

EC-Council

CEH
Certified Ethical Hacker

Module 03

Scanning Networks

Module Flow



1

Network Scanning Concepts

2

Scanning Tools

3

Host Discovery

4

Port and Service Discovery

5

**OS Discovery (Banner Grabbing/
OS Fingerprinting)**

6

Scanning Beyond IDS and Firewall

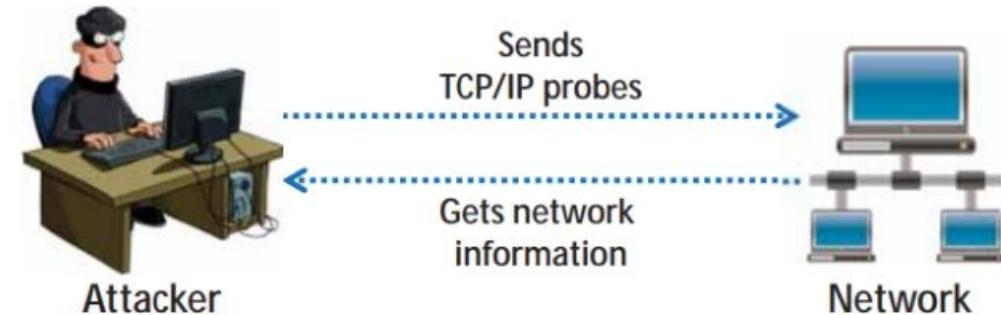
7

Draw Network Diagrams

Overview of Network Scanning

- Network scanning refers to a set of procedures used for **identifying hosts, ports, and services** in a network
- Network scanning is one of the **components of intelligence gathering** which can be used by an attacker to create a profile of the target organization

Network Scanning Process

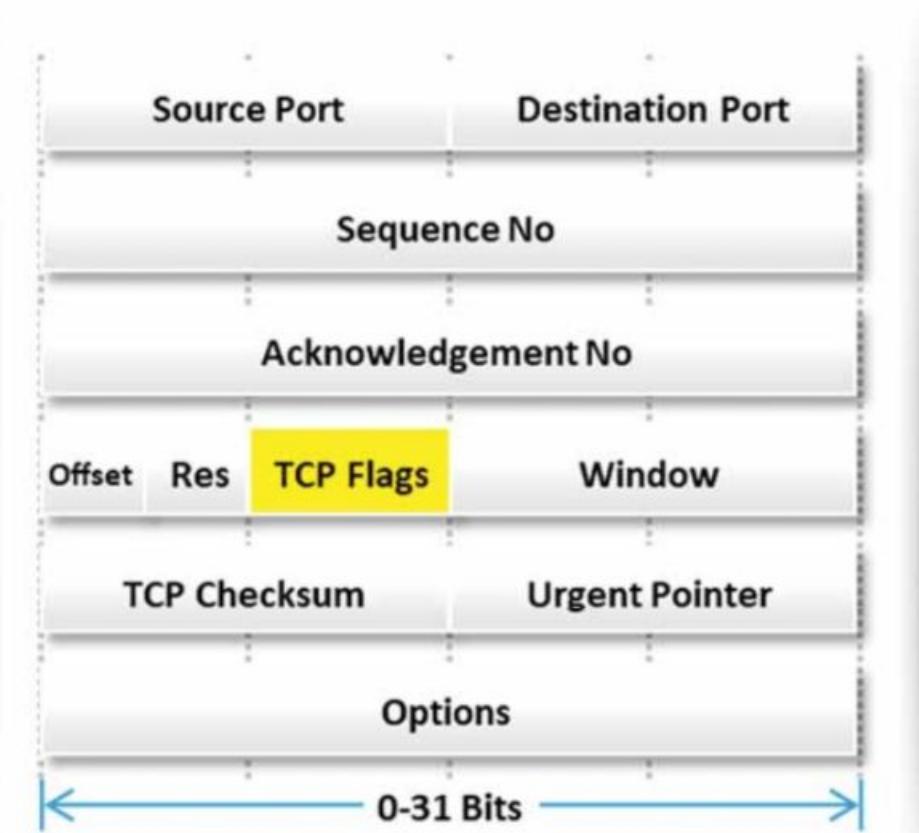
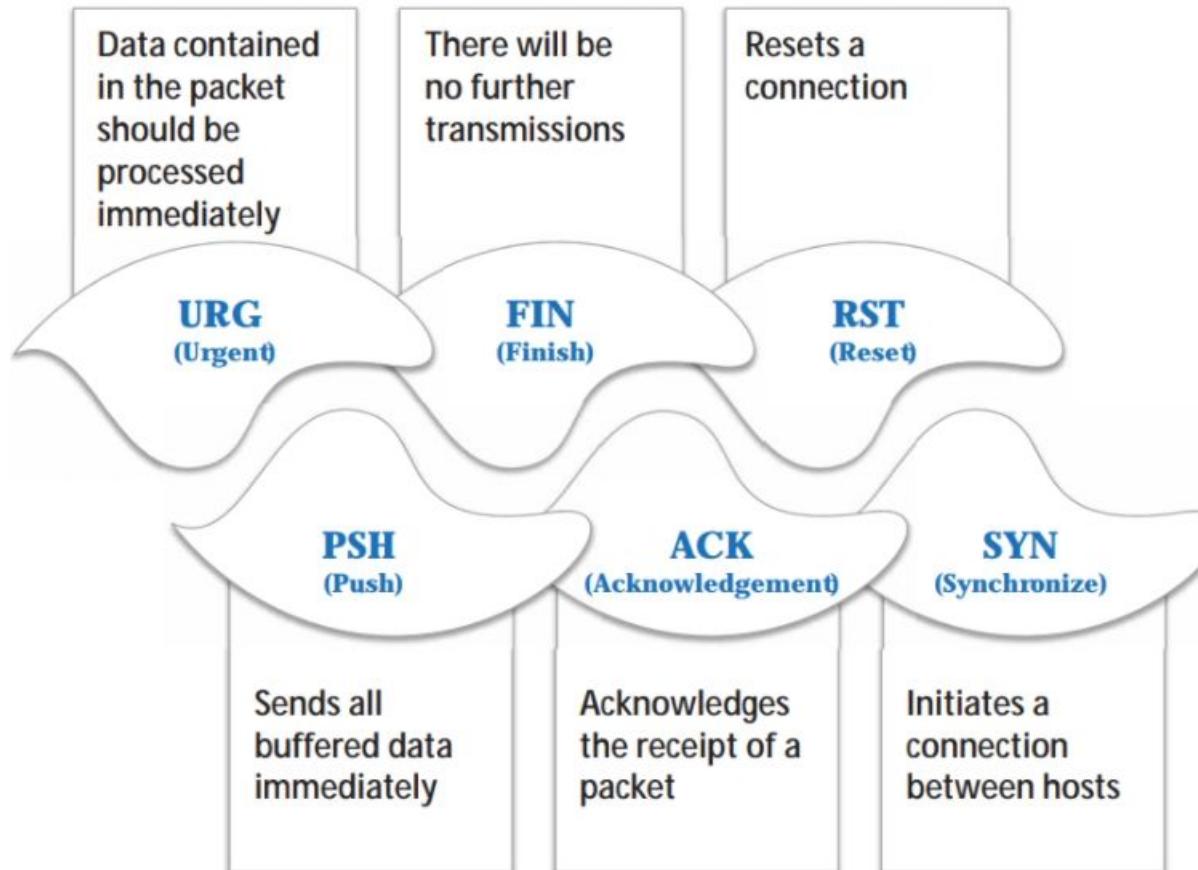


Objectives of Network Scanning

- ➊ To discover live hosts, IP address, and open ports of live hosts
- ➋ To discover operating systems and system architecture
- ➌ To discover services running on hosts
- ➍ To discover vulnerabilities in live hosts



