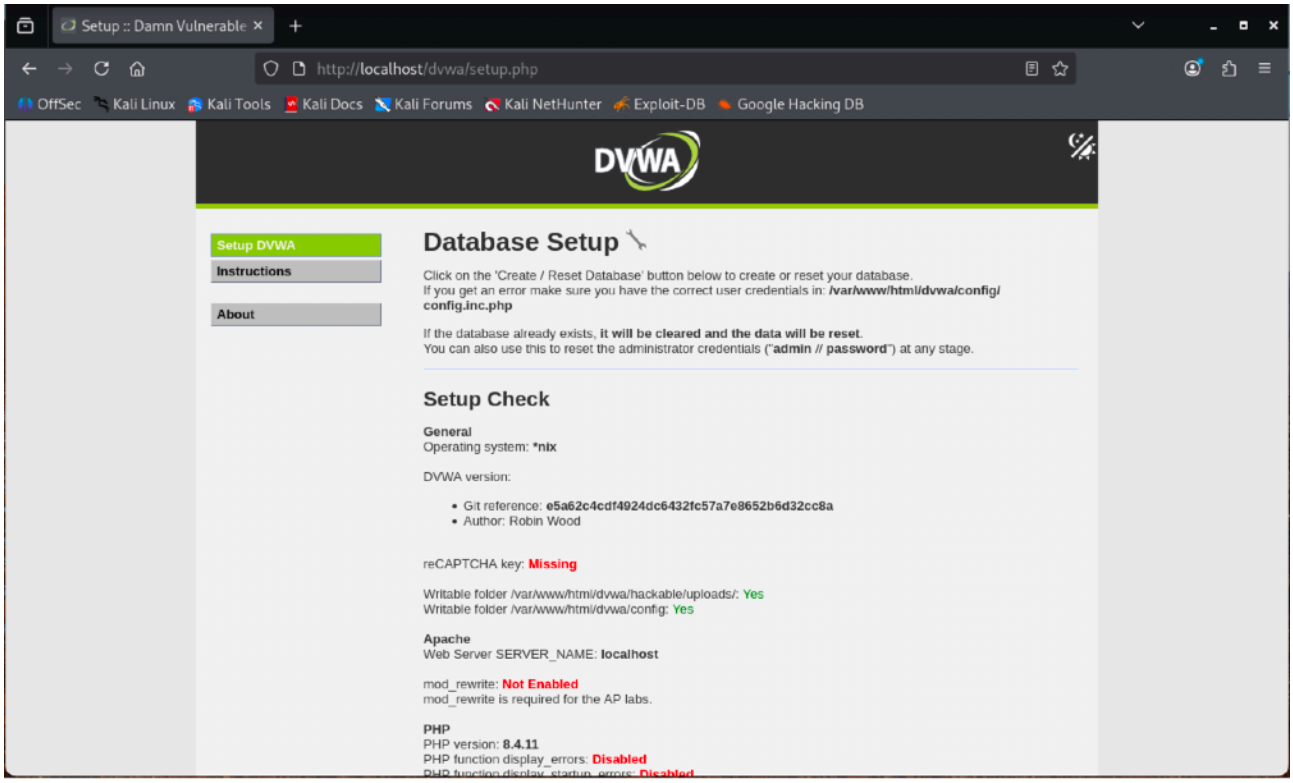
1. Introducción

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).

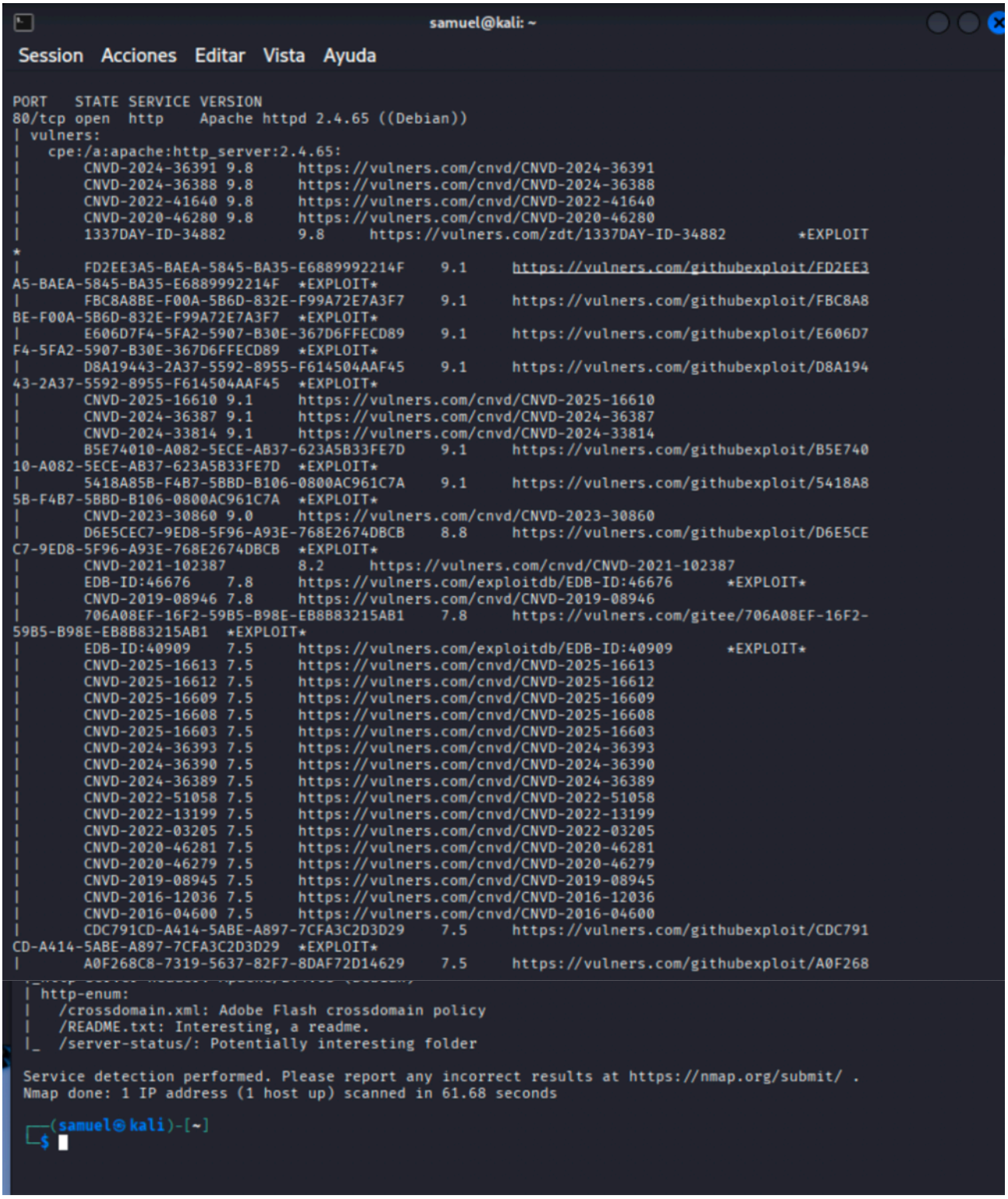


2. Metodología y Herramientas

- **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.



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).

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.