personal de la compañía puede estar inmiscuida en la realización de

delitos informáticos para la obtención de información por medios ilegales y que esta información es usada, suministrada, compartida y explotada para la obtención de beneficios económicos.

2. En las definiciones de información confidencial, en el numeral 2 se enuncia lo siguiente: “datos secretos como datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”. Lo anterior directamente se refiere a un acto penalmente condenable y que simboliza el robo de información de un tercero utilizando medios no autorizados y sin pleno consentimiento de la compañía afectada.

3. En las obligaciones de la parte receptora, en el numeral 3 se enuncia lo siguiente: “No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.” Lo anterior se puede considerar como una manera de complicidad con la o las personas que suministraron la información al no denunciar a las autoridades la realización de hechos punibles y que están penalmente castigados por las leyes colombianas.

4. En las obligaciones de la parte receptora, en el numeral 4 se enuncia lo siguiente: “Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.” Igualmente, que en el punto anterior se recae en una postura de cómplice con la o las personas de la compañía por el hecho de poseer, conocer o compartir información de un tercero que fue obtenida de manera irregular y sin el permiso de estos.

5. En las obligaciones de la parte receptora, en el numeral 4 se enuncia lo siguiente: “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.” Aunque dentro de la obligación se indica que no se puede compartir la información confidenciar que el personal de la compañía le suministra para la realización de sus labores, igualmente hace referencia a información ilegal lo que hace ver que parte o total de esa información pudo haber sido obtenida de manera irregular y por ello recae en delitos informáticos que no pueden omitirse y debe ser expuestos con las autoridades pertinentes.

6. En la solución de controversias, se enuncia lo siguiente: “En caso de 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.” Desde un punto de vista legal se evidencia que el acuerdo desde el inicio intenta librar a la compañía de responsabilidades por la obtención, divulgación y uso de la información obtenida de manera ilegal e intenta hacer responsable al empleado por su tenencia. Este es un acto condenable y que debe ser castigado porque desde el inicio el creador del acuerdo hace creer que desde el inicio el personal de la compañía utilizo métodos ilegales para la obtención de la información y aunque el empleado es culpable si conocía que la información es ilegal eso no libra a la compañía de responder por la realización de delitos informáticos cometidos por alguno de sus empleados.

Los ítems anteriormente descritos demuestran en su totalidad que en varias de las partes de este acuerdo se está incurriendo en la realización de delitos informáticos que son penalmente castigados según las leyes de Colombia y que aunque sin importar que la alta dirección de la compañía tenga o no conocimiento de ellos, igualmente la hace responsable por la actuación de uno de sus empleados y la manera como somete a los nuevos empleados a no denunciar cualquier acto ilegal que presencia y a su vez a utilizar la información ilegalmente obtenida en el desarrollo de sus actividades diarias.

2.2.2 Análisis de violaciones a la ley 1273.

De acuerdo con la verificación que se realizado del acuerdo, se encontró varias irregularidades y a continuación se enuncian los artículos de la ley 1273 que se podrían vulnerar debido a estas infracciones:

1. Artículo 269A, Artículo 269C. En el numeral 2 de las definiciones de información confidencial, se indica la posibilidad del manejo de información cuyo origen podría haber sido por medio de chuzadas, interceptaciones ilegales, accesos abusivos a sistemas de información. Lo anterior son actividades que están penadas y que se consideran como acciones delictivas bajo de pena de prisión.

2. Artículo 269F. En el numeral 4 de las obligaciones de la parte receptora, se indica que no se puede transmitir, intercambiar, comunicar, información que se puede caracterizar como ilegal. Lo anterior es un delito que se indica en el artículo y más indicando que la compañía podría estar utilizando esta información para la obtención de cualquier tipo de provecho.

3. Artículo 269H. En el numeral 3 y numeral 4 de las obligaciones de la parte receptora y en la solución de controversias, se indica que el profesional o persona que este firmando el acuerdo se debe abstener de denunciar, publicar y en los casos que sea sorprendido con información ilegal de involucrar a la compañía. Lo anterior es una manera de involucrar a un tercero en hechos ilegales e impide que en caso de que se dé cuenta de estas actividades realice la denuncia pertinente, siendo esto un hecho que se lista en el artículo y que puede provocar que personas de buena fe sean considerados cómplices y tengan que responder a las autoridades por actividades ilegales que no han cometido y de las cuales no tenían conocimiento alguno.

4. Articulo 269J. En algunos de los puntos que se enunciaron en el punto 1(punto 2, 3, 4, 5). Se evidencia que se asume un manejo de información ilegal cuya entrega se realiza de manera directa del personal de la compañía al empleado o estudiante que firmó el acuerdo. Esto está tipificado como delito en el artículo bajo pena de prisión.

2.2.3 Aplicación del código de ética para ingenieros de COPNIA

De acuerdo con las disposiciones encontradas en el anexo 3 – Acuerdo y teniendo en cuenta la ética profesional que recae en todas las profesiones legalmente reconocidas por el estado colombiano, mi decisión sería la de no aceptar el contrato.

La decisión se toma en primer lugar porque en varios de los numerales que hacen parte del acuerdo, se presumen que se pueda estar utilizando de manera directa y como insumo principal de trabajo información que no ha sido obtenida de manera legal. Esto por solo inicio, se puede considerar como un hecho legalmente punible generador de cualquier tipo de pena, sanciones, incapacidades, etc., para él o los servidores que tengan conocimiento de estas actividades.

En segundo lugar y de acuerdo con las leyes que están establecidas por la constitución política de Colombia, las leyes y/o decretos reglamentados por el Congreso de la república que son de conocimiento público y demás acuerdos internacionales donde se penalice actividades relacionadas con delitos informáticos, varias actividades propuestas van en contra de estas reglamentaciones.

En tercer lugar y teniendo en cuenta el código de ética de COPNIA, la cual es la entidad rectora para el ejercicio de la ingeniería en Colombia. En varios de sus artículos se tienen en cuenta la realización de actividades de carácter no legal como penalizables y que podrían incurrir en la cancelación de la matricula profesional. Entre esas actividades podemos encontrar las siguientes:

1. El artículo 31, numeral f. En donde se indica que se debe denunciar cualquier acto ilegal que vaya en contra del código de ética y sabiendo que en el acuerdo se presentan restricciones para la realización de denuncias sobre el uso indebida de información, esto va en contra directa del código de ética y las leyes del país.

2. El artículo 34, numeral a. En donde se indica la aceptación de trabajos en contra de las disposiciones legales. En el acuerdo se enumera la utilización de información ilegal, lo cual es una falta directa a las disposiciones legales que rigen en este momento en el país.

3. El artículo 35, numeral b. En donde se habla de los deberes de los profesionales y como el profesional debe hacerse valer su profesión y denunciar las trasgresiones que se hagan. Esto es muy importante porque en el acuerdo se habla mucho como el profesional no puede realizar denuncias del uso de información ilegal y que en dado caso que esta información sea encontrada en su poder por las autoridades, la compañía quedara exenta de esto y el único responsable será el profesional, sabiendo aun que fue la misma compañía la que podría haber suministrado inicialmente esta información.

4. El artículo 38, numeral a. En donde se habla de las prohibiciones a los profesionales. Se tiene en cuenta en la restricción de uso de manera ilegitima de cualquier tipo de información de terceros para el uso propio sea como insumo o aplicación en el trabajo. En el acuerdo se evidencia como se podría hacer el uso de información de terceros mediante la realización de hechos ilegales para uso y beneficio de la compañía.

En base a los anteriores puntos fue por los que se tomó la decisión de declinar por la propuesta. Es de aclarar que no se tienen certeza que estos hechos se estén cometiendo, pero de acuerdo con el documento que se recibió se da por entendido que así podría ser y más siendo un documento oficial de la compañía para el ingreso de nuevos funcionarios a laborar con dicha compañía.

2.2.4 Implicaciones legales y éticas para el caso operación andrómeda Buggly

Desde mi punto de vista fue uno de los casos más sonados en estos tiempos en nuestro país y sin lugar a duda el caso en donde más intervención militar en hechos

de delitos informáticos se ha conocido y en cierta manera se pudo comprobar su intervención en estos hechos.

Para poner en contexto la noticia, se habla de un local que a los ojos de cualquier persona desarrollaba muchas tareas, desde restaurante, servicios de internet u otros servicios. Del cual se hizo conocido por la intervención de la policía en donde luego se conoció que funcionaba un completo centro de interceptaciones ilegales de comunicaciones de las fuerzas militares.

Desde que la noticia salió a la luz pública se pudo evidenciar que estos hechos no eran recientes y llevaban mucho tiempo en desarrollo, a su vez que no solo se contaba con personal militar sino civiles que tenían acceso total a la información que allí se manejaba y de la cual se evidencio que uno de ellos lo comento por amigos cercanos.

Estos hechos dejaron en evidencia que algo que no se pensaba que ocurriera en Colombia, ya era un hecho y que no solo estaban involucrados personal de grupos al margen de la ley, sino políticos, periodistas y personas del común a los cuales podrían haberles interceptado desde llamadas telefónicas, mensajes de whatsapp, hasta sus propios correos electrónicos.

Durante la mayoría de las indagaciones se encontraron una gran cantidad de pruebas, varios de los llamados a declarar no pasaron la prueba del polígrafo y algunos otros decidieron realizar preacuerdos con la fiscalía para la búsqueda de disminución de la condena.

Al final resulto un hecho que no fue aislado, pero si lo intentaron limitar a lo más mínimo y aunque hubo condenas, sobre todo de militares, quedo como un error de un ejercicio de inteligencia militar donde se buscaba capacitar a los integrantes de las fuerzas militares en conocimientos de ciberseguridad y hacking ético pero que se salió de las manos y termino en violaciones de derechos fundamentales y generación de brechas de inseguridad dentro y fuera de las autoridades competentes.

Ahora teniendo en cuenta las implicaciones legales y éticas podemos encontrar los siguientes hechos que incurrieron en delitos informáticos y de los cuales dependiendo de su gravedad tendrán las penas pertinentes de acuerdo con cada ley:

Empezamos con la ley 1273 de 2009 y que artículos fueron vulnerados:

1. Artículo 269A. Acceso Abusivo a un sistema informático. En este podemos contemplar los hechos de los ingresos a los sistemas informáticos de whatsapp y blackberry.
2. Artículo 269C. Interceptación de datos informáticos. En este numeral encontramos las diferentes interceptaciones tanto en los dispositivos móviles como en los correos electrónicos.
3. Artículo 269D. Daño informático. En este numeral podemos encontrar la mayoría de los datos informáticos que fueron destruidos para impedir que se encontraran esas pruebas.
4. Artículo 269E. Uso de Software Malicioso. Se podría considerar los diferentes softwares que se utilizaron para la realización de las intervenciones.
5. Artículo 269F. Violación de datos personales. Desde la intervención a las aplicaciones y servicios móviles hasta el ingreso de manera indebida a correos electrónicos no solo de personas involucradas directamente sino de terceros que no tenían nada que ver con estos hechos y que por disposición del personal a cargo fueron violentados sus derechos.
6. Artículo 269H. Principalmente se ve desarrollado porque las personas que hicieron estos hechos punibles fueron funcionarios de entidades públicas y miembros de las fuerzas militares. Igualmente, que los civiles involucrados vendieron y utilizaron información para su propio beneficio.

Como se pudo evidenciar se cometieron una gran cantidad de violaciones a nivel de delitos informáticos y cada uno será tenido en cuenta para la evaluación de la pena en la cual incurrió esta persona adicional a los demás delitos por los cuales sean encontrados culpables.

A nivel ético se evidencia desde violaciones a la intimidad de las personas, al acceso no permitido a datos privados, conversaciones telefónicas y mensajes personales. También la utilización de personas ajenas para que sirvan de fachada del centro de operaciones sin que ellas supieran los delitos que se estuvieran cometiendo.

También tenemos la posible presencia de profesionales informáticos, los cuales podrían haber violado su código de conducta permitiendo el uso de información ilegalmente obtenida, no denunciando a quienes tenían, poseían u obtuvieron la información ilegal. La aceptación de dinero u otras preventas para la realización de hechos ilegales, la utilización de información ilegal para la obtención de beneficios propios y muy posiblemente la destrucción de información o datos informáticos para la ocultación de la realización de hechos ilegales.

