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

FABIO ANDRÉS LASSO ARTURO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2021

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

FABIO ANDRÉS LASSO ARTURO

Trabajo de grado para optar al título de especialista en Seguridad informática

Director
M.SC. JOHN F. QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Santiago de Cali, 12 de octubre de 2021

A Dios.
Por haberme permitido llegar hasta este logro, brindándome salud, además de su infinita bondad y amor,

A mis padres.
Quienes gracias a sus consejos y apoyo incondicional me llenan de fuerza cuando los problemas parecer no tener solución,

A mis allegados y compañeros.
Por tener palabras y acciones colaborativas en busca del éxito de mis actividades diarias.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACTIVO: Cualquier cosa que tiene valor para la organización. Existen varios tipos de activos, como la información, software, infraestructura tecnológica, servicios, las personas junto con sus conocimientos, habilidades y experiencia, o intangibles como la reputación o imagen de la empresa. Las marcas y la propiedad intelectual también son ejemplos de activos.

ACTIVO DE INFORMACIÓN: Conocimiento o datos que tienen valor para la organización.

CONTENEDOR: Ubicación donde los activos de información son almacenados, procesados o transportados, en otras palabras, el lugar donde “vive” el activo de información. Pueden ser clasificados en técnicos (hardware, software, aplicaciones, servidores o redes), físicos (archiveros) y humanos (personas que tienen acceso a la información).

SEGURIDAD DE LA INFORMACIÓN: disciplina responsable de sostener la disponibilidad, confidencialidad e integridad de la información.

CONFIDENCIALIDAD: Propiedad de la información para ser accesible únicamente por los individuos, entidades o procesos que poseen los privilegios y la autorización.

INTEGRIDAD: Propiedad de la información para mantener su exactitud y completitud.

DISPONIBILIDAD: Propiedad de la información para ser accesible y utilizable cuando una entidad lo requiera.

SEGURIDAD INFORMÁTICA: es solo una parte del alcance de la disciplina de la Seguridad de la Información, está limitado al ámbito tecnológico de la protección de la información.

AUTENTICIDAD: Propiedad de una entidad para mostrar que es quien dice ser.

RESPONSABILIDAD: Rendición de cuentas de una entidad por sus actos y decisiones.

NO REPUDIO: Capacidad de probar la ocurrencia de un evento o acción realizada por una entidad de origen.

FIABILIDAD: Propiedad de mantener la consistencia entre un comportamiento previsto y sus resultados.

EVENTO DE SEGURIDAD: Ocurrencia identificada en un sistema, servicio o estado de la red que indica una posible violación de las políticas de seguridad, la falla de los controles o una situación previamente desconocida que puede ser estar relacionada con la seguridad.

INCIDENTE DE SEGURIDAD: Evento o conjunto de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.

VULNERABILIDAD: Debilidad en un activo o control que puede ser explotada por una o más amenazas.

AMENAZA: Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización.

ATAQUE: Intento de destruir, exponer, alterar, inutilizar, robar, obtener acceso no autorizado o hacer uso indebido de los activos.

RIESGO: Efecto de la incertidumbre sobre los objetivos, es decir, sobre los resultados específicos que se desean obtener.

OBJETIVO DE CONTROL: Enunciado que describe lo que se desea alcanzar como resultado de la implementación de controles.

CONTROL: Medida que modifica el riesgo.

SGSI: Proceso utilizado para identificar los activos críticos de una organización, evaluar continuamente los riesgos de seguridad asociados a esos activos y aplicar medidas de seguridad razonables para su protección, a través de un conjunto de actividades aplicadas de manera coordinada y enmarcadas dentro un ciclo de mejora continua.

ESTÁNDAR: la Real Academia Española define estándar como un elemento que sirve como tipo, modelo, norma, patrón o referencia. De acuerdo con ISO (“*International Organization for Standardization”*), se trata de un documento que provee requisitos, especificaciones, guías o características que pueden ser utilizados de manera consistente, para asegurar que materiales, productos, procesos y servicios son adecuados para su propósito.

RESUMEN

El presente documento aborda conceptos básicos sobre los equipos RedTeam y BlueTeam.

Se definen términos, tales como, seguridad de la información, las propiedades que la conforman (confidencialidad, integridad y disponibilidad), vulnerabilidad, amenaza, riesgos, probabilidad, impacto, control y objetivo de control dentro del contexto del ética hacking, normas y leyes vigentes, para el desarrollo de pruebas de penetración a sistemas informáticos.

También se definen los procesos y elementos que permiten conformar una metodología para pruebas de penetración, desde un enfoque practico, como lo es, el seminario especializado en equipos BlueTeam y Redteam.

INTRODUCCIÓN

Las pruebas de penetración a sistemas informáticos datan de los años sesenta, por los llamados Tiger Teams, dedicados a generar pruebas al interior de los sistemas de gobierno y militares. (Ridge Marketing, 2021)

Posteriormente en los años noventa, estos Tiger Teams pasaron a dar origen a la terminología Hacking Ético. (Ridge Marketing, 2021)

Hoy en día, son escasas las pruebas de penetración, realizadas por terceros de manera manual y su evolución ha sido lenta con el pasar de los años. (Ridge Marketing, 2021)

De allí la importancia de conocer la mejor practica (acciones, metodologías, herramientas y técnicas) que actualmente se están aplicando y probando en el mundo en pro de llevar a un nivel más alto la seguridad de la información de las organizaciones.

El presente documento pretende ser una guía para conocer las capacidades técnicas, legales y de gestión para equipos Blue Team Y Red Team, en ámbitos de aplicación del Hacking Ético en organizaciones que buscan niveles de seguridad óptimos bajo los tres principios básicos de la seguridad en la informática: disponibilidad, integridad y confidencialidad.

1. OBJETIVOS

1.1 GENERAL

Planificar estrategias basadas en metodologías de ciberseguridad defensivas y ofensivas, que permitan hacer frente a un evento o incidente informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

1.2 ESPECIFICOS

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

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

Hoy en día, el activo de mayor valor para muchas organizaciones es la información y en tal sentido asumen una significativa importancia las acciones tendientes a garantizar su permanencia en el tiempo con un nivel de acceso controlable y seguro, ya que contribuye a facilitar el logro de los objetivos y la misión en las diferentes organizaciones, mediante el manejo de grandes volúmenes de información; las empresas públicas, privadas y mixtas, al igual que la gran mayoría de las personas, necesitan de las tecnologías de la información y comunicación, ya que son una herramienta esencial que facilita los procesos de negocio y las actividades cotidianas en la oficina y en el hogar.

Lo que conlleva a involucrarse con una gran variedad de riesgos, amenazas y vulnerabilidades de los sistemas informáticos. La seguridad informática hace referencia a la protección de los activos de información fundamentales para el éxito de cualquier organización. Los elementos de protección digital surgen como herramientas en este contexto, logrando que la información al interior de las organizaciones preserve su confidencialidad, integridad y disponibilidad, todo esto gracias al conocimiento, gestión y minimización de los posibles riesgos que atentan contra la seguridad de la información.

Por este hecho es importante la identificación de los factores de riesgo, tanto internos como externos, que pueden significar un factor de amenaza contra los tres principios básicos de la seguridad de la información empresarial, y a partir de ello buscar las mejores alternativas para el aseguramiento de un entorno de trabajo fiable.

En el caso práctico de estudio “Whitehouse Security”, al igual que en muchas de las empresas colombianas, no se cuenta con un proceso sistemático, documentado y de conocimiento por parte de todos los miembros de la organización, que permita la preservación de la confidencialidad, integridad y disponibilidad de la información al interior de sus procesos desde un enfoque de riesgo empresarial. Se generan fases o escenarios donde se pretende el reclutamiento para los equipos Blue Team y Red Team, mediante el conocimiento guiado de los procesos para llevar a cabo pruebas de penetración y Hacking Ético.

Este proceso debe contar las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y de las operaciones de la compañía en situaciones de riesgo que suspenda parcial o totalmente su operación, por lo tanto, ¿Es necesario conocer las capacidad técnicas, legales y de gestión para equipos Red Team y Blue Team?, como una solución eficiente para la protección de los activos de información del negocio, ya que se requiere

conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información al interior de la organizaciones.

3. JUSTIFICACIÓN

Los Equipos Blue Team y Red Team, generan desde un proceso multidisciplinar investigación que permiten poner en evidencia los riesgos informáticos al interior de los sistemas de información que representen relevancia en las organizaciones.

Porque mediante la aplicación de pruebas de penetración, hacking ético de carácter interno y externo, se realizan hallazgos de la necesidad del uso de controles que mitiguen las vulnerabilidades encontradas y a su vez permitan realizar investigación forense cuando se materialicen estas vulnerabilidades.

Aportando a los sistemas de gestión de la seguridad de la información desde la normatividad legal vigente y de reconocimiento internacional; ya que el volumen de información es a diario mayor y exige no escatimar esfuerzos en pro de fortalecer los niveles de disponibilidad, confidencialidad e integridad de la información, obligando así, a las organizaciones a involucrar dentro de su cultura organizacional, la definición, gestión y evaluación de estrategias se seguridad de la información a través de la conformación de equipos Blue Team y Red Team.

Y de igual manera, para que en la empresa “Whitehouse Security”, tenga claridad para la implementación de equipos Red Team y Blue Team con un enfoque no solo en capacidades técnicas sino de marco legal y gestión.

