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

Javier Pérez Zamudio

Universidad Nacional Abierta y a Distancia
Especialidad en Seguridad Informática
Bogotá, Colombia
2022

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

Javier Pérez Zamudio

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team:

Director de curso:

M.Sc. John F. Quintero

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

Universidad Nacional Abierta y a Distancia
Especialidad en Seguridad Informática
Bogotá, Colombia
2022

Resumen

Se platea realizar la etapa final del seminario de investigación de los equipos RedTeam y BlueTeam, finalizamos despues de un largo camino recorrido entre los diferentes planteamientos como lo son la parte legal, explorar mediante un laboratorio el funcionamiento de RedTeam y finalmente tambien por medio de un laboratorio el funcionamiento de BlueTeam.

Palabras clave: Red Team, Blue Team.

Abstract

It is planned to carry out the final stage of the research seminar of the RedTeam and BlueTeam teams, we finish after a long journey between the different approaches such as the legal part, exploring the operation of RedTeam through a laboratory and finally also through a laboratory the operation of BlueTeam.

Keywords: Red Team, Blue Team.

Índice

Contenido

1. Glosario

BlueTeam: Equipo de seguridad que está destinado a contener ataques de seguridad, por lo generar usan herramientas de monitoreo.

Escaneo de vulnerabilidades: se realiza con software especializado cuyo objetivo es detectar vulnerabilidades en el sistema.

Firewall: como su nombre lo indica es una pared que bloquea puertos abiertos en los sistemas y solo permite tráfico determinado.

Pilar: Soporte o base fundamental que se rige un sistema o proceso.

RedTeam: Equipo de seguridad enfocado en realizar pruebas de penetración a la organización con lineamientos y alcances definidos.

SO: Sistema operativo.

Puerto: es una interfaz virtual por la cual se envían y reviven paquetes informáticos.

2. Introducción

El tema para tratar en este trabajo es concluir con el seminario de investigación de RedTeam y BlueTeam, esta conclusión se da después de recorrer un camino, un camino que realizamos desde diferentes aspectos el primer aspecto temas legales leyes que se involucran para estos equipos, en donde exploramos consecuencias legales de un contrato mal realizado para un RedTeam, y sus consecuencias en aceptar este tipo de contratos, luego pasamos un laboratorio explorando condiciones reales de un ataque en donde se pierde información y como se replica dicho ataque para poder entender como operaban los ciberdelincuentes finalmente pasamos al BlueTeam en donde contuvimos el ataque a partir del mismo laboratorio echando mano de software libre y de conocimiento de cómo se realizó el ataque.

Todo ese camino recorrido nos lleva a afrontar en el mundo real como se desenvuelven estos dos equipos el RedTeam y el BlueTeam sin dejar de lado temas legales que son muy importantes, ahora lo concluiremos en este trabajo plasmaremos lo aprendido y concluiremos, además de realizar un video en el cual sustentaremos nuestro camino.

3. Objetivos

3.1 Objetivo General

Formular estrategias de capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam.

3.2 Objetivos Específicos

Desarrollar aspectos que aporten a las estrategias de RedTeam y BlueTeam.

Generar un resumen de las actividades de RedTeam y BlueTeam.

Analizar desde el punto de vista legal.

Realizar recomendaciones para el planteamiento de estrategias de seguridad en una organización.

Realizar un video que sustente el desarrollo del seminario de especialización en RedTeam y BlueTeam.

4. Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

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

De acuerdo a lo realizado durante el seminario se puede determinar tres aspectos como pilares principales al desarrollo de estrategias de RedTeam y BlueTeam, primero coloco los aspectos legales como lo son en Colombia la ley 1273 del 2009, 1377 de 2013 y la ley 1581 de 2012, estas leyes apalancan los alcances que se pueden realizar en estos equipos de seguridad, como lo vimos en uno de los trabajos anteriores un mal contrato llevaba a realizar espionaje infringiendo la ley con penas de cárcel por no tomar en cuenta estos aspectos y leer bien los contratos y limitar las actividades de los equipos.

Segundo pilar equipo RedTeam el equipo rojo realiza la ejecución del ataque para determinar cómo se realizó la perdida de información, en esta parte se realizan las pruebas de penetración desde una maquina Kali Linux a la máquina virtual de la empresa WhiteHose Security.

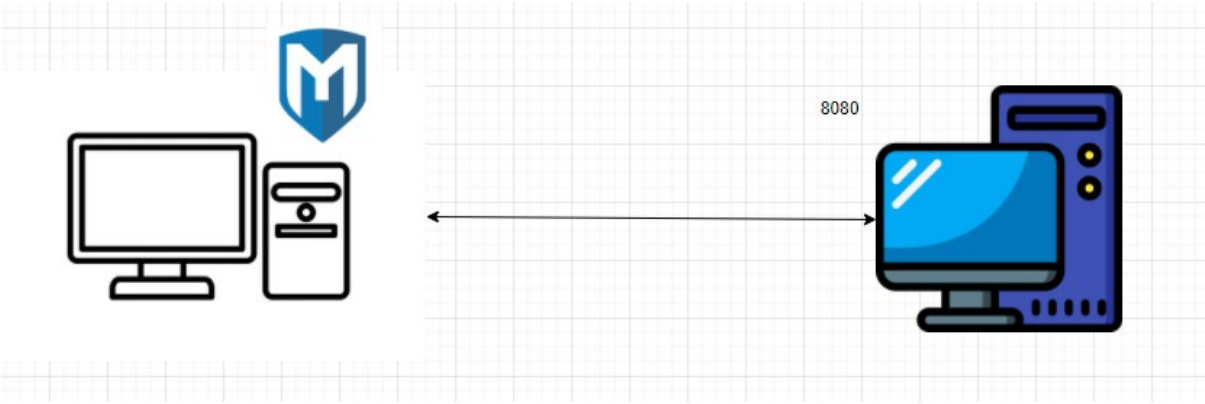
Tercer pilar equipo BlueTeam este equipo azul realiza el análisis de la prueba de penetración y detecta la mejor forma de bloquear el ataque por medio de herramientas de software libre y bloqueos del firewall de Windows.

Ahora bien, para el ejercicio de la empresa The WhiteHose Security, se va a desarrollar estos tres pilares, primero se revisará a nivel legal en este aspecto el atacante incurrirá en lo siguiente: en la ley 1273 de 2009 articulo 269C intercepción de datos informáticos, “Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta

y seis (36) a setenta y dos (72) meses."[1] el atacante está descargando mediante la vulnerabilidad información de la empresa y tiene como pena 36 a 72 meses de cárcel.

RedTeam, este equipo empieza a realizar una prueba de penetración en la máquina virtual con el indicio de una vulnerabilidad en el servicio de rejetto, como se muestra en la imagen 1, el servidor cuenta con el servicio de rejetto expuesto en el puerto 8080, y desde una maquina con Kali Linux se realizará las pruebas.

Imagen 1, esquema de arquitectura.



Fuente (el autor)

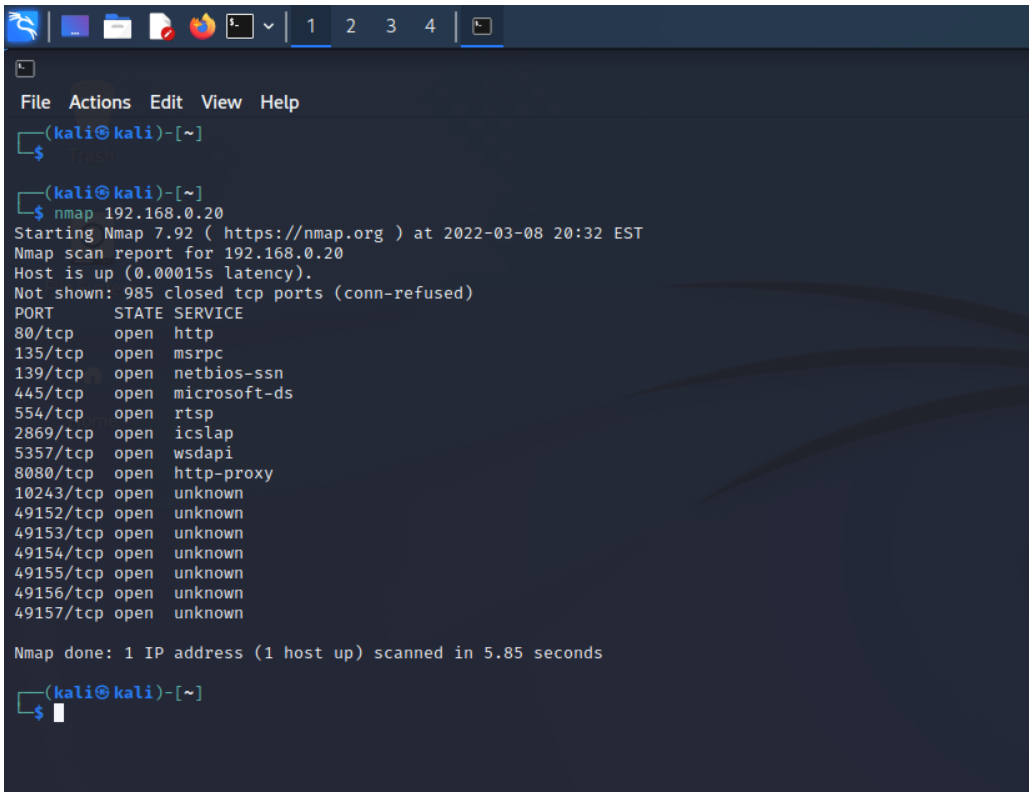
Luego se empieza a realizar los escaneos desde el Kali Linux con la herramienta nmap, como se muestra en la figura 2, "la siguiente fase es identificar cualquier puerto de servicio abierto en el sistema objetivo y determinar qué servicios están mapeados con esos puertos abiertos"[2]:

---

[1] SECRETARIA GENERAL DEL SENADO [sito web], LEY 1273 DE 2009. [consulta: 28 de marzo 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[2] SIBGH, Glen D.; The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire; 2nd Edition; texto en inglés. p198

