CorporateBlue

Scanning with NMAP

Michael Wylie

Co-Founder of Corporate Blue

Cybersecurity Consultant

MBA from Texas A&M

Instructor:

- ❑ US Department of Defense
- ❑ California State University, Northridge
- ❑ Moorpark College

CISSP	CEH
CEI	Pentest+
CCNA R&S	CCNA CyberOps
Security+	Project+
CHPA	VCP-DCV
Dell Security	GPEN

Disclaimer

"When used properly, Nmap helps protect your network from invaders. But when used improperly, Nmap can (in rare cases) get you sued, fired, expelled, jailed, or banned by your ISP. Reduce your risk by reading this legal guide before launching Nmap."

- NMAP.org

All the information provided in this course is for educational purposes only. Corporate Blue, Michael Wylie, an BSidesLV is no way responsible for any misuse of the information.

What is Scanning?

Learn more about target network/systems

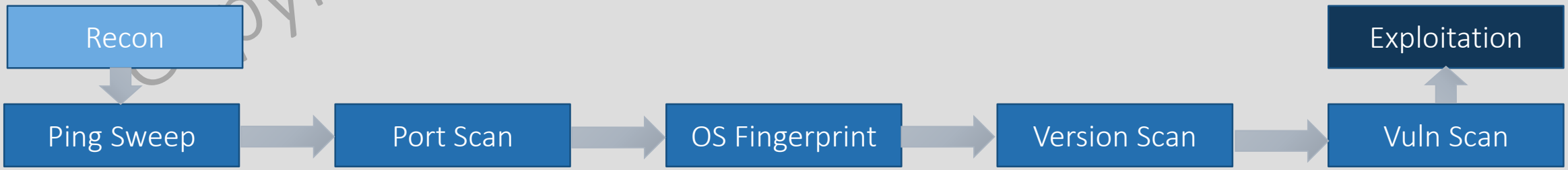
Inventory of environment

Identifying hosts, ports, and services

A probe is sent to a target and response is sent back

Objectives

- Discover live hosts, IP address, and open ports
- Find OS & version
- Locate services & versions
- Find vulnerabilities



How do we find IPs to scan?

OSSINT (e.g. Recon-NG)

Google Hacking (site:example.com)

RIR (ARIN)

Whois

Netcraft

Ping Sweep

Sub Domain Enumeration

- Zone Transfer
- Sublist3r
- Knockpy
- Burp Suite – Intruder
- theHarvester

Scanning Tips

Scan IPs, not hostnames

Scanning Phase

TCP Flags

```
.... ..0. .... = Urgent: Not set
.... ...0 .... = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
```

TCP headers have flags:

SYN = Synchronize = starts a connection between two devices
"Hello, I want to have a conversation with you"

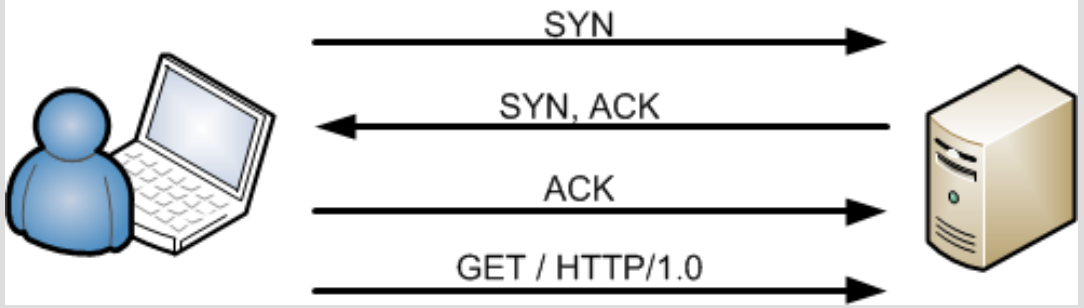
ACK = Acknowledgement = confirms receipt of a packet
"Got your hello, I can hear you loud and clear"

URG = Urgent = requests data to be processed immediately
"There's important data that needs to be handled quickly"

PSH = Push = sends all buffered data immediately
"Don't hold data waiting for more"

FIN = Finish = no more data is coming
"Thanks for the chat, goodbye!"

RST = Resets = resets the connection
"There was an error in the communication"



