

# **Class 10 - 05/09/2023**

# Nmap Cheat Sheet

Different usage options		
Port discovery and specification		
Host discovery and specification		
Vulnerability scanning		
Application and service version detection		
Software version detection against the ports		
Firewall / IDS Spoofing		
Port Specification Options		
Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-P	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-P-	nmap -p- 172.16.1.1	Port scan for all ports
-P	nmap -smtplib,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-P "*"	nmap -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan
Host /172.16.1.1 Discovery		
Switch/Syntax	Example	Description
-sl	nmap 172.16.1.1-5 -sl	List 172.16.1.1 without scanning
-sn	nmap 172.16.1.1/8 -sn	Disable port scanning
-Pn	nmap 172.16.1.1-8 -Pn	Port scans only and no host discovery
-PS	nmap 172.16.1.185 -PS22-25,80	TCP SYN discovery on specified port
-PA	nmap 172.16.1.185 -PA22-25,80	TCP ACK discovery on specified port
-PU	nmap 172.16.1.1-8 -PUS3	UDP discovery on specified port
-PR	nmap 172.16.1.1-8 -PR	ARP discovery within local network
-n	nmap 172.16.1.1 -n	no DNS resolution
Version Detection		
Switch/Syntax	Example	Description
-sV	nmap 172.16.1.1 -sV	Try to find the version of the service running on port
--version-intensity	nmap 172.16.1.1 -sV --version-intensity 6	Intensity level range 0 to 9.
-sV --version-all	nmap 172.16.1.1 -sV --version-all	Set intensity level to 9
-sV --version-light	nmap 172.16.1.1 -sV --version-light	Enable light mode
-A	nmap 172.16.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-O	nmap 172.16.1.1 -O	Remote OS detection
Firewall Proofing		
nmap -f [172.16.1.1]	scan fragment packets	
nmap -mtu [MTU] [172.16.1.1]	specify MTU	
nmap -sI [zombie] [172.16.1.1]	scan idle zombie	
nmap -source-port [port] [172.16.1.1]	manual source port - specify	
nmap -data-length [size] [172.16.1.1]	randomly append data	
nmap -randomize-hosts [172.16.1.1]	172.16.1.1 scan order randomization	
nmap -badsum [172.16.1.1]	bad checksum	
Nmap Timing Options		
Syntax	Description	
nmap -T0 172.16.1.1	Slowest scan	
nmap -T1 172.16.1.1	Tricky scan to avoid IDS	
nmap -T2 172.16.1.1	Timely scan	
nmap -T3 172.16.1.1	Default scan timer	
nmap -T4 172.16.1.1	Aggressive scan	
nmap -T5 172.16.1.1	Very aggressive scan	
Scanning Types		
Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-sF	nmap -sF 172.16.1.1	TCP FIN scan
-sX	nmap -sX 172.16.1.1	XMAS scan
-sP	nmap -sP 172.16.1.1	Ping scan
-sU	nmap -sU 172.16.1.1	UDP scan
-sA	nmap -sA 172.16.1.1	TCP ACK scan
-sL	nmap -sL 172.16.1.1	list scan
Scanning Command Syntax		
<b>nmap [scan types] [options] {172.16.1.1 specification}</b>		
Use of Nmap Scripts NSE		
nmap --script= test script 172.16.1.0/24	execute the listed script against target IP address	
nmap --script-update-db	adding new scripts	
nmap -sV -sC	use of safe default scripts for scan	
nmap --script-help="Test Script"	get help for script	
Nmap output Formats		
Default/normal output	nmap -oN scan.txt 172.16.1.1	
XML	nmap -oX scan.xml 172.16.1.1	
Grepable format	snmap -oG grep.txt 172.16.1.1	
All formats	nmap -OA 172.16.1.1	
172.16.1.1 Specification		
nmap 172.16.1.1	single IP scan	
nmap 172.16.1.1 172.16.100.1	scan specific IPs	
nmap 172.16.1.1-254	scan a range of IPs	
nmap xyz.org	scan a domain	
nmap 10.1.1.0/8	scan using CIDR notation	
nmap -il scan.txt	scan 172.16.1.1s from a file	
nmap --exclude 172.16.1.1	specified IP s exclude from scan	
Scan Options		
Syntax	Description	
nmap -sP 172.16.1.1	Ping scan only	
nmap -PU 172.16.1.1	UDP ping scan	
nmap -PE 172.16.1.1	ICMP echo ping	
nmap -PO 172.16.1.1	IP protocol ping	
nmap -PR 172.16.1.1	ARP ping	
nmap -Pn 172.16.1.1	Scan without pinging	
nmap -traceroute 172.16.1.1	Traceroute	

