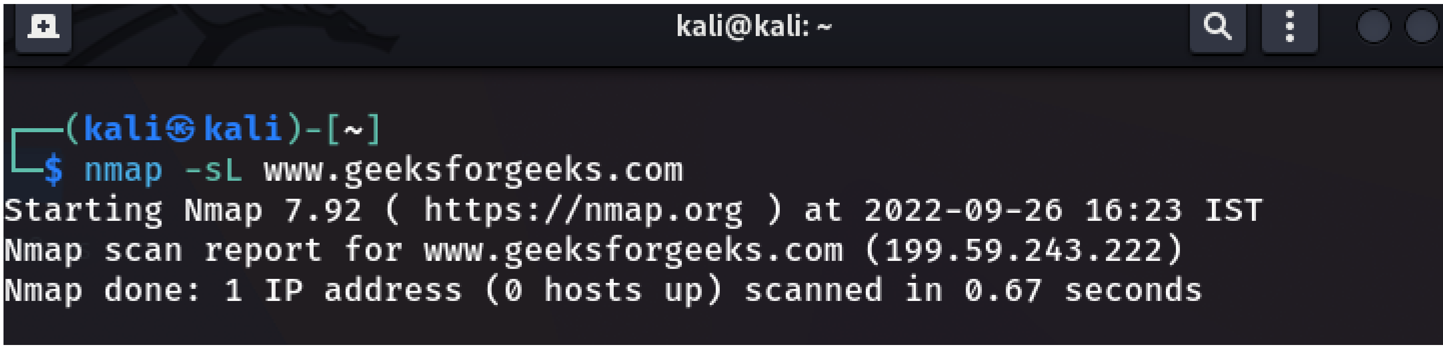
Host Discovery in Nmap Network Scanning

Nmap becomes the primary tool for scanning the network, while other scanner tools still compete with Nmap. Many hosts in the organization are filtered by the firewall which is not detectable in the network. But this can be possible using host discovery using Nmap. Host discovery in Nmap is the process of gathering information about the host in the respective network. Host discovery is also known as ping scan. Nmap uses options like ping or built-in script to look after ports, services, and running servers on respective IPs using TCP and UDP. This may lead to further enumeration.

The function of Host discovery in Nmap:

- **List Scan:** A list scan generally lists the possible host without sending any packets to the targeted host.

