Seguridad Informática – 2023

PROFESOR TITULAR: Mag. Ing. Bruno Roberti.
JEFE DE TRABAJOS PRÁCTICOS: Mag. Lic. Rosana Gimenez.

TRABAJO PRÁCTICO UNIDAD 2
VULNERABILIDADES

Presentación/Introducción

El Trabajo Práctico N° 2 propone la introducción del estudiante a los procedimientos y herramientas necesarios para la realización de un Test de Penetración.

Objetivos

El objetivo de esta entrega es que el estudiante sea capaz de realizar etapas asociadas a la realización de un test de penetración sobre un equipo corriendo la máquina virtual METASPLOITABLE2 y presentar evidencias de lo realizado.

Recursos

Para la realización de este TP es necesario haber estudiado y consultado los siguientes recursos presentes en el aula virtual de la asignatura:

- Guía “INSTALACION ZENMAP-OpenVAS-DIKTO en KALI”
- https://nmap.org/man/es/index.html
- https://docs.greenbone.net/GSM-Manual/gos-22.04/en/
- https://www.offsec.com/metasploit-unleashed/
- Apunte “OWASP Top 10 2021”
- https://owasp.org/www-project-top-ten/
- https://owasp.org/www-project-web-security-testing-guide/stable/

Además se debe instalar un laboratorio de práctica con el siguiente software:

- Virtual Box 6.1 o superior
- Máquina Virtual Kali 2021.1 o superior con las siguientes herramientas instaladas:
    - Última versión estable de NMap/ZenMap
    - Última versión estable de OpenVas/GMV
    - Última versión estable de Metasploit
- Maquina virtual “Metasploitable 2” (https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)

Formato y fecha de presentación/entrega

20/10/2023

Descripción:

En este ejercicio tomáis el papel de un experto en Seguridad Informática que ayuda al auditor jefe a cargo de elaborar el informe de una auditoría.

Recuerde adjuntar como papel de trabajo las pantallas de salida de la ejecución de las herramientas y toda otra salida que proporcionen las mismas y considere útil para demostrar la correcta utilización de las mismas y facilitar la generación del informe de auditoría.

El experto en seguridad informática debe realizar las pruebas técnicas de la auditoría que se ha encargado y las cuales se encuentran detalladas a continuación:

EJERCICIO A – Explotación Vulnerabilidades SO

A.1- Despliegue el entorno de trabajo del auditor y la aplicación a auditar, tenga en cuenta que ambos entornos deben poder comunicarse entre sí a través de la red

A.2- Realice un escaneo IP de la red donde se encuentran ambos equipos (auditor y auditado); identifique la IP del equipo a auditar

A.3- Realice acciones de fingerprinting para obtener la mayor información posible sobre el equipo auditado.

A.4- Realice acciones de escaneo de puertos para identificar los puertos expuestos en el equipo analizado). Se recomienda utilizar herramientas como Nmap y módulos de Metasploit como auxiliary/scanner/portscan/tcp

A.5- Realice un listado de puertos, servicios y versiones que se están ejecutando en el equipo analizado.

A.6- Utilice OpenVAS / Greenbone Vulnerability Management para realizar un escaneo en busca de vulnerabilidades del equipo auditado. Documente las configuraciones utilizadas para el escaneo.

A.7- Realice un listado de las principales vulnerabilidades de cada uno de los elementos identificados en el punto A.5, que incluya su código CVE y su enlace a la página Exploit-db (https://www.exploit-db.com)

A.8- Realice la explotación mediante Metasploit de las siguientes vulnerabilidades detectadas en el equipo analizado, de acuerdo al siguiente detalle:

- Explote un servicio con clave débil
- Ejecute un backdoor
- Obtenga una sesión en el servidor mediante un exploit que no sea del tipo 1 y 2
- Realice una conexión mediante un servicio de acceso remoto
- Realice el escalamiento de privilegios en una sesión
- Acceda a los datos de uno de los servidores SQL

Adjunte pruebas del resultado de cada explotación realizada, incluyendo identificación de la vulnerabilidad explotada y los pasos ejecutados.

EJERCICIO B – Explotación Vulnerabilidades Web

B.1- En base al listado de puertos y servicios verifique los sitios webs publicados en la dirección IP del equipo.

B.2- Realice un reconocimiento de los sitios web instalados en el equipo analizado. Identifique cuales de las vulnerabilidades detectadas en el punto A.6 se aplican a estos sitios. Realice un listado de sitios identificados en el servidor.

B.3- Dentro de la aplicación DVWA coloque el nivel de seguridad en bajo y navegu la misma para conocer su funcionalidad.

B.4- Realice la explotación con nivel de seguridad bajo de las siguientes vulnerabilidades implementadas en la aplicación DVWA:

- Brute Force
- File Upload

Adjunte pruebas del resultado de cada explotación realizada, incluyendo identificación de la vulnerabilidad explotada en OWASP y los pasos ejecutados.

B.5- Realice la explotación con nivel de seguridad medio de las siguientes vulnerabilidades implementadas en la aplicación DVWA:

- Command Execution
- File Inclusion

Adjunte pruebas del resultado de cada explotación realizada, incluyendo identificación de la vulnerabilidad explotada en OWASP y los pasos ejecutados.

B.6- Genere una estrategia de penetración sobre la aplicación web DVWA que combine al menos 2 vulnerabilidades analizadas en los puntos B.4 y B.5 para obtener un Shell con privilegios de administrador en el equipo analizado. Detalle y ejecute la estrategia diseñada.