NMAP LESSONS LEARNED

INTRODUCTION

WHO AM I

- Jose R. Hernandez
- Vulnerability Researcher / Former Pentester

WHY DID I DO THIS TALK

LESSON #1 - NMAP IS NOISY

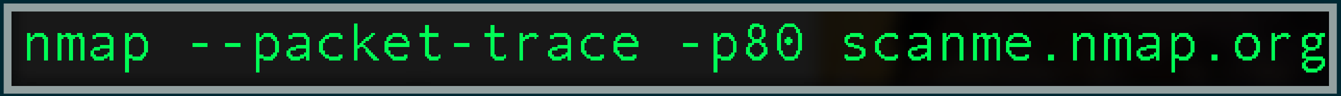
DEFAULT SCAN

- `nmap scanme.nmap.org`

DEFAULT SCAN CONTINUED

- nmap -PE -PS443 -PA80 -PP scanme.nmap.org

TRACING PACKETS

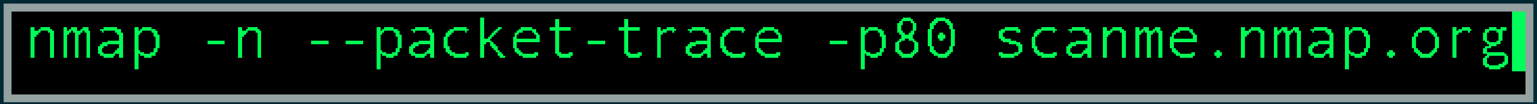
- 

```
nmap --packet-trace -p80 scanme.nmap.org
```

PHASES OF NMAP SCAN

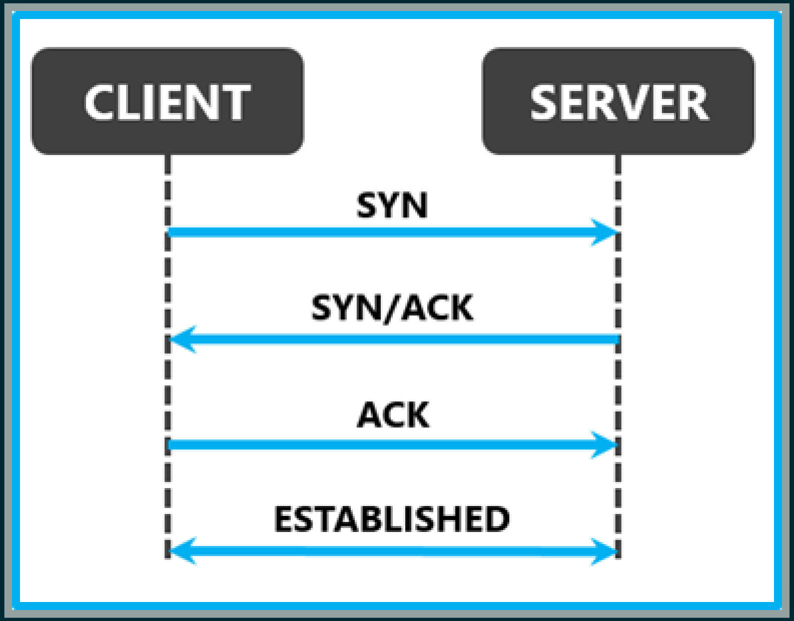
- Host Discovery
- Reverse-DNS Resolution
- Port Scanning
- Version Detection
- OS Detection
- Traceroute
- Script Scanning
- Output

