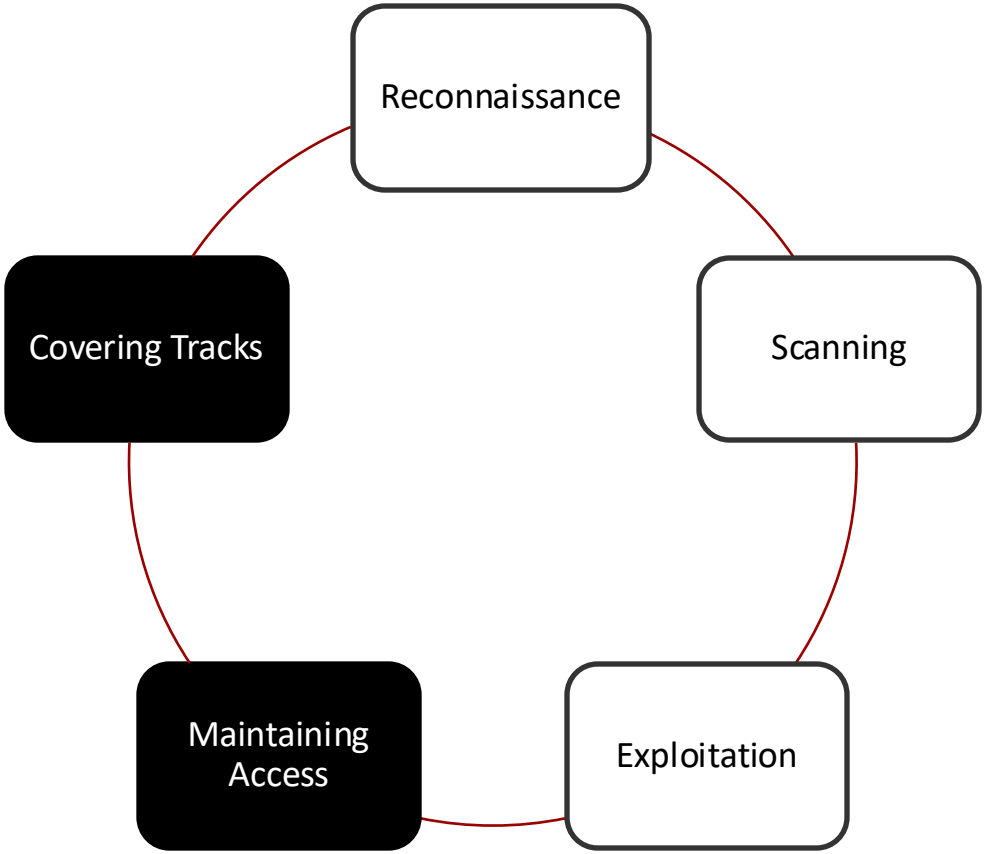
Computer Network Security

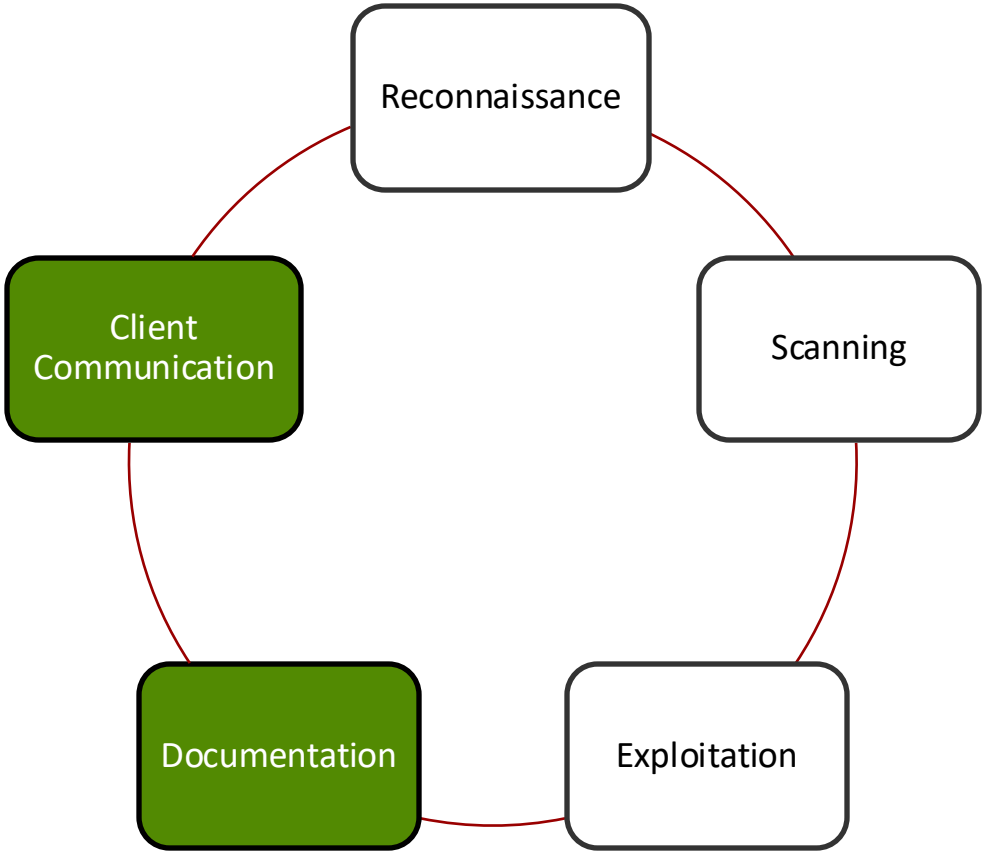
COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer

Penetration Testing: Scanning

Stages of an Attack



Stages of a Pen Test



Reconnaissance

- Investigating the target from public sources
- What did we learn?
  - Profile of company (marketplace, locations of major operations, executive/leadership team, major technology platforms)
  - Lists of “interesting systems” to investigate
  - IP subnets owned/operated by target
- Only interacted with target systems in the same way a legitimate customer/user would
  - e.g., Viewing their website

Next Step: Scanning

- Active network probing *in detail*
- Information of interest
  - Network addresses of hosts, categorized by purpose (servers, clients, routers, firewalls, …)
  - Network topology
  - Operating systems of active hosts
  - Network services and open ports of hosts
  - Vulnerabilities of hosts

Scanning

Minimize risks to hosts and network services during scanning phase

Types of Network Scans

- Sweeps/Traces
  - Send out a small number of probes to each IP address and listen for reply
  - Make note of active systems
  - Attempt to deduce network topology

Types of Network Scans

- Port scans
  - Send out a larger number of probes to each *active* IP address and listen for reply