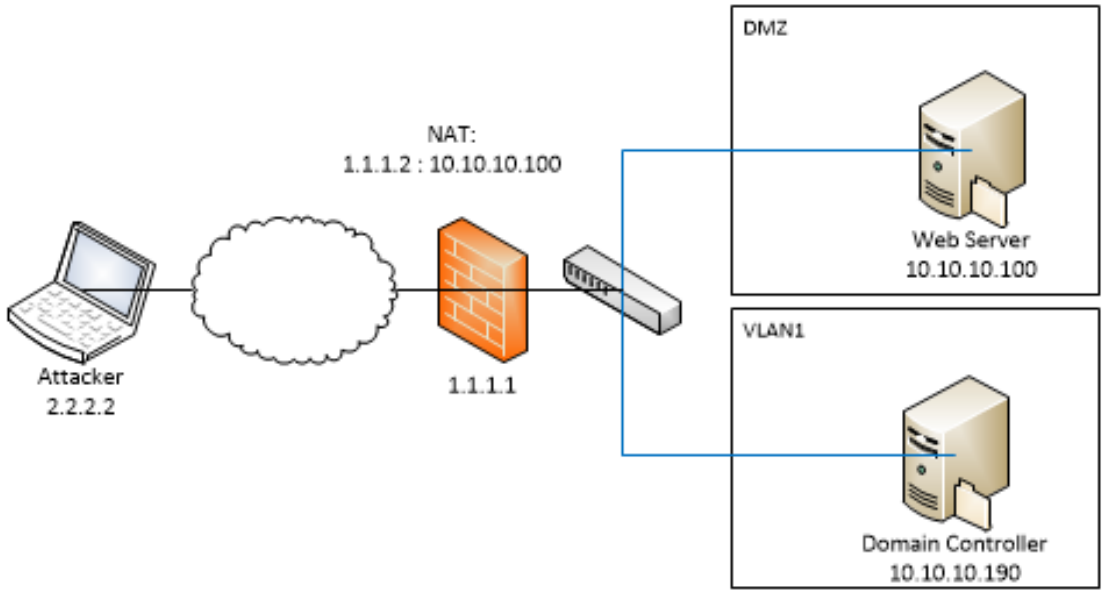
Creating Custom Packets

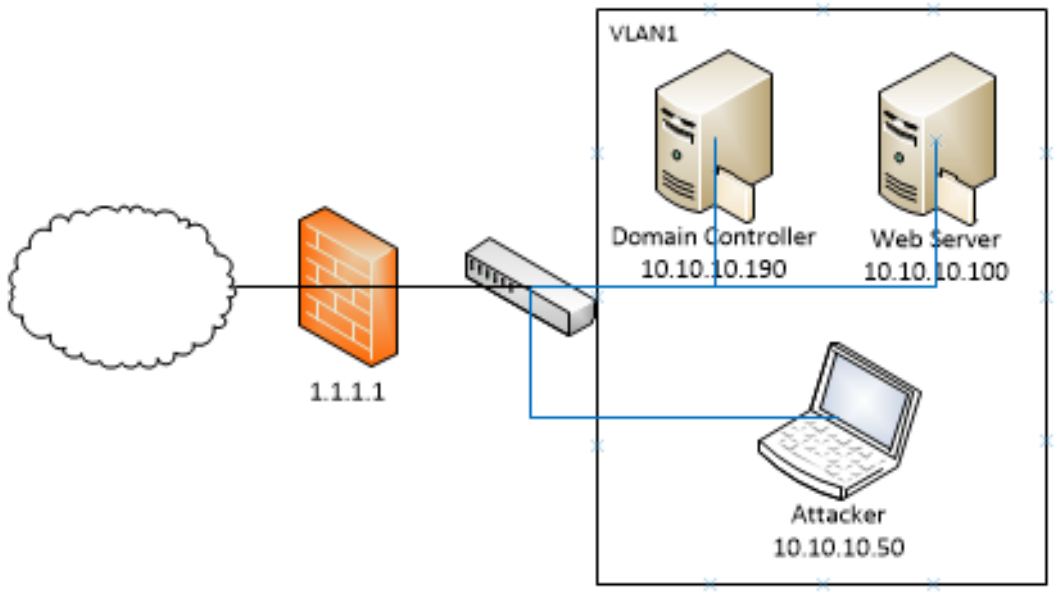
RFC 793 created in 1981 defines TCP protocol and expected behavior

Hackers can manipulate TCP packets to get unexpected results

Tools:

- Colasoft Packet Builder
- NMAP
- HPING3
- Metasploit
- Others
- Scapy





Where are you?

Scanning Bandwidth & Noise

Use iptables to monitor OUTPUT

Default port scan generates ~72KB of traffic

TCP Connect with all 65535 ports generate ~4.5 MB of traffic

Systematic approach helps limit noise and makes scanning faster

Use TCPDump while running NMAP

Measuring Scans

iptables -I INPUT 1 -s 10.10.10.19 -j ACCEPT
iptables -I OUTPUT 1 -d 10.10.10.19 -j ACCEPT
iptables -Z
nmap -sT 10.10.10.19
iptables -vn –L

Chain OUTPUT (policy ACCEPT 4 packets, 1052 bytes)
pkts bytes target prot opt in out source destination
1201 **71796** ACCEPT all -- * * 0.0.0.0/0 10.10.10.19

tcpdump -n -s0 host 10.10.10.1

14:17:29.673133 IP 192.168.1.118 > 10.10.10.1: **ICMP echo request**, id 56936, seq 0, length 8

14:17:29.673939 IP 192.168.1.118.58667 > **10.10.10.1.443: Flags [S],** seq 3993132205, win 1024, options [mss 1460], length 0

14:17:29.680917 IP 10.10.10.1.443 > **192.168.1.118.58667: Flags [R.],** seq 0, ack 3993132206, win 0, length 0

Step 1: Check for Live Systems

Sends ICMP Echo Request

- If alive = ICMP Echo Reply
- If dead = nothing

IP ranges, lists or CIDR (e.g. /24) can be used

Pinging each host one at a time (takes too long)

Ping sweep (much faster)

- Bash/CMD/PowerShell for loop
- Angry IP Scanner or Advanced IP Scanner
- NMAP (-sn switch)
- Hpring3 (-1 switch)
- Unicorn scan (machine gun SYN)

Ping Sweep One Liners

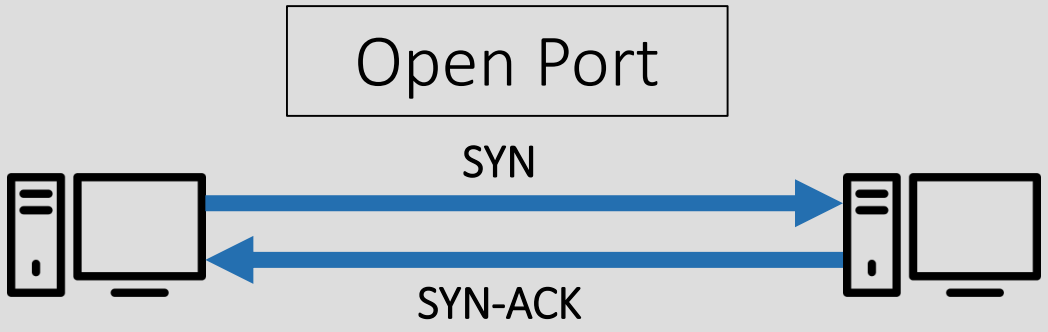
Shell	Code
Bash	for i in {1..254}; do ping -c 1 10.10.10.$i; done
CMD	(for /L %i IN (1,1,254) DO ping /n 1 /w 3 10.10.10.%i) | find "Reply"
PowerShell	1..254 | % {"10.10.10.$($_): $(Test-Connection -count 1 -comp 10.10.10.$($_) -quiet)"}