REVERSE DNS RESOLUTION

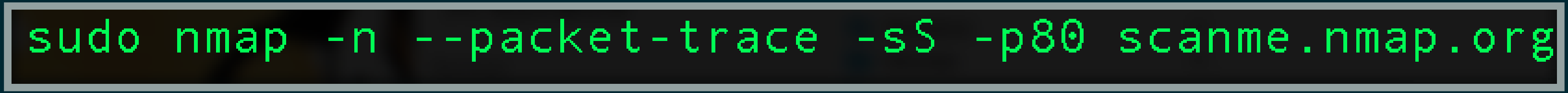
- List Scan `-sL`
- Disable rDNS `-n`
- 

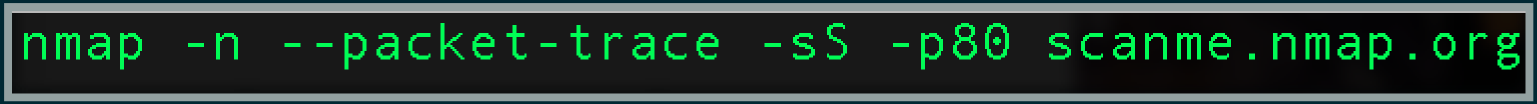
```
nmap -n --packet-trace -p80 scanme.nmap.org
```

TCP HANDSHAKE



ADMIN VS NON-ADMIN SCANS

- Stealth Scan vs TCP Connect Scan
- 

  ```
  sudo nmap -n --packet-trace -sS -p80 scanme.nmap.org
  ```
- 

  ```
  nmap -n --packet-trace -sS -p80 scanme.nmap.org
  ```

RESERVED IP SPACE - ARP SCANS

- `--disable-arp-ping`

RETRANSMISSION OF PROBES

- By Default Nmap Sacrifices Speed For Accuracy

NOT STEALTHY ADVANCED SCANNING

- Version Scans
- Script Scans
- OS Scans

LESSON #2 - HOST DISCOVERY IS ESSENTIAL

HOST DISCOVERY PROBES

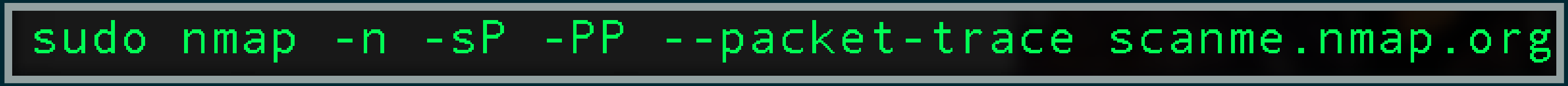
- Nmap Will Only Scan Hosts That Respond To Host Discovery Probes
- Ping Sweeps `-sP`

INTERNET CONTROL MESSAGE PROTOCOL (ICMP) PING

ICMP ECHO TYPE

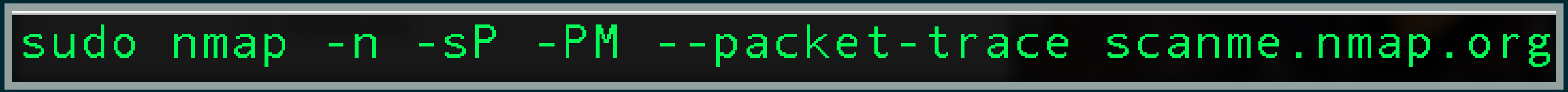
-
  ```
  sudo nmap -n -sP -PE --packet-trace scanme.nmap.org
  ```

ICMP TIMESTAMP TYPE

- 

```
sudo nmap -n -sP -PP --packet-trace scanme.nmap.org
```

ICMP ADDRESS MASK REQUEST TYPE

- 

```
sudo nmap -n -sP -PM --packet-trace scanme.nmap.org
```

PORT PING SWEEP

TCP SYN PING -PS<PORT LIST>

- nmap -sP -PS2222 192.168.1.0/24

TCP ACK PING -PA<PORT LIST>

- nmap -sP -PA2222 192.168.1.0/24

UDP PING -PU<PORT LIST>

- nmap -sP -PU2343 192.168.1.1

LESSON #3 - NOT ALL SCANS ARE CREATED EQUAL

PORT STATES

- Open - Application Actively Accepting Connections
- Closed - Port Is Accessible, No Application Accepting Connections

- Filtered - Cannot Determine If Port Is Open, Packet Filtering Blocking Probes.
- Unfiltered - Port Is Accessible, Cannot Determine If Port Is Open Or Closed.
- Open | Filtered - Cannot Determine If Port Is Open Or Filtered
- Closed | Filtered - Cannot Determine If Port Is Closed Or Filtered

