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

FRANCISCO JAVIER PULIDO AMAYA

JOHN FREDDY QUINTERO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE INGENIERIA DE SISTEMAS
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM - (202337164A_780)
BOGOTÁ 2021

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

BLUETEAM: Equipo de seguridad interno que realiza monitoreo constante para actuar contra posibles ataques informáticos

CIS: Center for Internet Security, organización sin ánimo de lucro que tienen como objetivo la generación de medidas de protección aplicables a las organizaciones.

ESCANEO: Análisis de un sistema.

EXPLOIT: Explotar o aprovechar software basado en debilidades de seguridad.

INCIDENTE INFORMATICO: Eventos que comprometen la operatividad o seguridad de la información de un individuo u organizaciones comprometiendo los datos o sistemas informáticos que se tengan.

PARCHE DE SEGURIDAD: Los parches de seguridad son correcciones o ajustes de sistemas que mejoran seguridad corrigiendo fallos eventuales o brechas detectadas.

REDTEAM: Equipo externo que realiza pentesting basado en las medidas de seguridad adoptadas por una organización.

SIEM: Gestión de Eventos e Información de Seguridad (Security Information and Event Management) Software como función principal es la de presentar información útil acerca de potenciales amenazas de seguridad para ser analizada y si es el caso actuar inmediatamente con esas eventualidades.

VULNERABILIDAD: Incapacidad de protección de un sistema.

RESUMEN

Reconocimiento de los pasos para la presentación de un informe técnico basado en los datos recibidos durante el seminario, enfocados al campo de acción de los equipos Redteam y Blueteam.

INTRODUCCIÓN

En la etapa de globalización de la tecnología se evidencia cada vez más la necesidad de generar un análisis de seguridad para apoyar los procesos de aseguramiento de sistemas y plataformas computacionales debido a los riesgos que se generan día a día, para tal fin es necesario conocer y plantear los controles informáticos enfatizados a la tecnología y seccionada en servicios y necesidades directamente ligadas al Core de negocio de las compañías, como la determinación de qué importancia se le da a los activos tecnológicos y su entendimiento del riesgo que se corre al no conocer su estado actual, para tales riesgos existen varias normas y métodos de análisis para mejorar la protección con herramientas de aseguramiento informático.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Encontrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas Redteam de intrusión aplicadas para la generación de un informe con aplicación de Blueteam

1.2 OBJETIVOS ESPECÍFICOS

Aplicar los conocimientos y habilidades adquiridas en seguridad informática mediante la metodología de recopilar información, escaneo y utilización de los exploit detectados

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

Mediante los datos recibidos de la intrusión debemos encaminar el análisis a encontrar como fue el camino de la intrusión y su posible víctima.

De acuerdo al tema enunciado la sospecha de fuga de información está fundamentada en la obsolescencia de los sistemas operativos que al caso son Windows 7 en versión x86 y x64 los cuales manejan un protocolo antiguo para compartir recursos de red como lo es el SMBv1 el cual es susceptible a varias versiones de exploits, a lo cual se suma el hecho que no han tenido actualizaciones por más de 3 años con lo cual es muy alto el riesgo de verse comprometida la seguridad y privacidad de la información en la empresa.

Se denota que existe una debilidad bastante preocupante de seguridad al no contar con políticas que garanticen métodos o buenas prácticas de aseguramiento las cuales permitirían tener los controles mínimos en seguridad de la información como lo pueden ser las actualizaciones de seguridad de los sistemas operativos o contar con software de protección como lo es un antivirus con administración de firewall local o elementos de análisis de comportamientos de red y gestión de accesos de usuarios, los cuales apoyarían la gestión de seguridad mediante las alertas que se puedan generar, a partir del análisis de un equipo Redteam se podrían identificar cómo fue posible la intrusión y hasta donde se comprometió la privacidad de la información

2.2 JUSTIFICACIÓN

Se debe realizar un análisis de la información para la correcta ejecución de escaneos de vulnerabilidades los cuales nos determinen sus falencias de seguridad para poder determinar técnicas de prevención y contención para su mejoramiento.

Es necesario conocer las técnicas de contención su funcionamiento y su efectividad basada en su aplicación por grupos como Blueteam para el mejoramiento de la seguridad donde los equipos Redteam podrán realizar pruebas sobre los sistemas comprometidos para encontrar los puntos de fallo o que presenten vulnerabilidades.

Al poder detectar y evidenciar las vulnerabilidades presentadas un equipo Blueteam podrá generar una estrategia de aseguramiento con lo cual se pueden tomar medidas que permitirán mitigar los riesgos que puedan comprometer la seguridad y privacidad de la información.

