

Report **Nmap** Metasploitable 192.168.50.101

- **Os fingerprint**

sudo nmap -O 192.168.50.101

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)~$ nmap -O 192.168.50.101
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

(kali@kali)~$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:18 CEST
EST
Nmap scan report for 192.168.50.101
Host is up (0.000825 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
2386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8000/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:88:26:67 (Oracle VirtualBox virtual NIC)
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 14.67 seconds

(kali@kali)~$

```

- **Syn Scan**

sudo nmap -sS 192.168.50.101

```

kali@kali: ~
File Actions Edit View Help

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 14.67 seconds

(kali@kali)~$ nmap -sS 192.168.50.101
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)~$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:28 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000655 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
2386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8000/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:88:26:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds

(kali@kali)~$

```

- TCP connect

`sudo nmap -sT 192.168.50.101`

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nmap -sT 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:40 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0031s 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: 08:00:27:88:26:67 (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds  
kali@kali:~$
```

- Version Detection

`sudo nmap -sV 192.168.50.101`

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nmap -sV 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:47 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0014s 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  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath gmrregistry  
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 66.15 seconds  
kali@kali:~$
```

Report *Nmap* Windows 7 192.168.50.102

- *Os fingerprint*

`sudo nmap -Pn -O 192.168.50.102`

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:00 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0016s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:2F:51:53 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update
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 15.95 seconds
(kali@kali)-[~]
$ 

```