
SCANNING NETWORKS

Module Objectives

- Understanding Network Scanning Concepts
- Understanding various Scanning Tools
- Understanding various Host Discovery and Port Scanning Techniques
- Understanding OS Discovery
- Understanding various Techniques to Scan Beyond IDS and Firewall
- Drawing Network Diagrams

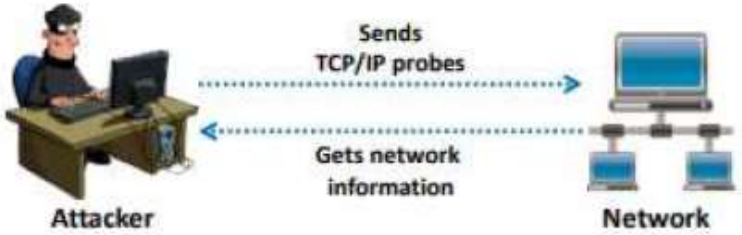
Module Flow

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

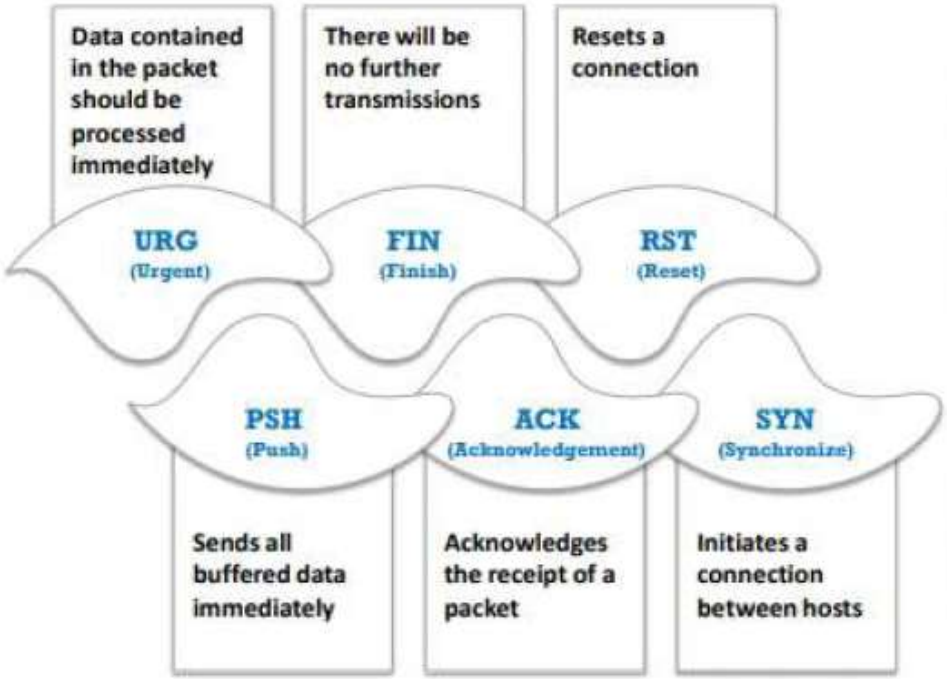
Network Scanning Process

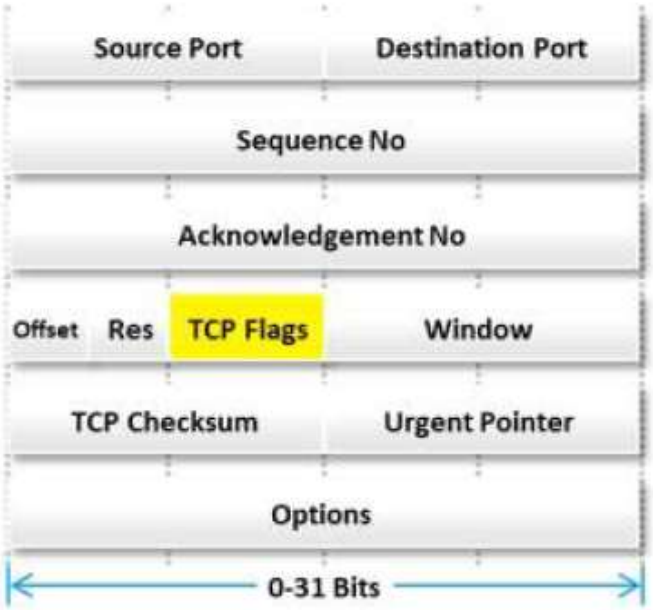


Objectives of Network Scanning

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

TCP Communication Flags



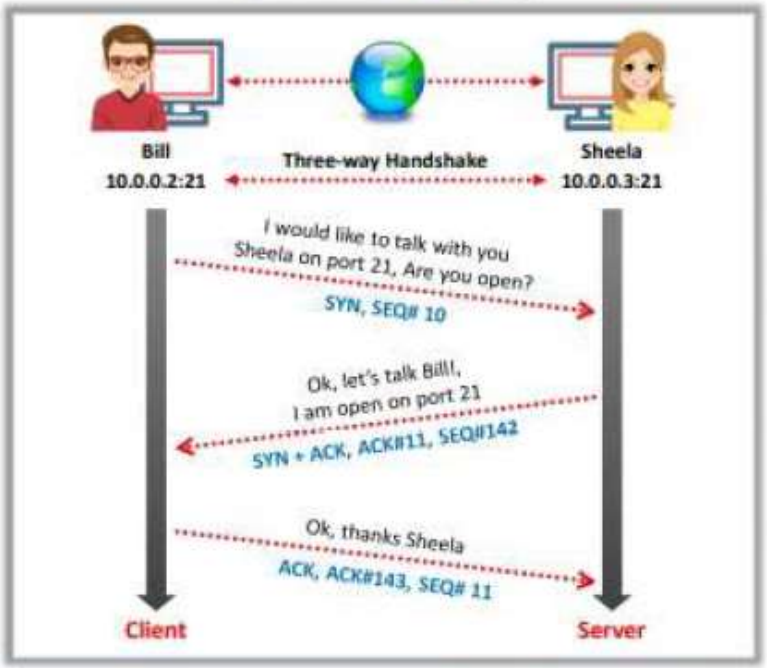


Standard TCP communications are controlled by flags in the TCP packet header

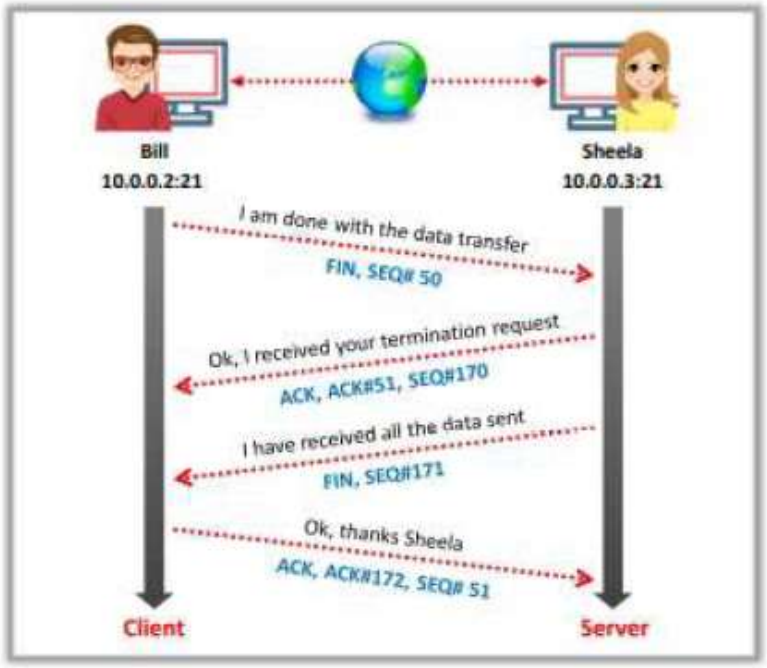
TCP/IP Communication

C|EH

TCP Session Establishment
(Three-way Handshake)



TCP Session Termination

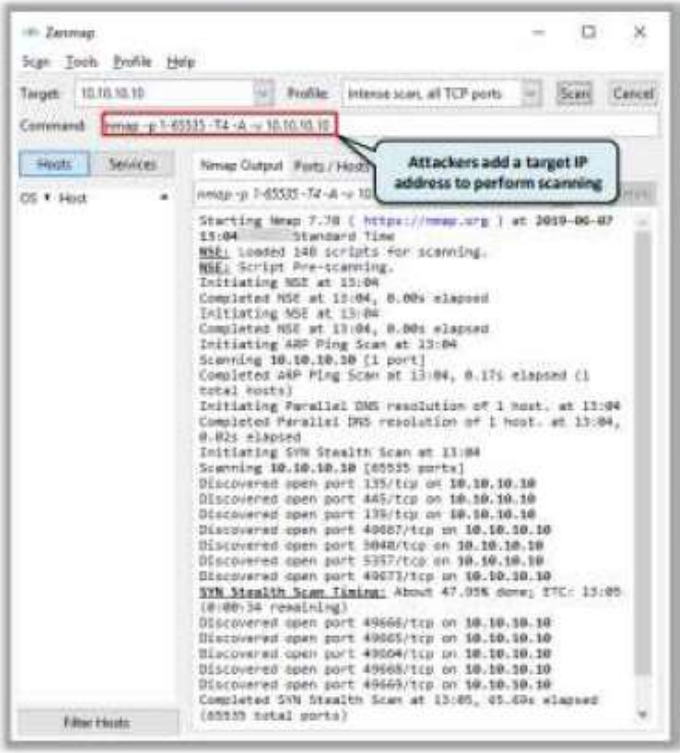


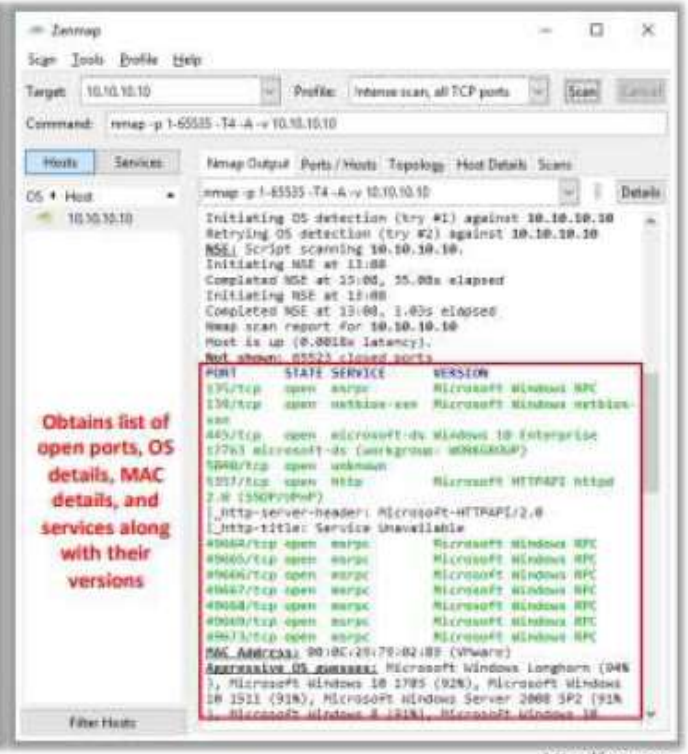
Module Flow

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**





Obtains list of open ports, OS details, MAC details, and services along with their versions

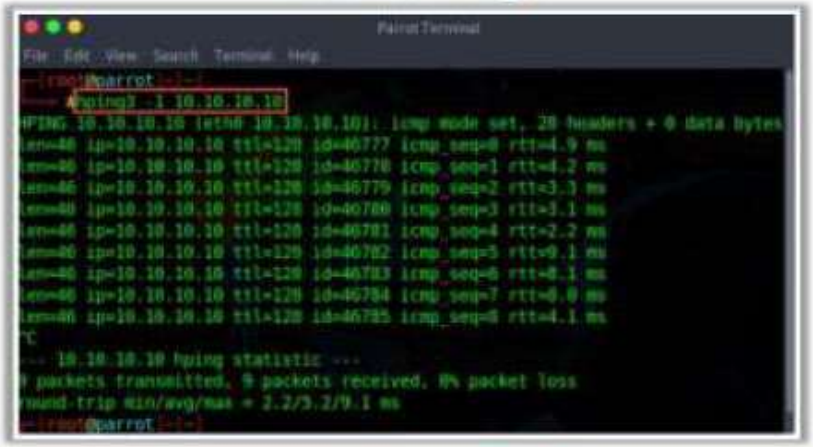
https://nmap.org

Scanning Tools: Hping2/Hping3

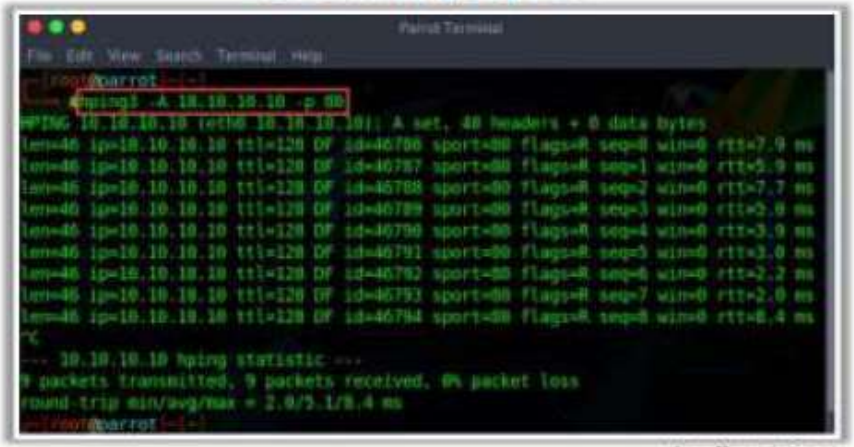
1. Command line **network scanning** and **packet crafting** tool for the TCP/IP protocol

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



ACK Scanning on port 80



http://www.hping.org

Hping Commands

ICMP Ping

```
hping3 -1 10.0.0.25
```

ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 -s
```

Firewalls and Timestamps

```
hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```

SYN scan on port 50-60

```
hping3 -8 50-60 -S 10.0.0.25 -V
```

FIN, PUSH and URG scan on port 80

```
hping3 -F -P -U 10.0.0.25 -p 80
```

Scan entire subnet for live host

```
hping3 -1 10.0.1.x --rand-dest -I eth0
```

Intercept all traffic containing HTTP signature

```
hping3 -9 HTTP -I eth0
```

SYN flooding a victim

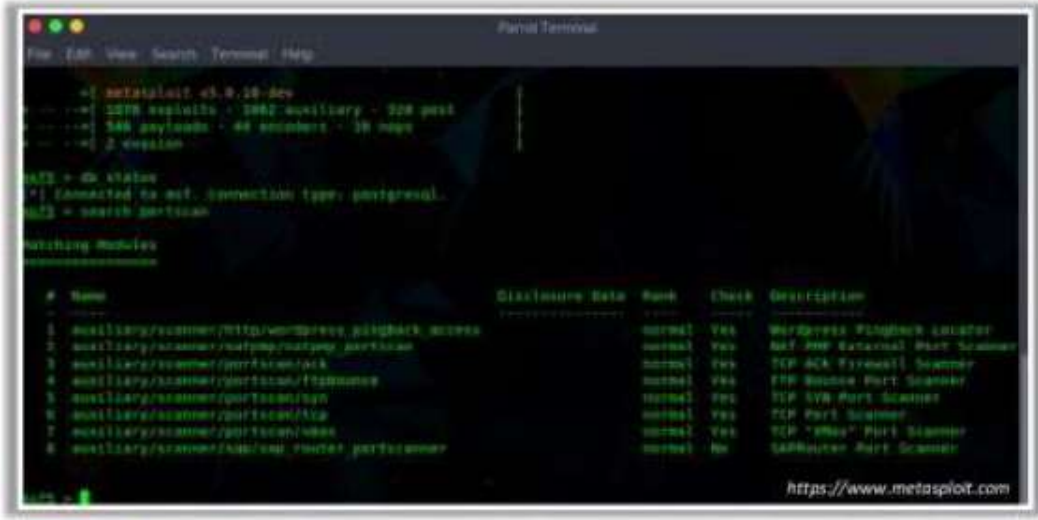
```
hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
```