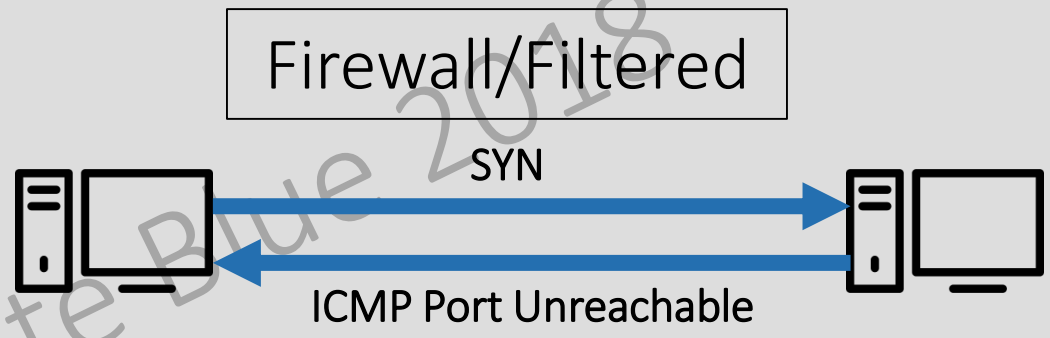
Step 2: Find Open Ports on Live Hosts

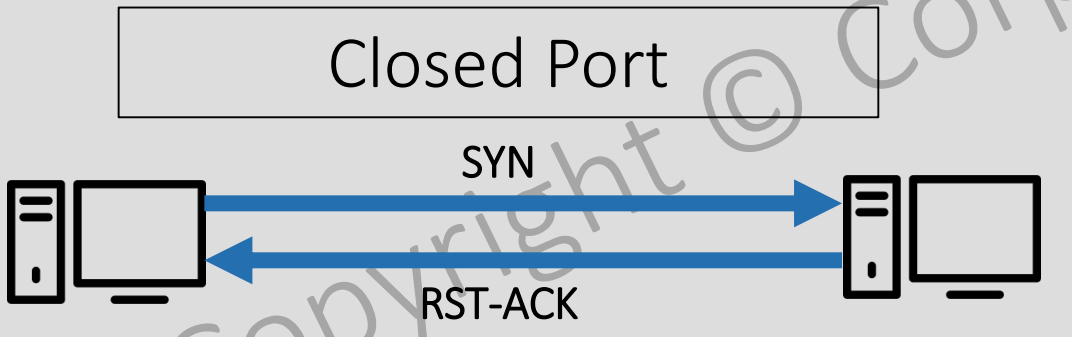
Tools:

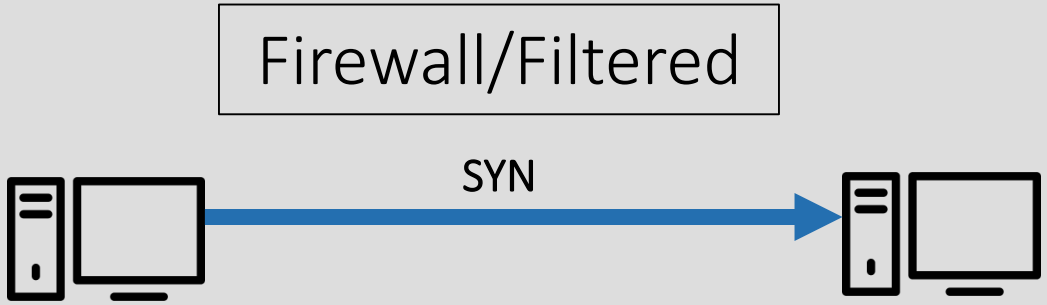
- NMAP (CLI)
- Zenmap (GUI)
- Hping3 (CLI)
- MassScan
- Others