Imagen 2, ejecución de nmap al servidor Windows



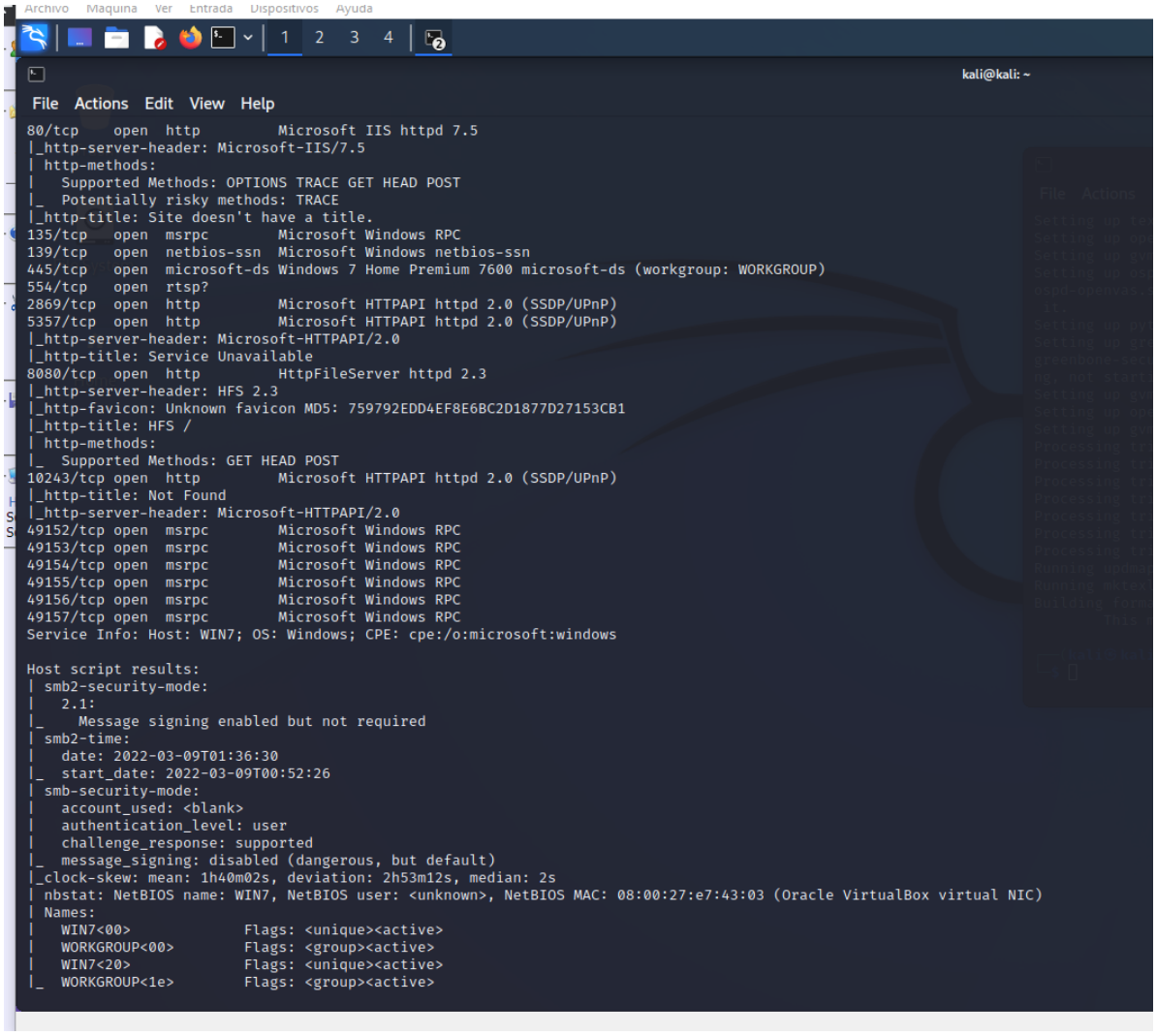
Fuente (el autor)

Dentro de los puertos escaneados se identifica el puerto de rejetto puede ser el 80 o el 8080, se corre un comando de nmap con más opciones para identificar mejor el puerto, “un escaneo avanzado para determinar el sistema operativo de objetivo, versión del servicio y escaneo de scripts, como para realizar un rastreo de ruta, utilizando el siguiente comando”[3]:

nmap -T4 -A -v 192.168.0.20

[3] SIBGH, Glen D.; The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire; 2nd Edition; texto en inglés. p199

Imagen 3. ejecución de nmap con opciones de identificar software en los puertos



Fuente (el autor)

Se identifica en la imagen 2 que el puerto es el 8080 se muestra la salida del comando que este puerto es de HFS 2.3, que es rejetto.

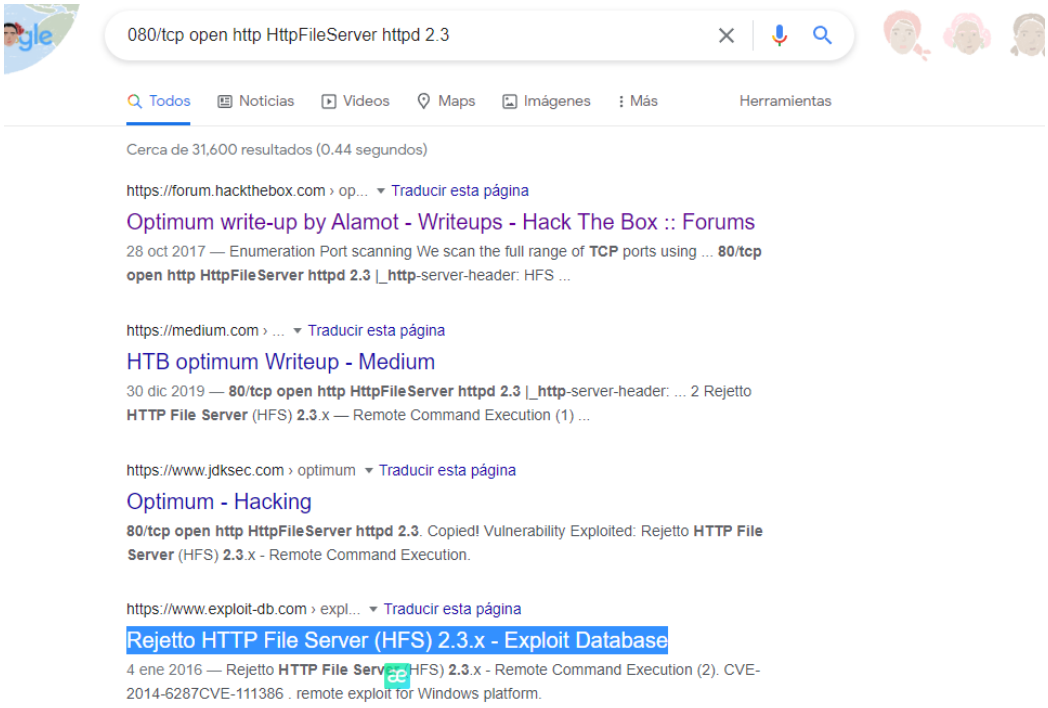
Procedemos a realizar un análisis más detallado de ese puerto como se muestra en la imagen 3:

Imagen 4. ejecución de nmap específico del puerto 8080

Fuente (el autor)

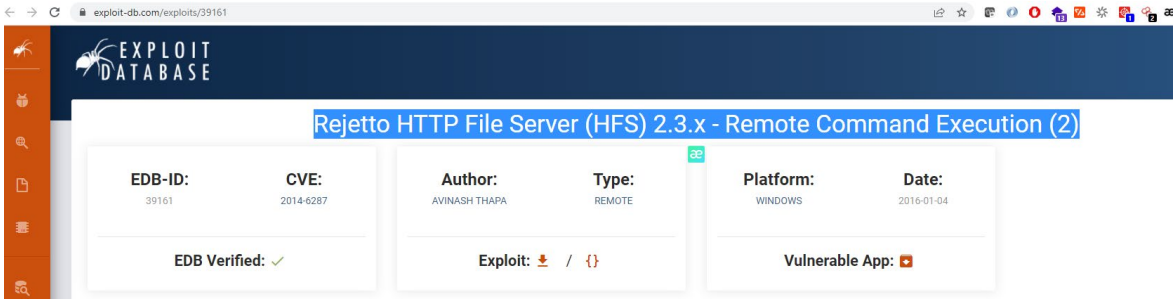
Con una pequeña búsqueda en internet se da cuenta de que es el puerto de programa rejetto y es lo que necesitamos, como se muestra en las imágenes 5 y 6

Imagen 5, búsqueda en Google



Fuente (el autor)

Imagen 6, resultado de la búsqueda en google



Fuente (el autor)

En primer lugar, ya es un software viejo con lo que lleva que si esta mucho tiempo en el mercado es propenso a que tenga vulnerabilidades porque ya no tiene soporte o porque no se actualiza depende de librerías viejas y eso hace que se pueda explotar.

La vulnerabilidad encontrada en este software es la siguiente:

CVE-2014-6287

En la base de datos de “cve details” indican que la vulnerabilidad es por:

“The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c allows remote attackers to execute arbitrary programs via a %00 sequence in a search action.”[4]

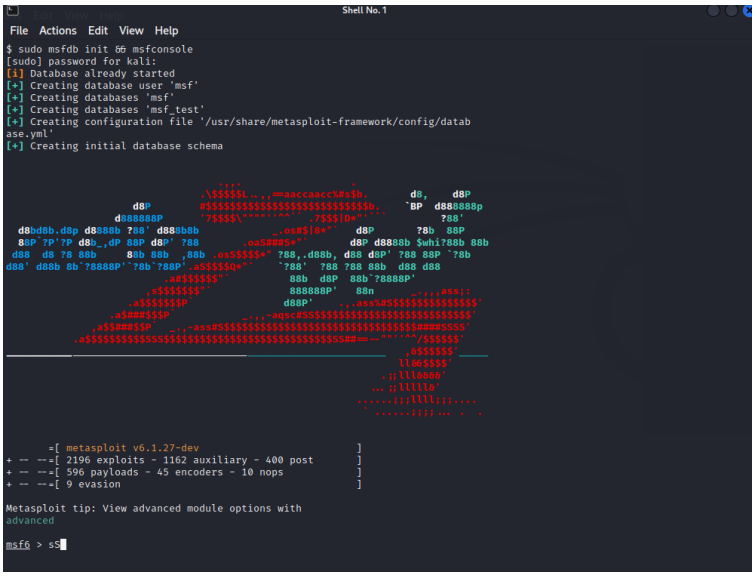
Traducción: “La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.”

