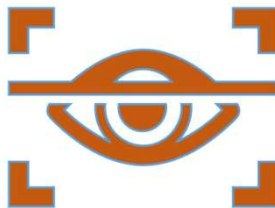




Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Scanning and Enumeration



Advanced Cybersecurity
(ACCB6000)

Applied Computing - WISA

VM Download

\\192.168.135.200\ACCB6000\$

Previous sessions...

- **Understanding Information Security, Risks involved, assessing, managing and monitoring Risks, Cyber risk resilience**
- **Purpose and role of Hackers, Penetration Testing, Various Laws and Standards**
- **Understanding Footprinting and Reconnaissance Concepts, Methodology.**
- **Using various Tools, Taking Countermeasures**

Lab/ Tutorials

- **Download and Setup your Lab.**
- **Coursework Description.**
- **Activity 1: Setup, Configure Lab Environment**
- **Activity 2: Foot printing your Network**

So far, we discussed about Information security, the threats and attack vectors. In continuation to that, I hope you all have understood the hacking concepts and the reasons to stay ethical. Add more insight, we also discussed various security laws and standards. To conclude, we covered various “Risk” concepts like risk factors, cyber risk resilience in the process of enhancing security.

In continuation, we discussed Footprinting concepts focusing on different methodologies like Search Engines, Google Hacking Techniques etc. giving a walkthrough on Website Footprinting, Email Footprinting, Competitive Intelligence, Network Footprinting etc.

During the tutorials, under isolated lab environment we used different Footprinting tools to understand the countermeasures and pen testing attacks.

Scanning and Enumeration

- **Network Scanning**
- **Tools and Techniques**
- **Banner Grabbing**
- **Scanning – Pen Testing**
- **Enumeration a**
 - **Concepts**
 - **Techniques**
 - **Countermeasures**

During this week, with applied knowledge and understanding on Foot printing your network, let us focus on Network Scanning, different tools and methodologies used etc. We shall also understand the concept of Banner Grabbing and scanning Penetration testing. we shall move ahead focusing on enumeration concepts, its different tools and techniques etc

Lab/ Tutorials

- **Activity 3 – Scanning and Enumerating your Network**

During the tutorials, under isolated lab environment you will be using different tools to scan a network and understand the outcomes.

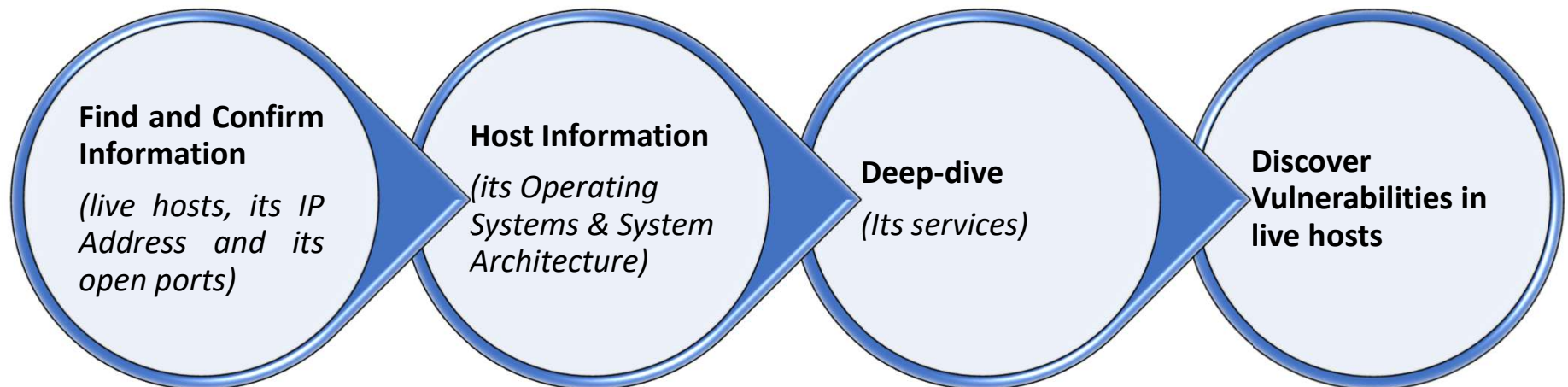
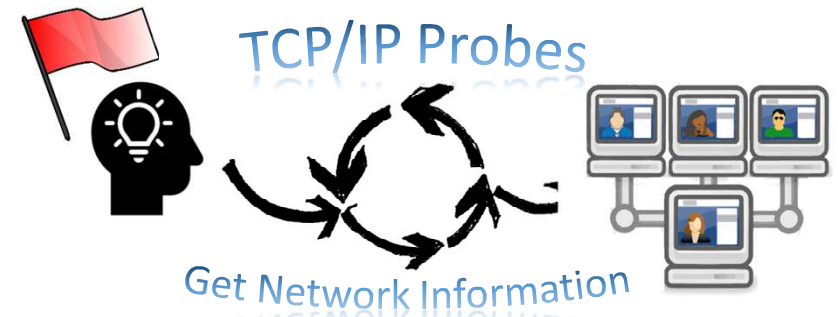
Scanning Networks

- 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.



Scanning Networks

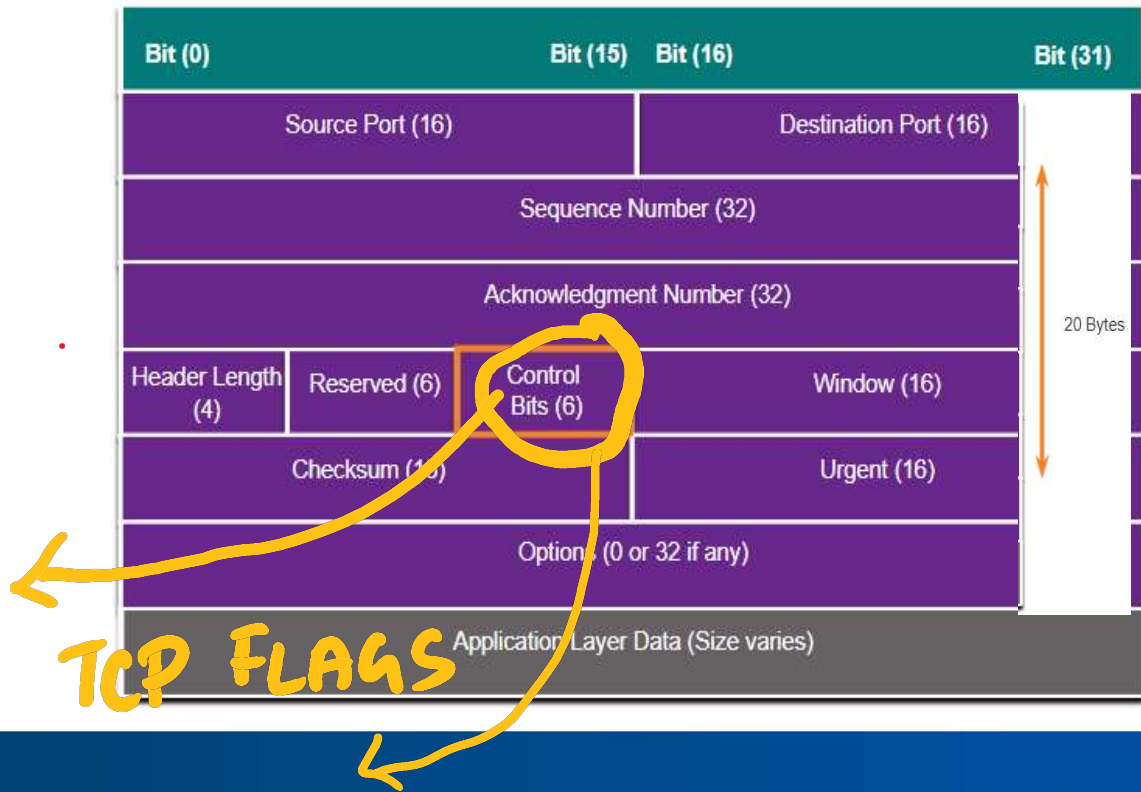
- The main objectives of network scanning



Scanning Networks – TCP Communication Flags

- URG Urgent**
✓ Data in the packet with this flag need to be processed immediately
- ACK Acknowledgment**
✓ Acknowledges the receipt of a packet
- PSH - Push**
✓ Sends all buffered data immediately
- RST- Reset**
✓ Resets a connection
- SYN - Synchronize**
✓ Initiates a connection between hosts
- FIN - Finish**
✓ No further transmissions

Earlier, we discussed about TCP Control Bits, As we know, TCP segment information appears immediately after the IP header.