TCP Communication Flags

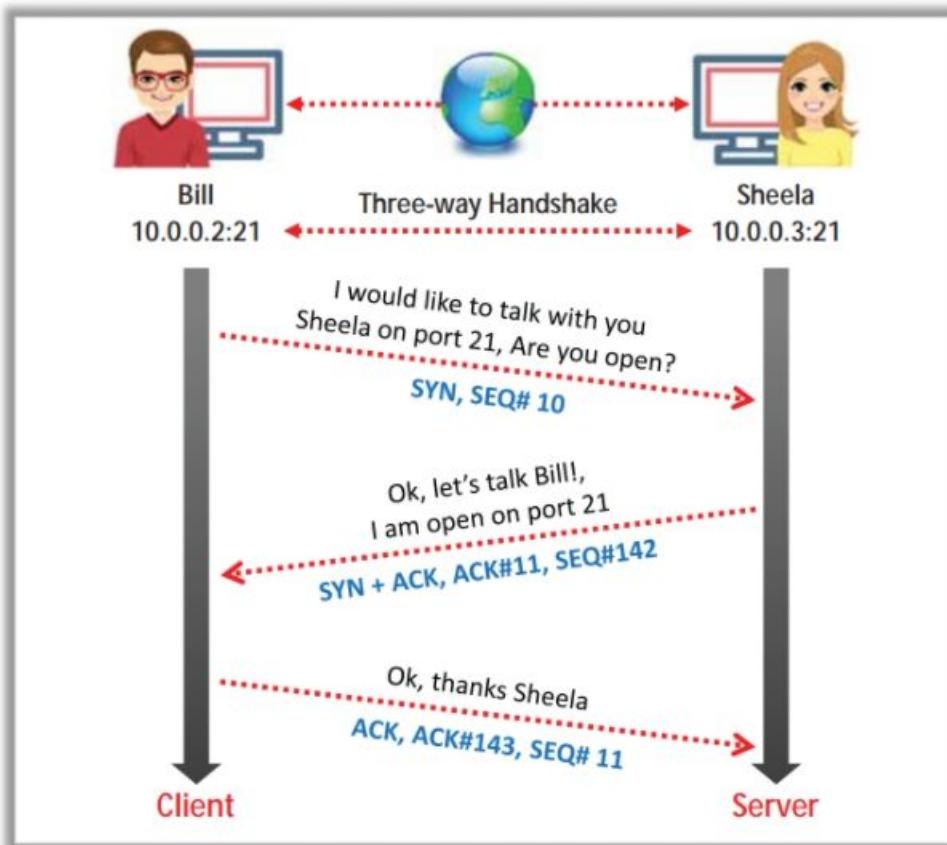


Standard TCP communications are controlled by flags in the TCP packet header

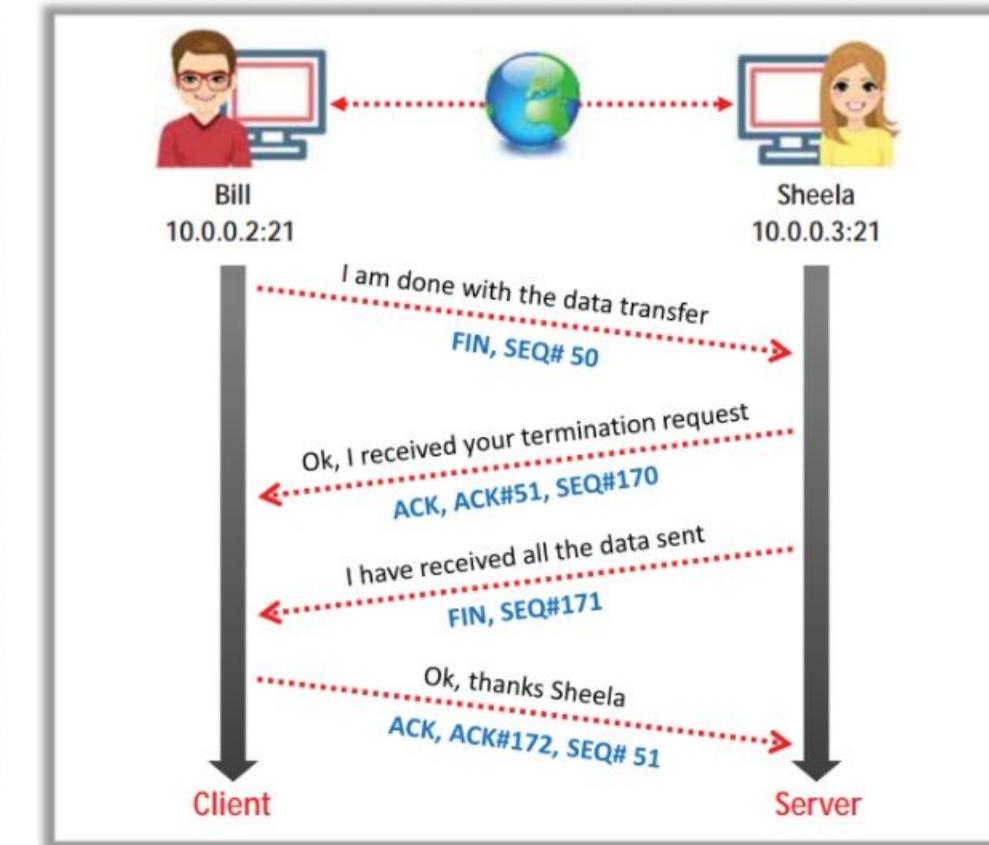
TCP/IP Communication

TCP Session Establishment

(Three-way Handshake)



TCP Session Termination



Module Flow



1

Network Scanning Concepts

2

Scanning Tools

3

Host Discovery

4

Port and Service Discovery

5

**OS Discovery (Banner Grabbing/
OS Fingerprinting)**

6

Scanning Beyond IDS and Firewall

7

Draw Network Diagrams

Scanning Tools: Nmap

Network administrators can use Nmap for **inventorying a network**, managing service upgrade schedules, and monitoring host or service uptime

Attackers use Nmap to extract information such as **live hosts on the network, open ports, services** (application name and version), **types of packet filters/firewalls**, as well as **operating systems and versions used**



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile: Intense scan, all TCP ports Scan Cancel

Command: **nmap -p 1-65535 -T4 -A -v 10.10.10.10**

Hosts Services Nmap Output Ports / Hosts OS Host

```
nmap -p 1-65535 -T4 -A -v 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-06-07
13:04   Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating NSE at 13:04
Completed NSE at 13:04, 0.00s elapsed
Initiating ARP Ping Scan at 13:04
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 13:04, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.02s elapsed
Initiating SYN Stealth Scan at 13:04
Scanning 10.10.10.10 [65535 ports]
Discovered open port 135/tcp on 10.10.10.10
Discovered open port 445/tcp on 10.10.10.10
Discovered open port 139/tcp on 10.10.10.10
Discovered open port 49667/tcp on 10.10.10.10
Discovered open port 5040/tcp on 10.10.10.10
Discovered open port 5357/tcp on 10.10.10.10
Discovered open port 49673/tcp on 10.10.10.10
SYN Stealth Scan Timing: About 47.95% done; ETC: 13:05 (0:00:34 remaining)
Discovered open port 49666/tcp on 10.10.10.10
Discovered open port 49665/tcp on 10.10.10.10
Discovered open port 49664/tcp on 10.10.10.10
Discovered open port 49668/tcp on 10.10.10.10
Discovered open port 49669/tcp on 10.10.10.10
Completed SYN Stealth Scan at 13:05, 65.69s elapsed (65535 total ports)
```

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile: Intense scan, all TCP ports Scan Cancel

Command: **nmap -p 1-65535 -T4 -A -v 10.10.10.10**

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 10 Enterprise
17763	microsft-ds	(workgroup: WORKGROUP)	
5040/tcp	open	unknown	
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
		_http-server-header:	Microsoft-HTTPAPI/2.0
		_http-title:	Service Unavailable
49664/tcp	open	msrpc	Microsoft Windows RPC
49665/tcp	open	msrpc	Microsoft Windows RPC
49666/tcp	open	msrpc	Microsoft Windows RPC
49667/tcp	open	msrpc	Microsoft Windows RPC
49668/tcp	open	msrpc	Microsoft Windows RPC
49669/tcp	open	msrpc	Microsoft Windows RPC
49673/tcp	open	msrpc	Microsoft Windows RPC
		MAC Address:	00:0C:29:79:02:B9 (VMware)
		Aggressive OS guesses:	Microsoft Windows Longhorn (94%), Microsoft Windows 10 1703 (92%), Microsoft Windows 10 1511 (91%), Microsoft Windows Server 2008 SP2 (91%), Microsoft Windows 8 (91%), Microsoft Windows 10

Filter Hosts

Scanning Tools: Hping2/Hping3



- 1 Command line **network scanning** and **packet crafting** tool for the TCP/IP protocol
- 2 It can be used for **network security auditing**, **firewall testing**, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc.

ICMP Scanning

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
# hping3 -1 10.10.10.10
HPING 10.10.10.10 (eth0 10.10.10.10): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.10.10.10 ttl=128 id=46777 icmp_seq=0 rtt=4.9 ms
len=46 ip=10.10.10.10 ttl=128 id=46778 icmp_seq=1 rtt=4.2 ms
len=46 ip=10.10.10.10 ttl=128 id=46779 icmp_seq=2 rtt=3.3 ms
len=46 ip=10.10.10.10 ttl=128 id=46780 icmp_seq=3 rtt=3.1 ms
len=46 ip=10.10.10.10 ttl=128 id=46781 icmp_seq=4 rtt=2.2 ms
len=46 ip=10.10.10.10 ttl=128 id=46782 icmp_seq=5 rtt=9.1 ms
len=46 ip=10.10.10.10 ttl=128 id=46783 icmp_seq=6 rtt=8.1 ms
len=46 ip=10.10.10.10 ttl=128 id=46784 icmp_seq=7 rtt=8.0 ms
len=46 ip=10.10.10.10 ttl=128 id=46785 icmp_seq=8 rtt=4.1 ms
^C
--- 10.10.10.10 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 2.2/5.2/9.1 ms
[root@parrot] ~
```

ACK Scanning on port 80

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
# hping3 -A 10.10.10.10 -p 80
HPING 10.10.10.10 (eth0 10.10.10.10): A set, 40 headers + 0 data bytes
len=46 ip=10.10.10.10 ttl=128 DF id=46786 sport=80 flags=R seq=0 win=0 rtt=7.9 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46787 sport=80 flags=R seq=1 win=0 rtt=5.9 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46788 sport=80 flags=R seq=2 win=0 rtt=7.7 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46789 sport=80 flags=R seq=3 win=0 rtt=5.0 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46790 sport=80 flags=R seq=4 win=0 rtt=3.9 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46791 sport=80 flags=R seq=5 win=0 rtt=3.0 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46792 sport=80 flags=R seq=6 win=0 rtt=2.2 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46793 sport=80 flags=R seq=7 win=0 rtt=2.0 ms
len=46 ip=10.10.10.10 ttl=128 DF id=46794 sport=80 flags=R seq=8 win=0 rtt=8.4 ms
^C
--- 10.10.10.10 hping statistic ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 2.0/5.1/8.4 ms
[root@parrot] ~
```

Scanning Tools

Metasploit

Metasploit is an open-source project that provides the infrastructure, content, and tools to **perform penetration tests** and **extensive security auditing**

```

Parrot Terminal
File Edit View Search Terminal Help

[+] metasploit v5.0.18-dev
+ --=[ 1878 exploits - 1062 auxiliary - 328 post
+ --=[ 546 payloads - 44 encoders - 10 nops
+ --=[ 2 evasion

msf5 > db status
[*] Connected to msf. Connection type: postgresql.

msf5 > search portscan

Matching Modules
=====
#  Name
1 auxiliary/scanner/http/wordpress_pingback_access
2 auxiliary/scanner/natpmp/natpmp_portscan
3 auxiliary/scanner/portscan/ack
4 auxiliary/scanner/portscan/ftpbounce
5 auxiliary/scanner/portscan/syn
6 auxiliary/scanner/portscan/tcp
7 auxiliary/scanner/portscan/xmas
8 auxiliary/scanner/sap/sap_router_portscanner

Disclosure Date Rank Check Description
normal Yes Wordpress Pingback Locator
normal Yes NAT-PMP External Port Scanner
normal Yes TCP ACK Firewall Scanner
normal Yes FTP Bounce Port Scanner
normal Yes TCP SYN Port Scanner
normal Yes TCP Port Scanner
normal Yes TCP "XMas" Port Scanner
normal No SAPRouter Port Scanner

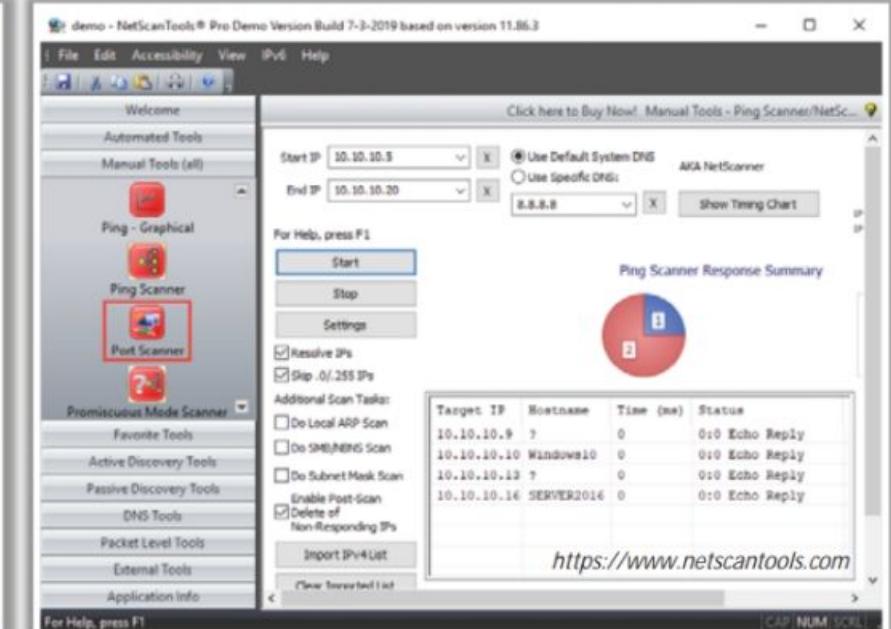
msf5 >

```

<https://www.metasploit.com>

NetScanTools Pro

NetScanTools Pro assists attackers in automatically or manually listing **IPv4/IPv6 addresses, hostnames, domain names, and URLs**



Other Scanning Tools:

