

(kali㉿kali)-[~]

\$ sudo nmap -O 192.168.50.102

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-06-26 09:37 EDT

Nmap scan report for 192.168.50.102

Host is up (0.00029s latency).

Not shown: 987 closed tcp ports (reset)

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
2869/tcp	open	icslap
5357/tcp	open	wsdapi
10243/tcp	open	unknown
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	unknown
49159/tcp	open	unknown

MAC Address: 08:00:27:2A:FD:FD (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 1

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

(kali@kali)-[~]

\$ sudo nmap -sS 192.168.5.101

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-06-26 09:10 EDT

Nmap scan report for 192.168.5.101

Host is up (0.0040s 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	filtered	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

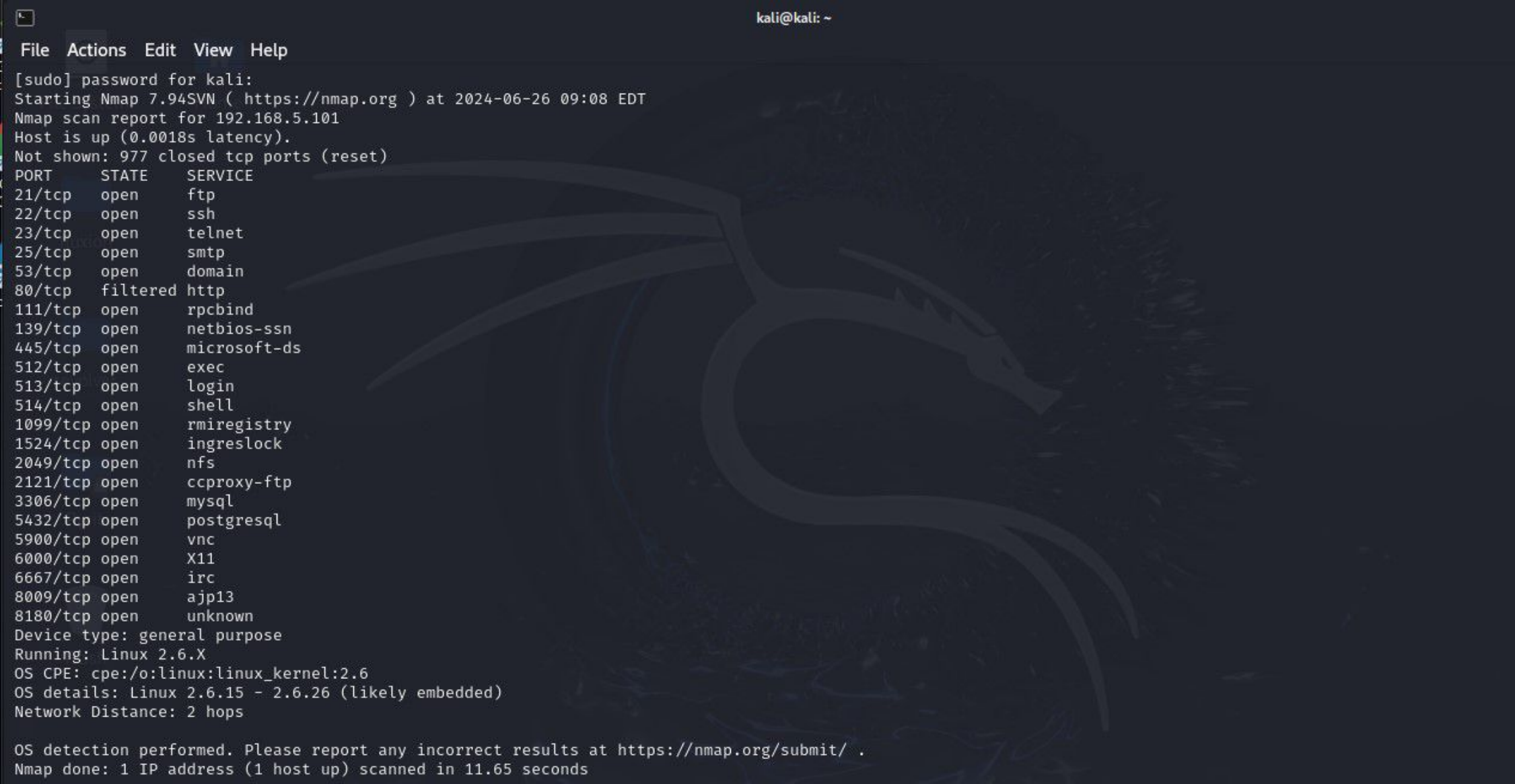
Nmap done: 1 IP address (1 host up) scanned in 8.78 seconds

(kali@kali)-[~]

\$

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.5.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 09:12 EDT
Nmap scan report for 192.168.5.101
Host is up (0.0042s 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    filtered   http
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?
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 29.41 seconds
```

A terminal window with a dark background featuring a large, faint dragon logo, which is the Kali Linux mascot. The terminal shows the output of an Nmap scan. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal text includes the command '[sudo] password for kali:', the Nmap version '7.94SVN', the target IP '192.168.5.101', and a list of open ports and services. The background dragon is a stylized, dark-colored creature with long, flowing wings and a long tail, coiled around the terminal text.

File Actions Edit View Help

[sudo] password for kali:
Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-06-26 09:08 EDT
Nmap scan report for 192.168.5.101
Host is up (0.0018s 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	filtered	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

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.15 - 2.6.26 (likely embedded)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 11.65 seconds

(kali㉿kali)-[~]

\$ sudo nmap -sT 192.168.5.101

Starting Nmap 7.94SVN (<https://nmap.org>) at 2024-06-26 09:11 EDT

Nmap scan report for 192.168.5.101

Host is up (0.0088s 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	filtered	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 7.99 seconds