FTP	21	File Transfer Protocol
SSH	22	Secure Shell
Telnet	23	The Telnet Service
SMTP	25	Simple Mail Transfer Protocol
DNS	53	Domain Name Service
HTTP	80	Hyper-Text Transfer Protocol
Kerberos	88	Kerberos Network Authentication System
POP2	109	Post Office Protocol Version 2
POP3	110	Post Office Protocol Version 3
NTP	125	Network Time Protocol
NETBIOS-NS	137	NetBIOS Name Service
NETBIOS-DGM	138	NetBIOS Datagram Service
NETBIOS-SSN	139	NetBIOS Session Service
IMAP	143	Internet Message Access Protocol
SNMP	161	Simple Network Management Protocol
IMAPv3	220	Internet Message Access Protocol Version 3
HTTPS	443	Secure Hyper-Text Transfer Protocol
Kerberos-DS	445	Server Message Block (SMB)
SOCKS	1080	SOCKS Network Application Proxy Services
NFS	2049	Network File System
MySQL	3306	MySQL Database Service

## Task - Performing nmap commands on Metasploitable

### Port Specification Options

- Scanning specific port

```
(kali㉿kali)-[~]
$ nmap -p 443 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:06 IST
Nmap scan report for 192.168.1.11
Host is up (0.00050s latency).

PORT      STATE    SERVICE
443/tcp    closed   https

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

(kali㉿kali)-[~]
$
```

- Different port type scan

```
(kali㉿kali)-[~]
$ nmap -pU:110,T:23-25,443 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:09 IST
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 192.168.1.11
Host is up (0.00038s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
24/tcp    closed priv-mail
25/tcp    open  smtp
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

## Scanning Types:

1. Top SYN port scan

```
(kali㉿kali)-[~]
$ sudo nmap 192.168.1.11 -sS
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:13 IST
Nmap scan report for 192.168.1.11
Host is up (0.00012s 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
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:50:2E:0E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

2. Top ACK port scan

```
(kali㉿kali)-[~]
└─$ sudo nmap 192.168.1.11 -sA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:14 IST
Nmap scan report for 192.168.1.11
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:50:2E:0E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

### 3. Ping scan

```
(kali㉿kali)-[~] you become, the more you are able to hear
└─$ nmap -sP 192.168.1.11 -vv
Warning: The -sP option is deprecated. Please use -sn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:19 IST
Initiating Ping Scan at 21:19
Scanning 192.168.1.11 [2 ports]
Completed Ping Scan at 21:19, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:19
Completed Parallel DNS resolution of 1 host. at 21:19, 0.01s elapsed
Nmap scan report for 192.168.1.11
Host is up, received syn-ack (0.00082s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

