
EC-Council
C|EH
Certified Ethical Hacker
Module 03
Scanning Networks

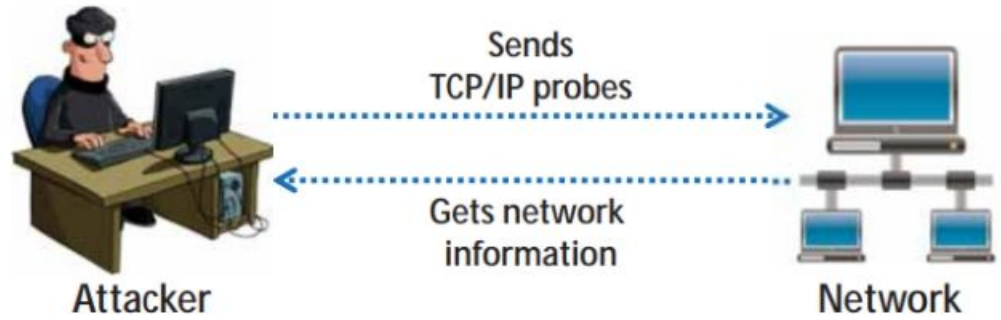
Module Flow

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

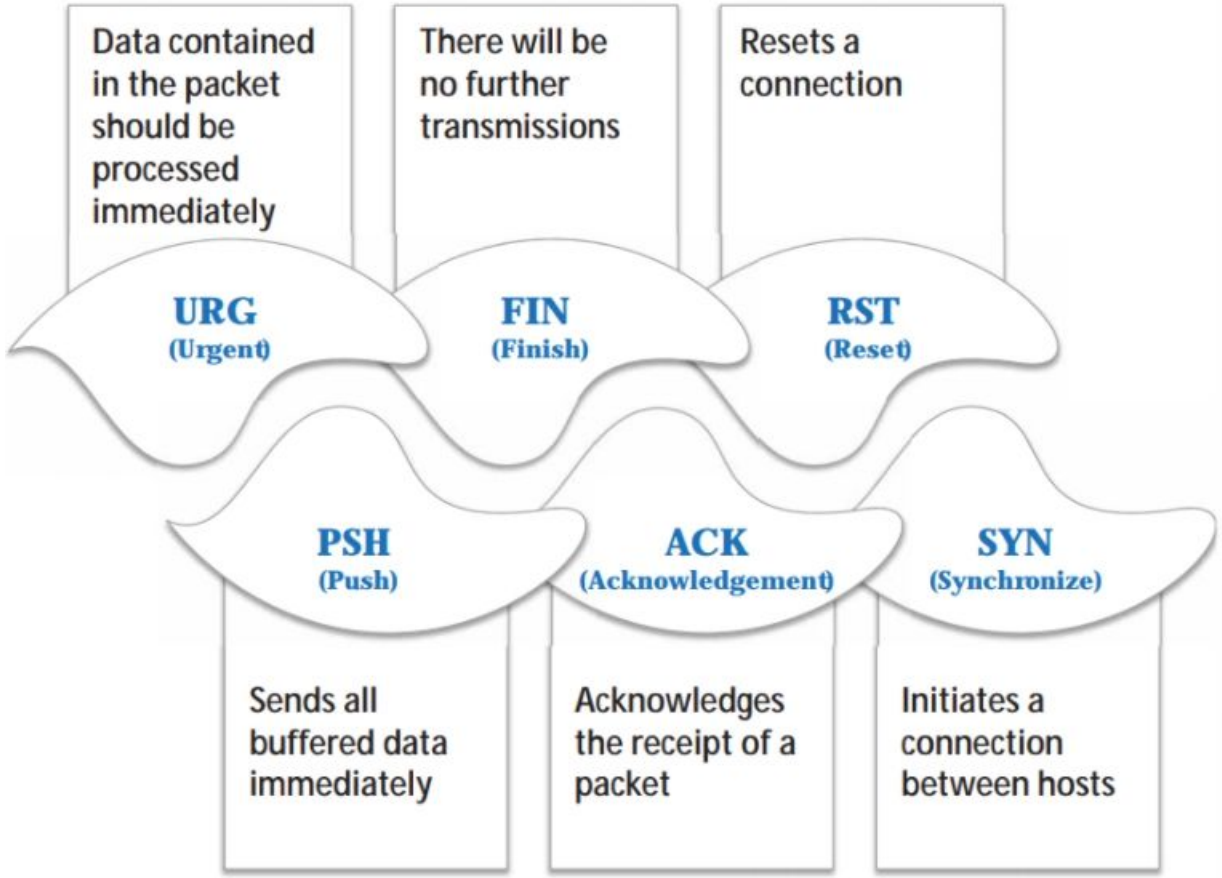