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and timestamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH, and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

Scanning Tools

Metasploit

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



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

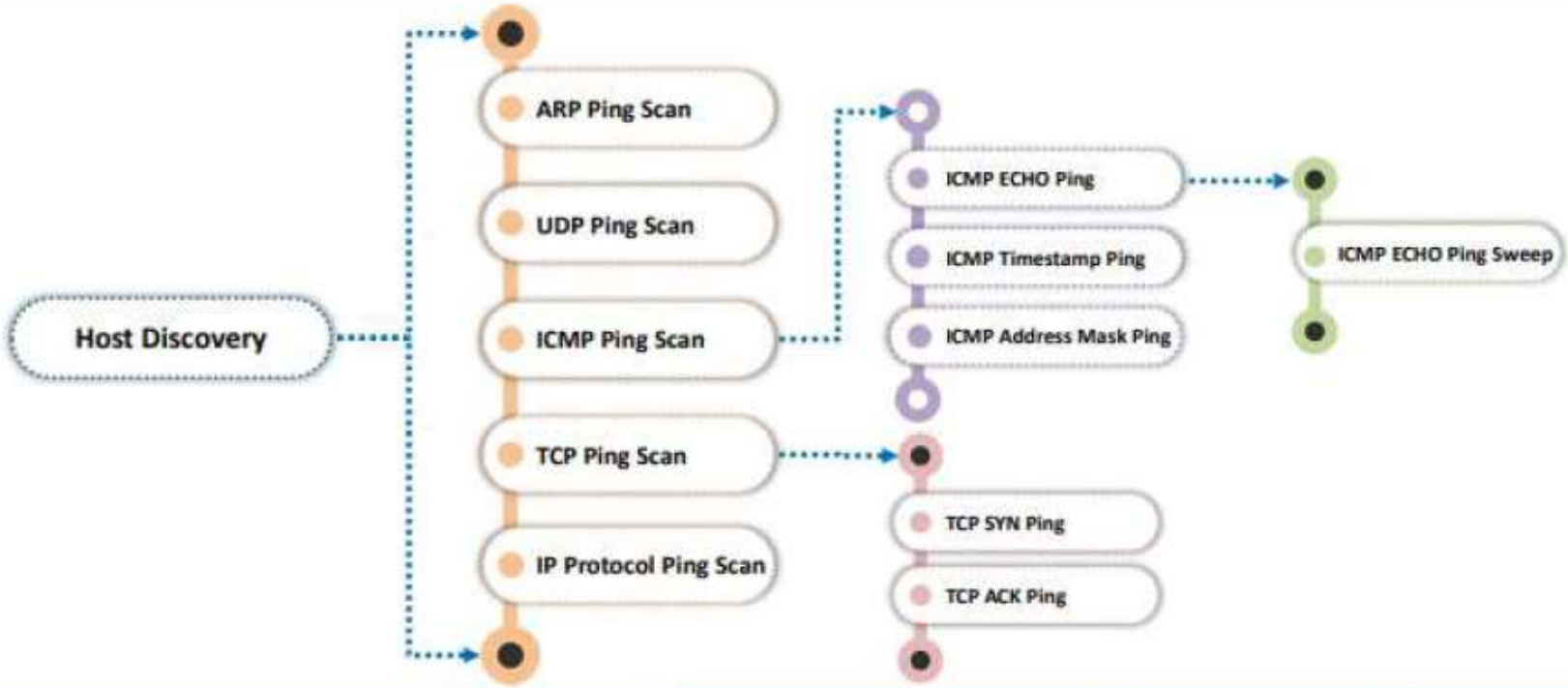
https://play.google.com

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

Host Discovery Techniques

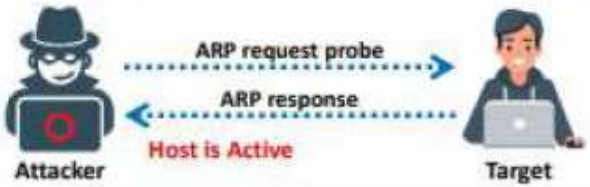
- Host discovery techniques are used to **identify the active/live systems** in the network

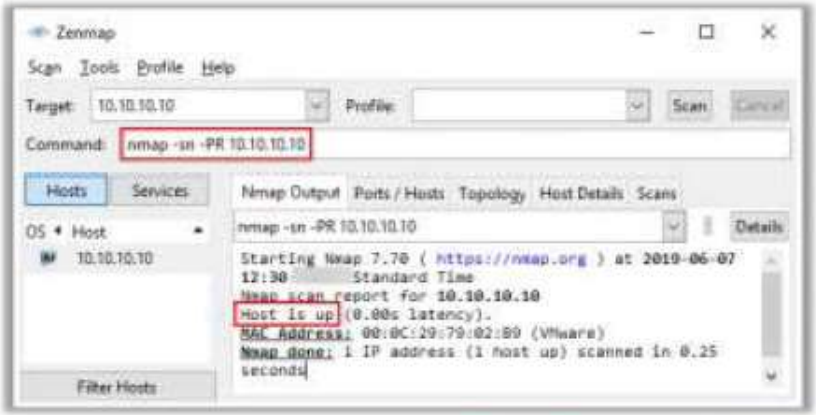


ARP Ping Scan and UDP Ping Scan

ARP Ping Scan

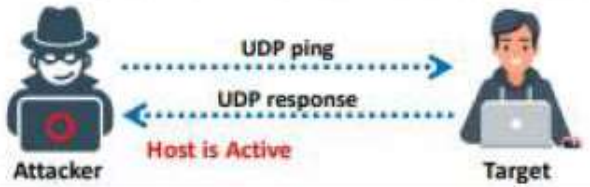
- Attackers send **ARP request probes** to target hosts, and an **ARP** response indicates that the **host is active**

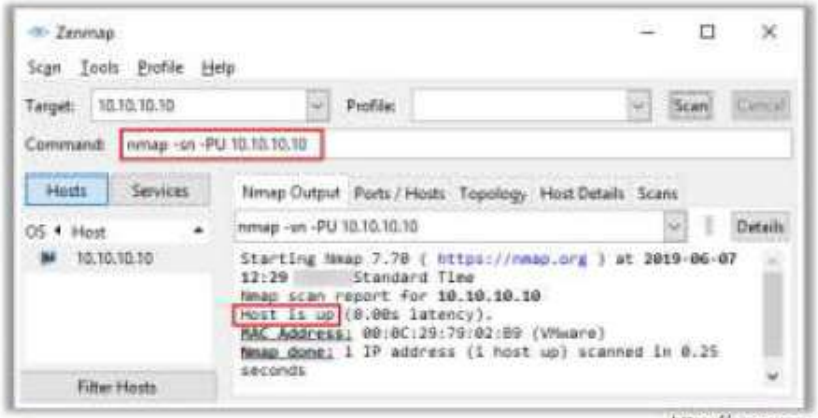




UDP Ping Scan

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



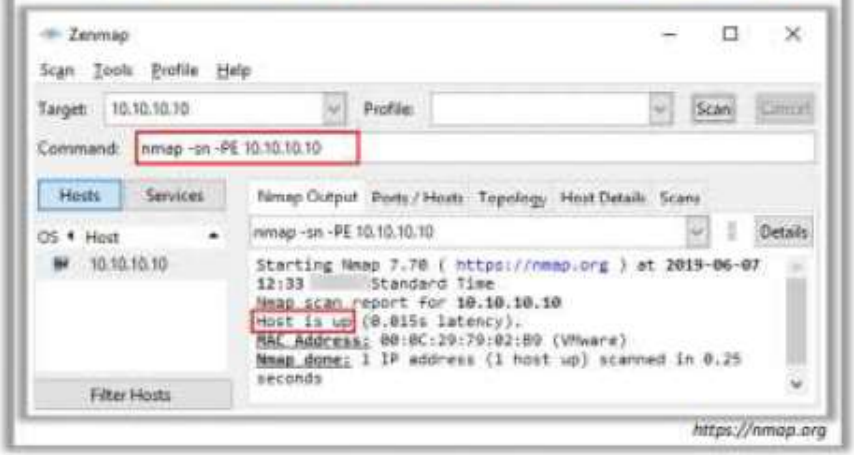


https://nmap.org

ICMP ECHO Ping Scan

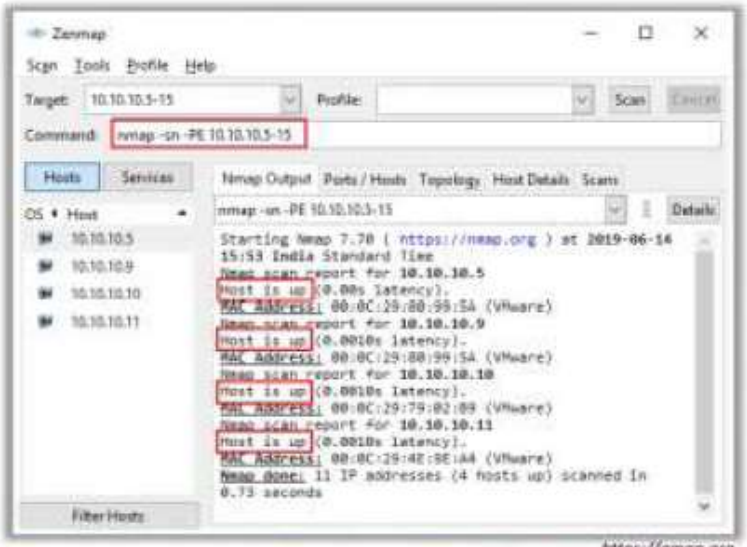
- ICMP ECHO ping scans involve sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply
- This scan is useful for **locating active devices** or determining if the **ICMP is passing through a firewall**

ICMP Echo ping scan output using Zenmap

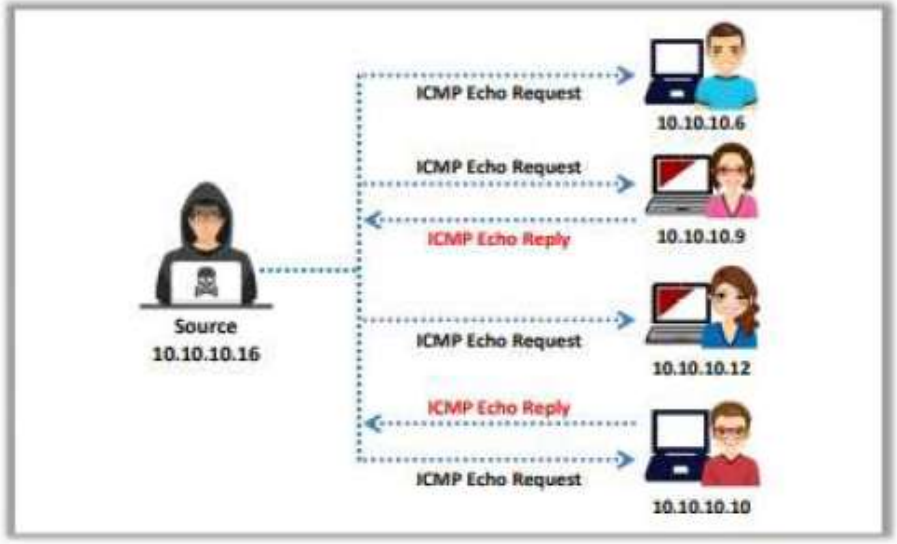


ICMP ECHO Ping Sweep

- 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



https://nmap.org



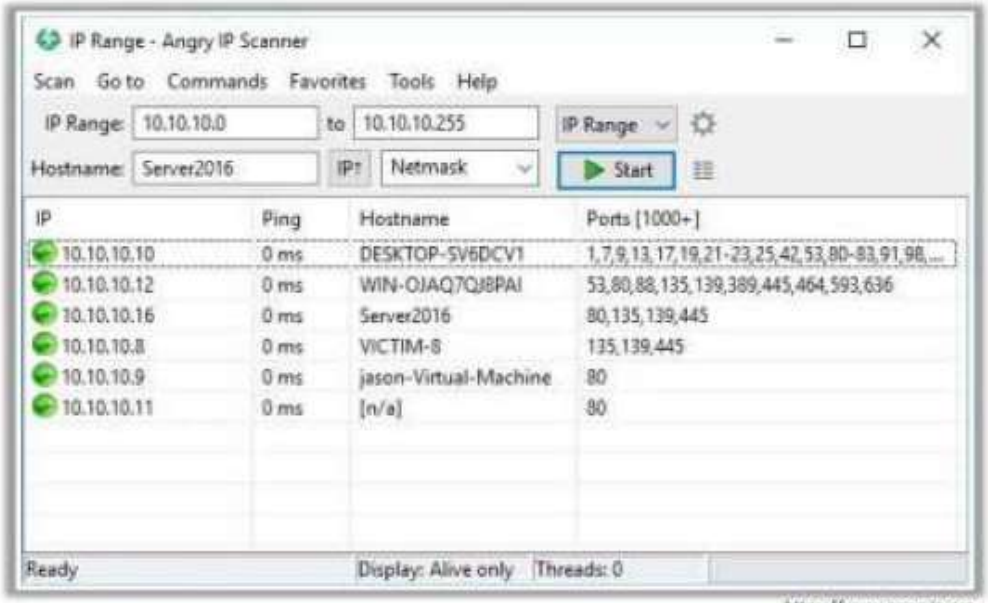
Ping Sweep Tools

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*)



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**
5. Use DMZs and allow only commands like **ICMP ECHO_REPLY**, **HOST UNREACHABLE**, and **TIME EXCEEDED** within a DMZ
6. **Limit ICMP traffic** using **Access Control Lists (ACLs)** and grant permissions only to specific IP addresses such as ISPs

Other Host Discovery Techniques

C|EH

ICMP Timestamp and Address Mask Ping Scan

- These techniques are alternatives for the traditional ICMP ECHO ping scan and are used to determine whether the target host is live, specifically when the administrators block ICMP ECHO pings

ICMP Timestamp Ping Scan

```
# nmap -sn -PP <target IP address>
```

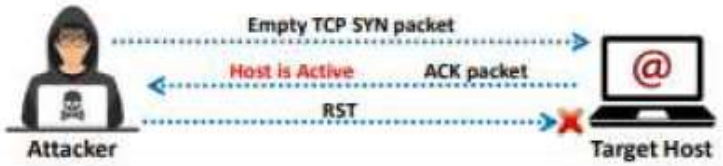
ICMP Address Mask Ping Scan

```
# nmap -sn -PM <target IP address>
```