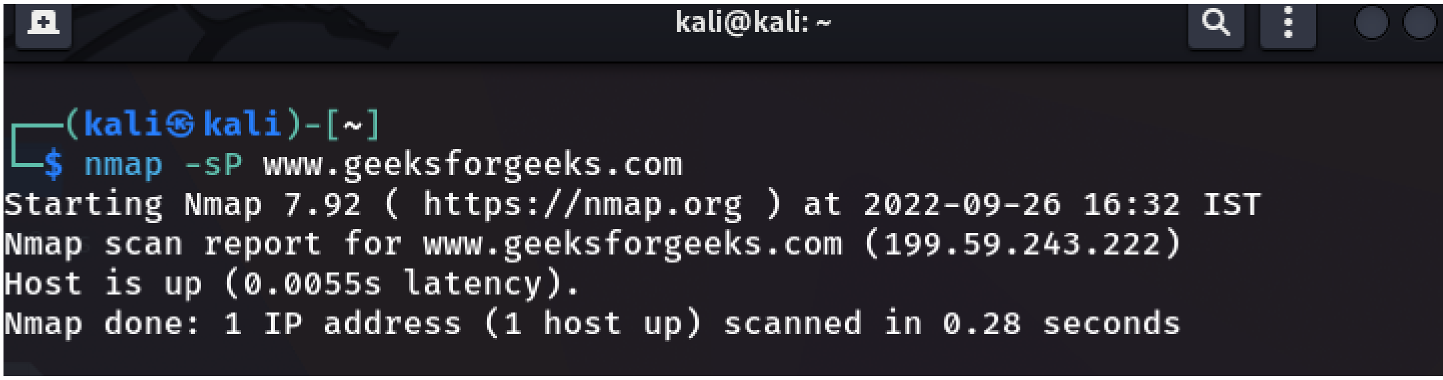
nmap -sL www.geeksforgeeks.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sL www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:23 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Nmap done: 1 IP address (0 hosts up) scanned in 0.67 seconds
```

- **Ping Sweep:** Ping sweep discovers on the basis the host is powered on.

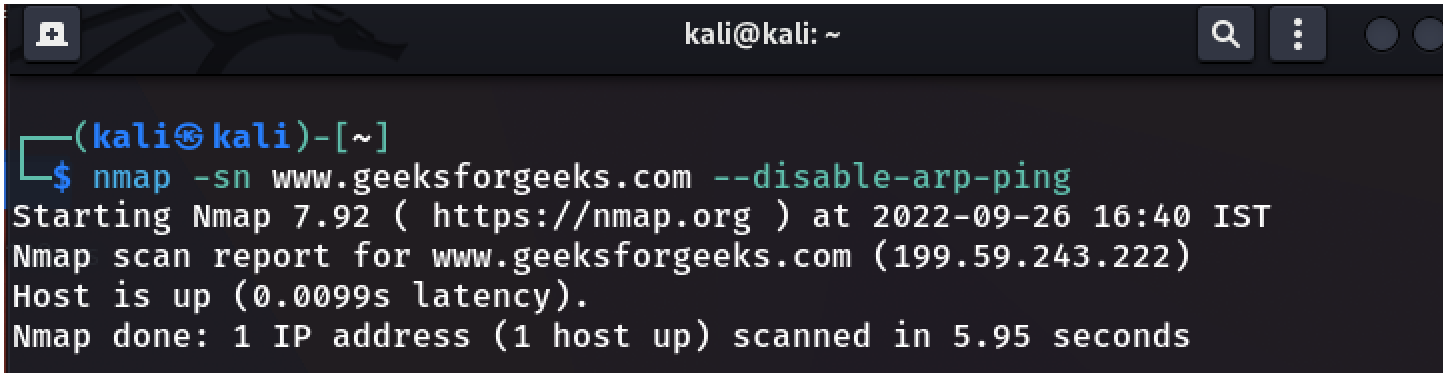
nmap -sP www.geeksforgeeks.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:32 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0055s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

