Introduction to nmap

SecureSet Academy

PATRICK MOONEY

Welcome and Warnings

- Welcome to SecureSet Academy's Hacking 101: nmap Session

- Port scanning in some jurisdictions is considered illegal and unauthorized access to a computer system. Port scan only with permission. Port scanning can also crash systems, resulting in loss of service for that system … and that system could be critical infrastructure. Again: port scan systems only with permission.

Before We Get Too Deep …

- Need a shell but don't have a VM or Linux machine handy? Do you have a web browser and a Gmail account?

https://console.cloud.google.com/cloudshell/editor?shellonly=true

```
sudo apt-get install nmap
sudo su
```

Network Protocols

- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- … and “sockets”

Addresses

- Each of these doors has an address. Let's call each of these doors the destination of an IP address
- There are 4,294,967,296 IP addresses that we format into four 8-bit values such as 127.0.0.1, with the '.' separating each 8-bit value

Ports

- We've gone inside the IP address/warehouse. Now we have a set of doors inside that space. Each of these doors is a port number. There are 65,535 doors (port numbers) for TCP and UDP each. That's a lot of doors to check.

Socket -> an address & port pair

- “Street Address” + “Door Number” == “IP Address” + “Port Number”
- You can have a street address but there’s not going to meet anyone if you are unable to find an open door.

- Nmap can go around and knock on every door at an address and let you know which doors opened.

Let’s kick some tires

```
root@cs-6000-devshell-vm-c4f38157-0df7-426b-8f33-e67d56e3dfe1:/# nmap 23.239.15.124
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 13:19 EDT
```

- How many doors is it knocking on and how quickly?
- And are we talking TCP or UDP or both?