## Host Discovery

### 1. Port Scans only and no host discovery

```

File Actions Edit View Help
└─(kali㉿kali)-[~]
$ nmap 192.168.1.11 -Pn -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:22 IST
Initiating Parallel DNS resolution of 1 host. at 21:22
Completed Parallel DNS resolution of 1 host. at 21:22, 0.01s elapsed
Initiating Connect Scan at 21:22
Scanning 192.168.1.11 [1000 ports]
Discovered open port 21/tcp on 192.168.1.11
Discovered open port 23/tcp on 192.168.1.11
Discovered open port 80/tcp on 192.168.1.11
Discovered open port 445/tcp on 192.168.1.11
Discovered open port 25/tcp on 192.168.1.11
Discovered open port 53/tcp on 192.168.1.11
Discovered open port 22/tcp on 192.168.1.11
Discovered open port 139/tcp on 192.168.1.11
Discovered open port 5900/tcp on 192.168.1.11
Discovered open port 3306/tcp on 192.168.1.11
Discovered open port 111/tcp on 192.168.1.11
Discovered open port 6000/tcp on 192.168.1.11
Discovered open port 2049/tcp on 192.168.1.11
Discovered open port 8180/tcp on 192.168.1.11
Discovered open port 1524/tcp on 192.168.1.11
Discovered open port 512/tcp on 192.168.1.11
Discovered open port 514/tcp on 192.168.1.11
Discovered open port 513/tcp on 192.168.1.11
Discovered open port 1099/tcp on 192.168.1.11
Discovered open port 6667/tcp on 192.168.1.11
Discovered open port 8009/tcp on 192.168.1.11
Discovered open port 5432/tcp on 192.168.1.11
Discovered open port 2121/tcp on 192.168.1.11
Completed Connect Scan at 21:22, 0.08s elapsed (1000 total ports)
Nmap scan report for 192.168.1.11
Host is up, received user-set (0.00027s latency).
Scanned at 2023-09-05 21:22:39 IST for 0s
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack
22/tcp    open  ssh          syn-ack
23/tcp    open  telnet       syn-ack
25/tcp    open  smtp         syn-ack
53/tcp    open  domain       syn-ack
80/tcp    open  http         syn-ack
111/tcp   open  rpcbind     syn-ack
139/tcp   open  netbios-ssn syn-ack
445/tcp   open  microsoft-ds syn-ack
512/tcp   open  exec        syn-ack
513/tcp   open  login       syn-ack
514/tcp   open  shell        syn-ack
1099/tcp  open  rmiregistry syn-ack
1524/tcp  open  ingreslock  syn-ack
2049/tcp  open  nfs         syn-ack
2121/tcp  open  ccproxy-ftp syn-ack

```

## 2. TCP Ack discovery on specified port

```
Kali㉿kali: ~
```

File Actions Edit View Help

```
└$ nmap 192.168.1.11 -PA22-25,80 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:24 IST
Initiating Ping Scan at 21:24
Scanning 192.168.1.11 [5 ports]
Completed Ping Scan at 21:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:24
Completed Parallel DNS resolution of 1 host. at 21:24, 0.10s elapsed
Initiating Connect Scan at 21:24
Scanning 192.168.1.11 [1000 ports]
Discovered open port 21/tcp on 192.168.1.11
Discovered open port 80/tcp on 192.168.1.11
Discovered open port 23/tcp on 192.168.1.11
Discovered open port 22/tcp on 192.168.1.11
Discovered open port 25/tcp on 192.168.1.11
Discovered open port 111/tcp on 192.168.1.11
Discovered open port 139/tcp on 192.168.1.11
Discovered open port 3306/tcp on 192.168.1.11
Discovered open port 5900/tcp on 192.168.1.11
Discovered open port 445/tcp on 192.168.1.11
Discovered open port 53/tcp on 192.168.1.11
Discovered open port 5432/tcp on 192.168.1.11
Discovered open port 512/tcp on 192.168.1.11
Discovered open port 6667/tcp on 192.168.1.11
Discovered open port 2121/tcp on 192.168.1.11
Discovered open port 514/tcp on 192.168.1.11
Discovered open port 8009/tcp on 192.168.1.11
Discovered open port 1099/tcp on 192.168.1.11
Discovered open port 2049/tcp on 192.168.1.11
Discovered open port 513/tcp on 192.168.1.11
Discovered open port 8180/tcp on 192.168.1.11
Discovered open port 6000/tcp on 192.168.1.11
Discovered open port 1524/tcp on 192.168.1.11
Completed Connect Scan at 21:24, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.1.11
Host is up, received syn-ack (0.00037s latency).
Scanned at 2023-09-05 21:24:44 IST for 0s
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack
22/tcp    open  ssh          syn-ack
23/tcp    open  telnet       syn-ack
25/tcp    open  smtp         syn-ack
53/tcp    open  domain       syn-ack
80/tcp    open  http         syn-ack
111/tcp   open  rpcbind     syn-ack
139/tcp   open  netbios-ssn syn-ack
445/tcp   open  microsoft-ds syn-ack
512/tcp   open  exec         syn-ack
513/tcp   open  login        syn-ack
514/tcp   open  shell        syn-ack
1099/tcp  open  rmiregistry  syn-ack
1524/tcp  open  ingreslock   syn-ack
```

## Use of nmap script scripts NSE

### 1. Use of safe default scripts

```
(kali㉿kali)-[~]
└─$ nmap -sV -sc 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:28 IST
Nmap scan report for 192.168.1.11
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.1.10
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2023-09-05T15:58:32+00:00; +5s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_sslv2:
|   SSLv2 supported
| ciphers:
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2 DES_64_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2 DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, NHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
|_rpcinfo:
```

## Version Detection

1. Try to find the version of service running on port

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:30 IST
Nmap scan report for 192.168.1.11
Host is up (0.00034s latency).

Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds
```

2. Enable OS Detection, version detection, script scanning and traceroute (Aggressive scanning)

```
(kali㉿kali)-[~]
$ nmap -A 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:33 IST
Nmap scan report for 192.168.1.11
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
| STAT:
| FTP server status:
|   Connected to 192.168.1.10
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
_|ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-date: 2023-09-05T16:03:47+00:00; +5s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, EHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

## Nmap Output format

### 1. Grepable format

```
(kali㉿kali)-[~]
$ nmap -A 192.168.1.11 -oX grep.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:36 IST
Nmap scan report for 192.168.1.11
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
| FTP server status:
| pictures Connected to 192.168.1.10
|_videos  Logged in as ftp
|_ideos   TYPE: ASCII
| download No session bandwidth limit
|_       Session timeout in seconds is 300
|_is      Control connection is plain text
| fileSyst Data connections will be plain text
|_       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2023-09-05T16:06:34+00:00; +5s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, EHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain        ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

## 2. Normal format

```
(kali㉿kali)-[~]
$ nmap -A 192.168.1.11 > scan.txt
```

# Firewall Proofing

## 1. Scan fragments packets

```
(kali㉿kali)-[~]
$ sudo nmap -f [192.168.1.11] -vv
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:40 IST
Failed to resolve "[192.168.1.11]".
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
    Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

## 2. Bad checksum

```
(kali㉿kali)-[~]
$ sudo nmap -badsum [192.168.1.11] -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:41 IST
Failed to resolve "[192.168.1.11]".
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
    Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

# Miscellaneous Commands

## 1. Show open ports only

```
(kali㉿kali)-[~]
$ nmap -open 192.168.1.11
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:45 IST
Nmap scan report for 192.168.1.11
Host is up (0.00029s 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

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

## 2. Scan IPv6 targets

```
(kali㉿kali)-[~]
$ nmap -6 ::1/128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:48 IST
Nmap scan report for localhost (::1)
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

# Specification

## 1. Scan a domain

```
(kali㉿kali)-[~]
$ nmap www.notion.so
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 21:53 IST
Nmap scan report for www.notion.so (104.18.39.102)
Host is up (0.0061s latency).
Other addresses for www.notion.so (not scanned): 172.64.148.154 2606:4700:4400::6812:2766 2606:
4700:4400::ac40:949a
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 7.15 seconds
```

## 2. Scan using CIDR notation

