

## Milestone2

Pieter\_Johannes\_Swart



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

## Table of Contents

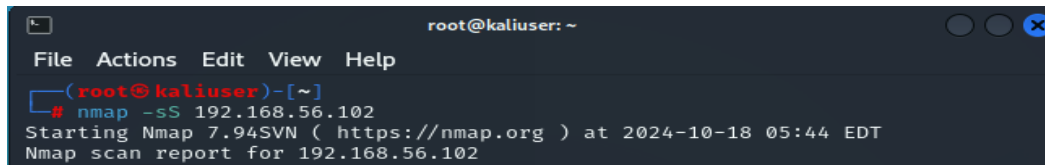
1. Stealth Scan (SYN Scan).....	3
2. TCP Connect Scan .....	4
3. UDP Scan .....	5
4. ACK Scan .....	6
Comparing the Output of Each Scan .....	6
Explanation of the difference between scans or if there is no difference why that should be expected.....	7
References .....	8

All four Nmap scans.

## 1. Stealth Scan (SYN Scan)

Type the following command:

**nmap -sS 'Metasploitable IP'**



```

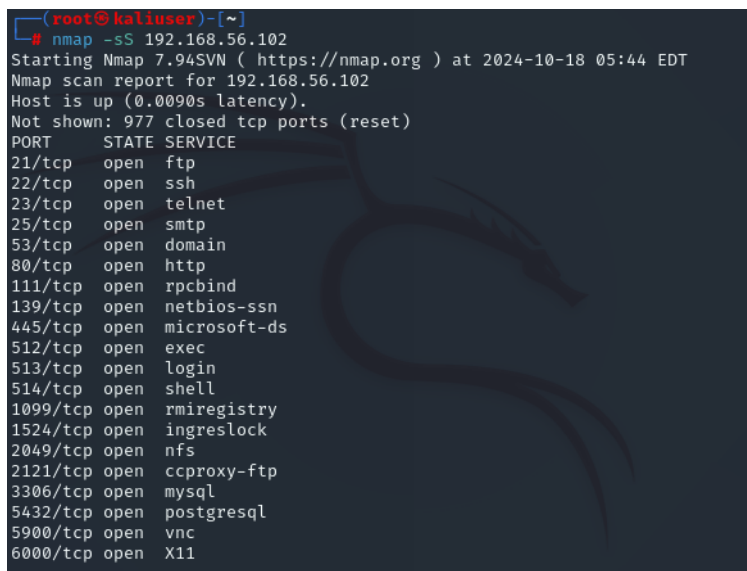
root@kaliuser: ~
File Actions Edit View Help
(root@kaliuser)~[~]
# nmap -sS 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 05:44 EDT
Nmap scan report for 192.168.56.102
  
```

### Explanation of Stealth scan.

The stealth scan, also known as a SYN scan, involves sending a TCP SYN packet to the target as if it allowed a TCP connection, but without completing the handshake. If the target port is open, it will respond with a SYN-ACK packet. The scanner then sends an RST "reset" packet to close the connection, leaving it half-opened to make it harder to detect.

### The Output

The scan typically reveals which ports are open, closed, or filtered. Open ports will respond with a SYN-ACK, closed ports with RST, and filtered ports may not respond at all or send an ICMP unreachable message.



```

(root@kaliuser)~[~]
# nmap -sS 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 05:44 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0090s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
  
```

Here it shows that all the PORTS are open. When Nmap returns a result of "open", it means that the target port is actively listening for connections and is ready to accept incoming traffic.

## 2. TCP Connect Scan

Type the following command:

**nmap -sT 'Metasploitable IP'**

```
(root@kaliuser)-[~]  
# nmap -sT 192.168.56.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 08:14 EDT
```

### Explanation of scan

This type of scan conducts a complete TCP connection (SYN, SYN-ACK, ACK) to check if a port is open. It goes through the entire TCP handshake process and promptly closes the connection. This method is easier to detect compared to a SYN scan since it fully connects to the target's ports.

### Output of Scan

Just like the SYN scan, this scan shows open, closed, or filtered ports. Since it completes the handshake, this scan can be more easily logged by the target's firewall or intrusion detection systems (IDS).

```
Nmap scan report for 192.168.56.102  
Host is up (0.012s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 08:00:27:3E:0B:04 (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

### 3. UDP Scan

Type the following command:

**nmap -sU 'Metasploitable IP'**

```
(root@kaliuser)-[~]
# nmap -sU 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 08:22 EDT
```

#### Explanation of scan

The UDP scan is different from the previous two scans, which are TCP-based. In the UDP scan, UDP packets are sent to the target to detect open UDP ports. Because UDP is connectionless, open ports will not send any acknowledgement. If a port is closed, the target typically responds with an ICMP port unreachable message.

#### Output of Scan

Open ports may not respond, while closed ports respond with ICMP messages. If ports are open and configured to respond, you might receive service-specific responses.