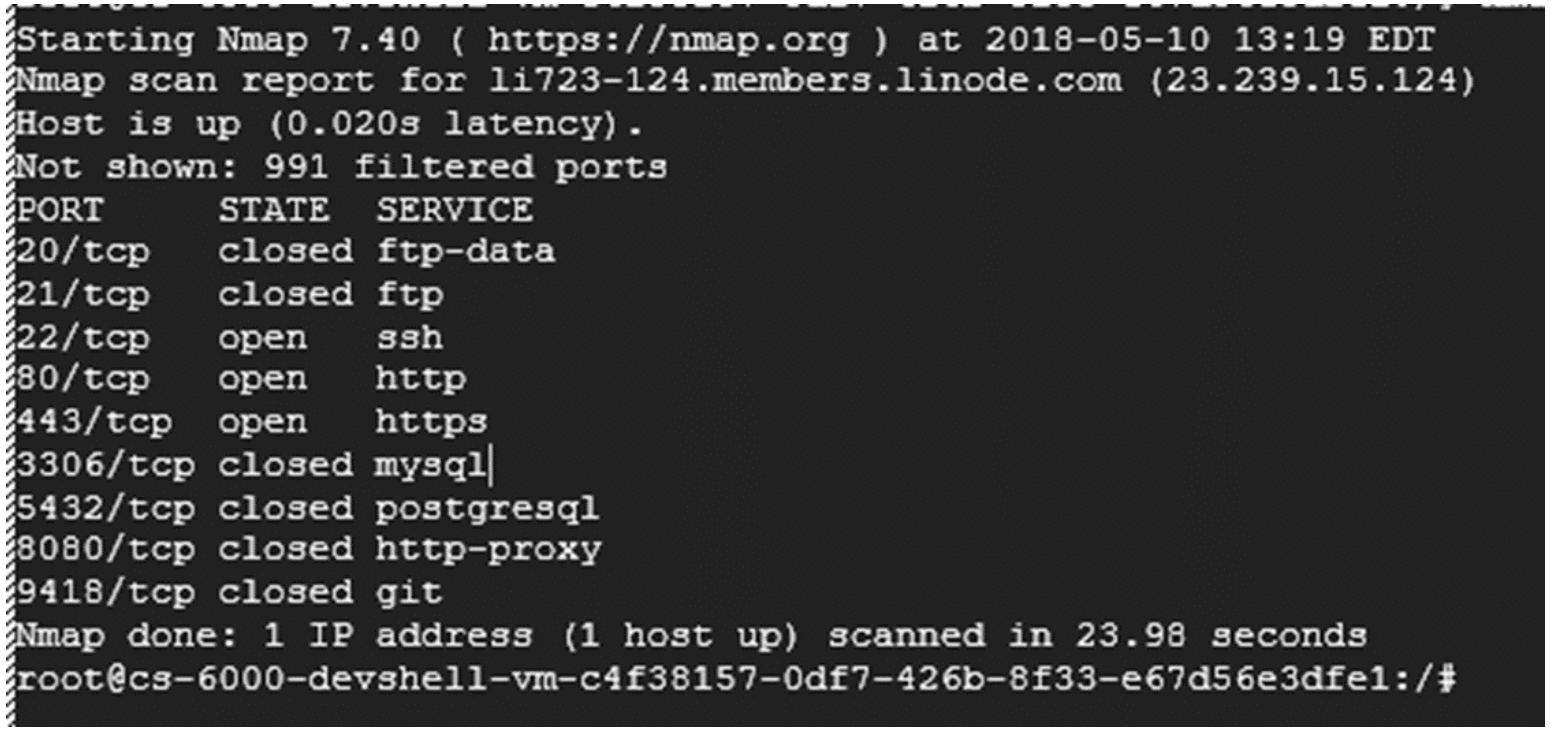
And decipher the results

- Basic nmap results

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 13:19 EDT
Nmap scan report for li723-124.members.linode.com (23.239.15.124)
Host is up (0.020s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3306/tcp closed mysql
5432/tcp closed postgresql
8080/tcp closed http-proxy
9418/tcp closed git
Nmap done: 1 IP address (1 host up) scanned in 23.98 seconds
root@cs-6000-devshell-vm-c4f38157-0df7-426b-8f33-e67d56e3dfe1:/#
```

Incomplete Information!

- But … what do you mean? Open? Closed? Why? How? Prove it!



```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 13:19 EDT
Nmap scan report for li723-124.members.linode.com (23.239.15.124)
Host is up (0.020s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3306/tcp closed mysql
5432/tcp closed postgresql
8080/tcp closed http-proxy
9418/tcp closed git
Nmap done: 1 IP address (1 host up) scanned in 23.98 seconds
root@cs-6000-devshell-vm-c4f38157-0df7-426b-8f33-e67d56e3dfe1:/#
```

A More Complete Answer

- Please give me a '--reason'

```
root@cs-6000-devshell-vm-c4f38157-0df7-426b-8f33-e67d56e3dfe1:/# nmap --reason 23.239.15.124
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 13:21 EDT
Nmap scan report for li723-124.members.linode.com (23.239.15.124)
Host is up, received echo-reply ttl 52 (0.020s latency).
Not shown: 991 filtered ports
Reason: 991 no-responses
PORT     STATE  SERVICE    REASON
20/tcp   closed ftp-data   reset ttl 53
21/tcp   closed ftp        reset ttl 52
22/tcp   open   ssh        syn-ack ttl 52
80/tcp   open   http       syn-ack ttl 52
443/tcp  open   https      syn-ack ttl 53
3306/tcp closed mysql      reset ttl 52
5432/tcp closed postgresql reset ttl 53
8080/tcp closed http-proxy reset ttl 52
9418/tcp closed git        reset ttl 53
Nmap done: 1 IP address (1 host up) scanned in 24.08 seconds
root@cs-6000-devshell-vm-c4f38157-0df7-426b-8f33-e67d56e3dfe1:/#
```

Ping scan

- What if you are not even sure what is on the subnet?

#nmap –sn 192.168.0.1

- This does not port scan but instead does a “ping sweep” (along with a SYN to tcp/443 and an ACK to tcp/80); when run as a priv user it also does ARP Neighbor Discovery

Traceroutes

- Can be done with other commands but …