- **Disable ARP Ping:** Nmap mostly uses ARP ping to discover the other host in the network. To disable ARP Ping, use option –disable-arp-ping.

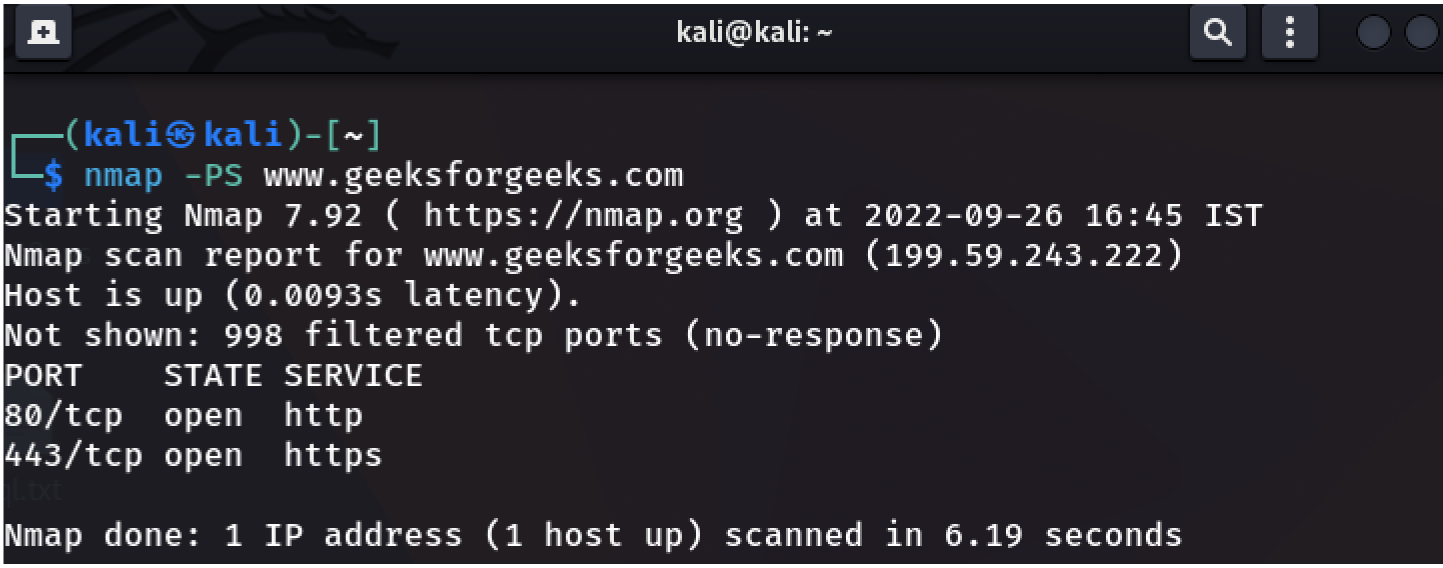
nmap -sn www.geeksforgeeks.com –disable-arp-ping



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn www.geeksforgeeks.com --disable-arp-ping
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:40 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0099s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds
```

