



Prifysgol Cymru  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

# Network Scanning and Enumeration

## Lecture 6

*Trawsnewid Addysg; Trawsnewid Bywydau*  
*Transforming Education; Transforming Lives*



[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)

# Learning Outcomes

- **Explain** the purpose and role of network scanning and enumeration
- **Identify** and differentiate common network scanning techniques
- **Apply** appropriate tools and methods to perform scanning and enumeration tasks
- **Evaluate** security risks and implement countermeasures

# Network Scanning and Enumeration

- This session introduces how attackers and security professionals discover systems on a network.
- We focus on scanning, banner grabbing, and enumeration in a safe, ethical, lab-based context.

**Goal:** understand techniques so we can better defend real-world networks.

# Where Scanning Fits

- **Footprinting**: passive information gathering (no direct contact).
- **Scanning**: identifying live hosts, open ports, and services.
- **Enumeration**: actively connecting to extract deeper system details.

# Network Scanning Explained

- Network scanning discovers devices and services running on a network.
- Think of it like checking which doors and windows are open in a building.
- Attackers and defenders use the same techniques, but for different goals.

# Scanning Networks

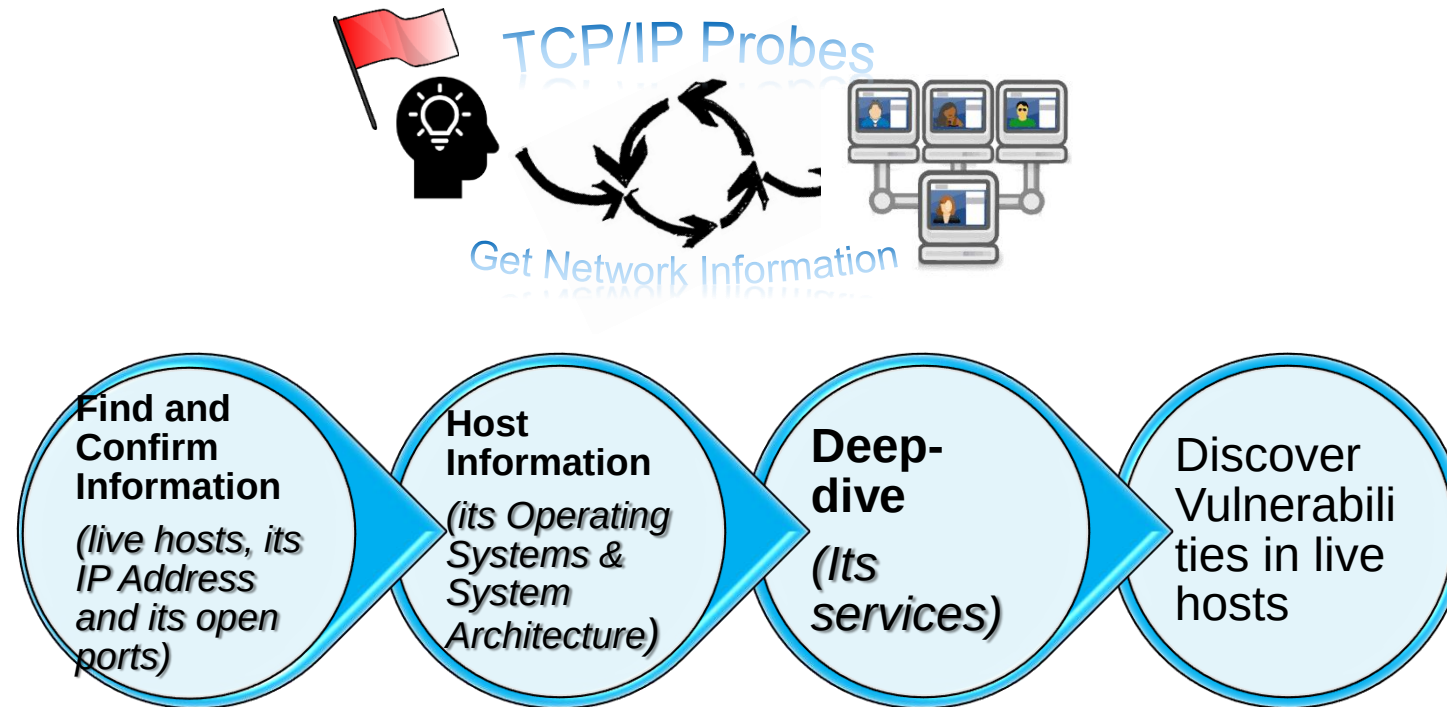
- Like, Reconnaissance is the method of collecting information about a target system without alerting it, also known as Footprinting, it is the first step in any form of hacking.
- It will help in understanding the target system and identify potential attack vectors & vulnerabilities
- Network scanning is the next process which helps in identifying hosts, ports and services in the network.
- Network scanning could be done using a set of procedures.
- It is one of the components of intelligence gathering that can be used by attackers to gather information and create a profile of their targets.



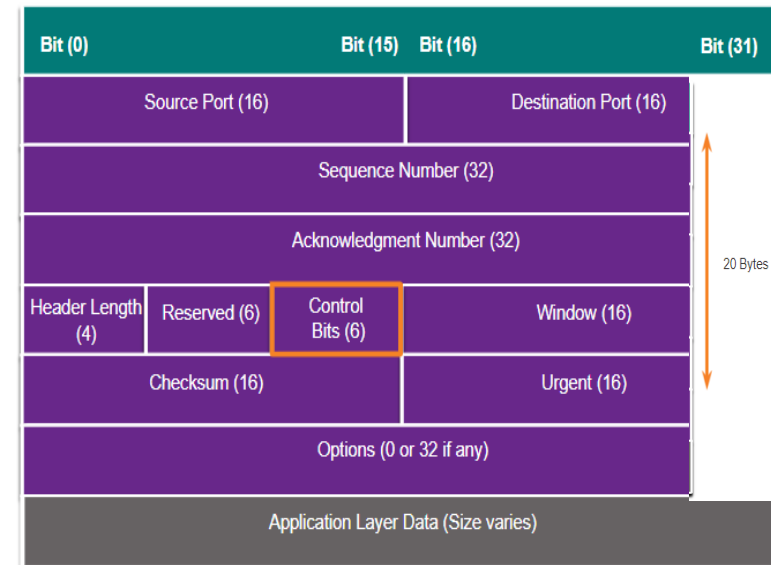
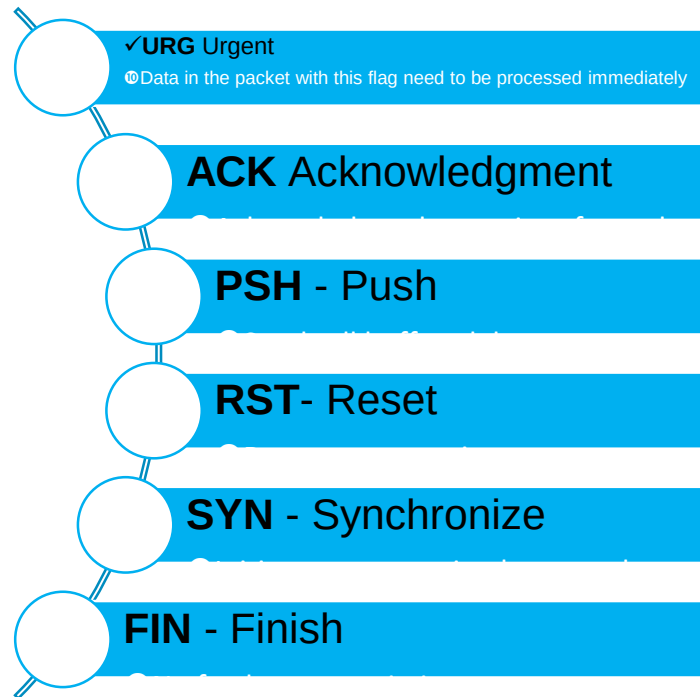
# Common Scanning Techniques

- ICMP scans: check if systems are alive.
- TCP scans: identify open and closed ports.
- UDP scans: detect services without a handshake.