4. MARCO REFERENCIAL

4.1 MARCO LEGAL DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES

Investigando el contexto vigente de la legislación colombiana referente a delito informático y protección de datos personales tenemos:

4.1.1 Ley 1273 de 2009:

Esta ley modifica el código penal, en el artículo 53 dando como agravante el uso de medios informáticos, electrónicos o telemáticos para la realización de conductas punibles a los delitos, tales como:

- Obstaculización ilegítima de sistema informático.
- Interceptación de datos informáticos.
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales. (Phishing)
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Esta ley incluye un capítulo de protección de la información y de los datos. (Acuña-Gamba, y otros, 2017)

4.1.2 Ley 1581 de 2021:

Esta ley se aplica a los datos personales que se registren en bases de datos o archivos de entidades públicas o privadas. Regula la recolección, almacenamiento, uso, circulación o supresión de datos personales registrados en dichos medios digitales, electrónicos o telemáticos. (Comercio, 2016)

4.2 MARCO CONCEPTUAL CIBERSEGURIDAD: PRUEBAS DE PENETRACIÓN (PENTESTING)

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

El pentesting es la fusión de dos palabras del inglés: “penetration” y “testing”, las pruebas de penetración son una técnica o práctica consistente en generar de manera controlada ataques a ambientes o sistemas con la finalidad de encontrar y prevenir de amenazas que pudiesen materializarse, convirtiendo así en riesgo informático. (Romero, y otros, 2019)

4.2.1 Etapas del proceso de pentesting (Romero, y otros, 2019)

4.2.1.1 Descubrimiento y Enumeración

Consisten en determinar la auditoría, el pen tester evaluará la información con que cuenta y que tipo de pen testing realizará. Eleven Paths FOCA es una herramienta para la búsqueda de metadatos e información oculta en documentos.

4.2.1.2 Análisis de vulnerabilidades

Consiste en la recogida de información, mediante pruebas para determinar vulnerabilidades o fuga de información. Utilizará varias herramientas y valorará aspectos claves del entorno y los comportamientos de los usuarios. NMAP es una herramienta que permite realizar exploración y búsqueda de vulnerabilidades.

4.2.1.3 Explotación

Consiste en el acceso al sistema, después de recolectar la información y de tener el plan de cómo se deberá actuar se organizan los ataques y se mantiene el acceso al objetivo del ataque. Metasploit Framework permite realizar pruebas de penetración y una extensa auditoría de seguridad.

4.2.1.4 Informe

La elaboración del informe presenta el alcance, el impacto de los fallos de seguridad atacados con las recomendaciones para minimizar o suprimir estas vulnerabilidades.

4.2.2 Herramientas De Ciberseguridad

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

4.2.2.1 Herramientas

- Metasploit: Es una herramienta como resultado de un proyecto de código abierto para la seguridad informática. Permite obtener información de vulnerabilidades y permite realizas pruebas de penetración.

- Nmap: Es una herramienta para rastreo de puertos para descubrir servicios o servidores, su operación consiste en el envío de paquetes definidos y analiza las respuestas a los mismos.

- OpenVAS: Es una herramienta que permite el escaneo de vulnerabilidades. (Seguridad en la Red: escáner de vulnerabilidades OpenVAS, 2012)

4.2.2.2 Servicios En Línea

- Exploit DB: Es un archivo de exploits con fines de seguridad pública, permite identificar vulnerabilidades en su red de datos.

- CVE (Vulnerabilidades y Exposiciones Comunes): Es un diccionario con el propósito de propiciar la distribución de datos en bases de datos de vulnerabilidades y herramientas de seguridad informática.

5. METODOLOGIA

La metodología empleada en este proyecto de grado se basa en la realización de un conjunto de escenarios prácticos que permitan la realización de cada uno de los objetivos trazados.

Se realizará un proceso documental con el fin de planificar estrategias basadas en metodologías de ciberseguridad defensivas y ofensivas, que permitan hacer frente a un evento o incidente informático en una infraestructura TI, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

El trabajo se fundamentará en la recopilación de información, experiencias, criterios y normativas nacionales e internacionales que permitan conocer los avances obtenidos, hasta ahora, referentes a capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team.

6. ESCENARIO 1 BANCO DE TRABAJO

Este resumen muestra el reconocimiento, análisis y configuración del “banco de trabajo” Escenario 1 sobre el cual se trabajarán actividades que contienen un alto grado de tecnicidad.

6.1 HERRAMIENTA DE VIRTUALIZACIÓN “VIRTUALBOX”

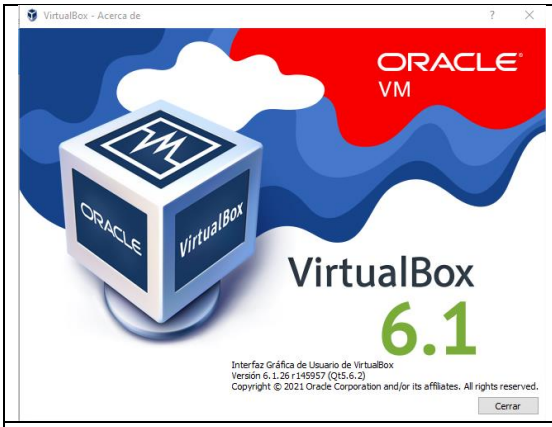
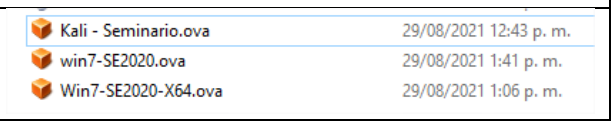
	Se realiza instalación de la herramienta de virtualización Oracle VM VirtualBox en su versión 6.1 en entorno Windows 10 x64.
Se descargan de la carpeta compartida en línea los OVA para importación de máquinas virtuales.	

Tabla 1 VirtualBox - Entorno de Virtualización

6.2 COMUNICACIÓN ETHERNET MV KALI LINUX Y MVs WINDOWS DEL ESCENARIO

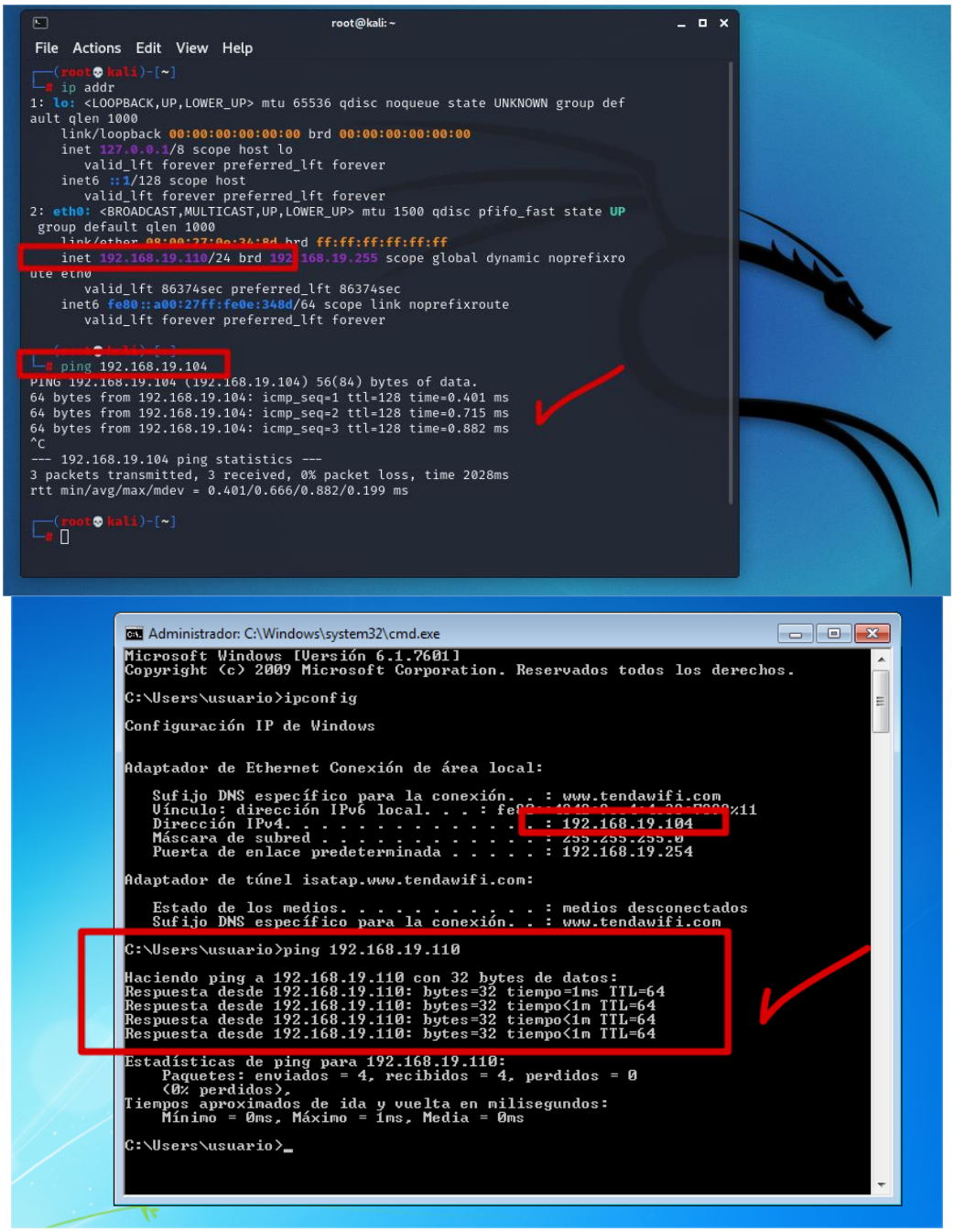


Figura 1 Comunicación entre equipos de la simulación

Se configuro la red para tener ping entre los equipos del Escenario 1.

Kali Linux Recibe IP de red local 192.168.19.104/24 ping exitoso a equipo Windows 7 SE2020-X64 192.168.19.104/24 y desde el equipo Win7 SE2020-X64 hacia Kali Linux.