```
(kali㉿kali)-[~]
$ nmap 192.168.1.11/8 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 22:41 IST
Initiating Ping Scan at 22:41
Scanning 4096 hosts [2 ports/host]
Ping Scan Timing: About 39.56% done; ETC: 22:43 (0:00:47 remaining)
Ping Scan Timing: About 66.82% done; ETC: 22:43 (0:00:30 remaining)
Completed Ping Scan at 22:43, 88.88s elapsed (4096 total hosts)
Initiating Parallel DNS resolution of 460 hosts. at 22:43
Completed Parallel DNS resolution of 460 hosts. at 22:43, 21.69s elapsed
Nmap scan report for 192.0.0.0 [host down, received no-response]
Nmap scan report for 192.0.0.1 [host down, received no-response]
Nmap scan report for 192.0.0.2 [host down, received no-response]
Nmap scan report for 192.0.0.3 [host down, received no-response]
Nmap scan report for 192.0.0.4 [host down, received no-response]
Nmap scan report for 192.0.0.5 [host down, received no-response]
Nmap scan report for 192.0.0.6 [host down, received no-response]
Nmap scan report for 192.0.0.7 [host down, received host-unreach]
Nmap scan report for 192.0.0.8 [host down, received host-unreach]
Nmap scan report for 192.0.0.9 [host down, received host-unreach]
Nmap scan report for 192.0.0.10 [host down, received no-response]
Nmap scan report for 192.0.0.11 [host down, received no-response]
Nmap scan report for 192.0.0.12 [host down, received host-unreach]
Nmap scan report for 192.0.0.13 [host down, received no-response]
Nmap scan report for 192.0.0.14 [host down, received no-response]
Nmap scan report for 192.0.0.15 [host down, received no-response]
Nmap scan report for 192.0.0.16 [host down, received no-response]
Nmap scan report for 192.0.0.17 [host down, received no-response]
Nmap scan report for 192.0.0.18 [host down, received host-unreach]
Nmap scan report for 192.0.0.19 [host down, received no-response]
Nmap scan report for 192.0.0.20 [host down, received host-unreach]
Nmap scan report for 192.0.0.21 [host down, received host-unreach]
Nmap scan report for 192.0.0.22 [host down, received host-unreach]
Nmap scan report for 192.0.0.23 [host down, received no-response]
Nmap scan report for 192.0.0.24 [host down, received no-response]
Nmap scan report for 192.0.0.25 [host down, received no-response]
Nmap scan report for 192.0.0.26 [host down, received host-unreach]
Nmap scan report for 192.0.0.27 [host down, received host-unreach]
Nmap scan report for 192.0.0.28 [host down, received no-response]
Nmap scan report for 192.0.0.29 [host down, received no-response]
Nmap scan report for 192.0.0.30 [host down, received no-response]
Nmap scan report for 192.0.0.31 [host down, received no-response]
Nmap scan report for 192.0.0.32 [host down, received no-response]
Nmap scan report for 192.0.0.33 [host down, received no-response]
Nmap scan report for 192.0.0.34 [host down, received no-response]
Nmap scan report for 192.0.0.35 [host down, received no-response]
Nmap scan report for 192.0.0.36 [host down, received host-unreach]
Nmap scan report for 192.0.0.37 [host down, received no-response]
Nmap scan report for 192.0.0.38 [host down, received host-unreach]
Nmap scan report for 192.0.0.39 [host down, received no-response]
```

## Nmap Timing Options

1. Tricky scan to avoid IDS

```
(kali㉿kali)-[~] nmap -T1 192.168.1.11 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 22:19 IST
Initiating Ping Scan at 22:19
Scanning 192.168.1.11 [2 ports]
Completed Ping Scan at 22:19, 15.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:19
Completed Parallel DNS resolution of 1 host. at 22:19, 0.01s elapsed
Initiating Connect Scan at 22:19
Scanning 192.168.1.11 [1000 ports]
Discovered open port 5900/tcp on 192.168.1.11
Connect Scan Timing: About 0.35% done
Discovered open port 53/tcp on 192.168.1.11
Connect Scan Timing: About 0.55% done
Connect Scan Timing: About 0.75% done
Connect Scan Timing: About 0.95% done
Connect Scan Timing: About 1.05% done; ETC: 03:05 (4:42:43 remaining)
Discovered open port 21/tcp on 192.168.1.11
Discovered open port 25/tcp on 192.168.1.11
Discovered open port 80/tcp on 192.168.1.11
Discovered open port 139/tcp on 192.168.1.11
Discovered open port 3306/tcp on 192.168.1.11
Discovered open port 445/tcp on 192.168.1.11
Connect Scan Timing: About 1.75% done; ETC: 02:51 (4:27:37 remaining)
Discovered open port 23/tcp on 192.168.1.11
```

## 2. Timely Scan