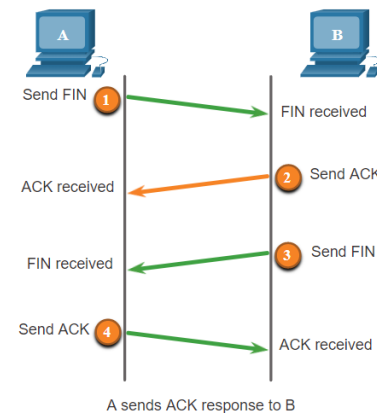
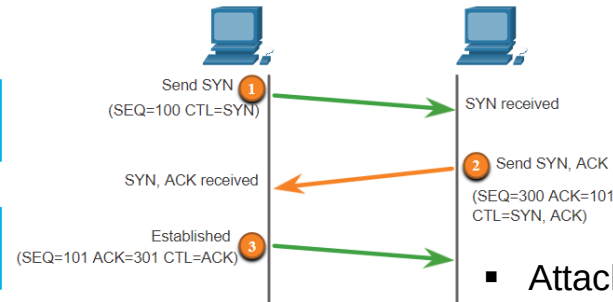
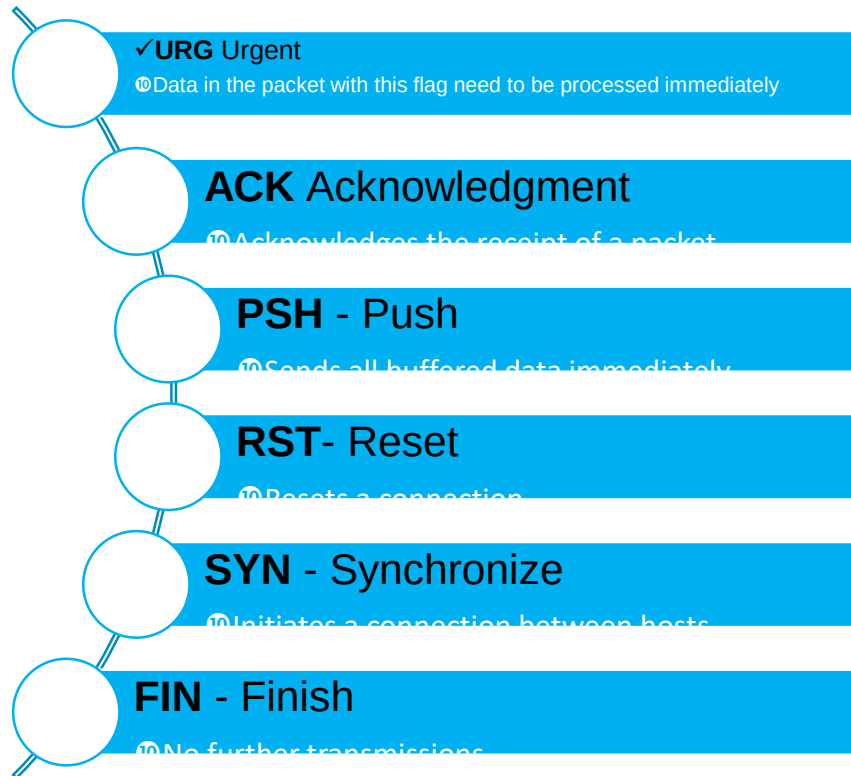
# Main Objectives of Network Scanning



# TCP Communication Flags



# TCP Communication Flags



- Attackers can also create fragmented packets to bypass security systems like firewalls, IDS/IPS.
- Packet Crafting Tools like NetScan Tools Pro, OSTINATO, LANforge FIRE etc can be used.
- Colasoft Packet Builder enables the creation of custom network packets to audit networks for various attacks

# Scanning Networks – IPv6

- Structure of IPv6 is comparatively sophisticated and secured with more levels of addressing hierarchy.
- Focusing on Traditional network scanning Techniques for IPv6 networks brings in complex situation due to its larger subnets.
- So, scanning IPv6 networks involve more techniques rather than using the traditional network scanning tool, as most of the scanning tools do not support ping sweeps on IPv6 networks.
- Need to look into the network traffic, recorded logs, header lines etc to get information about IPv6 addresses.
- However, if successfully scanned, the IPv6 networks gives more privileges. Eg: Compromising One host in the subnet can help in probing all other hosts using “all hosts” and “link-local multicast addresses”

# Scanning Networks: NMAP

## NMAP

- *Purpose of Nmap is to gather Network inventory, managing service upgrade schedules, monitoring hosts, its service uptime etc.*
- *Nmap can be also used to get live host, its services like application name, version, packet filters, firewalls, operating systems, its versions etc*

```
(kali@kali)~$ nmap -p 1-65535 -T4 -A -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 08:08 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating Ping Scan at 08:08
Scanning 10.10.10.16 [2 ports]
Completed Ping Scan at 08:08, 2.00s elapsed (1 total hosts)
Nmap scan report for 10.10.10.16 [host down]
NSE: Script Post-scanning.
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Initiating NSE at 08:08
Completed NSE at 08:08, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.38 seconds
```

```
(kali@kali)~$ nmap -p 1-65535 -T4 -A -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-12 08:09 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.00s elapsed
Initiating Ping Scan at 08:09
Scanning 10.10.10.16 [2 ports]
Completed Ping Scan at 08:09, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:09
Completed Parallel DNS resolution of 1 host. at 08:09, 0.03s elapsed
Initiating Connect Scan at 08:09
Scanning 10.10.10.16 [65535 ports]
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 5985/tcp on 10.10.10.16
Connect Scan Timing: About 23.02% done; ETC: 08:11 (0:01:44 remaining)
Connect Scan Timing: About 58.59% done; ETC: 08:11 (0:00:43 remaining)
Discovered open port 2103/tcp on 10.10.10.16
Discovered open port 49667/tcp on 10.10.10.16
Discovered open port 49668/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Completed Connect Scan at 08:10, 89.30s elapsed (65535 total ports)
Initiating Service scan at 08:10
Scanning 11 services on 10.10.10.16
Service scan Timing: About 54.55% done; ETC: 08:12 (0:00:41 remaining)
Completed Service scan at 08:11, 53.65s elapsed (11 services on 1 host)
NSE: Script scanning 10.10.10.16.
Initiating NSE at 08:11
Completed NSE at 08:12, 40.18s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.03s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Nmap scan report for 10.10.10.16
Host is up (0.0016s latency).
Not shown: 65524 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Microsoft IIS httpd 10.0
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1801/tcp  open  msmq?
2103/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49667/tcp open  msrpc            Microsoft Windows RPC
49668/tcp open  msrpc            Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: o:microsoft:windows

Host script results:
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: SERVER2016, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:1d:c0:ef (VMware)
|_ Names:
|_   WORKGROUP<00>          Flags: <group><active>
|_   SERVER2016<00>        Flags: <unique><active>
|_   SERVER2016<20>        Flags: <unique><active>
|_ smb2-security-mode:
|_   3.1.1:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2022-02-12T13:11:43
|_   start_date: 2022-02-12T13:08:51

NSE: Script Post-scanning.
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Initiating NSE at 08:12
Completed NSE at 08:12, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.78 seconds
```

