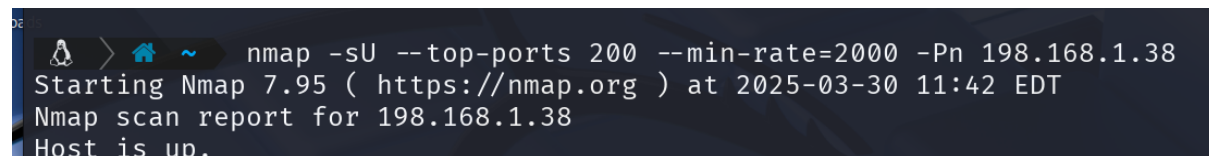


Escaneo de Puertos bajo el Protocolo UDP

Hasta ahora hemos visto escaneo de puerto bajo el protocolo TCP que seria lo mas común, pero puede haber caso que tengamos que hacer escaneo de puerto bajo el protocolo UDP.

```
nmap -sU --top-ports 200 --min-rate=2000 -Pn 198.168.1.38
```

A terminal window with a dark background and light blue text. The prompt is a root user icon followed by a tilde (~). The command entered is 'nmap -sU --top-ports 200 --min-rate=2000 -Pn 198.168.1.38'. The output shows 'Starting Nmap 7.95 (https://nmap.org) at 2025-03-30 11:42 EDT', 'Nmap scan report for 198.168.1.38', and 'Host is up.'

```
nmap -sU --top-ports 200 --min-rate=2000 -Pn 198.168.1.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 11:42 EDT
Nmap scan report for 198.168.1.38
Host is up.
```

nmap : Es la **herramienta** para escanear redes y puertos.

-sU : **Indica un escaneo de puertos UDP**. Esto busca servicios que se ejecuten sobre este protocolo, como DNS (puerto 53) o SNMP (puerto 161). Los escaneos UDP suelen ser más lentos que los de TCP debido a la naturaleza del protocolo.

--top-ports 200 : Le dice a Nmap que **escanee solo los 200 puertos más comunes** en lugar de todos los puertos disponibles. Esto acelera el análisis y se centra en puertos que tienen mayor probabilidad de estar en uso.

--min-rate=200 0 : Establece una **tasa mínima de 2000 paquetes por segundo**. Esto obliga a Nmap a realizar el escaneo de manera más rápida, ideal para sistemas con buena conexión y cuando se necesita un análisis rápido.

-Pn : **Desactiva la comprobación de "Ping"** previa al escaneo. Nmap asumirá que el host está activo incluso si no responde al ping. Es útil cuando el firewall bloquea los paquetes ICMP o cuando el sistema no responde a solicitudes de ping.

198.168.1.38 : Es la **dirección IP** del objetivo que deseas analizar.