Scanning Networks – TCP Communication Flags

URG Urgent

✓ Data in the packet with this flag need to be processed immediately

ACK Acknowledgment

✓ Acknowledges the receipt of a packet

PSH - Push

✓ Sends all buffered data immediately

RST- Reset

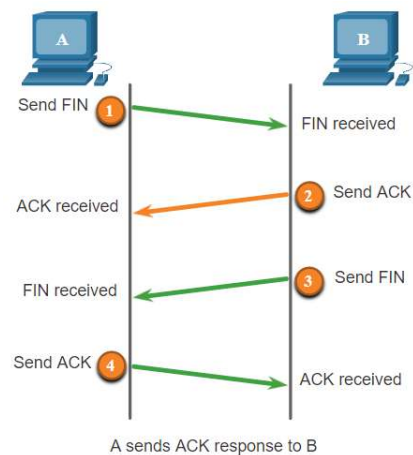
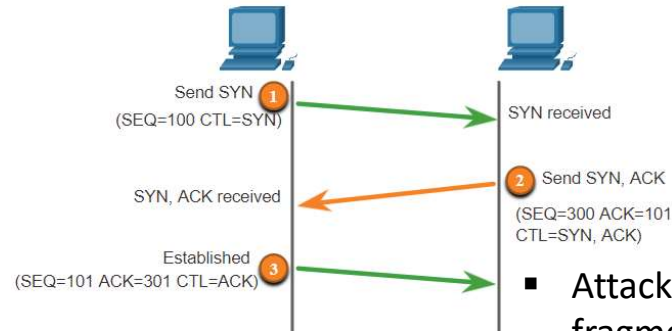
✓ Resets a connection

SYN - Synchronize

✓ Initiates a connection between hosts

FIN - Finish

✓ No further transmissions



- 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: Tools

Many tools are available

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 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
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 -Po
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?            Microsoft Windows RPC
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: 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: Tools

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 discovery*
 - *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
```

```
(root@ SC-205-03) [/home/ethical]
# hping3 --traceroute -V -i 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=tttrouter
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

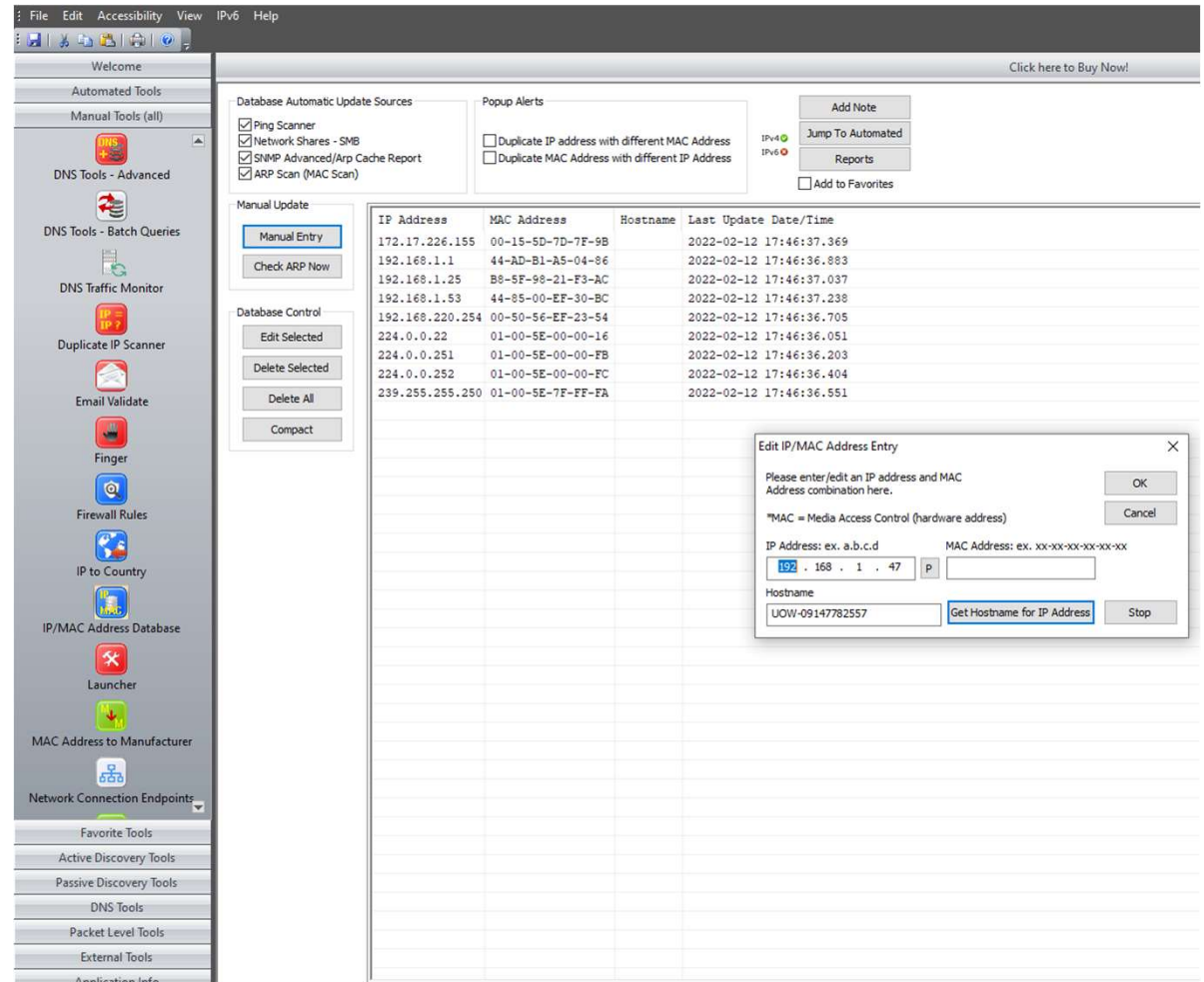
len=40 ip=192.168.1.27 ttl=63 DF id=9849 tos=0 iplen=40
sport=0 flags=RA seq=3 win=0 rtt=419.6 ms
seq=0 ack=1310585994 sum=9911 urp=0