Network Scanning Process

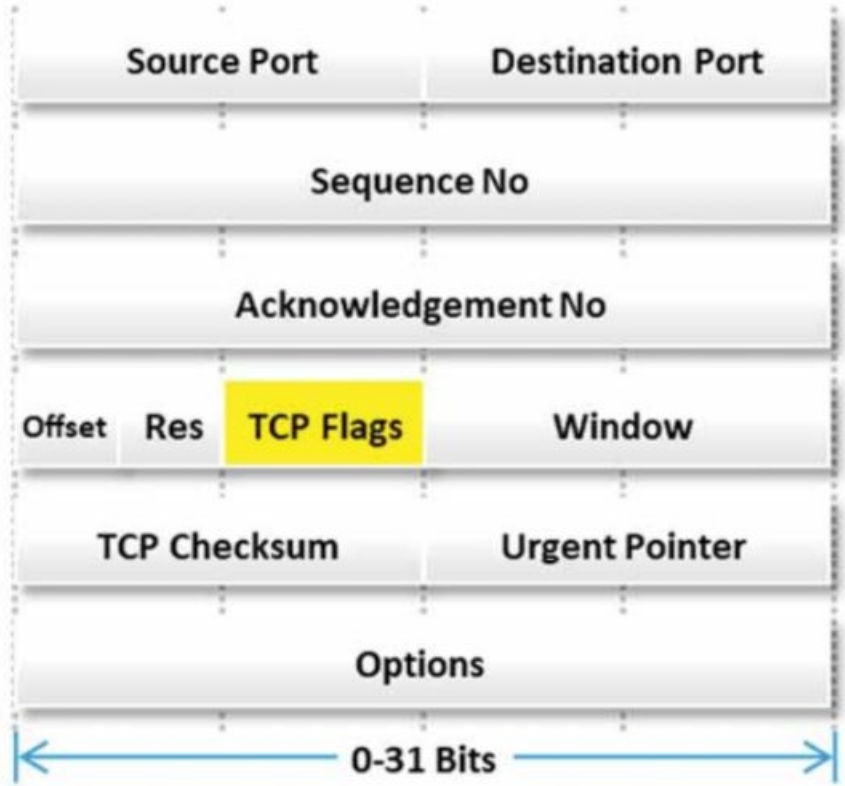


Objectives of Network Scanning

- 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



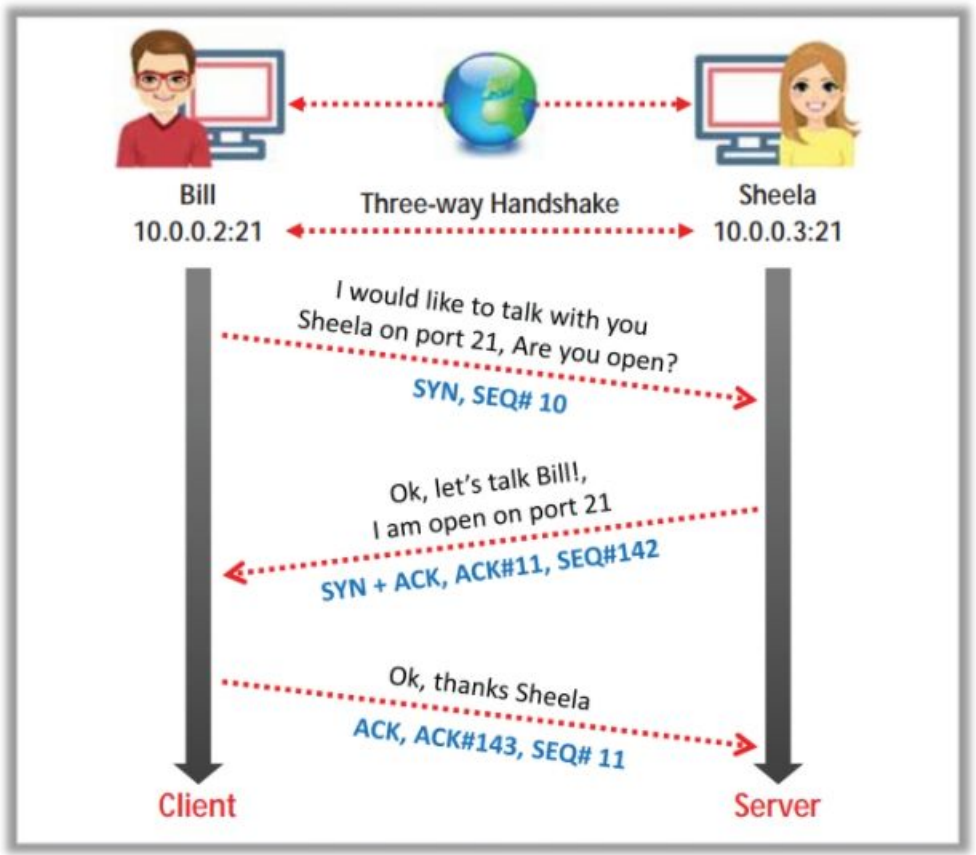