- **TCP SYN Ping:** Nmap checks whether a host is online.

nmap -PS www.geeksforgeeks.com

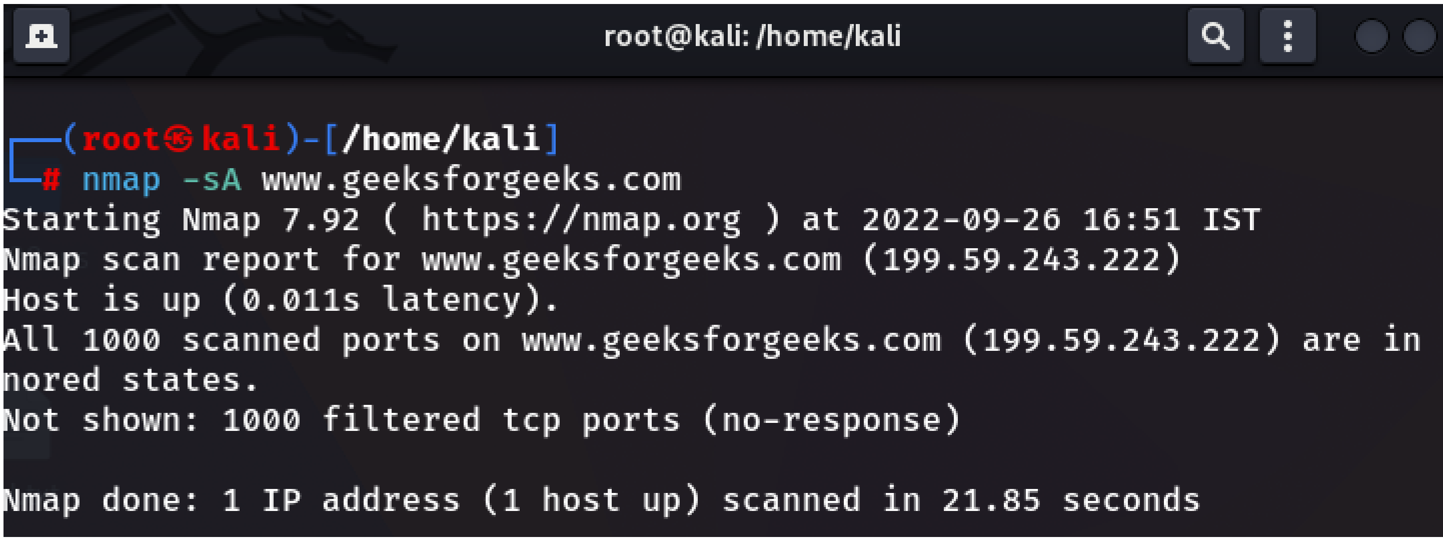


```
┌──(kali㉿kali)-[~]
└─$ nmap -PS www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:45 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0093s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

- **TCP ACK Ping:** Nmap checks whether the host is responding.

nmap -sA www.geeksforgeeks.com

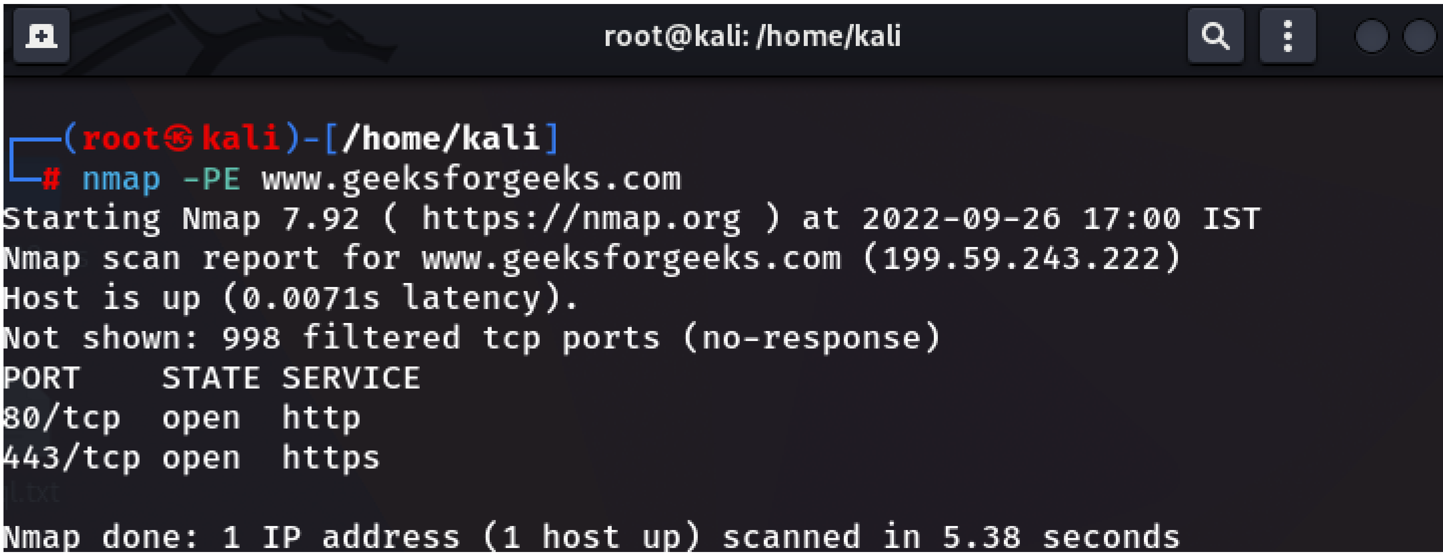


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:51 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.011s latency).
All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in
nored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
```