Unicornscan
<https://sourceforge.net>

SolarWinds Port Scanner
<https://www.solarwinds.com>

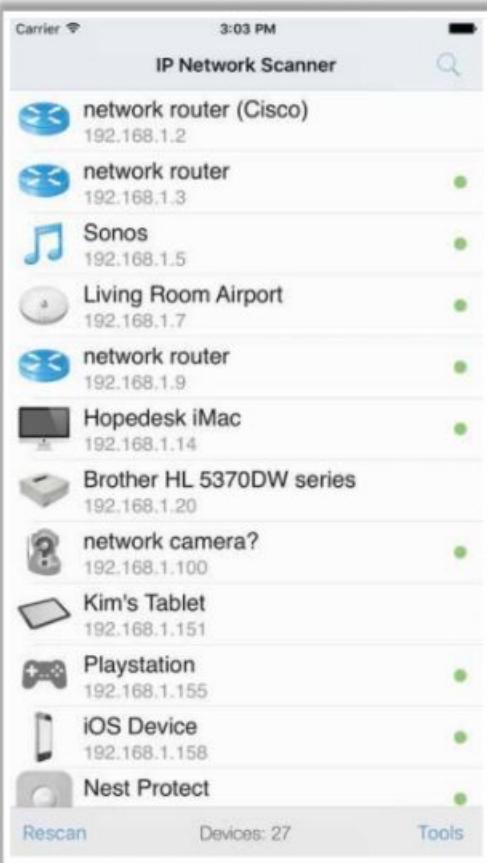
PRTG Network Monitor
<https://www.paessler.com>

OmniPeek Network Protocol Analyzer
<https://www.hotspotshield.com>

Scanning Tools for Mobile



IP Scanner



<https://10base-t.com>

Fing



<https://www.fing.io>

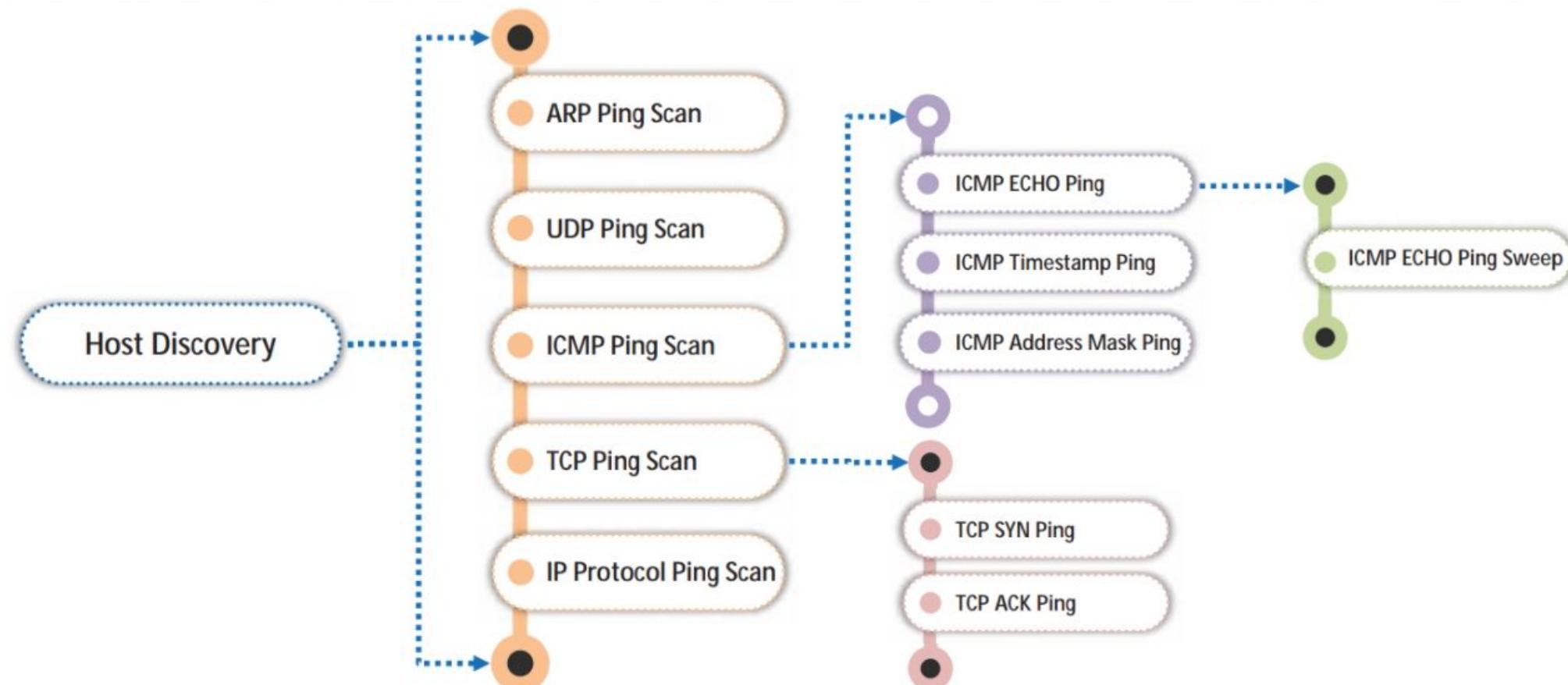
Network Scanner



<https://play.google.com>

Host Discovery Techniques

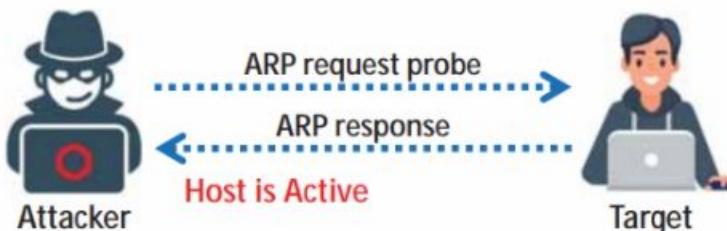
- Host discovery techniques are used to **identify the active/live systems** in the network



ARP Ping Scan and UDP Ping Scan

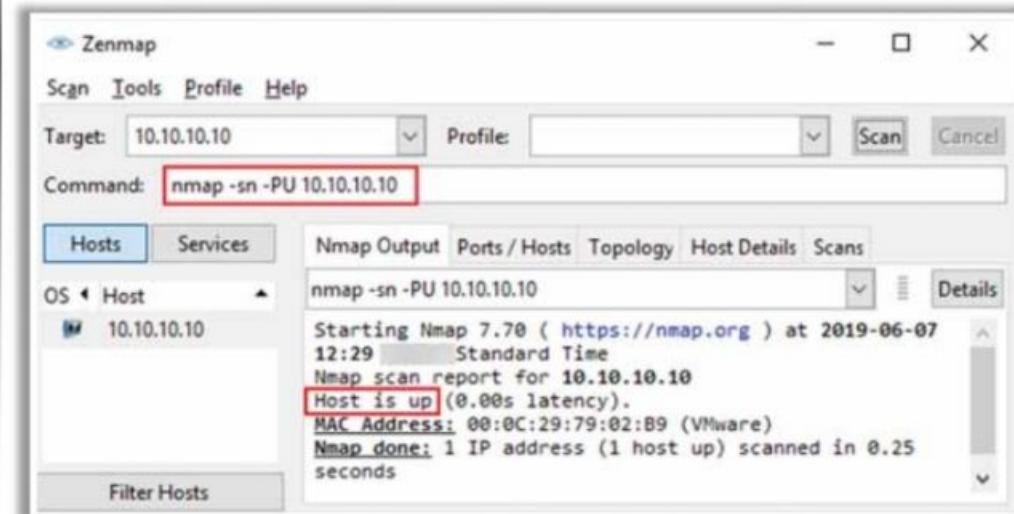
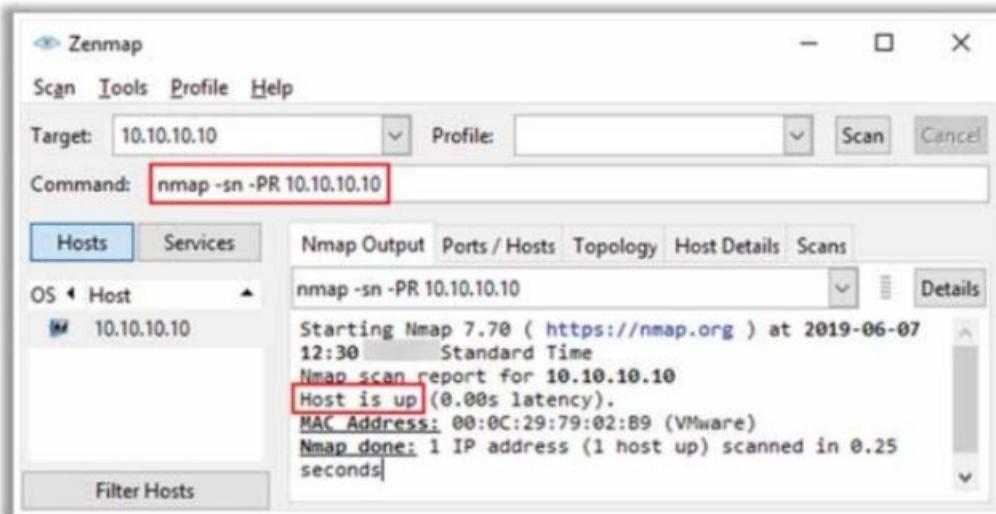
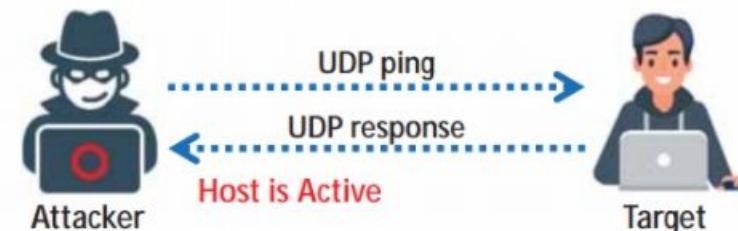
ARP Ping Scan

- Attackers send **ARP request probes** to target hosts, and an **ARP response** indicates that the **host is active**



UDP Ping Scan

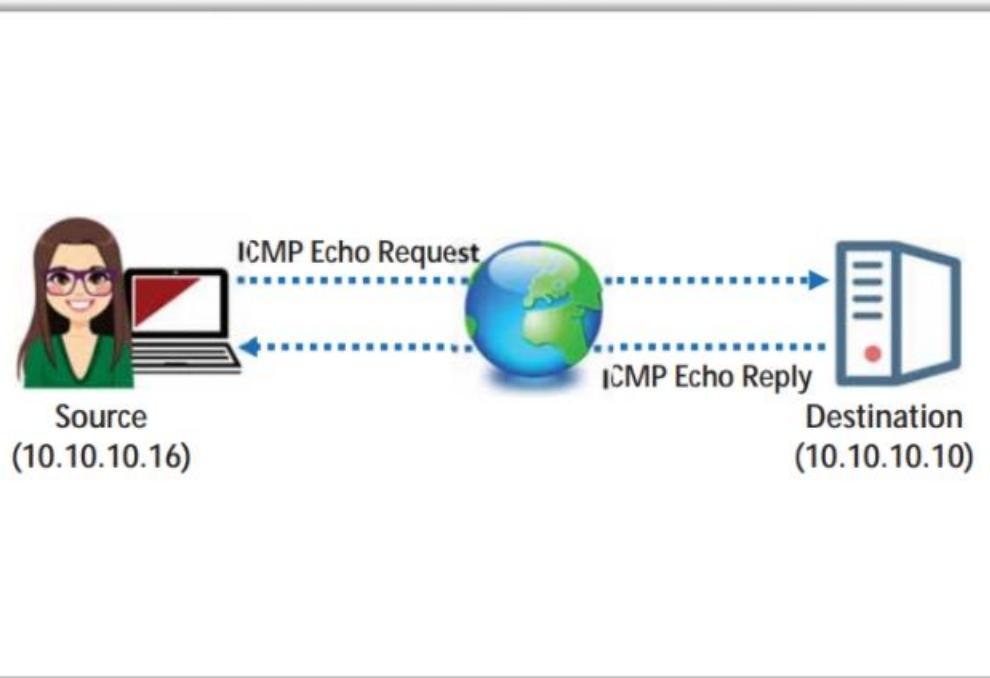
- Attackers send **UDP packets** to target hosts, and a **UDP response** indicates that the **host is active**