TCP SYN Ping Scan

- Attackers send empty TCP SYN packets to a target host, and an ACK response means that the host is active

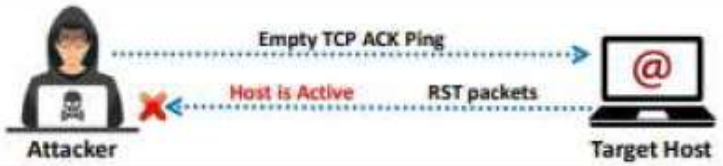
```
# nmap -sn -PS <target IP address>
```



TCP ACK Ping Scan

- Attackers send empty TCP ACK packets to a target host, and an RST response means that the host is active

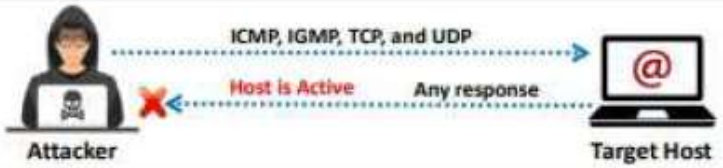
```
# nmap -sn -PA <target IP address>
```



IP Protocol Ping Scan

- Attackers send various probe packets to the target host using different IP protocols, and any response from any probe indicates that a host is active

```
# nmap -sn -PO <target IP address>
```

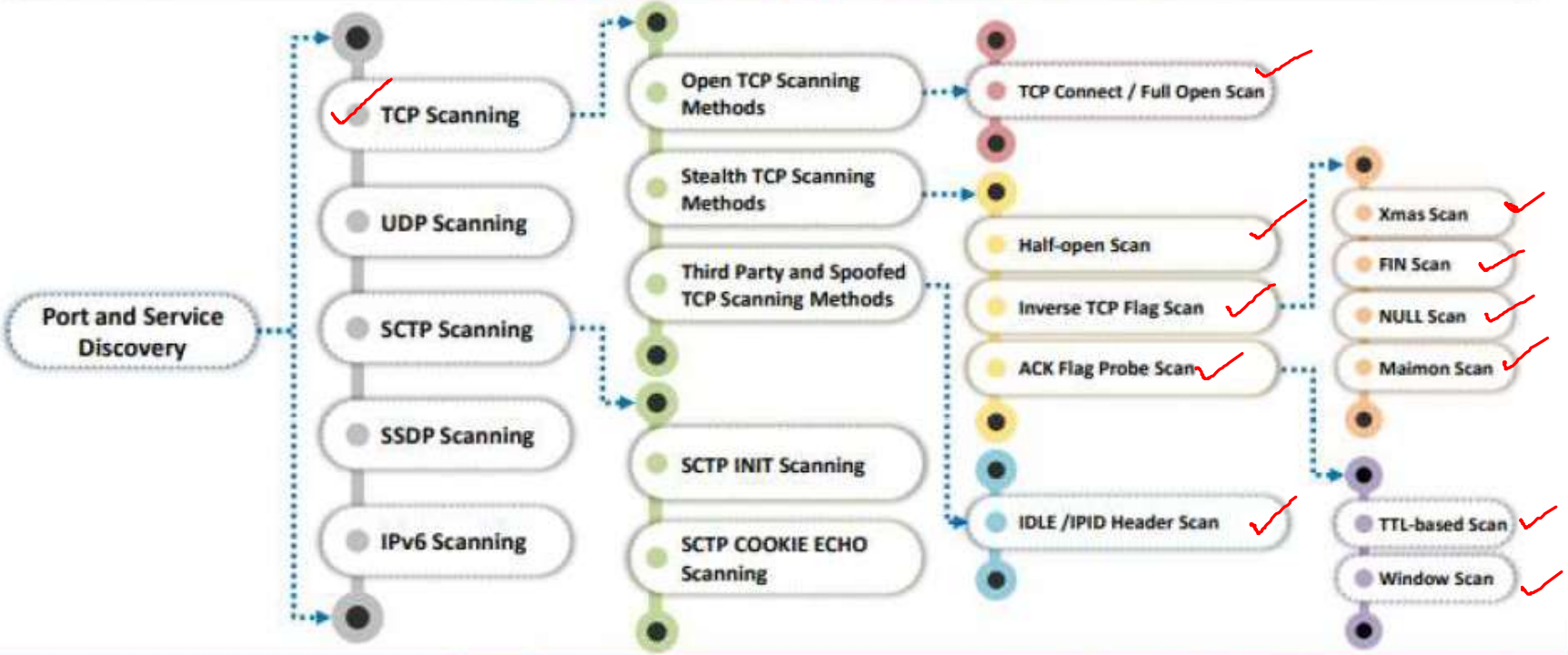


Module Flow

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

Port Scanning Techniques

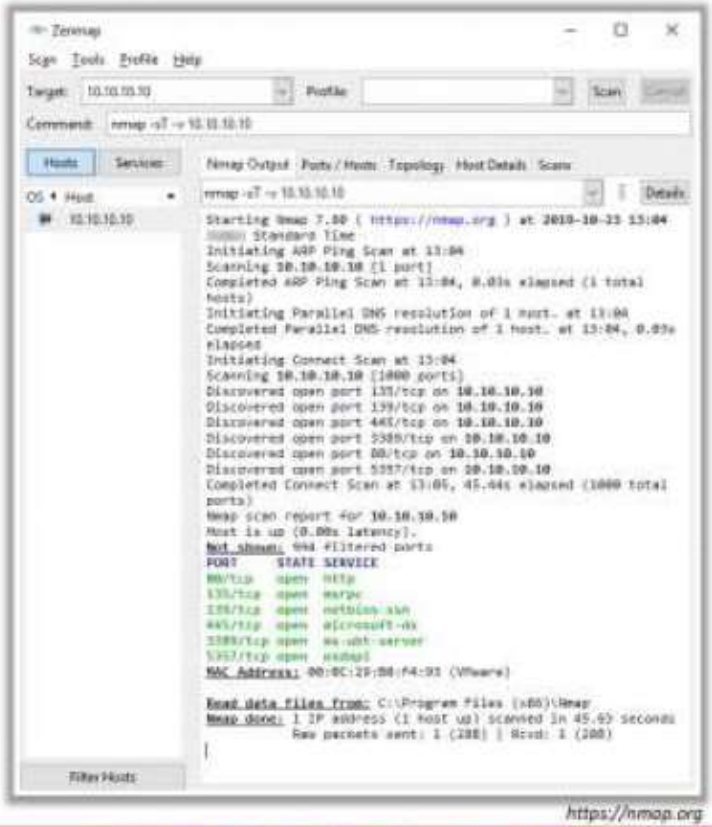
- The port scanning techniques are **categorized according to the type of protocol** used for communication



TCP Connect/Full Open Scan

nmap -sT -v ip address

- 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**



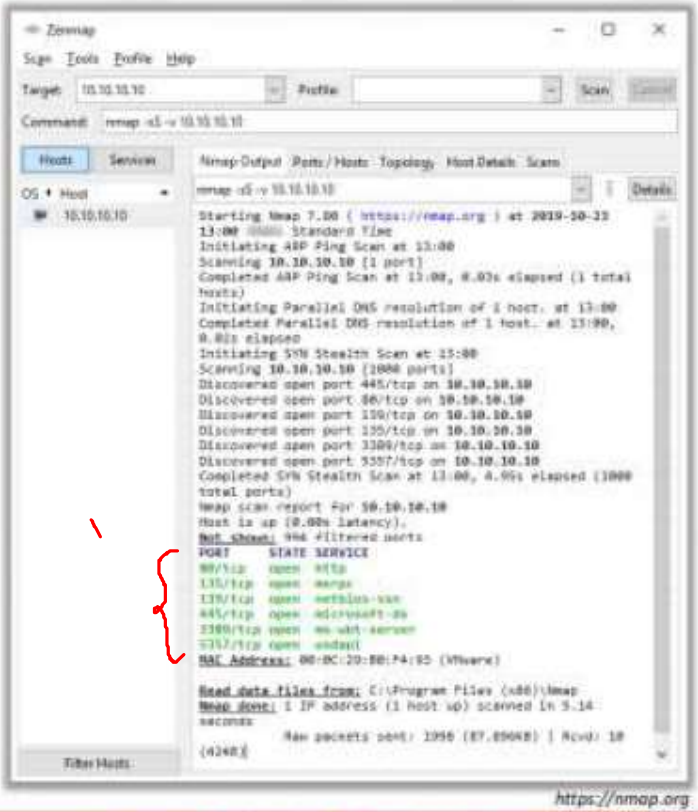
Stealth Scan (Half-open Scan)

nmap -sS -v ip address

- 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

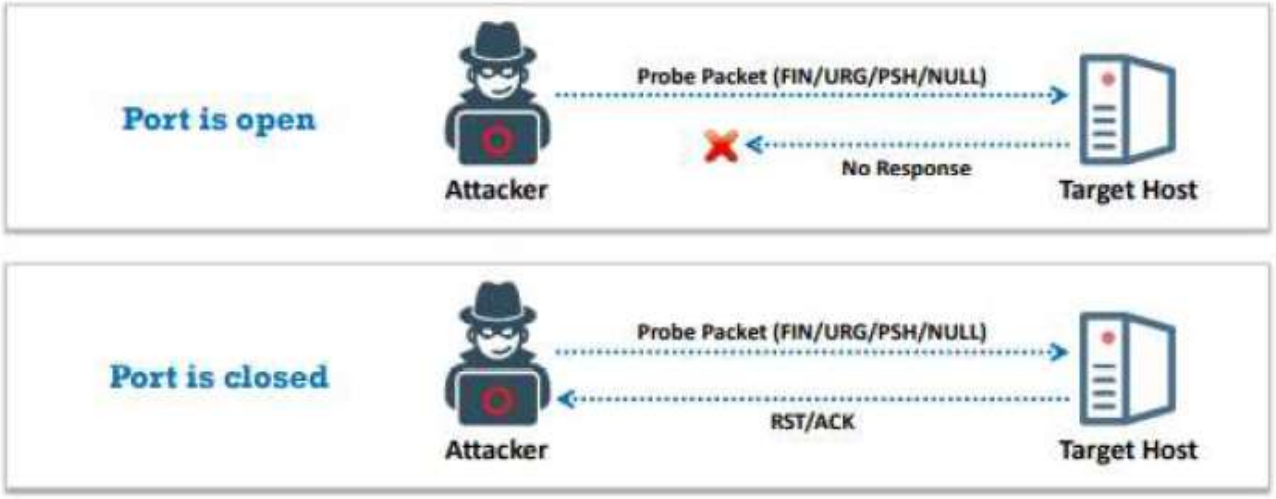
Scan result when a port is closed



https://nmap.org

Inverse TCP Flag Scan

- Attackers send **TCP probe packets** with a TCP flag (FIN, URG, PSH) set or with no flags, where no response implies that the port is open, whereas an RST response means that the port is closed



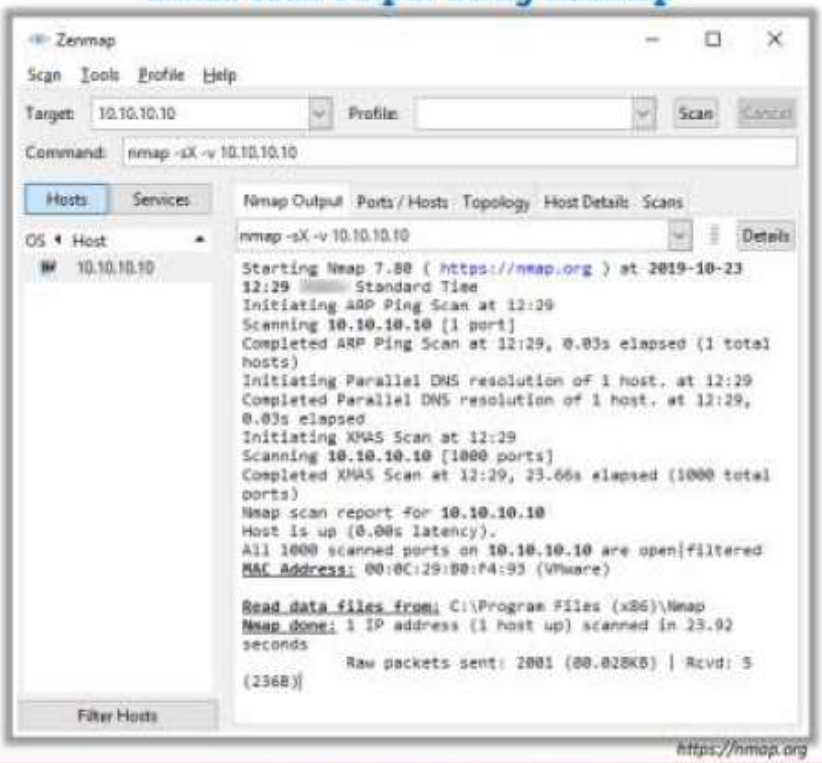
Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. It is known as null scanning if there is no flag set

Xmas Scan

nmap -sX -v ip address

- 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**

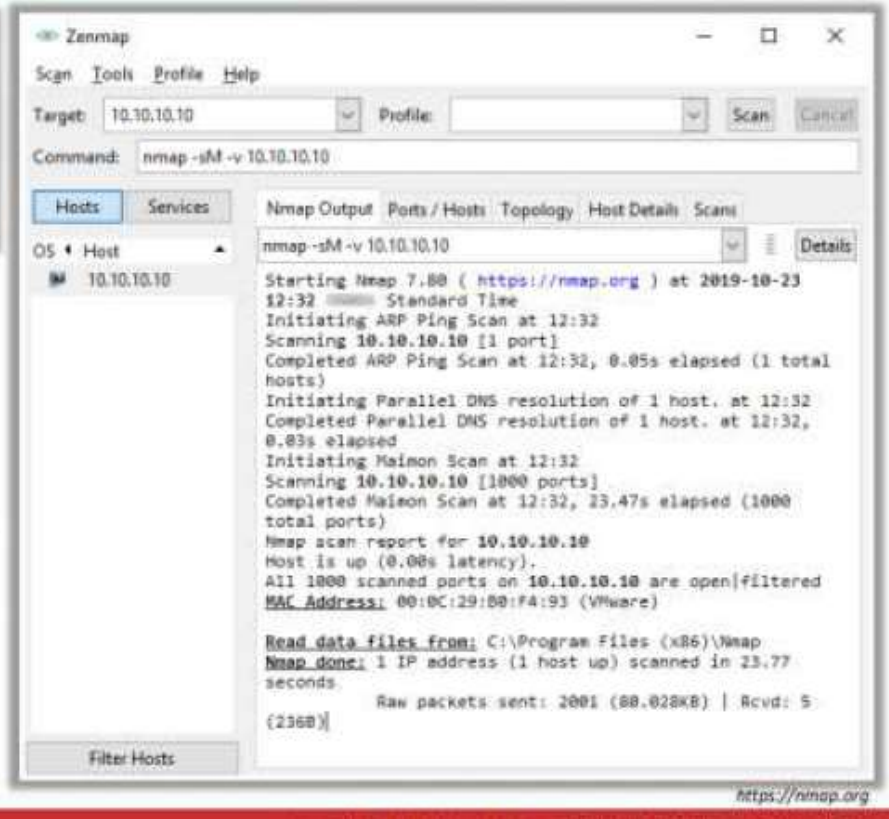
Xmas scan output using Zenmap



TCP Maimon Scan

nmap -sM -v

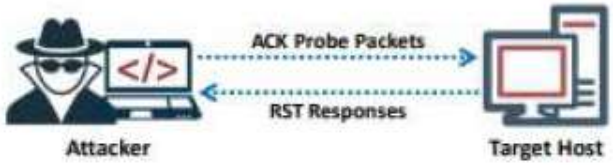
- Attackers send **FIN/ACK probes**, and if there is no response, then the port is **Open|Filtered**, but if an **RST packet** is sent in response, then the port is **closed**