TCP FLAGS

- SYN - Starting A Connection
- ACK - Acknowleges Received Data
- FIN - Last Packet From Sender, Closes A Connection
- RST - Reset The Connection
- PSH - Asks Receiving Application Not To Buffer Data But Process Packet
- URG - Packets Should Be Prioritized Over Other Packets

SCAN TYPES AND RESPONSES

TCP SYN STEALTH SCAN

Probe Response	Assigned State
TCP SYN/ACK Response	Open
TCP RST Response	Closed
No Response	Filtered
ICMP unreachable Error	Filtered

TCP CONNECT SCAN

Probe Response	Assigned State
TCP SYN/ACK Response	Open
TCP RST Response	Closed
No Response	Filtered
ICMP unreachable Error	Filtered

UDP SCAN

Probe Response	Assigned State
Any UDP Response	Open
No Response Received	Open / Filtered
ICMP Error (3)	Closed
ICMP Error (1,2,9,10,13)	Filtered

TCP FIN SCAN, NULL SCAN, XMAS SCAN

Probe Response	Assigned State
No Response	Open / Filtered
TCP RST Packet	Closed
ICMP Error (1,2,3,9,10,13)	Filtered

ACK SCAN

Probe Response	Assigned State
TCP RST Response Packet	Unfiltered
No Response	Filtered
ICMP Error (1,2,3,9,10,13)	Filtered

TCP WINDOW SCAN

Probe Response	Assigned State
TCP RST Response Non-zero Window Field	open
TCP RST Response zero Window Field	closed
No Response	Filtered
ICMP Error (1,2,3,9.10,13)	Filtered

TCP MAIMON SCAN

Probe Response	Assigned State
No Response	Open / Filtered
TCP RST Packet	Closed
ICMP Error (1,2,3,9,10,13)	Filtered

TCP IDLE SCAN

IP PROTOCOL SCAN

Probe Response	Assigned State
Any Response From Target	Open
ICMP Error (2)	Closed
ICMP Error (1,3,9,10,13)	Filtered
No Response	Open /Filtered

TCP FTP BOUNCE SCAN

- Deprecated

REASON

- `--reason`

CUSTOMIZE YOUR OWN SCAN

- `--flags`
- `nmap --scanflags URGACKPSHRSTSYNFIN localhost`

LESSON #4 - UDP + SERVICE DETECTION

UDP RESPONSES

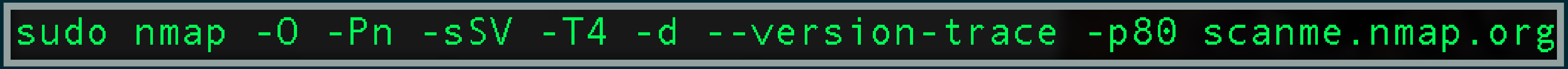
Probe Response	Assigned State
Any UDP Response	Open
No Response Received	Open / Filtered
ICMP Error (3)	Closed
ICMP Error (1,2,9,10,13)	Filtered

VERSION SCANS

- `nmap -sUV localhost`

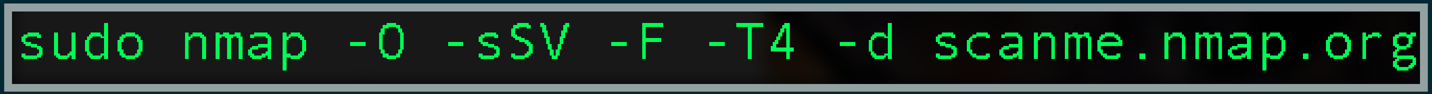
FINGERPRINTS

SERVICE

- 

```
sudo nmap -O -Pn -sSV -T4 -d --version-trace -p80 scanme.nmap.org
```

OS

- 

```
sudo nmap -O -sSV -F -T4 -d scanme.nmap.org
```

UDP SERVICE FINGERPRINTS

- Add Service Fingerprint to nmap-services-probes
- Submit To Nmap https://nmap.org/cgi-bin/submit.cgi

