AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

TASK-9: Explore nmap commands

Port Specification Options

Scanning Types

Host /192.168.0.100 Discovery


```
                                    manasa13@Kali: ~

File  Actions  Edit  View  Help

  ┌──(manasa13㉿Kali)-[~]
  └─$ nmap 192.168.0.100-105 -sL
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-07 14:54 IST
Nmap scan report for 192.168.0.100
Nmap scan report for 192.168.0.101
Nmap scan report for 192.168.0.102
Nmap scan report for 192.168.0.103
Nmap scan report for 192.168.0.104
Nmap scan report for 192.168.0.105
Nmap done: 6 IP addresses (0 hosts up) scanned in 0.03 seconds

  ┌──(manasa13㉿Kali)-[~]
  └─$ nmap 192.168.0.100/8 -sn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-07 14:54 IST
Stats: 0:02:09 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 66.97% done; ETC: 14:57 (0:01:04 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 86.46% done; ETC: 14:57 (0:00:26 remaining)
Stats: 0:03:04 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 88.23% done; ETC: 14:58 (0:00:25 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 91.09% done; ETC: 14:58 (0:00:21 remaining)
Nmap scan report for mailgw.elevatedcomp.com (192.0.3.12)
Host is up (0.24s latency).
Nmap scan report for spam.elevated.net (192.0.3.26)
Host is up (0.29s latency).
Nmap scan report for 192.0.3.27
Host is up (0.30s latency).
Nmap scan report for 192.0.3.38
Host is up (0.28s latency).
Nmap scan report for 192.0.3.50
Host is up (0.34s latency).
Nmap scan report for 192.0.3.188
Host is up (0.26s latency).
Nmap scan report for 192.0.3.231
Host is up (0.30s latency).
Nmap scan report for 192.0.8.1
Host is up (0.22s latency).
Nmap scan report for 192.0.8.2
Host is up (0.26s latency).
Nmap scan report for 192.0.8.3
Host is up (0.22s latency).
Nmap scan report for 192.0.8.7
Host is up (0.37s latency).
Nmap scan report for 192.0.8.8
Host is up (0.27s latency).
Nmap scan report for 192.0.8.9
Host is up (0.27s latency).
Nmap scan report for 192.0.8.10
Host is up (0.25s latency).
```



```
                                    manasa13@Kali: ~

File  Actions  Edit  View  Help

  ┌──(manasa13㉿Kali)-[~]
  └─$ nmap 192.168.0.100-105 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-07 15:02 IST
Nmap scan report for 192.168.0.100
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.0.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.101
Host is up.
All 1000 scanned ports on 192.168.0.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.102
Host is up.
All 1000 scanned ports on 192.168.0.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.0.103
Host is up (0.0017s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsdapi
6646/tcp  open  unknown
7070/tcp  open  realserver

Nmap scan report for 192.168.0.104
Host is up (0.0092s latency).
All 1000 scanned ports on 192.168.0.104 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.105
Host is up.
All 1000 scanned ports on 192.168.0.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 6 IP addresses (6 hosts up) scanned in 28.59 seconds
```

```
┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 -PS22-25,80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:17 IST
Nmap scan report for 192.168.0.100
Host is up (0.0013s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 5.12 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 -PA22-25,80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:18 IST
Nmap scan report for 192.168.0.100
Host is up (0.0023s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap 192.168.0.100-105 -PU53
[sudo] password for manasa13:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:19 IST
Nmap scan report for 192.168.0.100
Host is up (0.00041s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap scan report for 192.168.0.104
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.0.104 are in ignored states.
Not shown: 1000 closed tcp ports (reset)


MAC Address: 8E:00:5E:38:DE:B1 (Unknown)

Nmap scan report for 192.168.0.102
Host is up (0.000051s latency).
All 1000 scanned ports on 192.168.0.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 192.168.0.103
Host is up (0.000049s latency).
All 1000 scanned ports on 192.168.0.103 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 6 IP addresses (4 hosts up) scanned in 25.24 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 -n
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:20 IST
Nmap scan report for 192.168.0.100
Host is up (0.0017s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
```
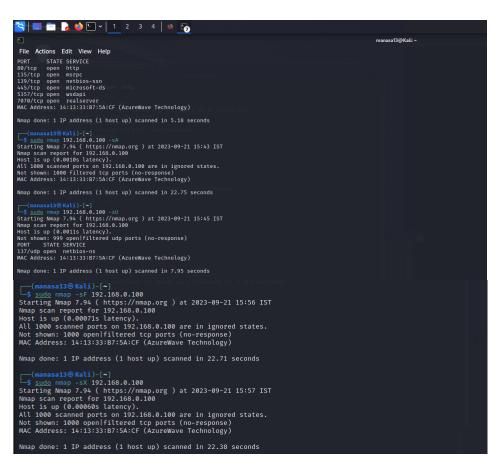
Scanning Command Syntax


```
┌──(manasa13㉿Kali)-[~]
└─$ nmap --script= test script 192.168.0.100/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:27 IST
Failed to resolve "test".
Failed to resolve "script".
Nmap scan report for 192.168.0.1
Host is up (0.0025s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE     SERVICE
23/tcp   filtered  telnet
80/tcp   open      http
1900/tcp open      upnp

Nmap scan report for 192.168.0.100
Host is up (0.00093s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap scan report for 192.168.0.102
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.0.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.103
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.0.103 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.104
Host is up (0.0046s latency).
All 1000 scanned ports on 192.168.0.104 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.106
Host is up (0.070s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (6 hosts up) scanned in 88.72 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap --script-update-db
nmap: unrecognized option '--script-update-db'
See the output of nmap -h for a summary of options.
```
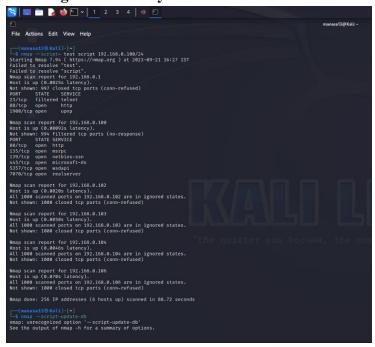
Version Detection

Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE   VERSION
80/tcp   open http   Microsoft IIS httpd 10.0
135/tcp open msrpc   Microsoft Windows RPC
139/tcp open netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp open ssl/realserver?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.66 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 -A
Starting Nmap 7.94 (https://nmap.org) at 2023-09-21 16:36 IST
Nmap scan report for 192.168.0.100
Host is up (0.0013s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE   VERSION
80/tcp   open http   Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc   Microsoft Windows RPC
139/tcp open netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
7070/tcp open ssl/realserver
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2022-10-05T14:40:22
|_Not valid after: 2072-09-22T14:40:22
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2023-09-21T11:06:29
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
|_nbstat: NetBIOS name: LAPTOP-H5HVJHRN, NetBIOS user: <unknown>, NetBIOS MAC: 14:13:33:b7:5a:cf (AzureWave Technology)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.12 seconds

┌──(manasa13㉿Kali)-[~]
└─$ ▮

7070/tcp open ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2022-10-05T14:40:22
|_Not valid after: 2072-09-22T14:40:22
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2023-09-21T11:06:29
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
|_nbstat: NetBIOS name: LAPTOP-H5HVJHRN, NetBIOS user: <unknown>, NetBIOS MAC: 14:13:33:b7:5a:cf (AzureWave Technology)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.12 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 -O
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap 192.168.0.100 -O
[sudo] password for manasa13:
Starting Nmap 7.94 (https://nmap.org) at 2023-09-21 16:38 IST
Nmap scan report for 192.168.0.100
Host is up (0.0011s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
7070/tcp open realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|10|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows Server 2022 (91%), Micros
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.47 seconds