2.3 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

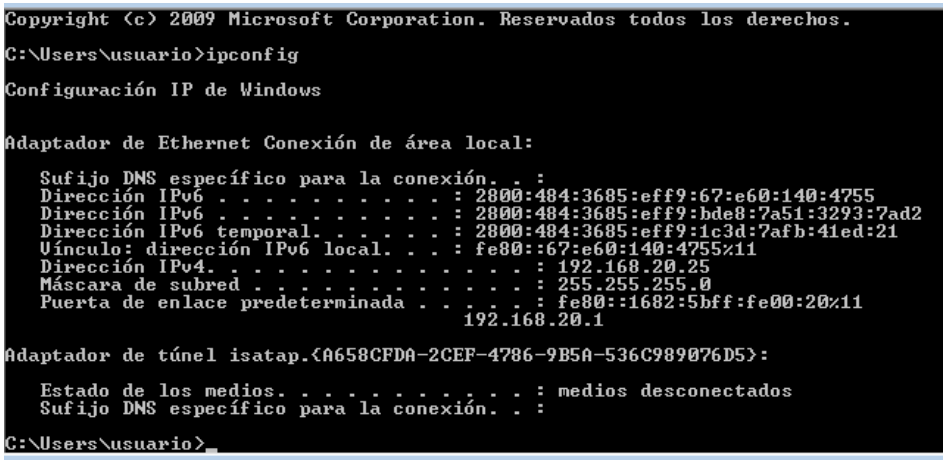
2.3.1 Ejecución de un Pentesting.

Para el desarrollo de la actividad propuesta se utilizaron 3 herramientas, las cuales fueron de suma importancia para poder evaluar de una manera más concreta la situación que se presentó con el caso.

2.3.1.1 Uso de la herramienta NMAP:

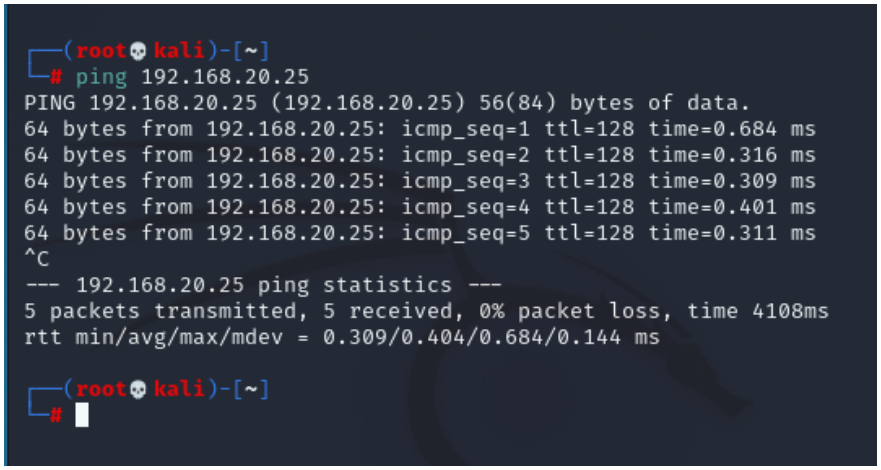
- En primer lugar, se verifico la dirección IP que tiene la maquina en la cual se presentó el inconveniente. Ver Gráfica 13.

Gráfico 13. Dirección IP Maquina Atacada.



- Posteriormente desde la maquina Kali, se abrió la interfaz de consola y se procedió a realizar un ping para validar conexión con la máquina. Ver Gráfica 14.

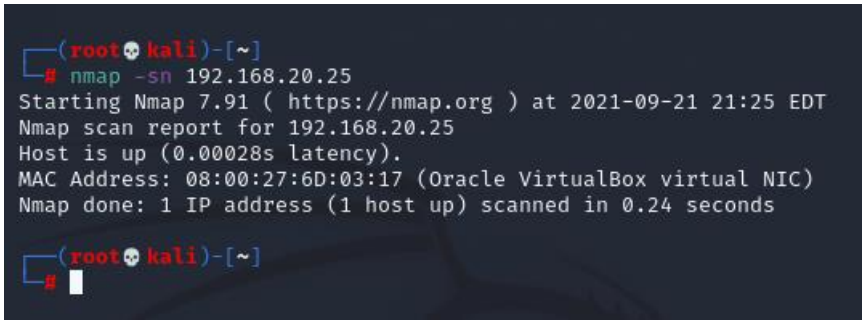
Gráfico 14. Ping Kali a Maquina Atacada.



- Una vez se concretó la conexión con la maquina se utilizó la herramienta nmap para verificar el host a inspeccionar.

  Se utiliza el comando nmap –sn 192.168.20.25 para validar si hay algún host disponible. Ver Gráfica 15.

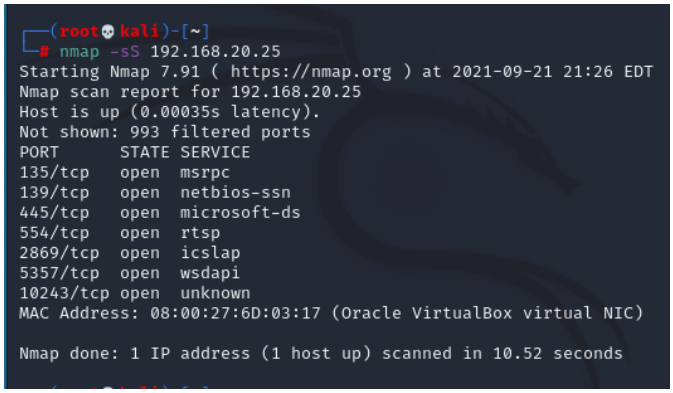
Gráfico 15. Comando -sn nmap



- Sabiendo que hay un host disponible, Se realiza una verificación de los puertos abiertos.

  Se utiliza el comando nmap –sS 192.168.20.25 para validar que puertos están abiertos en ese momento. Ver Gráfica 16.

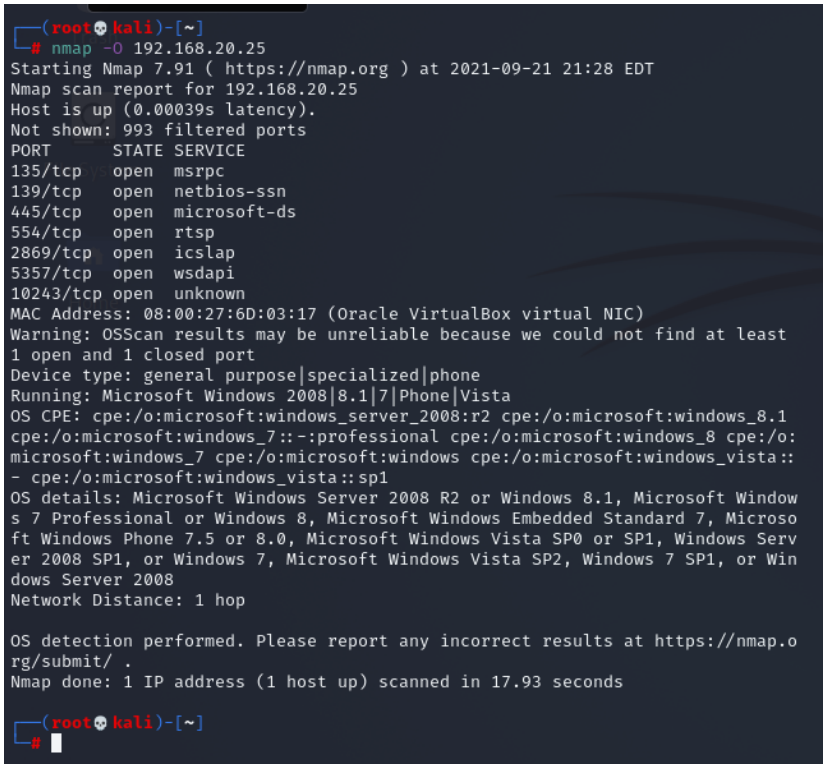
Gráfico 16. Comando -sS nmap



- Igualmente podríamos validar que sistema operativo tiene el equipo a validar.

  Se utiliza el comando nmap –O 192.168.20.25 para validar que puertos están abiertos y el sistema operativo que maneja el equipo. Ver Gráfica 17.

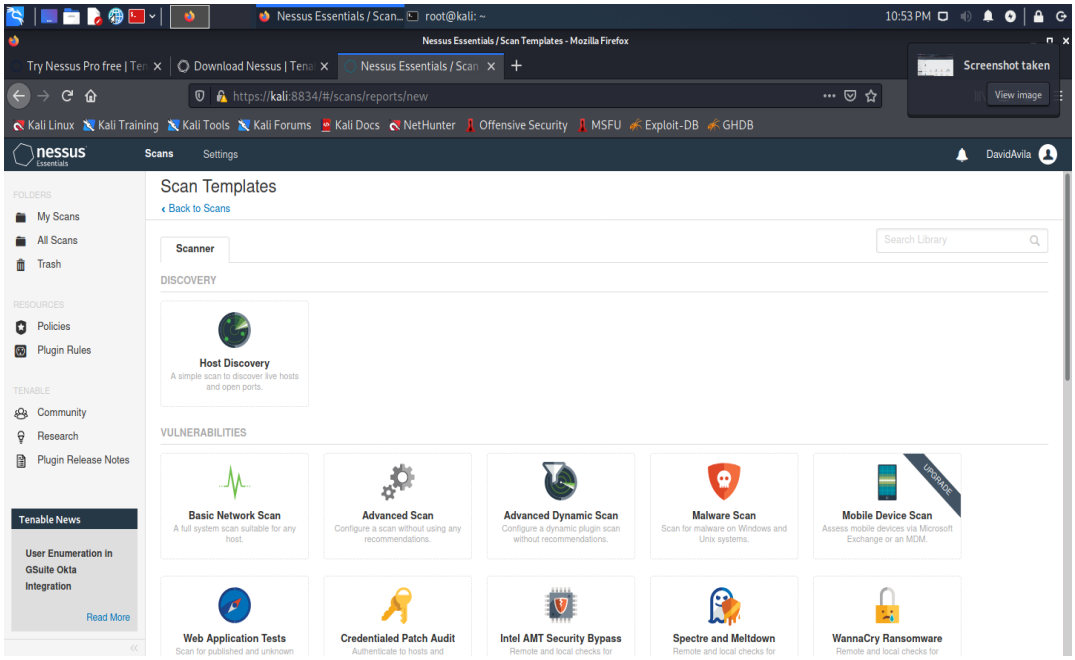
Gráfico 17. Comando -O nmap



2.3.1.2 Uso de la herramienta NESSUS:

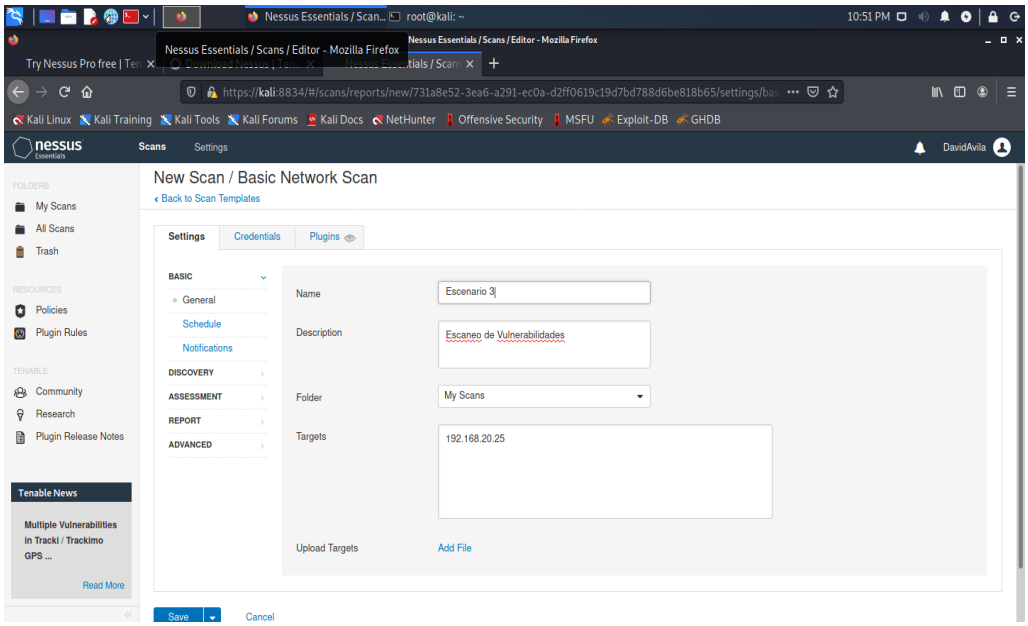
- Iniciamos con la configuración del escaneo a realizar sobre la máquina, para ello configuramos un nuevo escaneo. Ver Gráfica 18.