Por lo que depende de una función del software parserLib.pas

[4] CVEDETAILS [sito web] Vulnerability Details, CVE, CVE-2014-6287 [Consulta: 28 de marzo 2022]. Disponible en: https://www.cvedetails.com/cve/CVE-2014-6287/

Se realiza el ataque por medio de Metasploit para realizar la penetración de la vulnerabilidad como se muestra en la imagen 7:

Imagen 7. ejecución de metasploit



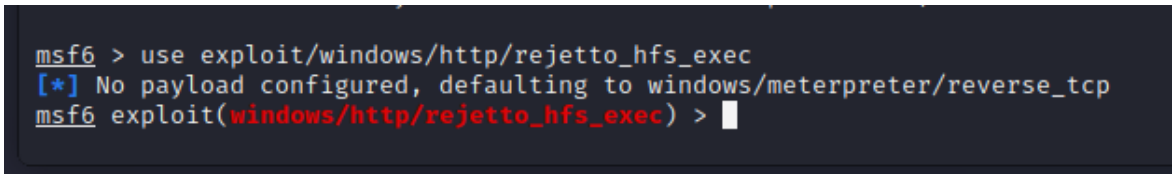
Fuente (el autor)

Como dice en el libro de Metasploit: The Penetration Tester's Guide “Muchas aplicaciones y servicios carecen de módulos personalizados en Metasploit. Afortunadamente, Framework tiene muchas funciones que pueden ser útiles cuando crea un escáner personalizado, incluido el acceso a todas sus clases de explotación. y métodos, y soporte para proxies, capa de sockets seguros (SSL), informes y subprocesos.”[5]

Se observa que el Framework tiene un exploit disponible para nuestro ataque, después lo colocamos en uso como se muestra en la imagen 8:

[5] KENNEDY, David; O'GORMAN, Jim; KEARNS, Devon y AHARONI Mati; Metasploit: The Penetration Tester's Guide 1st Edición; texto en inglés. p31

Imagen 8, uso del expliot

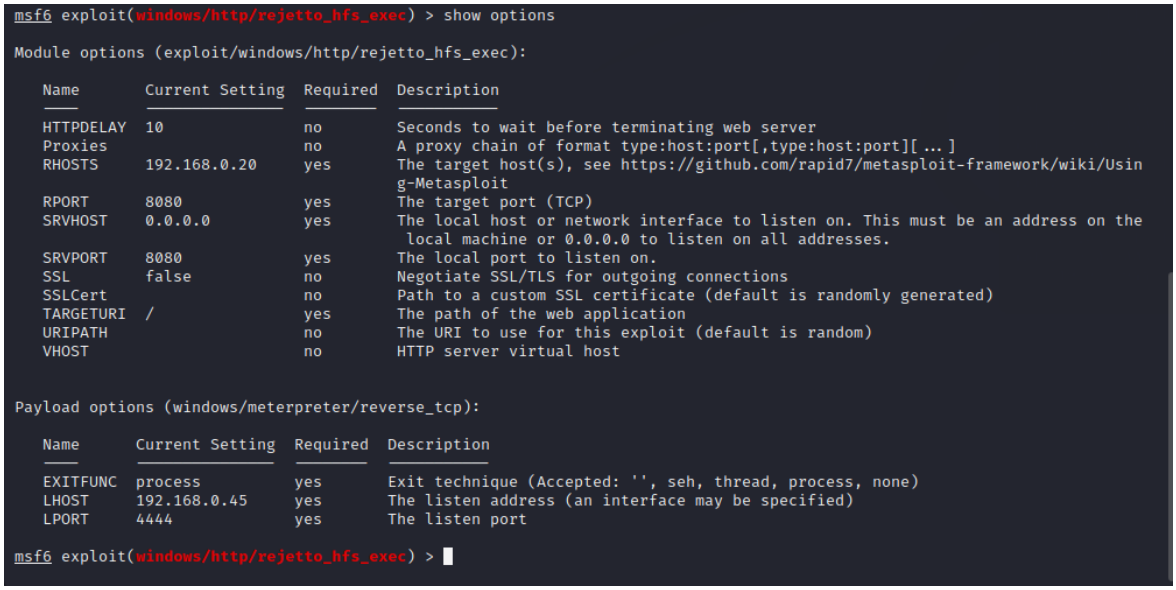


Fuente (el autor)

En esta parte se ejecuta un comando que ayuda a verificar que parámetros se necesitan para poder ejecutar el exploit el cual es, imagen 9:

show options

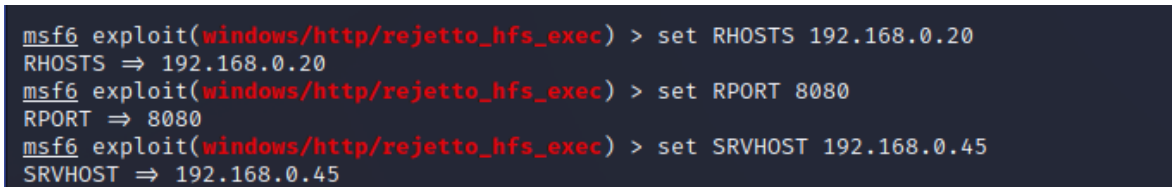
Imagen 9, salida del comando show options



Fuente (el autor)

Se ingresan las variables necesarias para poder ejecutar el exploit, como se muestra en la imagen 10:

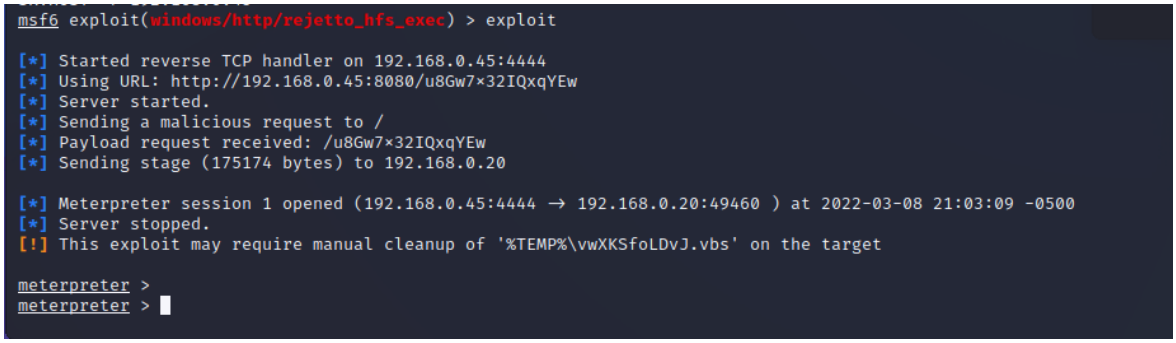
Imagen 10, set de variables.



Fuente (el autor)

Y finalmente se ejecuta el exploit, imagen 11:

Imagen 11, ejecución de exploit



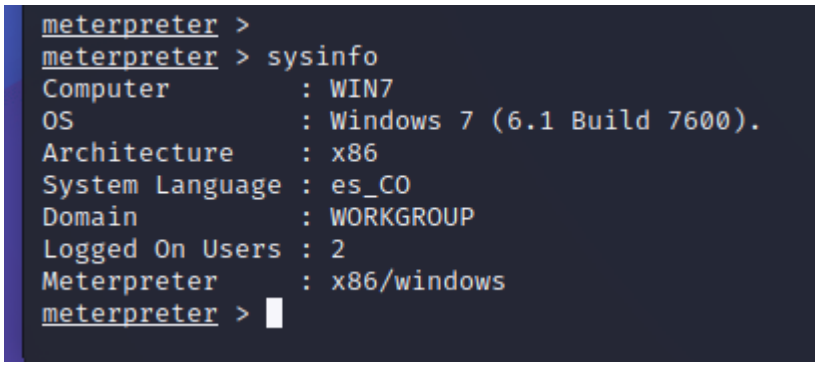
Fuente (el autor)

Y felizmente se ingresa a la maquina y se tiene una Shell reversa, esta parte es muy importante entender que gracias a una vulnerabilidad se puede tener control remoto de la máquina, como se indica en el libro de Metasploit: The Penetration Tester's Guide “Habiendo comprometido con éxito el objetivo y obtenido una consola Meterpreter en el sistema, podemos obtener más información con algunos Meterpreter básicos”[6]

Por ejemplo, con sysinfo verificamos los datos del Windows, como se muestra en la imagen 12:

[6] KENNEDY, David; O'GORMAN, Jim; KEARNS, Devon y AHARONI Mati; Metasploit: The Penetration Tester's Guide 1st Edición; texto en inglés. p80

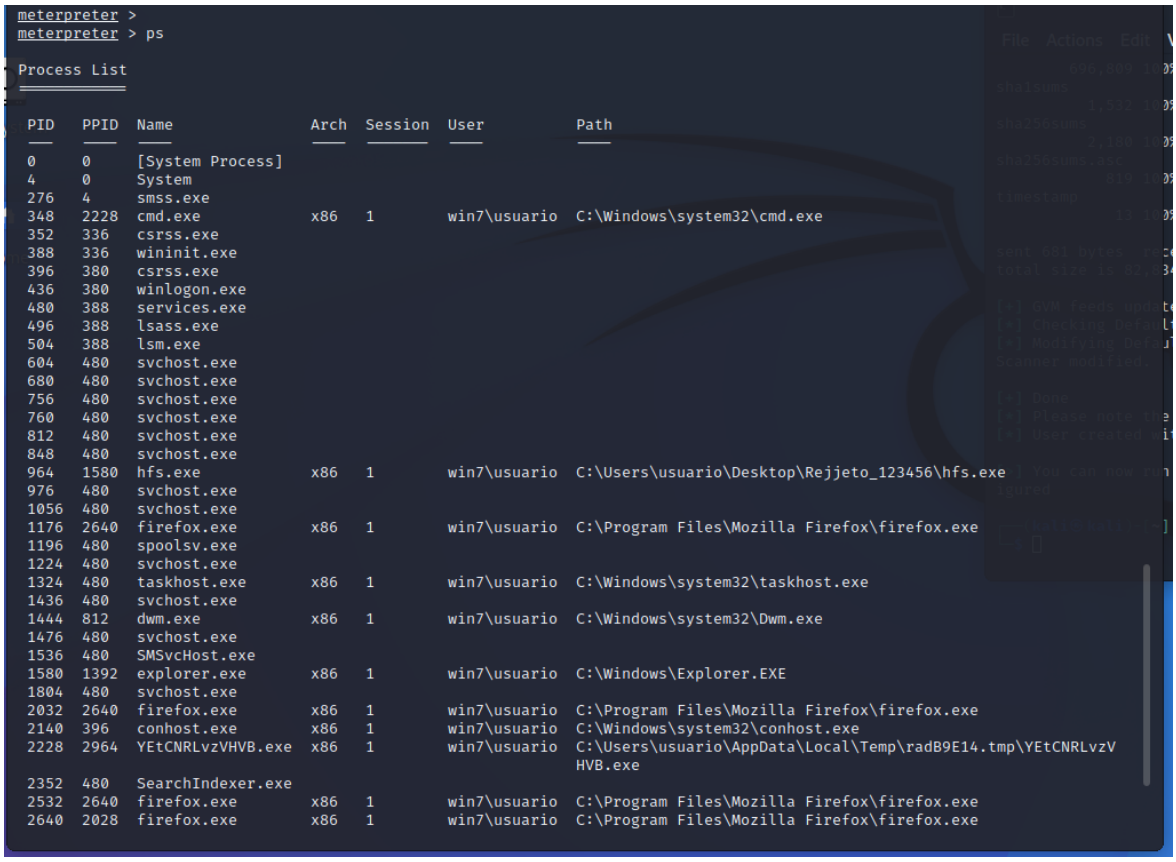
Imagen 12, salida sysinfo



Fuente (el autor)

