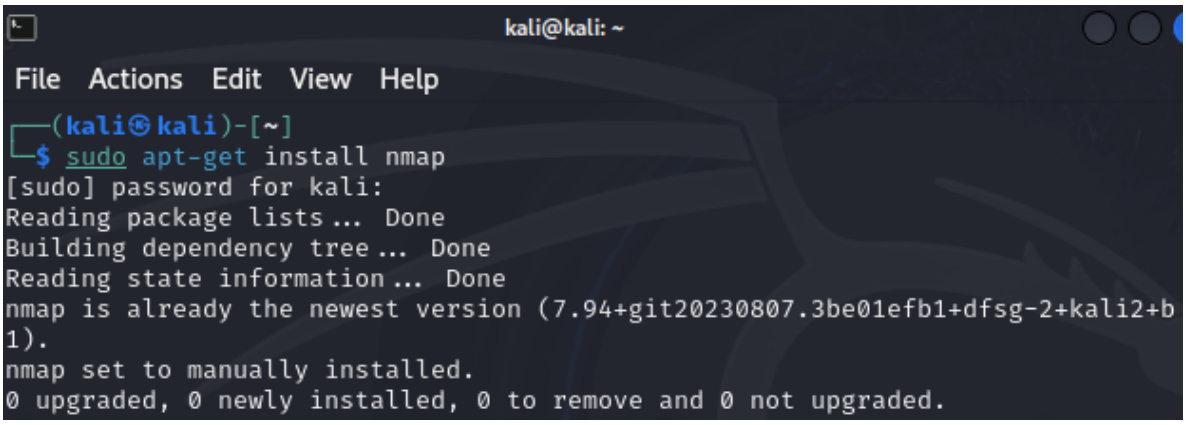
Escanear puertos con nmap

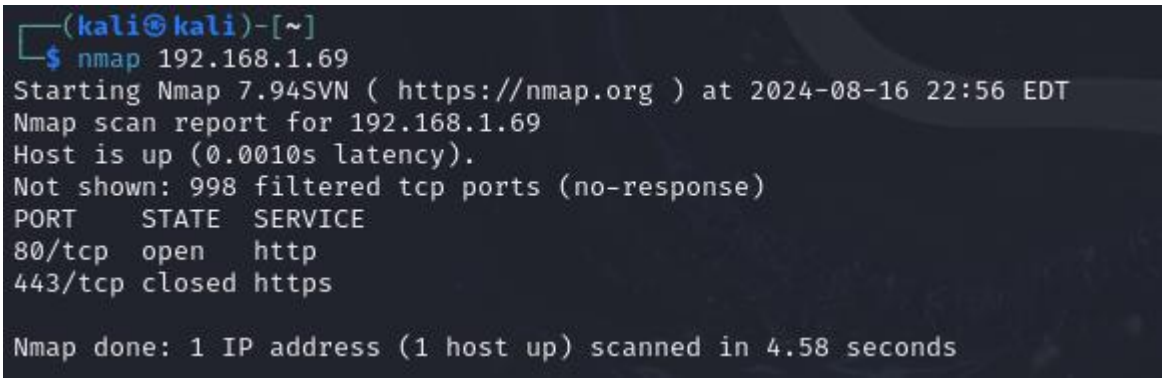
Instalación de Nmap en Kali



Saber cual es la dirección IP de la maquina Debian

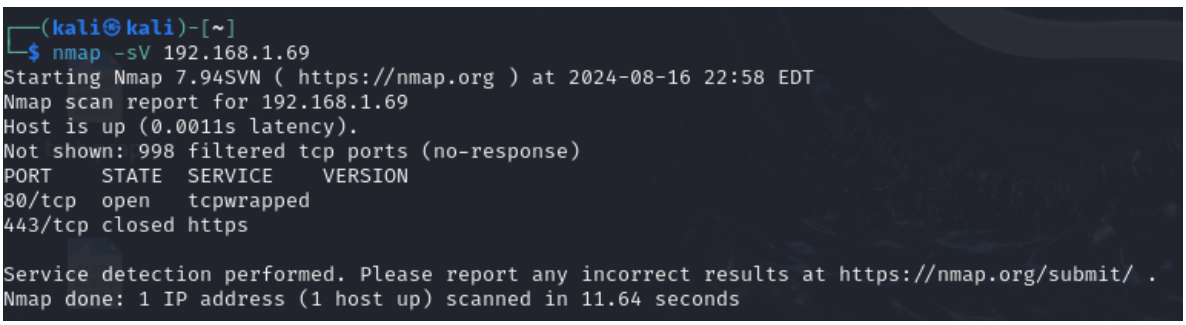
```
deb@debian:~$ hostname -I
192.168.1.69 2806:103e:2f:6d9f:2355:d887:dae0:5bc9 2806:103e:2f:6d9f:4664:34f6:2f6c:f457
deb@debian:~$
```