```
nmap --traceroute 23.239.15.124
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 15:27 EDT
Nmap scan report for li723-124.members.linode.com (23.239.15.124)
Host is up (0.020s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3306/tcp closed mysql
5432/tcp closed postgresql
8080/tcp closed http-proxy
9418/tcp closed git
TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   0.02 ms  172.17.0.1
2   17.93 ms 108.170.236.242
3   18.88 ms 209.85.255.53
4   19.02 ms 108.170.248.36
5   20.85 ms gw2.ewr1.us.linode.com (206.130.10.96)
6   20.86 ms 173.255.239.3
7   19.61 ms li723-124.members.linode.com (23.239.15.124)
Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
```

Scan a Specified Range of IP Addresses

- Let's say you're an administrator and want to check a range of your IP addresses for all connected devices …
- … or you are a penetration tester and your scope has been defined with a range of IP addresses

```
# nmap 23.239.15.124-126
```

Scan for Specific Port Numbers

- Nmap by default scans a large set of common ports.
- What if we need to check for a less common port?
- What if we want to save time (and network noise) and just scan for specific ports?

```
nmap --reason -p 21,22,80,443 23.239.15.124
```

Why is UDP so Difficult?

- Without getting into TCP and UDP fundamentals, UDP is a connectionless and unreliable protocol. Meaning it may not respond immediately.
- So we have to slow down and scan individual port numbers slower, wait for responses, and then move on. It's nasty and not done by default. And when done intentionally requires much patience.

NSE Scripting Engine

- The Nmap Scripting Engine (NSE) provides a way for users and the community to create custom specialized scripts for nmap to follow as it does its magic. This can include checking for specific vulnerabilities for different services. Or doing password guessing attacks. Use with care and with permission only.

Heartbleed NSE

```
nmap -p 443 --script ssl-heartbleed 23.239.15.124
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-10 12:52 EDT
Nmap scan report for li723-124.members.linode.com (23.239.15.124)
Host is up (0.020s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows
ed by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected
g memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encry
ryption keys themselves.
|
|     References:
|
|       http://www.openssl.org/news/secadv_20140407.txt
|_
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

What's my 'Go to'?

- I like to get as much useful information the first pass through as possible.
- Noisy to scan one target more than once to revisit it in order to get further information.

```
nmap -A --reason 23.239.15.124
```