Ver los procesos que corren en dicha máquina, imagen 13:

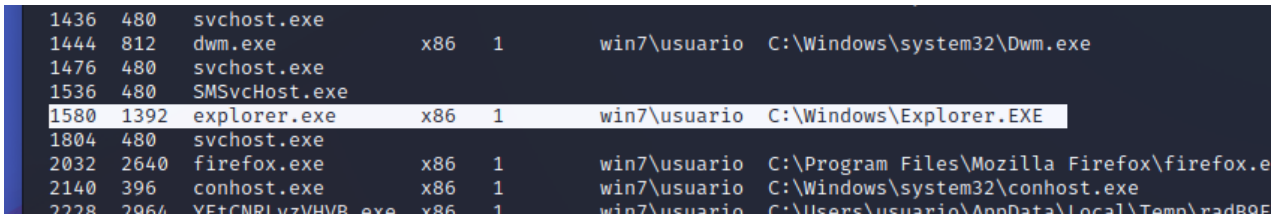
Imagen 13, procesos del servidor desde el exploit



Fuente (el autor)

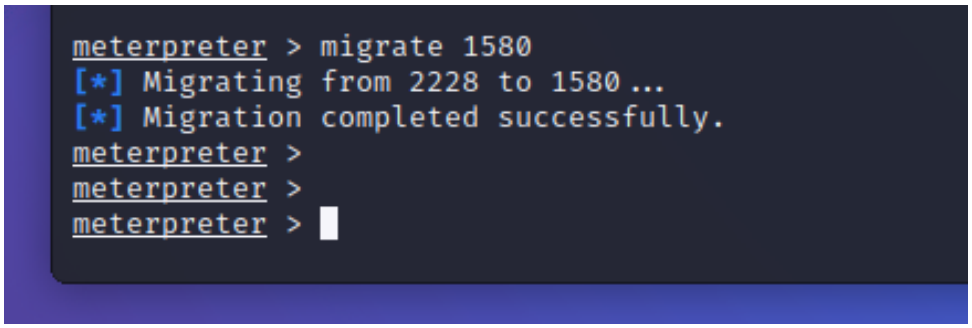
Se puede cambiar el PID de usuario que está conectado y se puede usar el servicio explorer.exe para podernos ocultar la conexión, imagen 14 y 15:

Imagen 14, PID de usuarios



Fuente (el autor)

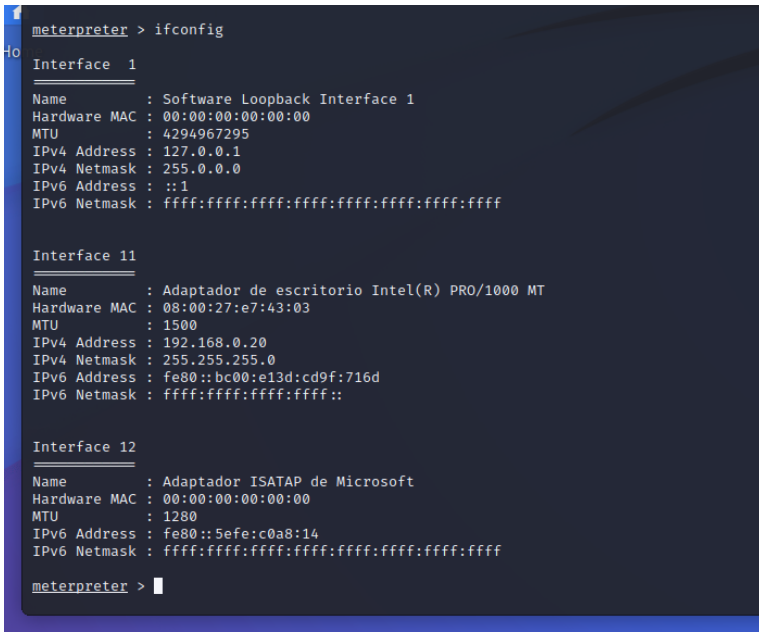
Imagen 15, Cambio de PID de usuario



Fuente (el autor)

También se puede ver ip de la máquina, imagen 16:

Imagen 16, salida del comando ifconfig

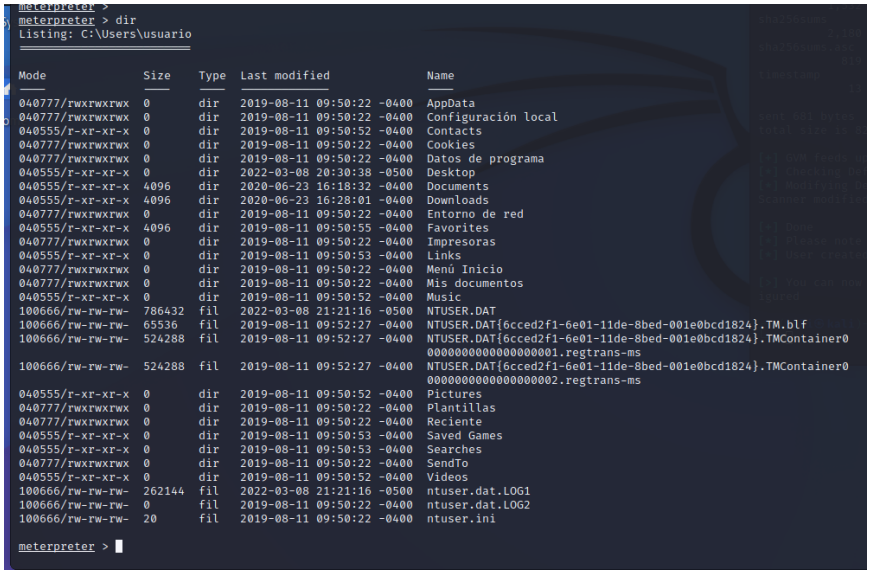


Fuente (el autor)

Y bueno lo importante es como poder sacar información de la maquina:

Se ve el directorio, imagen 17:

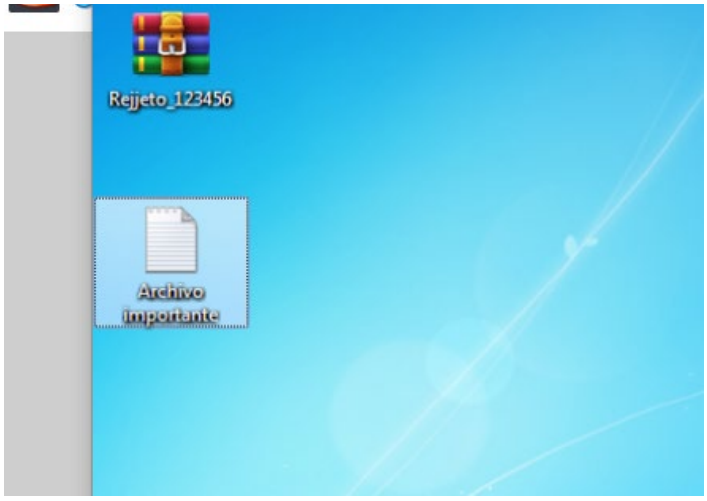
Imagen 17, salida del comando dir



Fuente (el autor)

Y se está por ejemplo a escritorio en donde se crea un archivo de texto para mostrar un ejemplo, imagen 18:

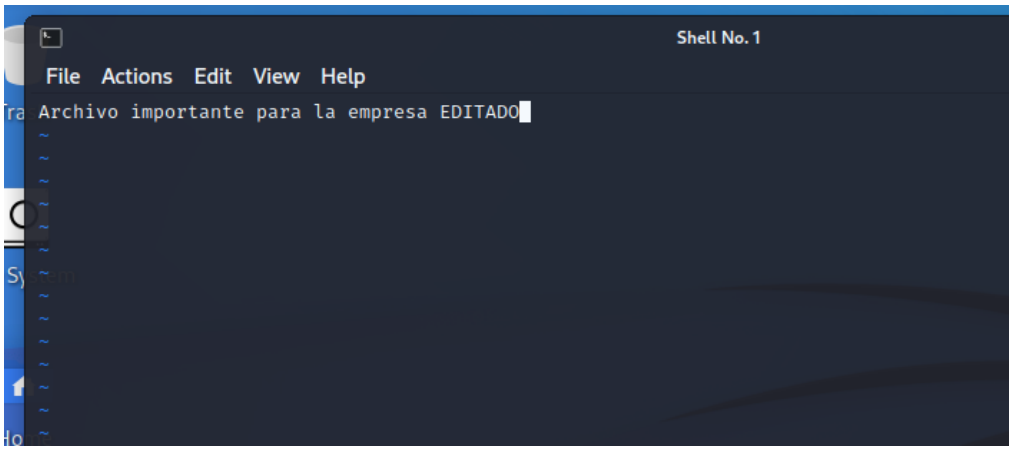
Imagen 18, archivo en el servidor Windows



Fuente (el autor)

Se puede entrar al archivo desde el metasploit y poderlo editar, imagen 19:

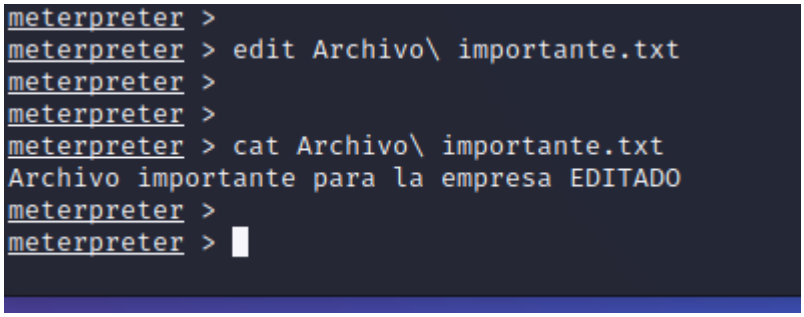
Imagen 19, ejemplo de edición del archivo.