TCP Port Scanning Scenarios

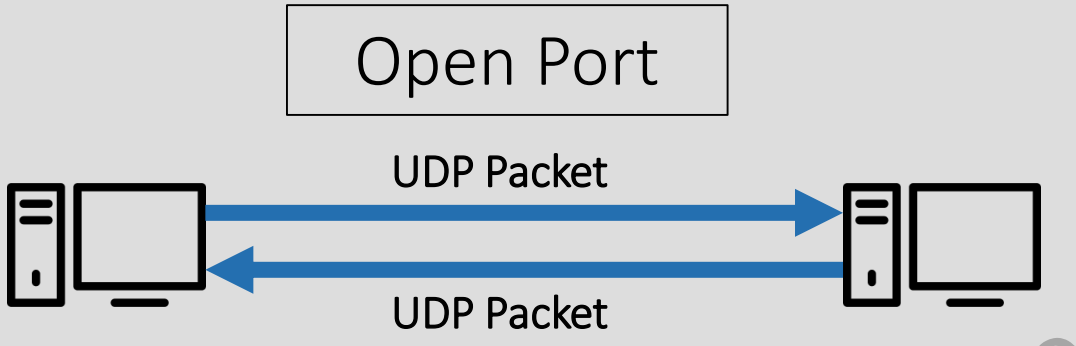


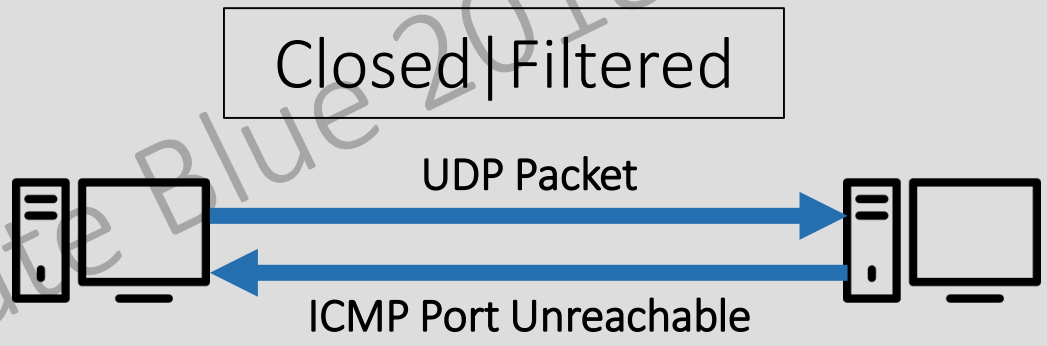


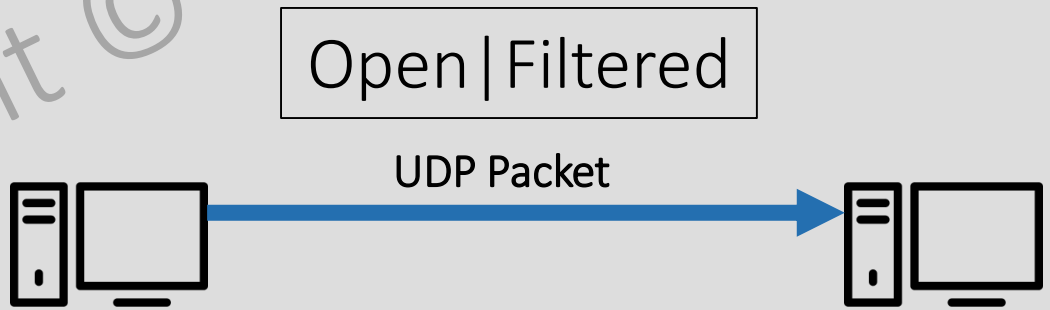




UDP Port Scanning Scenarios







Step 3: Enumeration

Services & version (-sV)

OS & version (-O)

Users & groups (--script)

- smtp-enum-users.nse
- http-wordpress-users.nse
- smb-enum-users

Banners (--script)

- banner.nse

Vulnerabilities (--script)

- smb-vuln*.nse

Step 4: Attempt Exploit

Analyze recon, scan, and enumeration data

Low hanging fruit

Look for vulnerabilities

- Vulnerability scanners (e.g. Nessus or OpenVAS)
- Searchsploit
- Exploit-db.com
- Metasploit
- NSE Scripts

Attempt to exploit weakest link

- POC from Exploit-db.com
- Metasploit module

"The good guys need to do everything right to stay secure. The bad guys need to find one vulnerability to break in."

-Unknown

Scanning Tools

Tool: NMAP

CLI tool built in 1997

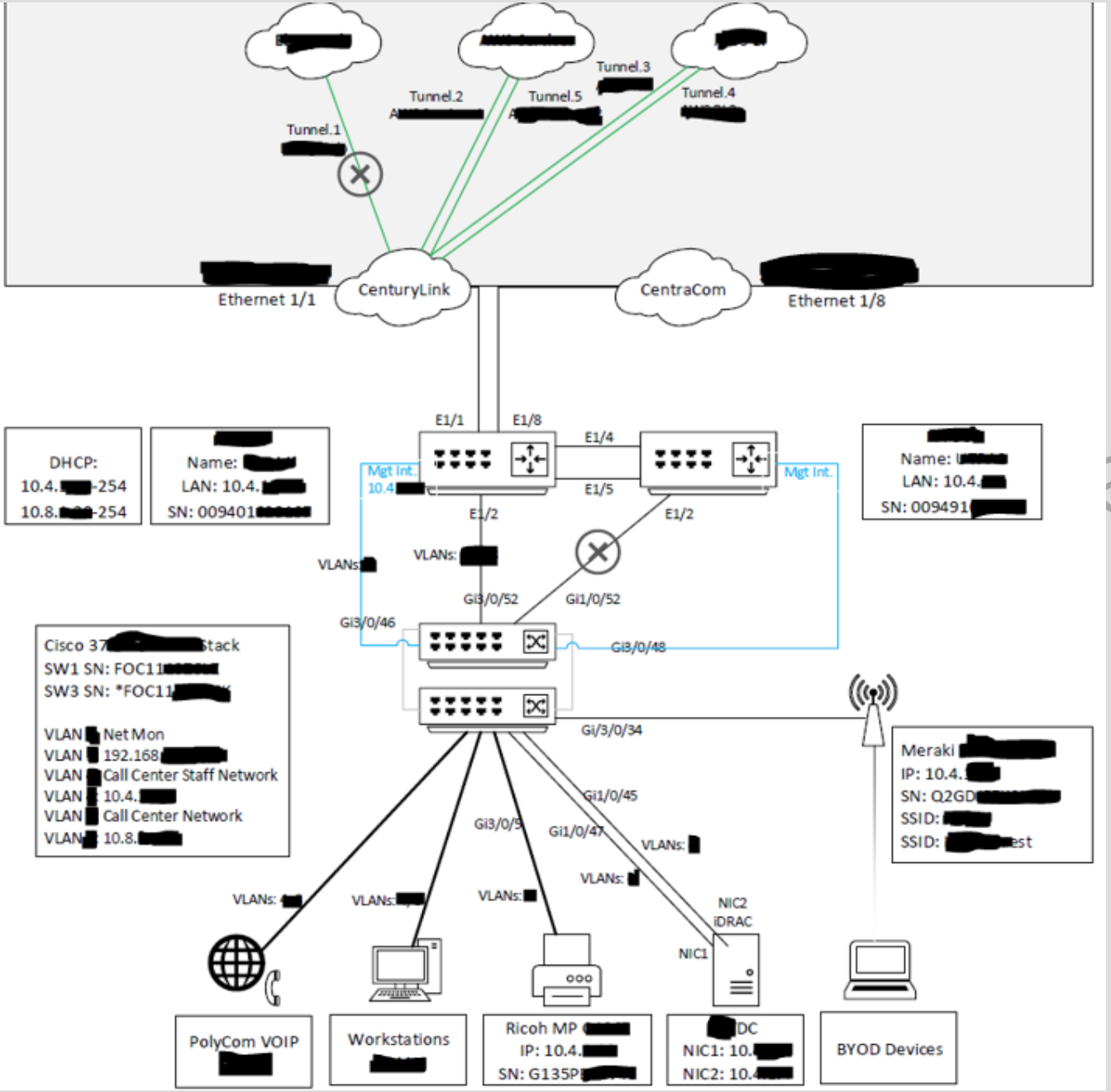
Zenmap (GUI) can be used on Windows

By default: nmap [host | ip]

- Pings a host, if offline, skips port scan
- Most common 1,000 ports
- DNS lookup
- (-sS) SYN scan for privileged users
- (-sT) TCP connect for non-privileged users

Defined as a network mapper

NSE = NMAP Scripting Engine



Without ever visiting the office, I was able to map out the network using NMAP

Why NMAP?