# Scanning Networks: HPING3

## Hping3

- *It is a command line network scanning and packet crafting tool focusing on TCP/IP protocol*
- *It can be used for*
  - *Auditing network security*
  - *Testing Firewall*
  - *manual path MTU discover*
  - *Advanced traceroute,*
  - *Remote OS Fingerprinting*
  - *Remote uptime guessing*
  - *TCP/IP stacks auditing etc*

```
# hping3 --help
usage: hping3 host [options]
-h --help      show this help
-v --version   show version
-c --count     packet count
-i --interval  wait (uX for X microseconds, for example -i u1000)
--fast        alias for -i u10000 (10 packets for second)
--faster      alias for -i u1000 (100 packets for second)
--flood       sent packets as fast as possible. Don't show replies.
-n --numeric   numeric output
-q --quiet     quiet
-I --interface interface name (otherwise default routing interface)
-V --verbose   verbose mode
-D --debug     debugging info
-z --bind      bind ctrl+z to ttl (default to dst port)
-Z --unbind   unbind ctrl+z
--beep        beep for every matching packet received

Mode
default mode  TCP
-0 --rawip    RAW IP mode
-1 --icmp     ICMP mode
-2 --udp      UDP mode
```

```
(root@ SC-205-03) - [/home/ethical]
# hping3 --traceroute -V -1 www.itsecgames.com
using eth0, addr: 172.17.226.155, MTU: 1500
HPING www.itsecgames.com (eth0 31.3.96.40): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.17.224.1 name=SC-205-03.mshome.net
hop=1 hoprtt=19.8 ms
hop=2 TTL 0 during transit from ip=192.168.1.1 name=ttrouter
hop=2 hoprtt=19.6 ms
hop=3 TTL 0 during transit from ip=78.144.1.17 name=ae54-ner001.csm.as13285.net
hop=3 hoprtt=19.6 ms
hop=4 TTL 0 during transit from ip=78.144.1.48 name=ae56-scr001.slh.as13285.net
hop=4 hoprtt=19.3 ms
hop=5 TTL 0 during transit from ip=78.144.1.134 name=ae64-scr101.thw.as13285.net
hop=5 hoprtt=19.1 ms
hop=6 TTL 0 during transit from ip=195.66.227.118 name=UNKNOWN
hop=6 hoprtt=18.9 ms
hop=7 TTL 0 during transit from ip=95.142.106.211 name=te0-14.cr1.nkf.as49685.net
hop=7 hoprtt=38.6 ms
hop=8 TTL 0 during transit from ip=176.74.228.8 name=eth42.eq3-iec-rtr-002.cloudvps.nl
hop=8 hoprtt=38.3 ms
len=28 ip=31.3.96.40 ttl=53 id=59312 tos=0 iplen=28
```

```
(root@ SC-205-03) - [/home/ethical]
# hping3 --traceroute -V 192.168.1.27
using eth0, addr: 172.17.226.155, MTU: 1500
HPING 192.168.1.27 (eth0 192.168.1.27): NO FLAGS are set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.17.224.1 name=SC-205-03.mshome.net
hop=1 hoprtt=19.9 ms
len=40 ip=192.168.1.27 ttl=63 DF id=9519 tos=0 iplen=40
sport=0 flags=RA seq=1 win=0 rtt=559.9 ms
seq=0 ack=12331971 sum=c427 urp=0

len=40 ip=192.168.1.27 ttl=63 DF id=9694 tos=0 iplen=40
sport=0 flags=RA seq=2 win=0 rtt=179.8 ms
seq=0 ack=1929757851 sum=a11c urp=0

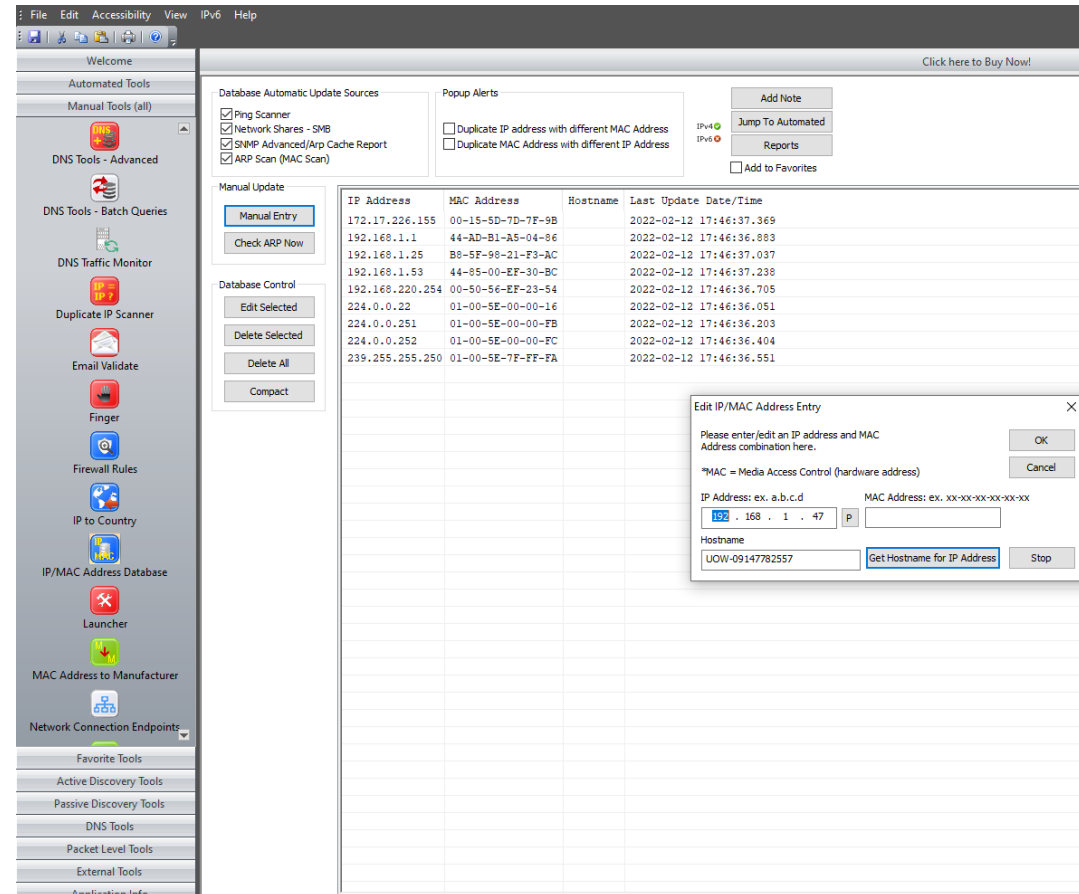
len=40 ip=192.168.1.27 ttl=63 DF id=9849 tos=0 iplen=40
sport=0 flags=RA seq=3 win=0 rtt=419.6 ms
seq=0 ack=1310585994 sum=9911 urp=0

len=40 ip=192.168.1.27 ttl=63 DF id=10101 tos=0 iplen=40
sport=0 flags=RA seq=4 win=0 rtt=339.4 ms
seq=0 ack=421650747 sum=e359 urp=0
```

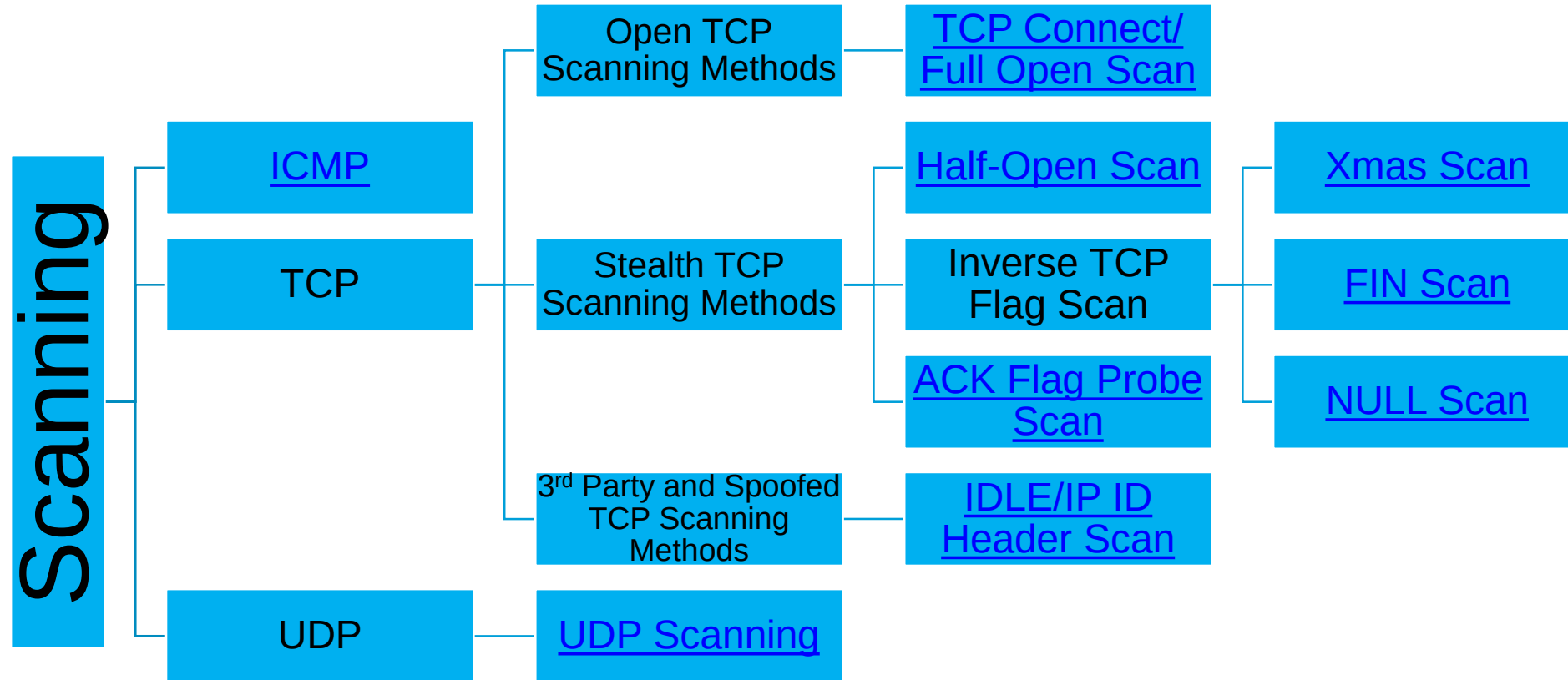
# Scanning Networks: NetScan

## NetScanTools Pro

- *It helps in troubleshooting, diagnosing, monitoring, discovering devices*
- *It lists IPv4, IPv6 Addresses, hostnames, domain names, email addresses, urls.*
- *It does automatically or manually.*



