Nmap, TCPDump and Grep

Jun 10, 2021

Nmap

Nmap stands for “Network Mapper.” It is an open source tool for network security, auditing and system administration. At the most basic level, nmap allows for scanning a network and returning which addresses are response and what ports are open.

Nmap Discovery Scans

Discovery scans are used to footprint a network. Footprinting allows provides an overall, high-level view of a network. Using nmap you can perform footprinting of a network.

```
nmap 10.0.2.0/24
```

- Scans all IP addresses in the subnet
- Default scan sends a ping and TCP ACK to ports 80 and 443
- If the host responds, nmap will initiate a port scan of the top 1000 ports on the host. This scan will alert an IDS.

In this instance I have scanned my virtual subnet. The host 10.0.2.4 is running the metasploitable VM and returns the following open ports.

```
kali@kali: ~
File  Actions  Edit  View  Help

Nmap scan report for 10.0.2.4
Host is up (0.00024s 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

Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
All 1000 scanned ports on 10.0.2.15 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 12.19 seconds
```

```
nmap -sn 10.0.2.0/24
```

- Performs a host discovery scan
- Does not perform a port scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 08:11 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00034s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00074s latency).
Nmap scan report for 10.0.2.4
Host is up (0.00045s latency).
Nmap scan report for 10.0.2.15
Host is up (0.000088s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.98 seconds
```

```
nmap -sL 10.0.2.0/24
```

- Lists all IP addresses from the range

- Attempts to discovery any host names associated with the IP addresses
- Passive method

```
nmap -PS -p80 10.0.2.0/24
```

- TCP SYN ping. Probes specific ports from the list
- Uses a TCP SYN packet instead of ICMP, as some firewalls will block ICMP and IDS will alert on ICMP.

```
┌──(kali㉿kali)-[~]
└─$ nmap -PS -p80 10.0.2.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 17:48 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00047s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 10.0.2.4
Host is up (0.00040s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 10.0.2.15
Host is up (0.00042s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.12 seconds
```

```
map --scan-delay 10s -p22,23,80  10.0.2.4
```

- Issues a 10 second scan delay between ports when scanning
- Helps avoid detection, although can still be picked up by an IPS

```
┌──(kali㉿kali)-[~]
└─$ nmap --scan-delay 10s -p22,23,80  10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 17:59 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0015s latency).

PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 40.14 seconds
```

```
nmap -T4 10.0.2.0/24
```

- Issues scanning probes with a timing pattern to avoid detection

- 0 is the slowest, 5 is the fastest.

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 08:29 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00017s 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
```

```
nmap -sI 10.0.2.0/24
```

- A stealth scan method
- Makes the can appear as if it is coming from somewhere else.
- Hides the identity of the scanning machine

```
nmap 10.0.2.0/24 -oN 'Desktop/output.txt'
nmap 10.0.2.0/24 -oX 'Desktop/output.xml'
nmap 10.0.2.0/24 -oG 'Desktop/output.txt'
```

- Outputs nmap to a text file, xml file or greppable output respectively. These file formats can then be ingested by a SIEM.

Nmap Port Scans

Port scanning allows us to determine which services and which version of the services are in use by a given host.

```
nmap 10.0.2.4 -sS
```

- TCP SYN, sends a half-open scan to identify the port state

- Does not send an ACK packet afterwards.
- May require admin priveleges on the system
- More of a stealthy approach

```
nmap 10.0.2.4 -sT
```

- TCP Connect Scan
- Sends the full 3 way handshake, SYN and SYNACK
- Does not require raw packet priveleges on a workstation
- Establishes a connection with a connect system call.

```
nmap 10.0.2.4 -sN
```

- A null scan
- Conducts scan by sending the header bit set to zero

```
nmap 10.0.2.4 -sF
```

- Conducts a scan by sending an unexpected FIN packed
- Not stealthy

```
nmap 10.0.2.4 -sX
```

- Christmas scan. Least stealthy, will set off alarm bells.
- Sends a packet by sending a packet with the FIN, PSH and URG flags set to one.

```
nmap 10.0.2.4 -sU
```

- UDP Scan
- Sends a UDP packet and waits for the packet to timeout, since there is no handshake.

```
nmap 10.0.2.4 -p80,22,23,443,53
```

- Scan a pre-specified port range.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# nmap 10.0.2.4 -p80,22,23,443,53
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 18:17 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00030s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
23/tcp  open   telnet
53/tcp  open   domain
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:E9:0E:D2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Nmap Fingerprinting Scans

Fingerprinting is a technique for collecting detailed information about an individual target. Nmap uses the Common Platfor Enumeration (CPE) scheme a standard scheme for identifying devices, operating systems and applications. Nmap compares responses to the CPE in order to determine the version of a service running.

```
nmap 10.0.2.4 -sV
```