Gráfico 18. Escaneo Nessus



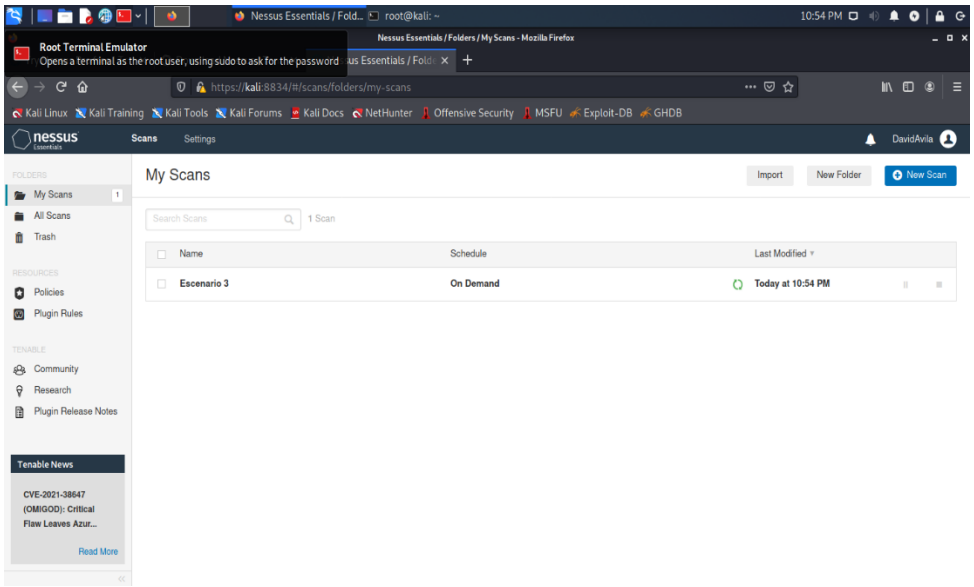
- Configuramos el nuevo escaneo a realizar. Ver Gráfica 19.

Gráfico 19. Configuración escaneo Nessus



- Ejecutamos el escaneo que se acaba de configurar. Ver Gráfica 20.

Gráfico 20. Ejecución escaneo Nessus



- Se realiza la revisión de los resultados que arrojó el escaneo de vulnerabilidades en la maquina objeto. Ver Gráficas 21,22,23.

Gráfico 21. Revisión escaneo Nessus1

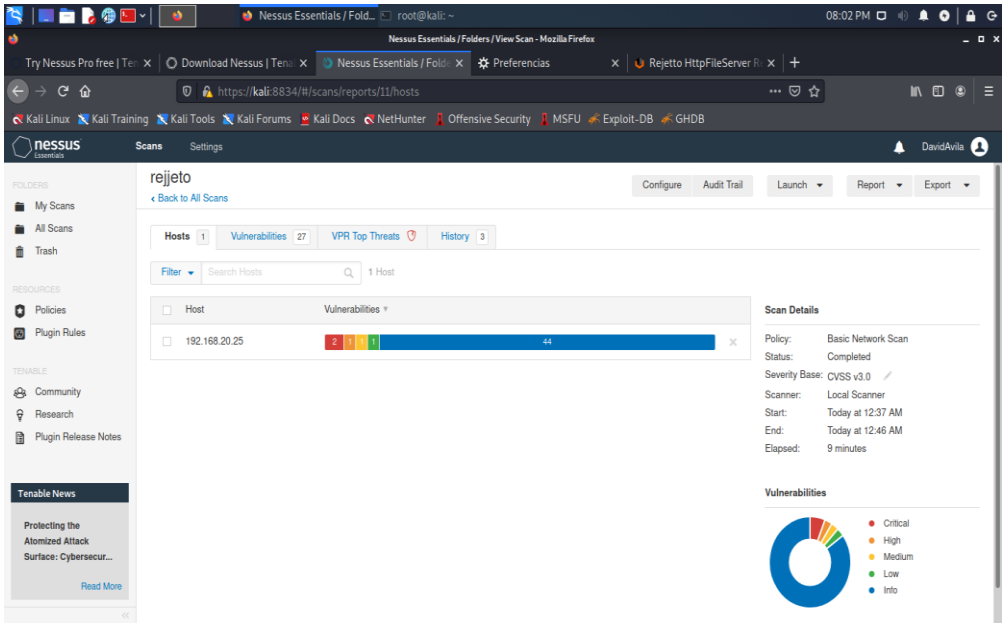


Gráfico 22. Revisión escaneo Nessus2

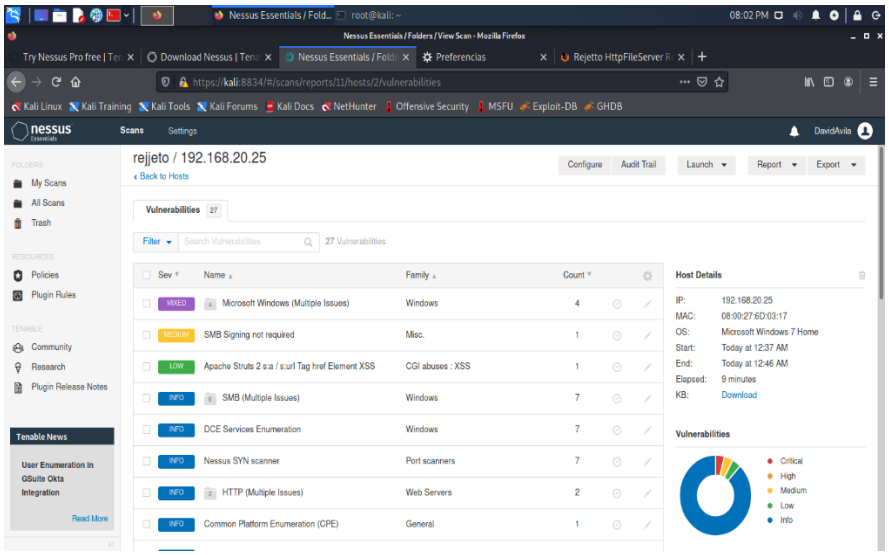
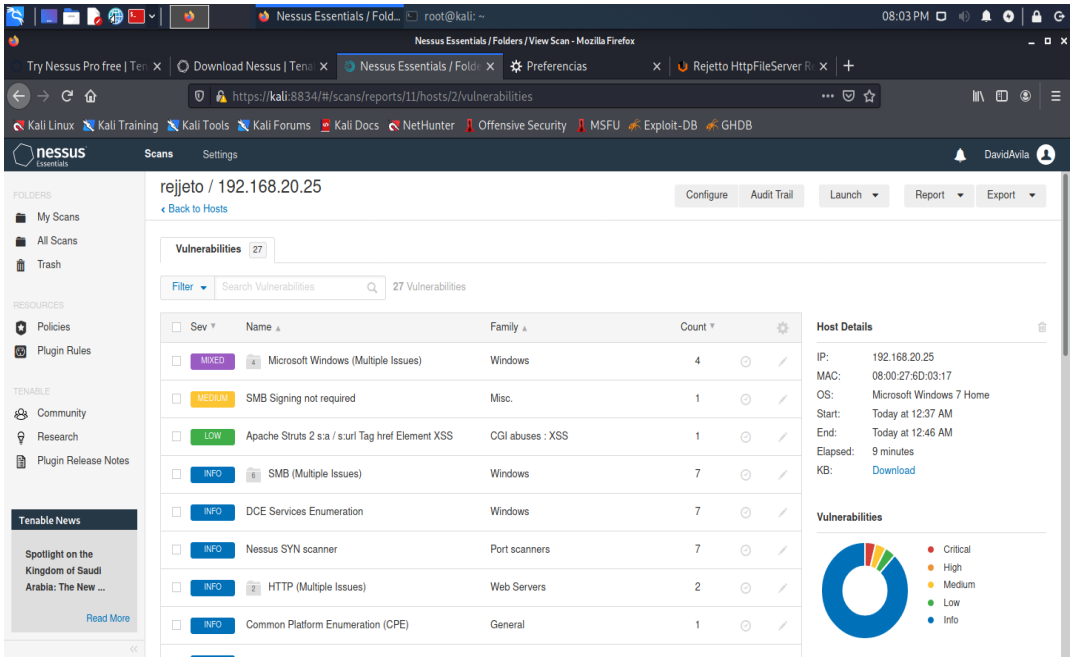


Gráfico 23. Revisión escaneo Nessus3



- Se evidencia que se encontraron 2 vulnerabilidades de carácter crítico, 1 vulnerabilidad de carácter alto y 1 vulnerabilidad de carácter bajo que deben evaluarse para su corrección o mitigación según corresponda.

2.3.1.3 Uso de la herramienta METASPLOIT:

Para la realización de esta etapa se utilizará la herramienta MetasploitFramework la cual es de mucha ayuda para proporcionar información sobre las posibles vulnerabilidades de seguridad y ayuda como herramienta en las pruebas de penetración para encontrar focos de inseguridad que a la larga podrían ser entradas para los ciberdelincuentes. Posteriormente se dará una exposición mas detalla del uso y ejecución de la herramienta.

Como fase final del pentesting se realiza el informe o reporte final, en el cual se indicarán cada uno de los componentes evaluados (Equipo Windows), las herramientas que se utilizaron (Nmap, Nessus y Mestasploit) y los resultados que cada una de ellas arrojaron para que sirvan de insumo en la evaluación del problema y la resolución de posibles recomendaciones para el mejoramiento de seguridad del sistema.

2.3.2 Descripción de la falla de seguridad

Se realizó un análisis del anexo 4 – escenario 3, en donde se evidenciaron los hallazgos frente al fallo de seguridad que se presenta en la maquina objetivo:

- La presencia en el equipo de cómputo de una aplicación llamada rejetto V, la cual tiene un exploit asociado. Por ahora no se sabe información más detallada de cómo, cuándo y dónde se obtuvo la aplicación descrita, pero si se conoce que es una aplicación potencialmente peligrosa.
- La posible presencia de una Shell inversa a la cual se hay conectado el equipo objetivo. De acuerdo con el anterior numeral la aplicación enunciada puede haber generado la conexión con el equipo remoto del atacante, lo que puede desembocar en que el atacante tenga el control del equipo sin que nadie en la organización se hay percatado de ello.
- Establecimiento de una sesión de meterpreter. Es muy probable que, si se está presentando una conexión debido a una Shell inversa, el atacante inicie la inyección de código para obtener el control de la maquina objetivo y a su vez ejecutar diversos programas para la obtención de información del equipo o a la cual el equipo pueda tener acceso.
- Posible creación de un usuario en el equipo con privilegios de administración. En este punto es de suma urgencia que, si se tiene la noción que puede haberse creado un usuario con esos privilegios o a un usuario existente se le otorgaron esos privilegios, realizar la comprobación de ello e iniciar la búsqueda de dicho usuario para su inmediata inactivación.

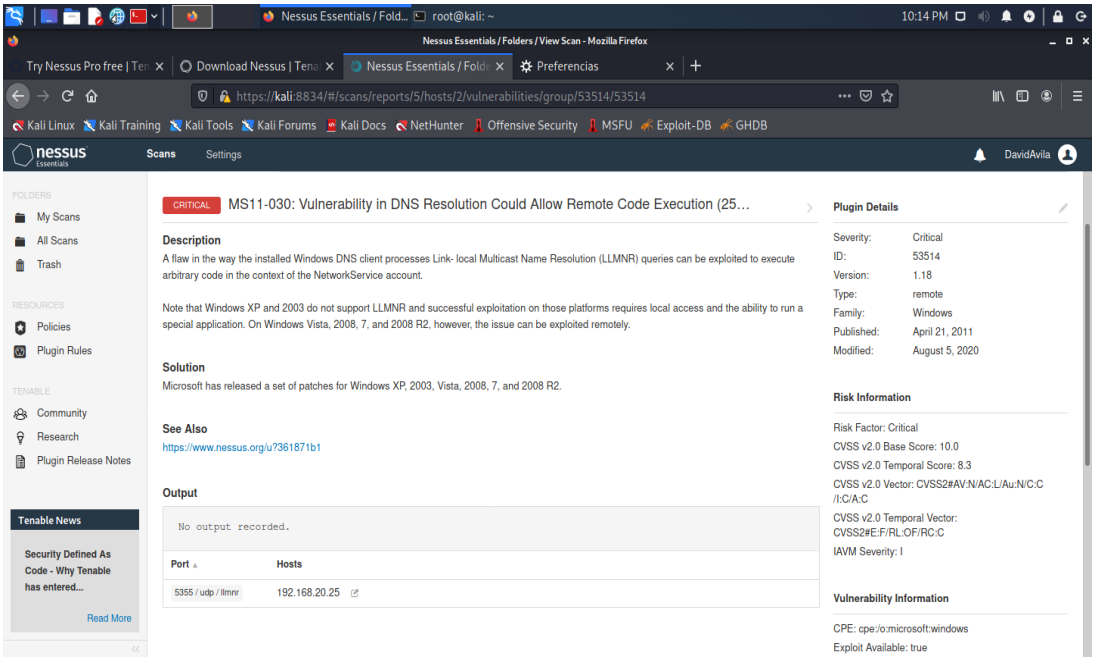
2.3.3 Identificación de la falla de seguridad

Para realizar el análisis de los fallos en la maquina objetivo, se decidió utilizar la aplicación Nessus para la evaluación de las posibles vulnerabilidades.

Luego de realizar el análisis pertinente, se encontró la presencia de 4 vulnerabilidades para evaluar (2 criticas, 1 de tipo alto y 1 de nivel bajo).