LESSON #5 - SPEEDRACER

AUTOMATIC VS MANUAL TRANSMISSION

NMAP AUTOMATIC

- Nmap Adapts To Network Condition
- Default Congestion Control Algorithms Are Recommended
- Host and Port Parallelization
- Retransmission of Probes

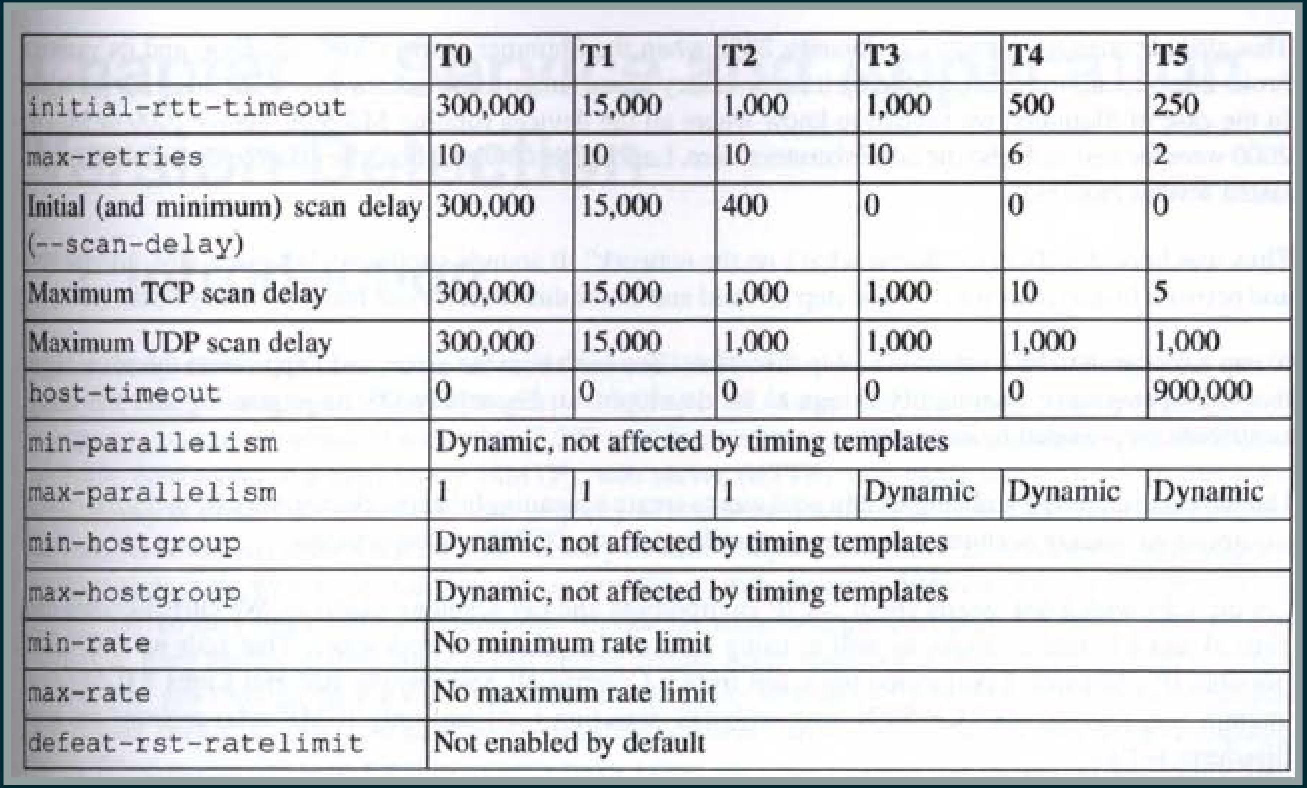
NMAP MANUAL

- Greater Control Over Scan
- Reduce Accuracy For Speed

TIMING TEMPLATES

- 0 - Paranoid
- 1 - Sneaky
- 2 - Polite
- 3 - Normal
- 4 - Aggressive
- 5 - Insane