Fuente (el autor)

Y verificar que cambio, como se muestra en la imagen 20:

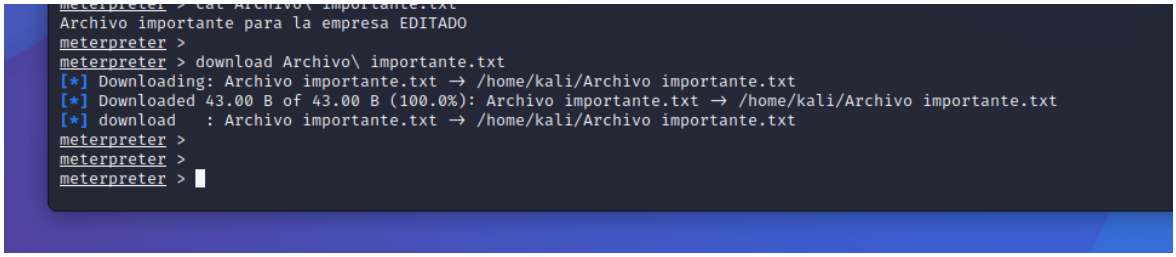
Imagen 20, muestra de que el archivo se editó desde el Kali Linux



Fuente (el autor)

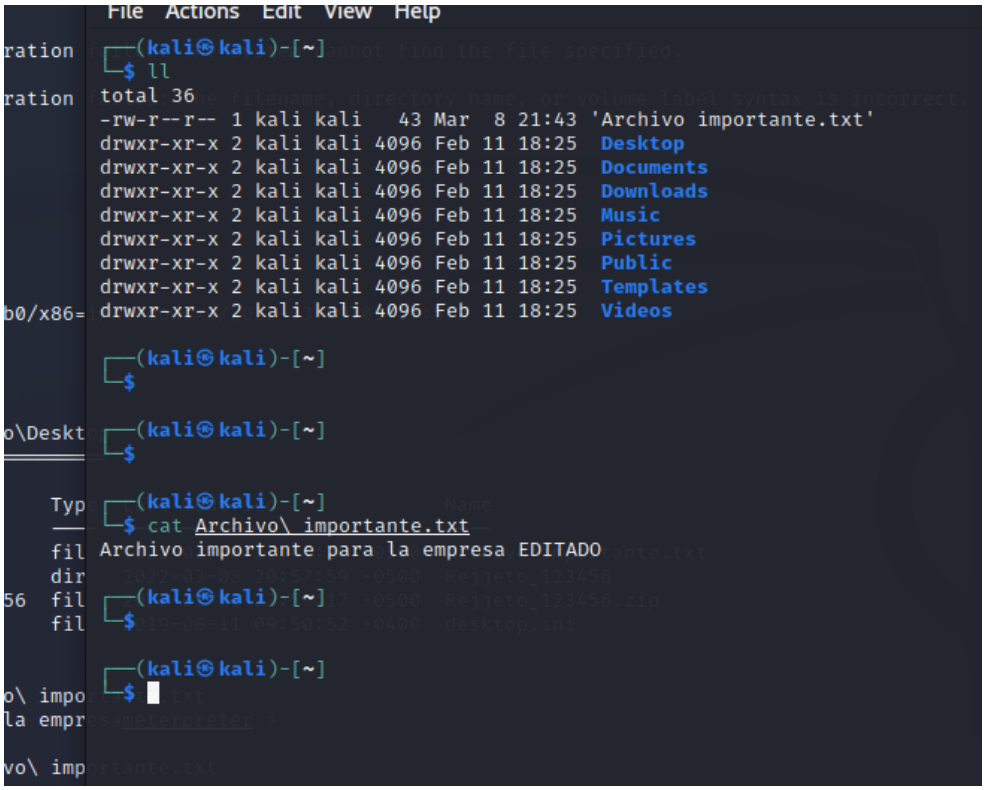
Y lo más importante descargarlo del servidor imagen 21 y 22:

Imagen 21, copiando archivo.



Fuente (el autor)

Imagen 22, muestra de que el archivo se copia al Kali Linux



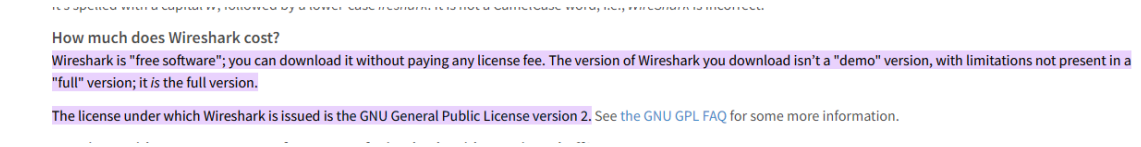
Fuente (el autor)

Se puede concluir que exactamente por la vulnerabilidad CVE-2014-6287, la cual cuenta con un exploit se pude usar herramientas como nmap y metasploit para poder ingresar al servidor y poder extraer información confidencial de la empresa.

Ahora para el equipo BlueTeam ellos realizan un análisis de dicha información y por medio de herramientas de software libre como wireshark, y el firewall propio de Windows podemos cerrar la brecha:

Lo primero que se realiza es encontrar como se está realizando el ataque, hay varias formas, pero dado a que solo se puede usar herramientas open source, usaremos un scaner de red para nuestro caso usaremos wireshark ya que es una herramienta open source como se muestra a continuación en la imagen 23:

Imagen 23, licencia wireshark.



How much does Wireshark cost?

Wireshark is "free software"; you can download it without paying any license fee. The version of Wireshark you download isn't a "demo" version, with limitations not present in a "full" version; it *is* the full version.

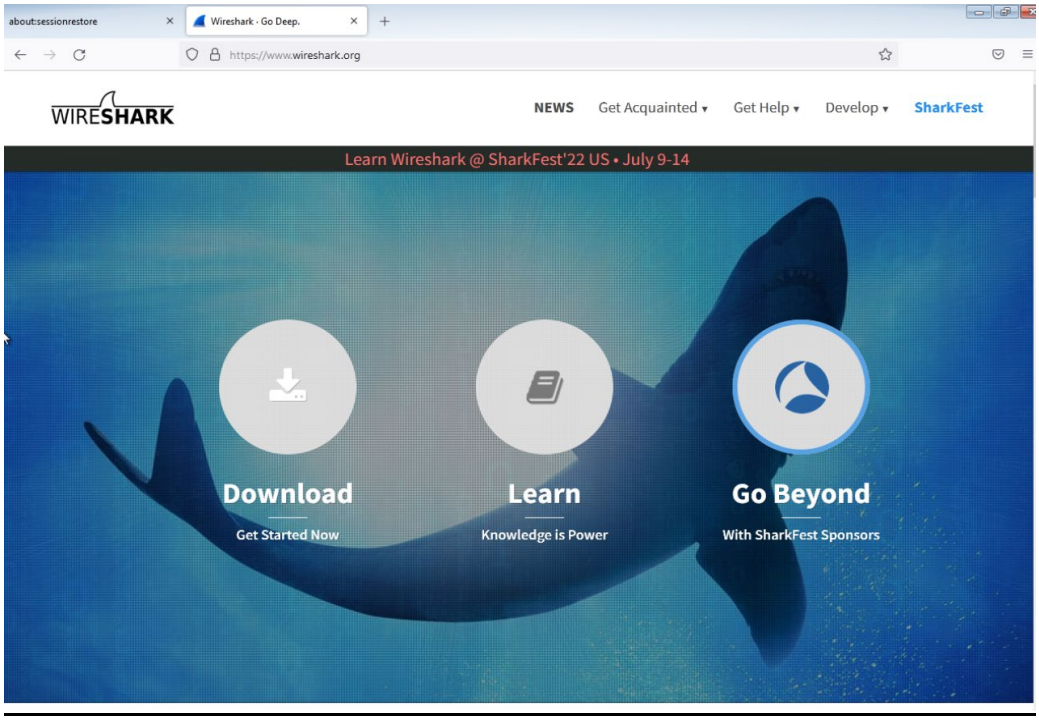
The license under which Wireshark is issued is the GNU General Public License version 2. See the GNU GPL FAQ for some more information.

Fuente (el autor)

"The license under which Wireshark is issued is the GNU General Public License version 2. See the GNU GPL FAQ for some more information."[7]

Se descarga y se instala en el Windows 7, como se muestra en las imágenes 24, 25 y 26

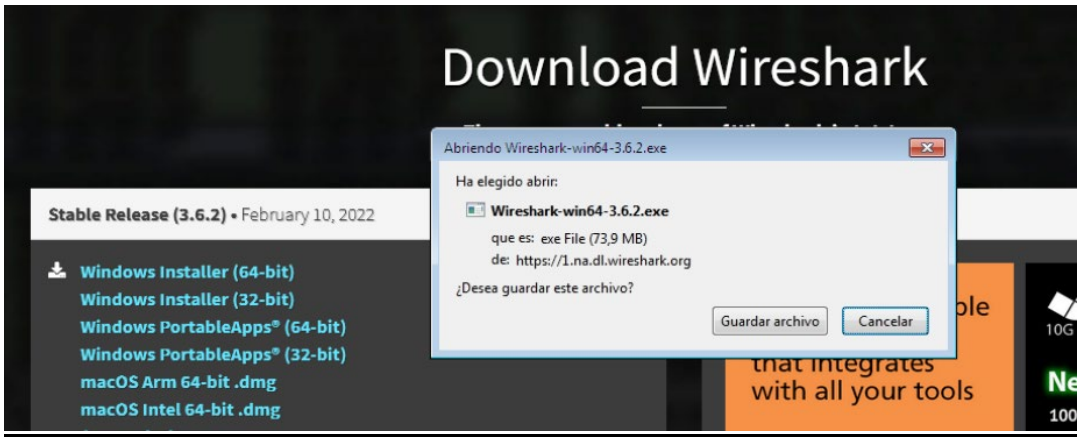
Imagen 24, página de Wireshark



Fuente (el autor)

[7] WIRESHARK [sitio web], Wireshark Frequently Asked Questions [Consulta: 28 de marzo 2022]. Disponible en: https://www.wireshark.org/faq.html#:~:text=Wireshark%20is%20%22free%20software%22%3B,General%20Public%20License%20version%202.

Imagen 25, descarga de Wireshark



Fuente (el autor)

Imagen 26, instalando Wireshark

Fuente (el autor)

Después de una captura se analiza el tráfico:

Esta parte lo realice en otra maquina dado que en el Windows 7 estaba muy lento:

Para fines del desarrollo mostrare las ip de las maquinas:

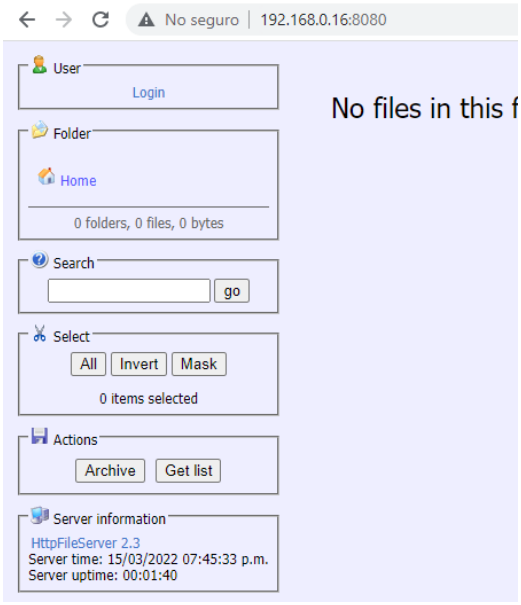
Windows 7: 192.168.0.16

Kali Linux: 192.168.0.45

Análisis:

Lo que se empieza a rastrear son conexiones a los puertos que tiene el servidor ya que en nuestro caso es un servidor de HFS, buscamos conexiones al puerto 8080 el cual es el que está exponiendo el servicio, imagen 27:

Imagen 27, imagen del servicio expuesto.