- Provides basic versioning info for ports, services and OS

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# nmap 10.0.2.4 -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 18:25 EDT
Nmap scan report for 10.0.2.4
Host is up (0.000092s 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: 08:00:27:E9:0E:D2 (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 12.02 seconds
```

```
nmap 10.0.2.4 -A
```

- Provides detailed versioning info

Nmap Port States

When performing fingerprinting and scanning ports, nmap will return a range of different port states.

Standard States:

- Open - Application on the host is accepting connections
- Closed - Port not open; responds to probes with a rest RST packet
- Filtered - Nmap cannot probe the port; possibly due to a firewall

Other States:

- Unfiltered - Rare; Nmap can probe the port, but not determine if open or closed.
-

Open	Filtered - Nmap cannot determine if a port is open or filtered

-

Open	Closed - Nmap cannot determine if a port is closed or filtered when doing a TCP idle scan

TCP Dump

TCP dump is a utility that records the contents of packets on a network interface. Here I will combine TCPdump with nmap in order to record the packet traces of a scan.

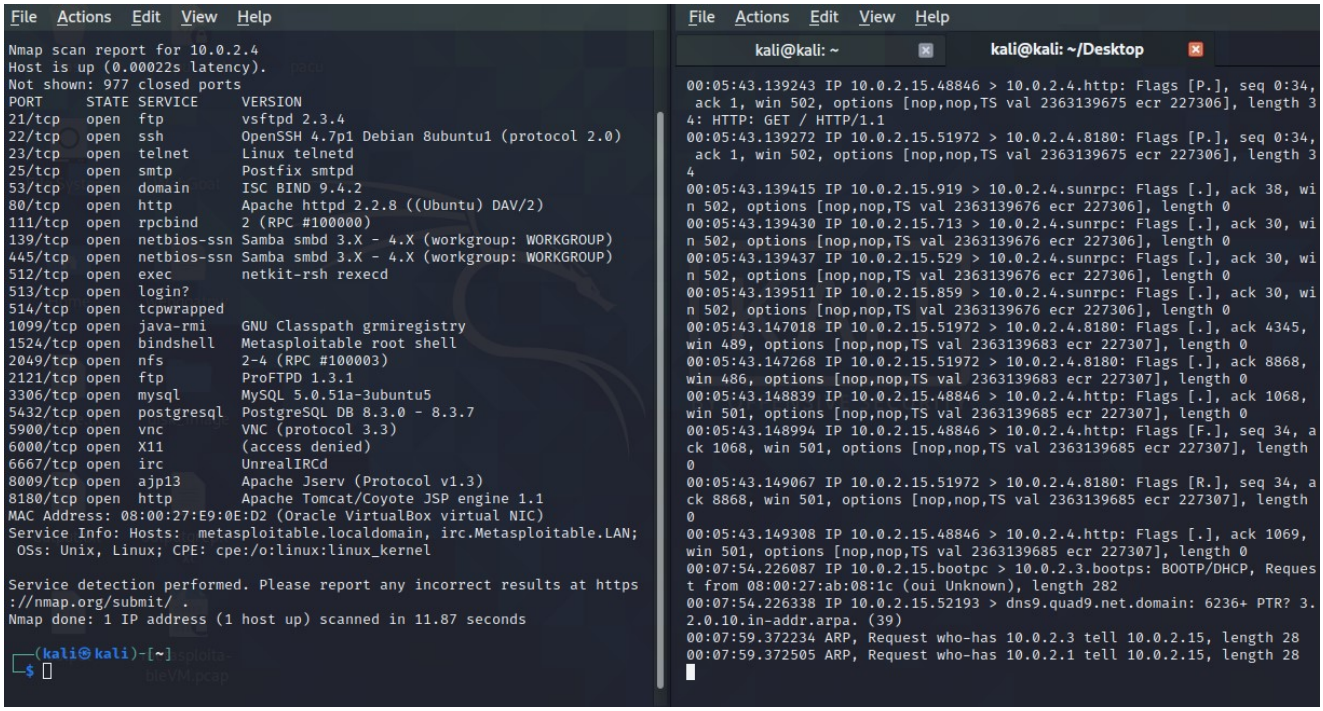
```
sudo tcpdump -i eth0
```

- Basic syntax to start tcpdump on the interface ethernet0.