ICMP ECHO Ping Scan



- ICMP ECHO ping scans involve sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply
- This scan is useful for **locating active devices** or determining if the **ICMP is passing through a firewall**



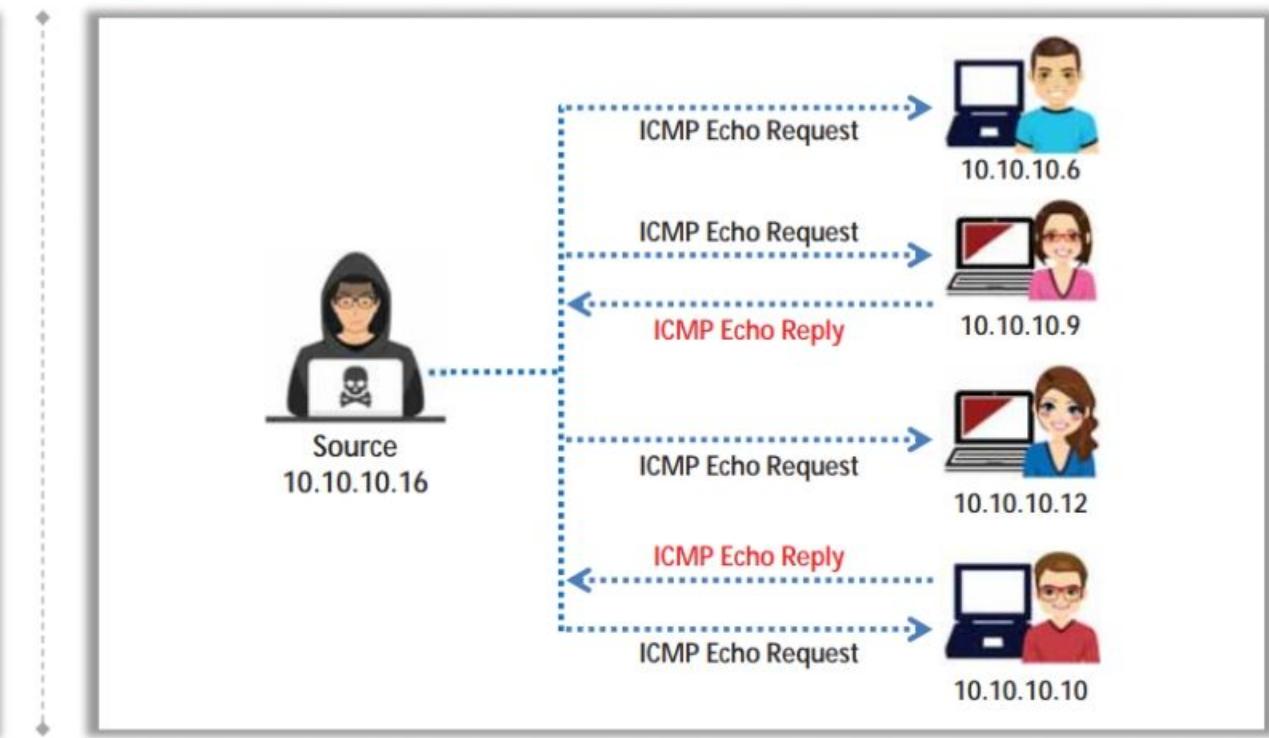
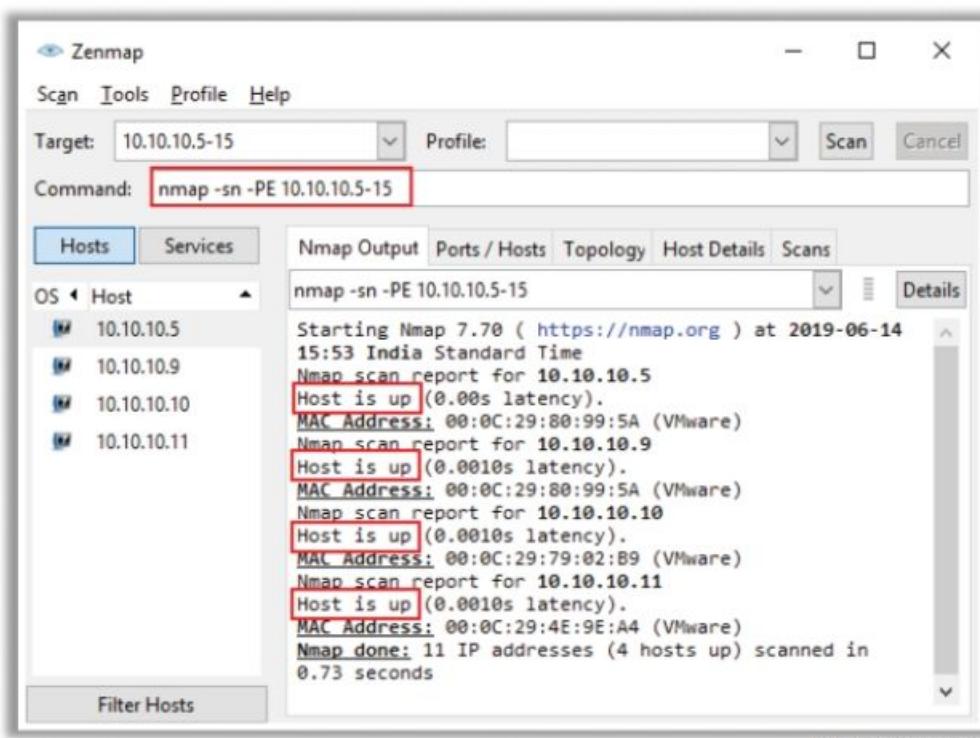
ICMP Echo ping scan output using Zenmap

The screenshot shows the Zenmap application window. The 'Targets' field contains '10.10.10.10'. The 'Command' field shows 'nmap -sn -PE 10.10.10.10'. The 'Hosts' tab is selected, listing '10.10.10.10' as 'Host is up (0.015s latency)'. The 'Nmap Output' tab displays the scan results:
Starting Nmap 7.70 (https://nmap.org) at 2019-06-07
12:33 Standard Time
Nmap scan report for 10.10.10.10
Host is up (0.015s latency).
MAC Address: 00:0C:29:79:02:B9 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

<https://nmap.org>

ICMP ECHO Ping Sweep

- Ping sweep is used to determine the **live hosts from a range of IP addresses** by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply
- Attackers calculate subnet masks by using a **Subnet Mask Calculator** to identify the number of hosts that are present in the subnet
- Attackers subsequently use a ping sweep to create an **inventory of live systems** in the subnet



Ping Sweep Tools



Angry IP Scanner

Angry IP Scanner pings each IP address to check if any of these addresses are live. Then, it optionally resolves hostnames, determines the MAC address, scans ports, etc.

Ping Sweep Tools

- SolarWinds Engineer's Toolset (<https://www.solarwinds.com>)
- NetScanTools Pro (<https://www.netscantools.com>)
- Colasoft Ping Tool (<https://www.colasoft.com>)
- Visual Ping Tester (<http://www.pingtester.net>)
- OpUtils (<https://www.manageengine.com>)

IP Range - Angry IP Scanner					
Scan Go to Commands Favorites Tools Help					
IP Range:		10.10.10.0	to	10.10.10.255	IP Range
Hostname:		Server2016	IP↑	Netmask	Start
IP	Ping	Hostname	Ports [1000+]		
10.10.10.10	0 ms	DESKTOP-SV6DCV1	1,7,9,13,17,19,21-23,25,42,53,80-83,91,98,...		
10.10.10.12	0 ms	WIN-OJAQ7QJ8PAI	53,80,88,135,139,389,445,464,593,636		
10.10.10.16	0 ms	Server2016	80,135,139,445		
10.10.10.8	0 ms	VICTIM-8	135,139,445		
10.10.10.9	0 ms	jason-Virtual-Machine	80		
10.10.10.11	0 ms	[n/a]	80		

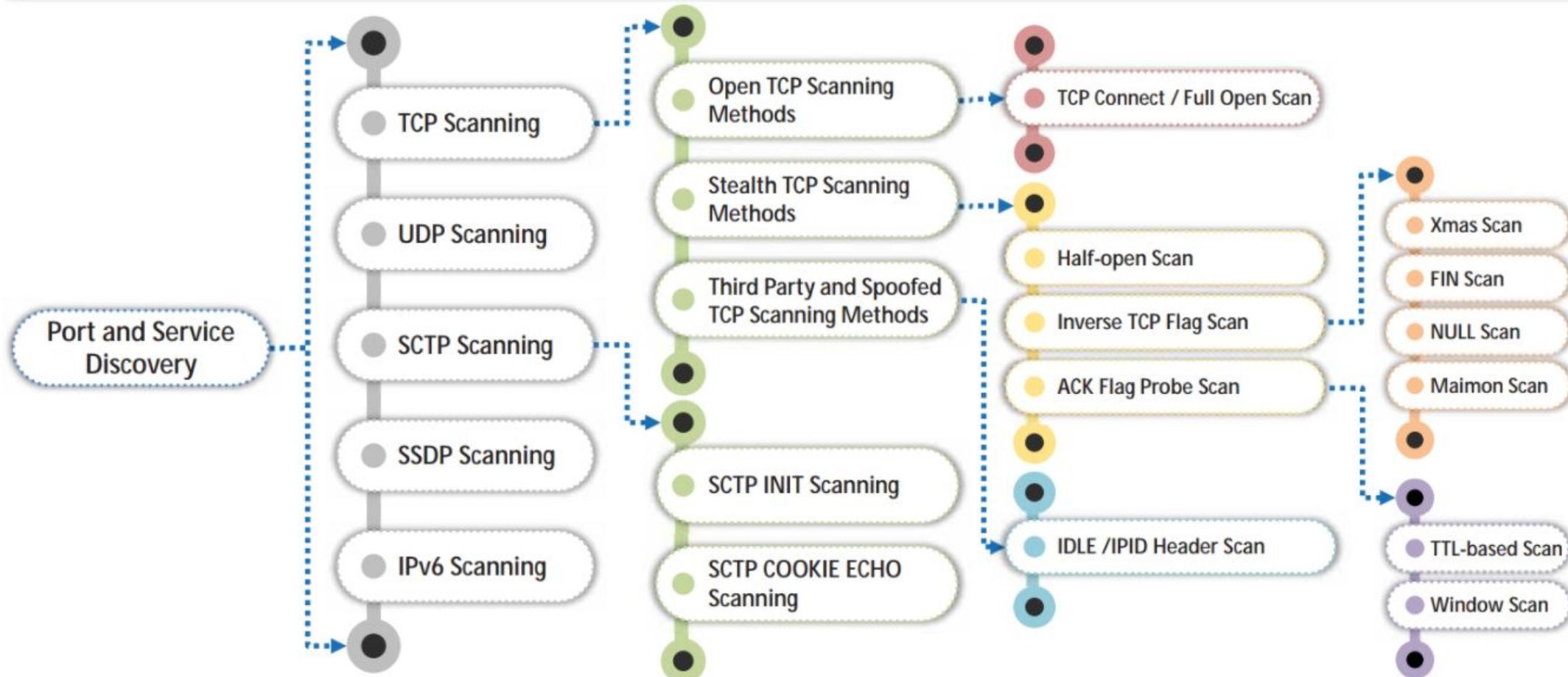
Ping Sweep Countermeasures



- 1** Configure firewalls to detect and prevent ping sweep attempts instantaneously
- 2** Use intrusion detection systems and intrusion prevention systems like Snort to detect and prevent ping sweep attempts
- 3** Carefully evaluate the type of ICMP traffic flowing through enterprise networks
- 4** Cut off connections with any host that performs more than 10 ICMP ECHO requests