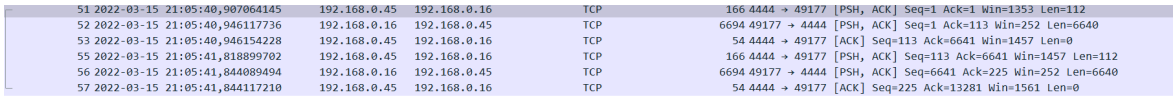


Fuente (el autor)

Luego se busca un patrón como lo es los puertos de origen a la conexión, en seguridad informática para que meterpreter puede hacer una Shell como se hizo en el trabajo anterior por lo general usa el puerto 4444, y nos vamos a centrar a estas conexiones con puerto origen 4444, (hay que aclarar que este puerto se puede cambiar, pero para encontrar conexiones por defecto de meterpreter está bien buscar estas conexiones).

Y encontramos lo siguiente expresado en la imagen 28 y 29:

Imagen 28, traza de trafico de Kali Linux y servidor Windows.



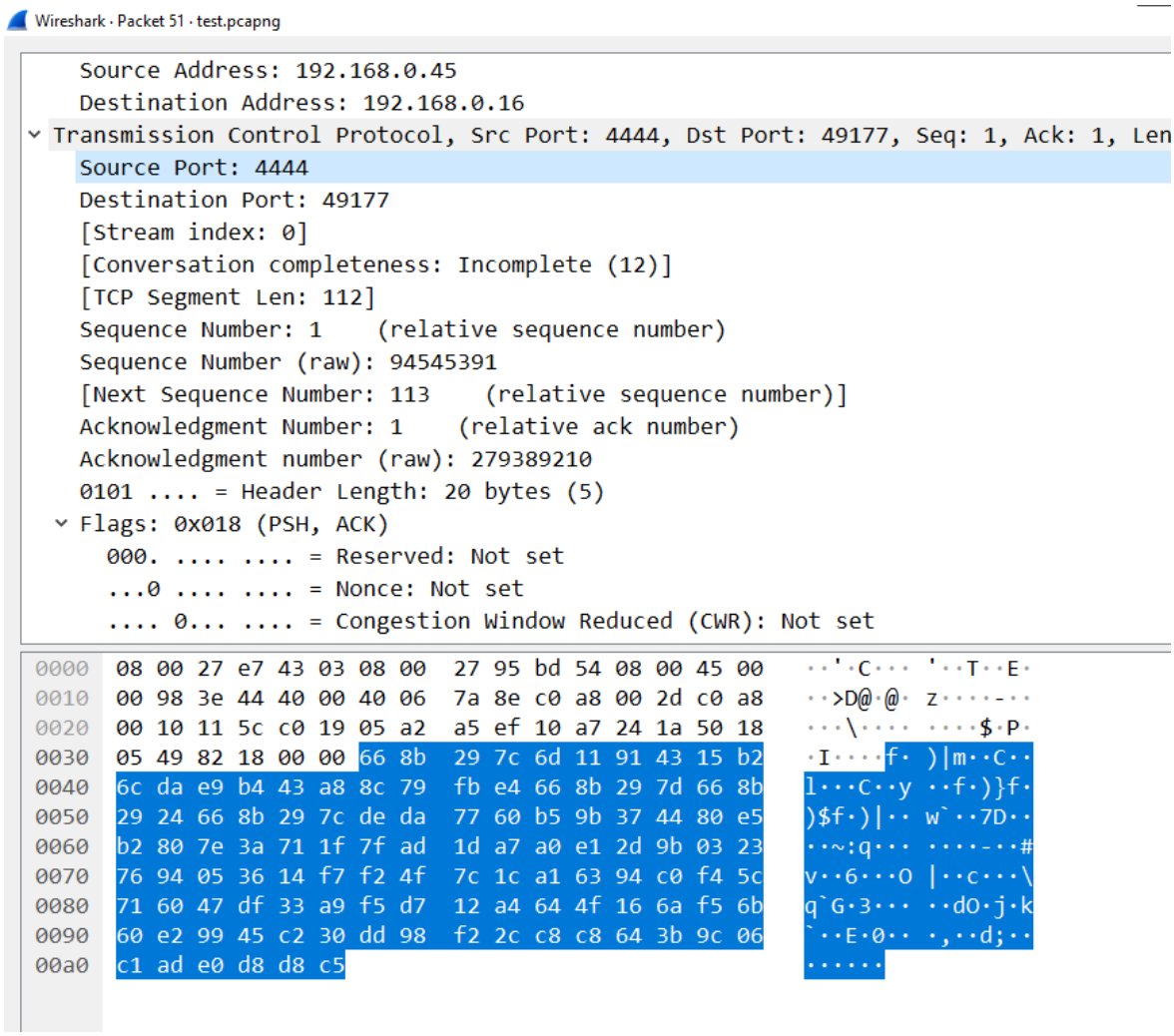
51	2022-03-15 21:05:40,907064145	192.168.0.45	192.168.0.16	TCP	166 4444 → 49177 [PSH, ACK] Seq=1 Ack=1 Win=1353 Len=112
52	2022-03-15 21:05:40,946117736	192.168.0.16	192.168.0.45	TCP	6694 49177 → 4444 [PSH, ACK] Seq=1 Ack=113 Win=252 Len=6640
53	2022-03-15 21:05:40,946154228	192.168.0.45	192.168.0.16	TCP	54 4444 → 49177 [ACK] Seq=113 Ack=6641 Win=1457 Len=0
55	2022-03-15 21:05:41,818899702	192.168.0.45	192.168.0.16	TCP	166 4444 → 49177 [PSH, ACK] Seq=113 Ack=6641 Win=1457 Len=112
56	2022-03-15 21:05:41,844089494	192.168.0.16	192.168.0.45	TCP	6694 49177 → 4444 [PSH, ACK] Seq=6641 Ack=225 Win=252 Len=6640
57	2022-03-15 21:05:41,844117210	192.168.0.45	192.168.0.16	TCP	54 4444 → 49177 [ACK] Seq=225 Ack=13281 Win=1561 Len=0

Fuente (el autor)

IP de origen: 192.168.0.45

IP destino: 192.168.0.16

Imagen 29, muestra detallada de los puertos usados en la conexión



Wireshark · Packet 51 · test.pcapng

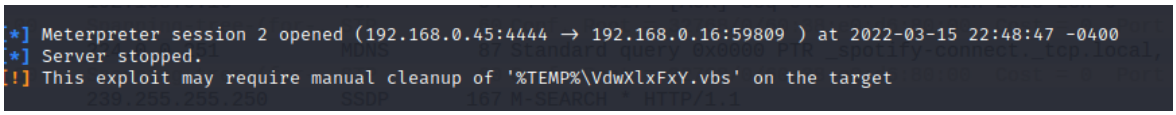
```
   Source Address: 192.168.0.45
   Destination Address: 192.168.0.16
▾ Transmission Control Protocol, Src Port: 4444, Dst Port: 49177, Seq: 1, Ack: 1, Len
   Source Port: 4444
   Destination Port: 49177
   [Stream index: 0]
   [Conversation completeness: Incomplete (12)]
   [TCP Segment Len: 112]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 94545391
   [Next Sequence Number: 113    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 279389210
   0101 .... = Header Length: 20 bytes (5)
 ▾ Flags: 0x018 (PSH, ACK)
     000. .... .... = Reserved: Not set
     ...0 .... .... = Nonce: Not set
     .... 0... .... = Congestion Window Reduced (CWR): Not set
```

```
0000  08 00 27 e7 43 03 08 00  27 95 bd 54 08 00 45 00   ··'·C··· '··T··E·
0010  00 98 3e 44 40 00 40 06  7a 8e c0 a8 00 2d c0 a8   ··>D@·@· z····-··
0020  00 10 11 5c c0 19 05 a2  a5 ef 10 a7 24 1a 50 18   ···\···· ····$·P·
0030  05 49 82 18 00 00 66 8b  29 7c 6d 11 91 43 15 b2   ·I····f· )|m··C··
0040  6c da e9 b4 43 a8 8c 79  fb e4 66 8b 29 7d 66 8b   l···C··y ··f·)}f·
0050  29 24 66 8b 29 7c de da  77 60 b5 9b 37 44 80 e5   )$f·)|·· w`··7D··
0060  b2 80 7e 3a 71 1f 7f ad  1d a7 a0 e1 2d 9b 03 23   ··~:q··· ····-··#
0070  76 94 05 36 14 f7 f2 4f  7c 1c a1 63 94 c0 f4 5c   v··6···O |··c···\
0080  71 60 47 df 33 a9 f5 d7  12 a4 64 4f 16 6a f5 6b   q`G·3··· ··dO·j·k
0090  60 e2 99 45 c2 30 dd 98  f2 2c c8 c8 64 3b 9c 06   `··E·0·· ·,··d;··
00a0  c1 ad e0 d8 d8 c5                                  ······
```

Fuente (el autor)

Puerto 4444: Se usa como puerta trasera, Caballo de troya, y en múltiples usos para espiar tráfico crear Shell reversas como es este caso con meterpreter y en múltiples usos. “Puerto 4444, Protocolo de control de transporte: Algunos programas de rootkit , puerta trasera y caballo de Troya se abren y utilizan el puerto 4444. Utiliza este puerto para espiar el tráfico y las comunicaciones, para sus propias comunicaciones y para exfiltrar datos de la computadora comprometida. También se utiliza para descargar nuevas cargas útiles maliciosas. Malware como el gusano Blaster y sus variantes usaban el puerto 4444 para establecer puertas traseras.”[8] Ver imagen 30

Imagen 30, muestra del uso del puerto por la Shell reversa



Fuente (el autor)

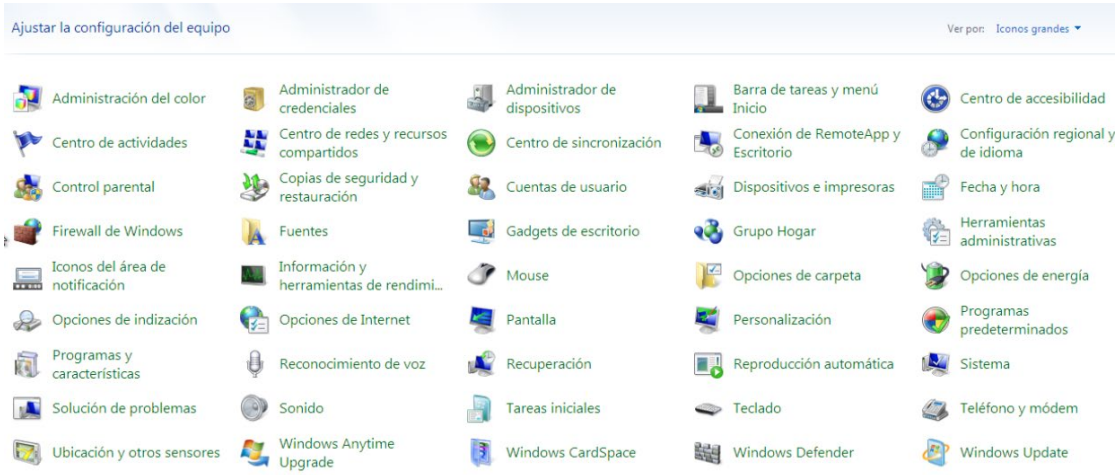
En la conexión que se hace desde el Kali Linux el usa el 4444 para poder realizar la conexión.