  - Make note of TCP and UDP ports that are listening

Types of Network Scans

- OS Fingerprinting and Version Scanning
  - Send a *larger* number of probes to active hosts with listening ports
  - Deduce the operating system of the host by closely examining the replies
  - Deduce the installed software and version of active network services on the host

Types of Network Scans

- Vulnerability Scanning
  - Armed with lists of active hosts, their OS, and network services, check for known vulnerabilities or common misconfigurations

Scan Challenges

- The more **detailed** the network scan, the **slower** it will be
  - Detecting a host is up: At little as one ICMP ping; fire and forget!
  - Detecting a port is open: One packet per port (65,535 if you scan them all) x 2 (TCP+UDP)
  - Detecting versions (of OS or network services): Dozens+ of packets per service, having a “legitimate” conversation with the service in the expected manner
  - Vulnerability scanning: *Even slower*
- Often send multiple probes to each host & port in case of packet loss

Scan Challenges

- Setting your network scanner to MAX DETAILS will not produce results in a timely manner
  - 100 IPs and potential hosts? *Ok*….
  - 10,000? 100,000? Days! *Need to refine your technique*
- Iterative approach (sweeps before targeted scans)
- Reduce specific ports scanned?
  - Pros: Faster
  - Cons: Might miss obscure (but vulnerable) ports