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
```

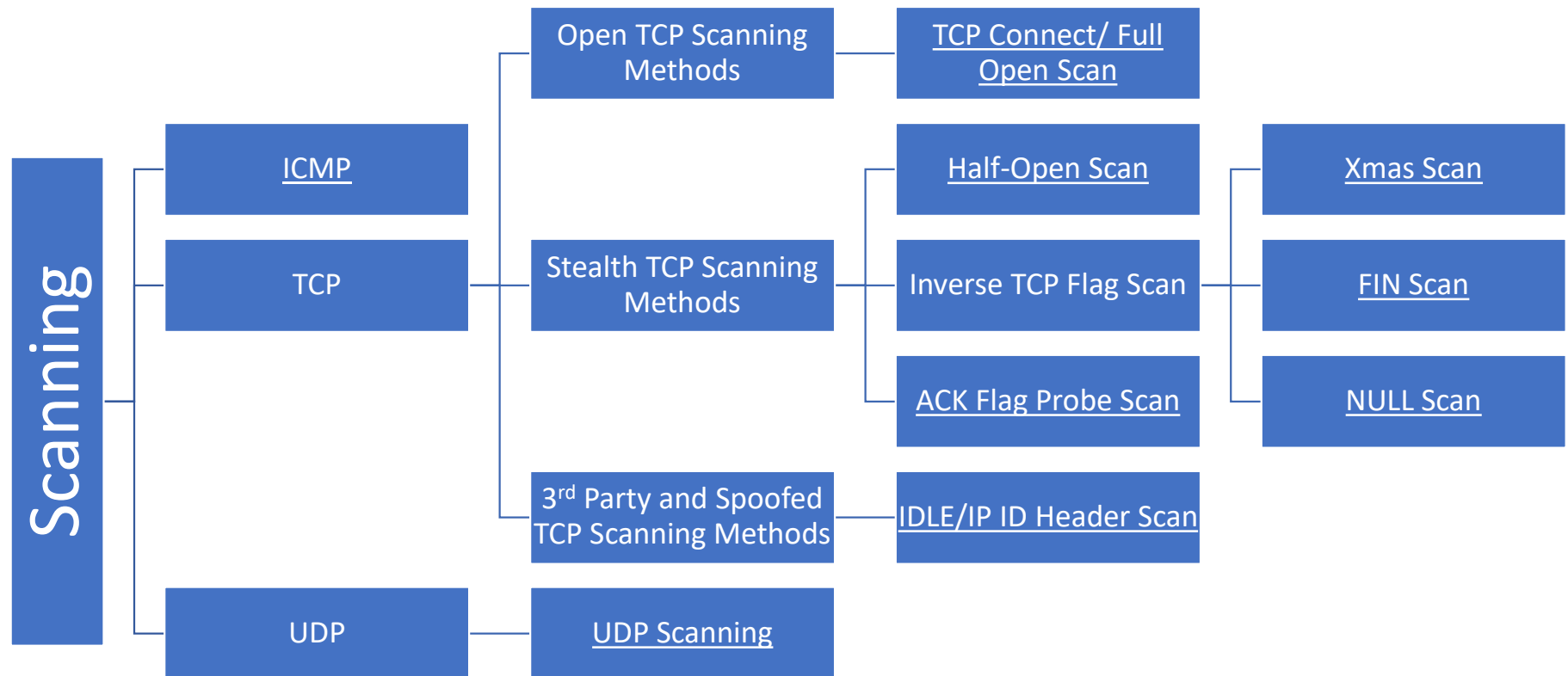
Scanning Networks: Tools

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



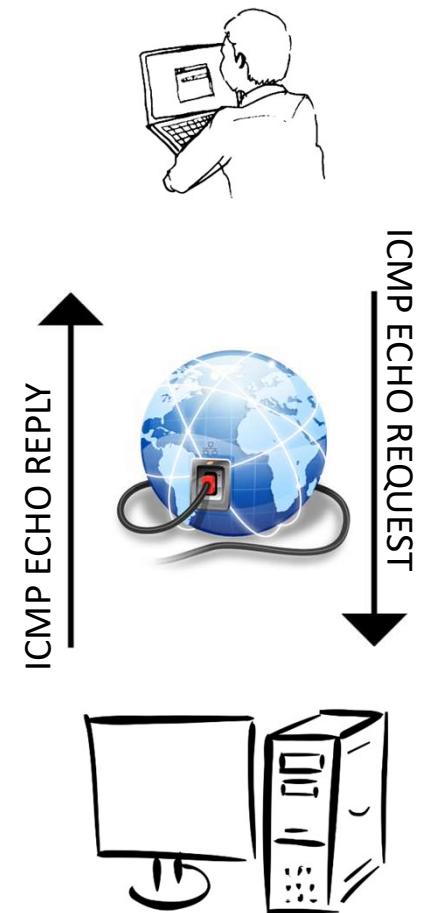
Scanning Networks – ICMP

- **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 192.168.1.47 (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

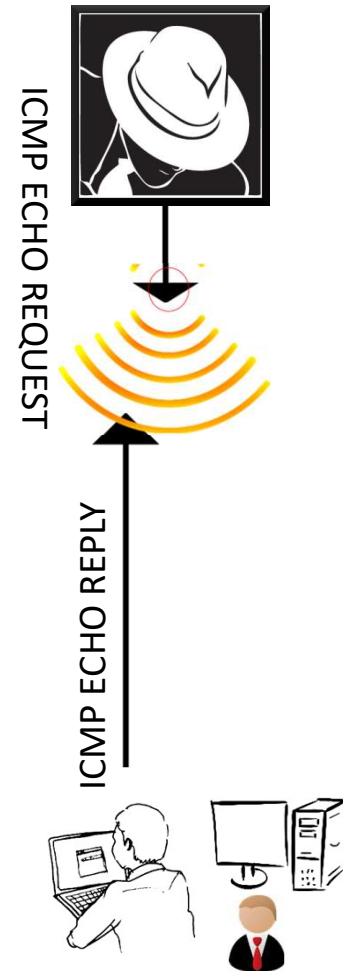
- **PING Sweep – To find live systems from a range of IP Addresses**
 - Ping Sweep will send ICMP ECHO requests to multiple host.
 - If the system is LIVE, it will send back an ICMP ECHO reply
 - You need to determine the subnet mask to find out the number of hosts that are found in the subnet.
 - Mostly,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

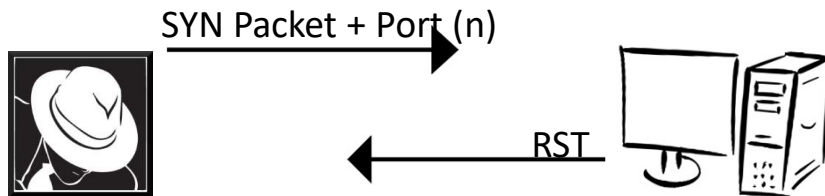
Nmap done: 256 IP addresses (3 hosts up) scanned in 8.32 seconds
```



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?

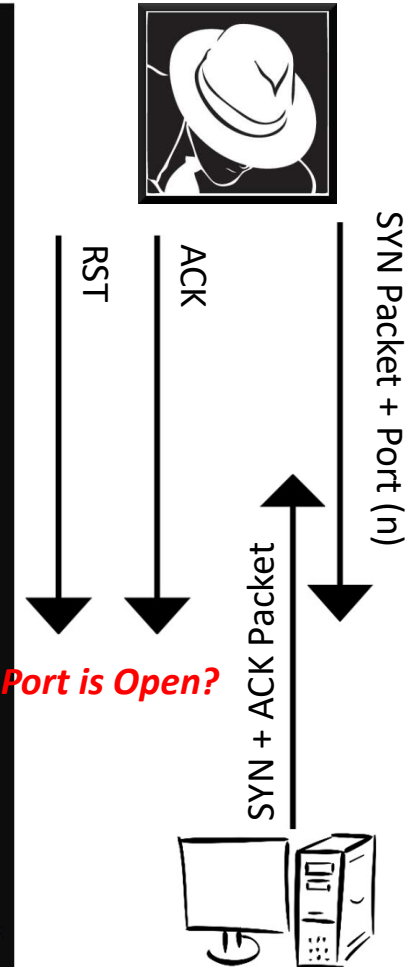


```
(root@ SC-205-03)-[/home/ethical]
# nmap -sT -v 192.168.1.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:01 GMT
Initiating Ping Scan at 06:01
Scanning 192.168.1.26 [4 ports]
Completed Ping Scan at 06:01, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
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  appleqt5
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  cgms
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)
```

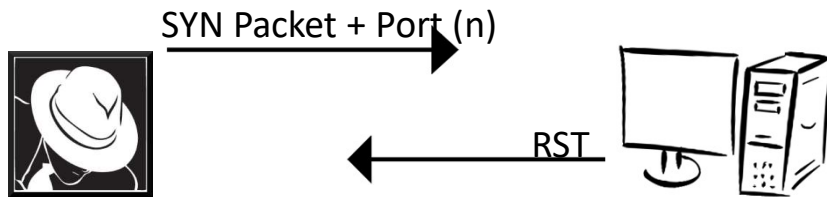
When a Port is Open?



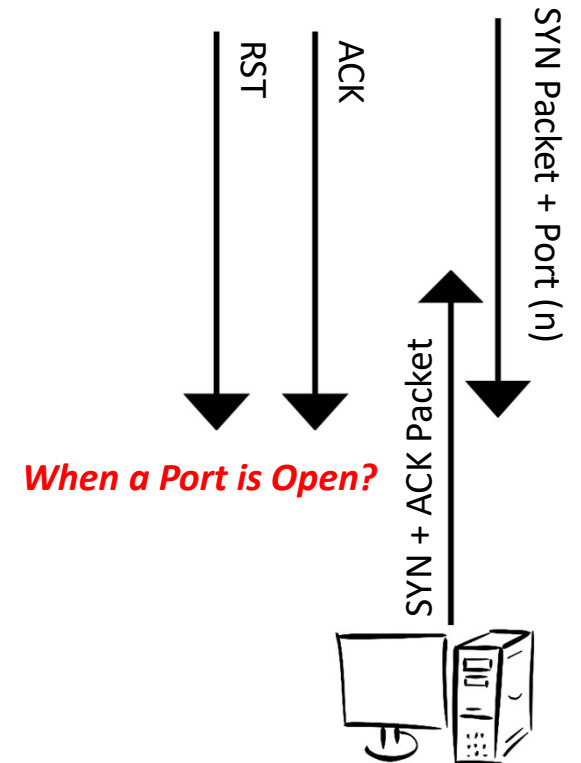
Scanning Networks – TCP Connect/ Full Open Scan

nmap -sT 192.168.0.1

When a Port is closed?