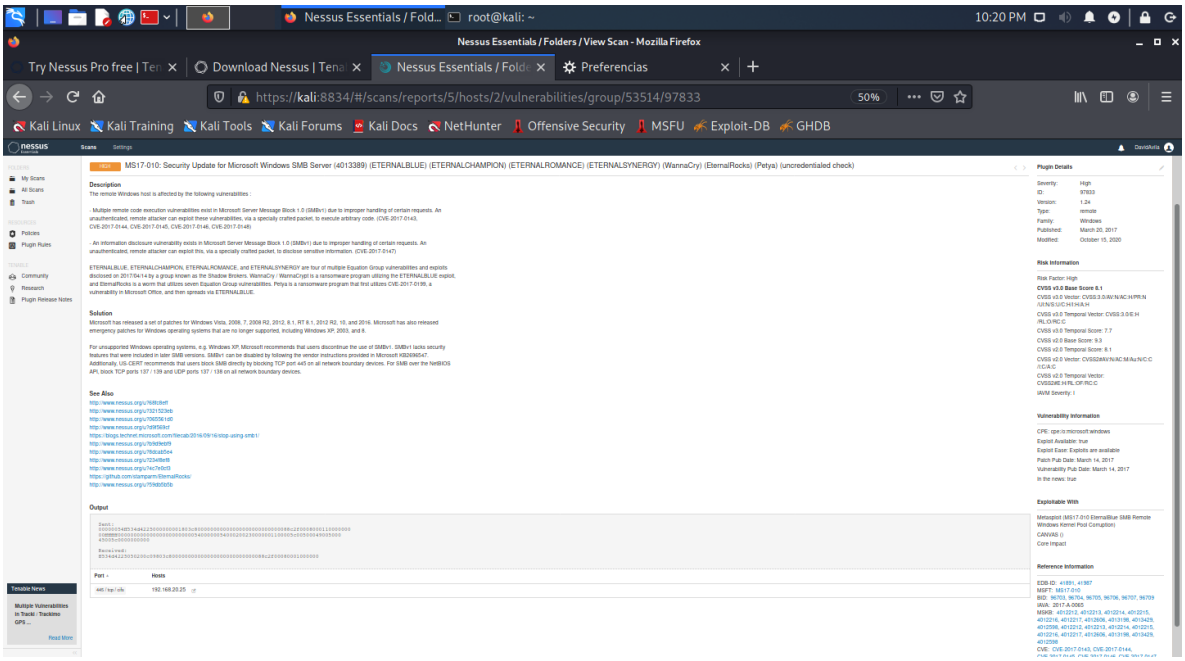
- La vulnerabilidad 1, consiste en la posibilidad de la ejecución de código malicioso de manera remota en el equipo atacado sin que se pueda detectar de manera inmediata y exponiendo no solo a la maquina sino a la organización a la pérdida de información o al daño de ella. El puerto que se evidencio en el análisis fue el 5355 / udp / llmnr. Ver Gráfica 24.

Gráfico 24. Vulnerabilidad 1



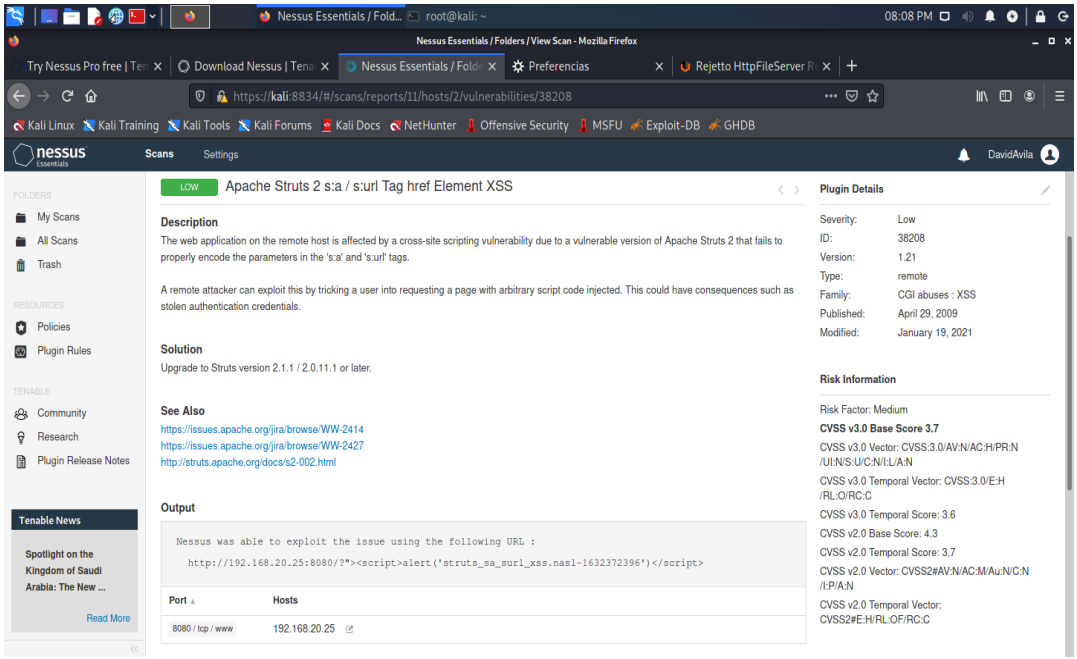
- La vulnerabilidad 2, consiste en la presencia de una serie de vulnerabilidades en el Security Update for Microsoft Windows SMB Server, el cual puede permitir la ejecución de software malicioso de manera remota por cualquier atacante que permita que ellos obtengan el control de la máquina y puedan provocar daños a la compañía. El puerto que se evidencio en el análisis fue el 445 / tcp / cifs. Ver Gráfica 25.

Gráfico 25. Vulnerabilidad 2



- La vulnerabilidad 3, consiste en la presencia de un problema de seguridad para la versión de Apache Struts 2, que podría permitir que un usuario no autorizado inyecte código y pueda robar las credenciales del o los usuarios del equipo. El puerto que se evidencio en el análisis fue el 8080 tcp. Ver Gráfica 26.

Gráfico 26. Vulnerabilidad 3



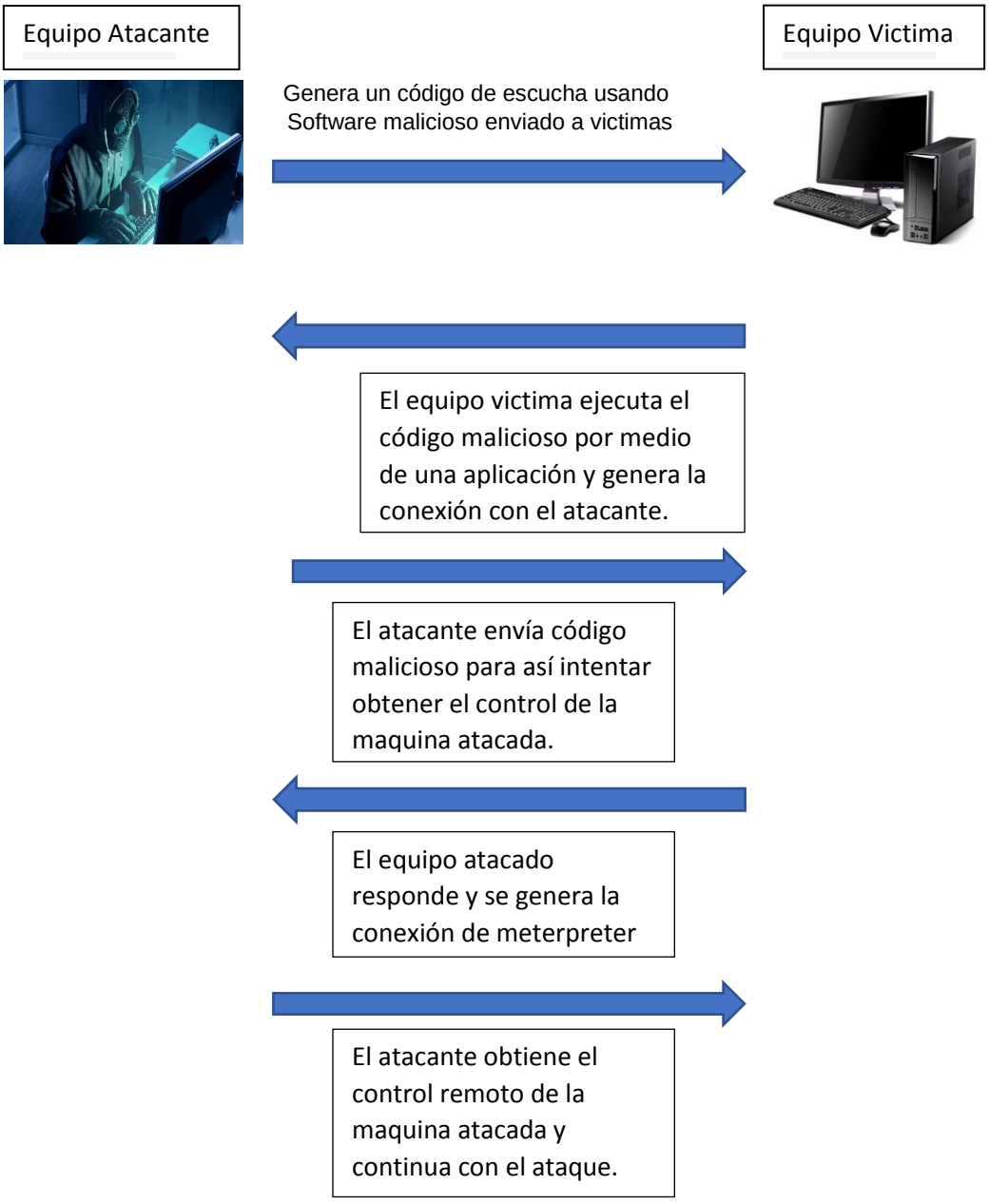
2.3.4 Afectación en la maquina atacada (Windows 7 X64).

De acuerdo con la lectura del anexo 4 – escenario 3 y luego de hacer le pertinente análisis de los hechos se llegó a la conclusión que todo pudo haber sucedido debido a que un usuario utilizando el equipo de cómputo haya de manera intencional o sin ella accedido a un enlace o ejecutado una aplicación con un código malicioso el cual posiblemente estaba conectado a un Shell inverso, el cual genero la conexión con el equipo atacante y permitió que este se comunicara con el equipo afectado.

Una vez realizada la conexión, el atacante pudo iniciar con el proceso de inyección de código en la maquina victima para la obtención de control remoto de esta y una vez que lo consiguiera, iniciaría con la ejecución de aplicaciones que le permita obtener mayores privilegios dentro de la red de la organización y así poder iniciar procesos de robo de información o en el peor de los casos de daño, corrupción o eliminación de datos importantes para el desarrollo de las actividades de la empresa.

Principalmente la maquina atacada se ve afectada no solo en su seguridad, sino que los archivos que en ella se encuentra almacenados quedan a disposición del atacante y a su vez si este equipo está conectado a una red, podría permitir a que el atacante mediante la manipulación de código y/o la obtención de mayores accesos pueda acceder a información privilegiada y de carácter privado para la empresa. Ver Gráfica 27.

Gráfico 27. Ataque a máquina victima



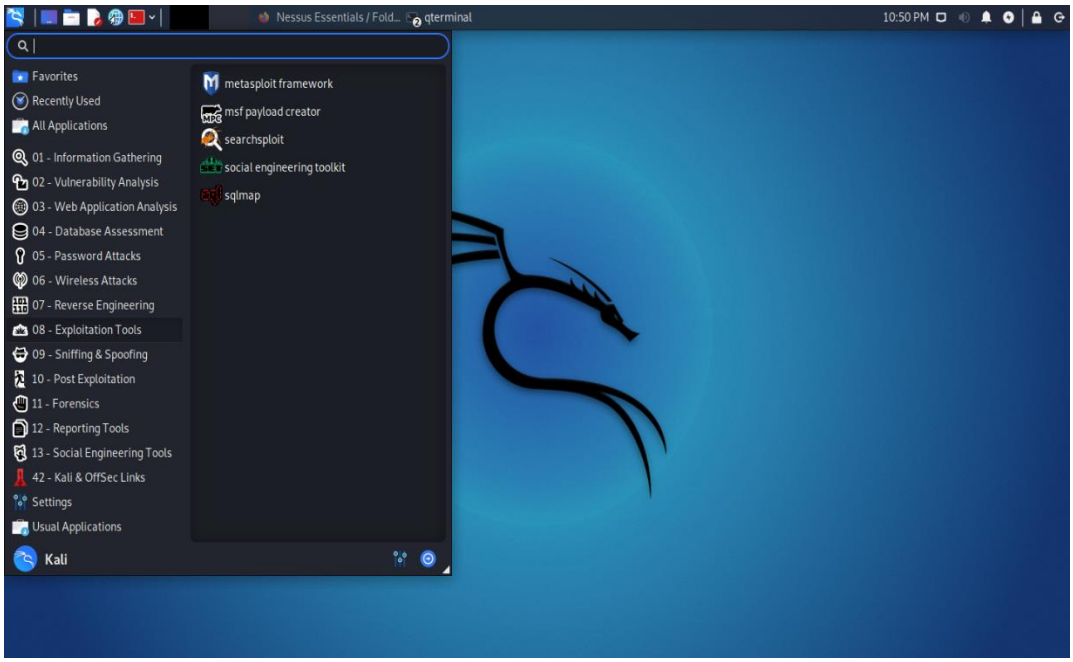
2.3.5 Explotación de vulnerabilidades

Para realizar la explotación de la vulnerabilidad se utilizó la herramienta Metasploit.