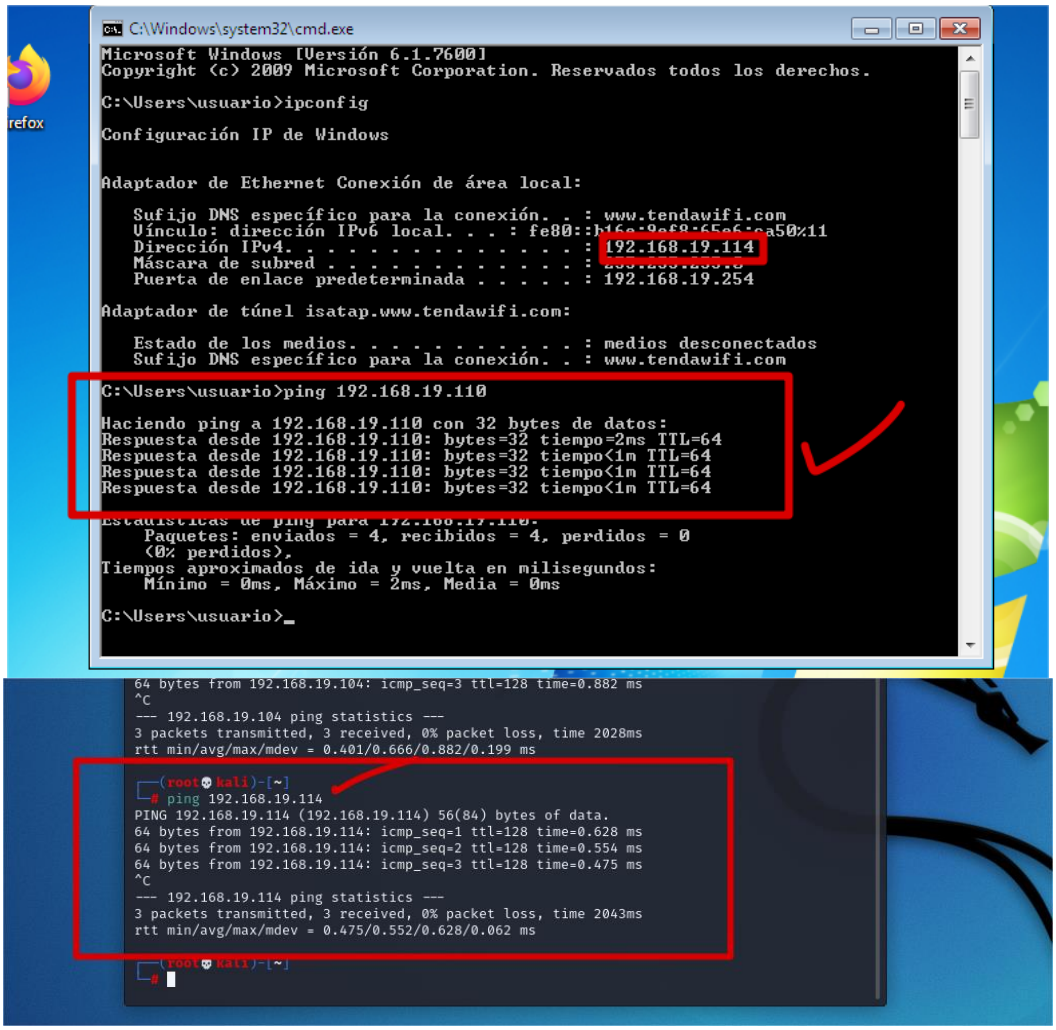


Figura 2 Comunicación entre equipos de la simulación

Se igual manera se tiene comunicación bidireccional entre Kali Linux y la máquina virtual de Windows-7 x86, con IP 192.168.19.114