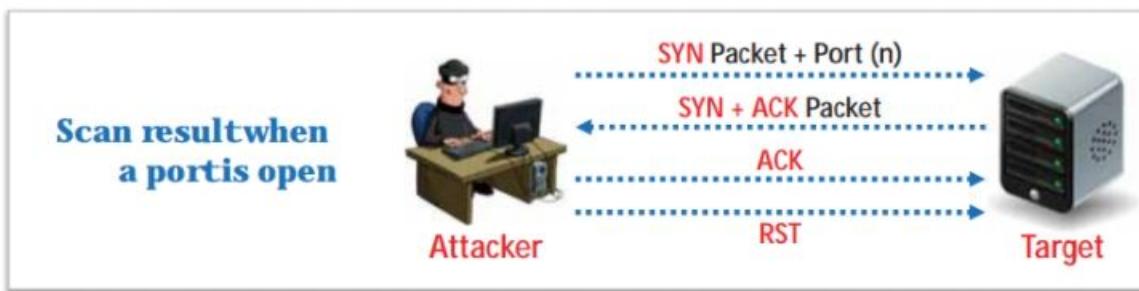
Port Scanning Techniques

- The port scanning techniques are **categorized according to the type of protocol** used for communication



TCP Connect/Full Open Scan

- The TCP Connect scan detects when a port is open after completing the **three-way handshake**
- TCP Connect scan **establishes a full connection** and then closes the connection by sending an **RST** packet
- It does not require **superuser privileges**



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile: Scan Cancel

Command: nmap -sT -v 10.10.10.10

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.10 Details

nmap -sT -v 10.10.10.10

Starting Nmap 7.80 (https://nmap.org) at 2019-10-23 13:04

Standard Time

Initiating ARP Ping Scan at 13:04

Scanning 10.10.10.10 [1 port]

Completed ARP Ping Scan at 13:04, 0.03s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:04

Completed Parallel DNS resolution of 1 host. at 13:04, 0.03s elapsed

Initiating Connect Scan at 13:04

Scanning 10.10.10.10 [1000 ports]

Discovered open port 135/tcp on 10.10.10.10

Discovered open port 139/tcp on 10.10.10.10

Discovered open port 445/tcp on 10.10.10.10

Discovered open port 3389/tcp on 10.10.10.10

Discovered open port 80/tcp on 10.10.10.10

Discovered open port 5357/tcp on 10.10.10.10

Completed Connect Scan at 13:05, 45.44s elapsed (1000 total ports)

Nmap scan report for 10.10.10.10

Host is up (0.00s latency).

Not shown: 994 filtered ports

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	microsoft-ds
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5357/tcp	open	wsdapi

MAC Address: 00:0C:29:80:F4:93 (VMware)

Read data files from: C:\Program Files (x86)\Nmap

Nmap done: 1 IP address (1 host up) scanned in 45.63 seconds

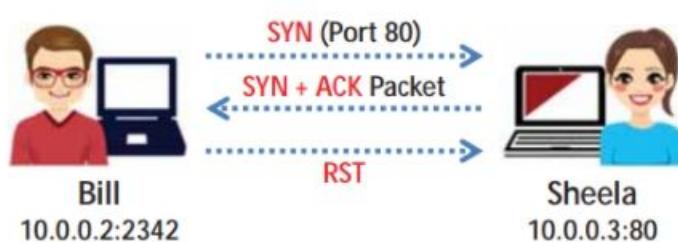
Raw packets sent: 1 (288) | Rcvd: 1 (288)

Filter Hosts

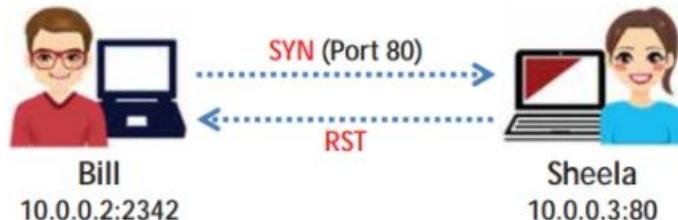
Stealth Scan (Half-open Scan)

- Stealth scanning involves abruptly resetting the TCP connection between the client and server before the completion of **three-way handshake signals**, thus leaving the connection half-open
- Attackers use stealth scanning techniques to **bypass firewall rules** as well as **logging mechanisms**, and hide themselves under the appearance of regular network traffic

Scan result when a port is open



Scan result when a port is closed



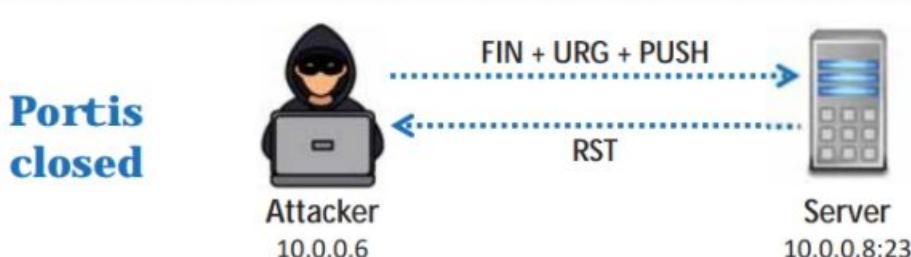
Zenmap interface showing the results of a nmap -sS -v scan on host 10.10.10.10. The output shows various open ports and service details.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-23 13:00 [Standard Time]
Initiating ARP Ping Scan at 13:00
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 13:00, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:00
Completed Parallel DNS resolution of 1 host. at 13:00, 0.02s elapsed
Initiating SYN Stealth Scan at 13:00
Scanning 10.10.10.10 [1000 ports]
Discovered open port 445/tcp on 10.10.10.10
Discovered open port 80/tcp on 10.10.10.10
Discovered open port 139/tcp on 10.10.10.10
Discovered open port 135/tcp on 10.10.10.10
Discovered open port 3389/tcp on 10.10.10.10
Discovered open port 5357/tcp on 10.10.10.10
Completed SYN Stealth Scan at 13:00, 4.95s elapsed (1000 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 00:0C:29:00:F4:93 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.14 seconds
Raw packets sent: 1998 (87.896KB) | Rcvd: 10 (4248)|
```

Xmas Scan

- Using the Xmas scan, attackers send a TCP frame to a remote device with **FIN**, **URG**, and **PUSH** flags set
- FIN scanning works only with OSes that use an **RFC 793-based** TCP/IP implementation
- The Xmas scan will not work against any current version of **Microsoft Windows**



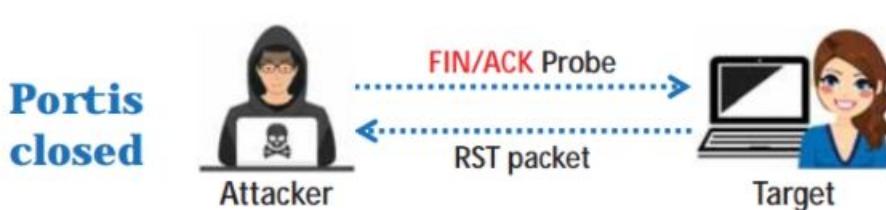
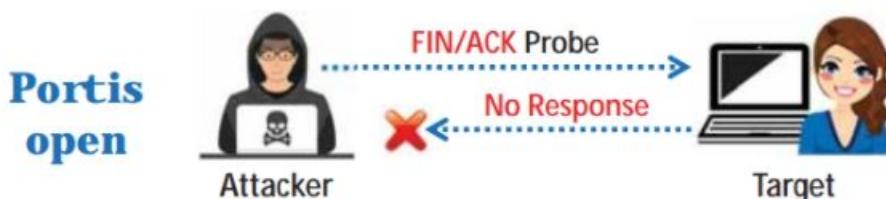
Xmas scan output using Zenmap

```
Zenmap
Scan Tools Profile Help
Target: 10.10.10.10 Profile: Scan Cancel
Command: nmap -sX -v 10.10.10.10
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 10.10.10.10
nmap -sX -v 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-23
12:29 Standard Time
Initiating ARP Ping Scan at 12:29
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 12:29, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:29
Completed Parallel DNS resolution of 1 host. at 12:29,
0.03s elapsed
Initiating XMAS Scan at 12:29
Scanning 10.10.10.10 [1000 ports]
Completed XMAS Scan at 12:29, 23.66s elapsed (1000 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.10 are open|filtered
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.92
seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 5
(2368)|
```

TCP Maimon Scan

- Attackers send **FIN/ACK probes**, and if there is no response, then the port is **Open|Filtered**, but if an **RST packet** is sent in response, then the port is **closed**



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile: Scan Cancel

Command: nmap -sM -v 10.10.10.10

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sM -v 10.10.10.10

```

Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-23
12:32 ██████████ Standard Time
Initiating ARP Ping Scan at 12:32
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 12:32, 0.05s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 12:32
Completed Parallel DNS resolution of 1 host. at 12:32,
0.03s elapsed
Initiating Maimon Scan at 12:32
Scanning 10.10.10.10 [1000 ports]
Completed Maimon Scan at 12:32, 23.47s elapsed (1000
total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
All 1000 scanned ports on 10.10.10.10 are open|filtered
MAC Address: 00:0C:29:B0:F4:93 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.77
seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 5
(236B)

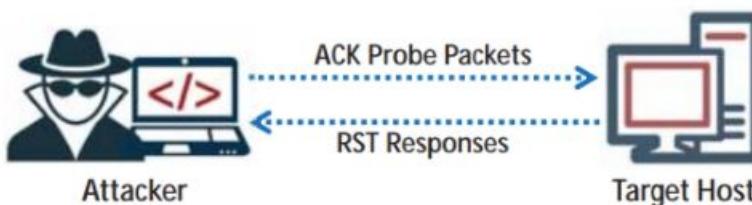
```

Filter Hosts

ACK Flag Probe Scan

- Attackers send **TCP probe packets set with an ACK flag** to a remote device, and then **analyze the header information** (TTL and WINDOW field) of received RST packets to determine if the **port is open or closed**

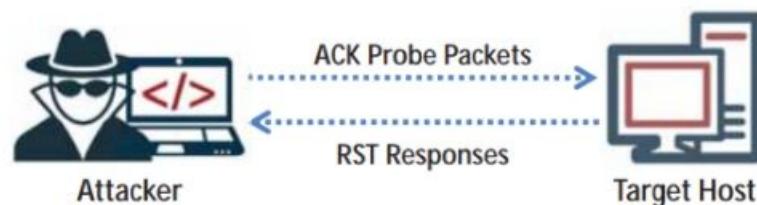
TTL-based ACK Flag Probe scanning