.

3. MARCO TEÓRICO

Teniendo en cuenta los datos recibidos de los anexos citados, como base para la generación de técnicas para la creación del informe técnico donde se demuestra el conocimiento aplicado acerca de los distintos grupos de seguridad y herramientas de apoyo para lograr la resolución del problema.

Debido a que cada día crece de manera exponencial los sistemas digitales las redes y servicios de información es necesario contar con profesionales que administren y protejan la información, la base de esta afirmación la obtenemos de la experiencia de pérdida de información siendo un riesgo palpable y medible dependiendo del tipo de información, debemos contar con tecnologías y profesionales que faciliten el trabajo de la detección y prevención de fugas informáticas.

Mediante la promoción desde dichas áreas de TI se debe generar el conocimiento mínimo para que se genere una cultura digital y sepan cómo actuar las personas con menos conocimiento de la organización, ya que las áreas de TI no tienen como única tarea la seguridad informática se deben crear políticas o esquemas que apoyen su labor ya sea basándose en un SGSI o políticas creadas a partir de la necesidad evidenciada y experimentada conjuntamente apoyados en grupos Redteam Blueteam con lo cual se podría llegar a la optimización de procesos de prevención y detección hasta una contención en tiempo real, logrando una trazabilidad de servicio.

4. DESARROLLO DEL INFORME

Situación presentada:

La empresa busca Identificar porqué medio o proceso se está generando una de fuga de información, dos de sus equipos de cómputo en la dependencia, se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. contando son protocolo de comunicación SMBv1 la fuga de información (10 de junio de 2020) última actualización 05 de febrero de 2017 CVE-2017-0144, MS17-010. Usted como parte de un equipo RedTeam deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, buscar el método de explotación por medio de algún framework o exploit Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de "winse20w0.exe"[1].

Análisis

Siendo el escenario una copia de los equipos que presentan como problemas y al ser autorizados por la empresa a realizar las validaciones y pruebas necesarias para la determinación de la fuga de información, podremos utilizar las herramientas que sean necesarias para llevar a cabo nuestra investigación sin llegar a incurrir en algún delito informático.

De acuerdo a la información recibida y recolectada, realizamos un escaneo de posibles vulnerabilidades de los sistemas presentados con un énfasis especial a la validación de las vulnerabilidades referentes al fallo de seguridad CVE-2017-0144. El cual denota "El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes diseñados, también conocidos como

[1] Anexo 4 – Escenario 3: https://campus102.unad.edu.co/ecbti81/pluginfile.php/2915/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

"Vulnerabilidad de ejecución remota de código SMB de Windows”.”[2] Se pueden observar los detalles e impacto de esta vulnerabilidad en la Tabla 1 y Tabla2 respectivamente.

Tabla 1. Vulnerabilidad en SMBv1 (CVE-2017-0144)

Tipo	Validación incorrecta de entrada	Fallo en la validación de datos introducidos en aplicaciones que afecta al flujo de control o de datos de un programa.
Gravedad	Alta	• Permite a un atacante remoto violar la protección de seguridad de un sistema (por ejemplo conseguir acceso de algún usuario o de tipo 'root') • Permite a un ataque local ganar control completo del sistema • Es lo suficientemente importante como para tener un consejo del CERT/CC (CERT advisory)
Fecha publicación		16/03/2017
Última modificación		20/06/2018[3]

Fuente Autor

Tabla 2. Impacto de la vulnerabilidad (CVE-2017-0144)

Vector de acceso	A través de red
Complejidad de Acceso	Media

[2] CVE MITRE
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

[3] INCIBE CERT
https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

Autenticación	No requerida para explotarla	
Tipo de impacto	Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema	• Confidencialidad: Si permite el robo de información. La confidencialidad se refiere a la limitación de la información únicamente a grupos o usuarios autorizados, previniendo el acceso a dicha información a los no autorizados. • Integridad: Si permite cambiar la información que reside o que pasa por un sistema. La integridad se define como la confianza y la garantía en la veracidad de una información. • Disponibilidad: Si la vulnerabilidad permite un ataque que imposibilita directamente a un usuario (humano o máquina) el acceso a un recurso del sistema en particular[4]

Fuente Autor

De acuerdo al análisis normalizamos los datos recibidos para lo cual utilizamos la siguiente metodología:

• Información recibida para análisis de los hechos (Datos entregados anexo 4 escenario 3 Fallo de seguridad CVE-2017-0144)
• Recolección de información sobre las victimas (Escaneo con Software LEGION)
• Reconocimiento de vulnerabilidades (Metasploit MS17-010)
• Explotación de vulnerabilidades (Metasploit MS17-010_eternalblue)