Standard TCP communications are controlled by flags in the TCP packet header

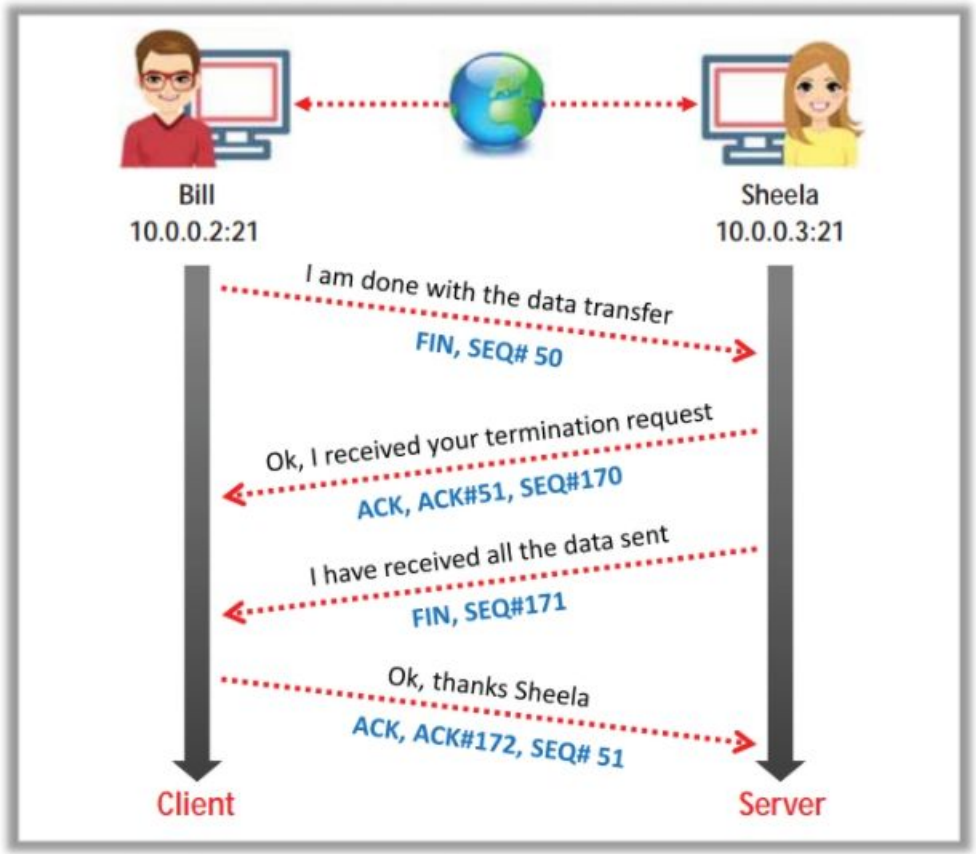
TCP/IP Communication

TCP Session Establishment

(Three-way Handshake)