TIMING TEMPLATES



	T0	T1	T2	T3	T4	T5
`initial-rtt-timeout`	300,000	15,000	1,000	1,000	500	250
`max-retries`	10	10	10	10	6	2
Initial (and minimum) scan delay (`--scan-delay`)	300,000	15,000	400	0	0	0
Maximum TCP scan delay	300,000	15,000	1,000	1,000	10	5
Maximum UDP scan delay	300,000	15,000	1,000	1,000	1,000	1,000
`host-timeout`	0	0	0	0	0	900,000
`min-parallelism`	Dynamic, not affected by timing templates					
`max-parallelism`	1	1	1	Dynamic	Dynamic	Dynamic
`min-hostgroup`	Dynamic, not affected by timing templates					
`max-hostgroup`	Dynamic, not affected by timing templates					
`min-rate`	No minimum rate limit					
`max-rate`	No maximum rate limit					
`defeat-rst-ratelimit`	Not enabled by default					

OPTIMIZE YOUR PORT SCANS

REVIEW SPEED VARIABLES

- `nmap -d localhost`

OPTIMIZE SCANS

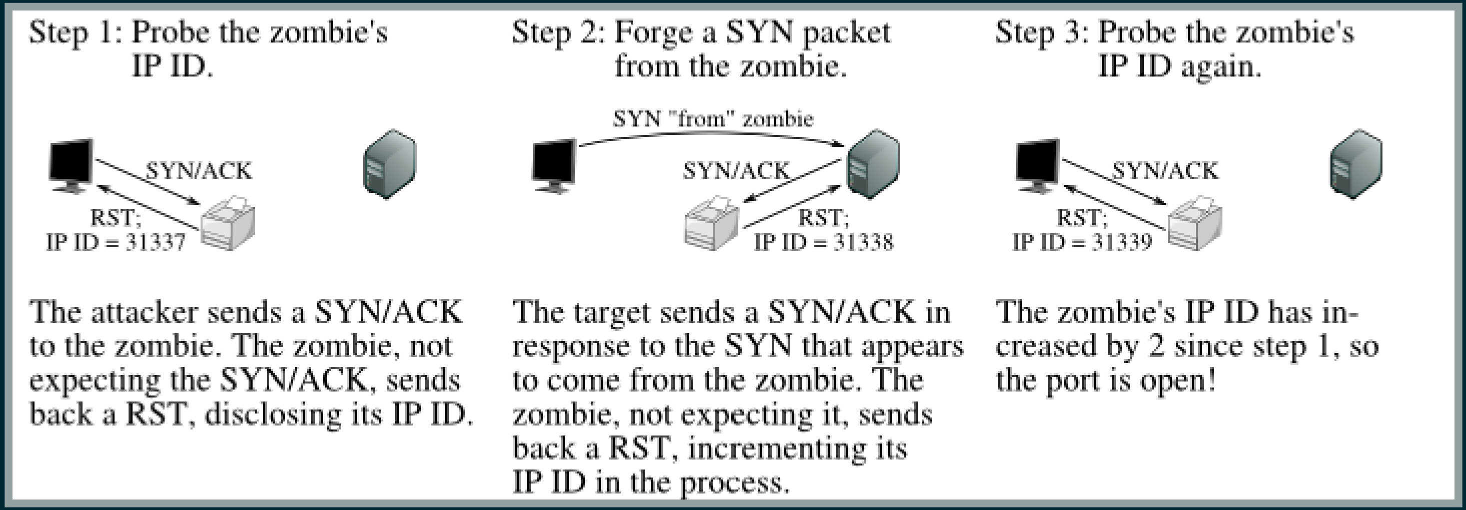
- Disable DNS
- Use Ping Scan
- Scan Top Ports Only `-F`
- Advanced Scan Types (NSE, Version, OS scan)
- Split Up TCP and UDP Scans

UDP SPEED UP UDP SCANS

- `nmap -sUV --version-intesity 0 localhost`

LESSON #6 - THE WALKING DEAD

OPEN



Step 1: Probe the zombie's IP ID.

Step 2: Forge a SYN packet from the zombie.