# Scanning Networks - Techniques



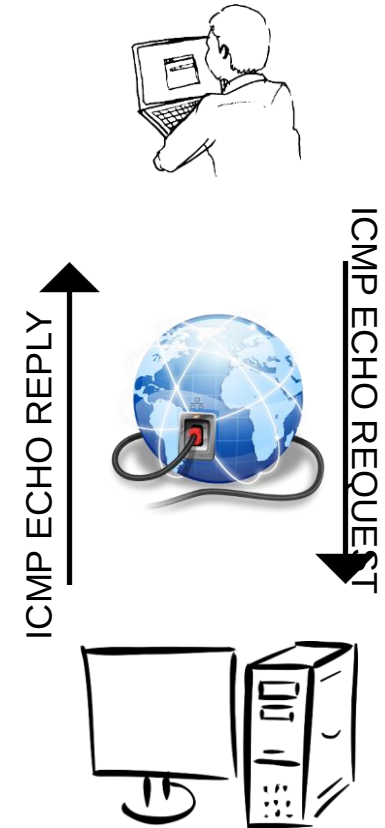
# Scanning Networks – ICMP

- ICMP Scanning – To check for live systems
  - ICMP Scan will send ICMP ECHO requests to a particular host.
  - If the system is LIVE, it will send back an ICMP ECHO reply
  - Using an ICMP Scan, you may
    - ✓ determine an active device.
    - ✓ determine if Firewall is blocking ICMP

≤≤

```
(root@ SC-205-03)-[/home/ethical]
# nmap -sn 192.168.1.27
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 05:17 GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds

≤≤ (root@ SC-205-03)-[/home/ethical]
# nmap -sn 192.168.1.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 05:18 GMT
Nmap scan report for [REDACTED] (192.168.1.47)
Host is up (0.0056s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
```



# Scanning Networks – Ping Sweep

- **PING Sweep – To find live systems from a range of IP Addresses**
  - Ping Sweep will send ICMP ECHO requests to multiple host.
  - If the system is LIVE, it will send back an ICMP ECHO reply
  - You need to determine the subnet mask to find out the number of hosts that are found in the subnet.
  - Mostly, Ping Sweeps are done to create an inventory of live systems in the subnet.

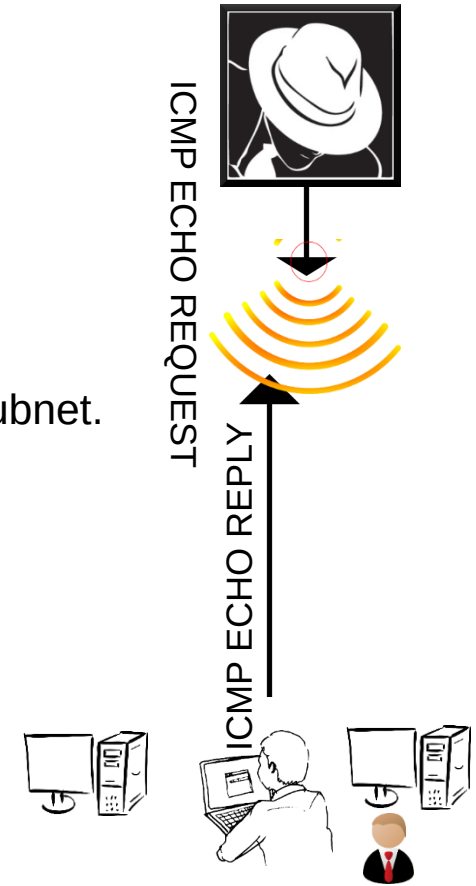
≤

```
Nmap scan report for ttrouter (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 845 closed tcp ports (reset), 151 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
49152/tcp open  unknown

Nmap scan report for 192.168.1.26
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.26 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for UOW-09147782557 (192.168.1.47)
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.32 seconds
```



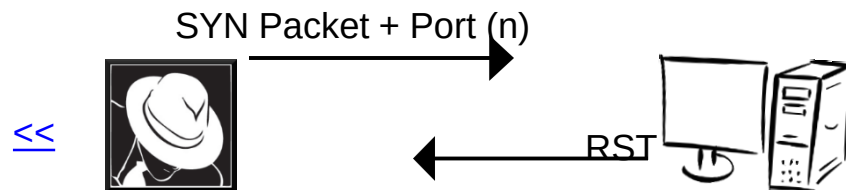
# TCP Scanning Simplified

- TCP uses a three-way handshake to establish connections.
- Full scan: completes the handshake (easy to detect).
- Half-open scan: stops midway to be stealthier.

# Scanning Networks – TCP Connect/ Full Open Scan

- Full Open Scan can detect when a port is open after the three-way handshake
- It **establishes full connection** and **sends back RST Packets** to bring down
  - Does not require super user privileges.