TCP Session Termination

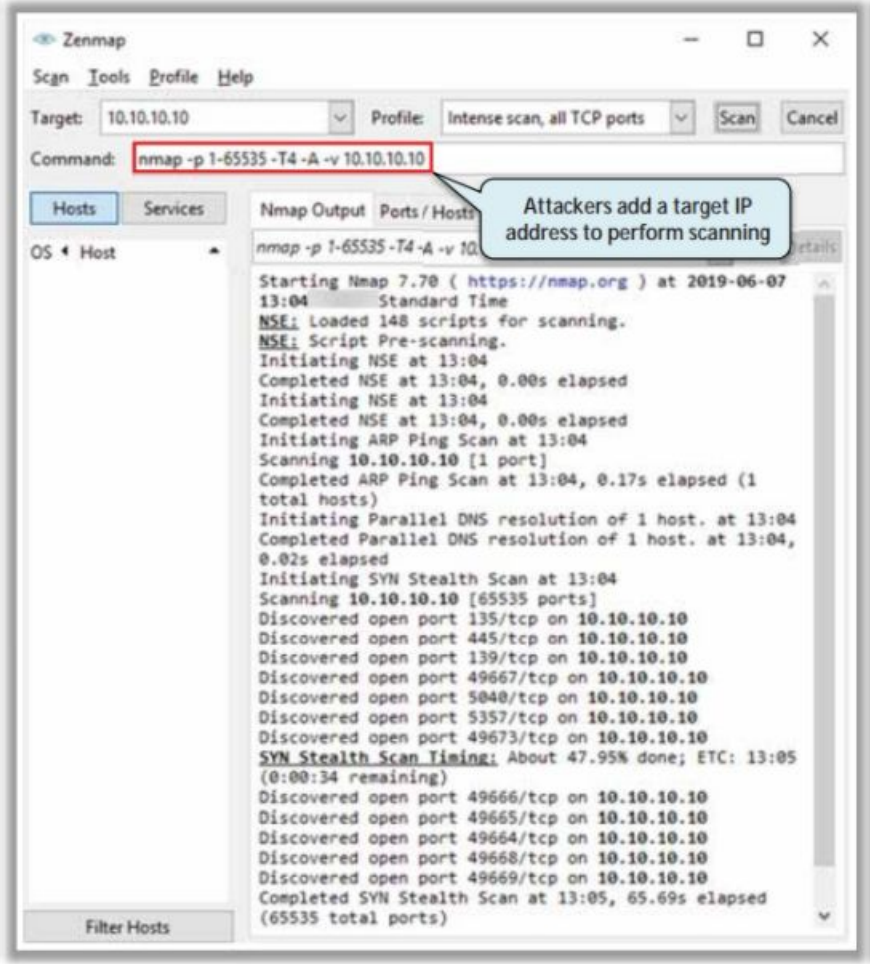


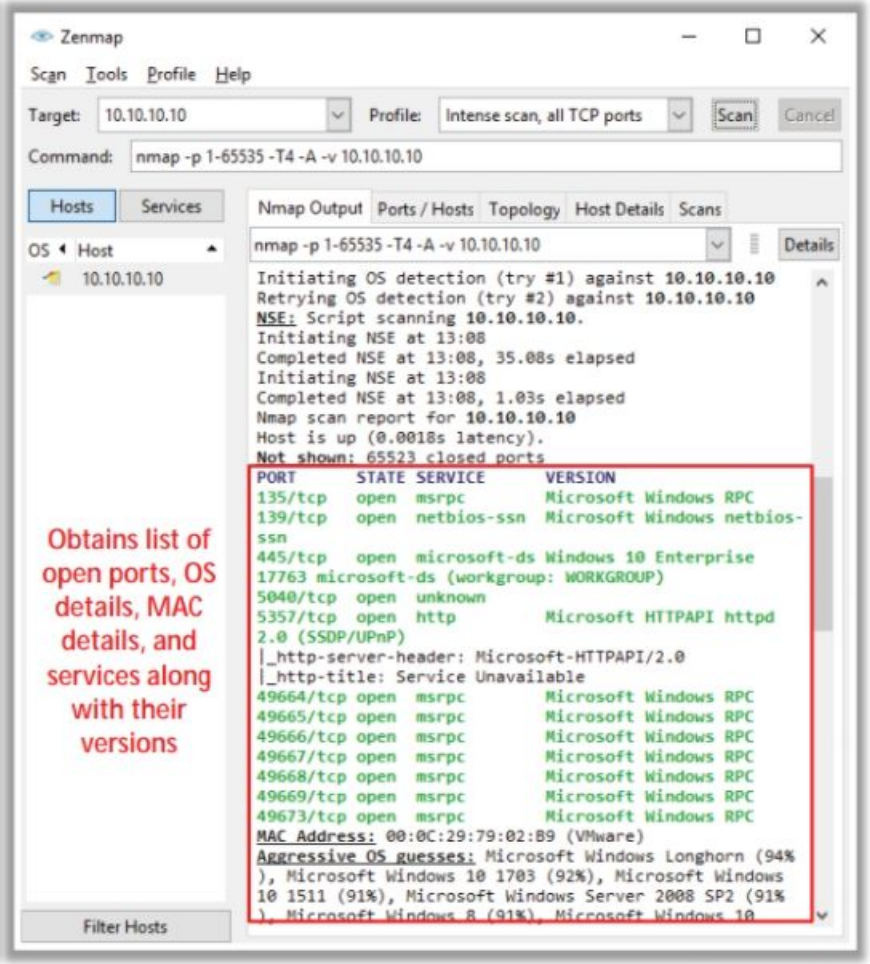
Module Flow

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