6.3 HARDWARE DE LOS EQUIPOS VIRTUALES DEL ESCENARIO 1

6.3.1 Kali Linux

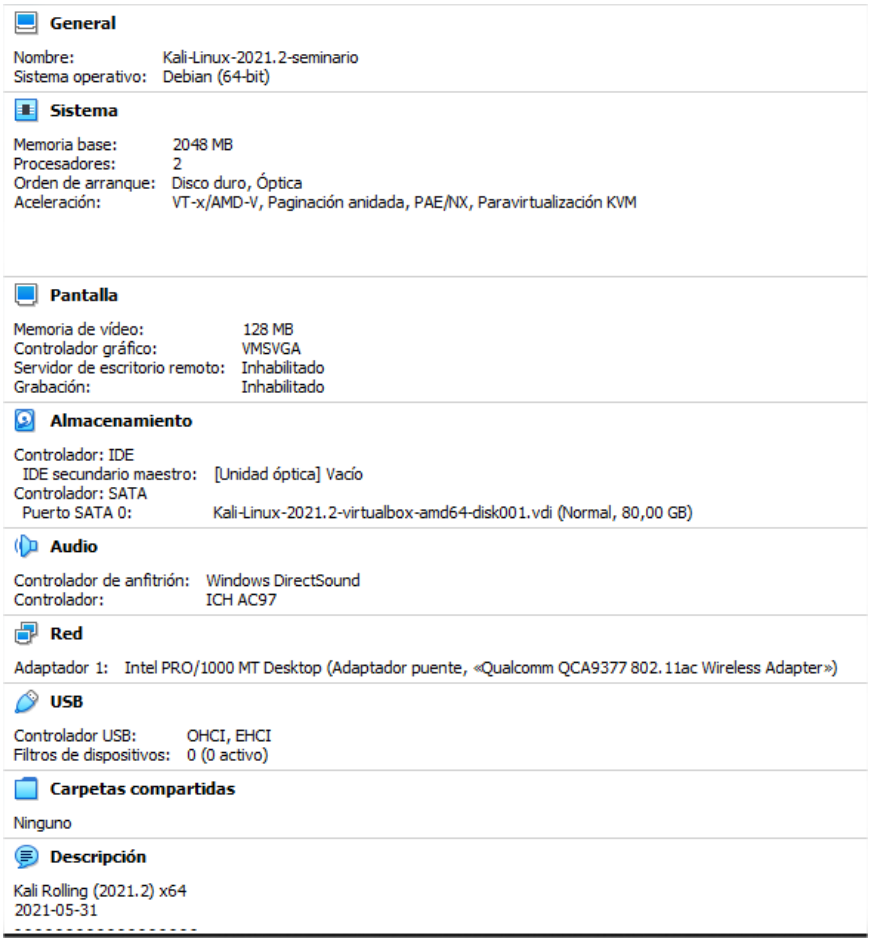


Figura 3 Hardware Equipo KaliLinux

6.3.2 Windows 7 X86

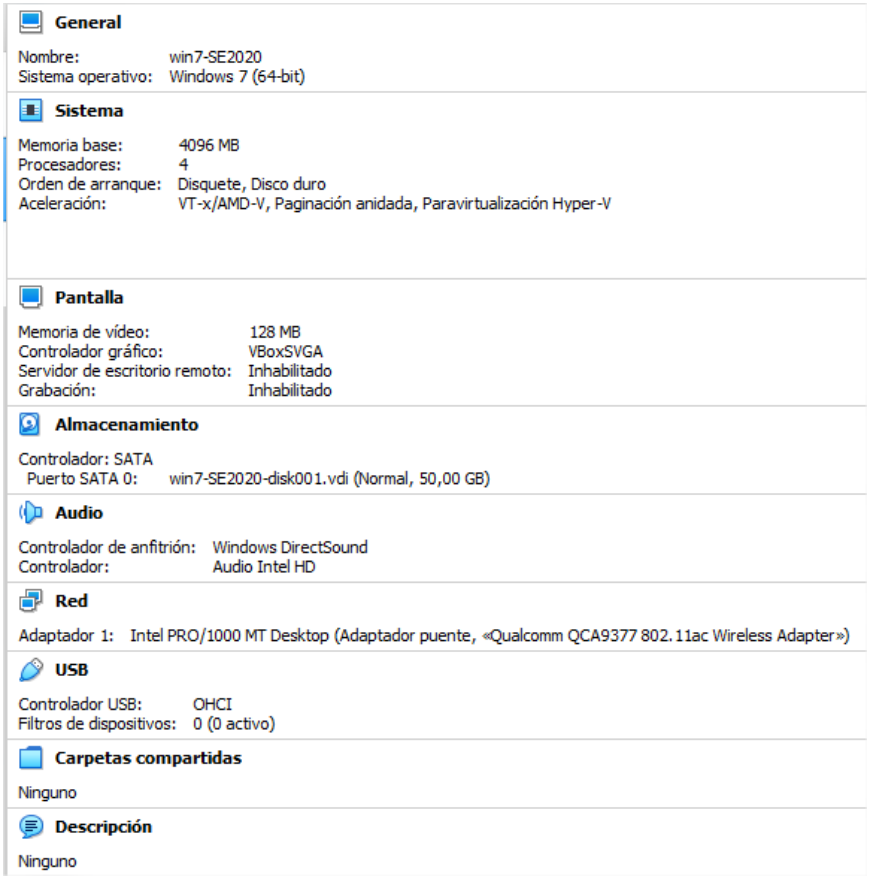


Figura 4 Hardware Equipo 32 Bits

6.3.3 Windows 7 X64

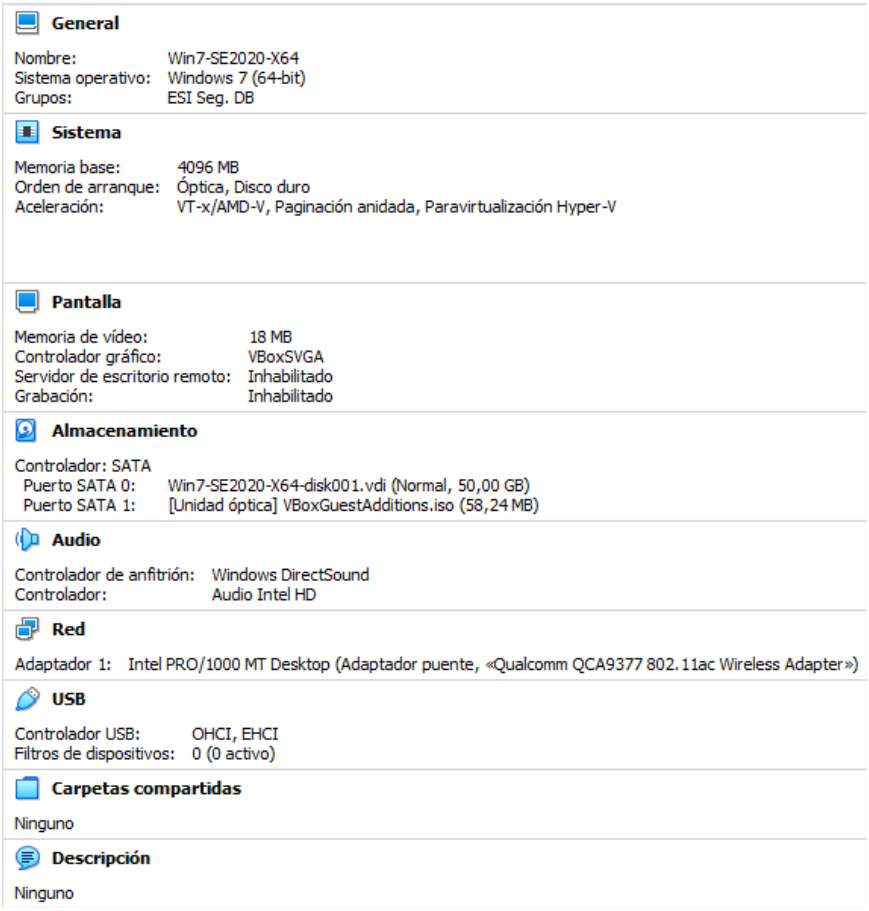


Figura 5 Hardware Equipo 64 bits

7. PROCESO ILEGAL Y NO ÉTICO ACUERDO WHITEHOUSE SECURITY - CANDIDATO

7.1 ANÁLISIS DOCUMENTAL: ACUERDO Y SITUACIÓN DEL PROBLEMA

Después de analizar el documento anexo 2, situación del problema: Análisis Legal. Se tienen los siguientes elementos como soporte evidencia de la existencia de proceso ilegal o falta a la ética profesional:

- ✓ El contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. (ECBTI Escuela de Ciencias Básicas, 2020)

- ✓ La alta gerencia no reviso los contratos con los que reclutará el nuevo personal. (ECBTI Escuela de Ciencias Básicas, 2020)

Teniendo en cuenta las anteriores afirmaciones se debe tener presenté que el proceso inicia con vacíos legales y un antecedente de despido de un abogado que por evidenciar procesos ilícitos fue despedido.

Adicionalmente, la revisión del Acuerdo de Confidencial complementa la evidencia de proceso ilegal o falta a la ética profesional:

- Adicional a la información confidencial, la parte receptora, se obliga a no divulgar sobre procesos ilegales dentro de Whitehouse Security. (ECTBI Escuela de Ciencias Básicas, 2020)
- Definen información confidencial como datos secretos “datos de chuzadas”, interceptación de información, accesos abusivos a sistemas informáticos. (ECTBI Escuela de Ciencias Básicas, 2020)
- El origen de la información confidencial puede provenir de fuentes no confiables o sin soporte y sin que requiera advertir su carácter confidencial. (ECTBI Escuela de Ciencias Básicas, 2020)
- Se obliga a la parte receptora a no denunciar antes las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros, adicional, denunciar y publicar la información confidencial e ilegal. (ECTBI Escuela de Ciencias Básicas, 2020)

- La parte receptora deberá responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento, acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. (ECTBI Escuela de Ciencias Básicas, 2020)

Este acuerdo reafirma procesos ilegales al interior de la organización y habla de cómo la información confidencial se genera violando las leyes vigentes y adicional compromete al contratista como responsable en caso de ser allanado o judicializado, sin apoyo legal a la defensa y obligando a dejar exente a la organización de responsabilidad legal y penal.

7.2 VIOLACIÓN A LA LEY 1273 DE 2009 EN EL ACUERDO WHITEHOUSE SECURITY

(Acuña-Gamba, et al., 2017)

7.2.1 Artículo 269C: Interceptación de datos informáticos.

El acuerdo define información confidencial como datos secretos “datos de chuzadas”, interceptación de información, accesos abusivos a sistemas informáticos. (ECTBI Escuela de Ciencias Básicas, 2020)

7.2.2 Artículos 269F: Violación de datos personales y artículo 269G: Suplantación de sitios web para capturar datos personales

El origen de la información confidencial puede provenir de fuentes no confiables o sin soporte y sin que requiera advertir su carácter confidencial. (ECTBI Escuela de Ciencias Básicas, 2020)

7.3 COMO EXPERTO APLICARÍA A EL TRABAJO EN THE WHITEHOUSE

Teniendo en cuenta el análisis donde se evidencia ilegalidad y el acuerdo es directo y responsabiliza de los actos al colaborador, NO aceptaría este empleo, ya que la ética profesional en este tipo de actividades es primordial, y el solo hecho de estar bien pago, no garantiza que a futuro tengas que ser juzgado legal y penalmente por obligaciones de la organización que te contrate e inclusive perder la tarjeta profesional y, por lo tanto, el no ser contratado nuevamente.

8. OPERACIÓN ANDROMEDA BUGGLY
(ENTER.CO, 2015)

El ejército colombiano llevo a cabo esta operación de inteligencia, con el propósito de reclutar hackers civiles, y obtener de ellos transferencia de conocimientos y entender cómo aplicar técnicas de hacking ético, pero en el fondo se fue convirtiendo en dominios de información confidencial que, a su vez, por el grado de importancia de esta, fueron influenciados y pasar de ético a ilegal con fines de enriquecimiento.

Iniciaron realizando interceptación de computadoras, móviles y bases de datos del ejercito que después fueron comercializadas con fines no determinados.

Este escenario, pone en vilo la labor del hacking ético, ya que la riqueza de la información puede ocasionar que todos los principios éticos sean abandonados y transformados en un hacker que viola las leyes con el propósito de obtener provecho de los recursos de información que pueda capturar.

De allí, importante reflexionar esta labor que, si bien es muy importante para poner en evidencias las vulnerabilidades de nuestros sistemas informáticos, se debe llevar a cabo con mucha responsabilidad, con conocimiento del marco legal y con principios éticos de la profesión como los emanados por el COPNIA para los ingenieros en Colombia.

9. INFORME DE HERRAMIENTAS Y PROCEDIMIENTOS

9.1 DESCUBRIMIENTO Y ENUMERACIÓN

Se reporta una serie de fuga de información dentro de una organización, se ha identificado uno de los equipos en red de una dependencia como posible sospechoso de permitir la fuga de información a través de una aplicación instalada denominada Rejetto HFS 2.3, la cual tiene vulnerabilidades reportadas conocidas y la cual tiene asociado Esploit que pueden terminar en la apertura de una consola reversa con sesión abierta desde meterpreter.

En esta investigación adicional a la fuga de información se tiene un escalamiento por privilegios de usuario, la cual, se derivó de la creación de un usuario administrador del sistema operativo.

El equipo forense genera una copia del servidor, con la cual se emula este escenario, ver ilustración 1., y se tiene como objetivo validar la falla de seguridad y si está explotada se deberá crear un usuario con su primer nombre y apellido, el usuario deberá ser de tipo administrador, para así poner en evidencia mediante una PoC los resultados, a la dirección de la compañía.

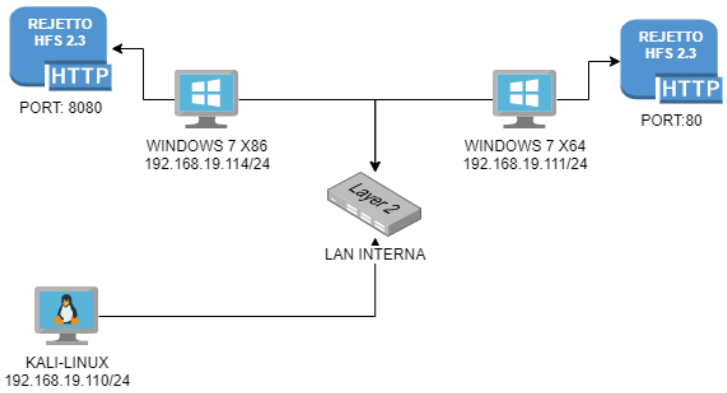


Figura 6 Infraestructura Escenario 3

9.1.1 Equipos En Ambiente Emulado

9.1.1.1 Servidor Entregado En Custodia Por El Equipo Forense

Recurso Virtual:	Win-7SE2020-X64	
Hw/Sw	Capacidad	Observaciones
CPU	1X 2.4Ghz	
RAM	1X 4Gb	
HDD	1X 50Gb	
SO	Windows 7	64 bits

Tabla 2 Servidor Sospechoso

9.1.1.2 Equipo Auditoría Para Pruebas de Penetración

Recurso Virtual:	Kali-Linux-2021.2-seminario	
Hw/Sw	Capacidad	Observaciones
CPU	1X 2.4Ghz	
RAM	1X 2Gb	
HDD	1X 80Gb	
SO	Debian64	Kali-Linux2021

Tabla 3 Equipo Auditoría Debian64

9.1.1.3 Servidor Pruebas 32 Bits

Recurso Virtual:	Win-7SE2020	
Hw/Sw	Capacidad	Observaciones
CPU	1X 2.4Ghz	
RAM	1X 4Gb	
HDD	1X 50Gb	
SO	Windows 7	32 bits

Tabla 4 Equipo Pruebas Windows 7 32 Bits

9.2 ANÁLISIS DE VULNERABILIDADES

9.2.1 Firewall de Windows y Windows Defender

Se tiene como primer hallazgo el estado inactivo del Firewall de Windows y la herramienta Windows Defender, adicionalmente no se cuenta con otra herramienta antivirus o antimalware que supla estas funcionalidades.