**When a Port is closed?**

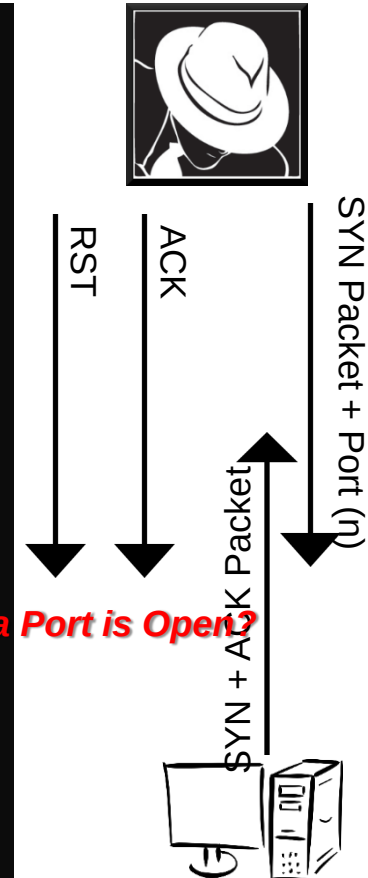


```
(root@ SC-205-03) [/home/ethical]
# nmap -sT -v 192.168.1.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:01 GMT
Initiating Ping Scan at 06:01
Scanning 192.168.1.26 [4 ports]
Completed Ping Scan at 06:01, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
Completed Parallel DNS resolution of 1 host. at 06:01, 1.01s elapsed
Initiating Connect Scan at 06:01
Scanning 192.168.1.26 [1000 ports]
Completed Connect Scan at 06:01, 4.28s elapsed (1000 total ports)
Nmap scan report for 192.168.1.26
Host is up (0.0068s latency).
Not shown: 975 closed tcp ports (conn-refused)
PORT      STATE SERVICE
458/tcp    filtered appletc
801/tcp    filtered device
880/tcp    filtered unknown
1174/tcp   filtered fnet-remote-ui
1434/tcp   filtered ms-sql-m
1443/tcp   filtered ies-lm
1984/tcp   filtered bigbrother
3003/tcp   filtered cgm
3301/tcp   filtered unknown
3784/tcp   filtered bfd-control
3851/tcp   filtered spectraport
4998/tcp   filtered maybe-veritas
5033/tcp   filtered jtnetd-server
5800/tcp   filtered vnc-http
7496/tcp   filtered unknown
9102/tcp   filtered jetdirect
9415/tcp   filtered unknown
9485/tcp   filtered unknown
9878/tcp   filtered kca-service
9900/tcp   filtered iua
24444/tcp  filtered unknown
49175/tcp  filtered unknown
50001/tcp  filtered unknown
55056/tcp  filtered unknown
57797/tcp  filtered unknown

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.65 seconds
Raw packets sent: 4 (152B) | Rcvd: 1 (40B)

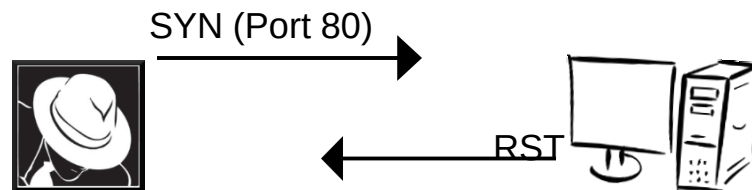
(root@ SC-205-03) [/home/ethical]
# nmap -sT -v 192.168.1.25
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:01 GMT
Initiating Ping Scan at 06:01
Scanning 192.168.1.25 [4 ports]
Completed Ping Scan at 06:01, 3.08s elapsed (1 total hosts)
Nmap scan report for 192.168.1.25 [host down]
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

**When a Port is Open?**



# Scanning Networks – Half Open Scan

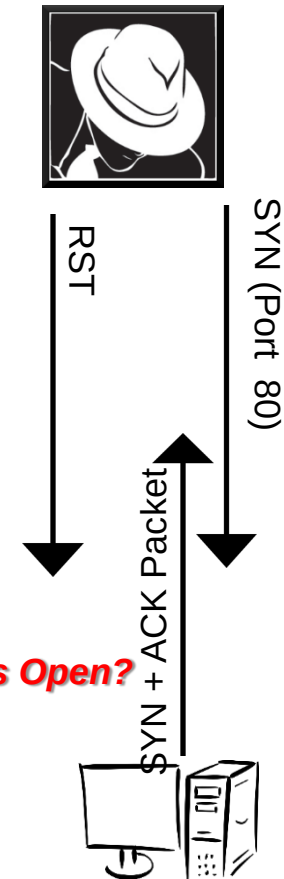
- Otherwise, Stealth Scan can reset the TCP Connection between the client and the server quickly before the three-way handshake, resulting in a half open connection.
- This technique is used to bypass firewall rules, logging mechanism and hide under network traffic.



≤

**When a Port is closed?**

- The Attacker sends a single SYN packet to the target to app. port
- An open port: sends the SYN/ACK packet
- The Attacker sends back RST packet, stating the remote port is in CLOSED state
- The Targets sends the RST packet to close the initiation before a connection is established

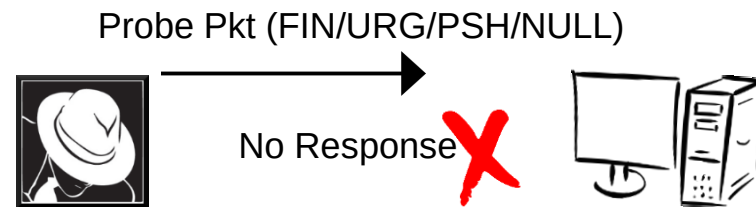


**When a Port is Open?**

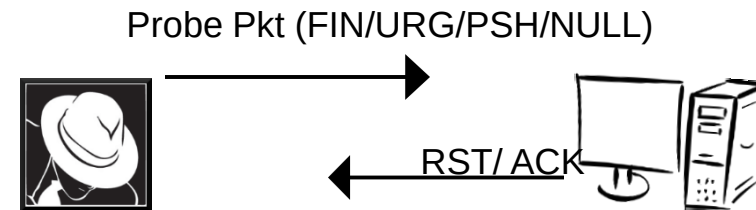
# Scanning Networks – Inverse TCP Flag Scan

- Attackers send TCP probe packets with a TCP Flag (FIN, URG, PSH) set or with no flags.
- No Response? → Port is Open
- RST → Port is Closed

**When a Port is Open?**



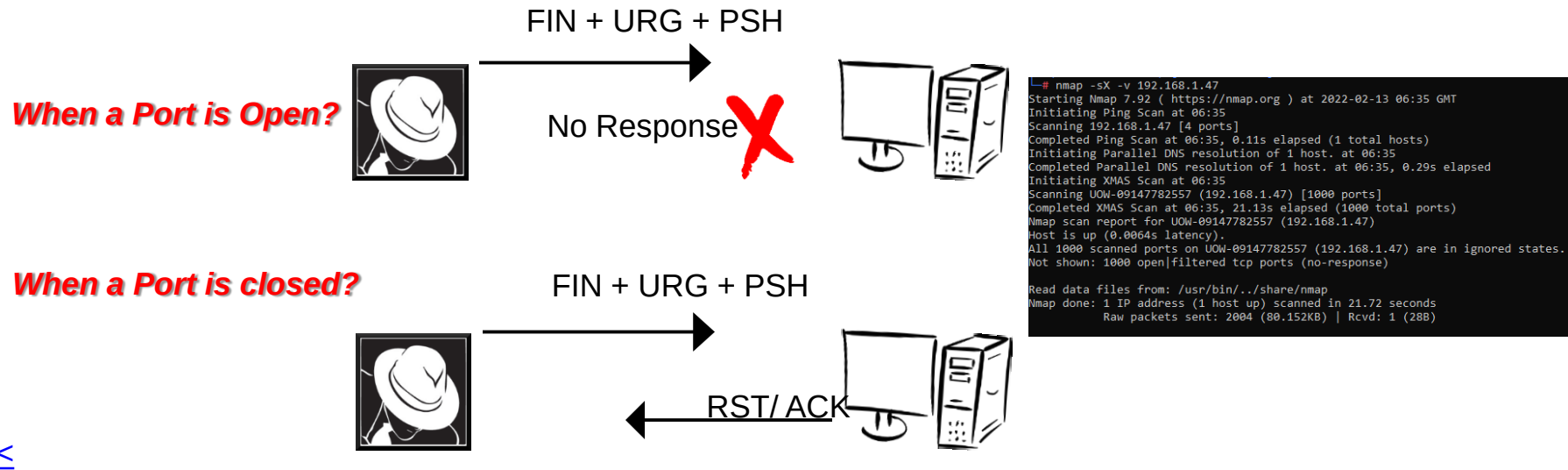
**When a Port is closed?**



≤

# Scanning Networks – Xmas Scan

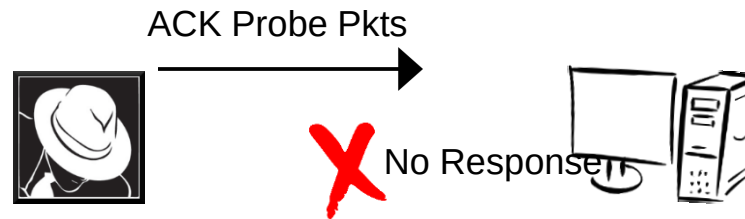
- Attackers send TCP frame to a remote device with (FIN, URG, PSH) set.
- Note: FIN scan works only with RFC 793-based TCP/IP implementation OS. It will not work with any of the current Windows version



# Scanning Networks – ACK Flag Probe Scan

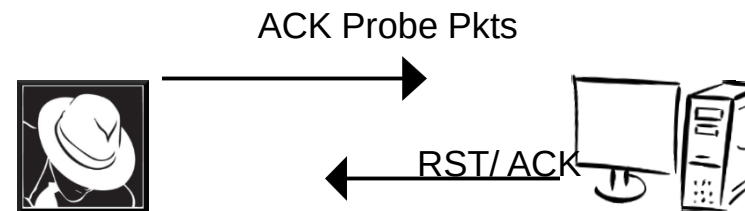
- Attackers send TCP probe pkts to remote devices with ACK Flag set.
- Analyse the header information like TTL, Window Field of received RST packets to find out the open/closed ports

**Stateful Firewall**



**No Firewall**

<<



```
(root@kali)~[/home/kali]
# nmap -sA -v 10.10.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 02:17 EST
Initiating Parallel DNS resolution of 1 host. at 02:17
Completed Parallel DNS resolution of 1 host. at 02:17, 1.07s elapsed
Initiating ACK Scan at 02:17
Scanning 10.10.10.11 [1000 ports]
Completed ACK Scan at 02:17, 0.04s elapsed (1000 total ports)
Nmap scan report for 10.10.10.11
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.10.10.11 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

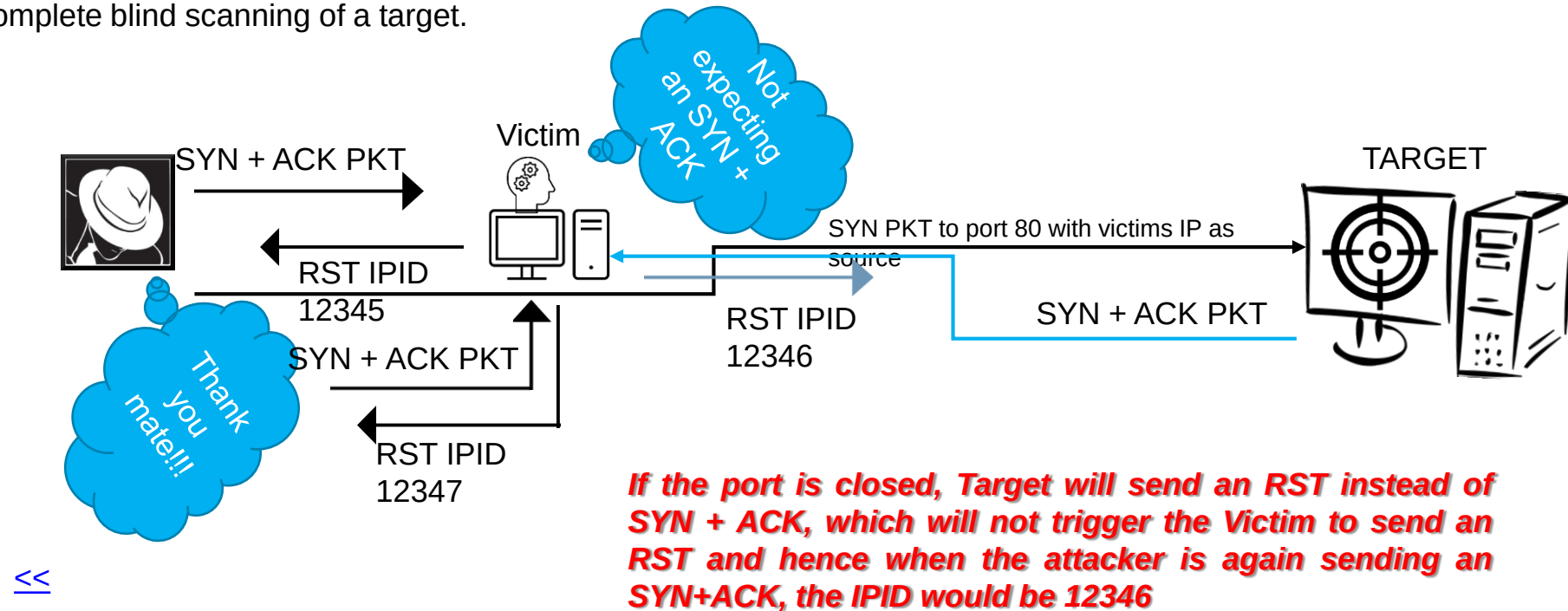
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
Raw packets sent: 1000 (40.000KB) | Rcvd: 2000 (80.000KB)
```

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0

1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
```