[4] INCIBE CERT
https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

Resultados Obtenidos:

Al realizar los escaneos de vulnerabilidades se encontraron fallos de seguridad en las maquinas windows 7 a nivel de Web server, que para este caso no son relevantes ya que estas máquinas tienen la configuración estándar de este tipo de servicios y no se presentan como publicadores de contenido web o como resultado de falsos positivos, el otro fallo hace referencia al protocolo SMBv1, con lo cual nos encamina hacia la búsqueda del exploit que aplique a esta vulnerabilidad, se realiza la prueba con el exploit y se encontró que las maquinas Windows 7 x64 y x86 presentan la vulnerabilidad tal como se observan en la Tabla 3 y Tabla 4 respectivamente, referida en el fallo de seguridad CVE-2017-0144, de acuerdo a este resultado intentamos explotar esta vulnerabilidad en las maquinas Windows x64 y x86, al realizar la pruebas del exploit solo en la maquina Windows 7 x64 se logró concretar exitosamente la ejecución remota de código, lo cual nos determina que la intrusión indebida o la fuga de información fue realizada por medio de la maquina Windows 7 x64.

Tabla 3. Vulnerabilidades maquina Windows 7 x64 (PC202006 - 10.10.10.2)

Fallos encontrados	Categoría	Descripción general
Puerto 5357 10243/TCP	Web Server/HTTPAPI/2.0	The anti-clickjacking x-frame-options header is not present
Puerto 5357 10243/TCP	Web Server/HTTPAPI/2.0	the x-xss-protection header is not defined
Puerto 5357 10243/TCP	Web Server/HTTPAPI/2.0	the x-content-type-options header is not set
Puerto 445/TCP	SMB	account_used: guest authentication_level: user challenge_response:supported message_signing: disabled (dangerous, but default)

Fuente Autor

Tabla 4. Vulnerabilidades maquina Windows 7 x86 (win7 - 10.10.10.3)

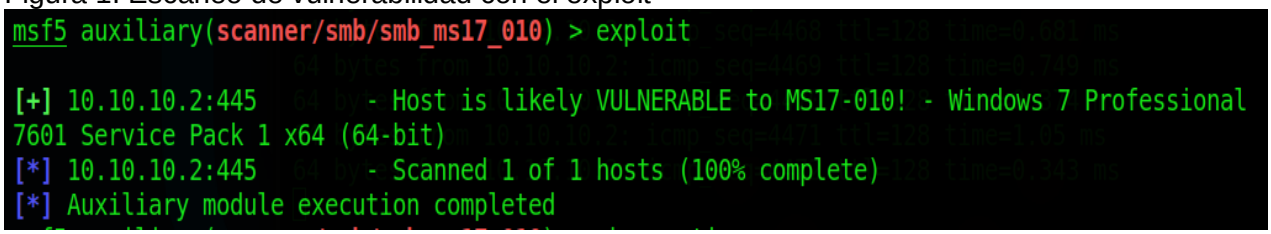
Fallos encontrados	Categoría	Descripción general
Puerto 80 5357/TCP	Web Server/IIS 7.5	The anti-clickjacking x-frame-options header is not present
Puerto 80 5357/TCP	Web Server/IIS 7.5	the x-xss-protection header is not defined
Puerto 80 5357/TCP	Web Server/IIS 7.5	the x-content-type-options header is not

		set
Puerto 80/TCP	Web Server/IIS 7.5	Allowed http methods: options, trace, get, head, post
Puerto 80/TCP	Web Server/IIS 7.5	Public http methods: options, trace, get, head, post
Puerto 445/TCP	SMB	account_used: guest authentication_level: user challenge_response:supported message_signing: disabled (dangerous, but default)

Fuente Autor

El ataque para las maquinas Windows 7 en cuestión, se pudo concretar al no contar con los parches de seguridad actualizados para la fecha del ataque, en especial el ms17-010 como una de sus principales vulnerabilidades ya que sin él se permitió la ejecución de código de manera remota en las 2 máquinas Windows 7 tal como se observa en la Figura 1.