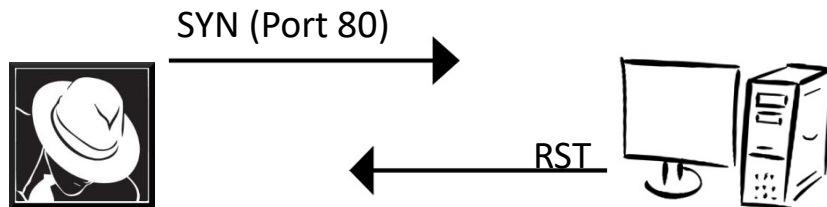


<<



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.



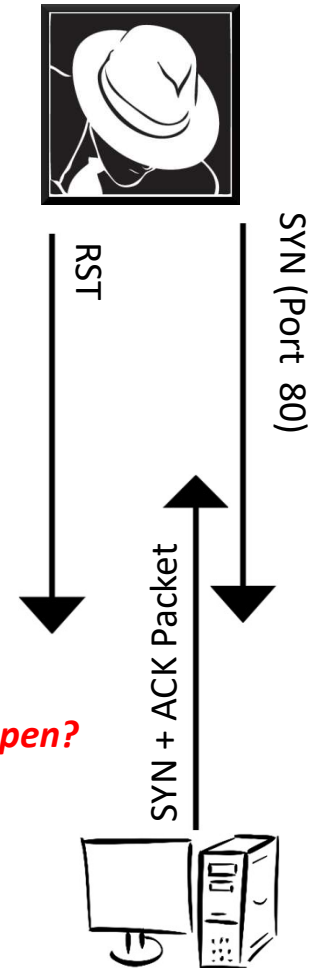
When a Port is closed?

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

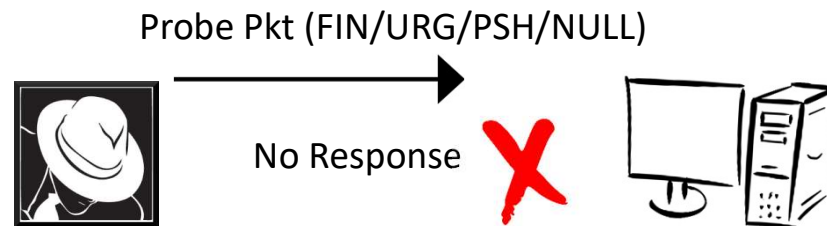


When a Port is Open?

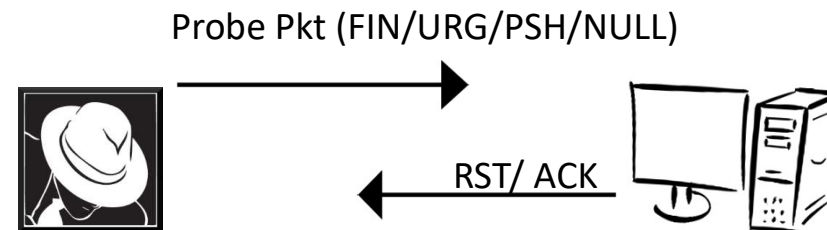
Scanning Networks – Inverse TCP Flag Scan

- 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?

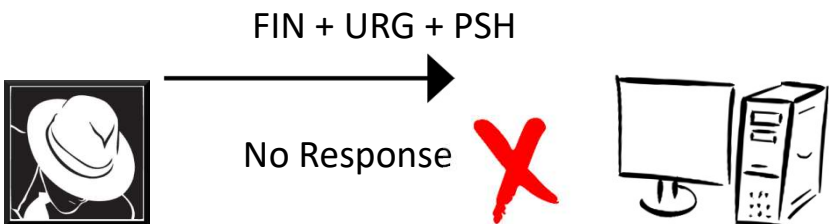


<<

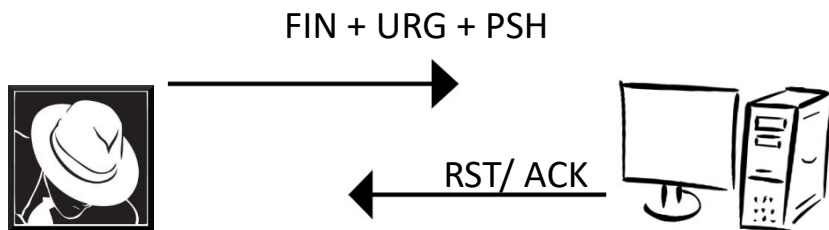
Scanning Networks – Xmas Scan

- 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.

When a Port is Open?



When a Port is closed?



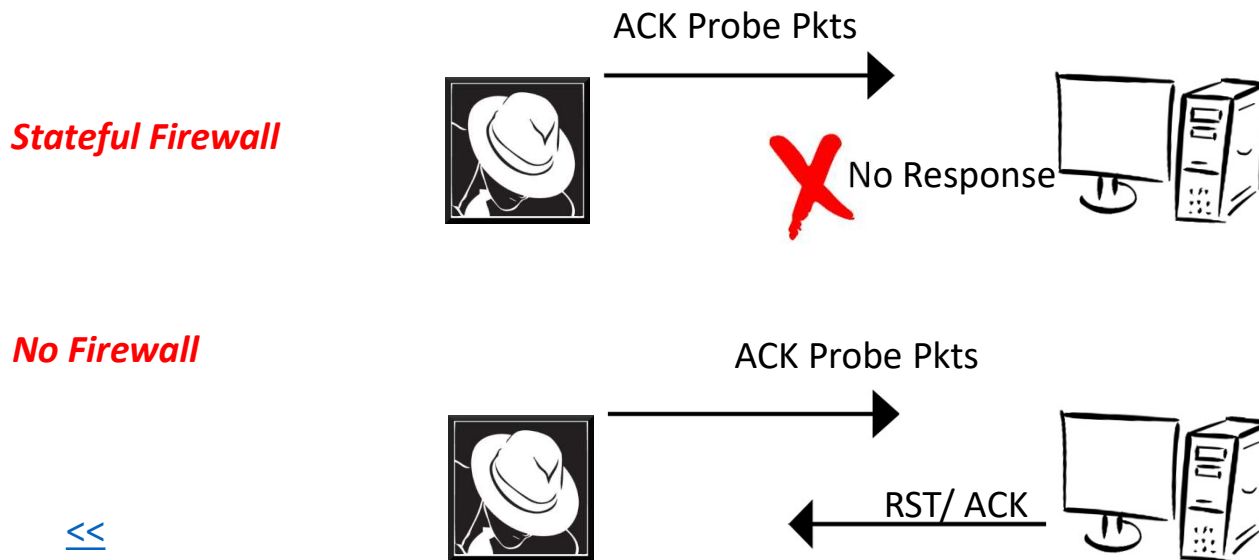
```
# nmap -sX -v 192.168.1.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 06:35 GMT
Initiating Ping Scan at 06:35
Scanning 192.168.1.47 [4 ports]
Completed Ping Scan at 06:35, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:35
Completed Parallel DNS resolution of 1 host. at 06:35, 0.29s elapsed
Initiating XMAS Scan at 06:35
Scanning UOW-09147782557 (192.168.1.47) [1000 ports]
Completed XMAS Scan at 06:35, 21.13s elapsed (1000 total ports)
Nmap scan report for UOW-09147782557 (192.168.1.47)
Host is up (0.0064s latency).
All 1000 scanned ports on UOW-09147782557 (192.168.1.47) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
Raw packets sent: 2004 (80.152KB) | Rcvd: 1 (28B)
```