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**

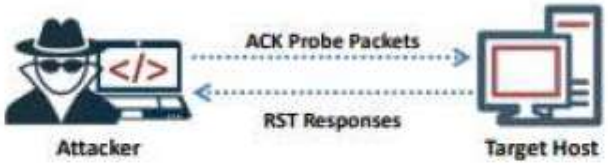
TTL-based ACK Flag Probe scanning




```
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



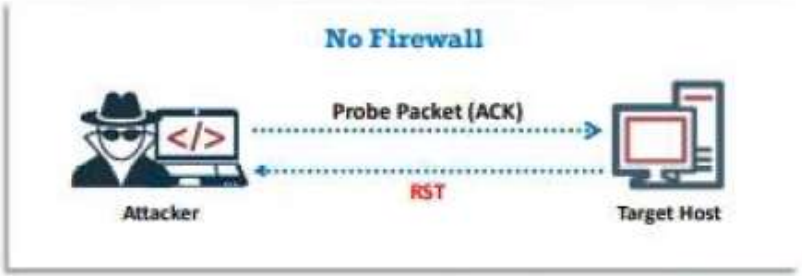

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

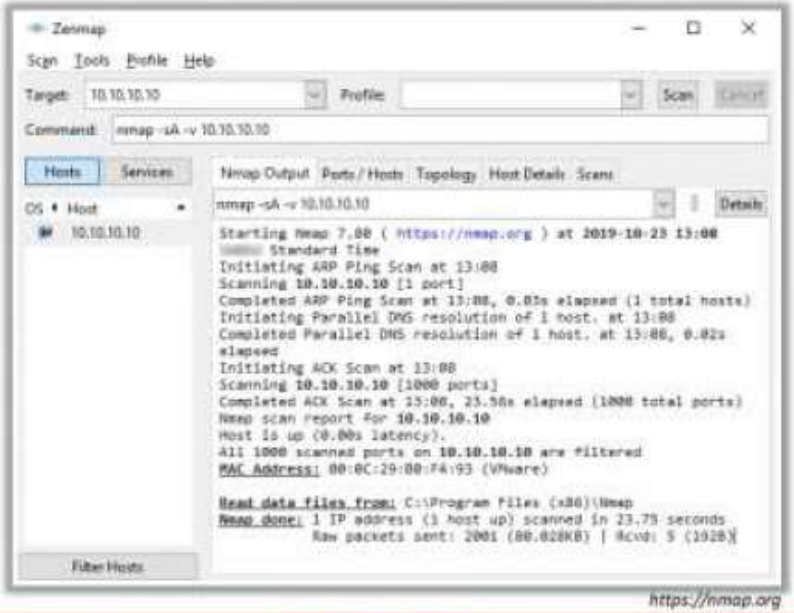
If the **window value of the RST packet** on a particular port has a **non-zero value**, then that **port is open**

ACK Flag Probe Scan (Cont'd)

nmap -sA -v

- 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**



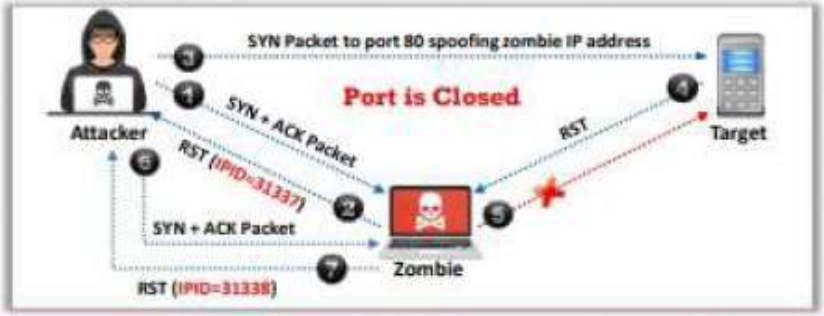


https://nmap.org

IDLE/IPID Header Scan

- Every IP packet on the Internet has a fragment identification number (IPID); an OS increases the IPID for each packet sent, thus, probing an IPID gives an attacker the **number of packets sent** after the last probe
- A machine that receives an **unsolicited SYN|ACK packet** will respond with an RST. An unsolicited RST will be ignored

1. Send SYN + ACK packet to the zombie machine to **probe its IPID number**
2. A zombie machine not expecting an SYN + ACK packet will send an **RST packet**, disclosing the IPID. Analyse the RST packet from the zombie machine to **extract the IPID**
3. Send a SYN packet to the **target machine (port 80)** to spoof the IP address of the "zombie"
4. If the port is open, the target will send a **SYN+ACK packet** to the zombie, and the zombie will send an RST to the target in response
5. If the port is closed, the target will send an **RST to the zombie**, but the zombie will not send anything back
6. Probe the zombie IPID again. An IPID increased by **2 will indicate an open port**, whereas an IPID increased by **1 will indicate a closed port**



UDP Scanning

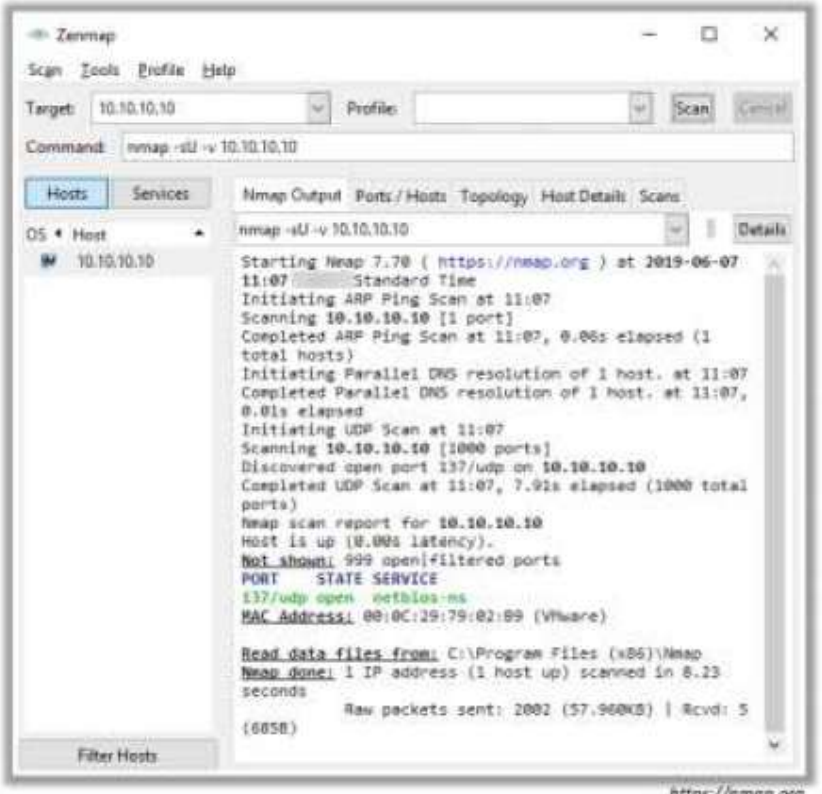
nmap -sU -v IP address

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

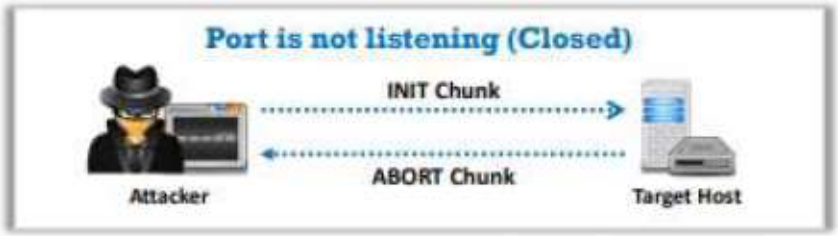
- If a UDP packet is sent to a closed port, the system will respond with an ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports

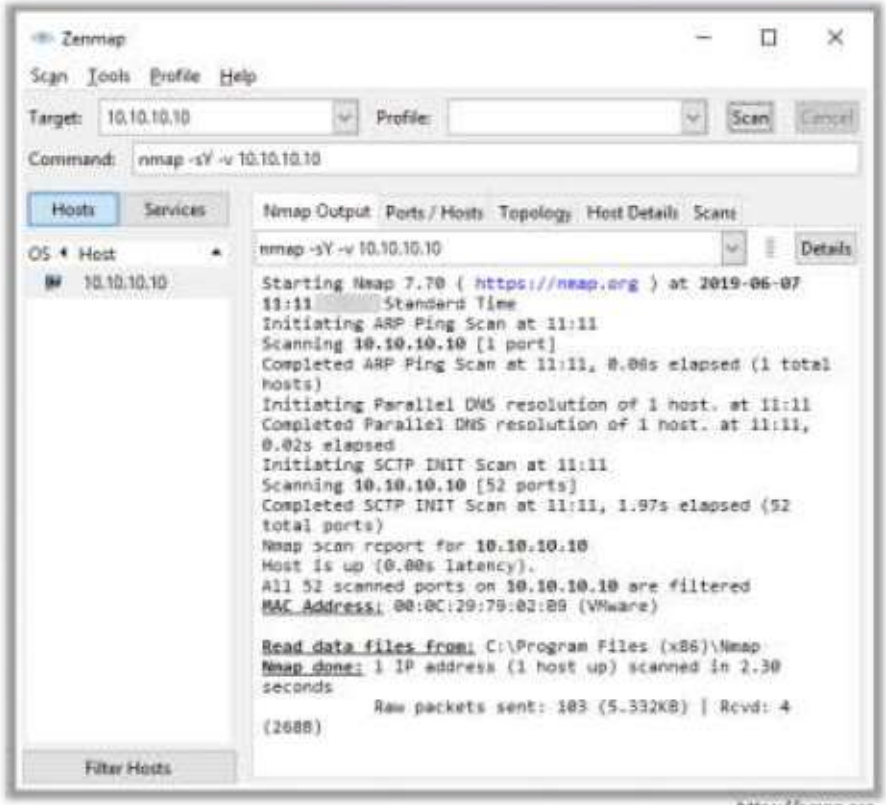


SCTP INIT Scanning

nmap -sY -v ipaddress

- 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**

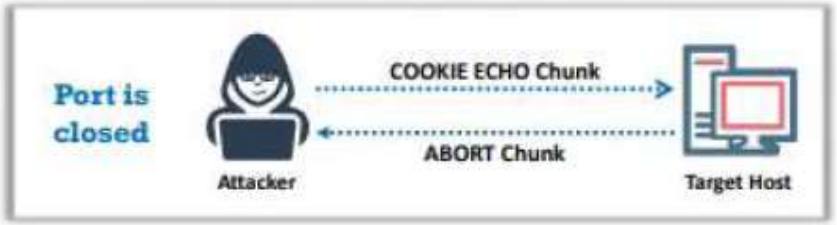


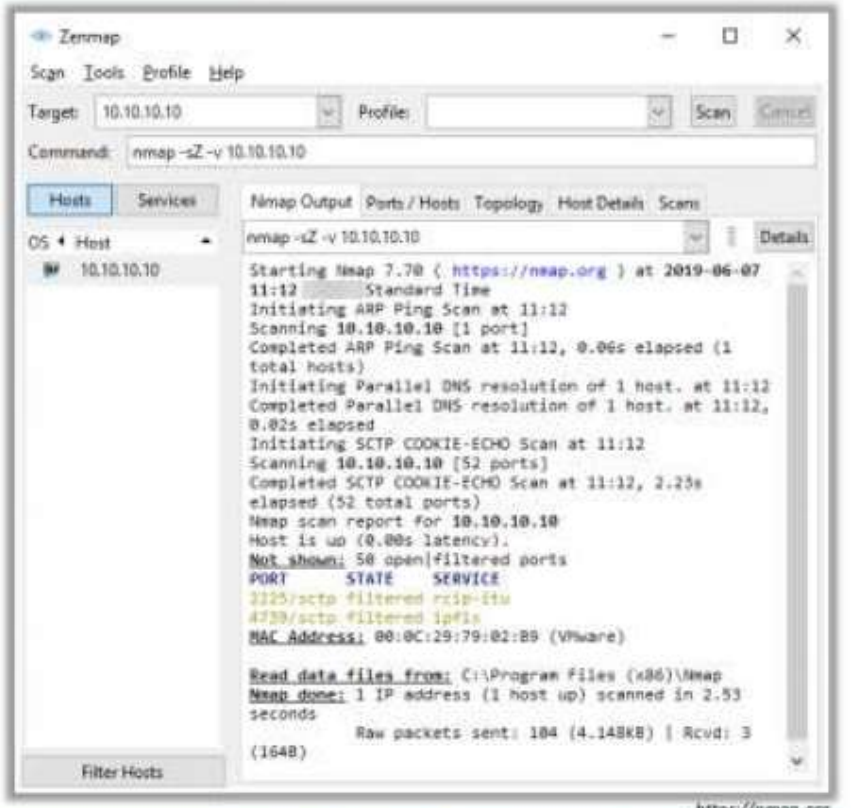


SCTP COOKIE ECHO Scanning

nmap -sZ -v ipaddress

- 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

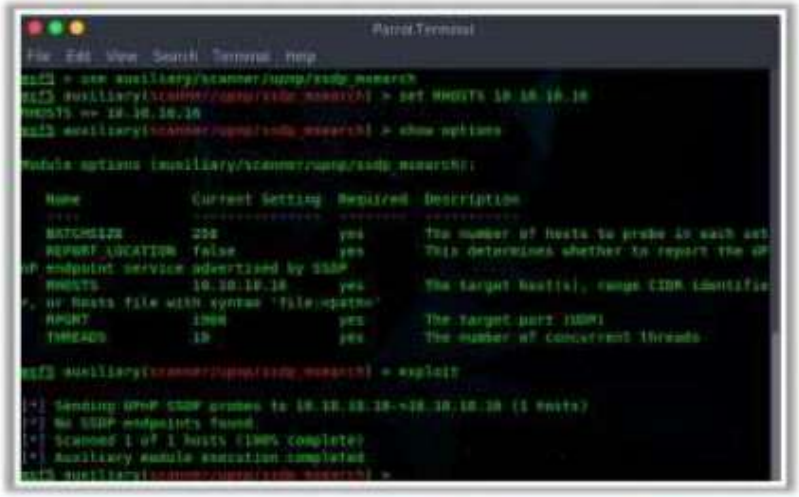




SSDP and List Scanning

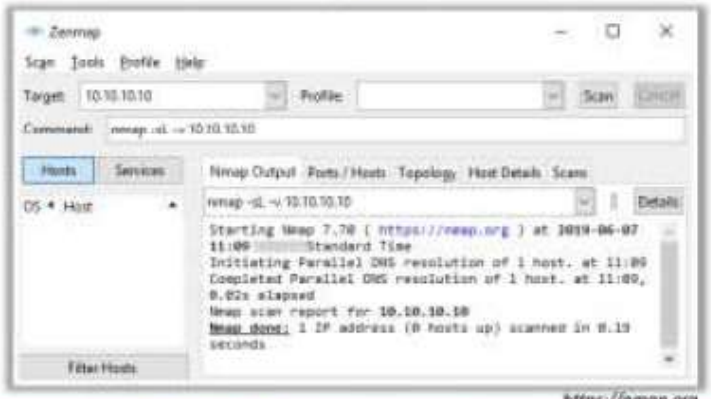
SSDP Scanning

- 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



List Scanning

- 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

IPv6 Scanning

- IPv6 increases the IP address size from **32 bits** to **128 bits** to support more levels of address hierarchy
- Attackers need to harvest IPv6 addresses from **network traffic**, **recorded logs**, or **Received from:** header lines in archived emails
- Attackers can use the **-6** option in Zenmap to **perform IPv6 scanning**

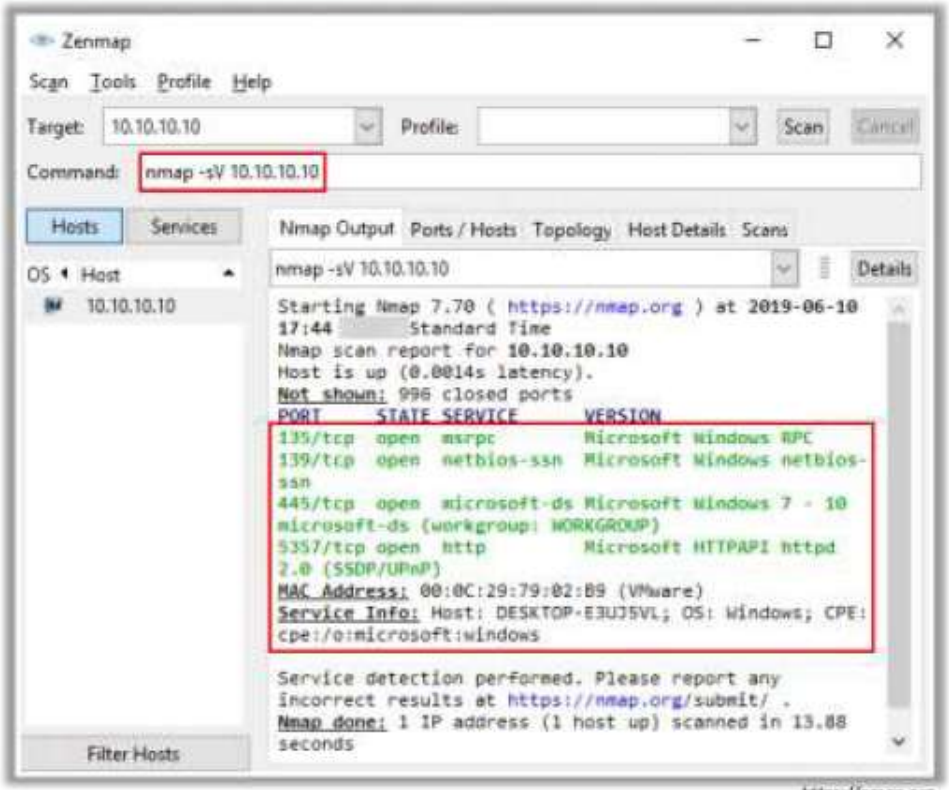
```
root@          :~# nmap -6 scanme.nmap.org