┌──(manasa13㉿Kali)-[~]
└─$ ▮

Nmap output formats

┌──(manasa13㉿Kali)-[~]
└─$ nmap -oN scan.txt 192.168.0.100
Starting Nmap 7.94 (https://nmap.org) at 2023-09-21 16:42 IST
Nmap scan report for 192.168.0.100
Host is up (0.0018s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
7070/tcp open realserver

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap -oX scanr.xml 192.168.0.100
Starting Nmap 7.94 (https://nmap.org) at 2023-09-21 16:43 IST
Nmap scan report for 192.168.0.100
Host is up (0.0015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
7070/tcp open realserver

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

┌──(manasa13㉿Kali)-[~]
└─$ nmap -oG grep.txt 192.168.0.100
Starting Nmap 7.94 (https://nmap.org) at 2023-09-21 16:43 IST
Nmap scan report for 192.168.0.100
Host is up (0.0016s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp   open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
7070/tcp open realserver

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds

Firewall Proofing


```
┌──(manasa13@Kali)-[~]
└─$ sudo nmap -f [192.168.0.100]
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:47 IST
Failed to resolve "[192.168.0.100]".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds

┌──(manasa13@Kali)-[~]
└─$ sudo nmap -f 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:47 IST
Nmap scan report for 192.168.0.100
Host is up (0.0062s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 10.94 seconds

┌──(manasa13@Kali)-[~]
└─$ sudo nmap -mtu [MTU] 192.168.0.100
Data payload MTU must be >0 and multiple of 8
QUITTING!

┌──(manasa13@Kali)-[~]
└─$ sudo nmap -sI [zombie] 192.168.0.100
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap g
ains from pings can allow for faster, more reliable scans.
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-07 16:00 IST
Skipping Idle Scan against 192.168.0.100 -- you can't idle scan your own machine (localhost).
Nmap scan report for 192.168.0.100
Host is up.

PORT      STATE    SERVICE
1/tcp     unknown  tcpmux
3/tcp     unknown  compressnet
4/tcp     unknown  unknown
6/tcp     unknown  unknown
7/tcp     unknown  echo
9/tcp     unknown  discard
13/tcp    unknown  daytime
17/tcp    unknown  qotd
19/tcp    unknown  chargen
20/tcp    unknown  ftp-data
21/tcp    unknown  ftp
22/tcp    unknown  ssh
23/tcp    unknown  telnet
24/tcp    unknown  priv-mail
25/tcp    unknown  smtp
26/tcp    unknown  rsftp
30/tcp    unknown  unknown
32/tcp    unknown  unknown
33/tcp    unknown  dsp
```

```
┌──(manasa13@Kali)-[~]
└─$ sudo nmap --source-port 53 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:48 IST
Nmap scan report for 192.168.0.100
Host is up (0.00045s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
```



```
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.15 seconds

┌──(manasa13@Kali)-[~]
└─$ sudo nmap --data-length 16 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:50 IST
Nmap scan report for 192.168.0.100
Host is up (0.00062s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.51 seconds

┌──(manasa13@Kali)-[~]
└─$ sudo nmap --randomize-hosts 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:50 IST
Nmap scan report for 192.168.0.100
Host is up (0.00047s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds

┌──(manasa13@Kali)-[~]
└─$ sudo nmap --badsum 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 16:50 IST
Nmap scan report for 192.168.0.100
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.0.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 22.37 seconds

┌──(manasa13@Kali)-[~]
└─$ 
```