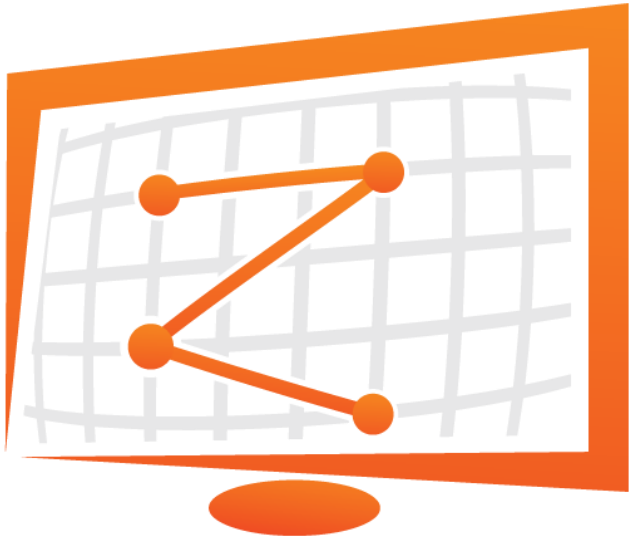
Common TCP Ports

- FTP – 21
- SSH – 22
- Telnet – 23
- SMTP – 25
- HTTP – 80
- NetBIOS over TCP – 135,137
- HTTPS – 443
- SMB over TCP - 445

Faster Scanners - ZMap

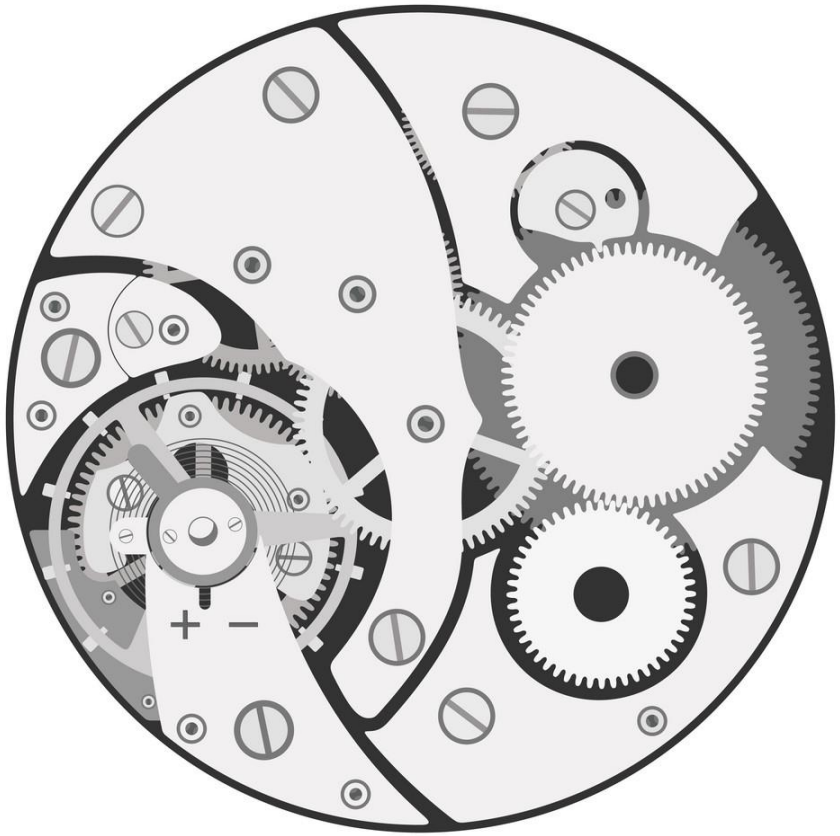
Extreme example of tradeoff between *speed* and *detail*

*ZMap is a fast **single-packet** network scanner optimized for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.*



Is this a scan or a DOS attack?

https://zmap.io/



Scanning Mechanics

Nmap

- Nmap ("Network mapper") is a tool for network discovery and security auditing
- Many scanning possibilities
  - What hosts are on the network?
  - What services (app name & version) are they offering?
  - What OS version are they running?
  - What packet filters / firewalls are in use?

https://nmap.org/

Nmap

Command Line (nmap)