Starting Nmap      ( http://nmap.org ) at          04:25 UTC
Nmap scan report for scanme.nmap.org (2600:3c01::f03c:91ff:fe18:bb2f)
Host is up (0.062s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

https://nmap.org

Service Version Discovery

nmap -sV ipaddress

- 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



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

→ Find appropriate tool to determine OS in target machine?

- 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 Banner Grabbing

- **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 Banner Grabbing

- **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**

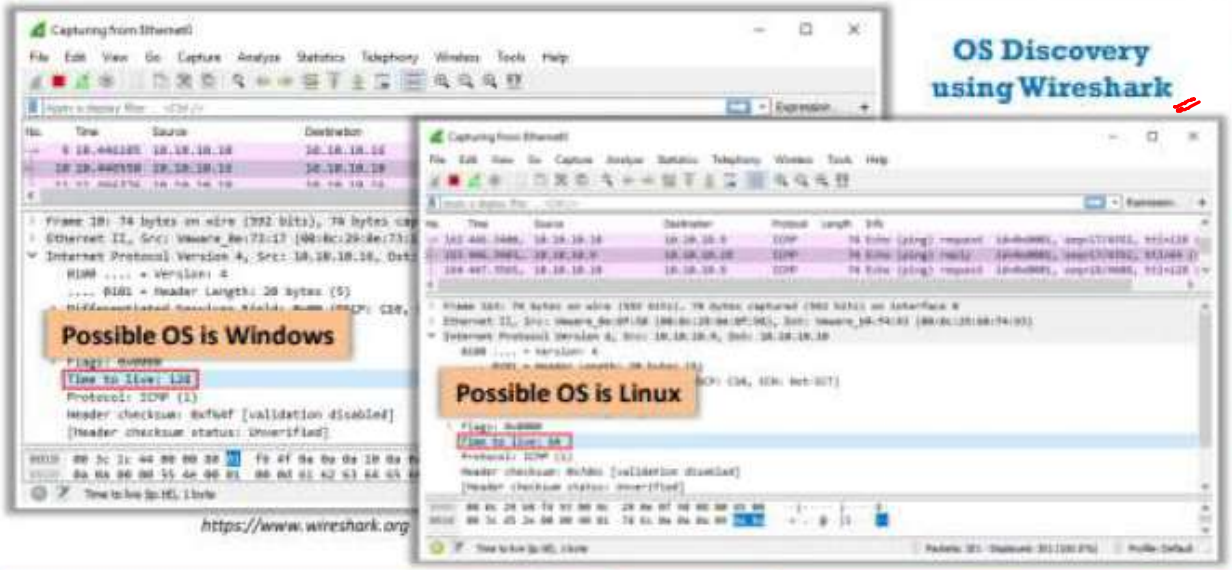
  Looking for an extension in the URL may assist in determining the application's version.

  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



OS Discovery using Wireshark

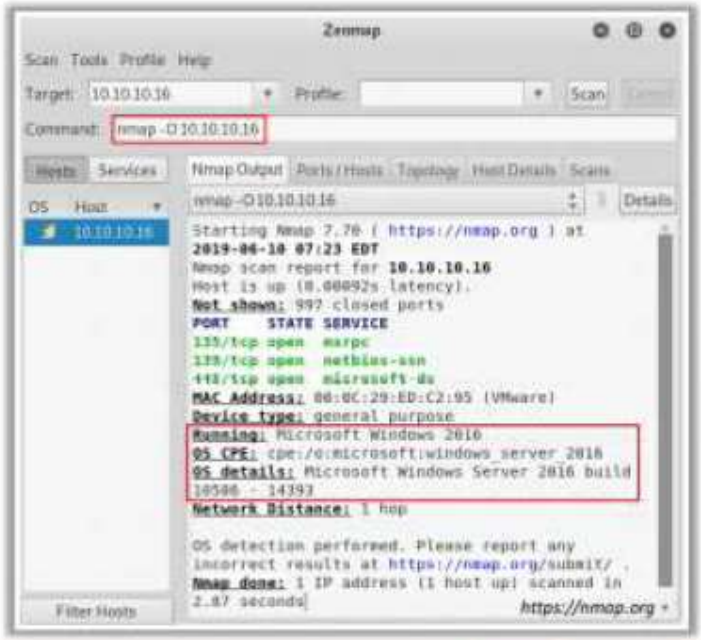
Window size values for OS

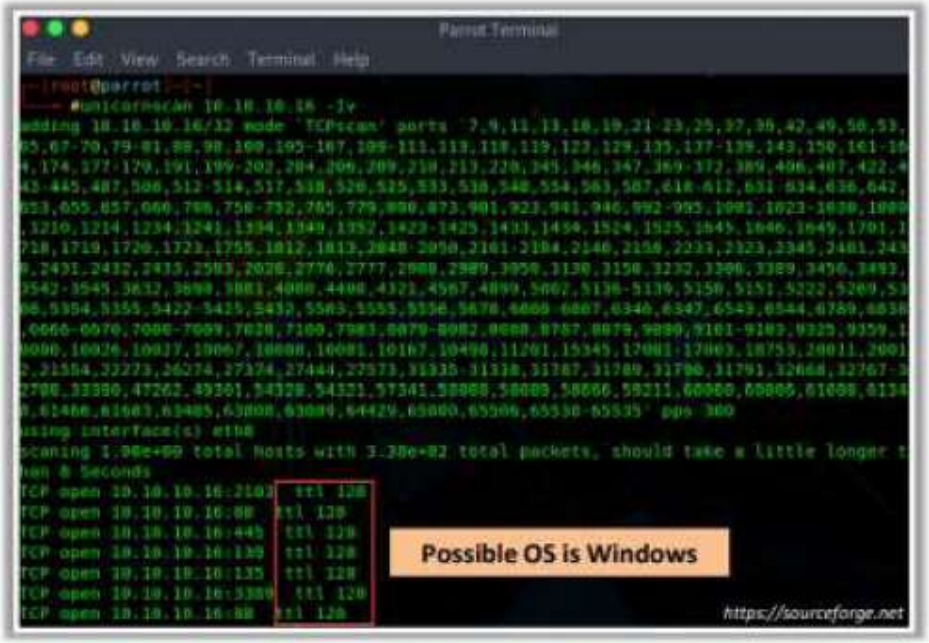
Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX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

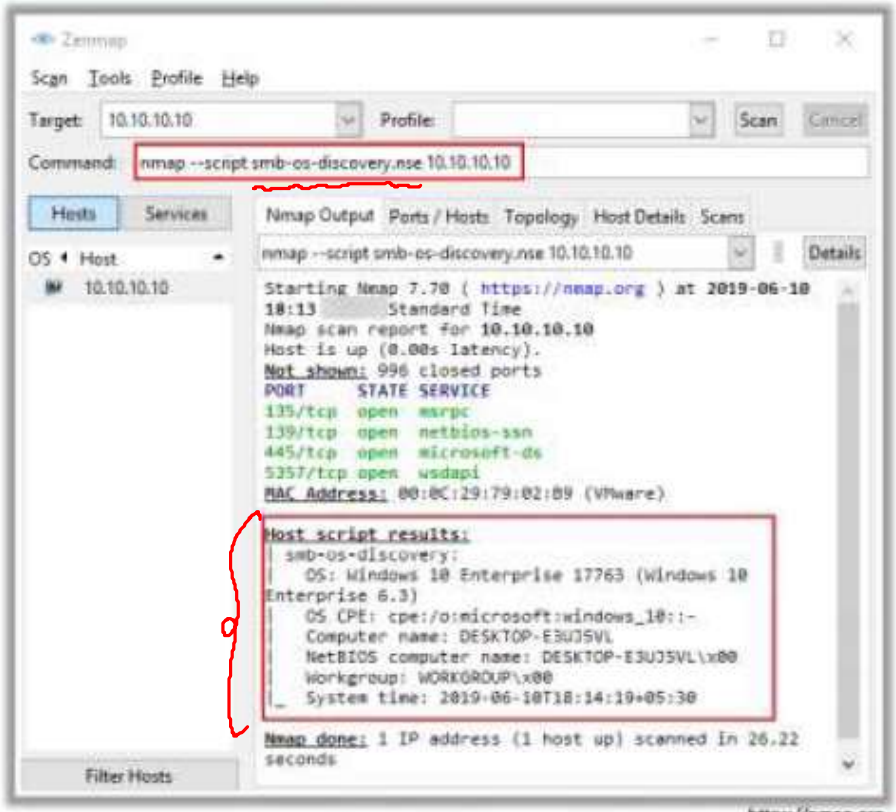
- In **Unicornscan**, the OS of the target machine can be identified by **observing the TTL values** in the acquired scan result





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



OS Discovery using IPv6 Fingerprinting

- IPv6 Fingerprinting can be used to **identify the OS running** on the target machine

- IPv6 fingerprinting has the **same functionality** as that of IPv4

- The difference between IPv6 and IPv4 fingerprinting is that the IPv6 uses several **additional advanced probes specific to IPv6** along with a **separate OS detection engine that is specialized for IPv6**

- In Zenmap, the **-6 option** and **-O option** are used to perform OS discovery using the IPv6 fingerprinting method
  - Syntax: **# nmap -6 -O <target>**

Banner Grabbing Countermeasures

Disabling or Changing Banner

- Display **false banners** to mislead or deceive attackers
- **Turn off unnecessary services** on the network host to limit the disclosure of information
- Use **ServerMask** (*http://www.port80software.com*) tools to disable or change banner information
- Apache 2.x with `mod_headers` module - use a directive in `httpd.conf` file to change banner information **Header set Server "New Server Name"**
- Alternatively, change the `ServerSignature` line to `ServerSignature Off` in `httpd.conf` file

Hiding File Extensions from Web Pages

- File extensions reveal information about the **underlying server technology** that an attacker can utilize to launch attacks
- Hide file extensions to **mask web technologies**
- Change **application mappings** such as .asp with .htm or .foo, etc. to disguise the identity of servers
- Apache users can use **mod_negotiation** directives
- IIS users use tools such as **PageXchanger** to manage the file extensions

✔ **It is better if the file extensions are not used at all**

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

IDS/Firewall Evasion Techniques

- Though firewalls and IDSs can prevent malicious traffic (packets) from entering a network, attackers can manage to **send intended packets to the target** by **evading an IDS or firewall** through the following techniques:

1. Packet Fragmentation
2. Source Routing
3. Source Port Manipulation
4. IP Address Decoy
5. IP Address Spoofing
6. Creating Custom Packets
7. Randomizing Host Order
8. Sending Bad Checksums
9. Proxy Servers
10. Anonymizers

Packet Fragmentation

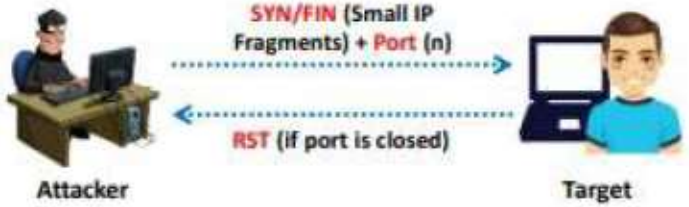
- Packet fragmentation refers to the **splitting of a probe packet into several smaller packets** (fragments) while sending it to a network
- It is not a new scanning method but a **modification** of the previous techniques

- The **TCP header** is split into several packets so that the packet filters are not able to detect what the packets are intended to do

Command Prompt

```
C:\>nmap -sS -T4 -A -f -v 10.10.10.10

Starting Nmap 7.80 ( http://nmap.org ) at
2019-08-10 11:03 EDT
Initiating SYN Stealth Scan at 11:03
Scanning 10.10.10.10 [1000 ports]
Discovered open port 139/tcp on 10.10.10.10
Discovered open port 445/tcp on 10.10.10.10
Discovered open port 135/tcp on 10.10.10.10
Discovered open port 912/tcp on 10.10.10.10
Completed SYN Stealth Scan at 11:03, 4.75s elapsed (1000
total ports)
```