>20 years old

Scripting engine (NSE)

Many uses

Flexible

Powerful

Portable

Easy

Free (GNU license)

Where to get NMAP?

Kali Linux: pre-installed

NMAP.org: https://nmap.org/download.html

CentOS: yum install nmap

Debian: apt-get install nmap

NMAP Help

> nmap --h

> man nmap

www.nmap.org

Scanme.nmap.org & Scanme.insecure.org

NMAP Cookbook

SANS NMAP Cheat Sheet

NMAP

C:\windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\MikeWylie>nmap -h
Nmap 7.40 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
```

Tell me more NMAP

Spacebar while scanning for status (

p while scanning to turn on packet tracing

v while scanning to increase verbosity

d while scanning to decrease verbosity

nmap -v

nmap –vv

nmap --packet-trace

NMAP Tips

-n = No reverse DNS resolution

-T[2] = Decrease the timing of the scan

-e [interface] = Pick the interface to send the scan out from

--top-ports=[100] = Pick the # of top ports to scan

-p- = All ports (excluding 0)

Using NMAP

> nmap [option] [IP or domain]

Domain: nmap example.com

Subnet: nmap 192.168.1.0/24

Range: nmap 192.168.100-200

Input List: nmap -iL Example.txt

Port 80: nmap example.com –p 80

Ping Sweep

NMAP Ping Sweep

nmap -sn 192.168.1.0/24

NOTE: some system may have ICMP disabled

Alternate Host Discovery Sweeps

Skip ICMP Echo Request

nmap 192.168.1.1 -PN

Alternative ping scans can be used:

ARP Ping: -PR

SYN Ping: -PS

NMAP Dealing Output

STDOUT to File: nmap example.com > Example.txt

Grepable: nmap example.com -oG Example

XML: nmap 192.168.1.1 -oX Example

NMAP: nmap example.com -oN Example

All formats: nmap 192.168.1.1 -oA Example

For loop: `for i in {100..200}; do nmap 10.10.10.$i -oA nmap-scan-10-10-10-$i;done`

For loop: `for i in $(cat input_list.txt); do nmap $i -oA nmap-scan-$i;done`

Ping Sweep Clean Up

Ping sweep and place output into a txt file:

```
# nmap -sn 10.10.10.0/24 > sweep-10-10-10-0-net.txt
```

Search the txt file for hosts that respond:

```
# cat sweep-10-10-10-0-net.txt | grep "Nmap scan report
for "
```

Cut out the junk and only show IP addresses:

```
# cat sweep-10-10-10-0-net.txt | grep "Nmap scan report
for " | cut -d " " -f 5 > hosts-live-10.10.10.0-net.txt
```

Port Scanning

NMAP Input File

Used when targets are not sequential

nmap -iL [filename]

NMAP Ports

Results:

- Open
- Closed
- Filtered

Define a port: -p [80]

Define a multiple ports: -p [80,443]

All ports except 0: -p-

Top ports: --top-ports=[75]

```
root@Kali-2017-3:~# nmap -p80 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:45 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0048s latency).

PORT    STATE SERVICE
80/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

```
root@Kali-2017-3:~# nmap -p81 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:47 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0037s latency).

PORT    STATE  SERVICE
81/tcp  closed hosts2-ns
```

root@Kali-2017-3: ~

File Edit View Search Terminal Help

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-23 17:54 PDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03
c:91ff:fe18:bb2f

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
```

default-nmap-scan.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.146	192.168.43.1	DNS	75	Standard query 0x13d3 A scanme.nmap.org
2	0.000236662	192.168.43.146	192.168.43.1	DNS	75	Standard query 0x11a4 AAAA scanme.nmap.org
3	0.005893019	192.168.43.1	192.168.43.1…	DNS	91	Standard query response 0x13d3 A scanme.nmap.org
4	0.005918591	192.168.43.1	192.168.43.1…	DNS	103	Standard query response 0x11a4 AAAA scanme.nmap.o
5	0.043647087	192.168.43.146	45.33.32.156	ICMP	42	Echo (ping) request id=0xed52, seq=0/0, ttl=59 (
6	0.043915956	192.168.43.146	45.33.32.156	TCP	58	50293 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.044043942	192.168.43.146	45.33.32.156	TCP	54	50293 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.044146569	192.168.43.146	45.33.32.156	ICMP	54	Timestamp request id=0x50d4, seq=0/0, ttl=46
9	0.099532569	45.33.32.156	192.168.43.1…	ICMP	60	Echo (ping) reply id=0xed52, seq=0/0, ttl=51 (
10	0.101339171	45.33.32.156	192.168.43.1…	TCP	60	443 → 50293 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.108729208	45.33.32.156	192.168.43.1…	ICMP	60	Timestamp reply id=0x50d4, seq=0/0, ttl=51
12	0.130820073	192.168.43.146	192.168.43.1	DNS	85	Standard query 0x4bfc PTR 156.32.33.45.in-addr.ar
13	0.134562104	192.168.43.1	192.168.43.1…	DNS	114	Standard query response 0x4bfc PTR 156.32.33.45.i
14	0.179920078	192.168.43.146	45.33.32.156	TCP	58	50549 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.180293693	192.168.43.146	45.33.32.156	TCP	58	50549 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.180498913	192.168.43.146	45.33.32.156	TCP	58	50549 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.180673521	192.168.43.146	45.33.32.156	TCP	58	50549 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.180858868	192.168.43.146	45.33.32.156	TCP	58	50549 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.181321971	192.168.43.146	45.33.32.156	TCP	58	50549 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.181625646	192.168.43.146	45.33.32.156	TCP	58	50549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.181863322	192.168.43.146	45.33.32.156	TCP	58	50549 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.182074643	192.168.43.146	45.33.32.156	TCP	58	50549 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.182294571	192.168.43.146	45.33.32.156	TCP	58	50549 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	0.420863494	45.33.32.156	192.168.43.1…	TCP	60	445 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.420965563	45.33.32.156	192.168.43.1…	TCP	60	21 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.420983709	45.33.32.156	192.168.43.1…	TCP	60	3389 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.420985673	45.33.32.156	192.168.43.1…	TCP	60	139 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.421048718	45.33.32.156	192.168.43.1…	TCP	60	80 → 50549 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
29	0.421070159	192.168.43.146	45.33.32.156	TCP	54	50549 → 80 [RST] Seq=1 Win=0 Len=0
30	0.425131611	45.33.32.156	192.168.43.1…	TCP	60	23 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	0.427920761	45.33.32.156	192.168.43.1…	TCP	60	25 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	0.437105416	45.33.32.156	192.168.43.1…	TCP	60	443 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.447060378	45.33.32.156	192.168.43.1…	TCP	60	110 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	0.623900492	45.33.32.156	192.168.43.1…	TCP	60	22 → 50549 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

root@Kali-2017-3: ~

File Edit View Search Terminal Help

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-23 17:54 PDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03
c:91ff:fe18:bb2f

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
root@Kali-2017-3:~#
```