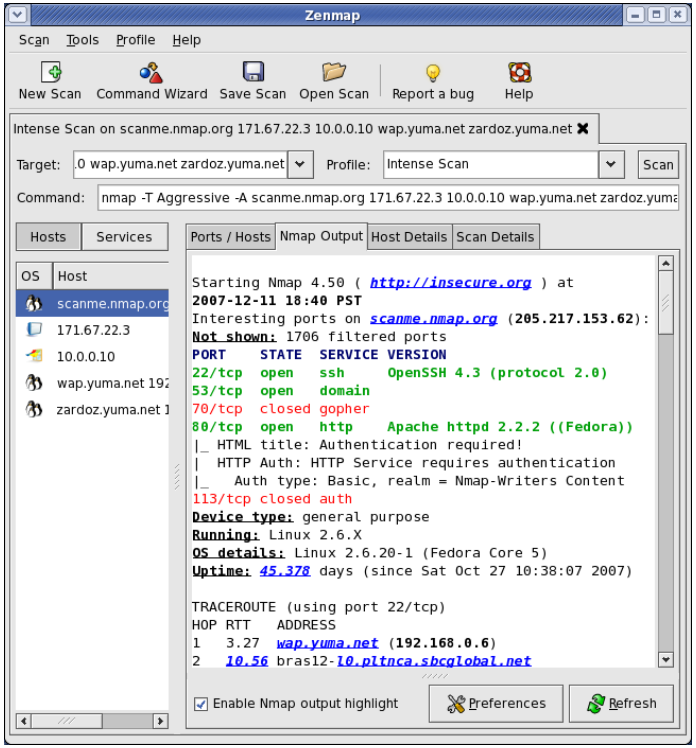
```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

GUI (zenmap)



Target Specification

- What systems do I want to scan?
  - `{target specification}`
- Hostnames: `scanme.nmap.org`
  - Challenge that one hostname might map to multiple systems (i.e. web servers behind a proxy)
  - Not preferred for serious analysis
- **IP address(es)** - either a single IP or a range
  - `192.168.0.1`
  - `192.168.0.0/24`
  - `10.0.0-255.1-254` (aka 10.0.0.0/16)

Scanning Mechanics

- Host Detection
  - How do we detect if a host is active?
  - Even if it is nominally configured to hide its presence
- Port Detection
  - How do we detect if a port is open/listening?

Host Detection

- What hosts are on the network?

```
nmap –sn [options] {target specification}
```

```
root@kali:~# nmap -sn scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-26 20:04
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00014s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:
Nmap done: 1 IP address (1 host up) bb2f  scanned in 0.16
```

Host Detection

Root User

- *Ability to generate arbitrary packets*
- Same subnet?
  - ARP request for IP
  - DNS Reverse Lookup
- Different subnet?
  - ICMP Echo Request
  - ICMP Timestamp
  - TCP SYN to port 443 (HTTPS)
  - TCP ACK to port 80 (HTTP)
  - DNS Reverse Lookup

Burst in parallel

Unprivileged User

- *Limited to normal network sockets (i.e. connect())*
- TCP SYN to port 80
- TCP SYN to port 443

Can customize – these defaults will not detect all hosts

https://nmap.org/book/man-host-discovery.html

TCP Port Detection

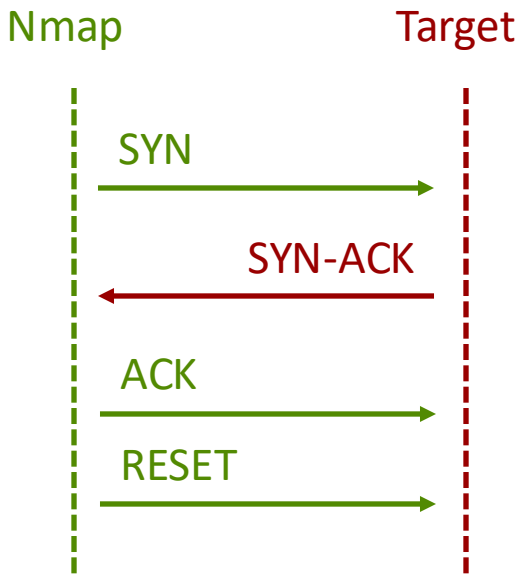
- What TCP ports are open on a host?