- **ICMP Echo Ping:** Nmap sends ICMP packets to the available host.

nmap -PE www.geeksforgeeks.com

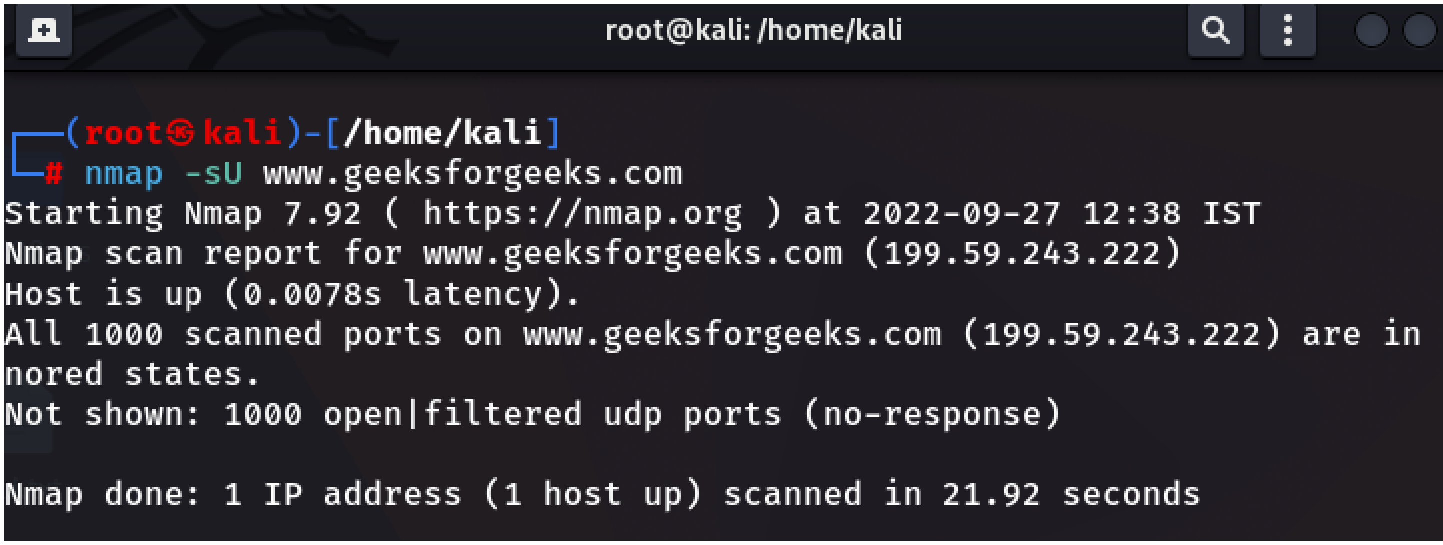


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PE www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 17:00 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0071s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds
```

- **UDP Ping:** Nmap sends the UDP packets to the targeted port.

nmap -sU www.geeksforgeeks.com

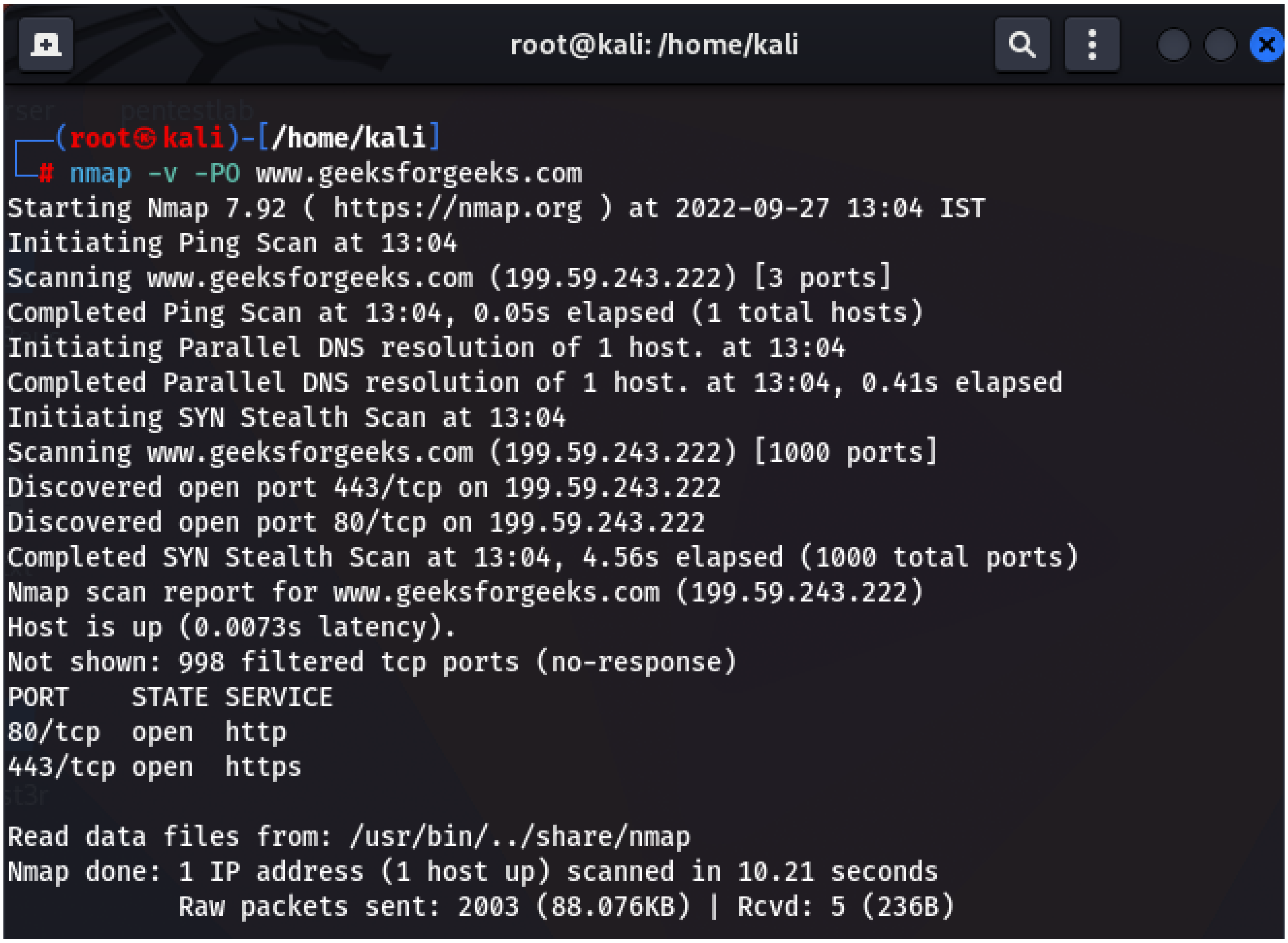


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 12:38 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0078s latency).
All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in
nored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds
```