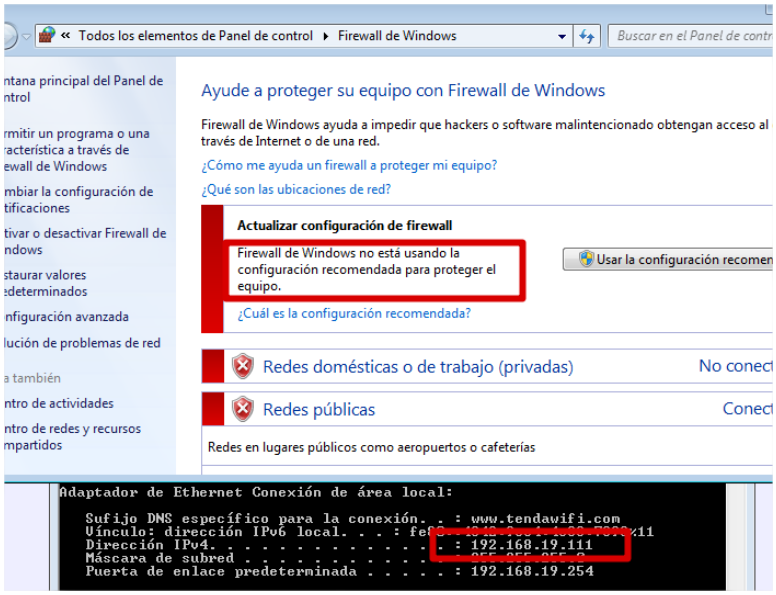


Figura 7 Firewall Windows Inactivo

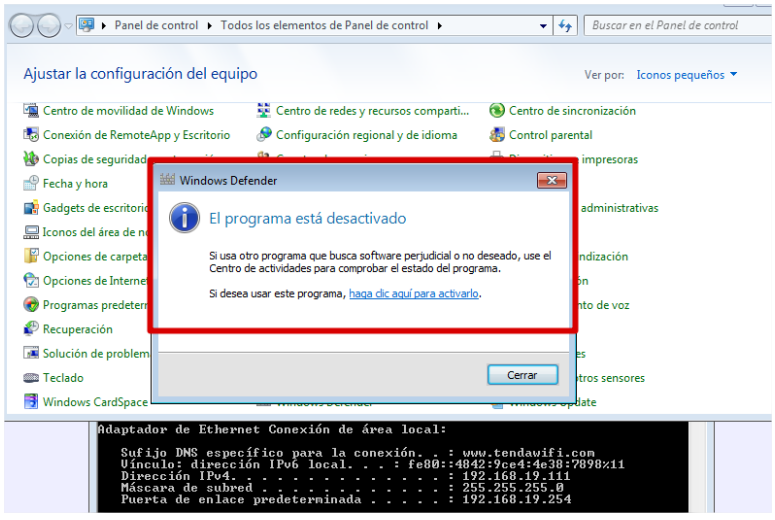


Figura 8 Windows Defender Inactivo

9.2.2 Aplicación HFS 2.3 Rejetto

En la carpeta descargas del usuario del equipo se encuentra el ejecutable de la aplicación Rejetto HFS 2.3, se ejecuta y mediante el uso de un navegador de internet se tiene acceso a ella por url, localhost, puerto http 80.

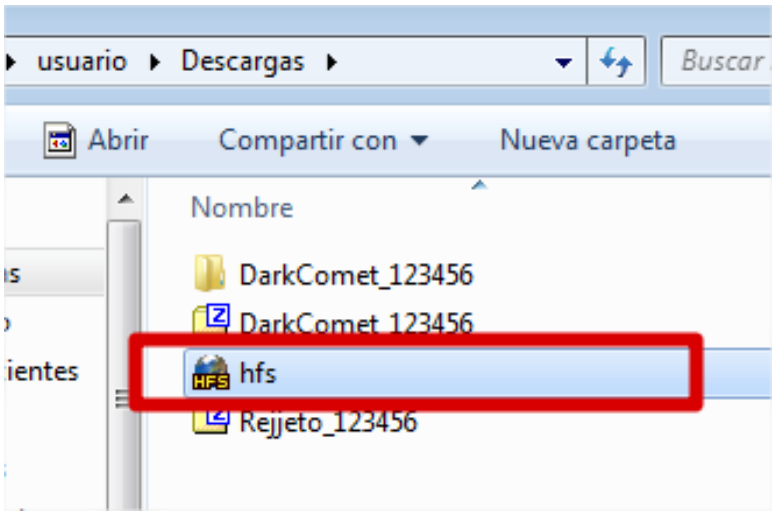


Figura 9 Carpeta Descargas de Usuario

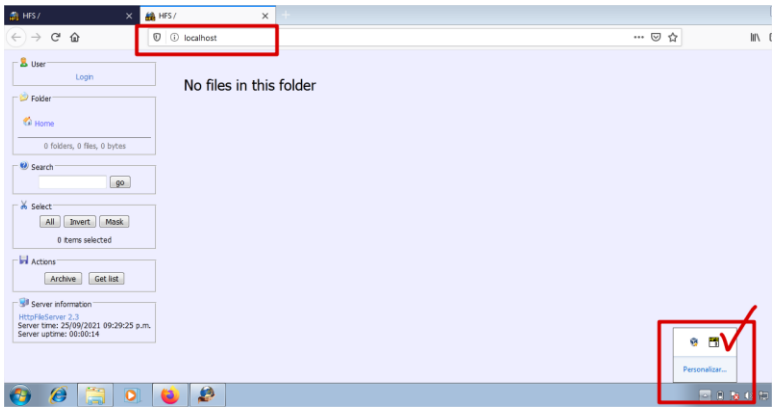


Figura 10 HFS 2.3 Servicio Activo

9.2.3 Exploración y Búsqueda de Vulnerabilidades NMAP

En primera instancia se procede a validar comunicación bidireccional a nivel de red, mediante el uso del comando ping.

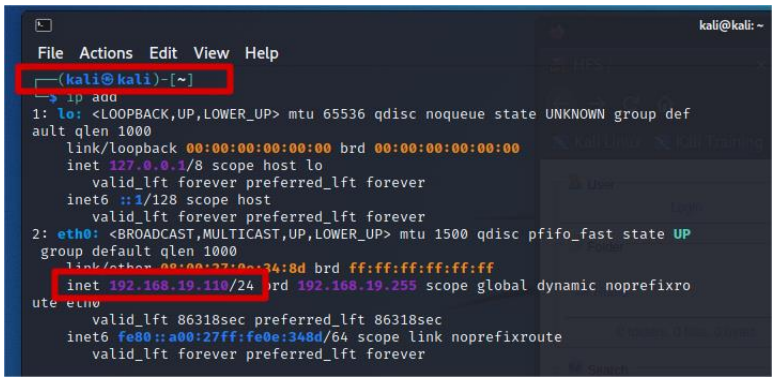


Figura 11 Configuración TCP/IP MV Kali Linux

Una vez en red, se realiza ping a la maquina servidor de Windows 7 64 bits.

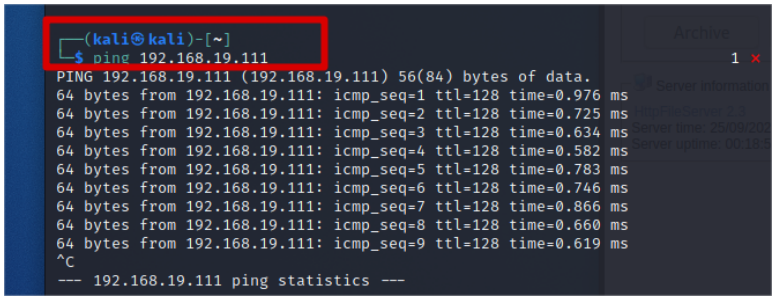


Figura 12 Resultado Ping a Servidor W7

Ya con pruebas de comunicación correctas, se procede a ejecutar la exploración y detección de vulnerabilidades para lo cual se usa Nmap y se tienen los puertos de servicio a la escucha en este servidor. En la ilustración 8, se puede apreciar el puerto http/80, abierto con un servicio HttpFileServer HTTP 2.3 con una cabecera de HFS en versión 2.3.

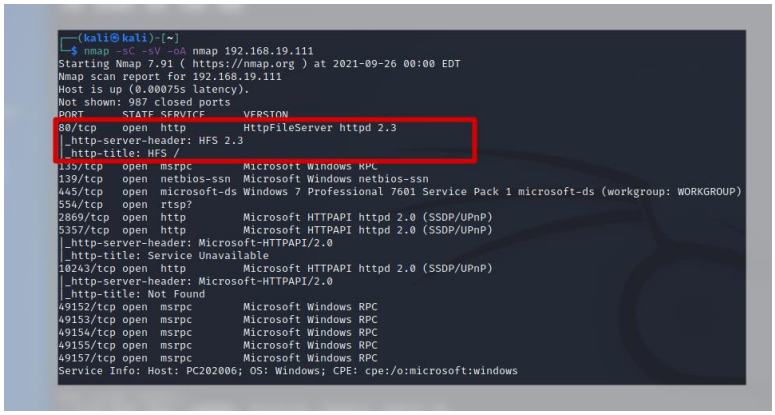


Figura 13 Resultado de Escaneo con Nmap

Atendiendo el alcance de la investigación y habiendo encontrado el servicio a la escucha se procede a buscar vulnerabilidades y la existencia de algún Esploit para materializar la penetración al sistema.

Se identifica por la corporación MITRE, la CVE-2014-6287, registro en base de datos nacional de vulnerabilidades, la cual describe que la función de búsqueda findMacroMarker en Rejetto HTTP File Server 2.3x permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia de acción de búsqueda. (MITRE Corporation, 2021)

9.3 EXPLOTACIÓN DE VULNERABILIDAD

Mediante la selecta agrupación de herramientas para la seguridad que ofrece la distribución GNU Linux Debian 64, Kali Linux. Usaremos Metasploit y se buscara si se tiene un Esploit para HFS 2.3, dado que ya se investigó y encontró la existencia de una vulnerabilidad para esta versión del servicio.