```
nmap -sT [options] {target specification}
nmap -sS [options] {target specification}
```

```
root@kali:~# nmap -sT scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-26 21:29 PST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.033s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

TCP Port Scan - Connect

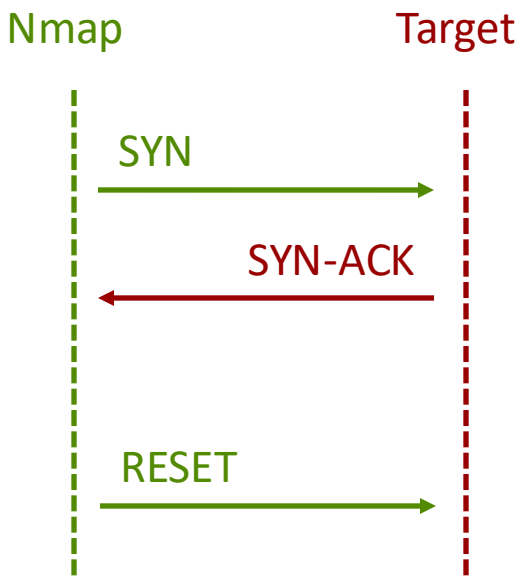
- **TCP Connect scan (`-sT`)**
- Can be run without root privileges
  - Uses OS `connect()`
- Less efficient (more packets required)
- Often logged by target machine as a connection failure



https://nmap.org/book/scan-methods-connect-scan.html

TCP Port Scan – SYN Scan

- **TCP SYN scan (-sS)**
  - Aka “half-open scanning”
- **Default** if you don’t specify scan type / **recommended**
- Requires root privileges to generate packets
- More efficient / fewer packets
- Less likely to be logged by target system (no connection is established)
  - Firewalls/IDSs still detect it



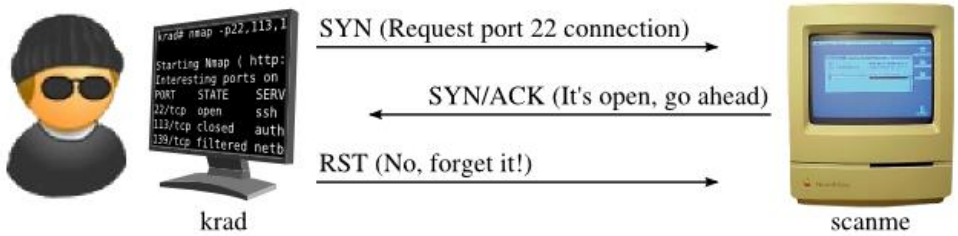
https://nmap.org/book/synscan.html

TCP Port Detection

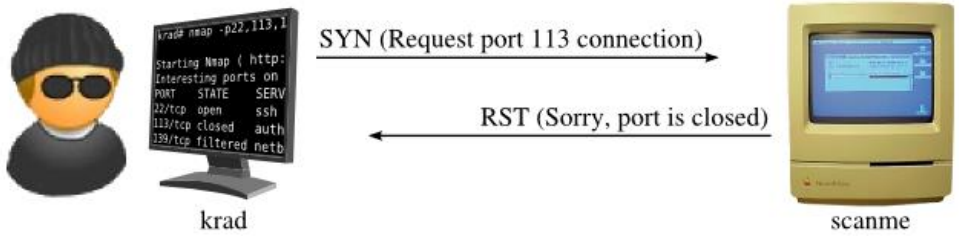
- Possible TCP port states from scanning
  - **Open** : Nmap confirmed there **is** an application listening for packets on that port
    - Nmap sent SYN, target responded SYN-ACK
  - **Closed** : Nmap confirmed there **is <u>not</u>** an application listening for packets on that port
    - Nmap sent SYN, target responded RST
  - **Filtered** : Nmap could not confirm port is open or closed
    - Nmap sent SYN, target responded *[radio silence]*
    - Likely firewall blocking scan (intentionally muddying results and slowing down scanning considerably)