```
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  
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

If the **TTL value of the RST packet** on a particular port is less than the boundary value of **64**, then that **port is open**

Window-based ACK Flag Probe scanning

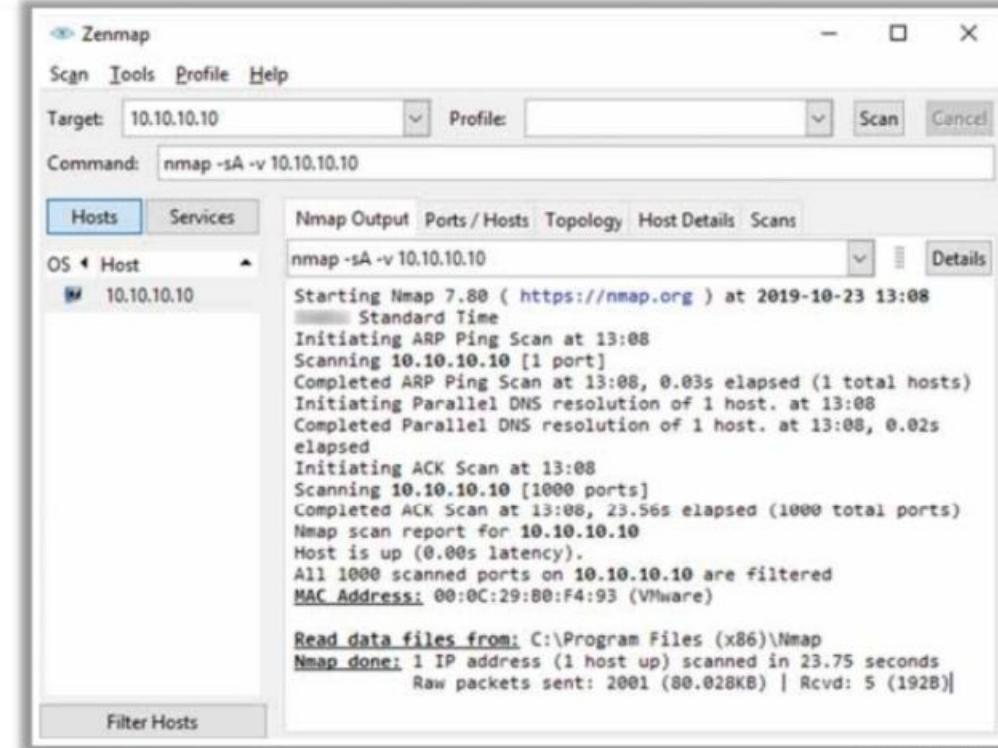
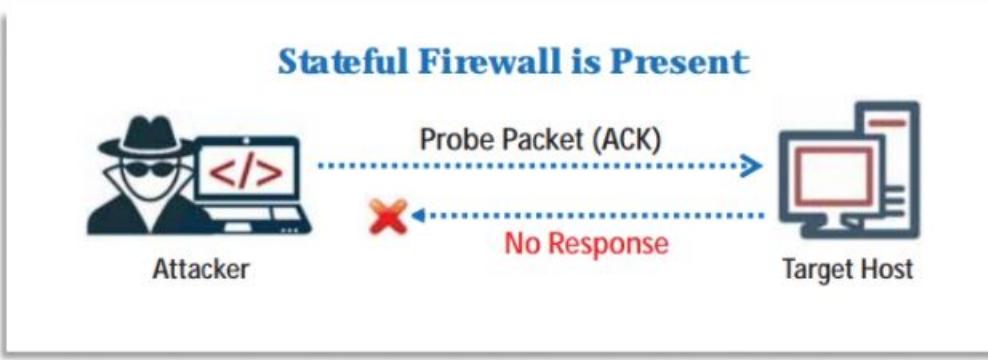


```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0  
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0  
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512  
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

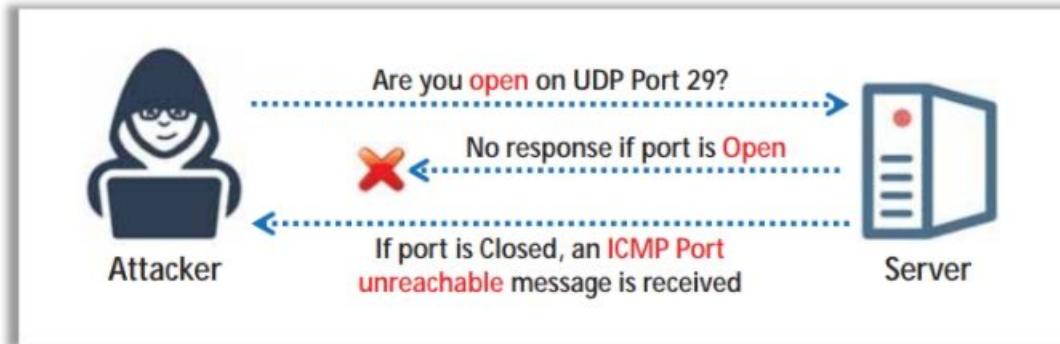
If the **window value of the RST packet** on a particular port has a **non-zero value**, then that **port is open**

ACK Flag Probe Scan (Cont'd)

- ACK flag probe scanning can also be used to **check the filtering system of a target**
- Attackers send an **ACK probe packet** with a random sequence number, and no response implies that the **port is filtered** (stateful firewall is present), whereas an RST response means that the **port is not filtered**



UDP Scanning



UDP Port Open

- There is no **three-way TCP handshake** for UDP scanning
- The system does not respond with a message when the **port is open**

UDP Port Closed

- If a UDP packet is sent to a closed port, the system will respond with an **ICMP port unreachable message**
- Spywares, Trojan horses**, and other malicious applications use UDP ports

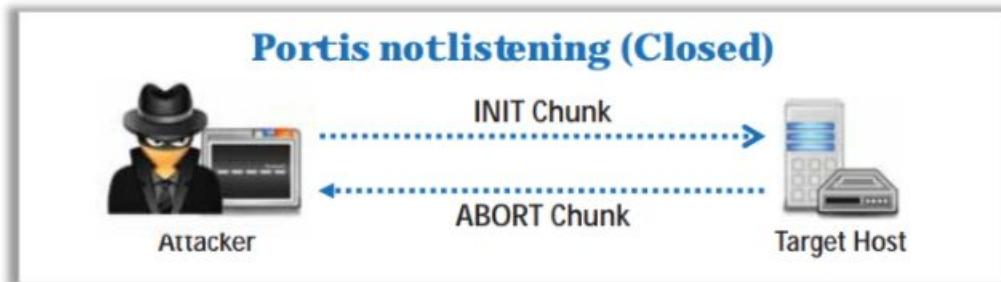
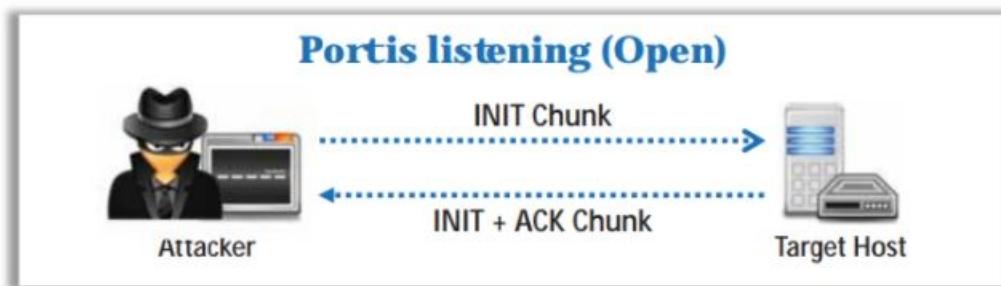
Zenmap interface showing a UDP scan on target 10.10.10.10. The command used is nmap -sU -v 10.10.10.10. The output shows the scan starting at 2019-06-07 11:07, performing an ARP ping scan, parallel DNS resolution, and a UDP scan. It discovers an open port 137/udp for netbios-ns service on the host.

```
Starting Nmap 7.00 ( https://nmap.org ) at 2019-06-07 11:07 Standard Time
Initiating ARP Ping Scan at 11:07
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 11:07, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.01s elapsed
Initiating UDP Scan at 11:07
Scanning 10.10.10.10 [1000 ports]
Discovered open port 137/udp on 10.10.10.10
Completed UDP Scan at 11:07, 7.91s elapsed (1000 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:0C:29:79:02:B9 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
Raw packets sent: 2002 (57.960KB) | Rcvd: 5 (685B)
```

SCTP INIT Scanning

- Attackers send an **INIT chunk** to the target host, and an **INIT+ACK chunk** response implies that the **port is open**, whereas an **ABORT Chunk** response means that the **port is closed**
- No response from the target, or a response of an **ICMP unreachable exception** indicates that the port is a **Filtered port**



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile:

Command: nmap -sY -v 10.10.10.10

Hosts Services

OS Host 10.10.10.10

nmap -sY -v 10.10.10.10

Starting Nmap 7.70 (https://nmap.org) at 2019-06-07
11:11 Standard Time
Initiating ARP Ping Scan at 11:11
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 11:11, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:11
Completed Parallel DNS resolution of 1 host. at 11:11,
0.02s elapsed
Initiating SCTP INIT Scan at 11:11
Scanning 10.10.10.10 [52 ports]
Completed SCTP INIT Scan at 11:11, 1.97s elapsed (52 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
All 52 scanned ports on 10.10.10.10 are filtered
MAC Address: 00:0C:29:79:02:B9 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
Raw packets sent: 103 (5.332KB) | Rcvd: 4 (268B)

Filter Hosts

SCTP COOKIE ECHO Scanning

- Attackers send a **COOKIE ECHO chunk** to the target host, and **no response** implies that the **port is open**, whereas an **ABORT Chunk** response means that the **port is closed**
- It is **not blocked** by non-stateful firewall rulesets
- Only a **good IDS** will be able to **detect SCTP COOKIE ECHO** chunk



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile:

Command: nmap -sZ -v 10.10.10.10

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.10

nmap -sZ -v 10.10.10.10

Starting Nmap 7.00 (https://nmap.org) at 2019-06-07
11:12 Standard Time
Initiating ARP Ping Scan at 11:12
Scanning 10.10.10.10 [1 port]
Completed ARP Ping Scan at 11:12, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:12
Completed Parallel DNS resolution of 1 host. at 11:12, 0.02s elapsed
Initiating SCTP COOKIE-ECHO Scan at 11:12
Scanning 10.10.10.10 [52 ports]
Completed SCTP COOKIE-ECHO Scan at 11:12, 2.23s elapsed (52 total ports)
Nmap scan report for 10.10.10.10
Host is up (0.00s latency).
Not shown: 50 open|filtered ports
PORT STATE SERVICE
2225/sctp filtered rcp-itu
4739/sctp filtered ipfix
MAC Address: 00:0C:29:79:02:B9 (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds
Raw packets sent: 104 (4.148KB) | Rcvd: 3 (1648)

Filter Hosts

SSDP and List Scanning



SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that **works in conjunction with the UPnP** to detect plug and play devices
- Vulnerabilities in UPnP may allow attackers to launch **Buffer overflow** or **DoS attacks**
- Attacker may use the **UPnP SSDP M-SEARCH** information discovery tool to check if the machine is vulnerable to UPnP exploits or not