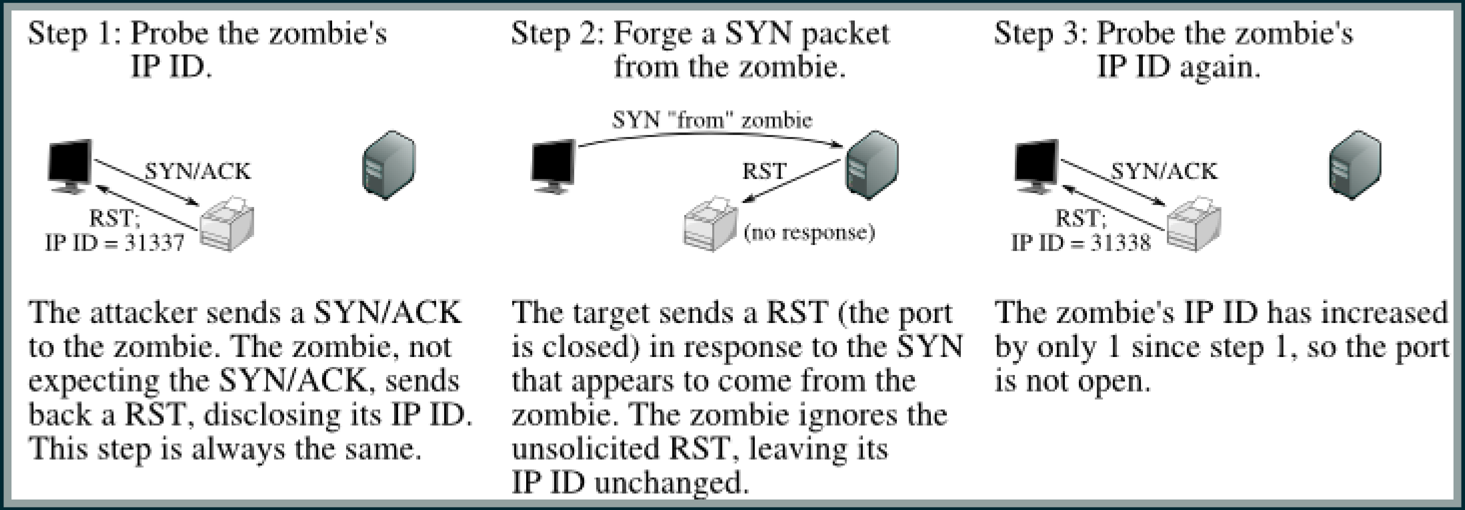
Step 3: Probe the zombie's IP ID again.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

CLOSED



Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

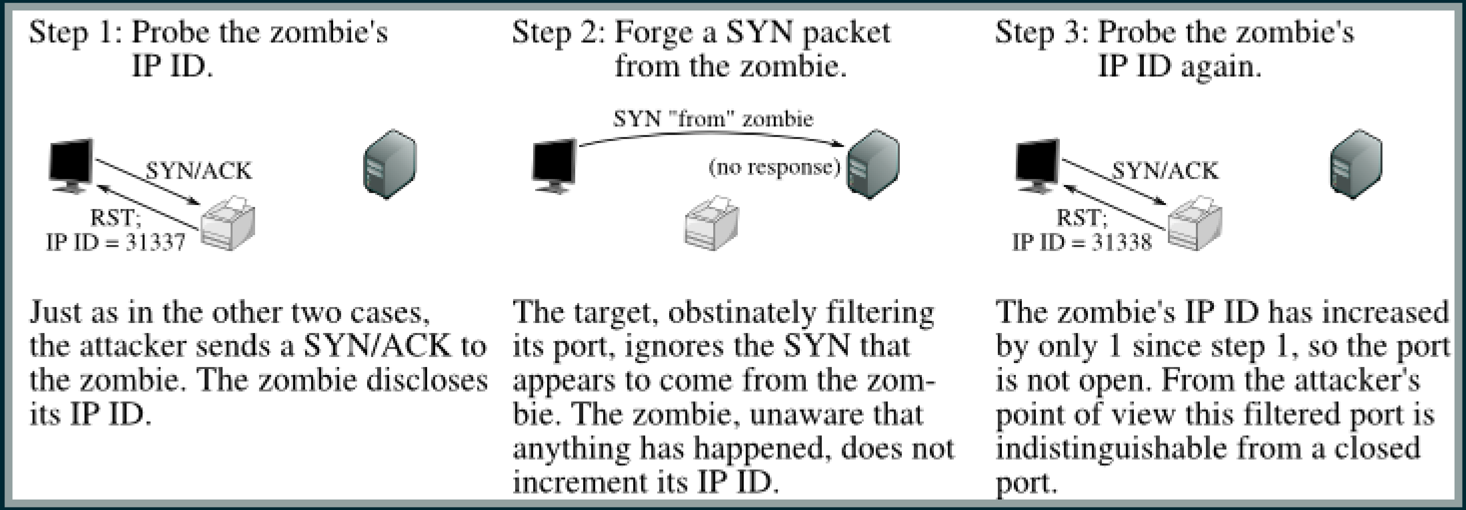
Step 2: Forge a SYN packet from the zombie.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