A continuación, se explican cada uno de los pasos realizados:

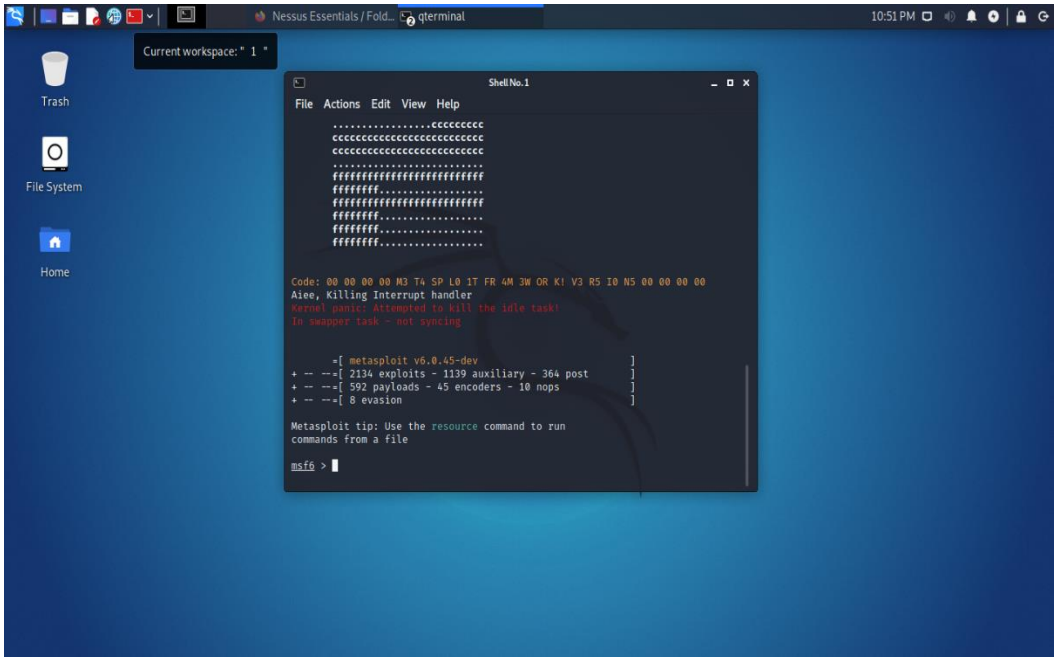
- Se ubica la aplicación de metasploit en Kali y se ingresa. Ver Gráfica 28.

Gráfico 28. Exploración con Metasploit1



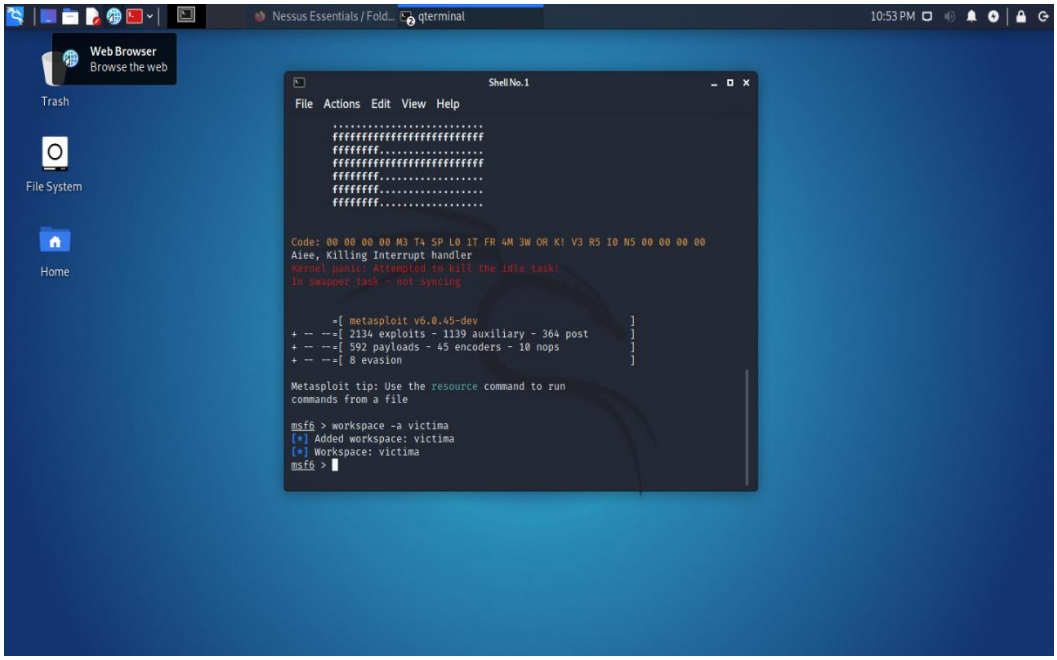
- Una vez que se realiza el ingreso a la aplicación se espera para que se cargue su interfaz. Ver Gráfica 29.

Gráfico 29. Exploración con Metasploit2



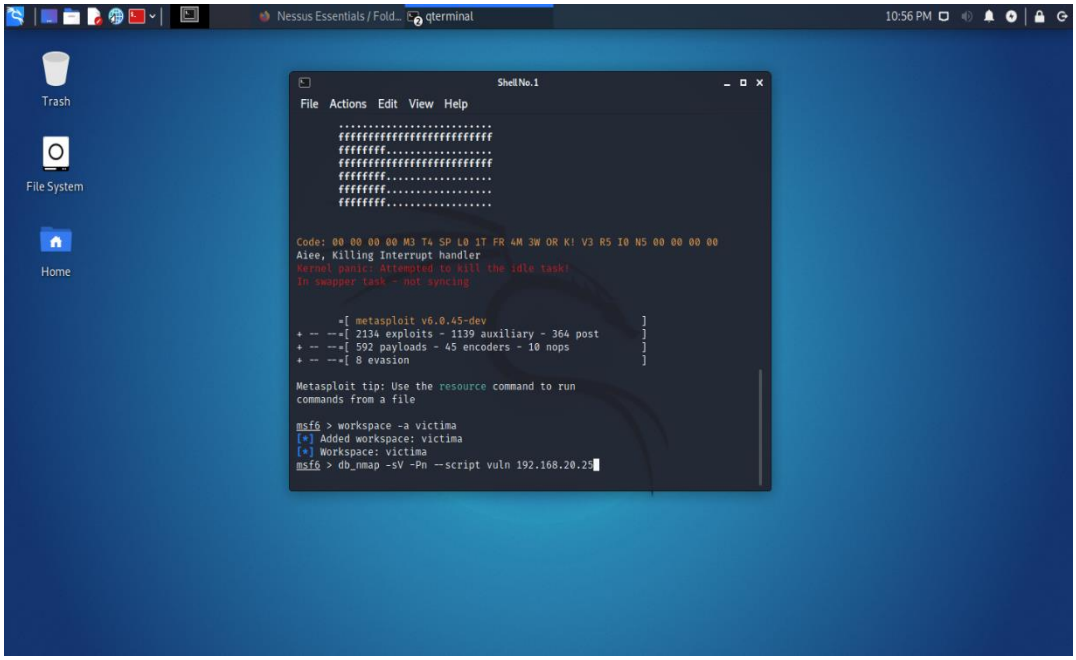
- Cuando cargue la aplicación, se configura un workspace para almacenar todos los comandos que se utilicen. Ver Gráfica 30.

Gráfico 30. Configuración de workspace



- Luego de la creación del workspace, se procede a realizar un análisis de las vulnerabilidades que se pueden encontrar en el equipo víctima. Ver Gráfica 31.

Gráfico 31. Análisis de Vulnerabilidades



- Luego de esperar que se realice la búsqueda se observa los resultados que se generan de la búsqueda de vulnerabilidades. Ver Gráficas 32,33,34

Gráfico 32. Resultados de Análisis de Vulnerabilidades1

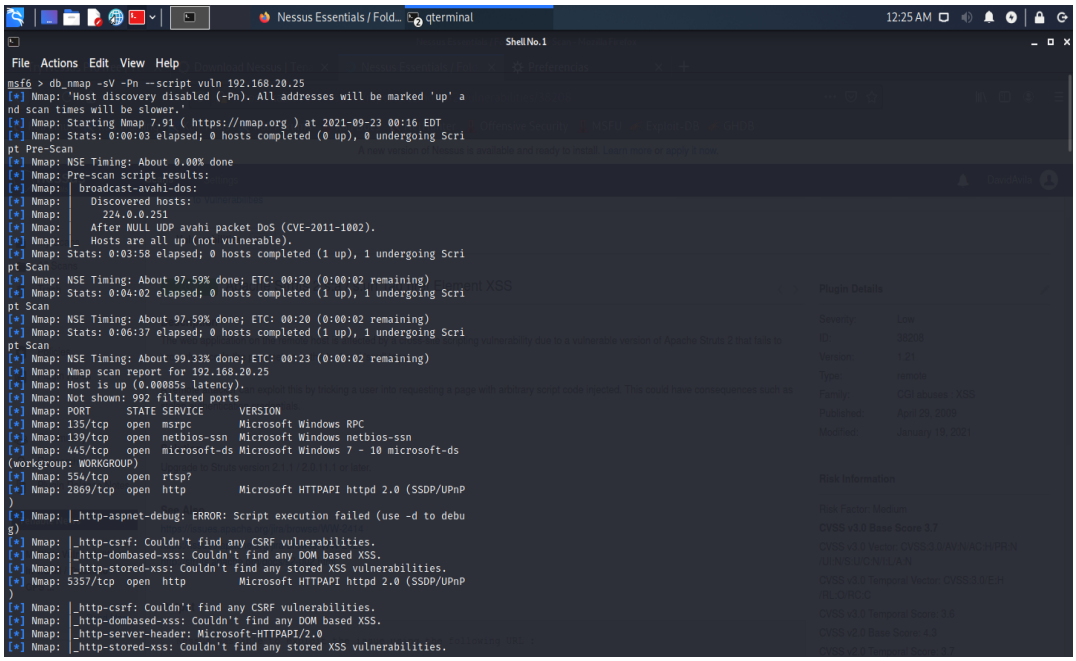
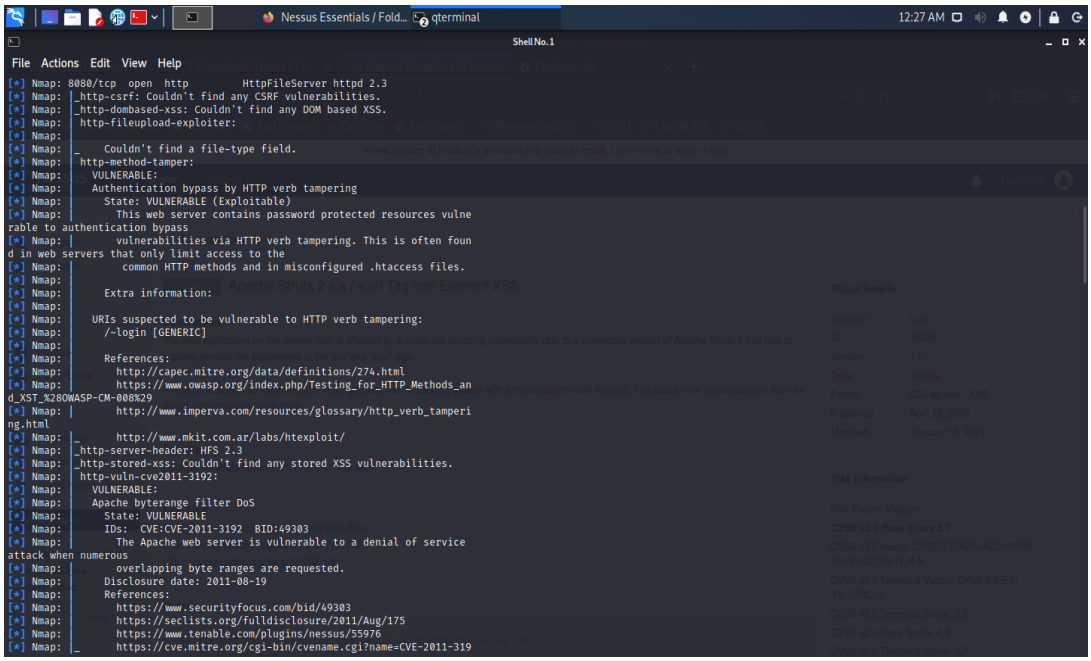
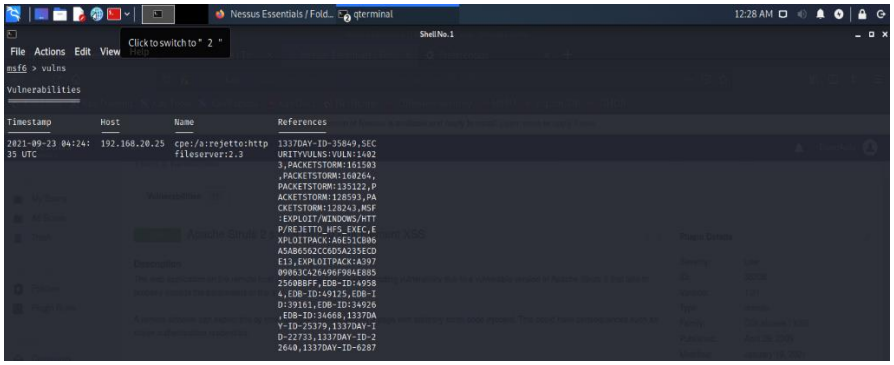


Gráfico 33. Resultados de Análisis de Vulnerabilidades2



- Si se desea ver de manera más ordenada las vulnerabilidades que se encontraron, se realiza el siguiente comando para que estas se listen.