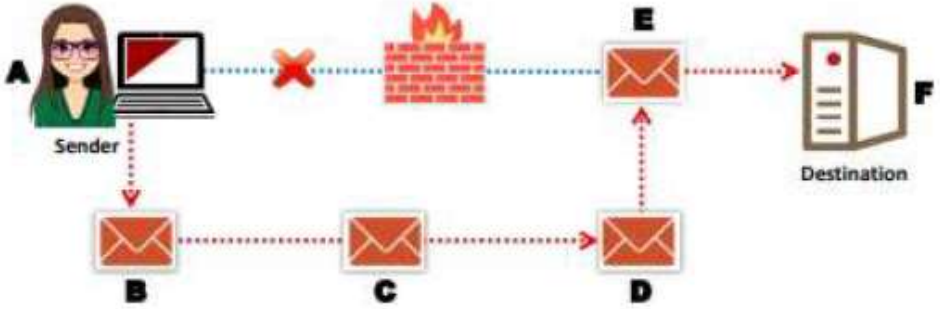
SYN/FIN Scanning Using IP Fragments



Source Routing

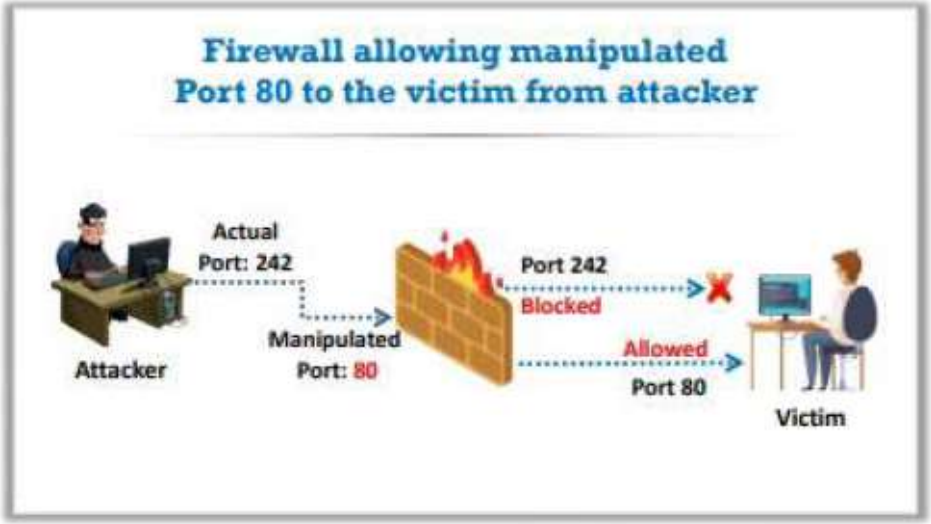
- As the packet travels through the nodes in the network, each **router examines** the destination IP address and **chooses the next hop** to direct the packet to the destination
- Source routing refers to sending a packet to the intended destination with a partially or completely **specified route** (without firewall-/IDS-configured routers) in order to evade an IDS or firewall
- In source routing, the **attacker** makes some or all of these decisions on the router

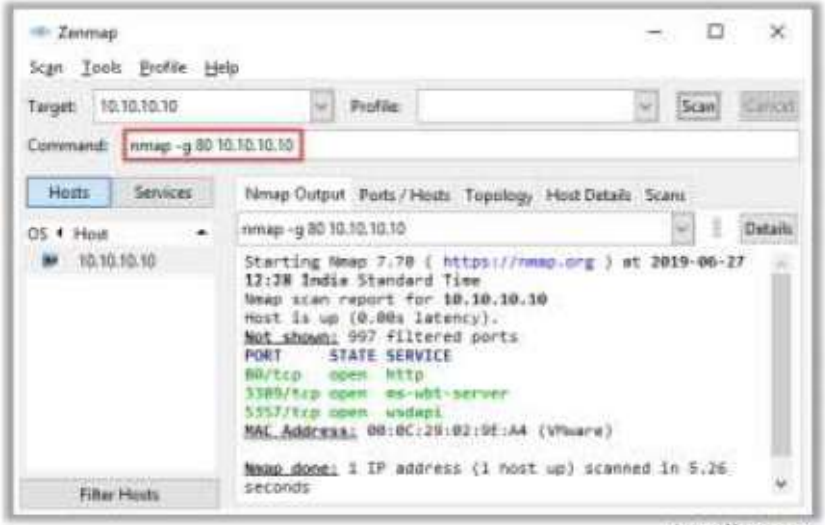
This figure shows source routing, where the originator dictates the eventual route of the traffic



Source Port Manipulation

- Source port manipulation refers to **manipulating actual port numbers with common port numbers** in order to evade an IDS or firewall
- It occurs when a firewall is **configured to allow packets** from well-known ports like HTTP, DNS, FTP, etc.
- **Nmap** uses the **-g** or **--source-port** options to perform source port manipulation





https://nmap.org

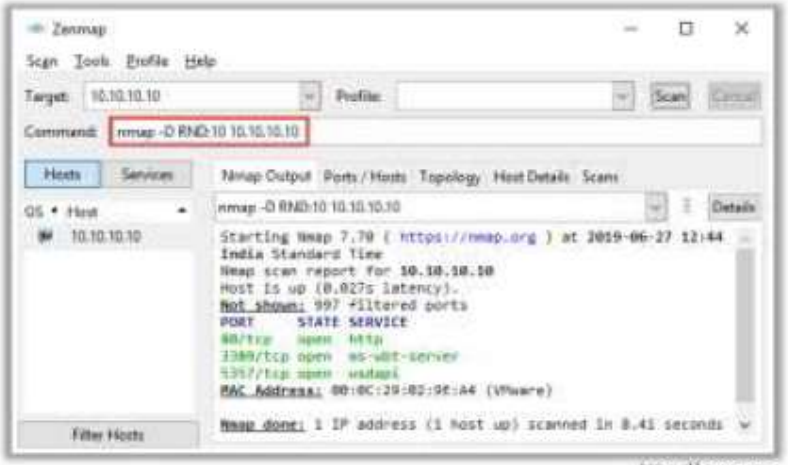
IP Address Decoy

- IP address decoy technique refers to **generating or manually specifying the IP addresses of decoys** in order to evade an IDS or firewall
- It appears to the target that the **decoys as well as the host(s)** are scanning the network
- This technique makes it **difficult for the IDS or firewall to determine** which IP address was actually scanning the network and which IP addresses were decoys

Decoy Scanning using Nmap

Nmap has two options for decoy scanning:

- **`nmap -D RND:10 [target]`**
  (Generates a random number of decoys)
- **`nmap -D decoy1,decoy2,decoy3,..`** etc.
  (Manually specify the IP addresses of the decoys)

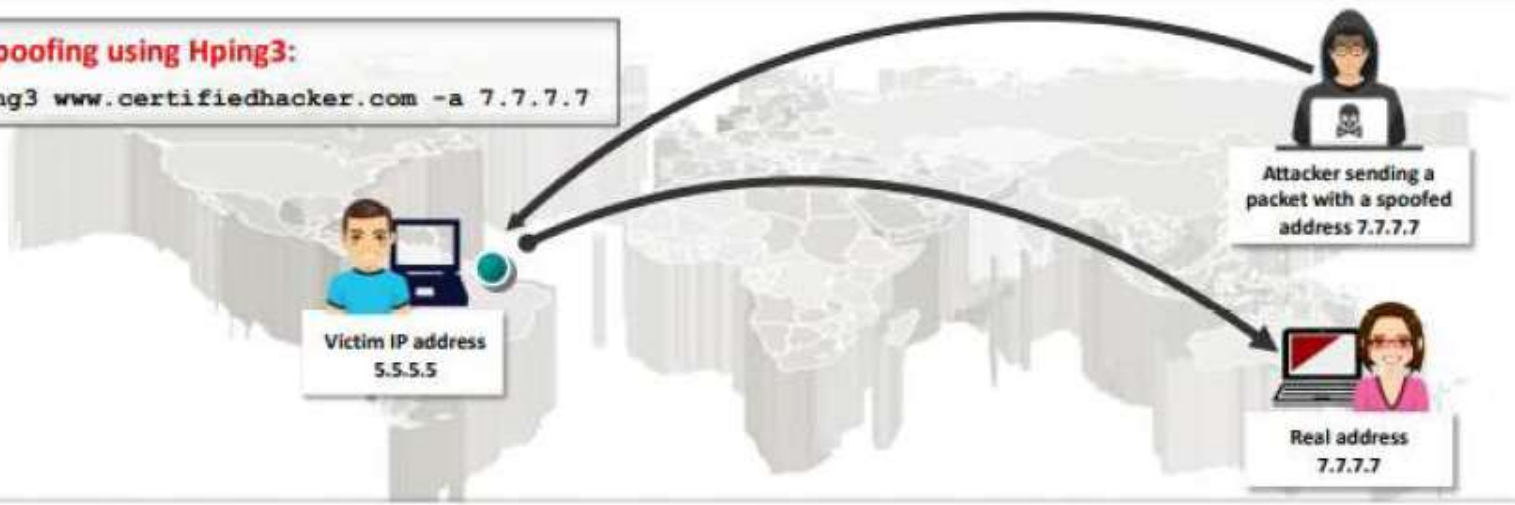


IP Address Spoofing

- IP spoofing refers to **changing the source IP addresses** so that the attack **appears to be coming from someone else**
- When the victim replies to the address, it goes back to the **spoofed address** rather than the **attacker's real address**
- Attackers modify the **address information** in the IP packet header and the source address bits field in order to bypass the IDS or firewall

IP spoofing using Hping3:

```
Hping3 www.certifiedhacker.com -a 7.7.7.7
```

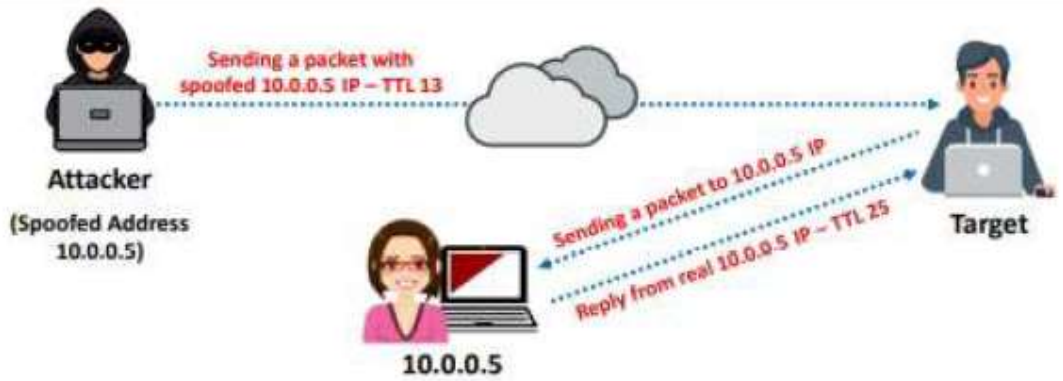


Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses

IP Spoofing Detection Techniques: Direct TTL Probes

1. Send a packet to the host of a suspected spoofed packet that triggers a reply and compare the TTL with that of the suspected packet; if the **TTL in the reply is not the same** as the packet being checked, this implies that it is a spoofed packet

2. This technique is successful when the attacker is in a **different subnet** from that of the victim



Note: Normal traffic from one host can contrast TTLs depending on traffic patterns

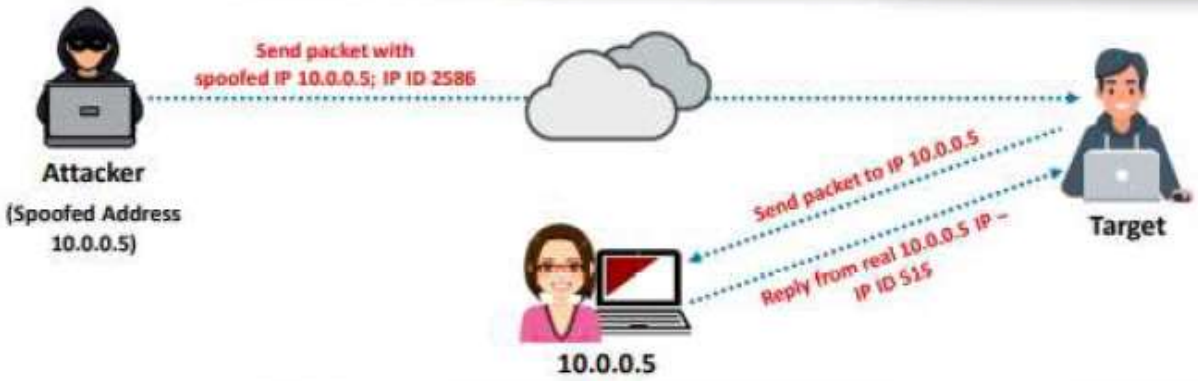
IP Spoofing Detection Techniques: IP Identification Number

C|EH

01 Send a probe to the host of a suspected spoofed traffic that triggers a reply and **compare the IPID** with the suspected traffic

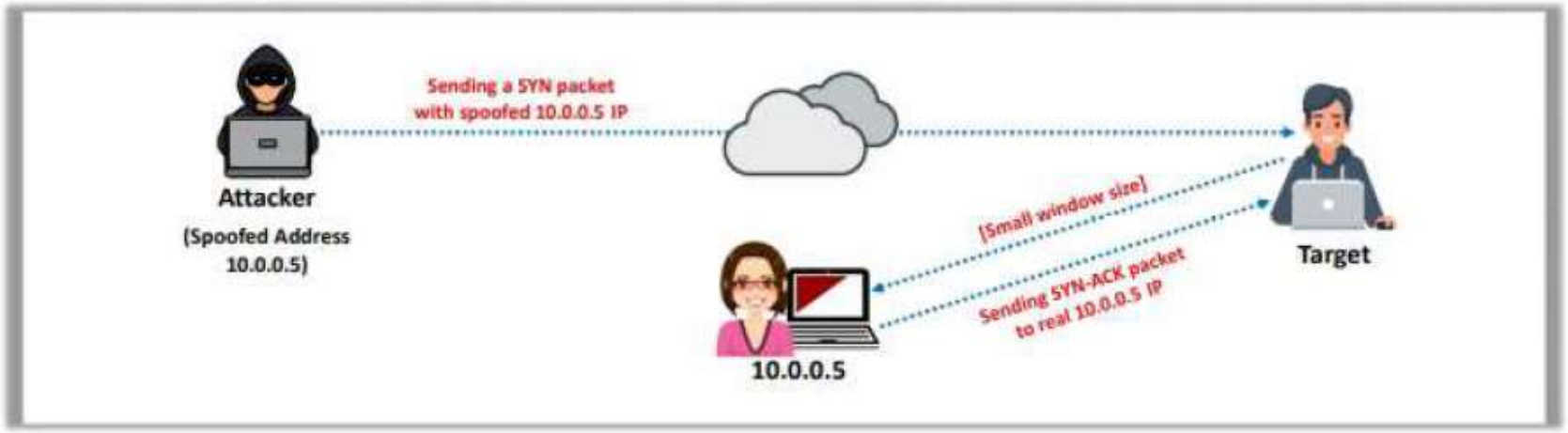
02 If the IPIDs are **not close in value** to the packet being checked, then the suspected traffic is spoofed