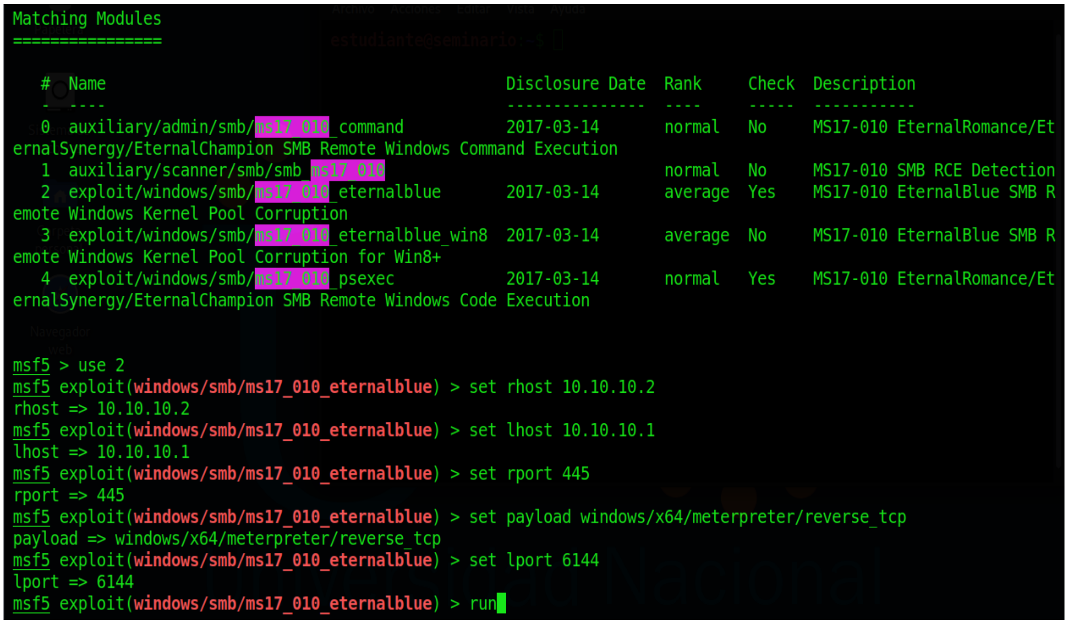
Figura 1. Escaneo de vulnerabilidad con el exploit



Fuente Autor

Para la continuación del ataque se realizó la configuración del exploit definiendo la maquina remota y desde donde se va ejecutar el exploit para que sea enviado el payload como puede ser observado en la Figura 2.

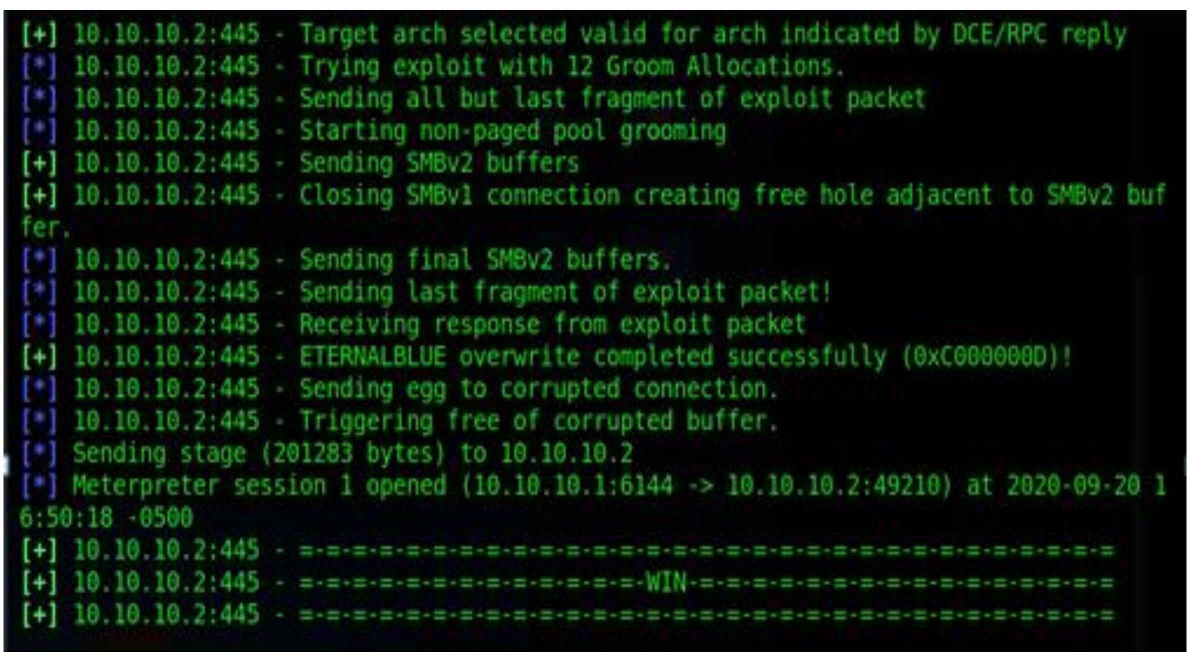
Figura 2. Envío del payload de la vulnerabilidad



Fuente Autor

Una vez enviado el payload se pudo observar que ha sido exitosa la carga al evidenciar la palabra WIN al final de las líneas como se puede ver en la Figura 3.