default-nmap-scan.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.146	192.168.43.1	DNS	75	Standard query 0x13d3 A scanme.nmap.org
2	0.000236662	192.168.43.146	192.168.43.1	DNS	75	Standard query 0x11a4 AAAA scanme.nmap.org
3	0.005893019	192.168.43.1	192.168.43.1…	DNS	91	Standard query response 0x13d3 A scanme.nmap.org
4	0.005918591	192.168.43.1	192.168.43.1…	DNS	103	Standard query response 0x11a4 AAAA scanme.nmap.o
5	0.043647087	192.168.43.146	45.33.32.156	ICMP	42	Echo (ping) request id=0xed52, seq=0/0, ttl=59 (
6	0.043915956	192.168.43.146	45.33.32.156	TCP	58	50293 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.044043942	192.168.43.146	45.33.32.156	TCP	54	50293 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.044146569	192.168.43.146	45.33.32.156	ICMP	54	Timestamp request id=0x50d4, seq=0/0, ttl=46
9	0.099532569	45.33.32.156	192.168.43.1…	ICMP	60	Echo (ping) reply id=0xed52, seq=0/0, ttl=51 (
10	0.101339171	45.33.32.156	192.168.43.1…	TCP	60	443 → 50293 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.108729208	45.33.32.156	192.168.43.1…	ICMP	60	Timestamp reply id=0x50d4, seq=0/0, ttl=51
12	0.130820073	192.168.43.146	192.168.43.1	DNS	85	Standard query 0x4bfc PTR 156.32.33.45.in-addr.ar
13	0.134562104	192.168.43.1	192.168.43.1…	DNS	114	Standard query response 0x4bfc PTR 156.32.33.45.i
14	0.179920078	192.168.43.146	45.33.32.156	TCP	58	50549 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.180293693	192.168.43.146	45.33.32.156	TCP	58	50549 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.180498913	192.168.43.146	45.33.32.156	TCP	58	50549 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.180673521	192.168.43.146	45.33.32.156	TCP	58	50549 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.180858868	192.168.43.146	45.33.32.156	TCP	58	50549 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.181321971	192.168.43.146	45.33.32.156	TCP	58	50549 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.181625646	192.168.43.146	45.33.32.156	TCP	58	50549 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.181863322	192.168.43.146	45.33.32.156	TCP	58	50549 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.182074643	192.168.43.146	45.33.32.156	TCP	58	50549 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.182294571	192.168.43.146	45.33.32.156	TCP	58	50549 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	0.420863494	45.33.32.156	192.168.43.1…	TCP	60	445 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.420965563	45.33.32.156	192.168.43.1…	TCP	60	21 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.420983709	45.33.32.156	192.168.43.1…	TCP	60	3389 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.420985673	45.33.32.156	192.168.43.1…	TCP	60	139 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.421048718	45.33.32.156	192.168.43.1…	TCP	60	80 → 50549 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
29	0.421070159	192.168.43.146	45.33.32.156	TCP	54	50549 → 80 [RST] Seq=1 Win=0 Len=0
30	0.425131611	45.33.32.156	192.168.43.1…	TCP	60	23 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	0.427920761	45.33.32.156	192.168.43.1…	TCP	60	25 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	0.437105416	45.33.32.156	192.168.43.1…	TCP	60	443 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.447060378	45.33.32.156	192.168.43.1…	TCP	60	110 → 50549 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	0.623900492	45.33.32.156	192.168.43.1…	TCP	60	22 → 50549 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

```
root@Kali-2017-3:~# nmap -p81 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:47 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0037s latency).

PORT   STATE  SERVICE
81/tcp closed hosts2-ns
```

```
root@T-Dev-01:/var/www/html# iptables -A INPUT -p tcp --destination-port 81 -j DROP
```

```
root@Kali-2017-3:~# nmap -p81 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:53 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0030s latency).

PORT   STATE    SERVICE
81/tcp filtered hosts2-ns
```

Why Filtered?