TCP Port Scan – SYN Scan

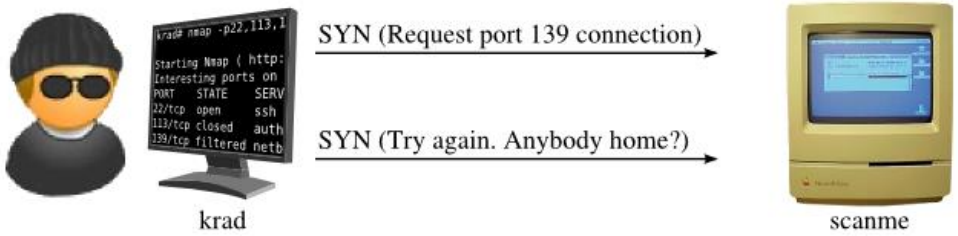
Open:



Closed:



Filtered:



https://nmap.org/book/synscan.html

TCP Port Detection

- Why were these ports filtered when I ran this scan at home? (AT&T Uverse)

```
root@kali:~# nmap -sT scanme.nmap.org
...
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

- TCP 25: SMTP
- TCP 135 : RPC
- TCP 139 : NetBIOS
- TCP 445 : SMB
- Bad history of malware abusing these services on unsuspecting (*unsophisticated*) home users!
  - AT&T blocking?

TCP Port Detection

- Result of identical scan, but from an EC2 virtual machine (AWS)

```
ubuntu@ip-172-31-52-244:~$ nmap -sT scanme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-27 07:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.021s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

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

Useful lesson about where you are scanning from?

UDP Port Detection

- What UDP ports are open on a host?

```
nmap –sU [options] {target specification}
```

```
root@kali:~# nmap -sU scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-26 21:31 PST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0043s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
```

https://nmap.org/book/scan-methods-udp-scan.html

UDP Port Detection

- Sends a UDP packet to each port in a scan and listens for any reply
- Empty payload for most ports
  - Hard to know what to send to a mystery application
  - Big challenge – most applications will just discard/ignore an empty UDP packet
- Protocol-specific payload for a few specific ports to elicit more replies (sneaky!)
  - UDP 53 (DNS)
  - UDP 161 (SNMP)
  - …

UDP Port Detection

- Possible UDP port states from scanning
  - **Open** : Nmap sent packet, target responded with any UDP packet
  - **Open|Filtered** : Nmap sent packet, no response from target (even after retransmissions)
  - **Closed** : Nmap sent packet, target responded with ICMP port unreachable (type 3, code 3)
  - **Filtered** : Nmap sent packet, target responded with ICMP unreachable (type 3, other codes)

Port Detection

- Nmap does **not** scan all ports by default!
  - Checking all 65,535 ports is *slooooooooow* and nearly all are closed
  - **Only most popular 1000 ports are checked by default**
  - Good odds for TCP, less so for UDP
  - Scanned in random order

Table 6.1. Required `--top-ports` values for reaching various effectiveness levels

Effectiveness	TCP ports required	UDP ports required
10%	1	5
20%	2	12
30%	4	27
40%	6	135
50%	10	1,075
60%	18	2,618
70%	44	5,157
80%	122	7,981
85%	236	9,623
90%	576	11,307
95%	1,558	13,035
99%	3,328	15,094
100%	65,536	65,536

https://nmap.org/book/performance-port-selection.html
https://nmap.org/book/port-scanning.html#most-popular-ports

Port Detection

- Can override with `--top-ports=n` option
- Can reduce to top 100 ports with `-F` (fast mode)
- Can specify specific ports with `-p` option
  - A single port: `-p 80`
  - A list: `-p 80,443`
  - A range: `-p 0-65535`
- UDP port scans can be *improved* with version detection (`-sV`) because the probes sent are tailored to the specific application that typically listens on that port

OS Detection

- What operating systems are on the network?

```
nmap -O [options] {target specification}
```

```
root@kali:~# nmap -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-27 20:19 PST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.027s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3
cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or
Windows 7 or Windows Server 2012
```

OS Detection

- Purposes of OS detection?
  - Check if hosts are vulnerable to known exploits
  - Inventory of systems on network
  - Detect unauthorized devices on the network (e.g. wireless access point)

OS Detection

- How is the OS detected?
  - "Nmap OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint. Every probe packet is tracked and resent at least once if there is no response."