03 This technique is considered reliable even if the attacker is in the **same subnet**



IP Spoofing Detection Techniques: TCP Flow Control Method

- Attackers sending spoofed TCP packets will not receive the **target's SYN-ACK packets**
- Therefore, attackers cannot respond to a change in the congestion window size
- When received traffic continues after a window size is exhausted, the **packets are most likely spoofed**



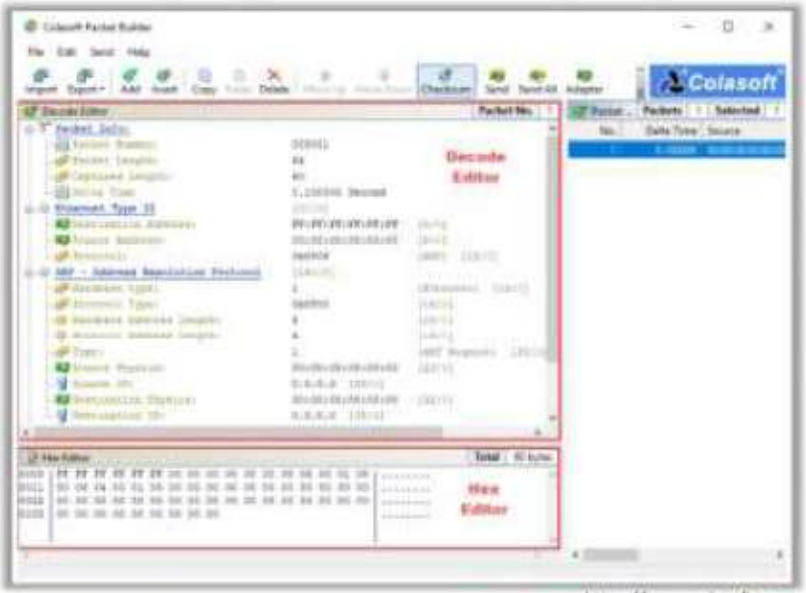
IP Spoofing Countermeasures

1. **Encrypt all the network traffic** using cryptographic network protocols such as IPsec, TLS, SSH, and HTTPS
2. **Use multiple firewalls** to provide a multi-layered depth of protection
3. Do not rely on **IP-based authentication**
4. **Use a random initial sequence number** to prevent IP spoofing attacks based on sequence number spoofing
5. **Ingress Filtering**: Use routers and firewalls at your network perimeter to filter incoming packets that appear to come from an internal IP address
6. **Egress Filtering**: Filter all outgoing packets with an invalid local IP address as the source address

Creating Custom Packets

Creating Custom Packets by using Packet Crafting Tools

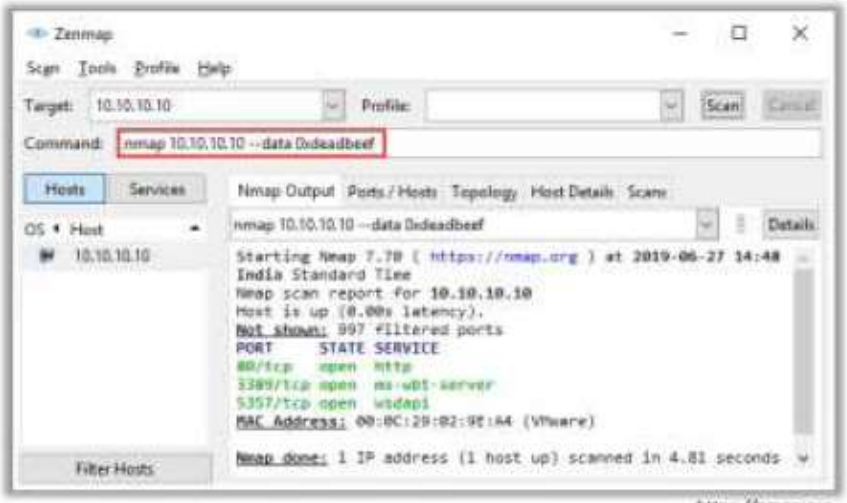
- Attackers **create custom TCP packets** using various packet crafting tools like **Colasoft Packet Builder**, **NetScanTools Pro**, etc. to scan a target beyond a firewall



https://www.colasoft.com

Creating Custom Packets by Appending Custom Binary Data

- Attackers send binary data (**0's and 1's**) as payloads in transmitted packets to scan beyond firewalls
- Example: **--data 0xdeadbeef**

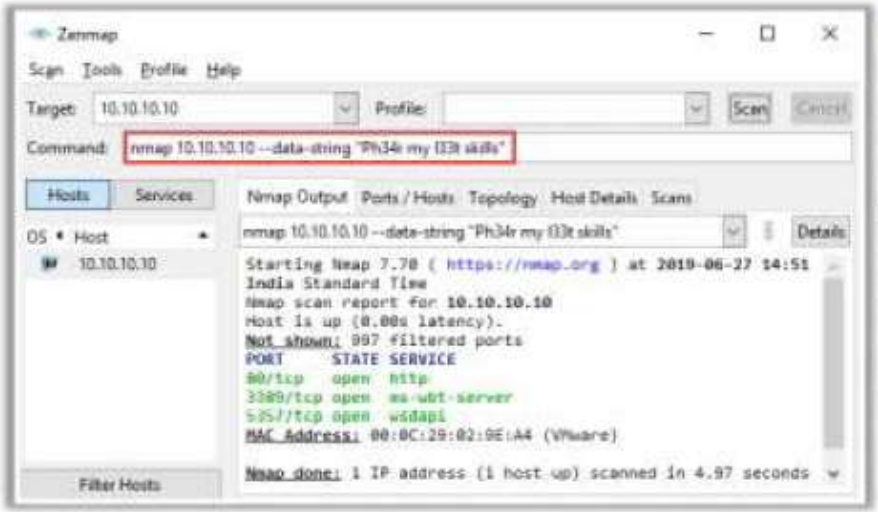


https://nmap.org

Creating Custom Packets (Cont'd)

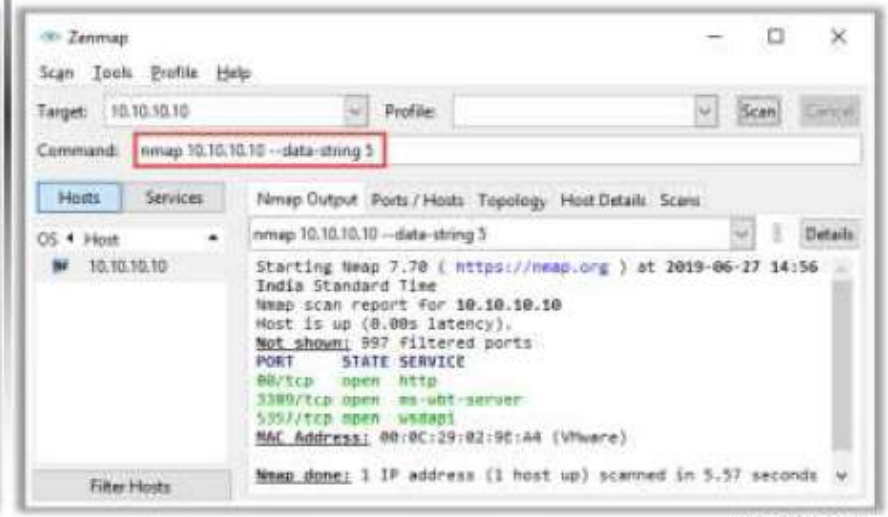
Creating Custom Packets by Appending Custom String

- Attackers send a **regular string as payloads** in the packets sent to the target machine for scanning beyond the firewall
- Example: **--data-string "Ph34r my l33t skills"**



Creating Custom Packets by Appending Random Data

- Attackers **append a number of random data bytes** to most of the packets sent without any protocol-specific payloads
- Example: **--data-string 5**



https://nmap.org

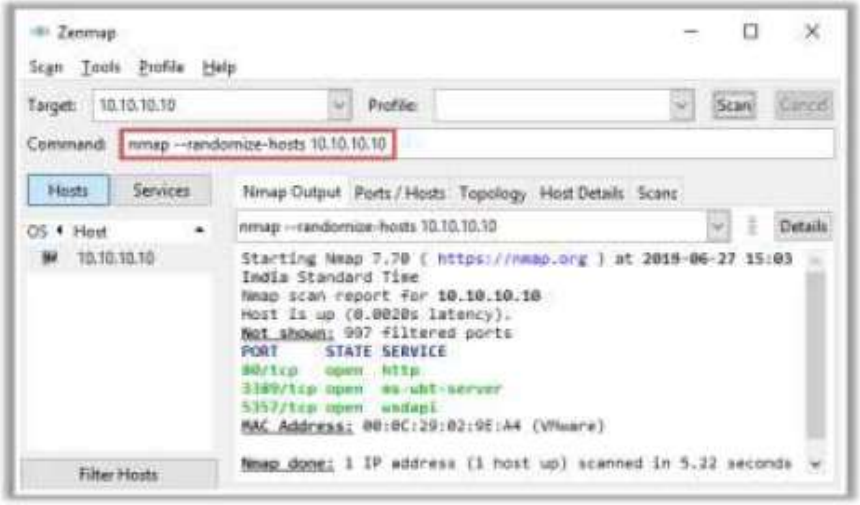
Randomizing Host Order and Sending Bad Checksums

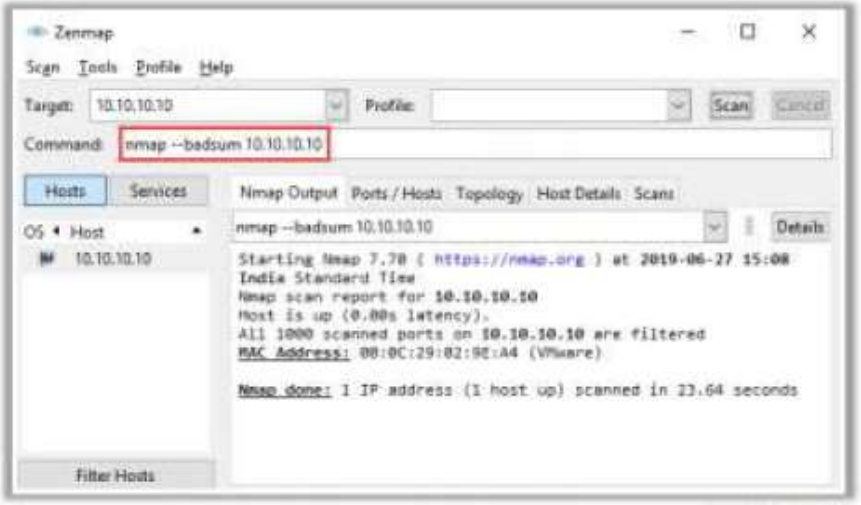
Randomizing Host Order

- Attackers **scan the number of hosts** in the target network **in random order** to scan an intended target that is behind a firewall

Sending Bad Checksums

- Attackers send packets with bad or bogus **TCP/UPD checksums** to the intended target to avoid certain firewall rulesets





https://nmap.org

Proxy Servers

A proxy server is an application that can **serve as an intermediary** for connecting with other computers

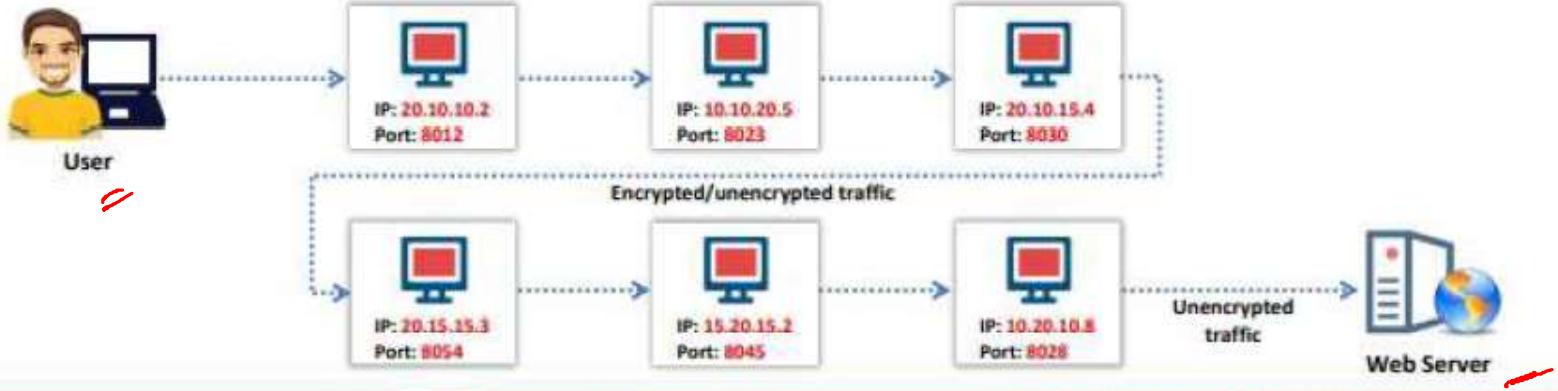
Why Attackers Use Proxy Servers?

1. To hide the actual source of a scan and **evade certain IDS/firewall restrictions**
2. To **mask the actual source** of an attack by impersonating the fake source address of the proxy
3. To **remotely access intranets** and other **website resources** that are normally restricted
4. To **interrupt all requests** sent by a user and transmit them to a third destination such that victims can only identify the proxy server address
5. To chain **multiple proxy servers** to avoid detection

Note: A search in **Google** will list thousands of **free proxy servers**

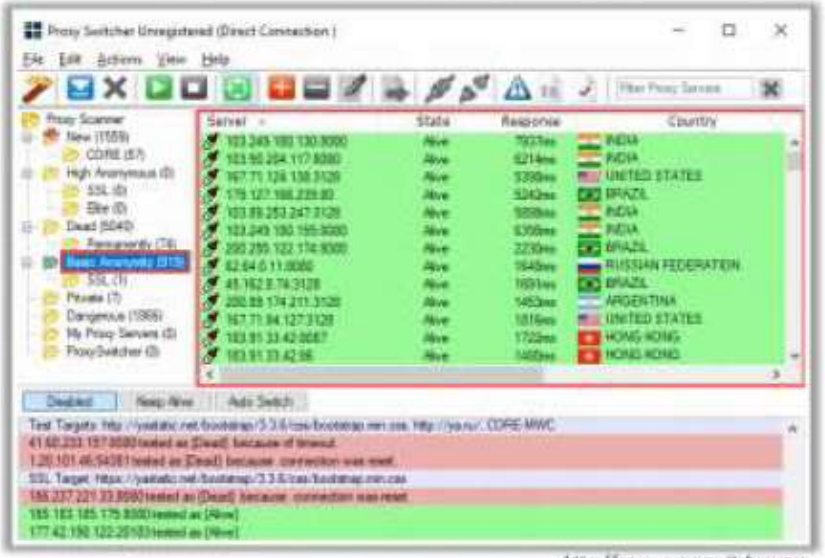
Proxy Chaining

1. User **requests a resource** from the destination
2. Proxy client at the user's system connects to a **proxy server** and passes the request to proxy server
3. The proxy server **strips the user's identification information** and passes the request to next proxy server
4. This process is repeated by all the proxy servers in the **chain**
5. At the end, the **unencrypted request** is passed to the web server



