Laboratorio
FUNDAMENTOS DE CIBERSEGURIDAD
Profesor: Juan Ignacio Iturbe A.

Laboratorio 3. Análisis de vulnerabilidades y ganando acceso

Exigencia 70%

1. INTRODUCCIÓN[1]

EC-Council ha definido el ethical hacking con cinco fases. Ya sea que el atacante sea ético o malicioso, estas cinco fases capturan todo el alcance del ataque. Estas etapas son: reconocimiento, scanning y enumeración, ganando acceso, mantener el acceso y cubriendo huellas. En el presente laboratorio se revisará principalmente la segunda y tercera fase.

En el *scanning y enumeración*, los profesionales de seguridad toman la información que recopilaron para reconocer y aplicar activamente herramientas y técnicas para recopilar información más detallada sobre los objetivos. Esto puede ser algo tan simple como ejecutar un barrido de ping o un mapeador de red para ver qué sistemas hay en la red, o tan complejo como ejecutar un escáner de vulnerabilidades para determinar qué puertos pueden estar abiertos en un sistema en particular. Por ejemplo, mientras que el reconocimiento puede haber mostrado que la red tiene más o menos 500 máquinas conectadas a una única subred dentro de un edificio, el escaneo y la enumeración le dirán cuáles son máquinas de Windows y cuáles ejecutan FTP.

La tercera fase, *ganando acceso*, como dicen, es donde ocurre la magia. Esta es la fase en la que la mayoría de las personas se frotan encantadas, deleitándose con la alegría que saben que recibirán al pasar por alto un control de seguridad. En la fase de ganando de acceso, ataques verdaderos están dirigidos contra los objetivos enumerados en la segunda fase. Estos ataques pueden ser tan simples como acceder a un punto de acceso inalámbrico abierto y no seguro y luego manipularlo para cualquier propósito, o tan complejo como escribir y entregar un desbordamiento de búfer o una inyección de SQL en una aplicación web.

[1] El presente texto introductorio es una traducción libre de un extracto del libro de Walker, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. McGraw-Hill Education.

2. ESCENARIO

Se supondrá que todos los grupos obtuvieron la siguiente información en la etapa de reconocimiento respecto de los sistemas de la empresa objetivo:

- En un anuncio en LinkedIn se publicó la búsqueda de Ingenieros de sistemas con experiencia en migración de sistemas Ubuntu Server 14.04 LTS a la versión 20.04 LTS y desde Microsoft Windows Server 2008 R2 a la versión Microsoft Windows Server 2019.
- El manejo de las cuentas de VPN no es muy restrictivo, por lo que, a través de ingeniería social, ha podido obtener una cuenta VPN de un empleado, con la cual tiene acceso a la LAN de la empresa.
- Se observa que la empresa entrega diversos tipos de servicios a clientes los cuales son administrados por ellos mismos.

3. HERRAMIENTAS

En el presente trabajo se recomienda utilizar las siguientes herramientas:

- **Metasploitable 3:** Con esta herramienta conseguiremos máquinas virtuales con servicios vulnerables. Un buen manual de instalación de metasploitable 3 se encuentra en [1] .
- **Virtualbox:** En esta herramienta se montan las máquinas virtuales. Se puede descargar en [2].
- **Nmap:** Con esta herramienta se realiza el escaneo de puertos y otros. Se puede descargar en [3] o en Kali Linux viene por defecto.
- **Wireshark:** Con esta herramienta se realizará sniffing de los paquetes que se dirijan y vuelvan desde el servidor. Se puede descargar en [4] o en Kali Linux viene por defecto.
- **OpenVAS/GVM o Nessus:** Es un escáner de seguridad de la red con herramientas asociadas como una interfaz gráfica de usuario. El componente central es un servidor con un conjunto de pruebas de vulnerabilidad de la red para detectar problemas de seguridad en sistemas y aplicaciones remotas. GVM viene con Kali Linux y Nessus es comercial por lo que se debe bajar desde [6].
- **OWASP ZAP:** Analizador de vulnerabilidades web.
- **Kali Linux - Metasploit Framework:** Con esta herramienta se desarrollará la etapa de ganando acceso. Se puede descargar en [5] o en Kali Linux viene por defecto.

Se pueden utilizar otras herramientas como Acunetix, Core Impact, Burp Suite, u otras

herramientas comerciales en sus versiones *trials o* gratuitas. La utilización de estas herramientas se considerará en la rúbrica de evaluación.