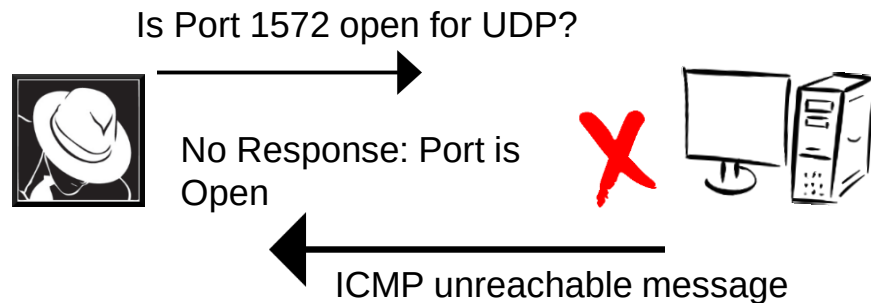
# Scanning Networks – IDLE/ IPID Header Scan

- It is a TCP port scan. However, it uses a spoofed source address to the target to find out the available services.
- It is a complete blind scanning of a target.



# Scanning Networks – UDP Scan

- For UDP, there is no 3-way Handshake. That means, the system won't respond with a message to tell the port status.
- If a UDP packet is sent to a port that is closed, the system will respond with ICMP port unreachable message
- Generally, malicious applications, Trojan horses, Spywares use UDP Ports.



```
(root@kali)~[/home/kali]
# nmap -sU -v 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 03:35 EST
Initiating ARP Ping Scan at 03:35
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 03:35, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:35
Completed Parallel DNS resolution of 1 host. at 03:35, 0.00s elapsed
Initiating UDP Scan at 03:35
Scanning 10.10.10.10 [1000 ports]
Discovered open port 137/udp on 10.10.10.10
Completed UDP Scan at 03:35, 7.30s elapsed (1000 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00039s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 00:0C:29:75:0F:C6 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
Raw packets sent: 2034 (94.116KB) | Rcvd: 10 (1.693KB)
```

## Scanning Networks – SSDP/ List Scan

- SSDP: Simple Service Discovery Protocol working with Universal Plug and Play to detect devices.
- This helps the attackers to launch Buffer Overflow or DoS attacks
- Metasploits, or UPnP SSDP M-Search info discovery tool could be used to check the UPnP vulnerability.
- List scan generates and prints the IP address and names without pinging them. A reverse DNS resolution could be carried out to identify the host names.

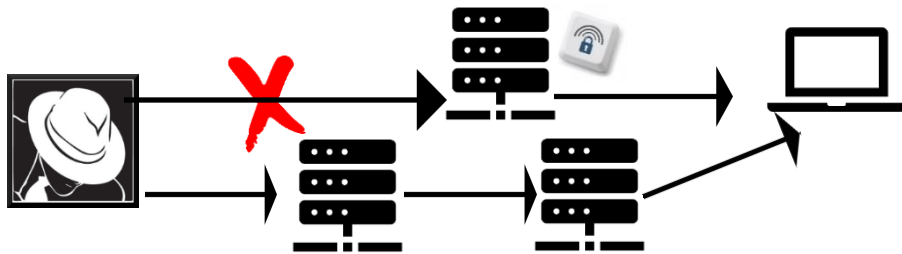
```
(rootkali)-[/home/kali]
# nmap -sL -v 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 03:49 EST
Initiating Parallel DNS resolution of 1 host. at 03:49
Completed Parallel DNS resolution of 1 host. at 03:49, 0.00s elapsed
Nmap scan report for 10.10.10.10
Nmap done: 1 IP address (0 hosts up) scanned in 0.00 seconds
```

# Why Firewalls Matter

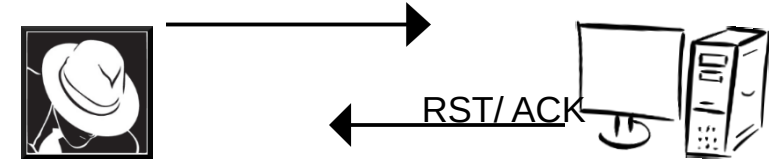
- Firewalls filter incoming and outgoing traffic.
- Attackers try to bypass them using fragmentation or spoofing.
- Defenders analyze packet patterns to detect suspicious behavior.

# Scanning Networks – Firewalls!!!

- *In many cases, placing a Firewall/ IDS, IPS Systems may protect the network from scanning networks. However, there are various methods to overcome Firewalls and other protection mechanisms.*
- One way, is to **fragment (divide into small packets) the probe packets**.
- TCP Header may be split into many small packets in order to avoid packet filtering mechanisms placed in the network.
- **Source Routing** is another way, where the attacker decides on the route (specified route) to ignore the IDS/IPS/Firewalls.



SYN/FIN Small IP Fragments + Port (n)



```
└─$ nmap -sS -T4 -A -f -v 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:21 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating ARP Ping Scan at 04:21
Scanning 10.10.10.16 [1 port]
Completed ARP Ping Scan at 04:21, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:21
Completed Parallel DNS resolution of 1 host. at 04:21, 0.03s elapsed
Initiating SYN Stealth Scan at 04:21
Scanning 10.10.10.16 [1000 ports]
Discovered open port 139/tcp on 10.10.10.16
Discovered open port 445/tcp on 10.10.10.16
Discovered open port 80/tcp on 10.10.10.16
Discovered open port 135/tcp on 10.10.10.16
Discovered open port 1801/tcp on 10.10.10.16
Discovered open port 2105/tcp on 10.10.10.16
Discovered open port 2107/tcp on 10.10.10.16
Discovered open port 2103/tcp on 10.10.10.16
Completed SYN Stealth Scan at 04:21, 4.42s elapsed (1000 total ports)
Initiating Service scan at 04:21
Scanning 8 services on 10.10.10.16
```