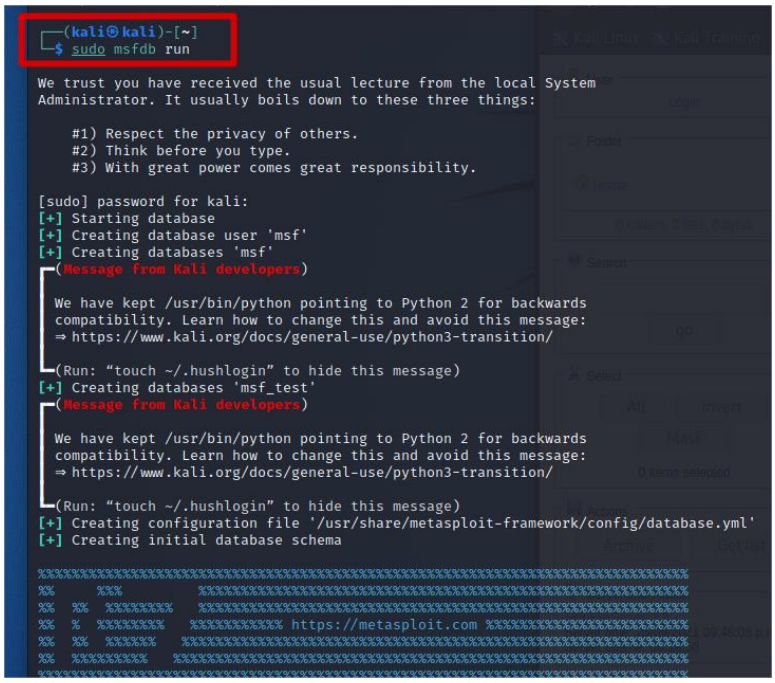


Figura 14 Ejecución de Metasploit en Kali Linux

Una vez se ingresa a la recopilación de Metasploit en la máquina virtual de Kali Linux, se hace uso del comando de búsqueda para HFS 2.3, se tienen los siguientes resultados: ver ilustración 10.

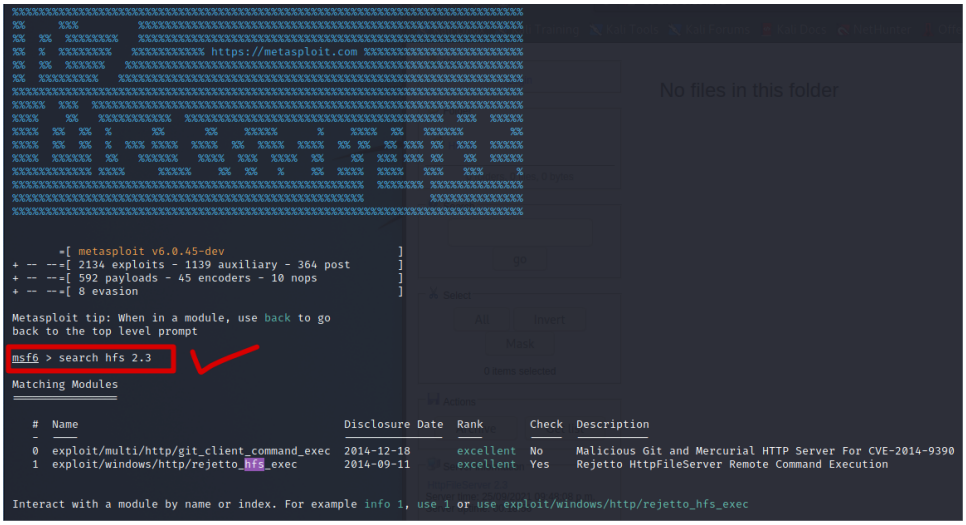


Figura 15 Búsqueda de Esploit para Rejetto HFS 2.3

9.3.1 Exploit Windows HTTP Rejetto HFS

Una vez la búsqueda en Metasploit versión 6, da como resultado una herramienta para explotar la vulnerabilidad en Windows para HTTP Rejetto HFS 2.3. Se ejecuta comando de uso y muestra de opciones para su ejecución.

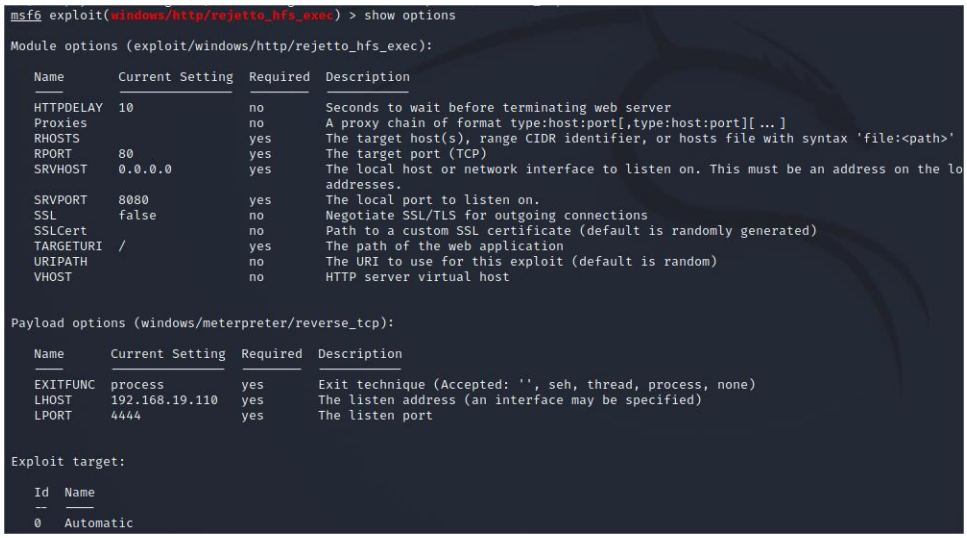


Figura 16 Uso y Opciones de Esploit Rejetto

Los comandos: 1) set rhost 192.168.19.111 (Equipo a atacar), 2) set lhost 192.168.19.100 Equipo atacante y 3) run, corre el script.

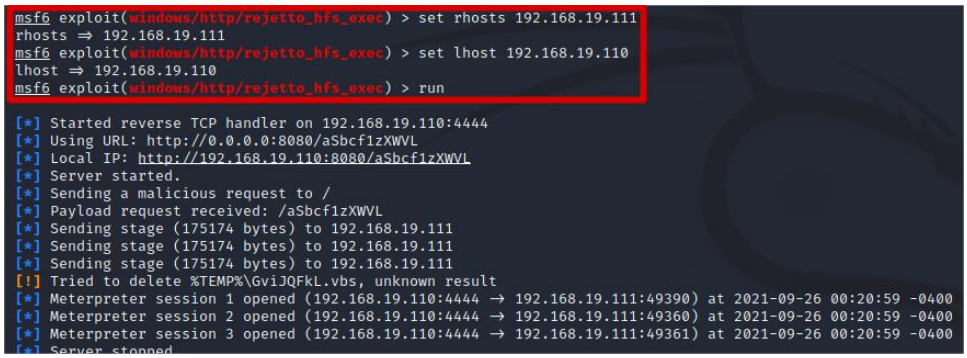


Figura 17 Correr Script de Explotación Inicial

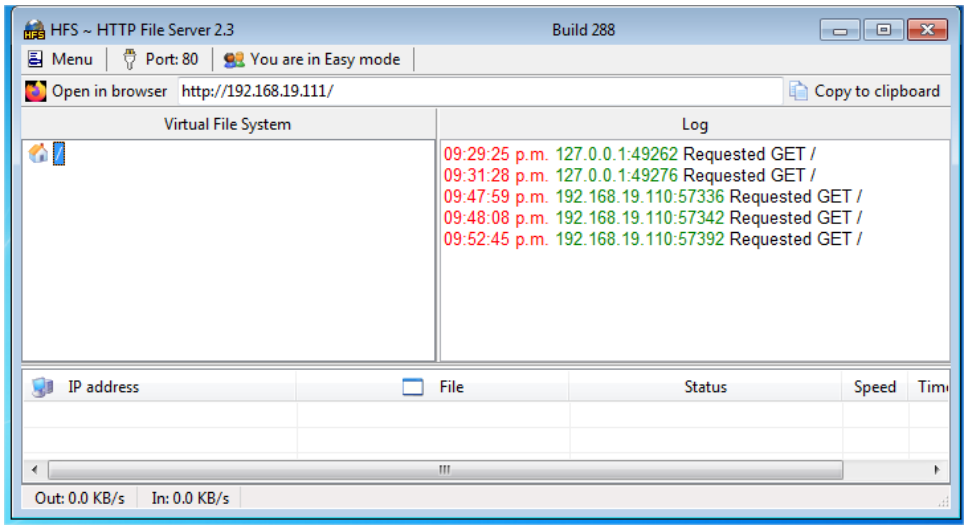


Figura 18 Consola de Servicio HFS en Equipo Servidor

Ya con acceso a comandos desde meterpreter, identificamos la cuenta de usuario en la maquina Windows 7 y el número de sesión y con el comando de búsqueda preguntamos por un módulo sugerido.

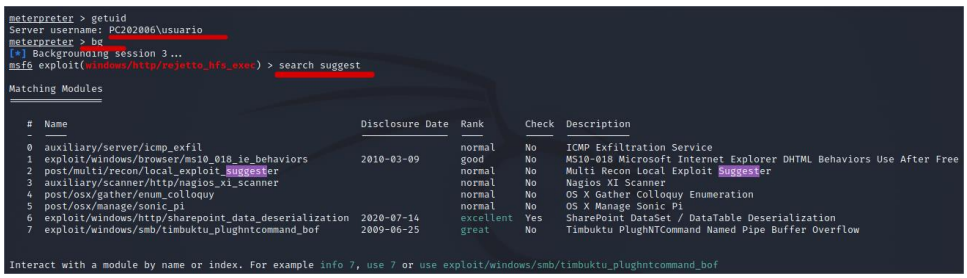


Figura 19 Módulo Sugerido Rejetto HFS EXEC Esploit Windows

9.3.1.1 Modulo Local Esploit Suggester

Se selecciona el uso del módulo multi/recon/local_exploit_suggester y se visualizan las opciones para su ejecución.

