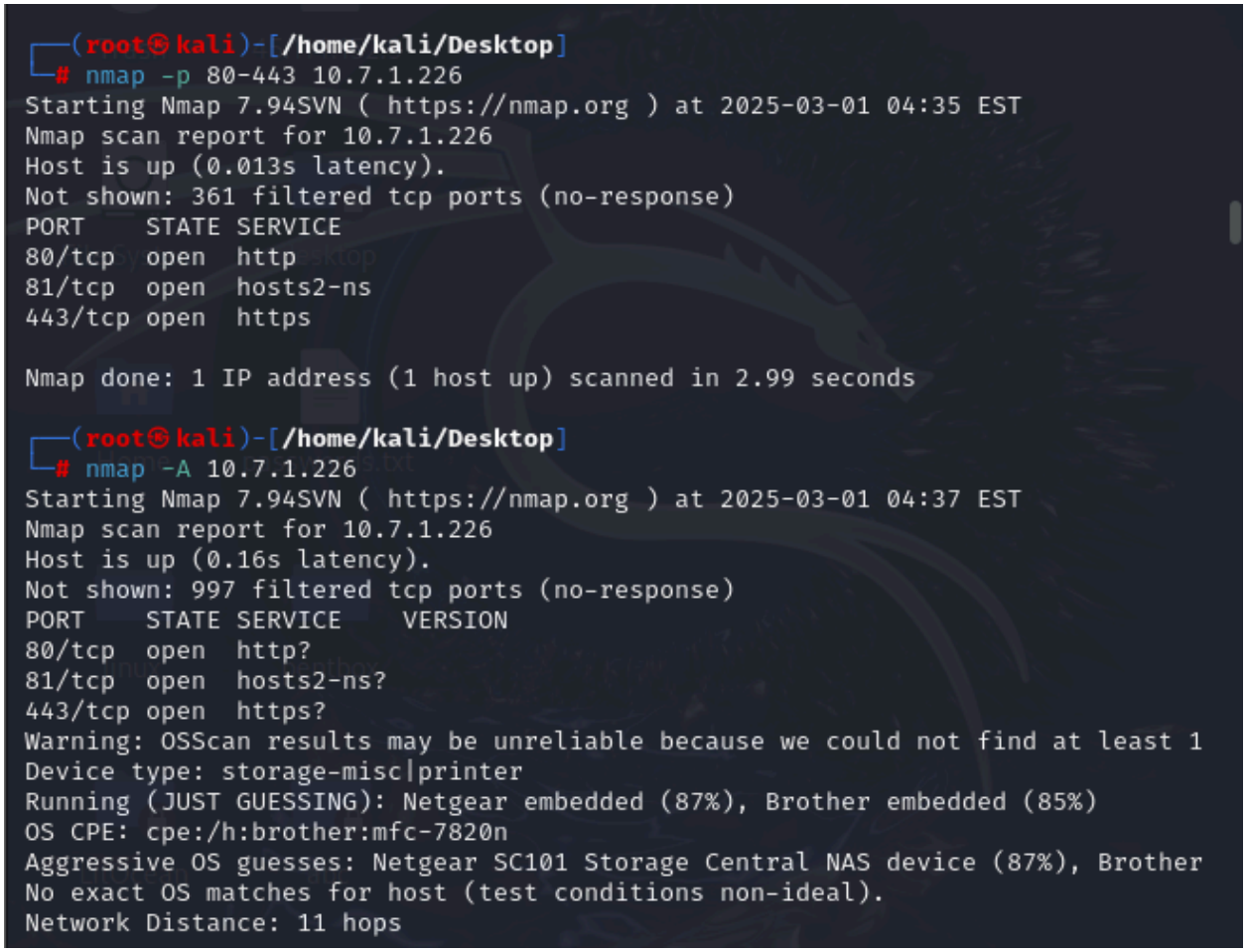
A project on network scanning using Nmap in Kali Linux



- This scans the target **10.7.1.226** for open ports and basic information.
- **nmap -p 80 10.7.1.226 Command Explanation**

This command tells **Nmap (Network Mapper)** to scan a specific **port (80)** on the target **IP address (10.7.1.226)**.

