Antes de comenzar verifiqué la identidad y dirección IP de la máquina objetivo.

- Comando ejecutado en la máquina Debian: ip a
- IP Confirmada: 192.168.1.10
- MAC Address: 08:00:27:d1:65:c7

```
debian@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default q
len 1000
    link/ether 08:00:27:d1:65:c7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed1:65c7/64 scope link
       valid_lft forever preferred_lft forever
```

Se realizaron dos niveles de escaneo desde la máquina atacante (Kali Linux) para profundizar en la superficie de exposición.

Escaneo de puertos

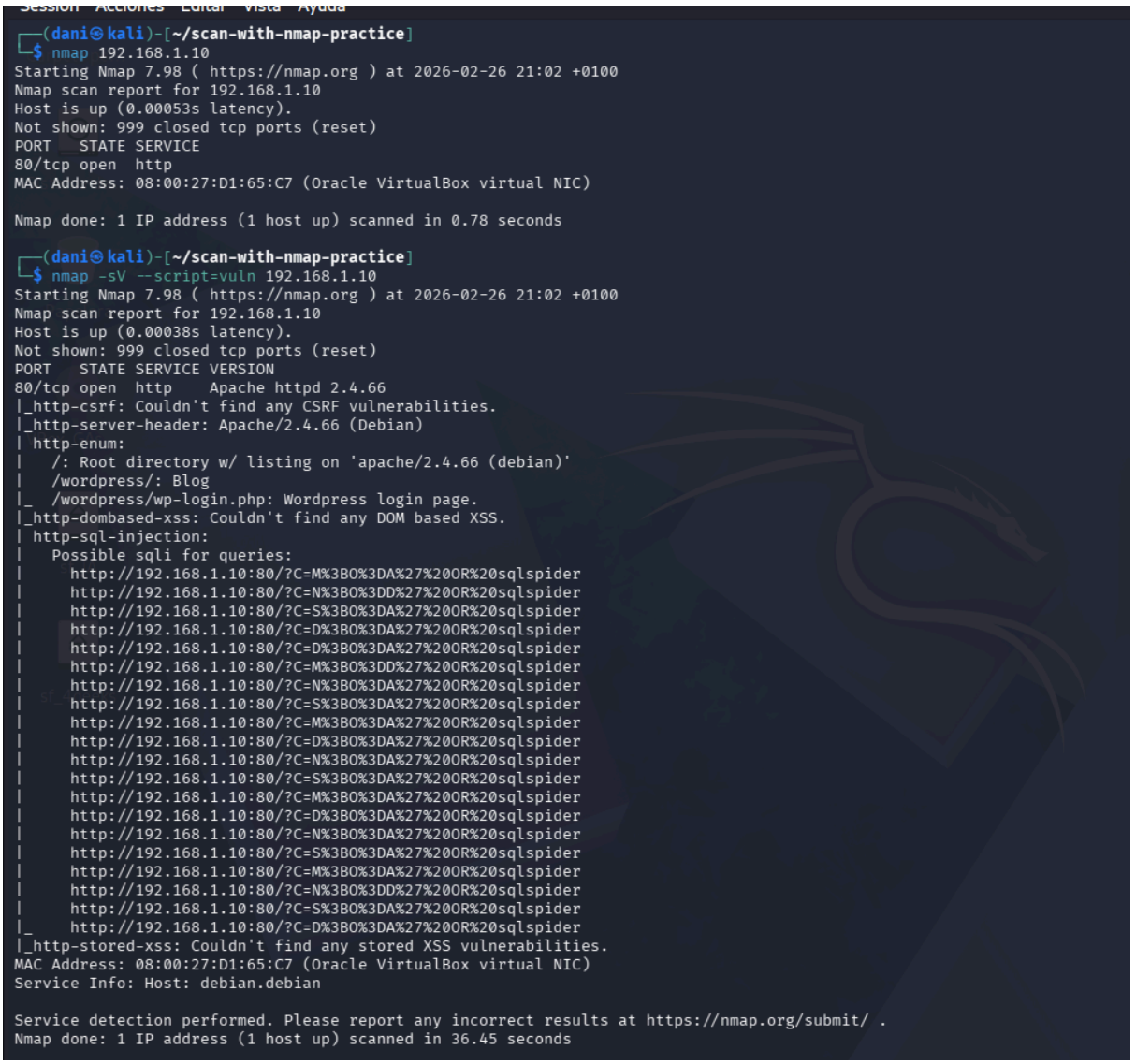
Se identificó el puerto 80/TCP en estado OPEN, ejecutando el servicio HTTP.

Escaneo de versiones y scripts de vulnerabilidades

Se utilizó el comando nmap `-vS --script=vuln 192.168.1.10` para obtener información detallada del servicio y detectar fallos conocidos.

Resultados:

- Servidor: Apache httpd 2.4.66 (Debian).
- Tecnología: WordPress detectado en el directorio `/wordpress/`.
- Página de login: `/wordpress/wp-login.php`.



Análisis de vulnerabilidades detectadas

Exposición de Directorios (Information Disclosure)

El script `http-enum` reveló que el listado de directorios está habilitado en la raíz del servidor. Esto permite a un actor malintencionado navegar por la estructura de archivos y localizar archivos de configuración o backups sensibles.

Posible Inyección SQL (SQLi)

El motor de scripts de Nmap identificó parámetros vulnerables a inyección SQL.

- Evidencia: `http://192.168.1.10:80/?C=M%3BO%3DA%27%20OR%20sqlspider`
- Impacto: Un atacante podría manipular las consultas a la base de datos para extraer información confidencial o evadir la autenticación del sitio.

Vulnerabilidad de versión (CVE-2024-40725)

La versión detectada (Apache 2.4.66) es susceptible a vulnerabilidades documentadas recientemente que podrían permitir el bypass de ciertas restricciones de seguridad dependiendo de la configuración del servidor.

5. Recomendaciones

1. Desactivar el listado de directorios modificando la directiva en el archivo de configuración (`Options -Indexes`).
2. Actualizar el servidor Apache a la última versión disponible para mitigar el riesgo asociado a CVEs conocidos.
3. Implementar un plugin de seguridad (como Wordfence) y asegurar que los parámetros de entrada estén debidamente sanitizados para prevenir ataques de SQL Injection.