Proxy Tools

Proxy Switcher | Proxy Switcher allows you to **surf anonymously on the Internet** without disclosing your IP address



http://www.proxyswitcher.com

CyberGhost VPN | CyberGhost VPN **hides your IP** and replaces it with one of your choice, thus allowing you to surf anonymously

https://www.cyberghostvpn.com

Other Proxy Tools:

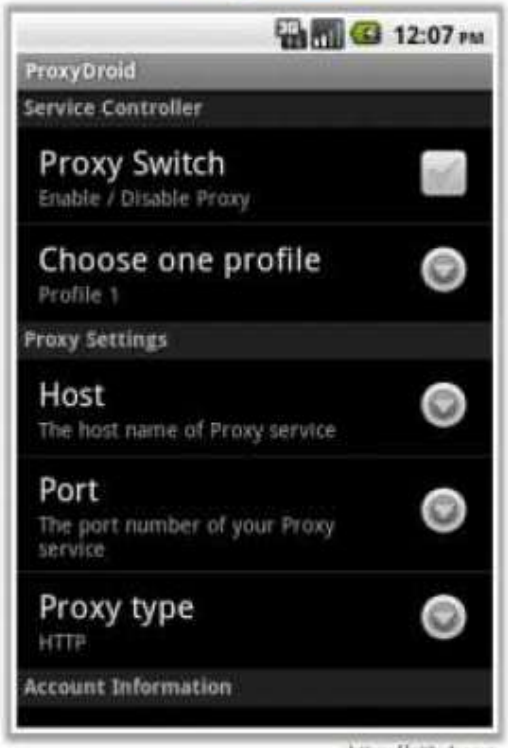
- **Burp Suite** — https://www.portswigger.net
- **Tor** — https://www.torproject.org
- **CCProxy** — https://www.youngzsoft.net
- **Hotspot Shield** — https://www.hotspotshield.com

Proxy Tools for Mobile

Shadowsocks

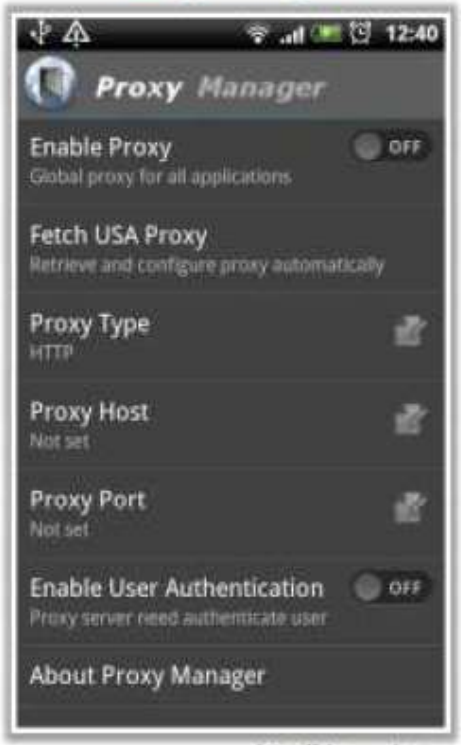
https://shadowsocks.org

ProxyDroid



https://github.com

Proxy Manager



https://play.google.com

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

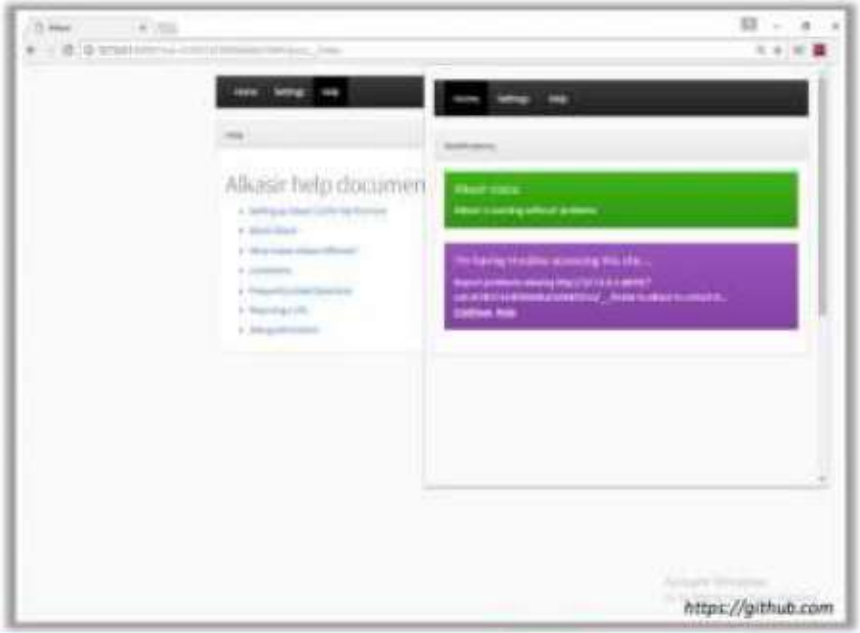
Why use an Anonymizer?

1. Privacy and anonymity
2. Protection against online attacks
3. Access restricted content
4. Bypass IDS and Firewall rules

Censorship Circumvention Tools: Alkasir and Tails

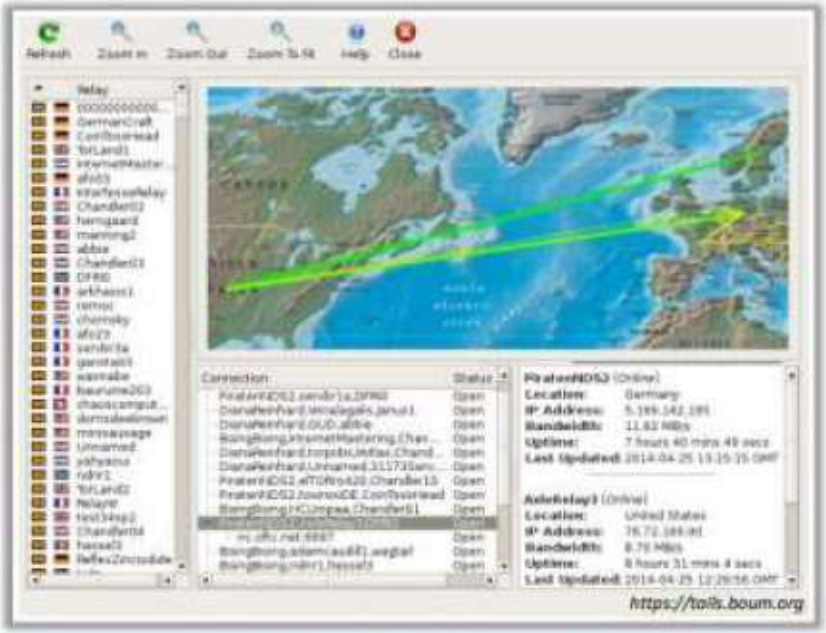
Alkasir

Alkasir is a **cross-platform**, open-source, and robust website censorship circumvention tool that also **maps censorship patterns** around the world



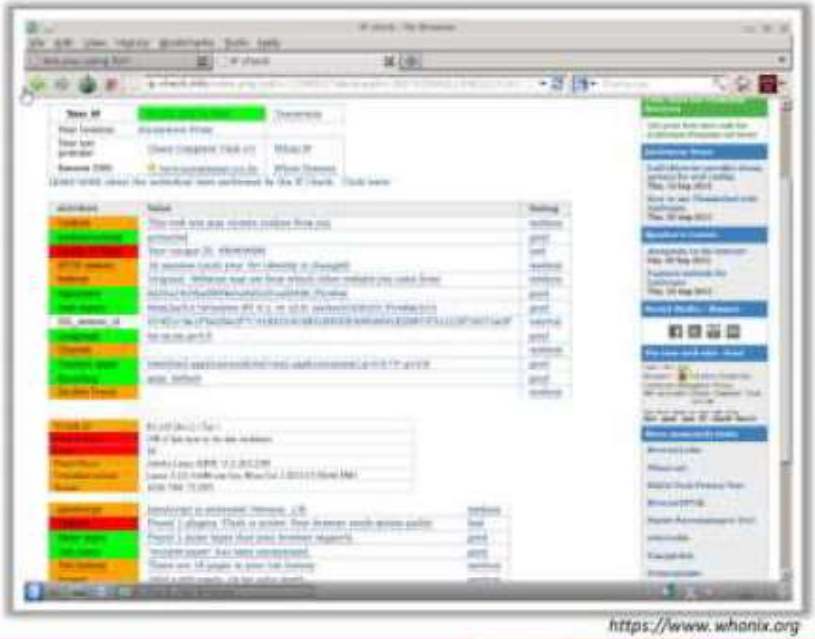
Tails

Tails is a **live operating system** that a user can start on any computer from a DVD, USB stick, or SD card



Anonymizers

Whonix | Whonix is a **desktop operating system** designed for advanced security and privacy



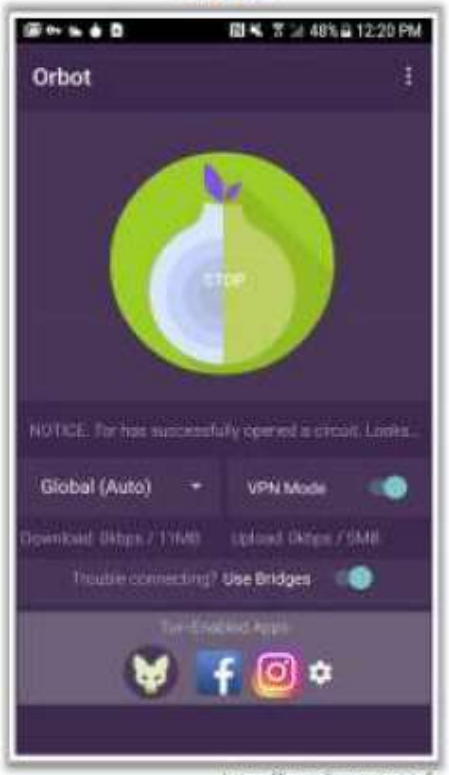
https://www.whonix.org

Psiphon | Psiphon is an open-source anonymizer software that allows attackers to surf the internet through a **secure proxy**

https://psiphon.ca

Anonymizers for Mobile

Orbot



https://guardianproject.info

Psiphon

https://psiphon.ca

OpenDoor

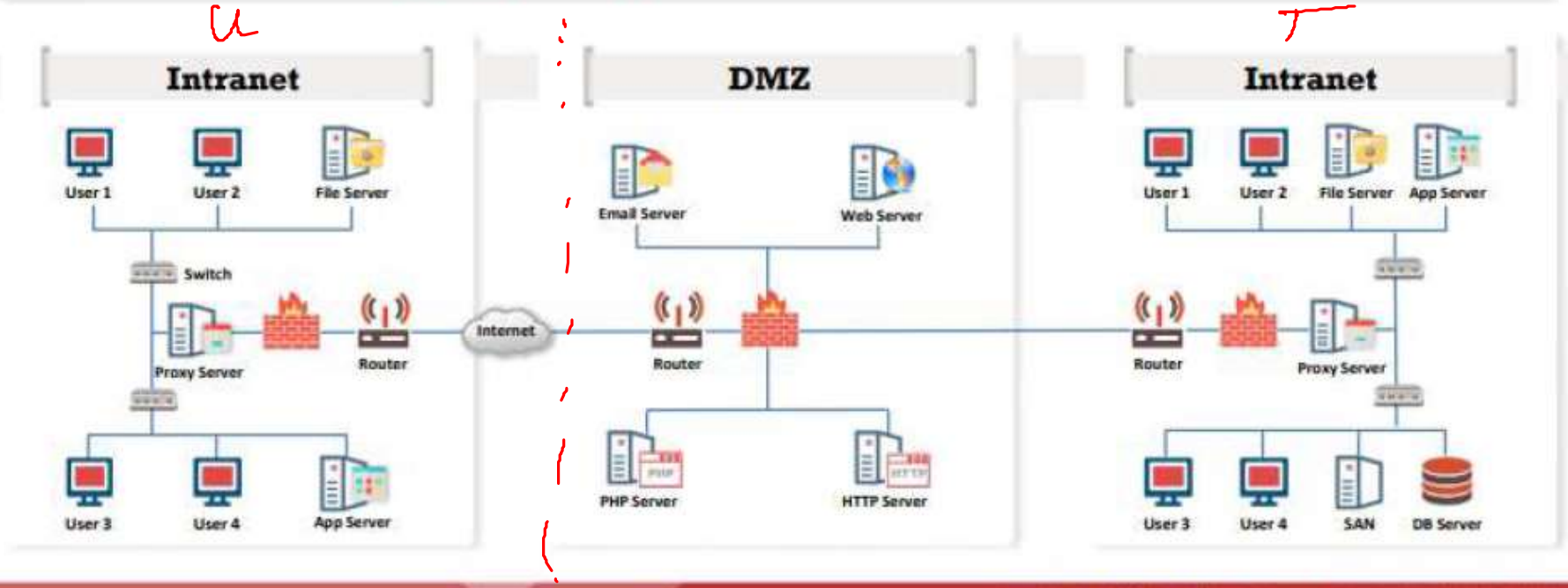
https://www.apple.com

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

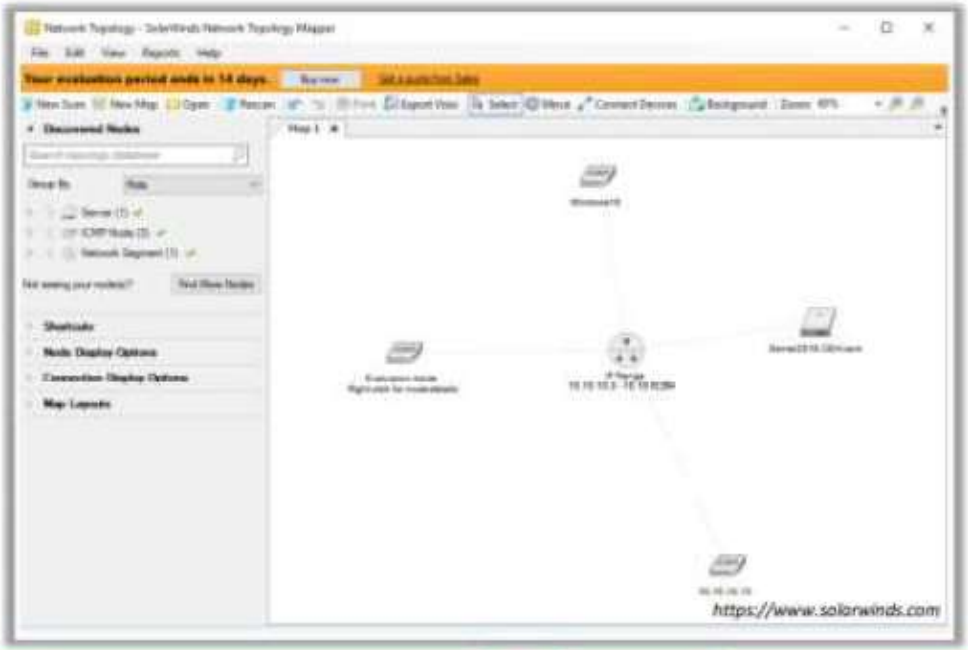
- A diagram of a target network provides an attacker with valuable information about the **network and its architecture**
- Network diagrams show **logical or physical paths** to a potential target



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

Network Discovery Tools for Mobile

Scany

http://happymagenta.com

Network Analyzer

https://play.google.com

PortDroid Network Analysis

https://play.google.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