```
Stats: 0:43:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 09:05 (0:00:00 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.0056s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
21186/udp open|filtered unknown
MAC Address: 08:00:27:3E:0B:04 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2648.22 seconds
```

**"Open | Filtered":** This status indicates that Nmap cannot determine whether the port is open or filtered. Nmap did not receive a response from the target, so it's unclear whether:

- The port is open but not responding
- The port is being filtered by a firewall or other security mechanism, which is blocking the response.

## 4. ACK Scan

Type the following command:

**nmap -sA 'Metasploitable IP'**

```
(root@kaliuser)-[~]  
# nmap -sA 192.168.56.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 09:09 EDT  
█
```

### Explanation of Scan

The ACK scan is mainly used to identify firewall rules. It involves sending TCP ACK packets to the target without establishing a session. The aim is to determine whether the firewall is stateful or stateless by observing the target's response.

### Output of Scan

Typically, open or filtered ports won't respond, while closed ports will respond with RST packets. This scan doesn't identify open ports but rather detects whether ports are filtered or unfiltered.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-18 09:34 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.010s latency).  
All 1000 scanned ports on 192.168.56.102 are in ignored states.  
Not shown: 1000 unfiltered tcp ports (reset)  
MAC Address: 08:00:27:3E:0B:04 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
```

**"All 1000 scanned ports on 192.168.56.102 are in ignored states"**: This indicates that Nmap did not receive any useful responses from the 1000 ports it scanned.

**"Not shown: 1000 unfiltered TCP ports (reset)"**: This indicates that all the scanned ports are unfiltered but returned "reset" packets. When receiving an RST packet in an ACK scan, it means the port is unfiltered, indicating it is not protected by a firewall.

## Comparing the Output of Each Scan

- **Stealth Scan vs. TCP Connect Scan**: Both identify open ports but differ in stealthiness. Stealth scans avoid detection, while TCP Connect is easier to log.
- **UDP Scan**: This will generally provide fewer responses than TCP scans due to UDP's connectionless nature. Results may be less reliable and slower.
- **ACK Scan**: This does not identify open ports but rather reveals firewall filtering. It's mainly used to understand firewall behaviour rather than to list open services.

Explanation of the difference between scans or if there is no difference why that should be expected.

### 1. **Stealth Scan (SYN Scan)**

This scan is less likely to be logged by a firewall or IDS compared to a full TCP Connect Scan.

### 2. **TCP Connect Scan**

Compared to the SYN scan, it is more likely to be detected since it completes the handshake. Also, it requires root privileges on Linux.

### 3. **UDP Scan**

UDP scans can be slower due to the lack of acknowledgements and ICMP rate limiting. They are often less reliable than TCP scans due to the challenge of interpreting responses.

### 4. **ACK Scan**

Unlike the SYN or TCP Connect scans, it doesn't reveal open ports but provides insights into firewall rules. It's useful for mapping out firewall configurations.

## References

AGR3, L., 2024. Nmap Advanced Port Scans. 7 Jan, pp.

<https://medium.com/@lavanya.agre.cyb/nmap-advanced-port-scans-c96def9090ac>.

Handy, N., 2018. Kali Linux & Metasploit: Getting Started with Pen Testing. 2 Aug, pp.

<https://medium.com/@nickhandy/kali-linux-metasploit-getting-started-with-pen-testing-89d28944097b>.

Jan, 2023. TCP Connect Scan. 19 Jan, pp.

<https://www.codecademy.com/resources/docs/cybersecurity/nmap/tcp-connect-scan>.

kanishka10, 2013 . Understanding port scanning results of Nmap. 7 June, pp.

<https://www.hackercoolmagazine.com/understanding-port-scanning-results-of-nmap/>.

PenTest-duck, 2019. Deep Dive Into Nmap Scan Techniques. 30 Sep, pp.

[https://medium.com/@PenTest\\_duck/deep-dive-into-nmap-scan-techniques-faf3a1dac2d8](https://medium.com/@PenTest_duck/deep-dive-into-nmap-scan-techniques-faf3a1dac2d8).

Saini, A., 2024. How to Use Nmap Port Scan with Commands?. 22 04, pp.

<https://www.serverwala.com/blog/how-to-use-nmap-port-scan-with-commands/>.