Gráfico 34. Resultados de Análisis de Vulnerabilidades3

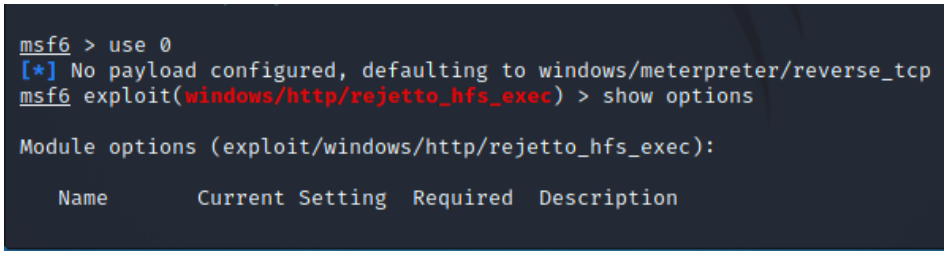


- Ahora que conocemos que hay una vulnerabilidad en el sistema. Realizamos su búsqueda para explotarla. Ver Gráfica 35.

Gráfico 35. Búsqueda de Exploits

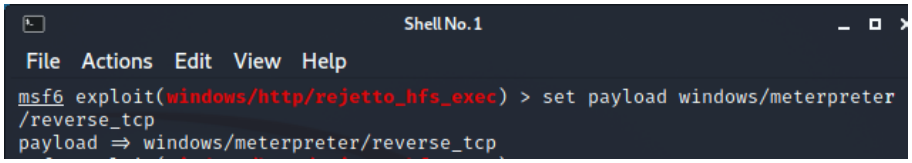
- Una vez que se conoce que hay un exploit para usar en la maquina víctima. Se selecciona y se valida que opciones tiene. Ver Gráfica 36.

Gráfico 36. Uso de exploit.



- A continuación, se configura el payload para poder realizar el ataque. Ver Gráfica 37.

Gráfico 37. Configuración de Payload.



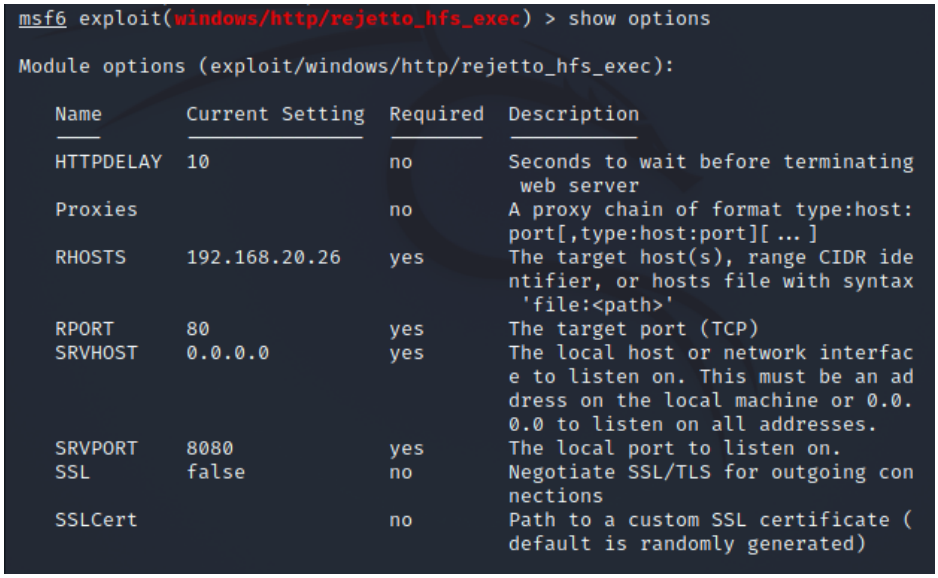
- Posteriormente se realiza la configuración del LHOST y del RHOST. Ver Gráficas 38 y 39.

Gráfico 38. Configuración de LHOST

Gráfico 39. Configuración de RHOST

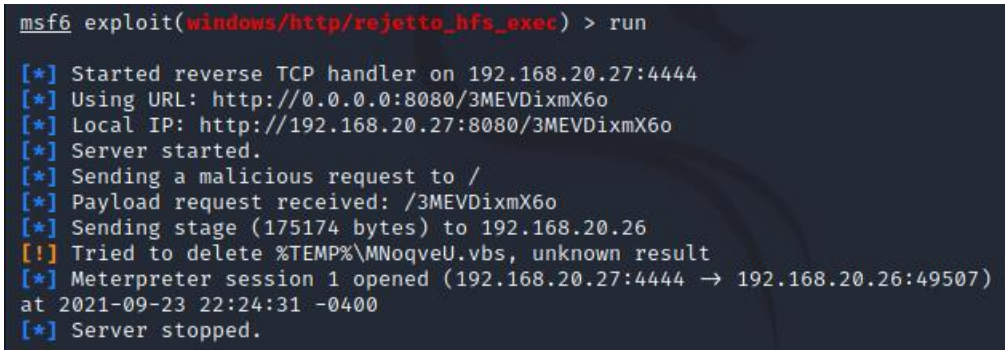
- Se validan las opciones configuradas para validar que todo esté según lo requerido. Ver Gráfica 40.

Gráfico 40. Verificación de opciones del exploit.



- Se ejecuta el exploit y se espera que se complete su ejecución. Ver Gráfica 41.

Gráfico 41. Ejecución del exploit

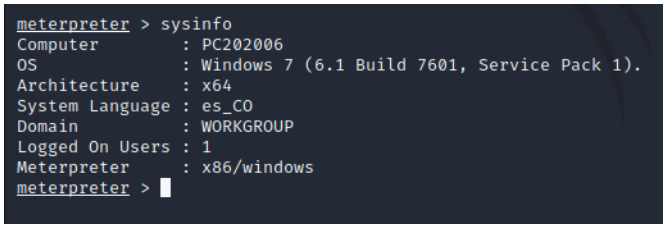


- Si el exploit fue efectivo, se genera una sesión de meterpreter. Para validar la conexión, se valida el usuario con el cual se está conectado al equipo víctima. Ver Gráfica 42.

Gráfico 42. Validación de usuario conectado.

- Una vez en la interfaz de meterpreter se valida la información del sistema operativo para validar el ingreso a este y que nivel de acceso se tiene. Ver Gráfica 43.

Gráfico 43. Validación del SO.



- Posterior utilizamos otros comandos para validar información del sistema. Como el SID, los privilegios, la dirección IP y la lista de procesos. Ver Gráfica 44,45 y 46.

Gráfico 44. Validación del Sistema.

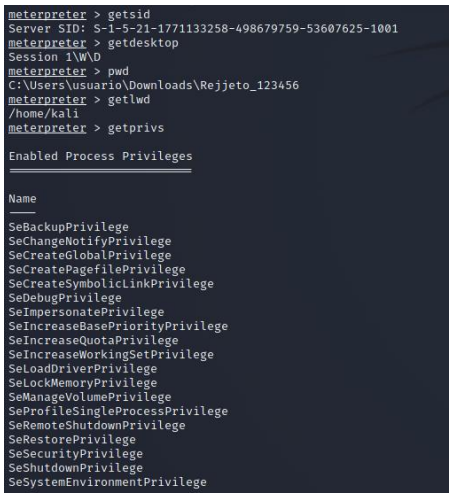
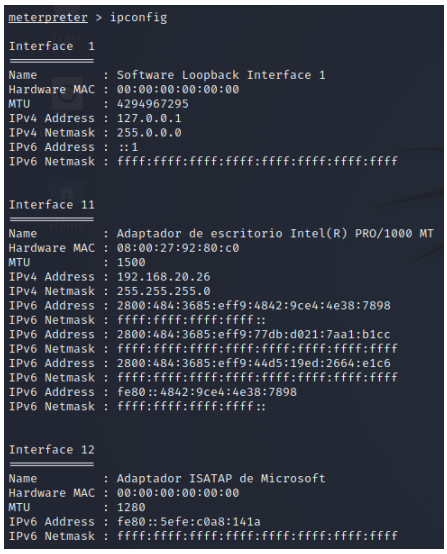


Gráfico 45. Validación de IP Maquina.



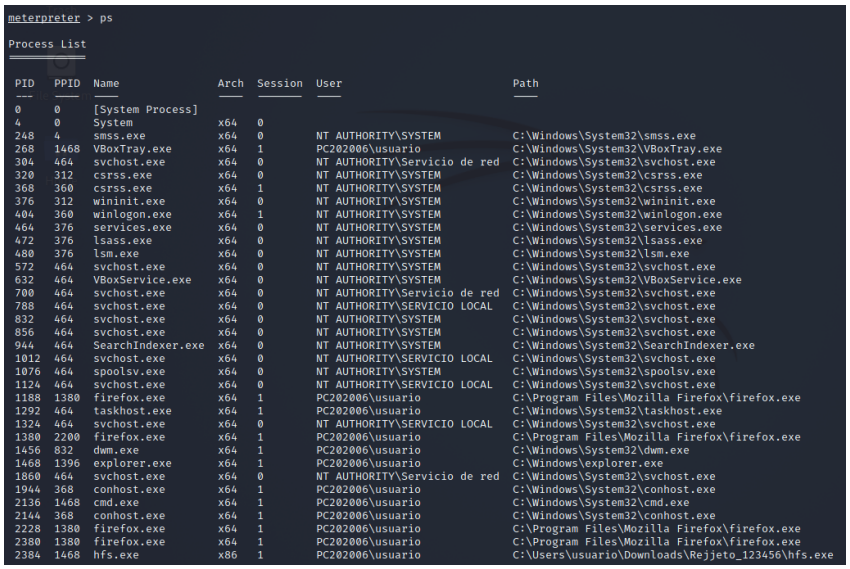
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:92:80:c0
MTU          : 1500
IPv4 Address : 192.168.20.26
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2800:484:3685:eff9:4842:9ce4:4e38:7898
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2800:484:3685:eff9:77db:d021:7aa1:b1cc
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : 2800:484:3685:eff9:44d5:19ed:2664:e1c6
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::4842:9ce4:4e38:7898
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Adaptador ISATAP de Microsoft
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:141a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Gráfico 46. Listado de procesos.