- Checks if **port 80 (HTTP)** is **open, closed, or filtered** on the target **10.7.1.226**.
- Determines if a web server or any service is running on **port 80**.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -A 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 04:37 EST
Nmap scan report for 10.7.1.226
Host is up (0.16s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http?
81/tcp  open  hosts2-ns?
443/tcp open  https?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: storage-misc|printer
Running (JUST GUESSING): Netgear embedded (87%), Brother embedded (85%)
OS CPE: cpe:/h:brother:mfc-7820n
Aggressive OS guesses: Netgear SC101 Storage Central NAS device (87%), Brother MFC-7820N printer (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   ... 10
11  208.03 ms 10.7.1.226

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 309.90 seconds
```

This command performs an **aggressive scan** on the target IP **10.7.1.226**, gathering detailed information about the system.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 04:43 EST
Nmap scan report for 10.7.1.226
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
81/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.52 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 04:44 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds
```

`nmap -sV 10.7.1.226` → Scans the target **10.7.1.226** to detect **open ports** and identify the **versions of running services**.

`nmap -O 10.7.1.226` → Detects the **operating system (OS)** running on the target **10.7.1.226** using TCP/IP fingerprinting

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 04:45 EST
Nmap scan report for 10.7.1.226
Host is up (0.16s latency).
Not shown: 962 filtered tcp ports (no-response), 35 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
81/tcp  open  hosts2-ns
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1124.93 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sU 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 05:20 EST
Nmap scan report for 10.7.1.226
Host is up (0.00042s latency).
All 1000 scanned ports on 10.7.1.226 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1670.65 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sn 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 05:49 EST
Nmap scan report for 10.7.1.226
Host is up (0.0012s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

nmap -Pn 10.7.1.226 → Performs a scan on **10.7.1.226** by **skipping the host discovery (ping scan)** and assuming the target is online, useful when ICMP is blocked.

nmap -sU 10.7.1.226 → Performs a **UDP scan** on the target **10.7.1.226** to detect open **UDP ports** and associated services, useful for finding DNS, SNMP, and DHCP services.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sC 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 05:50 EST
Nmap scan report for 10.7.1.226
Host is up (0.032s 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 238.98 seconds

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap nmap -F 10.7.1.226 -sC 10.7.1.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 05:55 EST
Failed to resolve "nmap".
Nmap scan report for 10.7.1.226
Host is up (0.00079s latency).
All 100 scanned ports on 10.7.1.226 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:21 S ttl=38 id=58034 iplen=44  seq=1448115198 w
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65066 > 10.7.1.226:80 S ttl=53 id=18084 iplen=44  seq=1448246268 w
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:80 S ttl=48 id=63651 iplen=44  seq=1448115198 w
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
```

`nmap -sn 10.7.1.226` → Performs a **ping scan** to check if the target **10.7.1.226** is **online**, without scanning ports or services. Useful for network discovery

`nmap -sC 10.7.1.226` → Runs **default Nmap scripts** on the target **10.7.1.226** to gather additional information, such as vulnerabilities, service details, and security misconfigurations.

```
All 100 scanned ports on 10.7.1.226 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:21 S ttl=38 id=58034 iplen=44  seq=1448115198
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65066 > 10.7.1.226:80 S ttl=53 id=18084 iplen=44  seq=1448246268
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:80 S ttl=48 id=63651 iplen=44  seq=1448115198
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65066 > 10.7.1.226:22 S ttl=56 id=52535 iplen=44  seq=1448246268
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:22 S ttl=48 id=53940 iplen=44  seq=1448115198
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65066 > 10.7.1.226:139 S ttl=56 id=9593 iplen=44  seq=1448246268
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:139 S ttl=57 id=49297 iplen=44  seq=144811519
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65066 > 10.7.1.226:199 S ttl=50 id=5150 iplen=44  seq=1448246268
sendto in send_ip_packet_sd: sendto(5, packet, 40, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65093 > 10.7.1.226:80 A ttl=51 id=57684 iplen=40  seq=0 win=1024
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.7.1.226, 16) ⇒ Network is unreachable
Offending packet: TCP 192.168.148.128:65068 > 10.7.1.226:199 S ttl=38 id=22504 iplen=44  seq=144811519
Omitting future Sendto error messages now that 10 have been shown.  Use -d2 if you really want to see
Nmap scan report for 10.7.1.226
Host is up (0.025s latency).
Not shown: 60 filtered tcp ports (no-response), 39 closed tcp ports (reset)
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 5840.00 seconds
```

`nmap -F 10.7.1.226` → Performs a **fast scan** by scanning only the **most common 100 ports** instead of all 65,535 ports.
`nmap -sC 10.7.1.226` → Runs **default Nmap scripts** for gathering detailed information on open ports.

This will **quickly scan common ports** and **run default scripts** on the detected services.