```
sudo tcpdump -i eth0 src 10.0.2.15
```

- Start tcpdump on the interface ethernet0.
- Only collects packets with a source of 10.0.2.15, i.e. my current system

Here is an example of running tcpdump while conducting an nmap sV scan against the 10.0.2.0/24 subnet:




```
sudo tcpdump -i eth0 dst 10.0.2.4
```

- Start tcpdump on the interface ethernet0.
- Only collects packets with a destination of 10.0.2.15, i.e. a target VM system

```
sudo tcpdump -i eth0 dst 10.0.2.4 -w /home/kali/Desktop/metasploitableVI
```

- Start tcpdump on the interface ethernet0.
- Only collects packets with a destination of 10.0.2.15, i.e. a target VM system
- Saves the capture to a file called “metasploitableVM.pcap” on my desktop

```
sudo tcpdump -r /home/kali/Desktop/metasploitableVM.pcap
```

- Reads the file just created via packet capture

```
sudo tcpdump dst port 23 -r /home/kali/Desktop/metasploitableVM.pcap
```

- Reads the file just created via packet capture
- Filters on traffic to port 23 for Telnet

```
sudo tcpdump dst port 23 -r /home/kali/Desktop/metasploitableVM.pcap
```

- Reads the file just created via packet capture
- Filters on traffic to port 23 for Telnet
- Shows the traffic in HEX and ASCII.

```
tcpdump -i en0 10.0.2.4
```

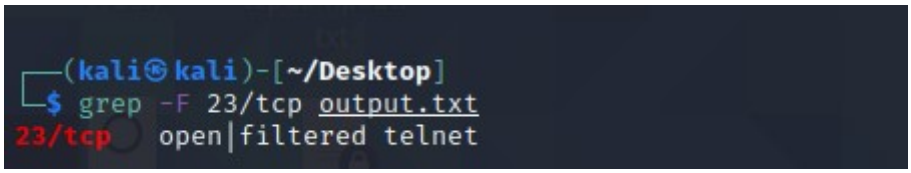
- Starts tcpdump on interface en0 and records all traffic going to 10.0.2.4

Grep

Command line tool on unix-based systems that invokes simple string matching and regex syntax. Using grep we can retrieve specific lines from the nmap and tcpdump commands run previously.

```
grep -F 23/tcp output.txt
```

- -F stands for simple search
- Searches all lines in output.txt for the ‘23/tcp’, i.e. telnet.




```
grep '23' *
```

- Searches all files in the current working directory for ‘23’, i.e. telnet
- Prints the output to the screen, showing which are files and which are directories.

grep practice

```
grep -r 10\.0\.2\.[0-255] output2grep.txt
```

- searches the output2grep.txt file for valid ip addresses in the above range
- -r is used for regular expressions
- \ is used as an escape character for regular expressions


```
grep -i
```

- -i ignores case sensivity.
- grep is case sensitive by default

```
rep -v '80/tcp' output.txt
```

- returns non-matching lines

- Excludes every line with has tcp 80

```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep -v -E '22|25|53|80' output.txt
# Nmap 7.91 scan initiated Sat Jun 12 02:12:11 2021 as: nmap -sX -oN output.txt 10.0.2.4
Nmap scan report for 10.0.2.4
Host is up (0.00021s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
23/tcp   open|filtered telnet
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
MAC Address: 08:00:27:E9:0E:D2 (Oracle VirtualBox virtual NIC)
```

```
grep -v -E '22|25|53|80' output.txt
```

- Returns all lines that do not match 22, 25, 53 or 80
- This could be used to narrow a search and look for specific ports.


```
┌──(kali㉿kali)-[~/Desktop]
└─$ grep -v -E '22|25|53|80' output.txt
# Nmap 7.91 scan initiated Sat Jun 12 02:12:11 2021 as: nmap -sX -oN output.txt 10.0.2.4
Nmap scan report for 10.0.2.4
Host is up (0.00021s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
23/tcp   open|filtered telnet
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
MAC Address: 08:00:27:E9:0E:D2 (Oracle VirtualBox virtual NIC)
```


```
grep -w
```

- treats search strings as distinct words

```
grep -c
```

- returns a count of matching words

```
grep -l
```

- returns names of files with matching lines

```
grep -L
```

- returns names of files without matching lines

cut

A command that enables a user to specify which text on a line which can be removed

```
cut -c5 syslog.txt
```

Returns only the fifth character in each line from the syslog file

```
cut -c5-5 syslog.txt
```

Return only the 5-10 characters from each line in the file

sort

Can be used to change the output order of a file

```
sort syslog.txt
```

Returns the file in alphabetical order

```
sort -r syslog.txt
```

Returns the file in reverse alphabetical order

```
sort -n syslog.txt
```

Returns the file in numerical order

```
sort -k 2 syslog.txt
```

Returns sorted based on the 2nd column

head & tail

Returns the first 10 or last 10 lines of a file specified

```
head syslog.txt
tail syslog.txt
```

Edge Thoughts

Edge Thoughts halfbackflip A tiny techy blog where I write stuff.