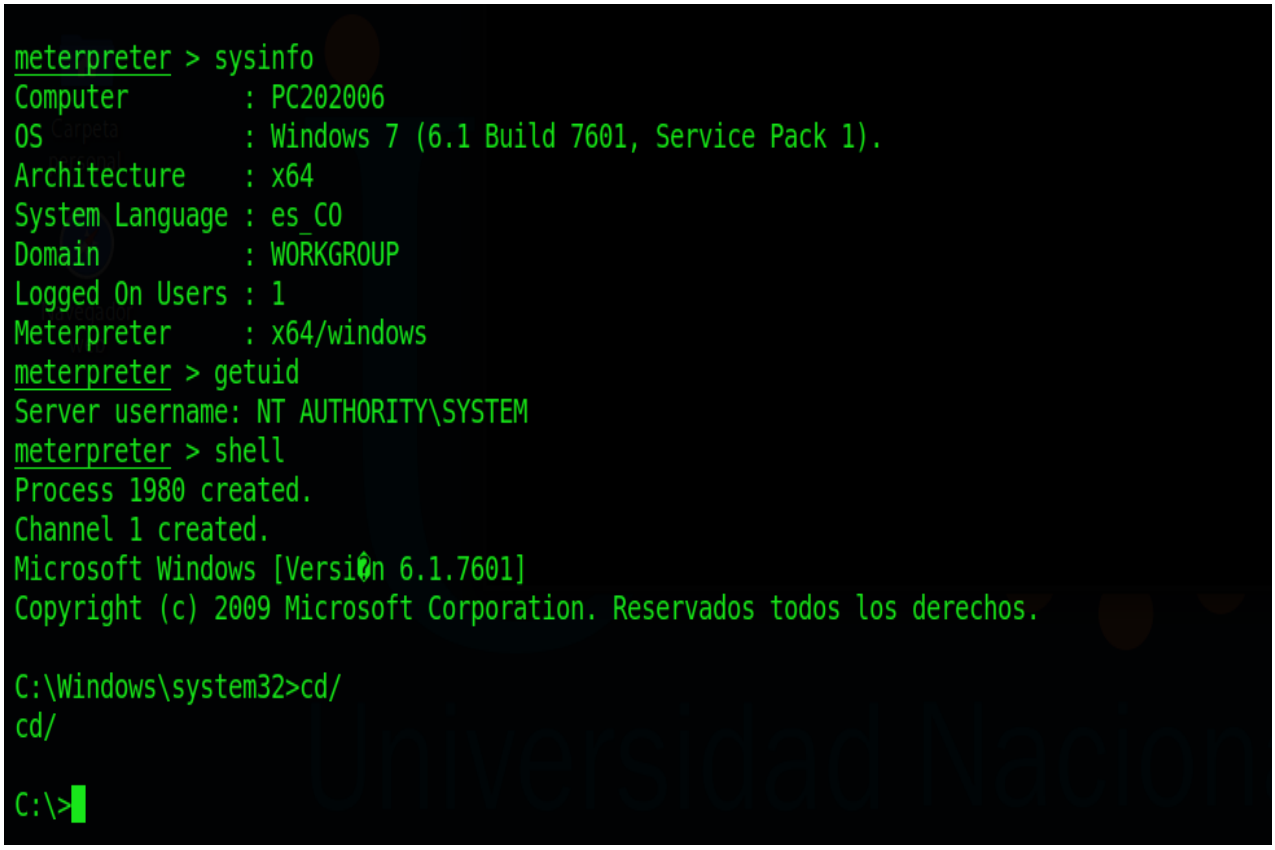
Figura 3. Carga remota de payload exitosa



Fuente Autor

Al estar con el payload meterpreter, se realizó la comprobación del sistema mediante el comando sysinfo y posteriormente el comando shell el cual nos mostró los datos del sistema operativo del equipo atacado tal como se puede observar en la Figura 4.