## IP Address Decoy / Spoofing

- Generate/ Manually assign an IP address to bypass the firewall. This is known as **IP Address decoy**.
- Change the source IP Address to make it look like an attack from a different source. This could bypass firewalls as 3-way handshake is not complete. This is **IP Address Spoofing**

```
(root@kali)~[/home/kali]
# nmap -D RND:10 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:33 EST
Nmap scan report for 10.10.10.16
Host is up (0.0022s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
MAC Address: 00:0C:29:1D:C0:EF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds

(root@kali)~[/home/kali]
# nmap -n -D 10.10.10.1,10.10.10.3 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-14 04:37 EST
Nmap scan report for 10.10.10.16
Host is up (0.00078s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
MAC Address: 00:0C:29:1D:C0:EF (VMware)

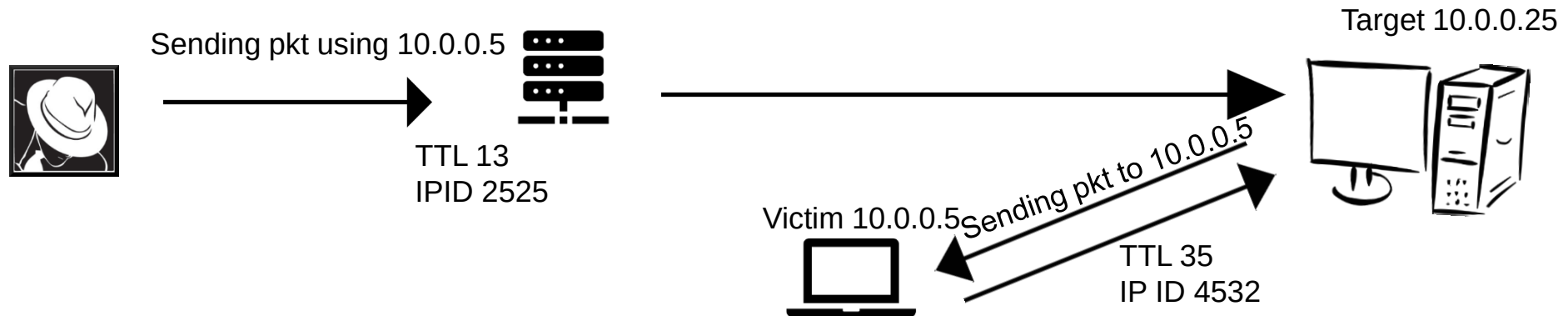
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

[illegible]

# Scanning Networks – Spoofed Packet

As a security professional, there is always ways to analyse the packets to identify these scans

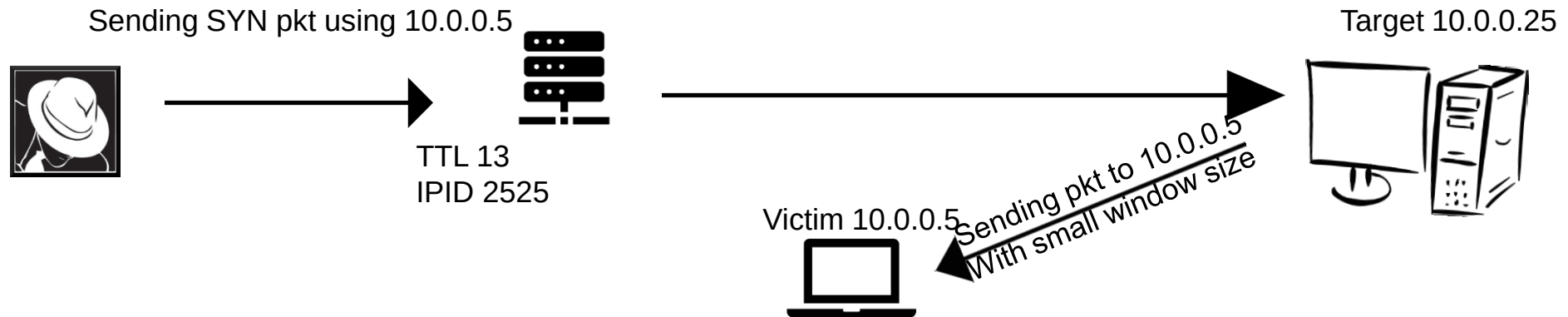
- Send a packet to the host. You will get a reply. **Look at the TTL** with the initial packet received. If the TTL is not same, it is a **spoofed packet**.
- Send probe to the suspected host. **Compare the IPID** in its reply. If IPID value is not any nearest value to the packet examining, it is a **spoofed traffic**.



# Scanning Networks – Spoofed TCP

As a security professional, there is always ways to analyse the packets to identify these scans

- If an attacker is sending a spoofed TCP packet, he/she will **not receive the SYN-ACK**. (as it is spoofed with a different ip address and the SYN-ACK will reach the original spoofed address). This will limit the attackers from receiving any updates. If the received traffic continues even **after a window size exhaustion, the packets are spoofed**.



# Scanning Networks - Countermeasures

- **Information is Wealth:** Restrict sensitive information from public access
- **Firewalls:** Always make sure firewalls/ IDS/ IPS are configured to identify and block probes. Use multiple firewalls.
- **Self-Test:** Try to do TCP and UDP scan along with ICMP probes against your networks IP address to check the status of your network
- **Configurations & Updates:** Have a look at routers and firewall configurations, firmware updates
- **Anti-Spoofing:** Make sure, anti-scanning & anti-spoofing rules are effective
- **Block:** Block unused ports
- **Filter:** Filter all inbound and outbound ICMP messages. Use routers and firewalls to filter incoming packets and outgoing packets.
- **Encrypt all the traffic:** Use Ipsec, TLS, SSH, HTTPS etc
- **IP-based authentication:** It is not reliable. Use random initial sequence number to prevent IP Spoofing attacks based on seq. number spoofing.

# Scanning Networks Proxys

---

*An intermediary device helping in connecting with devices is a proxy server. Proxys help in hiding the actual source of scan and bypass security restrictions.*

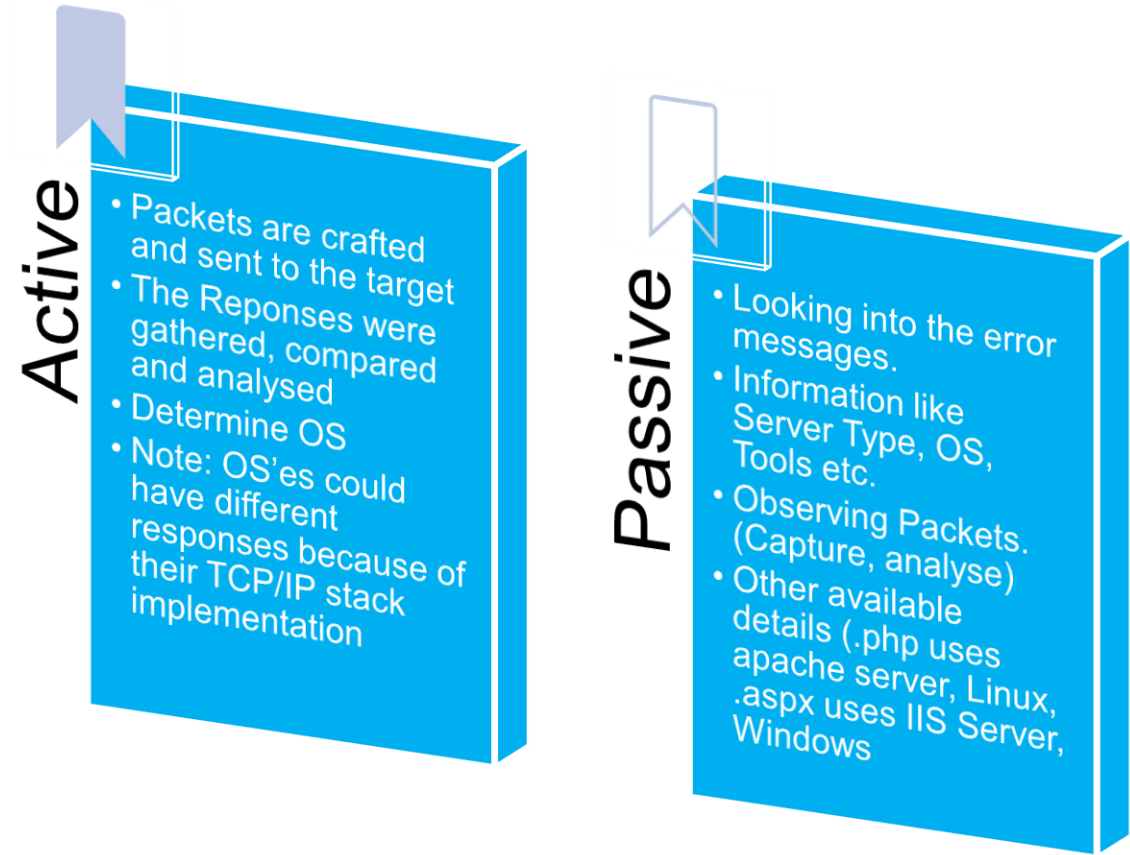
- A Request is made for a resource via a Proxy Client
- The Proxy Client connects to a Proxy server and passes the request
- The Proxy server removes the user id's and passes it to the next proxy server.
- The process continues until the request reaches the resource.
- From the source to the destination, the traffic is encrypted. It is decrypted when it reaches the destination.
- Tools like Proxy Switcher is used to browse internet without disclosing the IP address.
- CyberGhost VPN: Online Privacy, Anonymous Browsing, Access/Block censored contents etc

# Banner Grabbing

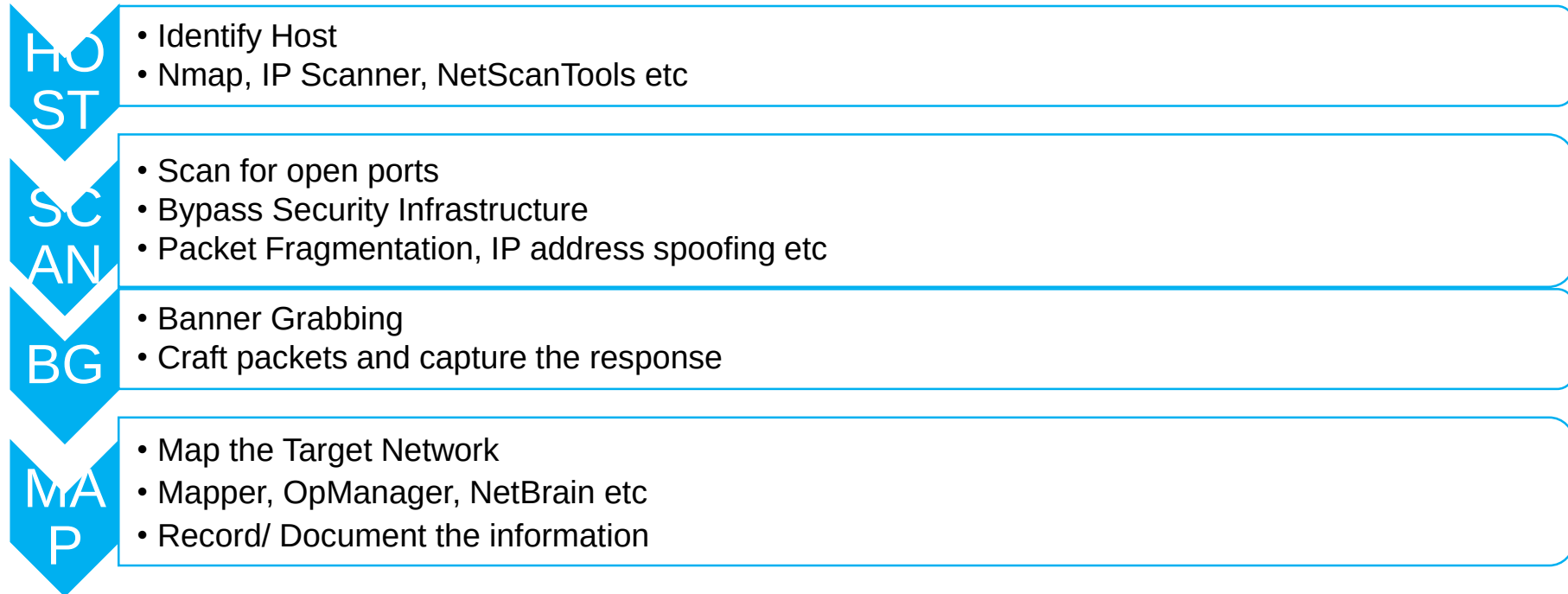
- Banner grabbing identifies software and operating systems.
- It is like reading a name tag on a service.
- Countermeasure: hide or fake banners and disable unused services.

# Scanning Networks – Banner Grabbing

- On discussing about scanning the target for concrete information which would be very helpful in identifying their vulnerabilities, details on Open Ports, Applications etc is good to know. Adding to those information, ***finding out the running operating system*** adds more value to the gathered information.
- Determining / Identifying the target's Operating System is Banner Grabbing.



# Scanning Networks – Steps



# Enumeration Explained

- Enumeration goes deeper than scanning.
- It extracts usernames, shares, services, and configurations.
- Requires domain knowledge of protocols and ports.

# Enumeration

- Like, **Reconnaissance** is the method of collecting information about a target system without alerting it, also known as **Footprinting**, it is the first step in any form of hacking that helps in understanding the target system and identify potential attack vectors & vulnerabilities followed by **network scanning** to identify hosts, ports and services in the network.
- Enumeration is when you try and connect to the system and do deliberate actions to gather more information.



# Key Enumeration Protocols

- NetBIOS: lists systems and shared resources.
- SNMP: gathers device and network configuration details.