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



Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

```
(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).
Not shown: 3 ports open on 10.10.10.11 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

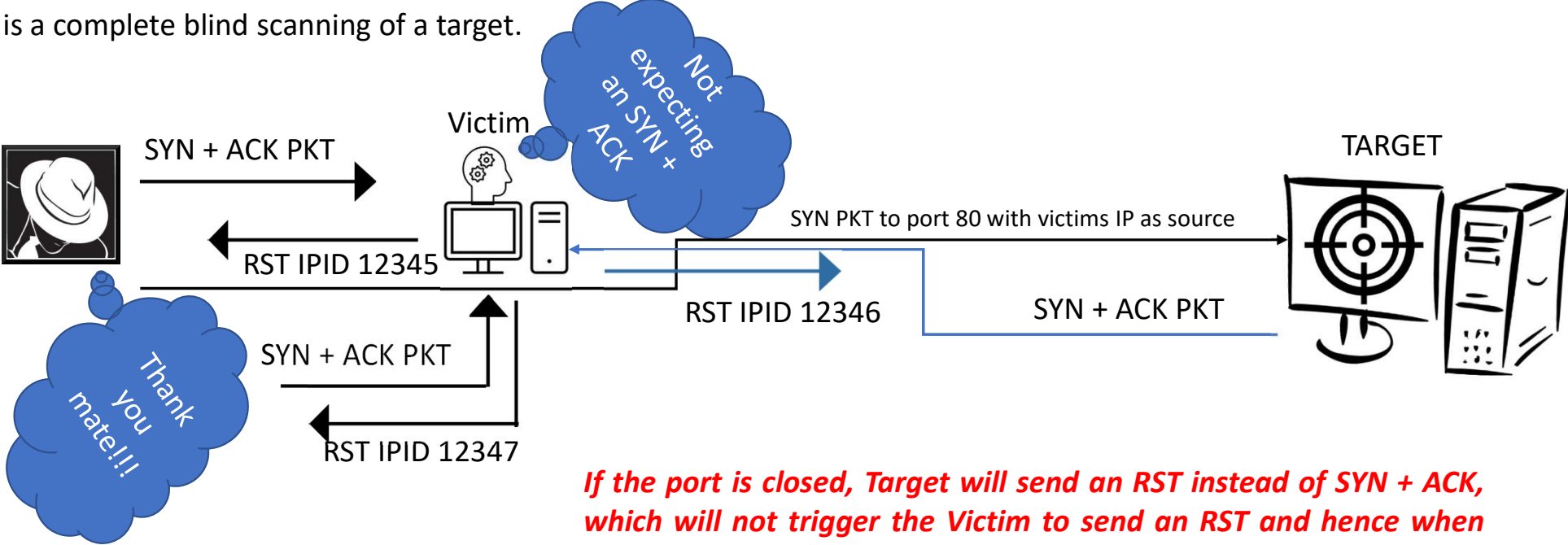
Read data files from: /usr/bin/ /share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds
Raw packets sent: 1000 (40.000KB) | Rcvd: 2000 (80.000KB)

[img alt="Screenshot of a terminal window showing Nmap scan results for 10.10.10.11. The output shows a successful ACK scan with 1000 ports scanned. The raw packet statistics show 1000 packets sent (40.000KB) and 2000 received (80.000KB). Below the main output, there are two detailed Nmap scan reports for 10.10.10.11, one for a standard scan and one for a scan with the --script=ssh option. Both reports show the host is up and provide detailed information about the scan process, including the number of ports scanned, the time taken, and the results of the scan." data-bbox="20 10 977 986"/>
h1
h2
h3
h4
h5
h6
h7
h8
h9
h10
h11
h12
h13
h14
h15
h16
h17
h18
h19
h20
h21
h22
h23
h24
h25
h26
h27
h28
h29
h30
h31
h32
h33
h34
h35
h36
h37
h38
h39
h40
h41
h42
h43
h44
h45
h46
h47
h48
h49
h50
h51
h52
h53
h54
h55
h56
h57
h58
h59
h60
h61
h62
h63
h64
h65
h66
h67
h68
h69
h70
h71
h72
h73
h74
h75
h76
h77
h78
h79
h80
h81
h82
h83
h84
h85
h86
h87
h88
h89
h90
h91
h92
h93
h94
h95
h96
h97
h98
h99
h100
h101
h102
h103
h104
h105
h106
h107
h108
h109
h110
h111
h112
h113
h114
h115
h116
h117
h118
h119
h120
h121
h122
h123
h124
h125
h126
h127
h128
h129
h130
h131
h132
h133
h134
h135
h136
h137
h138
h139
h140
h141
h142
h143
h144
h145
h146
h147
h148
h149
h150
h151
h152
h153
h154
h155
h156
h157
h158
h159
h160
h161
h162
h163
h164
h165
h166
h167
h168
h169
h170
h171
h172
h173
h174
h175
h176
h177
h178
h179
h180
h181
h182
h183
h184
h185
h186
h187
h188
h189
h190
h191
h192
h193
h194
h195
h196
h197
h198
h199
h200
h201
h202
h203
h204
h205
h206
h207
h208
h209
h210
h211
h212
h213
h214
h215
h216
h217
h218
h219
h220
h221
h222
h223
h224
h225
h226
h227
h228
h229
h230
h231
h232
h233
h234
h235
h236
h237
h238
h239
h240
h241
h242
h243
h244
h245
h246
h247
h248
h249
h250
h251
h252
h253
h254
h255
h256
h257
h258
h259
h260
h261
h262
h263
h264
h265
h266
h267
h268
h269
h270
h271
h272
h273
h274
h275
h276
h277
h278
h279
h280
h281
h282
h283
h284
h285
h286
h287
h288
h289
h290
h291
h292
h293
h294
h295
h296
h297
h298
h299
h300
h301
h302
h303
h304
h305
h306
h307
h308
h309
h310
h311
h312
h313
h314
h315
h316
h317
h318
h319
h320
h321
h322
h323
h324
h325
h326
h327
h328
h329
h330
h331
h332
h333
h334
h335
h336
h337
h338
h339
h340
h341
h342
h343
h344
h345
h346
h347
h348
h349
h350
h351
h352
h353
h354
h355
h356
h357
h358
h359
h360
h361
h362
h363
h364
h365
h366
h367
h368
h369
h370
h371
h372
h373
h374
h375
h376
h377
h378
h379
h380
h381
h382
h383
h384
h385
h386
h387
h388
h389
h390
h391
h392
h393
h394
h395
h396
h397
h398
h399
h400
h401
h402
h403
h404
h405
h406
h407
h408
h409
h410
h411
h412
h413
h414
h415
h416
h417
h418
h419
h420
h421
h422
h423
h424
h425
h426
h427
h428
h429
h430
h431
h432
h433
h434
h435
h436
h437
h438
h439
h440
h441
h442
h443
h444
h445
h446
h447
h448
h449
h450
h451
h452
h453
h454
h455
h456
h457
h458
h459
h460
h461
h462
h463
h464
h465
h466
h467
h468
h469
h470
h471
h472
h473
h474
h475
h476
h477
h478
h479
h480
h481
h482
h483
h484
h485
h486
h487
h488
h489
h490
h491
h492
h493
h494
h495
h496
h497
h498
h499
h500
h501
h502
h503
h504
h505
h506
h507
h508
h509
h510
h511
h512
h513
h514
h515
h516
h517
h518
h519
h520
h521
h522
h523
h524
h525
h526
h527
h528
h529
h530
h531
h532
h533
h534
h535
h536
h537
h538
h539
h540
h541
h542
h543
h544
h545
h546
h547
h548
h549
h550
h551
h552
h553
h554
h555
h556
h557
h558
h559
h560
h561
h562
h563
h564
h565
h566
h567
h568
h569
h570
h571
h572
h573
h574
h575
h576
h577
h578
h579
h580
h581
h582
h583
h584
h585
h586
h587
h588
h589
h590
h591
h592
h593
h594
h595
h596
h597
h598
h599
h600
h601
h602
h603
h604
h605
h606
h607
h608
h609
h610
h611
h612
h613
h614
h615
h616
h617
h618
h619
h620
h621
h622
h623
h624
h625
h626
h627
h628
h629
h630
h631
h632
h633
h634
h635
h636
h637
h638
h639
h640
h641
h642
h643
h644
h645
h646
h647
h648
h649
h650
h651
h652
h653
h654
h655
h656
h657
h658
h659
h660
h661
h662
h663
h664
h665
h666
h667
h668
h669
h670
h671
h672
h673
h674
h675
h676
h677
h678
h679
h680
h681
h682
h683
h684
h685
h686
h687
h688
h689
h690
h691
h692
h693
h694
h695
h696
h697
h698
h699
h700
h701
h702
h703
h704
h705
h706
h707
h708
h709
h710
h711
h712
h713
h714
h715
h716
h717
h718
h719
h720
h721
h722
h723
h724
h725
h726
h727
h728
h729
h730
h731
h732
h733
h734
h735
h
```

```
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.

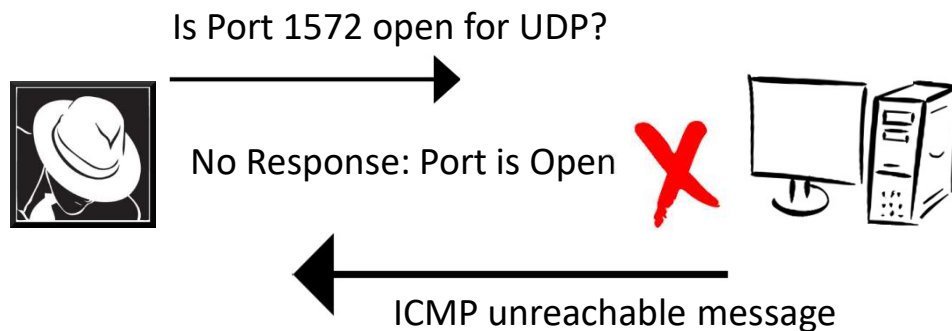


If the port is closed, Target will send an RST instead of SYN + ACK, which will not trigger the Victim to send an RST and hence when the attacker is again sending an SYN+ACK, the IPID would be 12346

<<

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)
```

