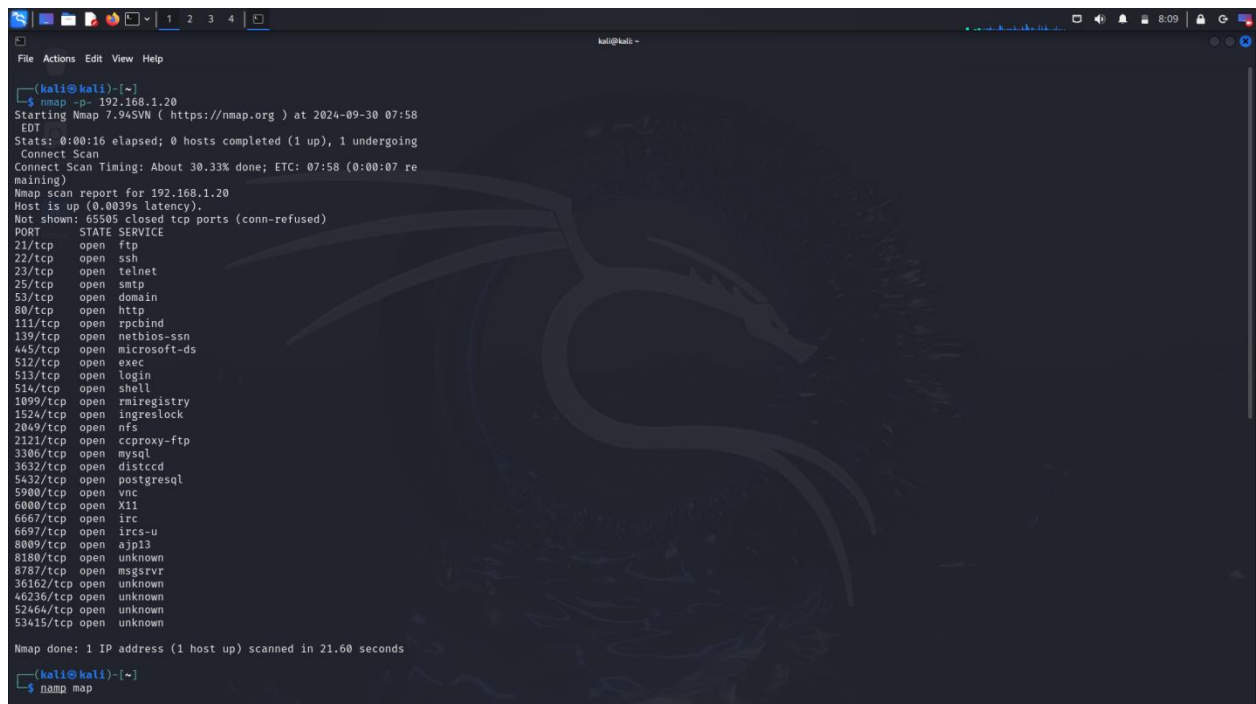


# Nmap Reference Guide

- **Commands :**

## 1)nmap -p-

The nmap -p- command instructs Nmap to scan all 65,535 TCP ports on a target host. This comprehensive scan helps identify open ports, which can reveal services running on the target and potential vulnerabilities.

A screenshot of a Kali Linux terminal window. The terminal shows the execution of the command 'nmap -p- 192.168.1.20'. The output displays the Nmap scan report for 192.168.1.20, indicating that the host is up and listing 28 open ports with their corresponding services. The scan took 21.60 seconds to complete. The terminal window has a dark background with a faint dragon logo in the background.

```
(kali@kali) ~  
$ nmap -p- 192.168.1.20  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 07:58 EDT  
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 30.33% done; ETC: 07:58 (0:00:07 remaining)  
Nmap scan report for 192.168.1.20  
Host is up (0.0039s latency).  
Not shown: 65505 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  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
6697/tcp  open  ircs-u  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
8787/tcp  open  msgsrvr  
36162/tcp open  unknown  
46236/tcp open  unknown  
52464/tcp open  unknown  
53415/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds  
  
(kali@kali) ~  
$ nmap map
```

## 2)nmap -sV

The nmap -sV command is used to perform a service version detection scan on a target. It identifies open ports and attempts to determine the versions of the services running on those ports, providing valuable information for vulnerability assessment and penetration testing.

```
kali@kali:~$ nmap -sV 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:25 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0051s 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 30.06 seconds

kali@kali:~$
```

### 3)nmap -A

The nmap -A command enables aggressive scanning, which include OS detection, service version detection, script scanning, and traceroute. This comprehensive approach provides detailed information about the target's operating system, open ports, services, and potential vulnerabilities, making it useful for in depth reconnaissance.

```
(kali@kali)~$ nmap -A 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:28 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0057s 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 192.168.1.32
|_  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
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 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_title: Metasploitable2 - Linux
|_http_server_header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_  program version  port/proto  service
|_  100000  2             111/tcp    rpcbind
|_  100000  2             111/udp    rpcbind
```

## 4)nmap -O

The nmap `-O` command is used for operating system detection on a target host. It analyzes various network characteristics and responses to identify the OS and its version, helping security professionals understand the environment they are assessing.

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ nmap -O 192.168.1.20  
TCP/IP fingerprinting (for OS scan) requires root privileges.  
QUITTING!  
[kali@kali]~  
$ sudo nmap -O 192.168.1.20  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:33 EDT  
Nmap scan report for 192.168.1.20  
Host is up (0.0022s 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  
6080/tcp  open  x11  
6667/tcp  open  irc  
8000/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 00:0C:29:17:0E:7C (VMware)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
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 1.84 seconds  
[kali@kali]~
```

## 5) nmap -sC

The `nmap -sC` command enables the use of default scripts from Nmap's scripting engine (NSE) during a scan. These scripts can perform a variety of task, such as service discovery, vulnerability detection, and more, providing additional insights into the target's security posture.



```
(kali@kali)-[~]
└─$ nmap -sC 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:37 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STATE:
|_FTP server status:
|_   Connected to 192.168.1.32
|_   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
|_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
25/tcp    open  smtp
|_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
|_ssl-date: 2024-09-30T12:39:16+00:00; +3s from scanner time.
|_sslsv2:
|_SSLv2 supported
|_ciphers:
|_   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_   SSL2_DES_64_CBC_WITH_MD5
|_   SSL2_DES_192_EDE3_CBC_WITH_MD5
|_   SSL2_RC4_128_WITH_MD5
|_   SSL2_RC2_128_CBC_WITH_MD5
|_   SSL2_RC4_128_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind
```