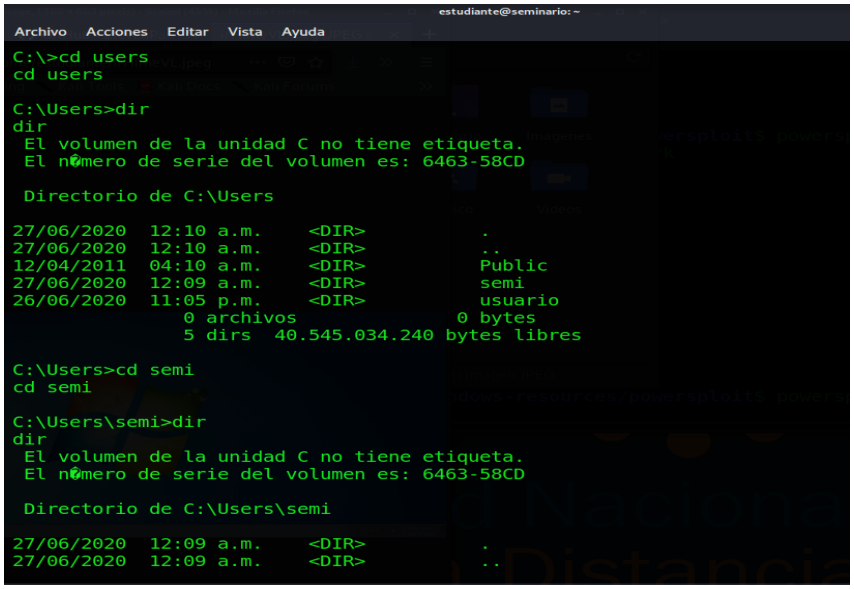
Figura 4. Intrusión remota desde meterpreter



Fuente Autor

Mediante el comando shell se realizó la intrusion a nivel del sistema operativo de la victima, donde se realizó la exploracion de directorios con su respectivo contenido en busqueda del archivo de fuga de informacion como se puede observar en la Figura 5.

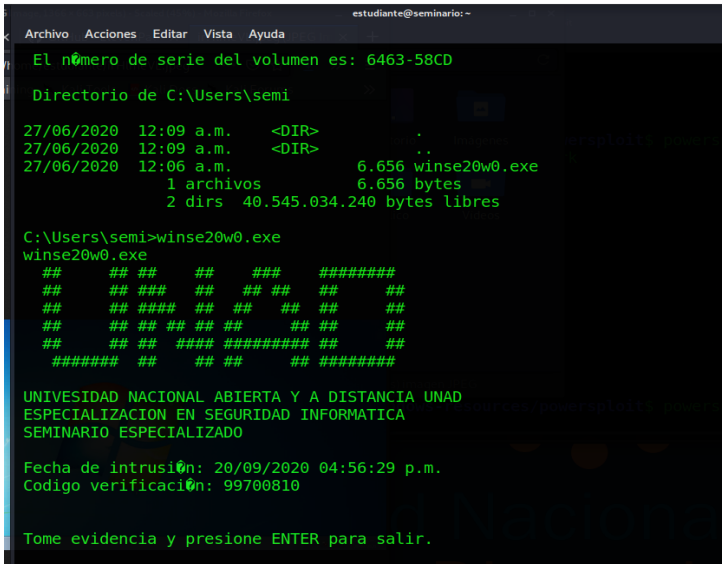
Figura 5. Comprobación de ruta en el sistema remoto



Fuente Autor

Una vez se revisaron los directorios en el equipo vulnerado se encontró y se ejecutó el archivo de fuga de información el cual se muestra en la Figura 6.