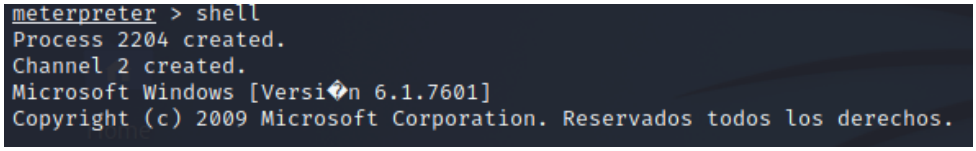
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 248   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 268   1468  VBoxTray.exe       x64   1        PC202006\usuario              C:\Windows\System32\VBoxTray.exe
 304   464   svchost.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
 320   312   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 368   360   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 376   312   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 404   360   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 464   376   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 472   376   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 480   376   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 572   464   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 632   464   VBoxService.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 700   464   svchost.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
 788   464   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 832   464   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 856   464   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 944   464   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 1012  464   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1076  464   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1124  464   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1188  1380  firefox.exe        x64   1        PC202006\usuario              C:\Program Files\Mozilla Firefox\firefox.exe
 1292  464   taskhost.exe       x64   1        PC202006\usuario              C:\Windows\System32\taskhost.exe
 1324  464   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1380  2200  firefox.exe        x64   1        PC202006\usuario              C:\Program Files\Mozilla Firefox\firefox.exe
 1456  832   dwm.exe            x64   1        PC202006\usuario              C:\Windows\System32\dwm.exe
 1468  1396  explorer.exe       x64   1        PC202006\usuario              C:\Windows\explorer.exe
 1860  464   svchost.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
 1944  368   conhost.exe        x64   1        PC202006\usuario              C:\Windows\System32\conhost.exe
 2136  1468  cmd.exe            x64   1        PC202006\usuario              C:\Windows\System32\cmd.exe
 2144  368   conhost.exe        x64   1        PC202006\usuario              C:\Windows\System32\conhost.exe
 2228  1380  firefox.exe        x64   1        PC202006\usuario              C:\Program Files\Mozilla Firefox\firefox.exe
 2380  1380  firefox.exe        x64   1        PC202006\usuario              C:\Program Files\Mozilla Firefox\firefox.exe
 2384  1468  hfs.exe            x86   1        PC202006\usuario              C:\Users\usuario\Downloads\Rejjeto_123456\hfs.exe
```

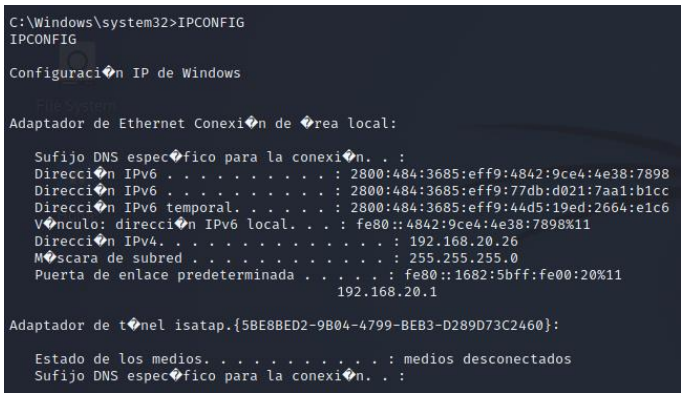
- A continuación se crea la Shell para tener el control del equipo víctima. Ver Gráfica 47.

Gráfico 47. Creación del Shell.



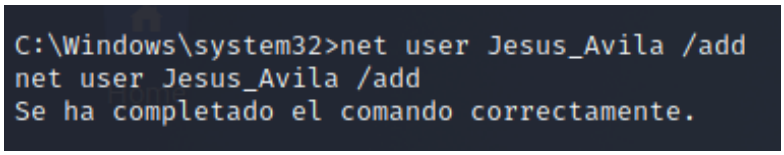
- Con la Shell creada, podemos ahora validar la información del sistema. Iniciamos con verificar la dirección IP de la máquina. Ver Gráfica 48.

Gráfico 48. Validación de la IP víctima.



- Según la solicitud del Anexo 4 – Escenario 3 se realiza la creación del usuario (Jesus_Avila) con privilegios de administración para evidenciar la vulnerabilidad del sistema operativo. Ver Gráfica 49.

Gráfico 49. Creación del usuario.



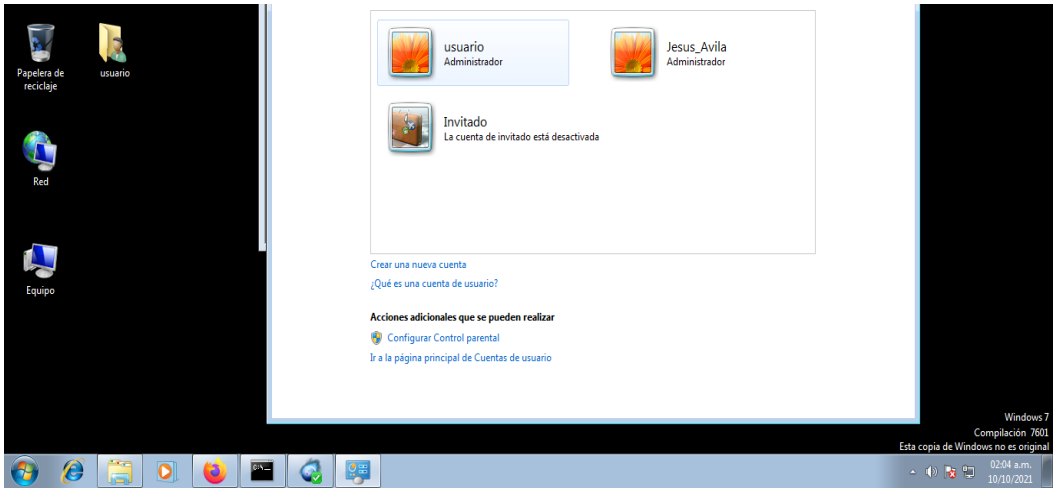
- Luego se le otorga los privilegios de administrador al usuario creado (Jesus_Avila). Ver Gráfica 50.

Gráfico 50. Otorgación privilegios de Administración.