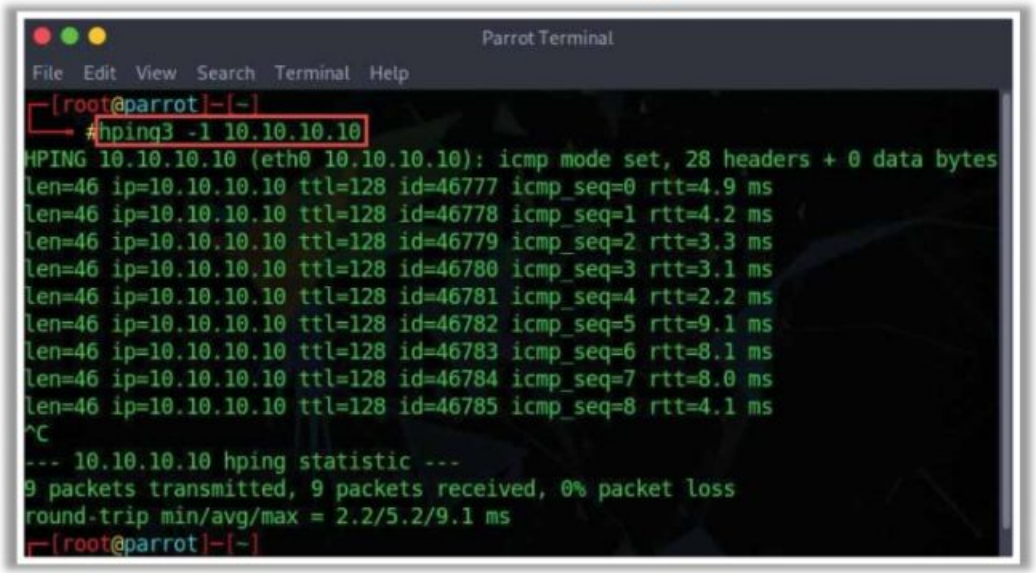
https://nmap.org

Scanning Tools: Hping2/Hping3

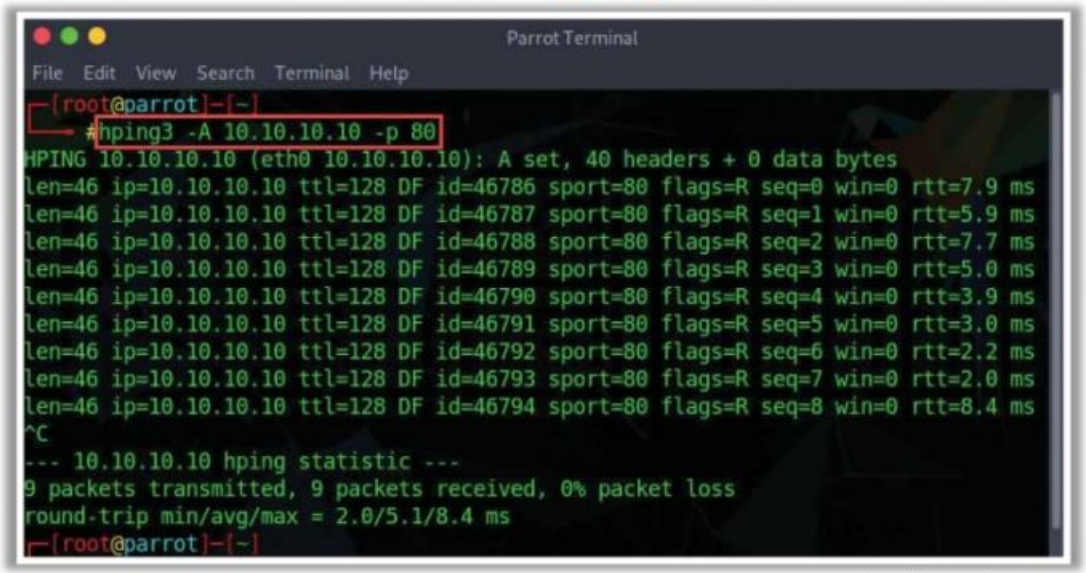
1. Command line network scanning and packet crafting tool for the TCP/IP protocol