More info: https://nmap.org/book/osdetect-methods.html

Service & Version Detection

- Final main piece of Nmap functionality
- Key challenges remaining
  - If a service is listening on TCP Port 80, are we sure it's a web server? (Nmap port scan will label it http without any verification)
  - If some service is listening on nonstandard port 12345, what is it?
  - Can we find more details about the specific service application and its version number?

Service & Version Detection

- What services are on the network?

```
nmap -sV [options] {target specification}
```

```
root@kali:~# nmap -sV scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-27 20:35 PST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.084s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
(Ubuntu Linux; protocol 2.0)
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Doing it ALL

(Host + Port + OS + Version + scripts)

```
nmap -A [options] {target specification}
```

```
ubuntu@ip-172-31-52-244:~$ nmap -A scanme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-27 08:22 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.021s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (EdDSA)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: 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 12.26 seconds
```

Big drawback for always using `-A`: 12.26 seconds vs 0.38 seconds for `-sT` for ONE HOST

Nmap Tips and Tricks

- **How close is my scan to finishing?**
  - Press any key while running to see current status (runtime, hosts scanned, hosts up, …)
- **How do I get more information / more debugging information?**
  - Press v or d while running to increase verbosity / debugging level
  - Press shift-v or shift-d while running to decrease verbosity / debugging level
  - Use the `--packet-trace` option to see all packets sent

Nmap Tips and Tricks

- **How do I control the speed at which Nmap scans?**

```
nmap -T[time option] [opt] {target}
```

- "Timing Templates"
  - `-T0`: Paranoid: 300s between probes
  - `-T1`: Sneaky: 15s between probes

  } *Sufficiently slow that IDS won't detect scan?*

  - `-T2`: Polite: 0.4s between probes
  - `-T3`: Normal *(default)*
  - `-T4`: Aggressive: More parallelism, shorter timeouts

    Consider -T4 for LAN
  - `-T5`: Insane: MOAR!!

https://nmap.org/book/performance-timing-templates.html

Nmap Tips and Tricks

- **How do I control the Nmap output format?**

```
nmap -o[output option] [opt] {target}
```

- Output Formats
  - No option – Default human-readable option
  - `-oN [filename]` – Similar output saved to file
  - `-oX [filename]` – XML output, easily imported
  - `-oG [filename]` – "Grepable" single-line-per-host
  - `-oA [dirname]` – Normal + XML + Grepable in a directory
  - `-oS [filename]` – `sCRiPt KiDDi3 OutPU+`
    - This format is provided for the `l33t haXXorZ`! ☺

https://nmap.org/book/output.html

Nmap Tips and Tricks

- **Why did Nmap mark that port as open, closed, filtered, …?**

```
nmap --reason [opt] {target}
```

```
root@kali:~# nmap -sT --reason scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-27 20:09 PST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 128 (0.043s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
Reason: 992 conn-refused
PORT      STATE    SERVICE      REASON
22/tcp    open     ssh          syn-ack
25/tcp    filtered smtp         no-response
80/tcp    open     http         syn-ack
135/tcp   filtered msrpc        no-response
139/tcp   filtered netbios-ssn  no-response
445/tcp   filtered microsoft-ds no-response
9929/tcp  open     nping-echo   syn-ack
31337/tcp open     Elite        syn-ack
```

Nmap Tips and Tricks

- **How do I reduce the scan time?**
- Omit non-critical tests
  - Skip the port scan (-sn) when you only need to know what hosts are online
  - Limit the number of ports scanned
  - Skip advanced scan types (-sC, -sV, -O, --traceroute, and -A)
  - Turn off DNS resolution when it isn't necessary
    - *Nmap does reverse DNS lookup against every host by default*
- Optimize Timing Parameters *(-T templates)*
- Separate and Optimize UDP Scans
- Scan From a Favorable Network Location
  - *Inside the LAN is almost always better!*

https://nmap.org/book/reduce-scantime.html