<<

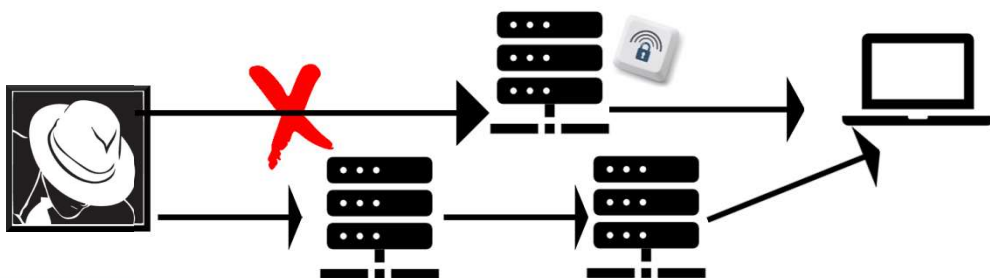
Scanning Networks – SSDP/ List Scan

- **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.

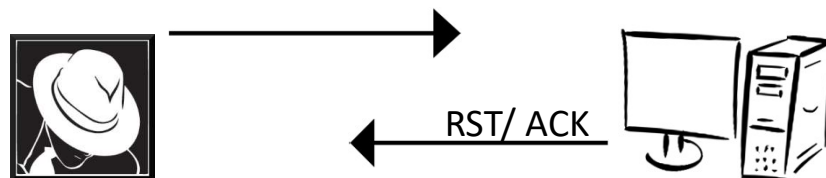
```
(root@kali)-[/home/kali]
# nmap -sL -v 10.10.10.10
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-13 03:49 EST
Initiating Parallel DNS resolution of 1 host. at 03:49
Completed Parallel DNS resolution of 1 host. at 03:49, 0.00s elapsed
Nmap scan report for 10.10.10.10
Nmap done: 1 IP address (0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

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
```

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.*
- 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)