- **IP Protocol Ping:** Nmap tries to send different packets using different protocols.

nmap -v -PO www.geeksforgeeks.com

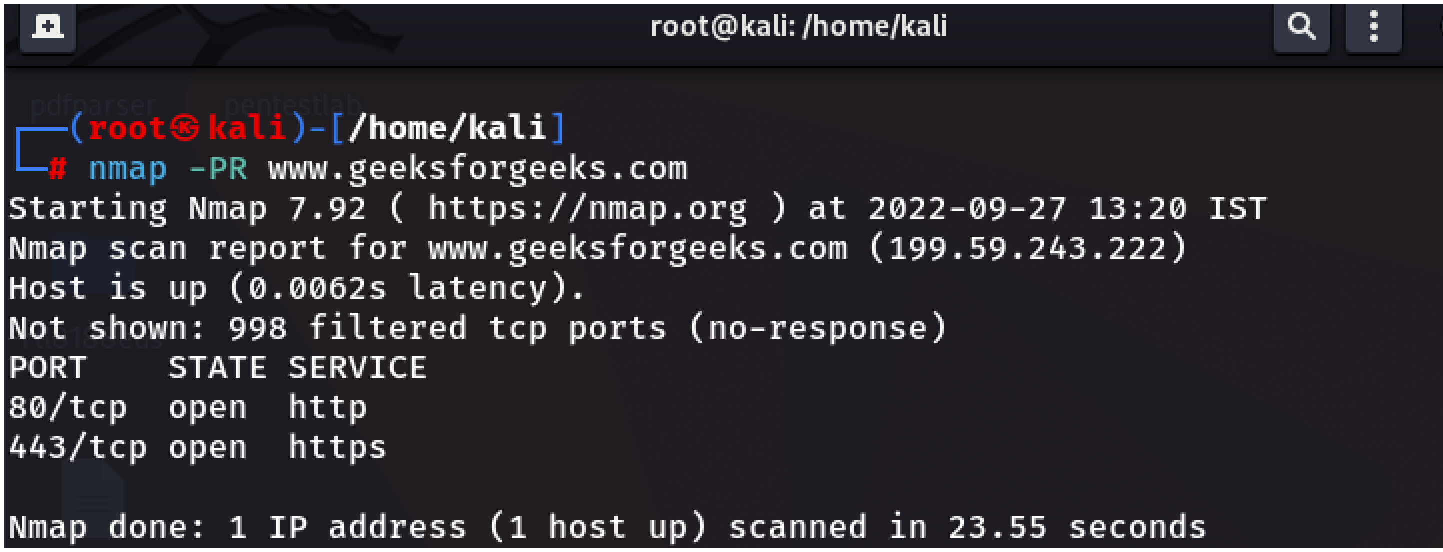


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -PO www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:04 IST
Initiating Ping Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [3 ports]
Completed Ping Scan at 13:04, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.41s elapsed
Initiating SYN Stealth Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [1000 ports]
Discovered open port 443/tcp on 199.59.243.222
Discovered open port 80/tcp on 199.59.243.222
Completed SYN Stealth Scan at 13:04, 4.56s elapsed (1000 total ports)
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.21 seconds
           Raw packets sent: 2003 (88.076KB) | Rcvd: 5 (236B)
```

- **ARP Ping:** ARP ping scan is used to discover the host devices in the same network. sometimes it will not visible due to firewall filtering.