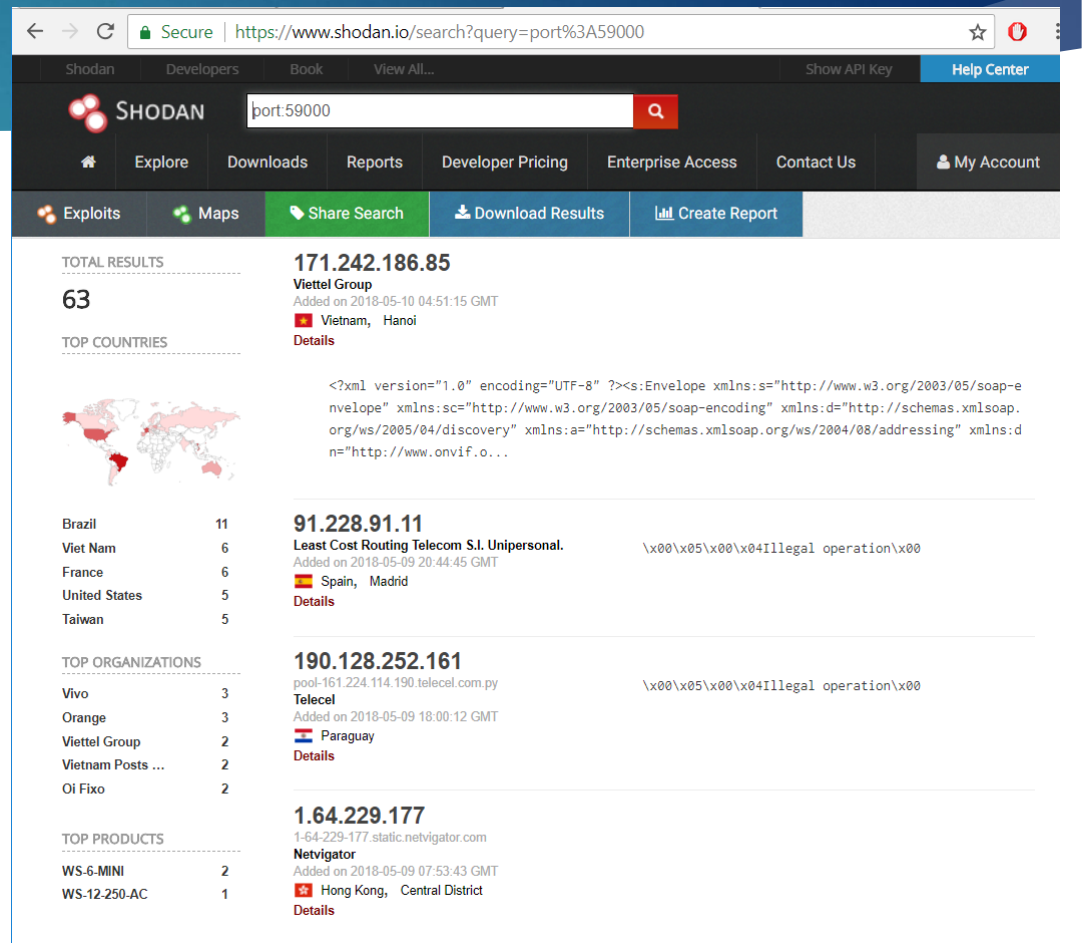
```
Not shown: 991 filtered ports
Reason: 991 no-responses
PORT     STATE  SERVICE    REASON         VERSION
20/tcp   closed ftp-data   reset ttl 53
21/tcp   closed ftp        reset ttl 52
22/tcp   open   ssh        syn-ack ttl 53 OpenSSH 6.0p1 Debian 4 (protocol 2.0)
| ssh-hostkey:
|   1024 f7:a1:af:21:6b:e2:92:10:ba:cd:aa:78:f4:ef:47:95 (DSA)
|   2048 42:e8:c8:b0:d3:38:be:b4:21:e6:14:8f:50:34:a6:ba (RSA)
|_  256 05:88:20:d9:20:63:a5:6f:5d:50:f3:3a:62:f0:53:bd (ECDSA)
80/tcp   open   http       syn-ack ttl 52 Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Scrooge-and-Marley
443/tcp  open   ssl/http   syn-ack ttl 53 Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Scrooge-and-Marley
| ssl-cert: Subject: organizationName=TurnKey Linux
| Not valid before: 2014-12-05T18:26:27
|_Not valid after:  2024-12-02T18:26:27
|_ssl-date: 2018-05-10T21:02:10+00:00; 0s from scanner time.
3306/tcp closed mysql      reset ttl 52
5432/tcp closed postgresql reset ttl 53
8080/tcp closed http-proxy reset ttl 53
9418/tcp closed git        reset ttl 52
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.2
Network Distance: 7 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   0.02 ms  172.17.0.1
2   18.85 ms 108.177.3.58
3   18.80 ms 216.239.62.194
4   20.38 ms 108.170.248.14
5   20.40 ms gw2.ewr1.us.linode.com (206.130.10.96)
6   20.16 ms 173.255.239.21
7   20.30 ms li723-124.members.linode.com (23.239.15.124)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.43 seconds
root@cs-6000-devshell-vm-08e29c96-31ca-4564-88d0-065dbd8b9319:/tmp#
```

Outsourced Port Scanning?

- There are a number of 'Interner Observatory' type businesses out there who perform daily port scans of the **entire IPv4 address space**.
- Not a terrible idea to check sites such as Shodan.io for your business IP addresses, domain name, etc, to see what is Internet-facing that maybe you are not aware ….



Closing Out

- Nmap is **noisy**. Do some of these exercises with Wireshark doing a packet capture (only if you are using nmap locally and not via Gmail ...). You will see a lot (a very lot) of packets. Many of which will have indicators IDS and IPS can take advantage of … there are more stealthy ways of doing this if you are an advanced attacker.

- In some jurisdictions even port scanning is considered illegal. Only port scan with permission.