Escaneo básico de un objetivo (El IP de la maquina debian <IP_debian>):

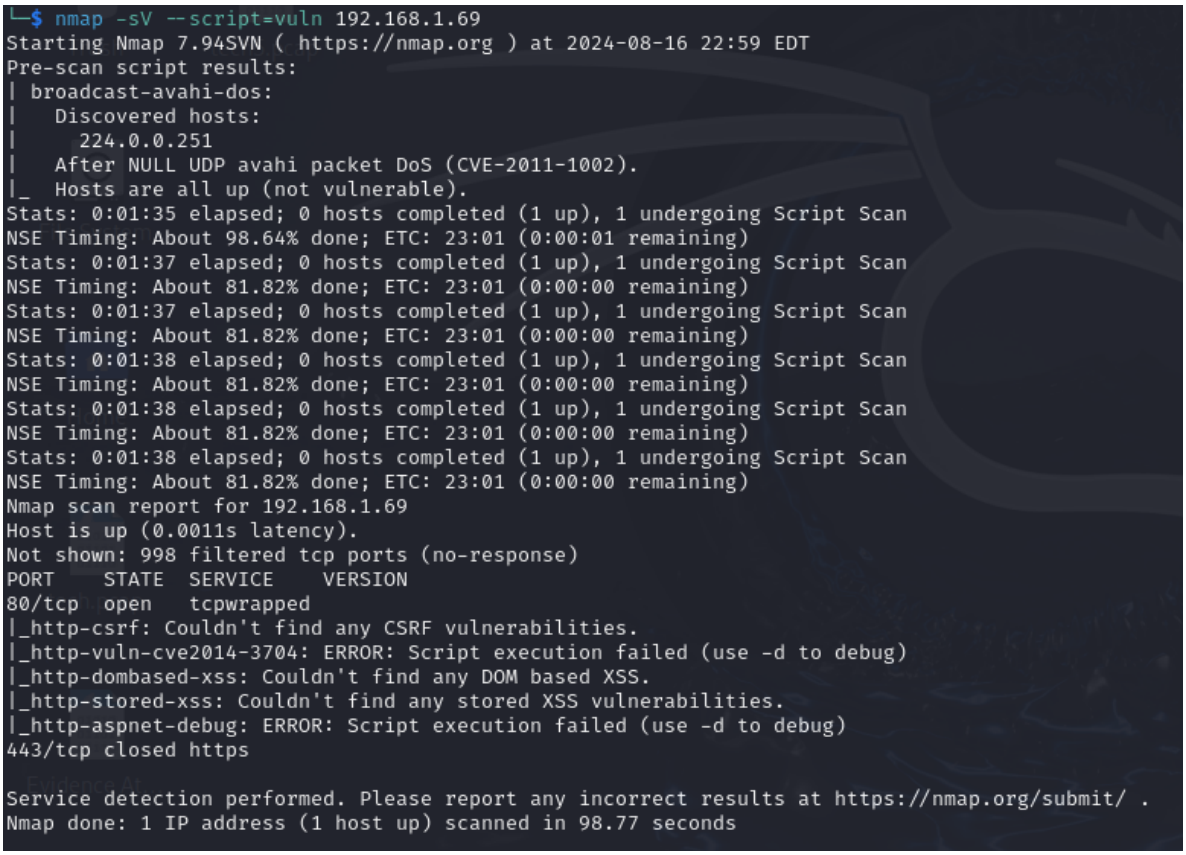


Después de realizar el escaneo, Nmap proporcionará una lista de puertos abiertos y los servicios que operan en esos puertos.

Escaneo de puertos y servicios:



Escaneo detallado y búsqueda de vulnerabilidades:



Documentar Vulnerabilidades Asociadas a los Servicios

http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Exploits CVE-2014-3704 también conocidos como 'Drupageddon' en Drupal. Se sabe que las versiones anteriores a la 7.32 del núcleo de Drupal están afectadas.

La vulnerabilidad permite a atacantes remotos realizar ataques de inyección SQL a través de una matriz que contiene claves creadas.

El script inyecta un nuevo usuario administrador de Drupal a través del formulario de inicio de sesión y luego intenta iniciar sesión como este usuario para determinar si el objetivo es vulnerable. Si ese es el caso, se realizan los siguientes pasos de explotación:

- Está habilitado el módulo de filtro PHP que permite evaluar fragmentos/código PHP incrustados.
- Se ha establecido el permiso para utilizar el código PHP para usuarios administradores.
- Se crea y se previsualiza un nuevo artículo que contiene la carga útil.

- limpieza: de forma predeterminada, se restauran todos los registros de la base de datos que fueron agregados o modificados por el script.

Vulnerabilidad descubierta originalmente por Stefan Horst de SektionEins.

La técnica de explotación utilizada para lograr RCE en el objetivo se basa en el módulo Metasploit exploit/multi/http/drupal_drupageddon.