4. INSTRUCCIONES

En el presente laboratorio se debe desarrollar parte de la segunda y tercera etapa del hacking ético. El objetivo del ataque será obtener la administración completa de un equipo. Para ello debe seguir las siguientes instrucciones:

a. Se debe preparar un ambiente simulado de la empresa en cuestión. Para ello puede utilizar metasploitable y Virtualbox siguiendo las instrucciones del tutorial referenciado.
b. Una vez que haya instalado dicho ambiente, se encontrará con dos sistemas operativos instalados en Virtualbox. Debe elegir uno a analizar.
c. Escaneo
    i. Realice un escaneo de puertos (nmap) sobre el sistema escogido, utilizando por lo menos 3 de sus opciones.
    ii. Use nmap para determinar cuáles son los servicios disponibles y sus versiones.
d. Análisis de vulnerabilidades
    i. Escoja y describa las herramientas a utilizar para realizar el presente análisis.
    ii. Analice las vulnerabilidades del equipo objetivo.
    iii. Revise bibliografía respecto a las características de la vulnerabilidad.
e. Ganando acceso:
    i. Indague si estos servicios se encuentran vulnerables y si tienen un exploit disponible para utilizar en metasploit.
    ii. Ejecute los exploits disponibles en metasploit sobre el servicio seleccionado.
    iii. En caso de que el ataque no sea exitoso, vuelva a intentarlo con otro exploit, vulnerabilidad u otro servicio de la máquina (al menos 3 intentos no exitosos, 1 exitoso).
f. Para verificar que el ataque fue exitoso, debe colocar en el escritorio del administrador un archivo cualquiera.

5. ENTREGA

La entrega corresponde a la presentación de lo desarrollado anteriormente en formato de video. Es importante que la presentación tenga un hilo conductor y se vaya desarrollando coherentemente a medida que se incorporan nuevos elementos. En total, el video no debe sobrepasar los 20 minutos.

Se sugiere la utilización de herramientas de edición de video para mejorar la presentación del video. Estas herramientas le permitirán eliminar tiempos muertos en el video, repartir la grabación entre los integrantes del grupo, agregar elementos gráficos y de texto al video entre otros. Se bonificará la buena utilización de este tipo de herramientas.

6. RÚBRICA

Descripción	**Puntaje**
Presenta introducción acorde al trabajo	40
Los conceptos se explican de forma correcta	20
Realiza la actividad de acuerdo a las instrucciones indicadas	30
Indica todos los supuestos requeridos.	20
Contextualiza el laboratorio indicando las etapas del hacking ético y profundizando en las que se explorarán en el presente.	30
Describe de forma genérica las vulnerabilidades a explotar.	20
Describe los exploit específicos utilizados.	20
Explica de forma genérica los comandos utilizados. Indica detalles del funcionamiento interno.	20
Configura adecuadamente y sin problemas el ambiente simulado	40
Realiza el escaneo de puertos (nmap) sobre el sistema escogido, utilizando por lo menos 3 de sus opciones.	20
Usa nmap para determinar cuáles son los servicios disponibles y sus versiones	20
Utiliza más de dos herramientas de análisis de vulnerabilidades y las describe correctamente.	20
Muestra los resultados obtenidos desde las herramientas y estos son	20

consistentes con lo afirmado.	
Gana el acceso de la máquina o tiene al menos 3 intentos fallidos correctamente ejecutados.	40
Entrega evidencia del éxito del ataque.	40
Desarrolla conclusión de acuerdo a los resultados obtenidos.	40
Incluye bibliografía y la utiliza para soportar sus afirmaciones.	20
Incluye evidencia que sustenta la información obtenida.	30
Se respeta el tiempo de la presentación (15 a 20 minutos máximo, entre la introducción, desarrollo y conclusión).	10
Se indica el integrante del grupo que está hablando en cada momento.	10
El video presenta figuras de acuerdo al contenido y un audio claro.	20

BIBLIOGRAFÍA

1. Metasploitable 3, Instalación en GNU/Linux, Windows y Mac OS, https://www.dragonjar.org/metasploitable-3-instalacion-en-gnulinux-windows-y-mac-os.xhtml , último acceso: 07/01/2022
2. Virtualbox, https://www.virtualbox.org/, último acceso: 07/01/2022
3. Nmap, https://nmap.org/, último acceso: 07/01/2022
4. Wireshark, https://www.wireshark.org/, último acceso: 07/01/2022
5. Kali Linux, https://www.kali.org/, último acceso: 07/01/2022
6. Nessus, https://www.tenable.com/products/nessus, último acceso: 22/07/2021