```
kali@kali:~  
File Actions Edit View Help  
(kali㉿kali)-[~]  
└─$ nmap -T2 192.168.1.11 -vv  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 22:25 IST  
Initiating Ping Scan at 22:25  
Scanning 192.168.1.11 [2 ports]  
Completed Ping Scan at 22:25, 0.40s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 22:25  
Completed Parallel DNS resolution of 1 host. at 22:25, 0.01s elapsed  
Initiating Connect Scan at 22:25  
Scanning 192.168.1.11 [1000 ports]  
Discovered open port 139/tcp on 192.168.1.11  
Discovered open port 80/tcp on 192.168.1.11  
Discovered open port 53/tcp on 192.168.1.11  
Discovered open port 445/tcp on 192.168.1.11  
Discovered open port 23/tcp on 192.168.1.11  
Discovered open port 21/tcp on 192.168.1.11  
Discovered open port 111/tcp on 192.168.1.11  
Discovered open port 22/tcp on 192.168.1.11  
Discovered open port 25/tcp on 192.168.1.11  
Discovered open port 3306/tcp on 192.168.1.11  
Discovered open port 5900/tcp on 192.168.1.11  
Connect Scan Timing: About 6.65% done; ETC: 22:33 (0:07:15 remaining)  
Connect Scan Timing: About 13.65% done; ETC: 22:33 (0:06:26 remaining)  
Connect Scan Timing: About 20.25% done; ETC: 22:33 (0:05:58 remaining)  
Discovered open port 513/tcp on 192.168.1.11  
Discovered open port 6667/tcp on 192.168.1.11  
Connect Scan Timing: About 27.25% done; ETC: 22:33 (0:05:23 remaining)  
Connect Scan Timing: About 34.05% done; ETC: 22:33 (0:04:58 remaining)  
Connect Scan Timing: About 40.95% done; ETC: 22:33 (0:04:25 remaining)  
Discovered open port 6000/tcp on 192.168.1.11  
Connect Scan Timing: About 47.45% done; ETC: 22:33 (0:03:57 remaining)  
Connect Scan Timing: About 54.15% done; ETC: 22:33 (0:03:27 remaining)  
Discovered open port 5432/tcp on 192.168.1.11  
Discovered open port 1524/tcp on 192.168.1.11  
Discovered open port 8180/tcp on 192.168.1.11  
Connect Scan Timing: About 59.95% done; ETC: 22:33 (0:03:03 remaining)  
Discovered open port 8009/tcp on 192.168.1.11  
Connect Scan Timing: About 66.25% done; ETC: 22:33 (0:02:35 remaining)  
Discovered open port 2121/tcp on 192.168.1.11  
Discovered open port 514/tcp on 192.168.1.11  
Connect Scan Timing: About 72.65% done; ETC: 22:33 (0:02:06 remaining)  
Connect Scan Timing: About 79.25% done; ETC: 22:33 (0:01:35 remaining)  
Connect Scan Timing: About 86.05% done; ETC: 22:33 (0:01:04 remaining)  
Discovered open port 512/tcp on 192.168.1.11  
Connect Scan Timing: About 93.35% done; ETC: 22:33 (0:00:30 remaining)  
Discovered open port 2049/tcp on 192.168.1.11  
Discovered open port 1099/tcp on 192.168.1.11  
Completed Connect Scan at 22:33, 451.51s elapsed (1000 total ports)  
Nmap scan report for 192.168.1.11  
Host is up, received syn-ack (0.00040s latency).  
Scanned at 2023-09-05 22:25:57 IST for 451s  
Not shown: 977 closed tcp ports (conn-refused)
```

## Scan Options

1. Scan without ping

```
(kali㉿kali)-[~] capng
└─$ sudo nmap -Pn 192.168.11.1 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 22:36 IST
Initiating Parallel DNS resolution of 1 host. at 22:36
Completed Parallel DNS resolution of 1 host. at 22:36, 0.01s elapsed
Initiating SYN Stealth Scan at 22:36
Scanning 192.168.11.1 [1000 ports]
SYN Stealth Scan Timing: About 15.00% done; ETC: 22:40 (0:02:56 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 22:40 (0:02:22 remaining)
SYN Stealth Scan Timing: About 44.50% done; ETC: 22:40 (0:01:53 remaining)
SYN Stealth Scan Timing: About 59.50% done; ETC: 22:40 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.00% done; ETC: 22:40 (0:00:53 remaining)
Completed SYN Stealth Scan at 22:40, 205.01s elapsed (1000 total ports)
Nmap scan report for 192.168.11.1
Host is up, received user-set.
Scanned at 2023-09-05 22:36:54 IST for 205s
All 1000 scanned ports on 192.168.11.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 205.11 seconds
Raw packets sent: 2000 (88.000KB) | Rcvd: 8 (672B)
```

## 2. Traceroute

```
(kali㉿kali)-[~]
└─$ sudo nmap -traceroute 192.168.11.1 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-05 22:41 IST
Initiating Ping Scan at 22:41
Scanning 192.168.11.1 [4 ports]
Completed Ping Scan at 22:41, 3.03s elapsed (1 total hosts)
Nmap scan report for 192.168.11.1 [host down, received no-response]
Read data files from: /usr/bin/../share/nmap
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 3.11 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```