

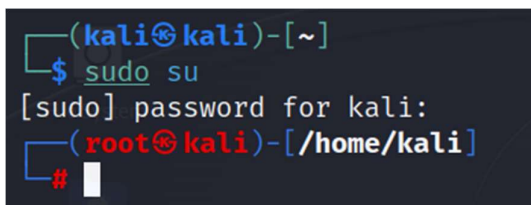
Understand Nmap commands and scan a target using Nmap

Nmap is a powerful network scanning and discovery tool used by network administrators and security professionals to analyze network hosts and services. It offers various features, including host discovery, port scanning, service and version detection, and the ability to adapt to different network environments.

Nmap is also capable of evading firewalls and intrusion detection systems, making it a valuable tool for assessing network security. Its extensible scripting engine (NSE scripts) allows for the automation and customization of scanning procedures, and it offers multiple output options for generating detailed reports and logs.

Attached for your reference are some of the Nmap commands executed on the Kali Linux virtual machine.

sudo su - Command used to become the superuser (root), granting you full control and elevated privileges over the system.



```
(kali㉿kali)-[~]  
$ sudo su  
[sudo] password for kali:  
(root㉿kali)-[/home/kali]  
#
```

nmap 192.168.1.1 - Command to scan and gather information about the network device with the IP address 192.168.1.1.

nmap 192.168.1.1 192.168.2.1 – Command used to perform network scanning on both IP addresses, 192.168.1.1 and 192.168.2.1, simultaneously. It allows you to scan and gather information about multiple network devices at once.

```
(root@kali)-[/home/kali]
# nmap 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 08:32 EDT
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
```

```
(root@kali)-[/home/kali]
# nmap 192.168.1.1 192.168.2.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 08:33 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.15% done; ETC: 08:33 (0:00:23 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.25% done; ETC: 08:33 (0:00:22 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.12% done; ETC: 08:33 (0:00:18 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.75% done; ETC: 08:33 (0:00:03 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.2.1
Host is up (0.032s latency).
All 1000 scanned ports on 192.168.2.1 are in ignored states.
```

nmap www.ssn.edu.in - Command used to perform network scanning on the domain name "www.ssn.edu.in." It initiates a scan to gather information about the network services and open ports associated with the web server hosted at that domain. Nmap will resolve the domain to its IP address and scan it for network-related details.

nmap www.kct.ac.in - Command used to initiate a network scan on the domain "www.kct.ac.in." This scan would attempt to identify open ports and services on the web server associated with that domain, providing information about the network configuration and potentially open vulnerabilities.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nmap www.ssn.edu.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:05 EDT
Nmap scan report for www.ssn.edu.in (182.75.25.233)
Host is up (0.00049s latency).
rDNS record for 182.75.25.233: nsg-static-233.25.75.182-airtel.com
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 4.99 seconds

(root@kali)-[/home/kali]
# nmap www.kct.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:06 EDT
Nmap scan report for www.kct.ac.in (172.67.187.85)
Host is up (0.00078s latency).
Other addresses for www.kct.ac.in (not scanned): 104.21.56.170 2606:4700:3035
::ac43:bb55 2606:4700:3037::6815:38aa
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```

nmap www.ssn.edu.in -sS – Command used to scan the domain "www.ssn.edu.in" using a SYN scan technique to identify open ports and services on the web server stealthily and quickly.

nmap www.ssn.edu.in -sU – Command used to perform a network scan on the domain "www.ssn.edu.in" using the UDP scan technique. This scan attempts to identify open UDP ports and services on the target server, providing information about the network configuration. It's particularly useful for discovering services that might not respond to traditional TCP scans.

nmap www.ssn.edu.in -sA – Command used to perform a network scan on the domain "www.ssn.edu.in" using the ACK scan technique. An ACK scan doesn't attempt to determine open ports; instead, it sends ACK (acknowledgment) packets to determine how the target system responds to them. This scan is often used for advanced troubleshooting and network analysis.

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# nmap www.ssn.edu.in -sS
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:06 EDT
Nmap scan report for www.ssn.edu.in (182.75.25.233)
Host is up (0.00047s latency).
rDNS record for 182.75.25.233: nsg-static-233.25.75.182-airtel.com
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 4.64 seconds

(root@kali)-[/home/kali]
# nmap www.ssn.edu.in -sU
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:06 EDT
Stats: 0:04:00 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.40% done; ETC: 23:17 (0:06:27 remaining)
Stats: 0:06:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 44.30% done; ETC: 23:20 (0:07:46 remaining)
Stats: 0:07:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 48.45% done; ETC: 23:22 (0:08:12 remaining)

zsh: suspended nmap www.ssn.edu.in -sU
```

nmap 192.168.1.1-3 -sL - Command to list the IP addresses within the range 192.168.1.1 to 192.168.1.3 without actively scanning or probing the hosts.