FILTERED



Step 1: Probe the zombie's IP ID.

Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

Step 2: Forge a SYN packet from the zombie.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

LESSON #7 - NMAP DATABASE FILES

LINUX / UNIX LOCATION

- `/usr/share/nmap/`

FILES

- nmap-os-db
- nmap-protocols
- nmap-service-probes
- nmap-mac-prefixes
- nmap-payloads
- nmap-rpc
- nmap-services

LESSON #8 - NMAP SCRIPTING ENGINE

SCRIPT CATEGORIES

- auth
- default
- discovery
- external
- intrusive
- malware
- safe
- version
- vuln

SCRIPT SCANNING

- `sudo nmap -sC localhost`
- `sudo nmap --script=default`

NMAP FUNCTIONALITY ENHANCED

- Whois Information
- Email Harvesting
- Bruteforce DNS records
- Bruteforce HTTP Authentication
- Bruteforce Database Passwords
- User account enumeration
- Detect XSS Vulnerabilities
- Detect SQL Injection Vulnerabilities

LESSON #9 - FIREWALL AND IDS MISCONFIGURATIONS

STATEFUL VS STATELESS FIREWALLS

- ACK Scan

FIREWALL MISCONFIGURATION - SOURCE PORT

- 53 / DNS
- 88 / Kerberos
- `sudo nmap -sS -v -Pn -g 88 localhost`

FIREWALL MISCONFIGURATION - IPV6

- `sudo nmap -6 scanme.nmap.org`

INTRUSION DETECTION SYSTEM - SLOW DOWN

- Threshold Detection
- Slow Down Use -T0 Paranoid

INTRUSION DETECTION SYSTEM - SCATTER PROBES

- Randomize the IPs That You Are Scanning
- `-sL` Randomize IP's with Scripting Language

INTRUSION DETECTION SYSTEM - DECOYS

- Blend In With Bad Traffic
- Decoys Must Be Online
- SYN Flooding
- DNS Queries or Service Detection `-sV or -A` Will Give You Away

LESSON $10 - NETWORK BASELINE AND NMAP DEFENSES

NDIFF

- Only Works on XML Files -oX
- Ndiff scan1.xml scan2.xml

CONTINUE LARGE SCANS

- `--resume` Option

CONFUSE NMAP

- Probes return SYN/ACK on All Ports

LESSON #11 - EXTRAS

NMAP HAPPY BIRTHDAY

- Verbose Scan on September 1

NMAP MERRY CHRISTMAS SCAN

- Verbose Scan December 25
- Offer To Do Xmas Scan

1337 OUTPUT

- `nmap -oS localhost`

LESSON #12 - USEFUL COMMANDS

COMMANDS

- `--packet-trace`
- `--version-trace`
- `-d`
- `--reason`
- `--disable-arp-ping`
- `-g`
- `-6`
- `--badsum`
- `--data-length`
- `--version-intesity 0`
- `--resume`

CONCLUSION

QUESTIONS?