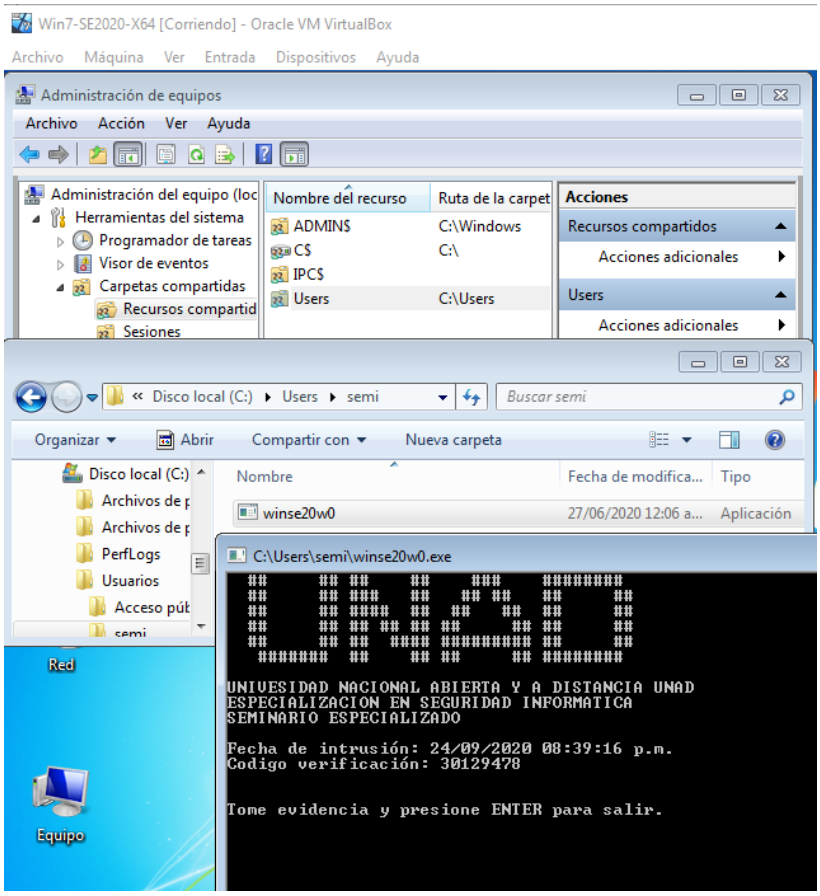
Figura 6. Evidencia de ejecución remota del archivo de fuga de información



Fuente Autor

Como dato adicional se evidenció una mala práctica en el equipo vulnerado, la de compartir la carpeta usuarios, ya que esto si no es bien administrado permite el acceso a la información de los usuarios del equipo tal como se puede observar en la Figura 7.

Figura 7. Malas prácticas compartir carpeta usuarios



Fuente Autor

Al terminar las pruebas de ejecución del exploit se pudo concluir que la vulnerabilidad que si bien se presentaba en ambas maquinas Windows 7, la unica que fue posible vulnerar fue la Windows 7 x64 tal como se observa en la Tabla 5.

Tabla 5. Estado de ejecución del exploit

WINDOWS 7 x64	WINDOWS 7 x86
Maquina donde se concretó la ejecución exitosa del exploit smb/ms17_010_eternalblue	Maquina vulnerable pero que no fue posible concretar la ejecución exitosa del exploit smb/ms17_010_eternalblue

Dirección ip: 10.10.10.2	Dirección ip: 10.10.10.3
Dirección ip atacante: 10.10.10.1	Dirección ip atacante: 10.10.10.1
Protocolo vulnerable: SMBv1	Protocolo vulnerable: SMBv1

Fuente Autor

5. CONCLUSIONES

Se aplicaron los conocimientos y habilidades adquiridas mediante la determinación de la Importancia de contar con información de primera mano para el análisis de la situación a nivel de fallos de seguridad

Mediante la metodología de recopilación de información se denotaron las clases de fallos generados de un tipo de vulnerabilidad

Mediante los escaneos de sistemas se pueden generar métodos de hardenización y pentesting para su aplicación y analisis de los sistemas minimizando la posibilidad de ejecuciones de exploits siendo de gran importancia y como objetivo primordial de los equipos Redteam Blueteam

6. RECOMENDACIONES

Instalación del parche de seguridad que Microsoft lanzó el 14 de marzo de 2017 con el nombre MS17-010 donde se realiza la corrección de la vulnerabilidad sobre el protocolo SMB v1 y actualizar a la más reciente versión de parches de seguridad.

Activación del firewall de Windows dejando activos solo los puertos que sean necesarios para las aplicaciones las cuales solo corren en esta versión de Windows.

Si no se dispone de antivirus y presupuesto para ello, montar una versión actualizada de Microsoft security essentials o un antivirus gratuito como puede ser el avast free con la activación de protección en tiempo real.

Creación de un usuario nuevo con perfil administrador, deshabilitar el usuario administrador local y el usuario invitado.

Revisar si está la cuenta de acceso del grupo todos y quitar esa cuenta del equipo.

Si es necesario que algunos usuarios tengan acceso a archivos compartidos del equipo se crearía una carpeta compartida con permisos de seguridad de solo lectura para cada usuario.

Aplicación, creación o contratación de una consultoría a nivel de BLUETEAM dentro de la empresa para verificación de seguridad y aplicación de políticas o directivas a nivel corporativo donde se ejecuten y definan buenas prácticas a nivel de aseguramiento de los sistemas o en su defecto realizarla con una periodicidad trimestral.