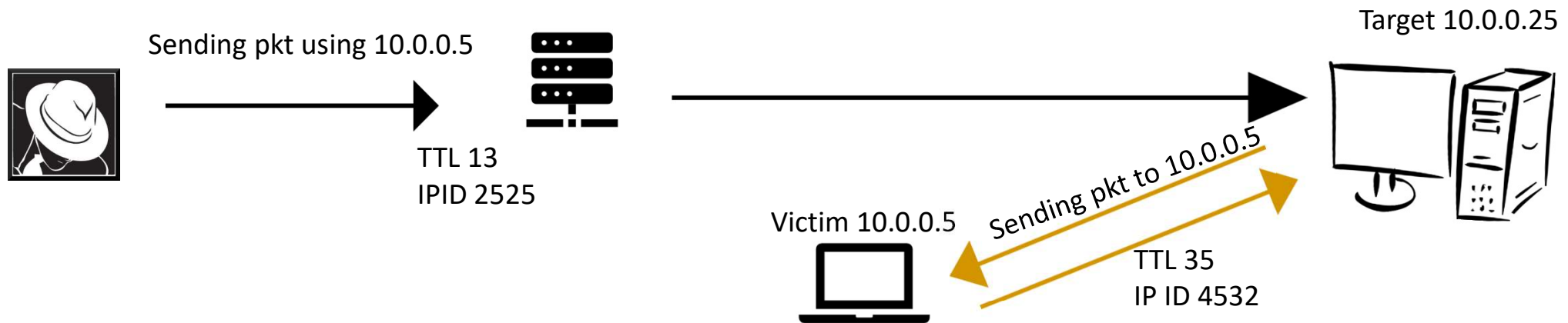
Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
```

[illegible]

Scanning Networks – Security Perspective

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

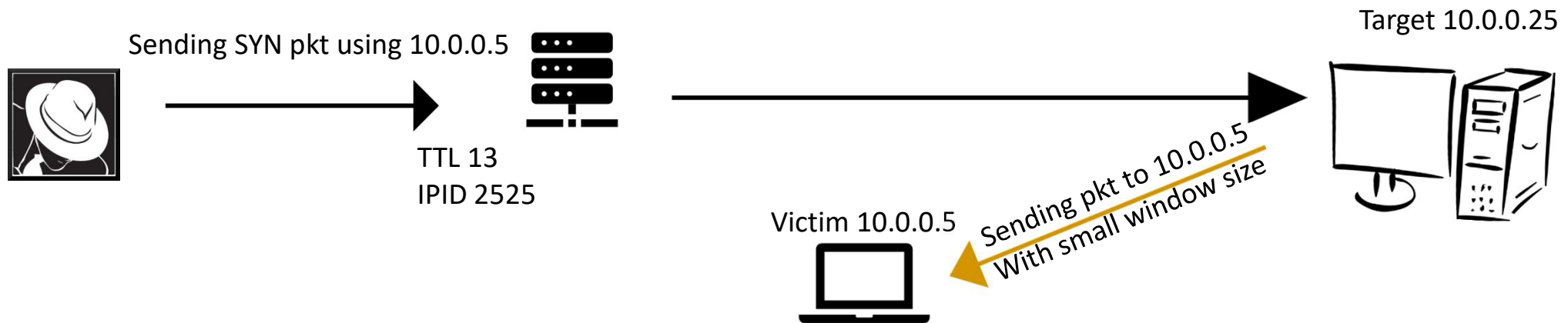
- Send a packet to the host. You will get a reply. **Look at the TTL** with the initial packet received. If the TTL is not same, it is a **spoofed packet**.
- Send probe to the suspected host. **Compare the IPID** in its reply. If IPID value is not any nearest value to the packet examining, it is a **spoofed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



Scanning Networks – Security Perspective

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

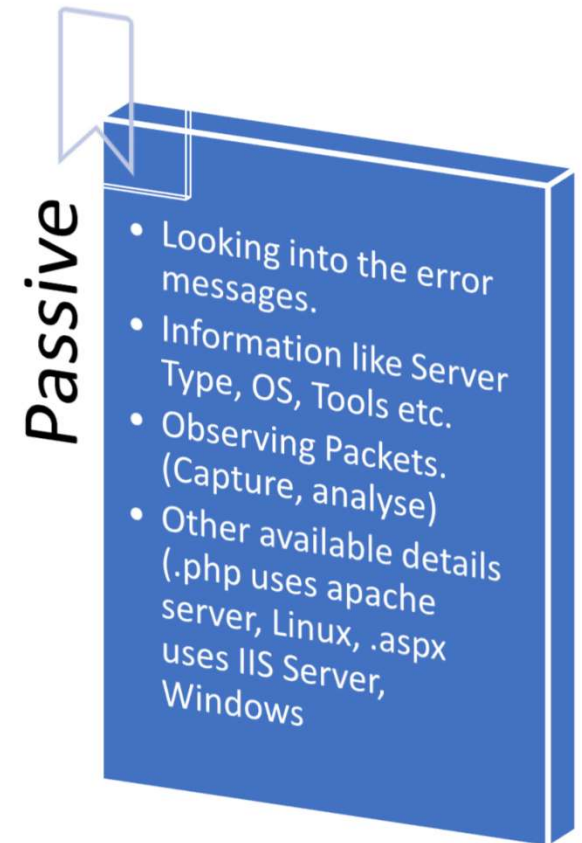
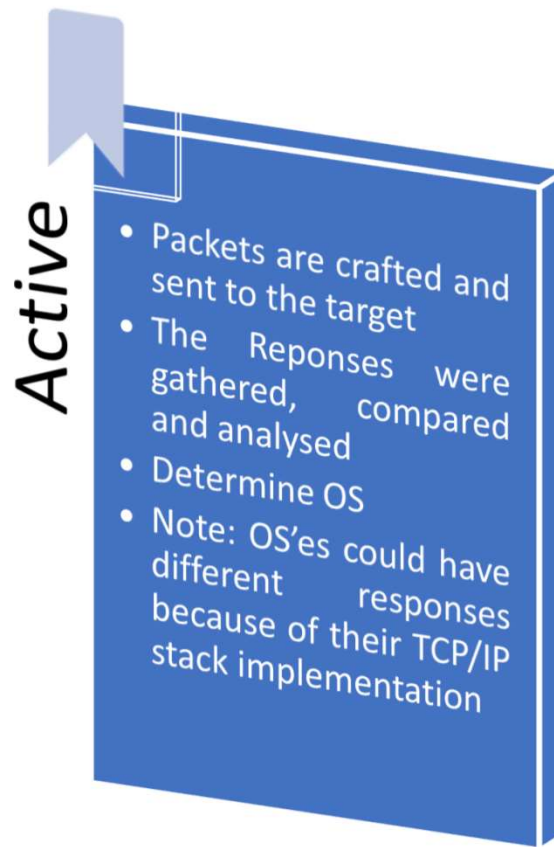
An intermediary device helping in connecting with devices is a proxy server. Proxys help in hiding the actual source of scan and bypass security restrictions.

- 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
- Tor, Burpsite, Proxifier etc...

Any Proxy's you know? List out....

- 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 – Banner Grabbing

Scanning Networks – Banner Grabbing

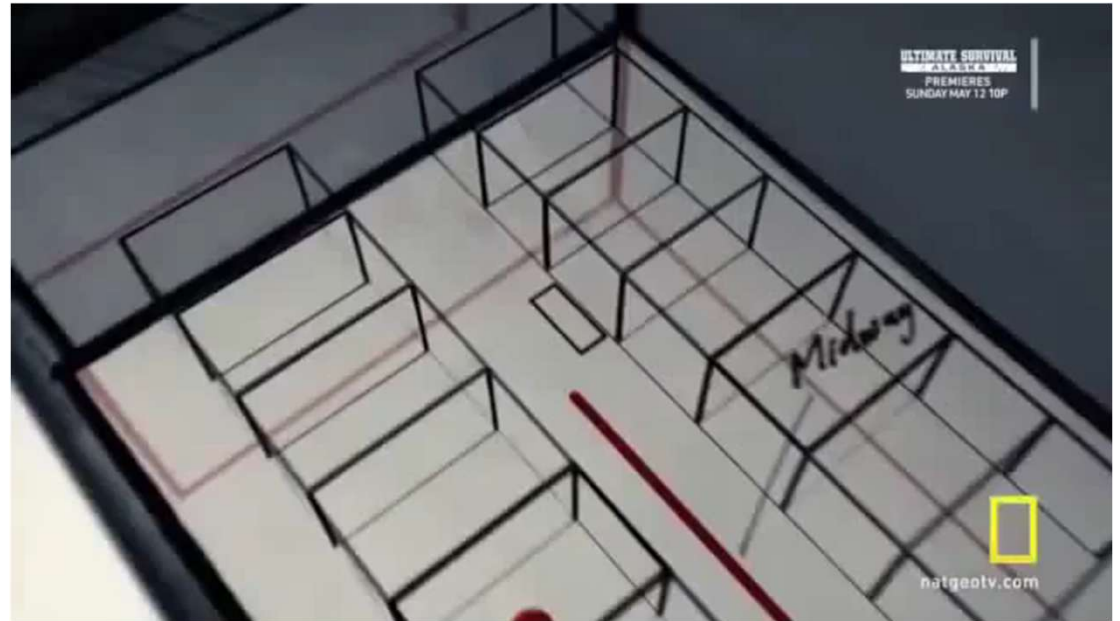
Countermeasures:

- Set False banners.
- Turn off Services that are not used/required
- Hide file extensions.

Scanning Networks –

Map the Infrastructure

- Logical/ Physical path.
 - Intranet
 - DMZ
 - Intranet



Scanning Networks – Security Perspective!!!

As a Security Professional, look at your Network's security.

- Look for
 - ✓ Live systems
 - ✓ Open Ports
 - ✓ Services Running
 - ✓ System Banners
 - ✓ Etc....
- Act on
 - ✓ Close all the unused ports
 - ✓ Disable Services that are not used
 - ✓ Hide Banners
 - ✓ Fix configuration errors
 - ✓ Check Firewall rules.

Scanning Networks – Steps

HOST

- Identify Host
- Nmap, IP Scanner, NetScanTools etc

SCAN

- Scan for open ports
- Bypass Security Infrastructure
- Packet Fragmentation, IP address spoofing etc

BG

- Banner Grabbing
- Craft packets and capture the response

MAP

- Map the Target Network
- Mapper, OpManager, NetBrain etc
- Record/ Document the information

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.

- OH!!! NO----- NOT AGAIN!!!! How many stages are there to collect information?

- Are you really tried? Are you in a hurry? Then this is not your



Enumeration

- 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

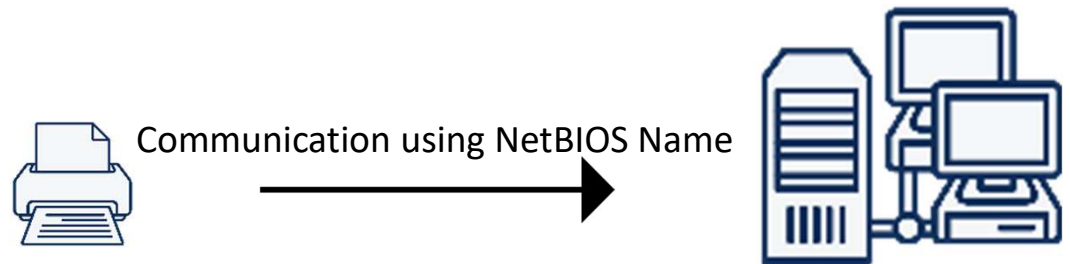
Enumeration

- **NetBIOS**

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



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



NetBIOS Name:

16 Digits

15 Digits – Device Name

1 Last Digit – Service/ Name Record Type

Enumeration

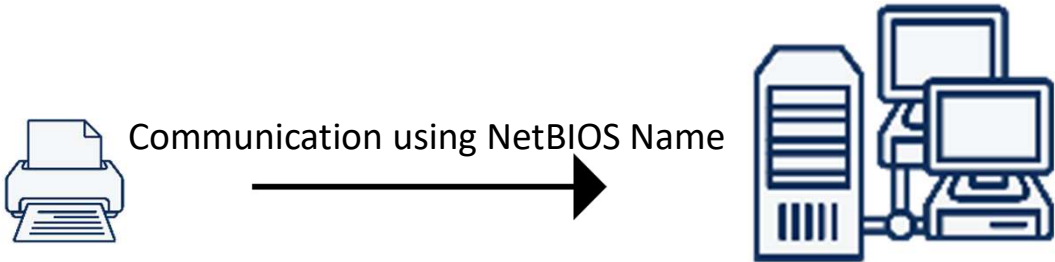
- **NetBIOS**

- 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

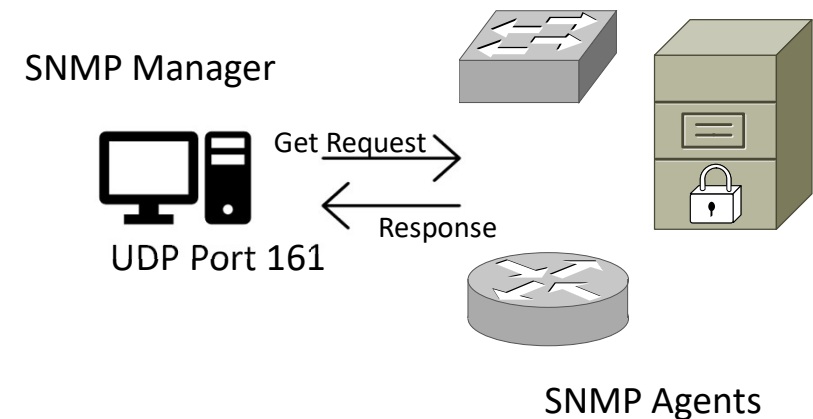


Name	NetBIOS Code	Type	Information
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain Name
<host name>	<03>	UNIQUE	Messenger Service for the computer
<user name>	<03>	UNIQUE	Messenger Service for the user logged in
<host name>	<20>	UNIQUE	Server services running
<domain>	<1D>	GROUP	Master Browser 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

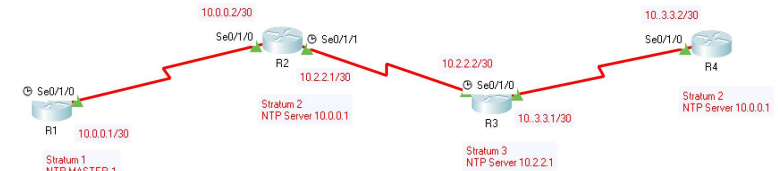
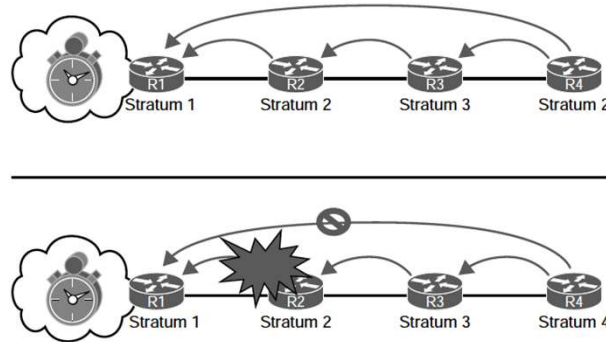
- Server Config
- SSO
- App-Specific Directory Info



- 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

○ NTP



- **Network Time Protocol (NTP)** is used to *synchronize a set of network clocks in a distributed client/server architecture*.
- NTP is a *UDP-based protocol* that connects with *servers* on *port 123*. The *client source port is dynamic*. The Time zone in Cisco devices is *UTC*
- NTP is based on a *hierarchical concept* of communication.
 - At the top of the hierarchy are authoritative devices that operate as an *NTP server with an atomic clock*.
 - The *NTP client queries the NTP server* for its time and then updates its time based on the response.
- The NTP synchronization process is *not fast*, gaining an *accuracy* of tens of milliseconds *requires hours or days of comparisons*.



- Attacker targets NTP server to look for the connected hosts to it, IP Addresses, System Names and Operating Systems.
- Internal IP Address can also be obtained if NTP Server is located in DMZ

Enumeration

- **SMTP**
- **Simple Mail Transfer Protocol (SMTP)** is used to *send emails*.
- SMTP has commands to validate users (vrfy), give actual deliver address and mailing lists (expn) and give the receivers details (rcpt to).
- The response to valid users and invalid users differs in SMTP servers.



- Attacker uses telnet connection to get the list of valid users from an SMTP Server

