

```
(kali㉿kali)-[~]  
$ sudo nmap -O 192.168.1.103  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:19 EST  
Nmap scan report for 192.168.1.103  
Host is up (0.00057s 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: 08:00:27:49:56:27 (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 18.95 seconds

```
(kali㉿kali)-[~]  
$
```

KALI LINUX

"the quieter you become, the more you are able to hear"

(kali㉿kali)-[~]

\$ sudo nmap -sS 192.168.1.103

Starting Nmap 7.93 (<https://nmap.org>) at 2023-02-22 08:25 EST

Stats: 0:00:14 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan

Parallel DNS resolution of 1 host. Timing: About 0.00% done

Nmap scan report for 192.168.1.103

Host is up (0.0011s 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: 08:00:27:49:56:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.86 seconds

KALI LINUX

"the quieter you become, the more you are able to hear"

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:25 EST
Stats: 0:00:14 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.1.103
Host is up (0.0011s 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: 08:00:27:49:56:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.86 seconds
```

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:31 EST
Nmap scan report for 192.168.1.103
Host is up (0.0022s 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: 08:00:27:49:56:27 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds
```

(kali@kali)-[~]

\$ sudo nmap -sV 192.168.1.103

Starting Nmap 7.93 (<https://nmap.org>) at 2023-02-22 08:40 EST

Nmap scan report for 192.168.1.103

Host is up (0.0017s latency).

Not shown: 977 closed tcp ports (reset)

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 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	unknown	

MAC Address: 08:00:27:49:56:27 (Oracle VirtualBox virtual NIC)

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 189.72 seconds

```
(kali㉿kali)-[~]  
$ sudo nmap -O 192.168.1.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 08:52 EST  
Nmap scan report for 192.168.1.101  
Host is up (0.00055s latency).  
All 1000 scanned ports on 192.168.1.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:58:60:A5 (Oracle VirtualBox virtual NIC)  
Too many fingerprints match this host to give specific OS details  
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 41.40 seconds
```

File Actions Edit View Help

(kali@kali)-[~] home

\$ sudo nmap -O 192.168.1.101 #ip di windows7

[sudo] password for kali:

Starting Nmap 7.93 (<https://nmap.org>) at 2023-02-22 10:19 EST

Nmap scan report for 192.168.1.101

Host is up (0.00048s latency).

All 1000 scanned ports on 192.168.1.101 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:58:60:A5 (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

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 41.94 seconds