```
Parrot Terminal
File Edit View Search Terminal Help
msf5 > use auxiliary/scanner/upnp/ssdp_msearch
msf5 auxiliary(scanner/upnp/ssdp_msearch) > set RHOSTS 10.10.10.16
RHOSTS => 10.10.10.16
msf5 auxiliary(scanner/upnp/ssdp_msearch) > show options

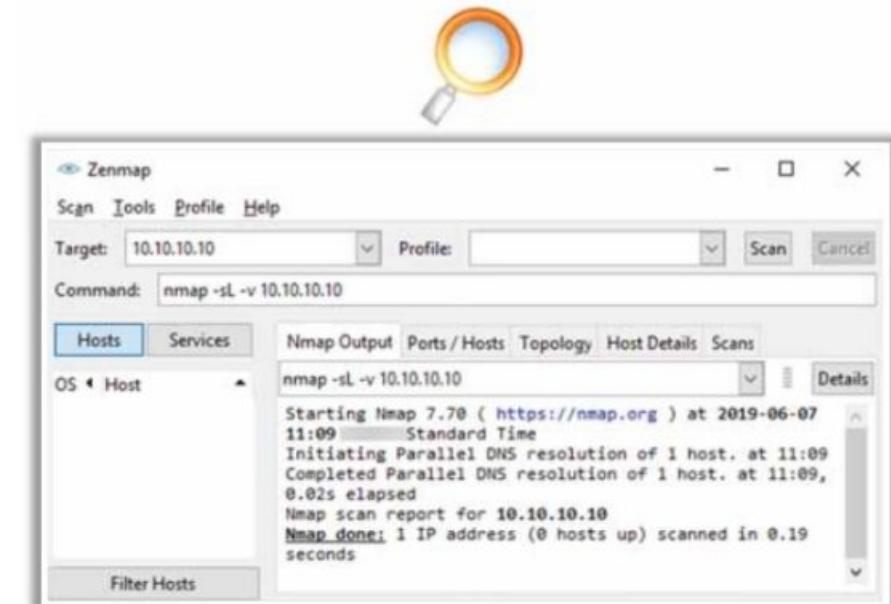
Module options (auxiliary/scanner/upnp/ssdp_msearch):
Name      Current Setting  Required  Description
----      -----          -----    -----
BATCHSIZE      256           yes       The number of hosts to probe in each set
REPORT_LOCATION  false         yes       This determines whether to report the UP
nP endpoint service advertised by SSDP
RHOSTS        10.10.10.16     yes       The target host(s), range CIDR identifie
r, or hosts file with syntax 'file:<path>'
REPORT        1900           yes       The target port (UPnP)
THREADS        10            yes       The number of concurrent threads

msf5 auxiliary(scanner/upnp/ssdp_msearch) > exploit

[*] Sending UPnP SSDP probes to 10.10.10.16->10.10.10.16 (1 hosts)
[*] No SSDP endpoints found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/upnp/ssdp_msearch) >
```

ListScanning

- This type of scan simply generates and prints a **list of IPs/Names** without actually pinging them
- A **reverse DNS resolution** is performed to identify the host names



<https://nmap.org>

Service Version Discovery

- Service version detection helps attackers to obtain information about running **services and their versions** on a target system
- Obtaining an accurate service version number allows attackers to **determine the vulnerability of target system to particular exploits**
- For example, when an attacker detects **SMBv1 protocol** as a running service on a target Windows-based machine, then the attacker can easily perform the **WannaCry ransomware attack**
- In Zenmap, the **-sV** option is used to detect service versions



Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile:

Command: nmap -sV 10.10.10.10

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 10.10.10.10

nmap -sV 10.10.10.10

Starting Nmap 7.70 (https://nmap.org) at 2019-06-10 17:44 Standard Time
Nmap scan report for 10.10.10.10
Host is up (0.0014s latency).
Not shown: 996 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

MAC Address: 00:0C:29:79:02:B9 (VMware)
Service Info: Host: DESKTOP-E3UJ5VL; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 13.88 seconds

<https://nmap.org>

Nmap Scan Time Reduction Techniques

💡 In Nmap, **performance** and **accuracy** can be achieved by reducing the scan timing

Scan Time Reduction Techniques

1 Omit Non-critical Tests

2 Optimize Timing Parameters

3 Separate and Optimize UDP Scans

4 Upgrade Nmap

5 Execute Concurrent Nmap Instances

6 Scan from a Favorable Network Location

7 Increase Available Bandwidth and CPU Time

Port Scanning Countermeasures



- 1 Configure **firewall** and **IDS rules** to detect and block probes
- 2 Run **port scanning tools** against hosts on the network to determine whether the firewall properly **detects port scanning activity**
- 3 Ensure that the mechanisms used for **routing** by routers and for **filtering** by firewalls **cannot be bypassed** using particular source ports or source-routing methods
- 4 Ensure that the **router**, **IDS**, and **firewall firmware** are updated to their latest releases/versions
- 5 Use a **custom rule set** to lock down the network and block **unwanted ports** at the firewall
- 6 Filter all **ICMP messages** (i.e., inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the **firewalls and routers**
- 7 Perform **TCP and UDP scanning** along with ICMP probes against your organization's IP address space to **check the network configuration and its available ports**
- 8 Ensure that **anti-scanning** and **anti-spoofing** rules are properly configured

Module Flow

1

Network Scanning Concepts

2

Scanning Tools

3

Host Discovery

4

Port and Service Discovery

5

**OS Discovery (Banner Grabbing/
OS Fingerprinting)**

6

Scanning Beyond IDS and Firewall

7

Draw Network Diagrams

OS Discovery/Banner Grabbing



- Banner grabbing or OS fingerprinting is the method used to **determine the operating system running on a remote target system**. There are two types of banner grabbing: active and passive
- Identifying the OS used on the target host allows an attacker to **figure out the vulnerabilities possessed by the system** and the exploits that might work on a system to further **carry out additional attacks**

Active BannerGrabbing

- **Specially crafted packets** are sent to the remote OS and the responses are noted
- The responses are then compared with a database to **determine the OS**
- Responses from different OSes vary due to differences in the **TCP/IP stack implementation**



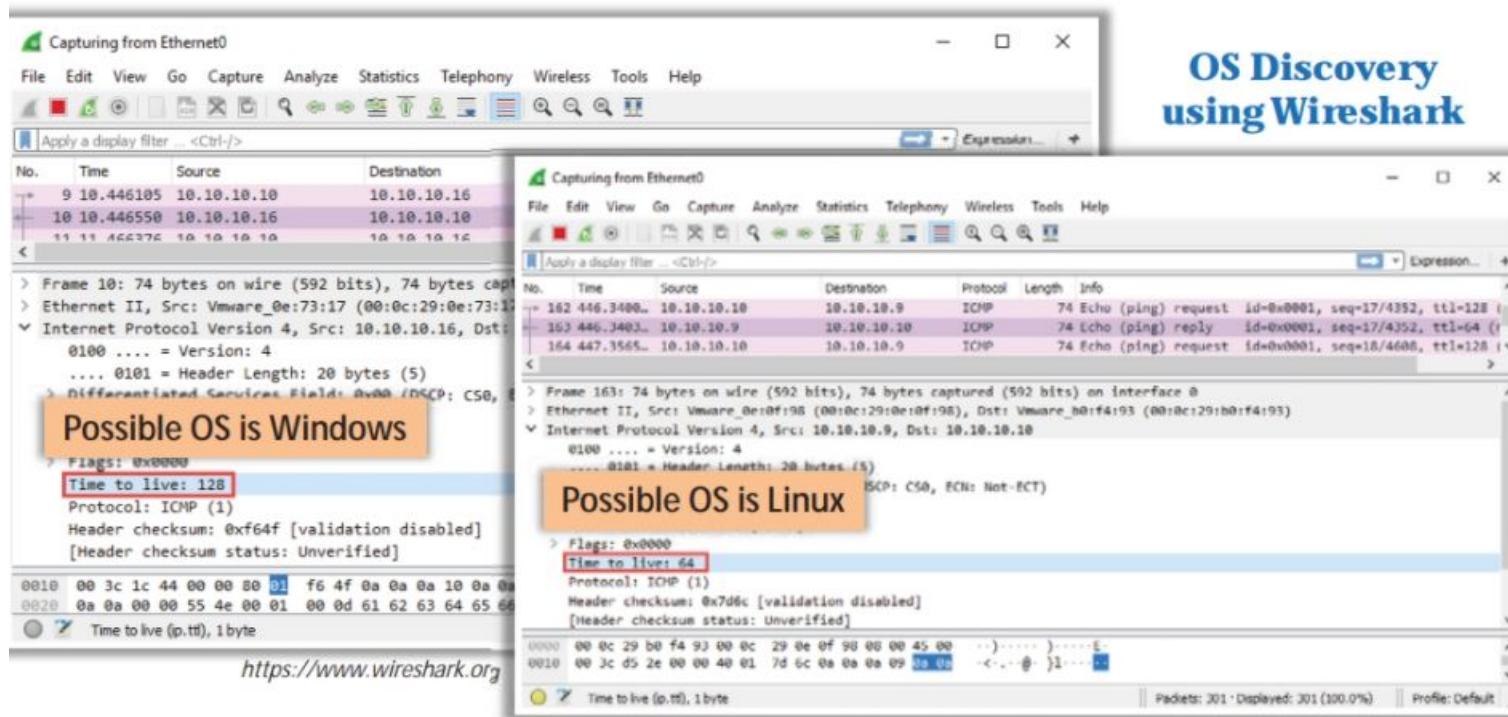
Passive BannerGrabbing

- **Banner grabbing from error messages**
Error messages provide information such as the type of server, type of OS, and SSL tool used by the target remote system.
- **Sniffing the network traffic**
Capturing and analyzing packets from the target enables an attacker to determine the OS used by the remote system.
- **Banner grabbing from page extensions**
Looking for an extension in the URL may assist in determining the application's version.
Example: .aspx => IIS server and Windows platform

Note: We will discuss passive banner grabbing in later modules.

How to Identify Target System OS

- Attackers can identify the OS running on the target machine by looking at the **Time To Live (TTL)** and **TCP window size** in the IP header of the first packet in a TCP session
- Sniff/capture the response** generated from the target machine using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields



Window size values for OS

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

OS Discovery using Nmap and Unicornscan



- In **Nmap**, the **-O** option is used to perform OS discovery, providing OS details of the target machine

Zenmap interface showing Nmap output for target 10.10.10.16. The OS detection section highlights "Microsoft Windows Server 2016 build 10586 - 14393".

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-10 07:23 EDT
Nmap scan report for 10.10.10.16
Host is up (0.00092s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:ED:C2:95 (VMware)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 1 hop

OS detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in
2.87 seconds
```

- In **Unicornscan**, the OS of the target machine can be identified by **observing the TTL values** in the acquired scan result