- LDAP: retrieves directory and user information.

# IT Infrastructure Enumeration in practice

The main objectives of Enumeration

- ✓ Use the earlier gathered information to look out the weak points to initiate system attack and gain access on the target system

Further get more information, ***but this time from an intranet environment.***

- ✓ Network Resources
- ✓ Shared Folders
- ✓ Routing Information
- ✓ System/ Security Settings
- ✓ Names, Users, Groups
- ✓ Applications
- ✓ SNMP, FQDN Information etc

# Enumeration

- **NetBIOS**

- What it is?
- Used to identify the network devices
- Uses TCP/IP



NetBIOS Name:  
16 Digits  
15 Digits – Device Name  
1 Last Digit – Service/ Name Record Type

- Enumerate NetBIOS information to
- List the computers of the domain.
- List the shares on the hosts
- Look for Policies and Passwords



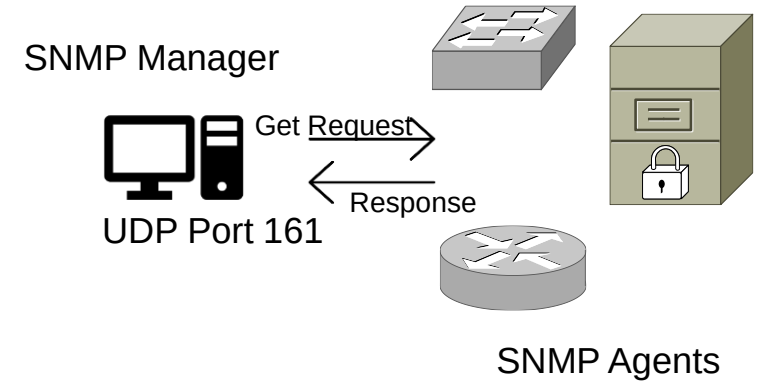
Communication using NetBIOS Name



| Name        | NetBIOS Code | Type   | Information                                                                                |
|-------------|--------------|--------|--------------------------------------------------------------------------------------------|
| <host name> | <00>         | UNIQUE | Hostname                                                                                   |
| <domain>    | <00>         | GROUP  | Domain Name                                                                                |
| <host name> | <03>         | UNIQUE | Messenger Service for the computer                                                         |
| <user name> | <03>         | UNIQUE | Messenger Service for the user logged in                                                   |
| <host name> | <20>         | UNIQUE | Server services running                                                                    |
| <domain>    | <1D>         | GROUP  | Master Browser name for the subnet                                                         |
| <domain>    | <1B>         | UNIQUE | Domain Master browser name: identifies the primary domain controller (PDC) for that domain |

# Enumeration

- **SNMP**
  - SNMP has Manager (NMS) and Agent (Each Network Device)
  - SNMP Manager uses 2 passwords to access and configure its Agents.
    - Read Community String: Public. View device Configuration
    - Read/Write community String: Private. Edit Configuration
  - Enumerating user accounts and devices on a Target System
    - Gathers default community strings information and gets details like hosts, intermediate devices, shares, routing tables, ARP tables, network traffic etc.
  - Community Strings are stored in MIB (Management Information Base) which needs to be matched. If not, an error message will be sent to the pre-configured SNMP Manager.
    - MIB is a virtual database with information related to network objects (*Scalar Objects – define a single object instance; Tabular Objects – Multiple related object instances are grouped*) managed used SNMP
    - MIB database is hierarchical, and they are addressed using Object Identifiers (OIDs). OIDs includes counter, string, address, access levels (not accessible, read-only, read-write), size restrictions, range information etc.
    - SNMP uses the MIB's hierarchical namespace containing Object Identifies (OIDs) to translate the OID numbers into a human-readable display.



# Enumeration

## ○ LDAP

### Active Directory LD Services

- Manageability
- Security
- Interoperability

- AD LDS is a hierarchical file-based directory store with directory information source and the service that makes the information available and usable

#### Network Devices

- Config
- QoS Policy
- Security Policy

#### Email Servers

- Mailbox Information
- Address Book

#### Windows User

- Account Information
- Privileges
- Profiles
- Policies

#### Application

- Server Config
- SSO
- App-Specific Directory Info



- Queries LDAP services and gets information like usernames, department details, address etc.
- Tools like LDAP Admi Tools, LDAP Search, Active Directory Explorer could be used to enumerated LDAP.

# Enumeration from a Defender View

- Close unused ports and services.
- Use strong authentication and access controls.
- Monitor logs and unusual network queries.

# Key Takeaways

- Scanning and enumeration are powerful but risky techniques.
- Understanding them helps us design stronger defenses.
- Always practice ethically and in controlled environments.

# Next Week

- **Learn how to break down systems** to identify critical assets, likely threats, and realistic attack paths before issues arise
- **Discover practical ways to assess** and prioritize security risks using impact, probability, and exposure
- **Explore proven threat modelling** techniques like STRIDE, attack trees, and trust boundaries through real-world examples
- **See how modern teams apply threat modelling** in Agile and DevSecOps to choose effective, risk-based mitigations



Prifysgol Cymru  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

# Any Questions?

*Trawsnewid Addysg; Trawsnewid Bywydau*  
*Transforming Education; Transforming Lives*



[www.uwtsd.ac.uk](http://www.uwtsd.ac.uk)