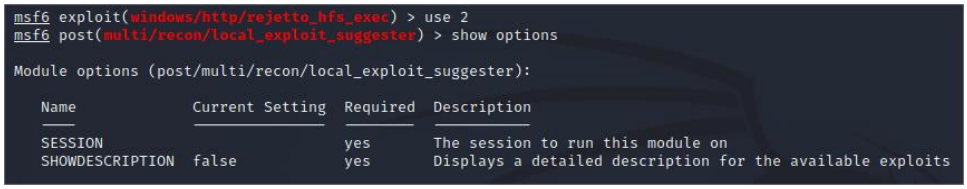


Figura 20 Módulo Sugerido Para Explotar Vulnerabilidad

Con los comandos: 1) set session 3, acorde al comando bg en paso anterior, 2) run, corremos el módulo.

Esto nos entregará como resultados los objetivos para atacar la vulnerabilidad en el equipo Servidor.

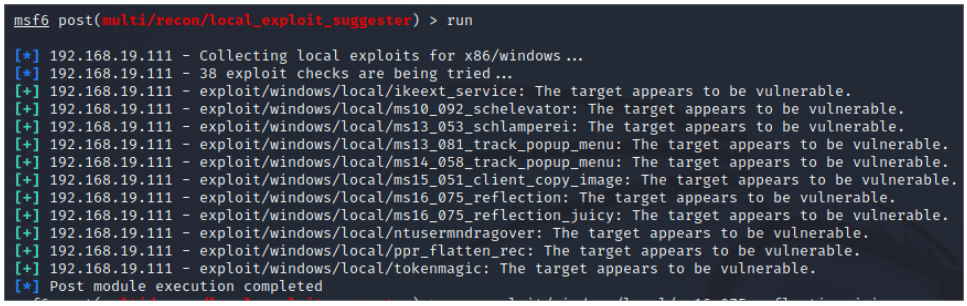


Figura 21 Puntos Objetivos para atacar la vulnerabilidad

Se toma uno de los puntos objetivo y se visualiza las opciones para ejecución:

- *windows/local/ms16_075_reflection_juicy*
  Se realiza proceso de ejecución del Esploit se completa, pero no es capaz de crear la sesión de consola reversa en el equipo servidor Windows 7 64 bits.

- *exploit/windows/local/tokenmagic*
  Se realiza proceso de ejecución del Exploit se completa, pero no es capaz de crear la sesión de consola reversa en el equipo servidor Windows 7 64 bits, a pesar de tener un mensaje de disfrutar el Shell, no fue posible.

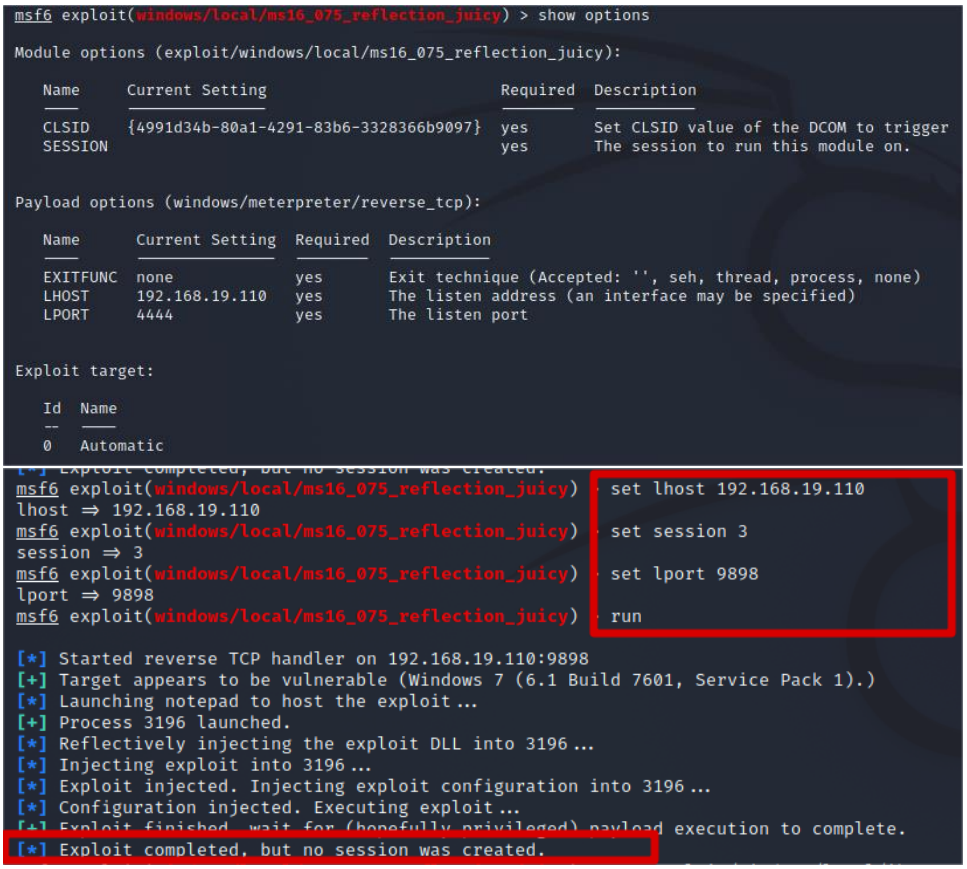


Figura 22 windows/local/ms16_075_reflection_juicy

- *windows/local/ppr_flatten_rec*
  Este tercer objetivo una vez mas no obtiene el resultado esperado, ya que no es compatible con sistemas de 64 bits.

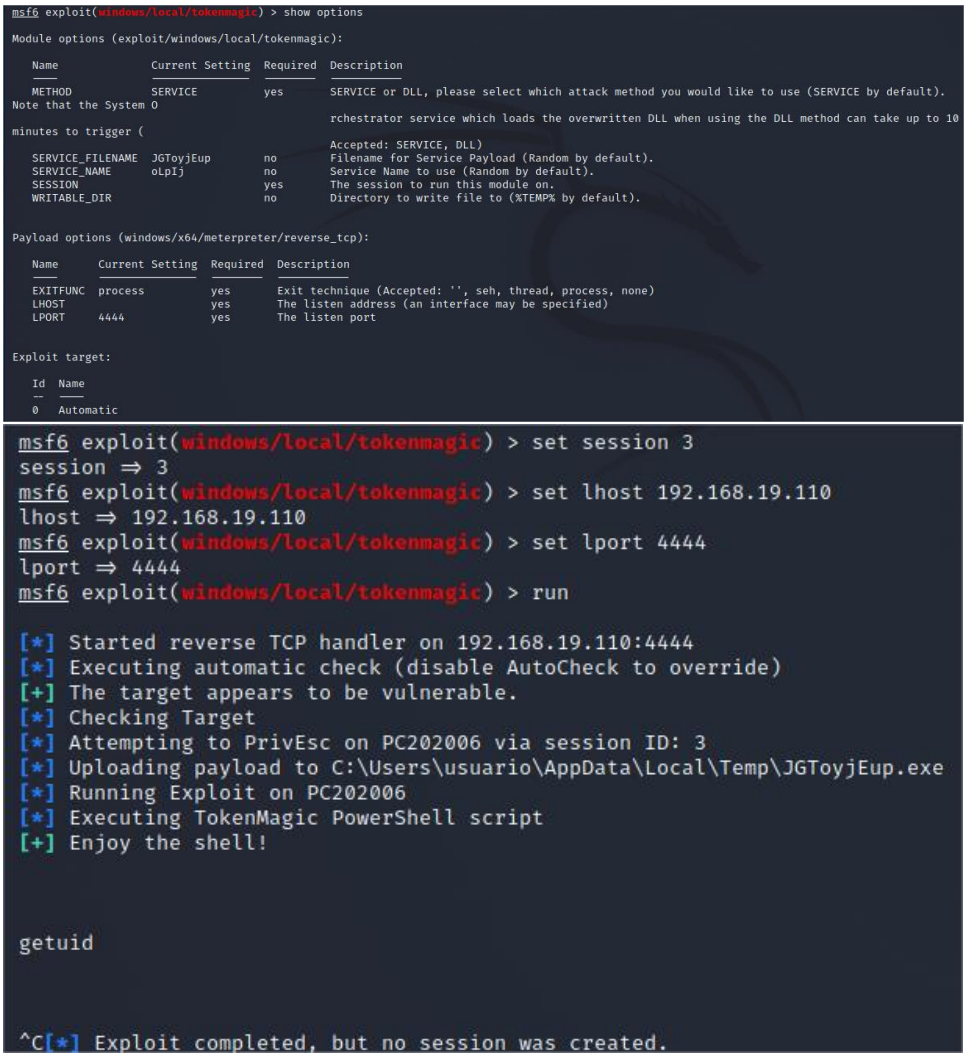


Figura 23 windows/local/ppr_flatten_rec

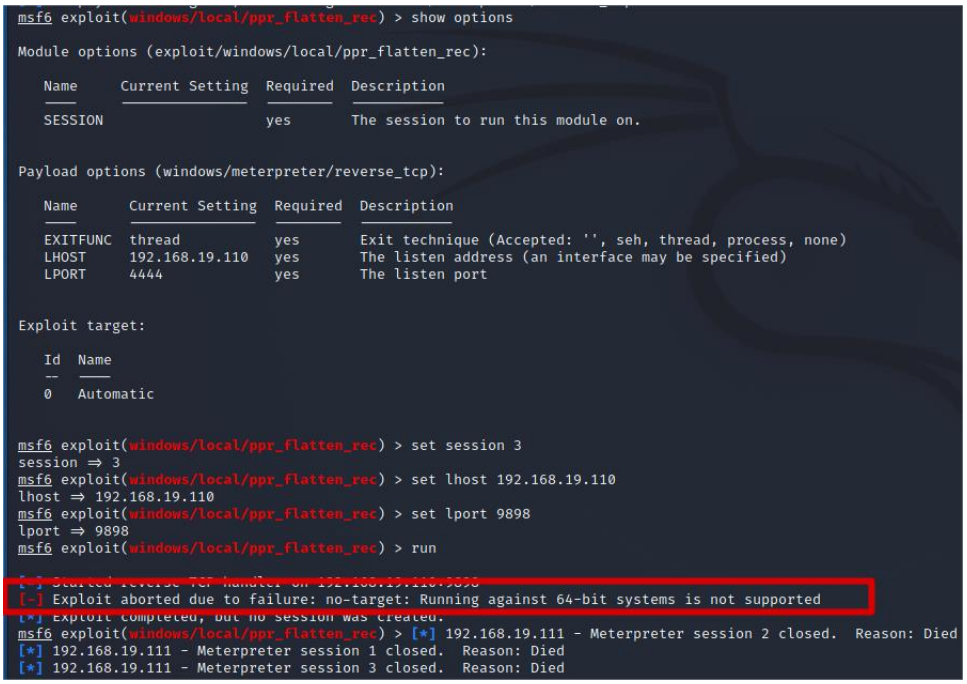


Figura 24 windows/local/ppr_flatten_rec

9.4 RESULTADOS DE PRUEBAS DE PENETRACIÓN

- Se realizo proceso de investigación, y se encontró vulnerabilidad para HFS 2.3 Rejetto, en sistema operativo Windows 7 64 bits. CVE-2014-6287. (MITRE Corporation, 2021)

- Se busco exploit para explotar dicha vulnerabilidad, sin éxito, a pesar de que la vulnerabilidad existe y esta comprobaba mediante el escaneo de Nmap. No fue posible explotar y obtener consola reversa.