Para hardenisar el servidor lo primero que se va a hacer el subir el firewall y bloquear el puerto 4444:

Lo primero que se hace es activar el firewall de Windows, se muestra en las imágenes 31, 32 y 33:

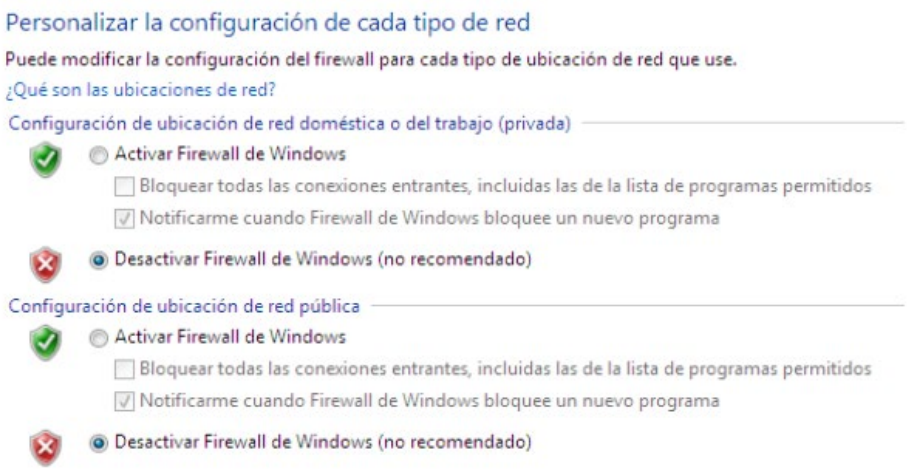
[8] TEMAS RELACIONADOS CON INTERNET TECNOLOGÍA Y LA CIENCIA [sitio web], Porque algunos puertos de red son peligrosos y como se protegen. [consulta: 28 de marzo 2022]. Disponible en: https://www.clasesordenador.com/porque-algunos-puertos-de-red-son-peligrosos-y-como-se-protegen/

Imagen 31, panel de control de Windows



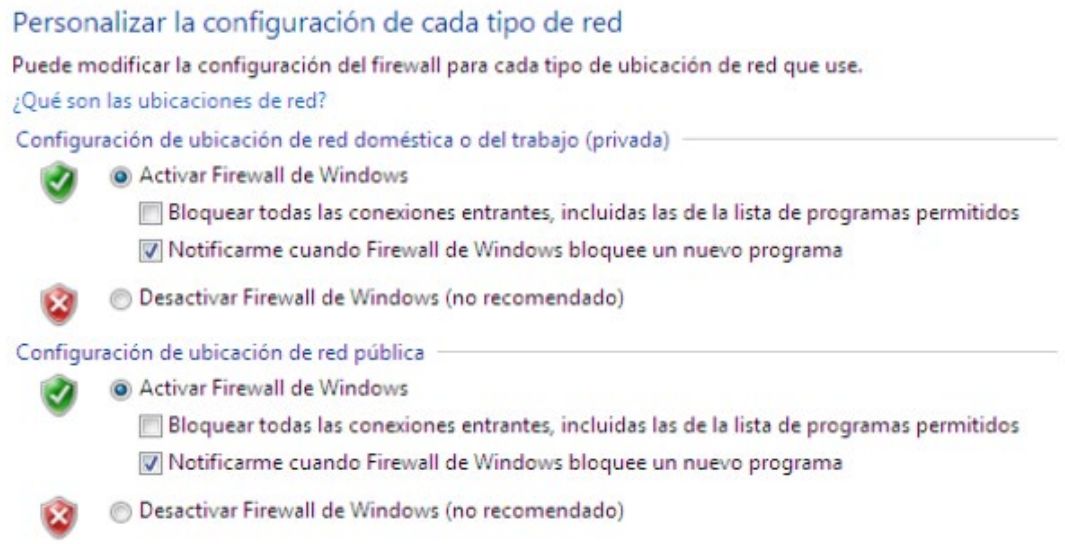
Fuente (el autor)

Imagen 32, Firewall desactivado.



Fuente (el autor)

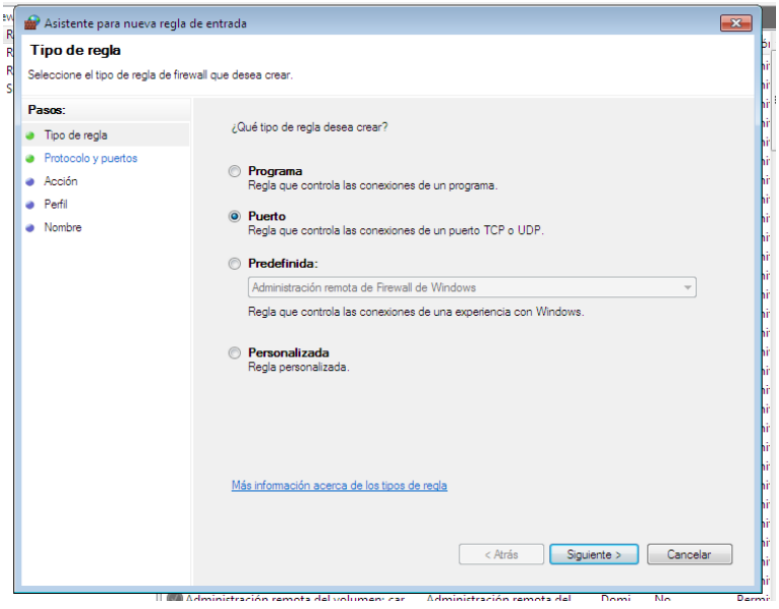
Imagen 33, Firewall activo



Fuente (el autor)

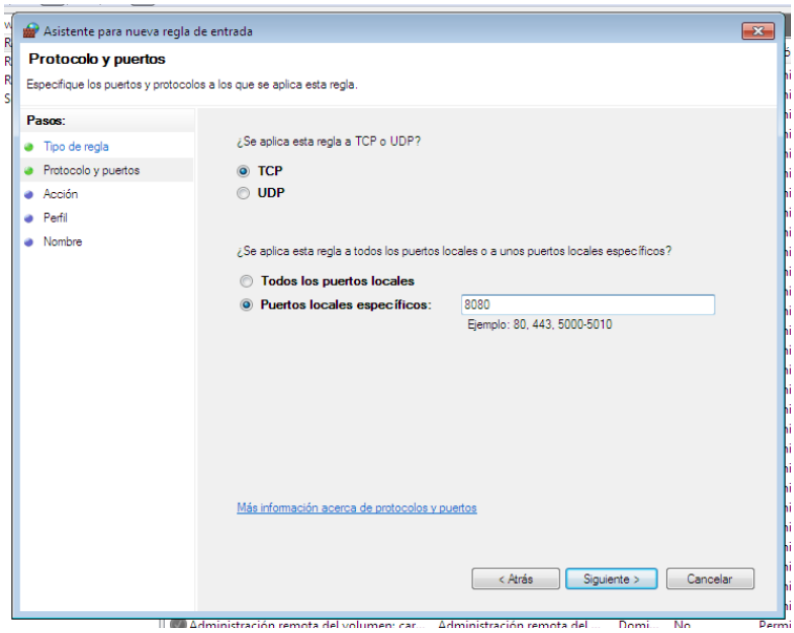
Una vez activo se procede a crear una regla específica para el puerto 8080 el cual es el servicio, se muestra en la imagen 34 y 35:

Imagen 34, configuración de la regla de firewall.



Fuente (el autor)

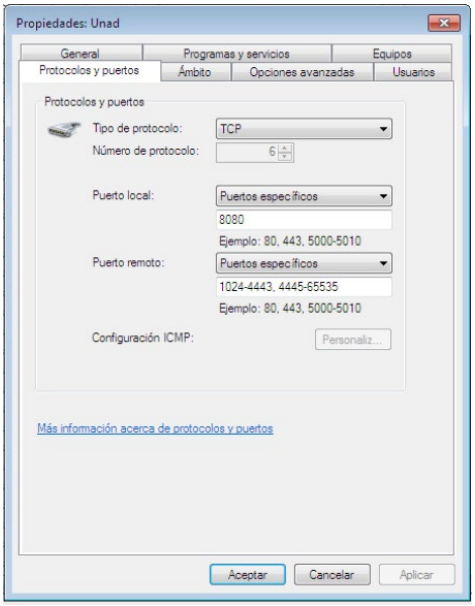
Imagen 35, configuración de la regla con el puerto 8080



Fuente (el autor)

Y después se procede a cerrar las conexiones origen para que no se puede conectar con el puerto 4444, imagen 36:

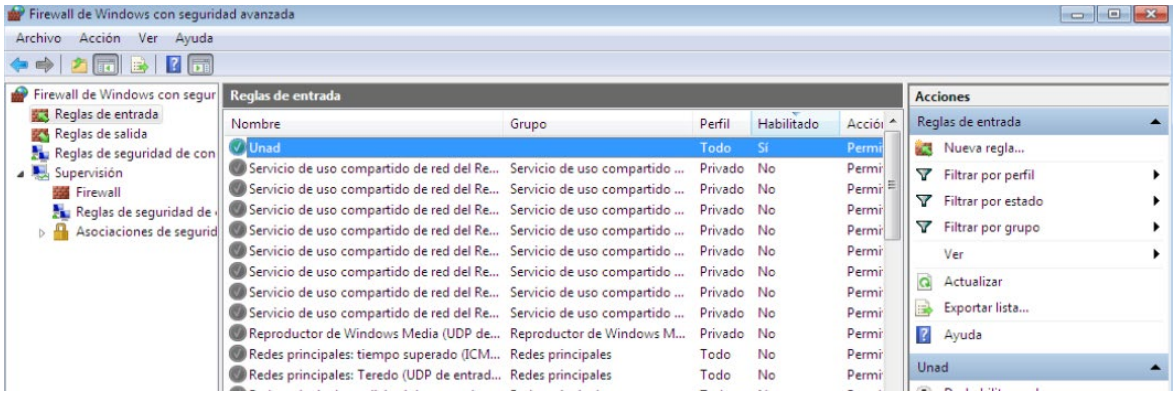
Imagen 36, configuración de la regla con los puertos origen.