```
root@kali: /home/kali
File Actions Edit View Help

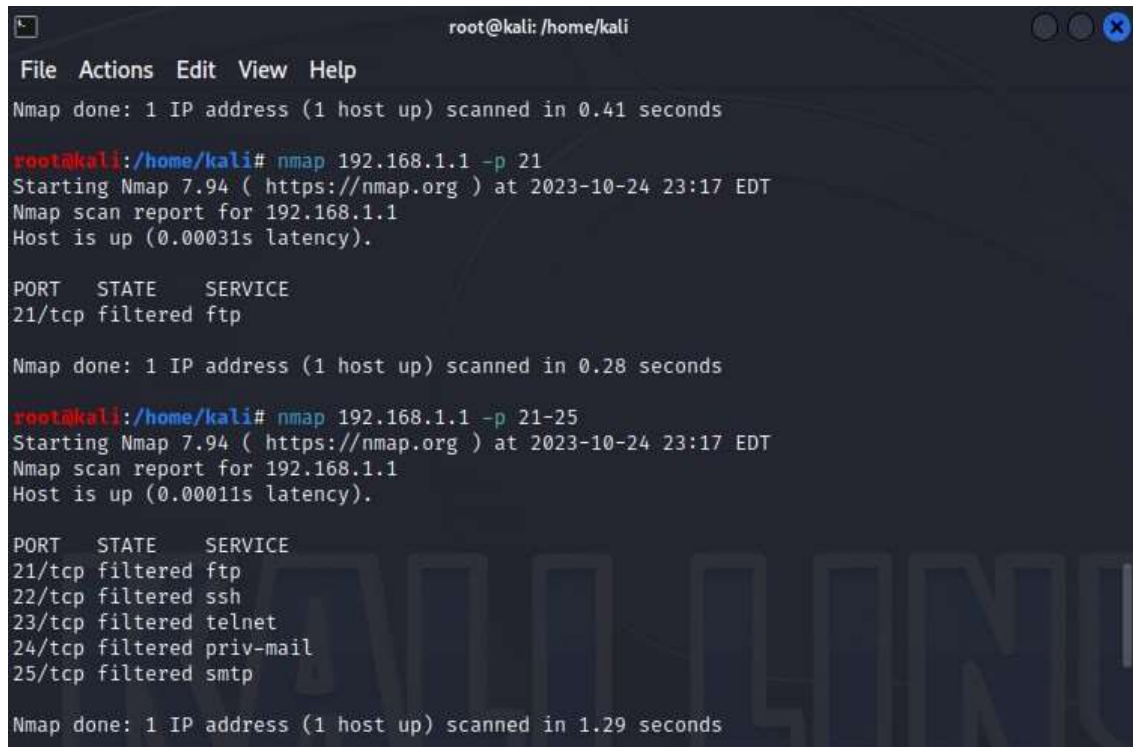
(root@kali)-[/home/kali]
# nmap www.ssn.edu.in -sA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:15 EDT
Nmap scan report for www.ssn.edu.in (182.75.25.233)
Host is up (0.00015s latency).
rDNS record for 182.75.25.233: nsg-static-233.25.75.182-airtel.com
All 1000 scanned ports on www.ssn.edu.in (182.75.25.233) are in ignored state s.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

root@kali: /home/kali# nmap 192.168.1.1-3 -sL
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:15 EDT
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap done: 3 IP addresses (0 hosts up) scanned in 0.00 seconds
```


nmap 192.168.1.1 -p 21 – Command used to scan the IP address 192.168.1.1 to check if port 21 (FTP) is open on the target device.

nmap 192.168.1.1 -p 21-25 – Command that scans IP address 192.168.1.1 to check if ports 21 to 25 are open or closed on the target device.



```
root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@kali:/home/kali# nmap 192.168.1.1 -p 21
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:17 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00031s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
root@kali:/home/kali# nmap 192.168.1.1 -p 21-25
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:17 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00011s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
24/tcp    filtered  priv-mail
25/tcp    filtered  smtp

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

nmap 192.168.1.1 -sV - Command that scans the IP address 192.168.1.1 to identify open ports and services while attempting to determine the versions of those services on the target device.

nmap 192.168.1.1 -F - Command used to fast network scan that quickly identifies open ports on the IP address 192.168.1.1, providing a basic overview of available network services.

```
root@kali: /home/kali
File Actions Edit View Help

root@kali:/home/kali# nmap 192.168.1.1 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:18 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.30 seconds

root@kali:/home/kali# nmap 192.168.1.1 -F
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:19 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00021s latency).
All 100 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

nmap 192.168.1.1 --top-ports 10 – Command used to perform a network scan on the IP address 192.168.1.1, focusing on the top 10 most commonly used ports. This scan targets the ports that are frequently associated with essential network services and aims to identify open ports among them, offering a streamlined view of key services on the target device.

```
root@kali: /home/kali
File Actions Edit View Help

root@kali:/home/kali# nmap 192.168.1.1 --top-ports 10
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:20 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00029s latency).

PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    filtered http
110/tcp   filtered pop3
139/tcp   filtered netbios-ssn
443/tcp   filtered https
445/tcp   filtered microsoft-ds
3389/tcp  filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

nmap 192.168.1.1 -sC - Command used to perform a network scan on the IP address 192.168.1.1 while enabling the default NSE (Nmap Scripting Engine) scripts. These scripts provide additional information and automated testing of common vulnerabilities and network services on the target device. It's a convenient way to gather more detailed information about the services and potential security issues on the target.

```
root@kali:/home/kali# nmap 192.168.1.1 -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-24 23:21 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 9.34 seconds
```

Result

Through this exercise, we've learned how to use Nmap for network scanning and analysis, including scanning IP addresses and domain names, utilizing various scanning techniques, and identifying open ports and services. This knowledge equips us with valuable skills for network assessment and security.