- Por lo tanto, se concluye que la fuga de información puede estar ligada a esta vulnerabilidad, pero desde un servidor de 32 bits, ya que se hizo el mismo procedimiento en una maquina Windows 32 bits y se logró apertura de consola reversa y a su vez crear un usuario como administrador local. Ver Anexo A. (Explotación de vulnerabilidad para Rejetto HFS 2.3 en Windows 7 32 bits.)

10. ATAQUE EN TIEMPO REAL

10.1 QUÉ HACER ANTE UN INMINENTE ATAQUE EN TIEMPO REAL

Durante un ataque en tiempo real, en primera instancia es estar informado de los servicios que se tienen en DMZ, y estar expectante de que alguna solicitud a la mesa de ayuda o algún reporte de cliente o usuario final genere alerta de una posible denegación de servicio o ataque informático.

Normalmente ante un ataque en tiempo real evidenciaremos la caída de un servicio publicado, y al intentar volver a levantar puede ser difícil o casi imposible llevarlo a cabo.

En estos casos se deben conocer las rutas de logs de servicio e ingresar a ellos, una tarea difícil, ya que en ocasiones nos damos cuenta del ataque muy tarde y estos archivos por su peso no permiten leer los eventos sucedidos.

Si es este el caso, se encontrarán direcciones IP públicas de atacantes, para lo cual es importante poder automatizar la lectura del log, obteniendo el mayor número de direcciones IP y haciendo uso de script poder crear reglas de denegación o bloqueo en el firewall, esto con el propósito de lograr levantar nuevamente el servicio.

Una vez se tenga el servicio en línea nuevamente es crucial, investigar si no contamos con los parches actualizados del fabricante del software o si existe alguna vulnerabilidad explotada.

Proceder a actualizar y entrar en cuarentena al servicio, monitoreo de paquetes de red hacia el equipo, copias de seguridad con mayor regularidad y en cuanto se detecte una nueva incursión, validar la posibilidad de implementar en una nueva máquina desde cero el servicio, ya que muchas veces el daño es irreversible y los bots atacantes capturan nuevamente con mayor facilidad el servidor propio.

10.2 MEDIDAS PREVENTIVAS DE HARDENIZACIÓN

- Evitar la instalación de software no necesario para el correcto funcionamiento del o de los servicios.

- Diseñar tareas automáticas de ejecución de los comandos de actualización a nivel del sistema operativo, parches del servicio, etc. Con la periodicidad pertinente que garantice la actualización ante vulnerabilidades detectadas en el pasar del tiempo.

- Practica de envejecimiento de contraseñas, cambios obligatorios, niveles de complejidad altos, capacitación a los usuarios para no compartir, ni entregar a anónimos sus credenciales, bloqueo ante intentos fallidos de inicio de sesión.

- Realizar análisis de vulnerabilidades con herramientas como Nmap y consulta a las bases de datos globales de vulnerabilidades de los servicios en las versiones implementadas, para adelantarse ante una posible explotación de estas.

10.3 BLUE TEAM vs EQUIPO DE RESPUESTA ANTE INCIDENTES (it Digital Security, 2021)

BLUETEAM es un grupo multidisciplinar de índole investigativa que rastrean los ciber incidentes que se generan un sistema informático, a diferencia de un equipo de respuesta ante incidentes el cual normalmente no tiene un número suficiente de miembros, por lo cual, es más específico en lo técnico para así atender incidentes de ciberseguridad mediante herramientas preventivas, correctivas y procedimientos.

10.4 CIS – CENTER FOR INTERNET SECURITY

Si se tiene la posibilidad de trabajar con un centro para la seguridad en internet, se pueden tener varios usos para la investigación multidisciplinar de ciber incidentes (cisecurity, 2021):

- Protección mediante controles de ataques informáticos.

- Usos de software de marcas reconocidas contra las amenazas cibernéticas.

- Acceso a recursos para prevenir, proteger, rápida respuesta y recuperación ante las amenazas.

10.5 SIEM – SECURITY INFORMATION AND EVENT MANAGMENT

SIEM es una solución que provee la capacidad de detección, respuesta y neutralización de amenazas informáticas (nsit, 2021).

Esta solución, permite el control absoluto a nivel de seguridad informática de una compañía, garantizando una línea de tiempo corta segundo a segundo de los sucesos de un sistema informático.

Funcionalidades:

- Centralización de la información de seguridad.
- Automatización de tareas.
- Respuesta automática a eventos y amenazas.
- Disminución del tiempo de detección de ataques.
- Información rápida y eficiente para realizar análisis forense.
- Alertas de seguridades eficientes.
- Análisis y correlación de logs en tiempo real.
- Seguimiento de eventos.
- Mejor manejo del riesgo.
- Manejo de métricas de seguridad.
- Detección de activos.
- Evaluación de vulnerabilidades.
- Detección de violaciones de seguridad.
- Monitoreo de comportamiento.

10.6 CONTENCIÓN DE ATAQUES INFORMÁTICOS

Herramientas para contener un ataque informático:

- Reglas de Firewall
- IDS (Sistemas de Detección de Intrusos)
- Antivirus

CONCLUSIONES

El marco legal colombiano carece de buenas herramientas para evaluar las conductas antes penetración de sistemas de información, sin embargo, existen leyes vigentes que soportan los procesos de ético hacking, y es fundamental en conjunto con las conductas éticas de la profesión, llevar a cabo los procesos de pruebas de penetración ajustados a esta normativa.

Los equipos Blue Team y Red Team, se deben justificar desde la necesidad de la seguridad informática. Es importante que estas técnicas permitan poner en videncia las vulnerabilidades antes de que se materialicen y posterior a ello, generar investigación forense.

RECOMENDACION

Los miembros de infraestructura TI de las organizaciones dedicados a la seguridad informática, deben lograr llegar hacia los altos mandos, logrando llevar a cabo, capacitación sobre la importancia del Etical Hacking y la implementación de pruebas de penetración a través de los equipos Blue Team y Red Team.

BIBLIOGRAFÍA

Ridge Marketing. 2021. El pasado, el presente y el futuro de las pruebas de penetración. El pasado, el presente y el futuro de las pruebas de penetración. [En línea] 08 de 10 de 2021. https://ridgesecurity.ai/es/blog/el-pasado-el-presente-y-el-futuro-de-las-pruebas-de-penetracion/.

Acuña-Gamba, Eduardo José y Sotelo-Vargas, Diego Andres. 2017. LEY 1273 DE 2009: ¿LOS JUECES DEL CIBERCRIMEN? [En línea] 2017. [Citado el: 29 de 8 de 2021.] http://revistas.ustatunja.edu.co/index.php/iaveritatem/article/view/1339.

cisecurity. 2021. Making the Connected World a Safer Place. Making the Connected World a Safer Place. [En línea] 04 de 10 de 2021. https://www.cisecurity.org/.

Comercio, Superintendencia de Industria y. 2016. Ámbito de aplicación de la Ley 1581 de 2012. [En línea] 2016. [Citado el: 29 de 8 de 2021.] https://bibliotecadigital.ccb.org.co/handle/11520/14472.

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2020. Anexo 2 - Escenario 2. [aut. libro] Universidad Nacional ABierta y a Distancia UNAD. 2020, pág. 1.

ECTBI Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2020. Anexo 3 - Acuerdo. [aut. libro] Universidad Nacional Abierta y A Distancia UNAD. 2020, pág. 6.

ENTER.CO. 2015. Detrás de Buggly: la historia de la fachada Andrómeda. [En línea] 09 de 12 de 2015. https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/.

it Digital Security. 2021. ¿Qué es un Blue Team y cómo trabaja? ¿Qué es un Blue Team y cómo trabaja? [En línea] 04 de 10 de 2021. https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

MITRE Corporation. 2021. National Vulnerability Database (NVD). National Vulnerability Database (NVD). [En línea] 24 de 09 de 2021. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287.

nsit. 2021. ¿Qué es SIEM en seguridad informática? Alcance e implementación. ¿Qué es SIEM en seguridad informática? Alcance e implementación. [En línea] 04 de 10 de 2021. https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

Romero, Vanegas y Yucenid, Alfonso. 2019. Pentesting, ¿porque es importante para las empresas? [En línea] 2019. [Citado el: 29 de 8 de 2021.] http://repository.unipiloto.edu.co/handle/20.500.12277/6286.

Seguridad en la Red: escáner de vulnerabilidades OpenVAS. Drilling, Thomas. 2012. 88, 2012, Linux magazine, págs. 28-33.

ANEXO A URL VIDEO SUSTENTACIÓN

https://youtu.be/JLOA4w6hhWI