

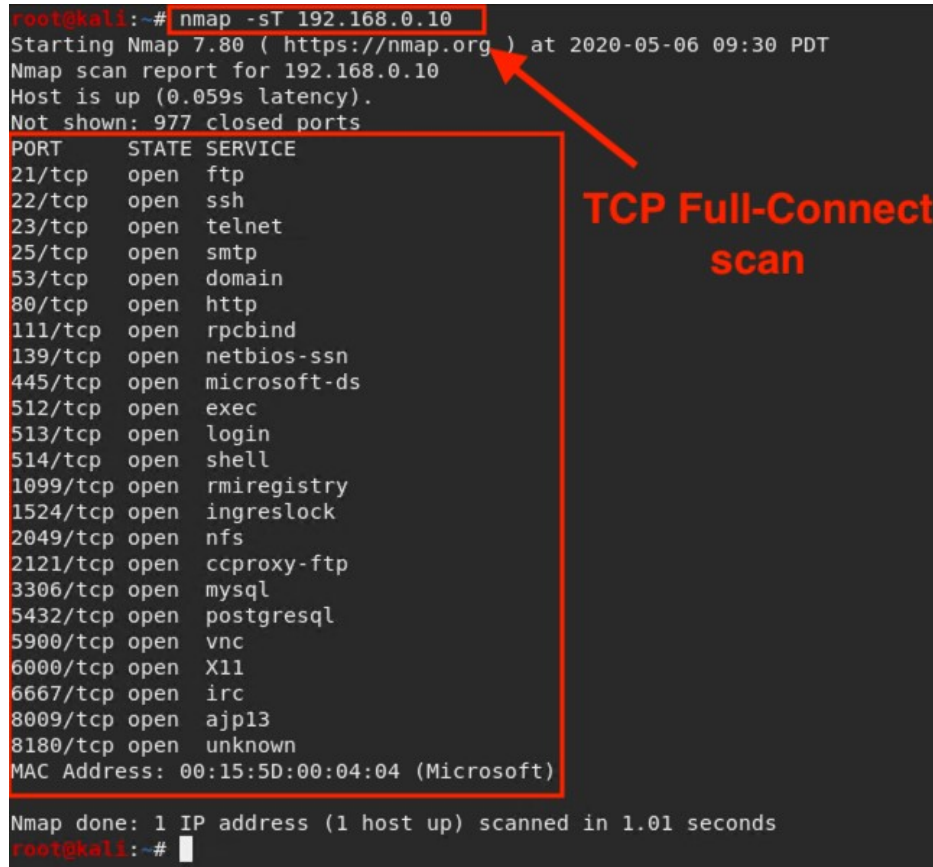
Solution Guide: Port Scanning with Nmap

In this activity, you used Nmap in an investigative capacity.

1. Perform a basic TCP connect scan against Metasploitable 2.

- Run the command to perform a TCP connect scan:

```
■ nmap -sT 192.168.0.10
```



```
root@kali:~# nmap -sT 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-06 09:30 PDT
Nmap scan report for 192.168.0.10
Host is up (0.059s latency).
Not shown: 977 closed ports
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: 00:15:5D:00:04:04 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
root@kali:~#
```

TCP Full-Connect scan

- Of the ports listed, which two present the biggest potential vulnerability and why?
 - Port 5900 , service VNC, is a remote desktop connection that could be exploited to provide remote control to an attack.
 - Port 6667 , service IRC, can be used as a C2 channel that receives instructions from a botnet.

2. Run the command that performs a service and version detection scan against the target:

- `nmap -sV 192.168.0.10`

Notice that in addition to the service type, Nmap displays the enumerated version numbers.

```

root@kali:~# nmap -sV 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) 2020-05-06 09:31 PDT
Nmap scan report for 192.168.0.10
Host is up (0.041s latency).
Not shown: 977 closed ports
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
MAC Address: 00:15:5D:00:04:04 (Microsoft)
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 12.79 seconds
root@kali:~#

```

- What web service and version is running?

- Apache httpd 2.2.8 ((Ubuntu) DAV/2)

- Is this web service version vulnerable and if so what is it?

- Yes, very. One possible vulnerability is CVE-2016-4975 (possible CRLF injection), which allows HTTP response splitting attacks for sites that use `mod_userdir`.

3. Look at port 21 . Google VSFTPD v2.3.4.

- VSFTPD v2.3.4 is vulnerable to backdoor command execution, which presents a threat to organizations running this particular version of software.

• How is this information useful to an attacker?

- Knowing the web server type and version number allows an attacker to compile a list of potential vulnerabilities to exploit.

3. Experiment with using various scan techniques and interpret the results.

- Type `nmap` at the command prompt to get a list of commands that you can play with.