NMAP --reason provides reason for port status

Recommend using TCPDump while scanning for more details

NMAP Common Scans

-sT = Full TCP Connect Scan / TCP Connect Scan

-sS = SYN Scan / Stealth Scan / Half Open Scan

-sU = UDP Scan

-sA = ACK Scan

-sF = FIN Scan

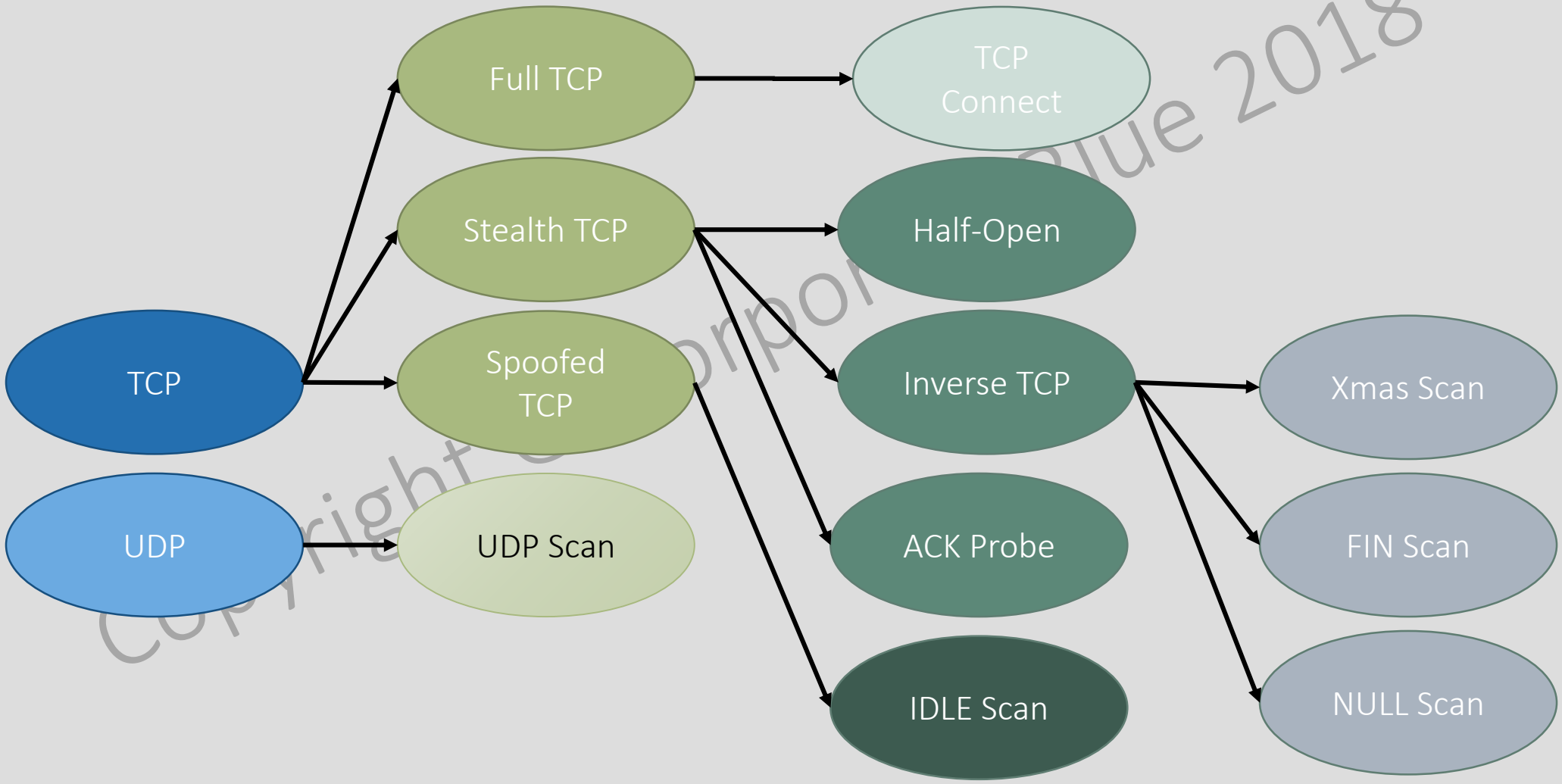
-sN = NULL Scan

-sX = XMAS Scan / XMAS Tree Scan

-sI = Idle Scan / Zombie Scan

Customer Flags = --scanflags [SYNPSH]

Scanning Techniques



Enumeration

NMAP Enumeration

Service version detection: -sV

OS detection: -O

Aggressive scan: -A

- Scripts (-sC)
- Traceroute (--traceroute)
- Service enumeration (-sV)
- OS detection (-O)

```
root@Kali-2017-3:~# nmap -p80 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:45 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0048s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

```
root@Kali-2017-3:~# nmap -sV -p80 10.10.10.107

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 18:46 PDT
Nmap scan report for 10.10.10.107
Host is up (0.0030s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

Banner Grabbing

Banner Grabbing

When a port is found open, next step is to find the service running

Port 80 is open. Is IIS, Apache or Ngenx running? Linux or Windows?

The results of banner grabbing allow us to find vulnerabilities

Types of banner grabbing

- Active
  - *Special packets that elicit a response*
- Passive
  - *Error messages*
  - *Sniffing*
  - *Page extensions (e.g. .aspx)*

Banner Grabbing Tools

ID Serve

Netcraft

Telnet

telnet [example.com] 80

Netcat

Netcat --vv [example.com] 80

NMAP

Nmap –sV –p 80 [example.com]

Nmap --script=banner –p 80 [example.com]

C:\windows\system32\cmd.exe

```
 HTTP/1.1 400 Bad Request
Date: Thu, 29 Jun 2017 00:42:29 GMT
Content-Type: text/html
Content-Length: 177
Connection: close
Server: -nginx
CF-RAY: -

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>cloudflare-nginx</center>
</body>
</html>


C:\Users\MikeWylie>lost.
```

```
root@kali:~# netcat -vv certifiedhacker.com 80
DNS fwd/rev mismatch: certifiedhacker.com != box393.bluehost.com
certifiedhacker.com [69.89.31.193] 80 (http) open
 sent 0, rcvd 0
```

```
root@kali:~# nmap -p80 --script=banner certifiedhacker.com

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-06-28 20:47 EDT
Nmap scan report for certifiedhacker.com (69.89.31.193)
Host is up (0.0015s latency).
rDNS record for 69.89.31.193: box393.bluehost.com
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.46 seconds
```

NSE

NMAP Scripts

Comes with built in scripts (NSE)

Written in Lua programming language

Activated with -sC or --script (specific script)

- Usage: --script=[Script Name or Category]
- Location (Linux): /usr/share/nmap/scripts/
- Location (Windows): C:\Program Files (x86)\Nmap\scripts\

Tip: use * as a wildcard (e.g. --script=smb-vuln*)

Searching for scripts: > ls /usr/share/nmap/scripts/*http*

Downloading scripts: wget https://github.com/example/sample.nse

NMAP Scripts (Cont.)

Categories Examples:

- Auth
- Default (-sC OR -A)
- Discovery
- Vuln
- Brute
- Malware
- All (includes DoS scripts)

Usage: --script=[default]

Update database: > nmap –script-updated

NMAP Scripts (Cont.)