Miscellaneous Commands

```
┌──(manasa13㉿Kali)-[~]
└─$ nmap -6
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:01 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap -proxies proxy https://www.google.com, proxy https://www.youtube.com
libnsock proxy_node_new(): Invalid protocol in proxy specification string: proxy
Invalid proxy chain specification
QUITTING!

┌──(manasa13㉿Kali)-[~]
└─$ nmap -open
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:01 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
```
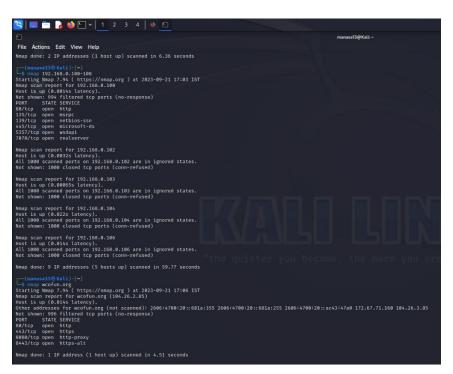
192.168.0.100 Specification

```
┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:03 IST
Nmap scan report for 192.168.0.100
Host is up (0.0015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:03 IST
Nmap scan report for 192.168.0.100
Host is up (0.0021s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 2 IP addresses (1 host up) scanned in 6.36 seconds
```

```
Nmap done: 2 IP addresses (1 host up) scanned in 6.36 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap 192.168.0.100-108
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:03 IST
Nmap scan report for 192.168.0.100
Host is up (0.0014s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap scan report for 192.168.0.102
Host is up (0.0032s latency).
All 1000 scanned ports on 192.168.0.102 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.103
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.0.103 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.104
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.0.104 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.0.106
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 9 IP addresses (5 hosts up) scanned in 59.77 seconds

┌──(manasa13㉿Kali)-[~]
└─$ nmap wcofun.org
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:06 IST
Nmap scan report for wcofun.org (104.26.2.85)
Host is up (0.014s latency).
Other addresses for wcofun.org (not scanned): 2606:4700:20::681a:355 2606:4700:20::681a:255 2606:4700:20::ac43:47a0 172.67.71.160 104.26.3.85
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.51 seconds
```

Nmap Timing options

```
┌──(manasa13⊕Kali)-[~]
└─$ nmap -T2 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:19 IST
Nmap scan report for 192.168.0.100
Host is up (0.0027s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 893.19 seconds
```

```
┌──(manasa13⊕Kali)-[~]
└─$ nmap -T3 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:20 IST
Nmap scan report for 192.168.0.100
Host is up (0.0030s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver
Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

```
┌──(manasa13⊕Kali)-[~]
└─$ nmap -T4 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:20 IST
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 73.55% done; ETC: 17:20 (0:00:01 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 80.35% done; ETC: 17:20 (0:00:01 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 85.25% done; ETC: 17:20 (0:00:01 remaining)
Nmap scan report for 192.168.0.100
Host is up (0.0014s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

```
┌──(manasa13⊕Kali)-[~]
└─$ nmap -T5 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 17:21 IST
Nmap scan report for 192.168.0.100
Host is up (0.0028s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds
```

Scan Options


```
┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -sP 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:46 IST
Nmap scan report for 192.168.0.100
Host is up (0.0011s latency).
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -PU 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:47 IST
Nmap scan report for 192.168.0.100
Host is up (0.0010s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.34 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -PE 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:47 IST
Nmap scan report for 192.168.0.100
Host is up (0.00076s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -PO 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:48 IST
Nmap scan report for 192.168.0.100
Host is up (0.0010s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -PR 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:48 IST
Nmap scan report for 192.168.0.100
Host is up (0.00064s latency).
Not shown: 994 filtered tcp ports (no-response)
```



```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -Pn 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:48 IST
Nmap scan report for 192.168.0.100
Host is up (0.00096s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds

┌──(manasa13㉿Kali)-[~]
└─$ sudo nmap -traceroute 192.168.0.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-21 19:49 IST
Nmap scan report for 192.168.0.100
Host is up (0.0010s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
MAC Address: 14:13:33:B7:5A:CF (AzureWave Technology)

TRACEROUTE
HOP RTT      ADDRESS
1   1.01 ms 192.168.0.100

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds
```