Parrot Terminal window showing the output of the command `#unicornscan 10.10.10.16 -I`. A box highlights the TTL values for several open ports, and a callout box states "Possible OS is Windows".

```
[root@parrot] ~
#unicornscan 10.10.10.16 -I
adding 10.10.10.16/32 mode 'TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,
65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-16
4,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-372,389,406,407,422,4
43-445,487,500,512-514,517,518,520,525,533,538,548,554,563,587,610-612,631-634,636,642,
653,655,657,666,706,750-752,765,779,808,873,901,923,941,946,992-995,1001,1023-1030,1080
,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1646,1649,1701,1
718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,243
0,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,
3542-3545,3632,3690,3801,4000,4400,4401,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,53
08,5354,5355,5422-5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838
,6666-6670,7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,1
0000,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2001
2,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,32668,32767-3
2780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,6134
8,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer t
han 8 Seconds
TCP open 10.10.10.16:2103 ttl 128
TCP open 10.10.10.16:80 ttl 128
TCP open 10.10.10.16:445 ttl 128
TCP open 10.10.10.16:139 ttl 128
TCP open 10.10.10.16:135 ttl 128
TCP open 10.10.10.16:3389 ttl 128
TCP open 10.10.10.16:88 ttl 128
```

Possible OS is Windows

OS Discovery using Nmap Script Engine

- Nmap script engine (NSE) can be used to automate a wide variety of networking tasks by allowing the users to write and share scripts
- Attackers use various scripts in the Nmap Script Engine to perform OS discovery on the target machine
- For example, in Nmap, **smb-os-discovery** is an inbuilt script that can be used for collecting OS information on the target machine through the SMB protocol
- In Zenmap, the **-sC** option or **--script** option is used to activate the NSE scripts

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.10.10.10
- Command:** nmap --script smb-os-discovery.nse 10.10.10.10
- Host:** 10.10.10.10
- Ports:** 135/tcp open msrpc, 139/tcp open netbios-ssn, 445/tcp open microsoft-ds, 5357/tcp open wsdapi
- MAC Address:** 00:0C:29:79:02:89 (VMware)
- Host script results:**
 - OS: Windows 10 Enterprise 17763 (Windows 10 Enterprise 6.3)
 - OS CPE: cpe:/o:microsoft:windows_10::-
 - Computer name: DESKTOP-E3UJ5VL
 - NetBIOS computer name: DESKTOP-E3UJ5VL\x00
 - Workgroup: WORKGROUP\x00
 - System time: 2019-06-10T18:14:19+05:30
- Nmap done:** 1 IP address (1 host up) scanned in 26.22 seconds

Anonymizers

- ❑ An anonymizer **removes** all identity information from the user's computer while the user surfs the Internet
- ❑ Anonymizers make activity on the Internet **untraceable**
- ❑ Anonymizers allow you to **bypass Internet** censors



Why use an Anonymizer?

- ❶ Privacy and anonymity
- ❷ Protection against online attacks
- ❸ Access restricted content
- ❹ Bypass IDS and Firewall rules

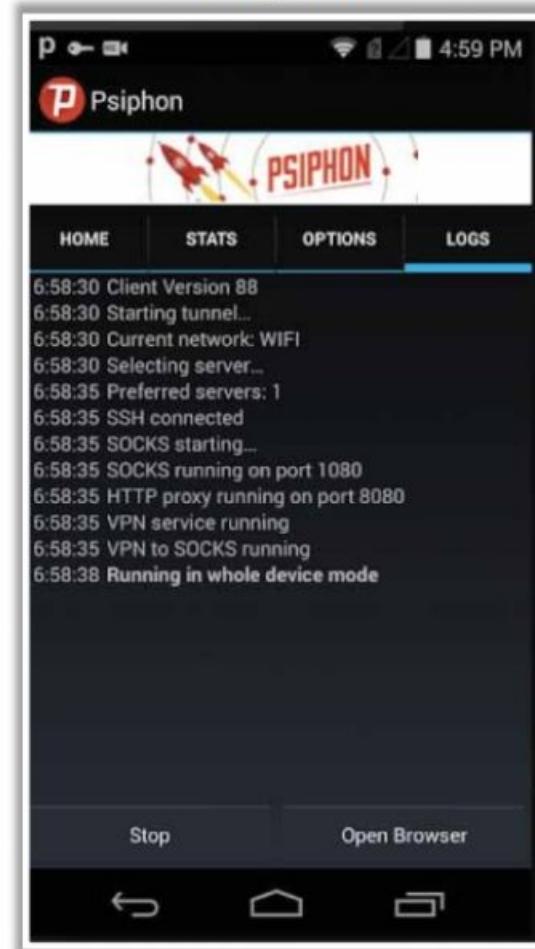


Anonymizers for Mobile

Orbot



Psiphon



OpenDoor



<https://guardianproject.info>

<https://psiphon.ca>

<https://www.apple.com>

Module Flow



1

Network Scanning Concepts

2

Scanning Tools

3

Host Discovery

4

Port and Service Discovery

5

**OS Discovery (Banner Grabbing/
OS Fingerprinting)**

6

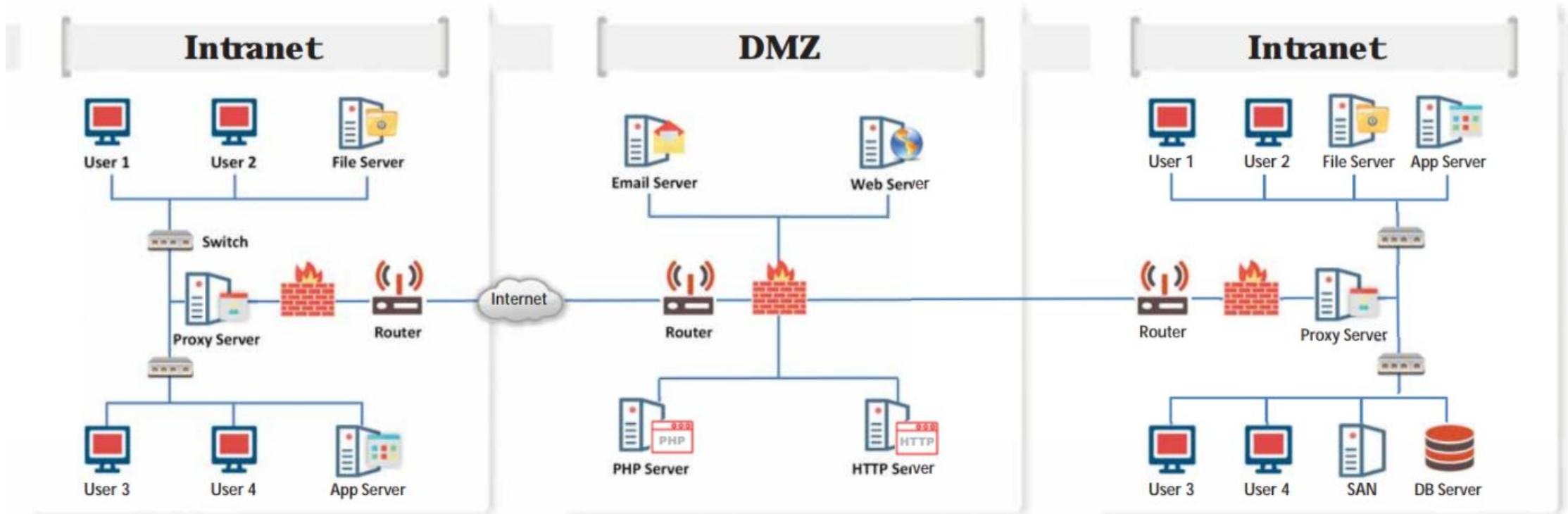
Scanning Beyond IDS and Firewall

7

Draw Network Diagrams

Drawing Network Diagrams

- A diagram of a target network provides an attacker with valuable information about the **network and its architecture**
- Network diagrams show **logical or physical paths** to a potential target

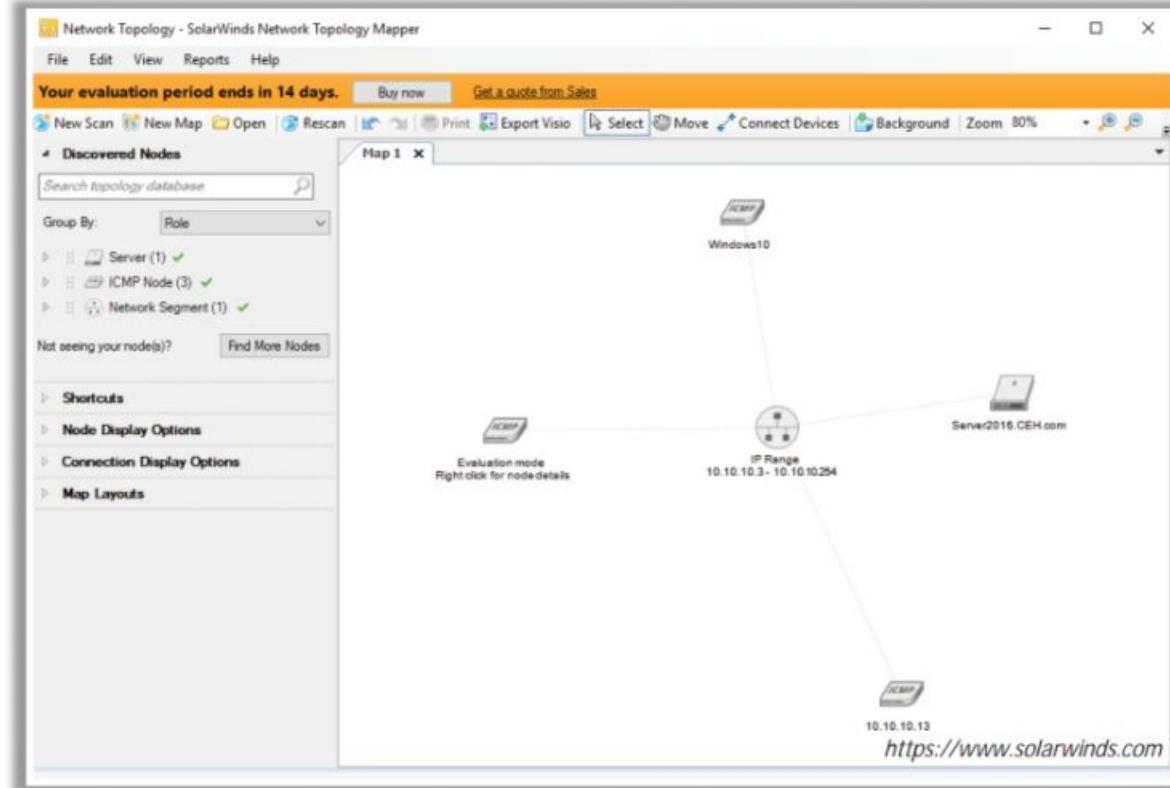


Network Discovery and Mapping Tools



Network Topology Mapper

- Network Topology Mapper discovers a network and produces a comprehensive network diagram
- It displays in-depth connections such as OSI Layer 2 and Layer 3 topology data



OpManager

<https://www.manageengine.com>



The Dude

<https://mikrotik.com>



NetSurveyor

<http://nutsaboutnets.com>



NetBrain

<https://www.netbraintech.com>



Spiceworks Network Mapping Tool

<https://www.spiceworks.com>

Module Summary



- In this module, we have discussed the following:
 - How attackers discover live hosts from a range of IP addresses by sending various ping scan requests to multiple hosts
 - How attackers perform different scanning techniques to determine open ports, services, service versions, etc. on the target system
 - How attackers perform banner grabbing or OS fingerprinting to determine the operating system running on a remote target system
 - Various scanning techniques that attackers can employ to bypass IDS/firewall rules and logging mechanisms, and disguise themselves as regular network traffic
 - Drawing diagrams of target networks and their significance in providing valuable information about a network and its architecture to an attacker
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform enumeration to collect information about a target before an attack or audit