BIBLIOGRAFÍA

AZUAX. {En línea}. {Consultado Octubre 2020}. El Reporte Técnico De Un Pentest. Disponible en: https://www.azuax.com/2017/6/13/el-reporte-tecnico-de-un-pentest/index.html

BLACKMANTISECURITY. {En línea}. {Consultado Octubre 2020}. Introducción al Red Team. Disponible en: https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

COMPUTING. {En línea}. Necesitas un “Purple Team” para el uso efectivo de escenarios de “Red Team”. {Consultado Octubre 2020}. Disponible en: https://www.computing.es/seguridad/opinion/1112071002501/necesitas-purple-team-uso-efectivo-de-escenarios-de-red-team.1.html

CVE-2017-0144. {En línea}. Alerta temprana vulnerabilidades. {Consultado Octubre 2020}. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

CVE MITRE. {En línea}. Common Vulnerabilities and Exposures. {Consultado Octubre 2020}. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

CYTOMIC. {En línea}. Red Team – Blue Team, la simulación estratégica y preventiva. {Consultado Octubre 2020}. Disponible en: https://www.cytomic.ai/es/threat-hunting/simulacion-red-team-blue-team

ESIC BUSSINES MARKETING SCHOOL. {En línea}. Red team: qué es, estrategias y ejemplo de un caso real. {Consultado Octubre 2020}. Disponible en: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

GITHUB. {En línea}. Public-Pentesting-Reports. Disponible en: https://github.com/juliocesarfort/public-pentesting-reports

INFOSECINSTITUTE. {En línea}. The Art of Writing Penetration Test Reports. {Consultado Octubre 2020}. Disponible en:

https://resources.infosecinstitute.com/writing-penetration-testing-reports/

IT SECURITY TOOLS. {En línea}. CVE-2017-0143 | Metasploit | Kali Linux MS17-010 EternalBlue. {Consultado Octubre 2020}. Disponible en: https://www.youtube.com/watch?v=x6EWQ2lsumA&ab_channel=ITSecuritytools

INNOTEC.SECURITY. {En línea}. Equipo Red Team, de Entelgy Innotec: como poner a prueba las capacidades de defensa. {Consultado Octubre 2020}. Disponible en: https://innotec.security/documentos/medios/2019SIC133_168-169.pdf

MKIT. {En línea}. Red Team Operations. {Consultado Octubre 2020}. Disponible en: https://mkit.com/es/services/red-team-operations

OFFENSIVE-SECURITY. {En línea}. Penetration Test Report. {Consultado Octubre 2020}. Disponible en: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

OFFENSIVE SECURITY. {En línea}. Scanner Smb Auxiliary Modules. {Consultado Octubre 2020}. Disponible en: https://www.offensive-security.com/metasploit-unleashed/scanner-smb-auxiliary-modules/

RIDGESECURITY. {En línea}. Audit report generated by ridgebot metafull. {Consultado Octubre 2020}. Disponible en: https://.ai/wp-content/uploads/Metasploitable_2_Test_by_RidgeBot_07282020.pdf

SECURITYARTWORK. {En línea}. Test de intrusión informe de resultados. {Consultado Octubre 2020}. Disponible en: https://www.securityartwork.es/2013/07/17/test-de-intrusion-informe-de-resultados/

SANS INSTITUTE. {En línea}. Information Security Reading Room. Disponible en: https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

SEGURIDADXREDES. {En línea}. Pentesting (V): Informe. {Consultado Octubre 2020}. Disponible en: http://seguridadxredes.blogspot.com/2015/11/pentesting-v-informe.html

TÉRMINOS Y CONDICIONES. {En línea}. Derecho tecnológico y Legaltech. {Consultado Octubre 2020}. Disponible en: https://terminosycondiciones.es/2019/04/23/como-redactar-un-contrato-de-pentesting/

UNAD. Anexo4 – Escenario3. {En línea}. {Consultado Octubre 2020}. Disponible en: https://campus102.unad.edu.co/ecbti81/pluginfile.php/2915/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

UNAD. Anexo 5 - Escenario 4. {En línea}. {Consultado Octubre 2020}. Disponible en: https://campus102.unad.edu.co/ecbti81/pluginfile.php/2917/mod_folder/content/0/Anexo%205%20-%20Escenario%204.pdf?forcedownload=1

UNIR INGENIERÍA Y TECNOLOGÍA. {En línea}. Revista Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?. {Consultado Octubre 2020}. Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

WIZLYNXGROUP. {En línea}. Servicio de Simulación de Amenazas Red Team. {Consultado Octubre 2020}. Disponible en: https://www.wizlynxgroup.com/mx/ciberseguridad-mexico/servicio-simulacion-de-amenazas-red-team

LINK DE VIDEO

https://youtu.be/Kcqct8ynW9k