Locating script categories:

grep [safe] /usr/share/nmap/scripts/script.db

Script Help:

--script-trace = detailed script output during runtime

--script-help = details about a script

--script-args [arguments] = supported arguments to use


```
mwylie@DESKTOP-ALEJ00Q:~$ grep safe /usr/share/nmap/scripts/script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
```

NMAP Scripts to Try

- Banner Grabbing
- HTTP Enumeration
- HTTP Methods
- SMB Vulnerabilities

Vulnerability Scanning with NMAP

namp --script=vuln*

Multiple scripts

Includes CVE vuln testing

Examples:

- http-cookie-flags
- http-csrf
- smb-vuln-ms08-067

Evasion

Splunk View of NMAP Scans

```
index="bro" sourcetype="bro_conn" | stats count by src_ip, dest_ip
```

Last 60 minutes

✓ 1,007 events (1/23/18 5:25:00.000 AM to 1/23/18 6:25:18.000 AM) No Event Sampling

Job Verbose Mode

Events (1,007) | Patterns | Statistics (21) | Visualization

20 Per Page Format Preview

< Prev 1 2 Next >

src_ip	dest_ip	count
172.16.1.7	172.16.1.18	925
192.168.1.25	172.16.1.6	24
172.16.1.18	172.16.1.7	7
172.16.1.7	209.133.217.165	7
172.16.1.6	45.127.112.2	4
172.16.1.7	172.16.1.255	4
172.16.1.7	255.255.255.255	4

IDS Flagging a SYN Scan

Dashboard / **Log Monitor**

Filter View

Filter: tcp Display: Last 5 minutes Status Refresh: 10 sec.

Local Time	ID	Category	Priority	Message	Source	Destination	IP Protocol	Notes
16:06:44 Apr 22	712	Network	Debug	TCP connection reject received; TCP connection dropped	[redacted], 80, X1	[redacted] 46823, X1	tcp	TCP Flag(s): ACK RST
16:06:17 Apr 22	1199	Security Services	Alert	Responder from country blocked: Responder IP:91.190.217.47 Country Name:Luxembourg	[redacted] 65391, X0	[redacted] 12350, X1	tcp	
16:06:12 Apr 22	713	Network	Debug	TCP connection abort received; TCP connection dropped	[redacted] 34881, X0	[redacted], 443, X1	tcp	TCP Flag(s): ACK RST
16:05:50 Apr 22	1226	Network	Inform	HTTPS Handshake: SSL Handshake failure with error 252	47.156.228.194, 54889, X1	[redacted], 443, X1	tcp	
16:05:44 Apr 22	860	Firewall Settings	Alert	Possible SYN Flood on IF X1	47.156.228.194, 20815, X1	[redacted], 880	tcp	
16:05:43 Apr 22	83	Security Services	Alert	Probable port scan detected	47.156.228.194, 8939, X1	[redacted], 1025, X1	tcp	TCP scanned port list, 53, 23, 8...
16:05:43 Apr 22	82	Security Services	Alert	Possible port scan detected	47.156.228.194, 35265, X1	[redacted]176, 3306, X1	tcp	TCP scanned port list, 53, 23, 8...
16:05:37 Apr 22	712	Network	Debug	TCP connection reject received; TCP connection dropped	[redacted] 59818, X1	[redacted], 10999, X1	tcp	TCP Flag(s): SYN
16:05:01 Apr 22	713	Network	Debug	TCP connection abort received; TCP connection dropped	47.156.228.194, 49993, X1	[redacted], 443, X1	tcp	TCP Flag(s): ACK RST
16:04:						[redacted], 90, X1	tcp	TCP Flag(s): SYN
16:04:						[redacted], 443, X1	tcp	admin at GUI from 47.1...
16:04:						[redacted]6, 443, X1	tcp	admin
16:03:						[redacted]443, X1	tcp	TCP Flag(s): ACK RST
16:03:						[redacted] 12350, X1	tcp	

C:\windows\system32\cmd.exe

```
C:\Users\mwyli_000>nmap -sV -sS -O   .   .216.176

Starting Nmap 6.46 ( http://nmap.org ) at 2017-04-22 16:04 Pa
```

NMAP User Agent

Method	Uri	User Agent	Proxied
OPTIONS	/ RTSP /1.	(blank)	
GET	/nice ports,/Trinity.txt.bak	(blank)	
OPTIONS	sip:nm SIP/2.	(blank)	VIA -> SIP/2.0/TCP nm;branch=foo
GET	/	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
OPTIONS	/	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/master.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/robots.txt	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/.git/HEAD	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/auth/auth.asp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/flumemaster.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/browseDirectory.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/status.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/tasktracker.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/dfshealth.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	
GET	/jobtracker.jsp	Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)	

SOC Evasion

Timing: -T0

Idle/Zombie Scan: -sI

Fragment packets: -f

Random IPs: -iR [5]

Exclude: --exclude

Encrypt if possible

Spoof IP

Decoy Packets: nmap -D [decoy1 IP] [decoy2 IP], etc.

Source routing (define what path the packet takes)

Proxy

Spoofing IP Addresses

Change the source IP address

Traffic will appear it’s coming from a different location

Can be used to bypass ACLs

NMAP

Nmap –S [fake IP] [target]

Hping3

Hping3 [target] –a [fake IP]

Scanning Countermeasures

Port Scanning Countermeasures

Firewalls/IDS/IPS/ACLs

Run the tools on your own network

Filter ICMP messages

Anti scanning/spoofing tools

Look for the default nmap user agent:

Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)

IP Spoofing Countermeasures

Use random sequence numbers

Ingress/Egress filtering on firewalls

Use multiple firewalls

What’s Next?

Other Uses for NMAP

Network admin

Troubleshooting

System admin

Asset inventory (CIS Top 20)

Thank You!

Email:
mike-bsides@CorporateBlue.com

Twitter:
@TheMikeWylie

LinkedIn:
linkedin.com/in/mwylie

Lab Time

CTF Board:

http://10.10.10.10

Submitting Flags:

flag{ }