```
# smtp-user-enum -M VRFY -u rot -t 192.168.1.47
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
| Scan Information |
-----

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Sun Feb 20 07:31:15 2022 #####
##### Scan completed at Sun Feb 20 07:31:20 2022 #####
0 results.

1 queries in 5 seconds (0.2 queries / sec)

(root@SC-205-03)-[/home/ethical]
#
```

Enumeration

DNS

- Enumerating DNS is a process of finding out the DNS Server of the target.
- Enumerating DNS can give an attacker information like DNS Server Names, usernames, IP Address, Host name, machine names etc.
- **DNS Zone Transfer enumeration** is used to get a copy of entire zone file for the domain from DNS Server

IPsec

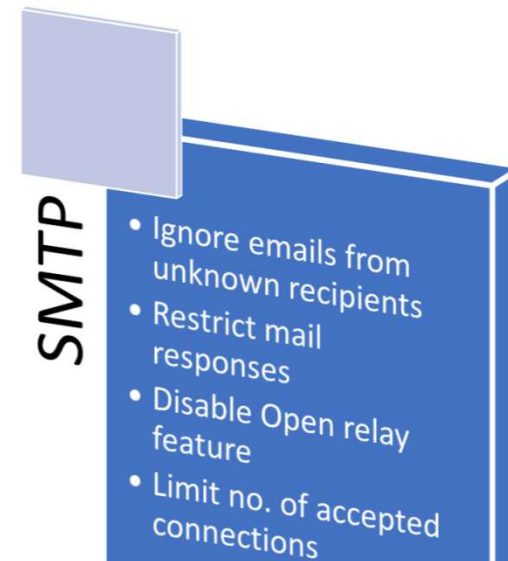
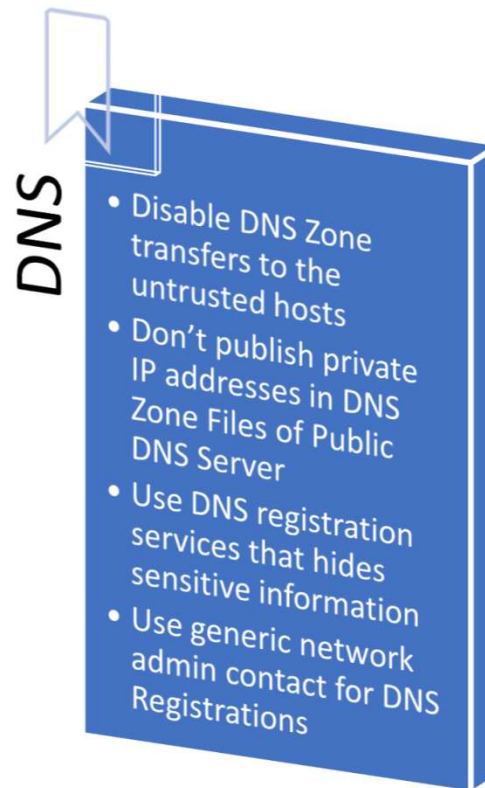
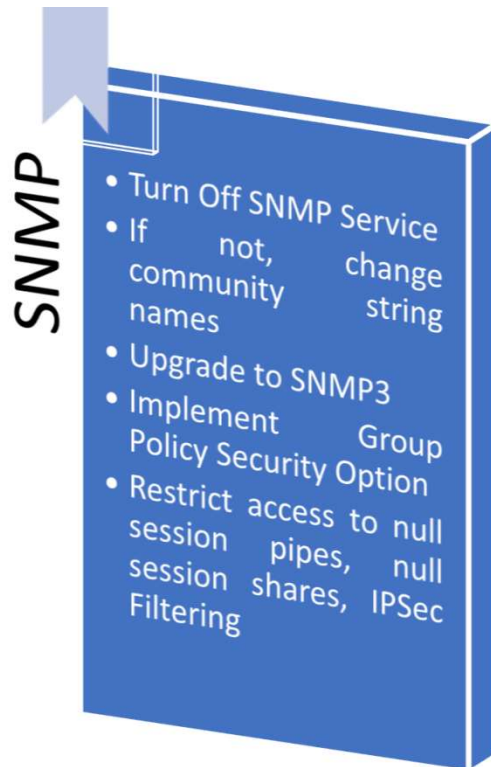
- A scan for ISAKMP in UDP port (???) can indicate the presence of a VPN Gateway.
- Using various available tools, attackers can get information like encrypting & hashing algorithms, authentication type, SA life duration etc.

VoIP

- VoIP (SIP) uses UDP/TCP ports (???)
- Using various available tools, attackers can get information like VoIP gateway/servers, IP-PBX Systems, client softwares/ VoIP Phones, user-extensions etc.
- Later, these information may be used to attack the target.

RPC

- By enumerating RPC endpoints, attackers gather information on vulnerable services on the ports.



```
C:\Users\nitheesh>nslookup
Default Server: ttrouter
Address: 192.168.1.1

> server 31.3.96.40
Default Server: web.mmebvba.com
Address: 31.3.96.40

> set type=any
> ls -d itsecgames.com
ls: connect: No error
*** Can't list domain itsecgames.com: Unspecified error
The DNS server refused to transfer the zone itsecgames.com to your computer. If this
is incorrect, check the zone transfer security settings for itsecgames.com on the DNS
server at IP address 31.3.96.40.

>
```

Enumeration - Countermeasures

LDAP

- Encrypt LDAP traffic
- Enable account lockout

SMB

- Disable SMB protocol on Web & DNS Servers, Internet Facing servers, TCP Ports.
- Restrict anonymous access

Enumeration - Countermeasures

Enumeration – Steps



- Identify Network Range, Calculate Subnet Mask, Discover Host, Scan the Ports
- Whois Lookup, Nmap etc



- Start with NetBIOS Enumeration, SNMP Enumeration, LDAP Enumeration, NTP Enumeration, SMTP Enumeration, DNS Enumeration, Ipsec, VoIP, RPC



- Document all the findings

Module Feedback



VM Download

\\192.168.135.200\ACCB6000\$

Any Questions?

References

- EC-Council CEH
- Cisco Networking Academy
- Tevel Cyber Corps
- Certified Ethical Hacker (CEH) Version 10 Cert Guide, 3rd edition
- Wikipedia
- Other website sources given in this presentation

* The intension of usage is for Educational Purpose Only