Fuente (el autor)

Llama a la regla UNAD, se prueba que no se pueda conectar desde un navegador al servicio que es para lo que lo necesitamos:

Imagen 37, regla configurada.

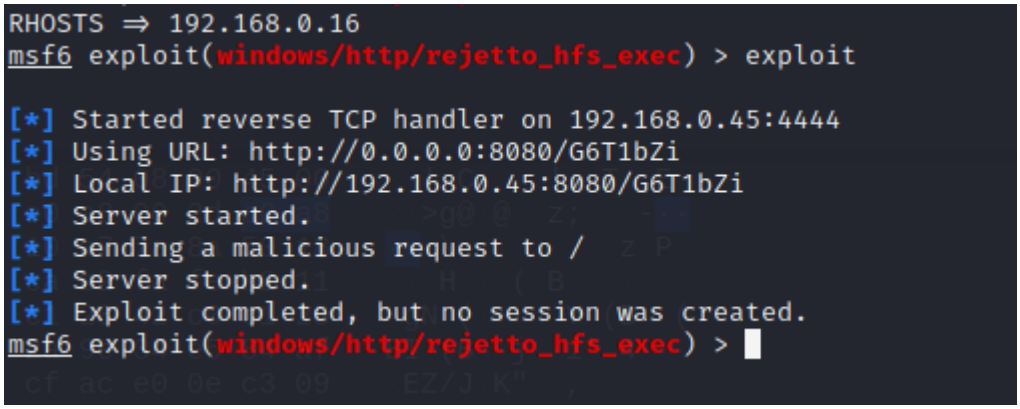


Fuente (el autor)

También se cierra las conexiones a los demás puertos solo dejamos la conexión 8080.

Y Finalmente se prueba que no se puede explotar la vulnerabilidad con Metaexploit:

Imagen 38, ejecución fallida del exploit.



Fuente (el autor)

4.2 Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

Las recomendaciones que se pueden dar de acuerdo a lo visto en este seminario son las siguientes:

Creación de equipos de RedTeam y BlueTeam en la organización.

Definir metodologías de implementación de dichos equipos.

Dentro de las actividades del RedTeam definir claramente los alcances que se tienen para realizar pentest en la compañía.

Proveer de herramientas al equipo BlueTeam, herramientas básicas como un SIEM, definir el monitoreo 7x24, y si existe un incidente de seguridad que se detecte tener una vía de ruta definida para mitigar o detener el ataque.

Capacitar técnicamente al personal de los dos equipos RedTeam y BlueTeam, llevarlos a seminarios, pagarles cursos, etc.

Capacitarlos en aspectos legales a los dos equipos para poder tener una visión más amplia del panorama de seguridad.

Realizar seguimiento constante y mejorar el proceso cada vez que se requiera.

También es importante que los altos directivos de la empresa se involucren en estas actividades primero para que sepan lo peligroso que puede ser no invertir en seguridad segundo para que tengan claro los lineamientos y conozcan las limitaciones que pueden tener estas actividades en la compañía.

4.3 Link del Video

Link: https://youtu.be/7CmGmfaKuKc

5. Conclusiones

Se explora con un ejemplo práctico los alcances y roles de los equipos RedTeam y BlueTeam, realizando un ataque a una máquina virtual a la cual se le estaba atacando para filtrar información, el RedTeam realiza el ataque y muestra cómo se realiza la filtración de la información y el BlueTeam realiza acciones para no permitir el ataque, este escenario practico de la empresa WhiteHose Security, es perfecto para poder aprender los alcances de estos dos equipos en el mundo real.

También se explora aspectos legales que incurren los atacantes en dado caso que se pueda determinar quién está haciendo el robo de información para poderlo denunciar por lo siguiente: en la ley 1273 de 2009 articulo 269C intercepción de datos informáticos, el atacante está descargando mediante la vulnerabilidad información de la empresa y tiene como pena 36 a 72 meses de cárcel.

Además de las dos conclusiones anteriores también aprendimos el uso de herramientas como nmap, Metasploit para realizar ataques para pruebas de penetración y poder explorar en el mundo real estas herramientas como interactúan.

Aprendimos a poder contener un ataque en este caso un ataque de robo de información, y como poder detenerlo con el uso básico de firewall conociendo como se realiza el ataque podemos bloquear los puertos y detener el ataque sin bajar el servicio expuesto con la vulnerabilidad.

6. Recomendaciones

Las organizaciones deben contar con los equipos RedTeam y BlueTeam, es muy importante para poder blindar poco a poco las vulnerabilidades de la compañía, constante mente las compañías son atacadas y es necesario realizar auto ataques con probas de penetración controladas con el RedTeam con esto se logra detectar vulnerabilidades y mejorar los tiempos de respuesta del BlueTeam.

Mejorar día tras día con implementaciones de metodologías para los dos equipos y capacitaciones constantes en lo legar y lo técnico para mejorar el alcance de los equipos.

Mostar estas actividades a los altos mandos para que entiendan los problemas que se pueden presentar si no se invierte en estos equipos y en ejercicios constantes de seguridad ya que la pregunta no es si nos pueden atacar si no cuando nos atacaran y si nos atacan ¿estamos preparados?

7. Bibliografía

SIBGH, Glen D.; The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire; 2nd Edition; ISBN-13: 978-1801818933

HERTZOG, Raphael y O'GORMAN Jim; Kali Linux Revealed: Mastering the Penetration Testing Distribution; ISBN-10: 0997615605

KENNEDY, David; O'GORMAN, Jim; KEARNS, Devon y AHARONI Mati; Metasploit: The Penetration Tester's Guide 1st Edición; ISBN-10: 159327288X

JASWAL, Nipun; Mastering Metasploit: Exploit systems, cover your tracks, and bypass security controls with the Metasploit 5.0 framework; 4th Edition; ISBN-10: 1838980075

TEIXEIRA, Daniel; SINGH, Abhinav y AGARWAL Monika; Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition Edición; ISBN-10: 1788623177

CHAPPELL, Laura; Wireshark® 101: Essential Skills for Network Analysis - Second Edition: Wireshark Solution Series; ASIN: B06XRXLSB9

BOCK, Lisa; Learn Wireshark: Confidently navigate the Wireshark interface and solve real-world networking problems; ISBN-10: 1789134501

Wireshark Network Analysis (Second Edition) [Anónimo]: The Official Wireshark Certified Network Analyst Study Guide 2nd Revised ed. Edición; ISBN-10: 1893939944

DUNKERLEY, Mark y TUMBARELLO, Matt; Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats, ISBN-10: 1839216417

BOYCE, Jim; Windows 7 Bible 3rd Edición; ISBN-10: 0470509090

THOMAS, Arun E; Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence; ISBN-10: 1986862011

MILLER, David R.; HARRIS, Shon, HARPER, Allen; VANDYKE, Stephen y BLASK Chris; Security Information and Event Management (SIEM) Implementation (Network Pro Library) 1st Edición; ASIN: B004BKIFDY

CLARK, Ben; Rtfm: Red Team Field Manual Tapa blanda – 11 febrero 2014; ISBN-10: 1494295504

VEST, Joe y TUBBERVILLE, James; Red Team Development and Operations: A practical guide; ISBN-13: 979-8601431828

MURDOCH, Don; Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter; ISBN-10: 1091493898

TANNER, Nadean H.; Cybersecurity Blue Team Toolkit 1st Edición; ISBN-10: 1119552931

SECRETARIA GENERAL DEL SENADO [sito web], LEY 1273 DE 2009. [consulta: 28 de marzo 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONSEJO PROFESIONAL NACIONAL DE INGENIERIAS ELÉCTRICA, MECÁNICA Y PROFESIONES AFINES [sitio web], LEY 842 DE 2003, [consulta: 28 de marzo 2022]. Disponible en: https://www.consejoprofesional.org.co/resources/uploaded/files/files/LEY%20842%20DE%202003(1).pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [sitio web], ley 1273 del 5 de enero de 2009. [consulta: 28 de marzo 2022]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

CVE DETAILS [sitio web], cvedetails Vulnerability Details: CVE-2014-6287, [consulta: 28 de marzo 2022]. Disponible en: https://www.cvedetails.com/cve/CVE-2014-6287/

RAPID7 [sitio web], Rejetto HttpFileServer Remote Command Execution, [consulta: 28 de marzo 2022]. Disponible en: https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/

ADVANCE YOUR KNOWLEDGE IN TECH [sitio web], Vulnerability analysis of HFS 2.3. [consulta: 28 de marzo 2022]. Disponible en: https://subscription.packtpub.com/book/networking_and_servers/9781786463166/1/ch01lvl1sec20/vulnerability-analysis-of-hfs-2-3.

EXPLOIT DATABASE [sitio web], Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2), [consulta: 28 de marzo 2022]. Disponible en: https://www.exploit-db.com/exploits/39161

CYBERSEGURIDAD [sitio web], Las fases de un test de penetración. [consulta: 28 de marzo 2022]. Disponible en: https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

ORACLE [sitio web], ¿Qué es un WAF? [consulta: 28 de marzo 2022]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-waf.html

INFOTECS [sitio web], IPS: Sistema de Prevención de Intrusos, [consulta: 28 de marzo 2022]. Disponible en: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

NSIT - CIBERSEGURIDAD, SISTEMAS Y TECNOLOGÍA INFORMÁTICA (TI) [sitio web], ¿Qué es SIEM en seguridad informática? Alcance e implementación, [consulta: 28 de marzo 2022]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

WIRESHARK [sitio web], Wireshark Frequently Asked Questions [Consulta: 28 de marzo 2022]. Disponible en: https://www.wireshark.org/faq.html#:~:text=Wireshark%20is%20%22free%20software%22%3B,General%20Public%20License%20version%202.

TEMAS RELACIONADOS CON INTERNET TECNOLOGÍA Y LA CIENCIA [sitio web], Porque algunos puertos de red son peligrosos y como se protegen. [consulta: 28 de marzo 2022]. Disponible en: https://www.clasesordenador.com/porque-algunos-puertos-de-red-son-peligrosos-y-como-se-protegen/