nmap -PR www.geeksforgeeks.com

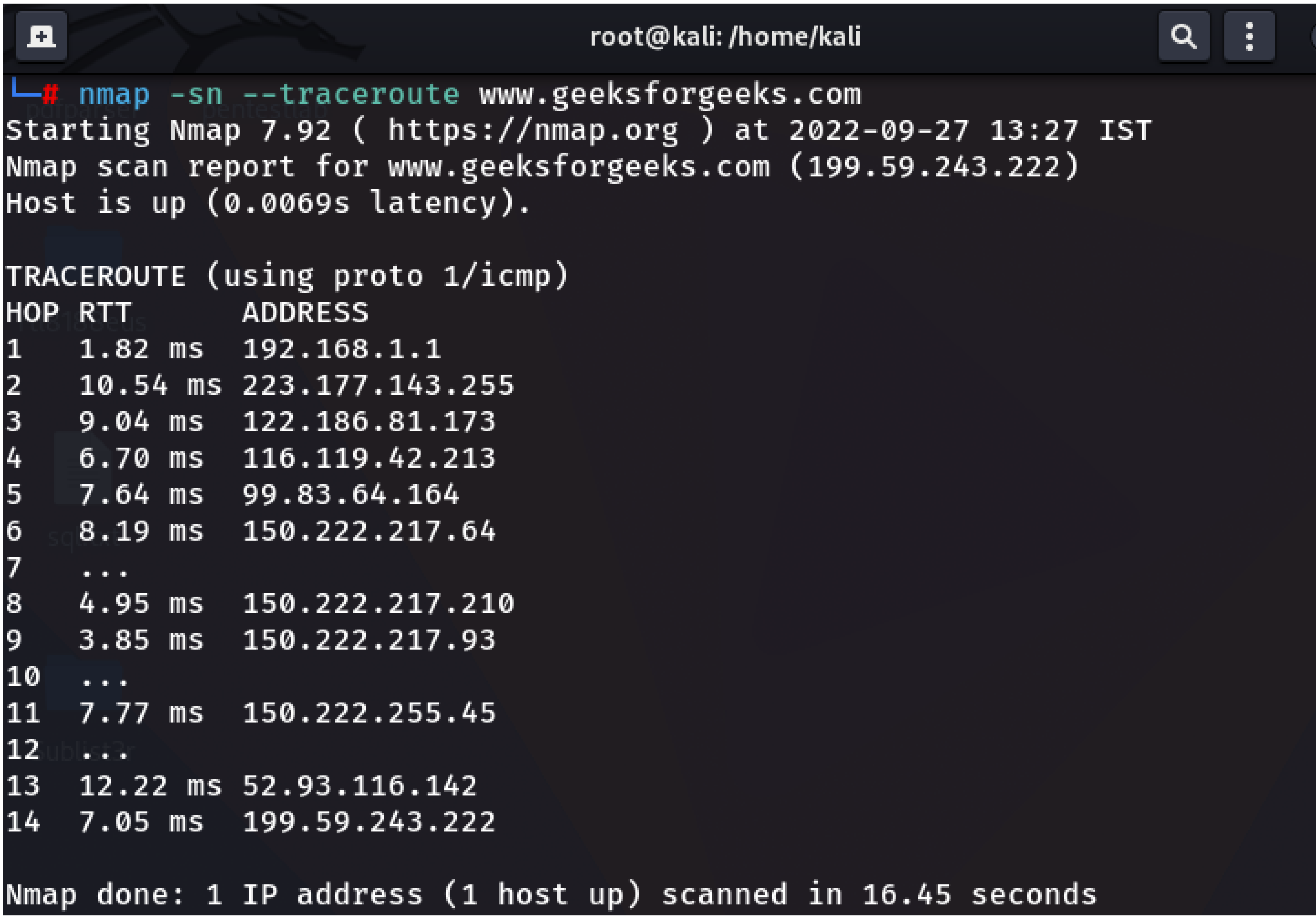


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:20 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0062s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 23.55 seconds
```

- **Traceroute:** Traceroute helps to discover the following hops or pathways to the targeted host.

nmap -sn –traceroute www.geeksforgeeks.com



```
└─# nmap -sn --traceroute www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:27 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0069s latency).

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   1.82 ms  192.168.1.1
2   10.54 ms 223.177.143.255
3   9.04 ms  122.186.81.173
4   6.70 ms  116.119.42.213
5   7.64 ms  99.83.64.164
6   8.19 ms  150.222.217.64
7   ...
8   4.95 ms  150.222.217.210
9   3.85 ms  150.222.217.93
10  ...
11  7.77 ms  150.222.255.45
12  ...
13  12.22 ms 52.93.116.142
14  7.05 ms  199.59.243.222

Nmap done: 1 IP address (1 host up) scanned in 16.45 seconds
```