```
C:\Windows\system32>net localgroup administradores Jesus_Avila /add
net localgroup administradores Jesus_Avila /add
Se ha completado el comando correctamente.
```

- Por último se valida por la interfaz gráfica del SO la creación del usuario con privilegios de administrador. Ver Gráfica 51.

Gráfico 51. Verificación Usuario por Windows.



2.4 CONTENCIÓN DE ATAQUES INFORMATICOS

2.4.1 Consideraciones en un ataque en tiempo real:

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

Si se llegara a presentar un ataque en tiempo real el proceso que realizaría sería el siguiente:

- La compañía cuenta con unas políticas de seguridad establecidas que abarquen los diversos delitos informáticos que se puedan presentar.
- Indagaría si la compañía donde se presentó el ataque cuenta con un equipo de respuesta a incidentes informáticos.
- Posteriormente se debería realizar la identificación del incidente.
- Luego indagaría si tienen la posibilidad de identificar que sistemas fueron infectados por el ataque y si hay posibilidad de recuperarlos.
- Cuenta con sistemas de control de los usuarios para validar si la realización del ataque fue debido a un ataque interno.
- Es factible desconectar o aislar los sistemas infectados por el ataque para evaluar los posibles daños que se hayan presentado, la información que se haya comprometido y en dado caso si hubo una sustracción, cuanto de eso cayó en manos de terceros.
- Por último, se debe recopilar los hallazgos realizados y realizar el informe pertinente de resultados.

Aunque las pautas anteriormente descritas pueden ayudar a iniciar con la indagatoria para la evaluación del ataque informático, de por si se requiere de un proceso más laborioso y elaborado para la evaluación correcta de un ataque informático.

Lo más recomendable es seguir las pautas de un análisis forense establecido para realizar la mejor evaluación posible y así generar un verdadero diagnóstico del problema presentado.

Es por ello por lo que como primera medida para evitar la presencia de un incidente de seguridad es tomar las correctas medidas de prevención entre las que se pueden encontrar:

- Mantener actualizado los sistemas informáticos para minimizar las vulnerabilidades nativas de los sistemas informáticos.
- Asegurar los servidores, para ello es otorgar los privilegios de acceso, uso y modificación según corresponda y evitar que cualquier usuario pueda realizar modificaciones críticas en el sistema.
- Asegurar la red con contrafuegos, medidas de seguridad como monitoreo de red, usos de protocolos de seguridad y denegación de ingresos no autorizados.
- Utilizar software antivirus para evitar la ejecución de código malicioso.
- Realizar la capacitación a los usuarios del sistema para que velen por la seguridad de este y sigan las políticas de seguridad establecidas.

Luego de la prevención lo más recomendable es elaborar las pautas de respuestas a incidentes. Como siempre es recomendable, la prevención es la mejor forma para evitar inconvenientes y para ello realizar el documento pertinente donde se tengan

establecidos los objetivos y alcances del plan de acción, el organigrama de respuesta a los incidentes, las manera de actuar de acuerdo al incidente que se pueda presentar, los procedimientos a seguir para la recuperación y minimización del problema, establecer la manera de realizar la investigación del incidente y la elaboración de los informes pertinentes son la principal manera para tener a la empresa siempre lista para estos hechos y que pueda responder de la manera más rápida, efectiva y contundente y con ello minimizar las pérdidas y proteger los insumos de alto valor.

2.4.2 Medidas de hardenización

De acuerdo con el ataque que se ejecutó en el ejercicio de Red Team y basándose en la información que se recopilo de los posibles focos de riesgo que allí se detectaron, se realiza la presentación de las siguientes medidas para asegurar el sistema de una mejor forma para que responda a incidentes:

En primer lugar, se tomarán medidas a nivel del sistema de cómputo como:

- Aseguramiento de los equipos de software y de hardware, para lo anterior es recomendable contar con los parches, actualizaciones de los fabricantes en donde se puedan eliminar vulnerabilidades que puedan tener y que puedan ser aprovechados por delincuentes informáticos.
- Configuración adecuada de los dispositivos como la Bios, deshabilitar dispositivos ópticos, usb o similar que no sean necesarios y sean focos para la ejecución de malware.
- Separación del sistema operativo de los archivos importantes. Para ello es recomendable tener separado la partición del sistema operativo de la partición de los datos sensibles y limitar el acceso a esta para usuarios privilegiados que requieran su uso.
- Instalación de los antivirus, Antispyware y filtros antispam de acuerdo con lo que sea requerido por el sistema.
- Configuración adecuada de las políticas locales del sistema, como contraseñas, almacenamiento de estas, bloqueo de cuentas por intentos de acceso, deshabilitación de cuentas caducadas o no usadas y asignación de perfiles y roles de usuario según sea requerido.

- Configuración de la seguridad de la red, entre la que encontramos el uso de recursos de red, impresoras, carpetas compartidas, unidades de red, entre otros.
- Configuración de los protocolos de red, acceso a las maquinas, permisos a las maquinas dentro de la red, conexiones, entre otros.
- Configuración de seguridad de los programas que tengan acceso a la red y realicen el uso de esta según lo corresponda.
- Adecuada configuración del acceso remoto, realizar la validación de credenciales y permisos según sea este necesario para las labores dentro de la compañía.
- Realizar un cifrado de archivos según sean los niveles de importancia de los datos y la manera en que se va a interactuar con estos, sea por acceso compartido, mensajería instantánea o correo electrónico.
- Mantener un sistema de respaldo correspondiente a los tiempos de manejo y actualización del sistema y que comprenda no solo los datos principales sino también los aplicativos y demás información importante para las labores de la compañía.

En segundo lugar, tomar las medidas correspondientes a los usuarios, porque a la larga son ellos los que van a manipular el sistema y por ende son el primer filtro de inseguridad que se pueden presentar:

- Capacitación y conocimiento en las políticas de seguridad de la compañía.
- No permitir que se descargue datos, programas, archivos desde sitios no seguros ni reconocidos, o que sean catalogados como posibles fuentes de inseguridad informática.
- Enseñar en no abrir archivos que procedan de fuentes no conocidas, poco confiables o que no se conozca de manera directa el remitente de esta información.
- Generación de contraseñas robustas, con uso de caracteres especiales, que no involucren cosas personales, familiares o conocidas por muchas personas.
- Mantener su sistema de cómputo actualizado en dado caso que utilicen equipos que no sean de la organización para el acceso a los servicios de red que la compañía permita.
- Mantener buenas prácticas en el uso de la información, correcto uso de esta dentro y fuera de la organización y no permitir que usuarios externos puedan tener acceso a esta.

- Evitar el uso de dispositivos externos como usb que no hayan pasado por un proceso de verificación de software malicioso, malware a través de un programa de antivirus.

Hay que tener en cuenta que no hay medidas suficientes para prevenir que se presente un ataque en un sistema informático, pero si se pueden tomar medidas para minimizar los riesgos que se presenten, minimizar el acceso que se pueda tener a la información importante, minimizar las vulnerabilidades que se tengan en el sistema y sobre todo aprender, conocer e identificar las posibles amenazas que pueden afectar el sistema y sobre las cuales se deben tener y tomar las pertinentes recomendaciones.

2.4.3 Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

De acuerdo con las definiciones de un equipo de Blueteam y un equipo de respuesta a incidentes informáticos podemos encontrar lo siguiente:

- Mientras el equipo de Blueteam realiza tareas de rastreo e investigación de diversos delitos informáticos y su comportamiento. El equipo de respuesta a incidentes informáticos controla y en algunos casos minimiza posibles daños que se puedan presentar a la información de una organización.
- El equipo de Blueteam realiza monitoreo de un sistema informático, el comportamiento de los usuarios que acceden a él, las acciones que se realizan, las conexiones que se realizan habitualmente. El equipo de respuesta a incidentes informáticos debe reaccionar de manera inmediata durante la presencia de un ataque o delito informático e intentar salvaguardar y minimizar los daños que pueden acarrear con este ataque.
- Por último, podemos destacar que, aunque ambos equipos están compuestos por especialistas informáticos en la detección y minimización de ataques informáticos. Mientras el equipo de Blueteam está más enfocado en realizar análisis de todo el sistema, de sus componentes, comportamientos, interacción con la red interna y con internet para encontrar posibles ataques que hayan parecido inadvertidos, acciones que potencien la posibilidad de ataques o vulnerabilidades que puedan ser explotadas, el equipo de respuesta a incidentes informáticos está más enfocado a analizar y aprender de los ataques que se hayan presentado no solo en la compañía sino en el ambiente laborar que se desempeñe y con ello intentar estar preparados cuando se presente un ataque y sean capaces de responder de la manera

más rápida y oportuna para minimizar, perdidas, daños y demoras en los servicios que la compañía tenga u ofrezca.

2.4.4 Definición y uso de un CIS “Center For Internet Security”

CIS o según sus siglas en inglés, Center For Internet Security son un conjunto de las buenas prácticas que se deben tener en un sistema informático para así minimizar de acuerdo con la categoría de la compañía, a la infraestructura con la que cuente y a la importancia de la información que en ella se maneje, todo posible delito informático, vulnerabilidad presente en el sistema y posibles focos de inseguridad que pueda comprometer los recursos vitales de la compañía.

Igualmente son muy importantes porque están realizadas gracias al aprendizaje de los diversos ataques informáticos que se han presentado en la historia y de los cuales se tienen registros y son muy importantes para impedir que la compañía se relaje y tienda a dejar desprotegido zonas de su estructura que queden vulnerables a ataques y que a la larga le pueden costar grandes pérdidas no solo a nivel monetario sino a nivel de información.

En el dado caso que dentro del equipo de Blueteam tuviera que utilizar o trabajar con CIS, lo utilizara principalmente como herramienta para la prevención de posibles ataques informáticos que se pudieran presentan dentro de la organización o las organizaciones a las cuales el Blueteam les brinda sus servicios.

Por conocimiento pleno, es recomendable conocer que los controles CIS se dividen en 3 tipos de controles cada uno específico para un tipo de organización que realice su implementación. Ver Tablas 1, 2, 3.

Tabla 1. Controles de CIS Básicos.

Control 1: Inventario y control de activos de hardware
Control 2: Inventario y control de activos de software
Control 3: Gestión continua de vulnerabilidades
Control 4: Uso controlado de los privilegios administrativos
Control 5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores
Control 6: Mantenimiento, monitoreo, y análisis de logs de auditoría

Tabla 2. Controles de CIS Fundamentales.

Control 7: Protección de correo electrónico y navegador web
Control 8: Defensas contra malware
Control 9: Limitación y control de puertos de red, protocolos y servicios
Control 10: Funciones de recuperación de datos
Control 11: Configuración segura para dispositivos de red, tales como firewalls, routers y switches
Control 12: Protección perimetral
Control 13: Protección de datos
Control 14: Control de acceso basado en la necesidad de saber
Control 15: Control de acceso inalámbrico
Control 16: Monitoreo y control de cuentas

Tabla 3. Controles de CIS Organizacionales.

Control 17: Implementar un programa de concienciación y capacitación en seguridad
Control 18: Seguridad del software de aplicación
Control 19: Respuesta y gestión de incidentes
Control 20: Pruebas de penetración y ejercicios de equipo rojo

2.4.5 Funciones y características principales de un SIEM.

De acuerdo con lo que podríamos denominar como SIEM, una herramienta que se enfoca en evaluar, categorizar, interpretar y detectar las posibles amenazas que se presenten en tiempo real en un sistema informático para así responder de la manera más rápida y precisa y mitigar los riesgos y el impacto negativo que pueda tener un ataque informático a la infraestructura de la organización donde se esté ejecutando

Las funciones y características que contempla un SIEM son:

- Análisis en tiempo real de los eventos que se estén ejecutando en un sistema informático.

- Documentación y almacenamiento de los eventos para su evaluación, procesamiento y solución. Todo con el fin que sirvan de insumo y ayuda en los problemas que se presenten en el futuro.
- Detección de tendencias y/o patrones de comportamiento en un sistema informático para detectar aquellos que no correspondan a los habituales realizados en el sistema informático.
- Centralización e Implementación inmediata de soluciones a las posibles vulnerabilidades o ataques que se presenten en un sistema informático.
- Categorización de amenazas para conocer cuáles deben ser evaluadas y resueltas de manera inmediata y cuales no justifican esfuerzos o no se deben tener en cuenta porque su impacto es mínimo o nulo.
- Redirigir cuando sea requerido los temas eventos que se presente al personal especializado para la evaluación correspondiente y posterior solución de la manera más rápida posible.
- Cumplir con las normas y legislaciones vigentes que se establezcan a nivel de la protección de los datos, la información y la posibilidad de delitos informáticos.

2.4.6 Herramientas de contención de ataques informáticos

A continuación, se especifican las herramientas que pueden ser utilizadas para la contención de ataques informáticos en un sistema:

2.4.6.1 FIREWALL:

Como lo dice su nombre un firewall es una herramienta que mediante una serie de reglas genéricas o especificas definidas por el administrador del sistema, escanea los paquetes que se transmiten por la red y los permite o bloquea según las reglas establecidas.

La configuración de dichas reglas puede iniciar desde un modo bajo y poco restrictivo a un nivel alto y que solo permita conexiones especificas con la red. Siempre es recomendable tener un firewall funcionando en la red interna y en su caso en que trae por defecto los sistemas operativos Windows para aumentar el nivel de seguridad que se tenga.

2.4.6.2 CIFRADO DE PUNTO FINAL O END POINT DISK ENCRYPTION:

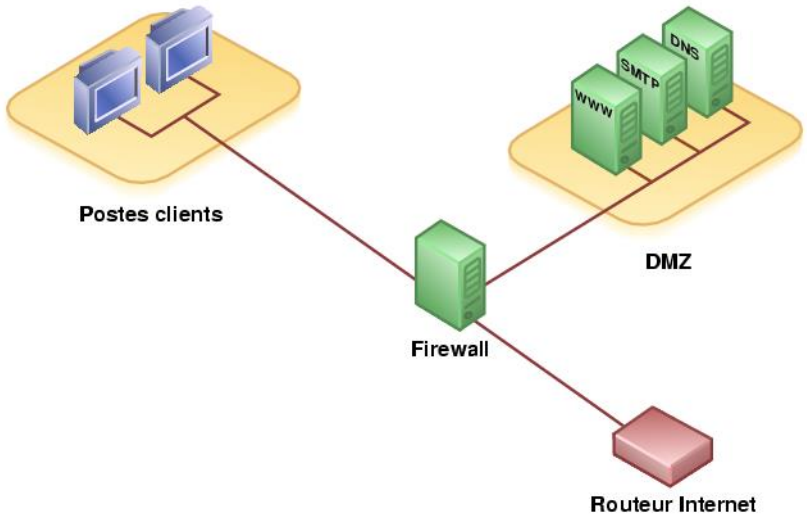
Consiste en el cifrado de los datos, estén estos en un disco físico, en carpetas o en unidades extraíbles, todo con el fin de impedir que usuarios no autorizados puedan tener acceso a la información y con ello generar daños a la organización.

2.4.6.3 DMZ:

Las zonas desmilitarizadas, se entiende como una red que aísla la red interna de la compañía con la red externa y permite servir de intermedio para que en caso de ataques informáticos los atacantes solo puedan tener acceso a la DMZ y no comprometan los datos privados e importantes que se encuentran en la red interna. Ver Gráfica 52.

Normalmente las DMZ son configuradas en los firewalls, de acuerdo con los parámetros que se deseen permitir acceso y los servicios que esta vaya a realizar o utilizar en la red externa.

Gráfico 52. Modelo de DMZ.



2.4.6.4 SNORT:

Es un software de código abierto, que se utiliza para el análisis de datos y paquetes que se transmiten por la red y con ello identificar posibles alteraciones que lleven a detectar intrusos o anomalías que pueden desembocar en posibles daños a la organización.

Se basa principalmente en reglas para saber que analizar, cuando analizar, para así tomar la medida establecida en cada regla y ayudar a controlar posibles ingresos no autorizados en el sistema de información.

3. CONCLUSIONES

A continuación, se indican las conclusiones que se encontraron de acuerdo con el desarrollo de la actividad propuesta en este documento.

- Los aspectos de seguridad informática no son algo novedoso, pero en la proliferación de plataformas., aplicaciones y personal capacitado para su uso, ha hecho que los delitos informáticos vayan en crecimiento y por ende el compromiso que deben tener ahora las compañías es más que tener software licenciados sino llega hasta adquirir personal capacitado para hacerle frente a estas nuevas amenazas que han aparecido.

- Muchos creemos que pasando por una universidad es suficiente para generar un sentido de ética profesional y valores morales. Pero es de hecho que es allí donde los valores que nosotros tenemos, los que se traen desde el hogar salen a la luz y se dejan ver en su totalidad. Es muy probable que una persona con altos valores nace así y es durante su vida donde se va formando y distinguiendo que es lo bueno y malo y es ahí donde se podría cultivar esos valores que luego en su vida adulta les permitan tomar las correctas decisiones y no dejarse llevar por cosas monetarias o bienes materiales que los inciden a cometer delitos.

- Las organizaciones nunca deben escatimar en tener sistemas robustos de seguridad informática y más sabiendo que la información es su insumo más importante porque cada vez hay más ciberdelincuentes y ellos si se están capacitando con nuevas herramientas para violar los controles de seguridad.

- Conocer las leyes existentes sobre delitos informáticos que hay establecidas en nuestro país es de alta importancia para así tomar las correspondientes posiciones en caso de percatarse de infracciones, delitos o si no se está muy seguro de realizar alguna acción por consecuencia al trabajo que luego pueda ser catalogada como delito.

4. RECOMENDACIONES

De acuerdo con las actividades realizadas y teniendo en cuenta los resultados obtenidos en cada una de ellas se proponen las siguientes recomendaciones:

- Fomentar la capacitación continúa de los empleados de la organización frente a aspectos de seguridad informática, lo anterior porque la ciberdelincuencia nunca deja de evolucionar y mientras ellos no se queden estáticos, igualmente las organizaciones deben mantenerse alerta y siempre resguardando la información vital para sus actividades.

- Contar con equipos de Red Team & Blue Team son puntos a favor para las organizaciones porque mientras uno te mantiene seguro de posibles ataques informáticos, el otro pone a prueba los sistemas con los que se cuenta para evaluar las falencias y vulnerabilidades mejorando así la seguridad con la que se cuente.

- Las leyes para la protección de delitos informáticos son importantes y cada profesional en el área de sistemas está en la obligación de conocerlas y usarlas cuando tenga conocimiento de su infracción y no puede convertirse en un cómplice de ello, aunque esto signifique perder un cargo alto o perdida de retribuciones monetarias.

- Si las organizaciones quieren estar en un ambiente digital, no solo deben acudir a su facilidad y cobertura para su mercado sino también deben asumir los riesgos que hay y con ellos los problemas que puedan venir y provocar pérdidas de información valiosa. Por eso deben prepararse y siempre tener en mente que, aunque no sean blancos de ataques eso no los hace invisible para siempre.

- Contar con buenos estándares de seguridad, políticas de seguridad definidas, personal capacitado y actualizado y una infraestructura robusta, son los mejores amigos para que una compañía se sienta segura y este en la capacidad de responder a la gran cantidad de ataques informáticos que se presentan día a día en el mundo.

BIBLIOGRAFIA

APRENDAAHACKEAR, Metasploit, tomar control de equipos remotos Internet: (http://www.cursodehackers.com/metasploit.html).

CISCO, ¿What is Cybersecurity? Internet: (https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html).

COLOMBIA. CONGRESO DE LA REPÚBLICA. Constitución política de Colombia. Art. 15. De los derechos fundamentales.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599 (24, julio, 2000). Art. 192. Por medio de la cual se especifica los cambios de pena para quien realice violación ilícita de comunicaciones.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679 (03, agosto, 2001). Por medio de la cual se expide el estatuto para prevenir y contrarrestar la explotación, pornografía y el turismo sexual con menores de edad.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1377. (27, junio, 2013). Por medio de la cual se expide el régimen general de protección de datos personales.

COPNIA, Código de ética. Internet: (https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica).

EKU, Security Management Guide: Essentials, tips & definitions Internet: (https://safetymanagement.eku.edu/blog/security-management-guide/).

GRUPO SMARTEKH, ¿Qué es Hardening? Internet: (https://blog.smartekh.com/que-es-hardening).

HACKNOID, 5 Herramientas de seguridad informática claves en empresas. Internet: (https://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/).

ITDIGITALSECURITY, ¿Qué es un Blue Team y cómo trabaja? Internet: (https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja).

MANAGEENGINE, ¿Qué son y cómo implementar los controles de seguridad crítica CIS? Internet: (https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html).

MARKER, Graciela, DMZ, ¿Qué es? Tipos y usos. Internet: (https://www.tecnologia-informatica.com/dmz-que-es-tipos-usos/).

MCAFEE, ¿What is Endpoint Encryption? Internet: (https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-endpoint-encryption.html).

RAMIRO, Ruben, Reglas SNORT, detección de intrusos y uso no autorizado. Internet: (https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/).

RAPID7, Vulnerabilities, Exploits, and Threats Internet: (https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/).

SHIVANANDHAN, Manish, What is Nmap and how to use it – A tutorial for the geatest scanning tool of all time Internet: (https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/).

TECHTARGET, ¿What is Cybersecurity? Internet: (https://searchsecurity.techtarget.com/definition/cybersecurity).

TUNGGAL, Abi Tyas, ¿What is a Vulnerability? Internet: (https://www.upguard.com/blog/vulnerability).

ANEXOS

- Enlace del video de sustentación del desarrollo del seminario: https://youtu.be/-ktDxowcbUM