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

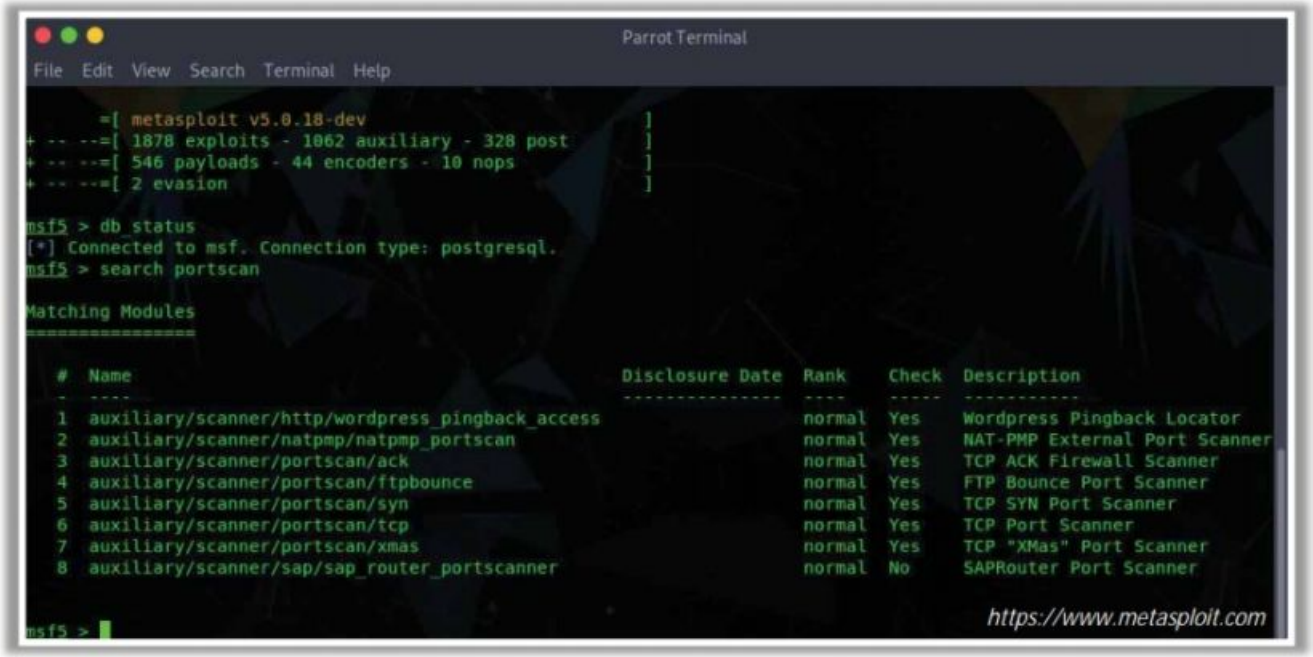


http://www.hping.org

Scanning Tools

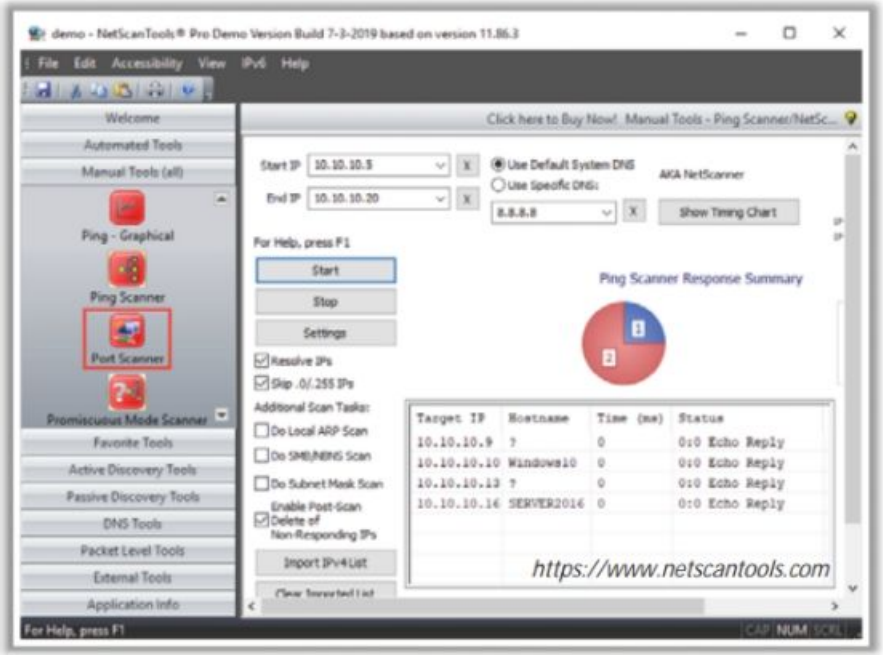
Metasploit

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

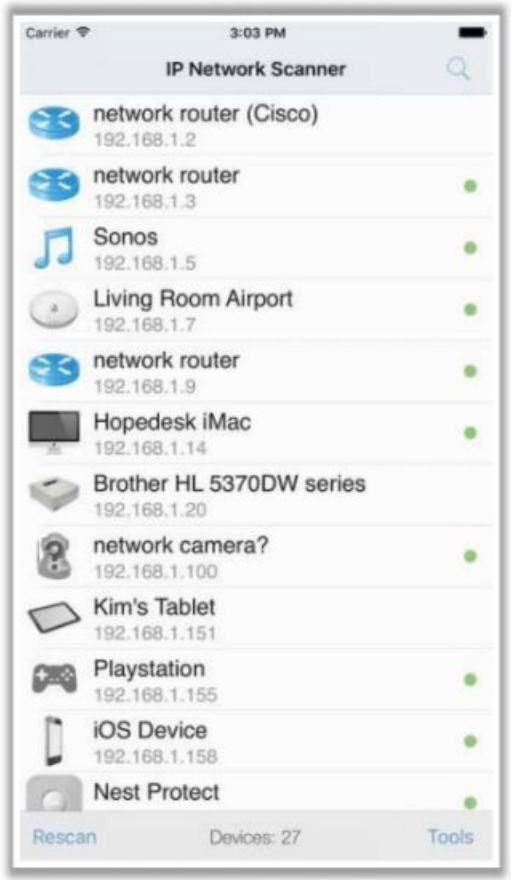


Other Scanning Tools:

- 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*

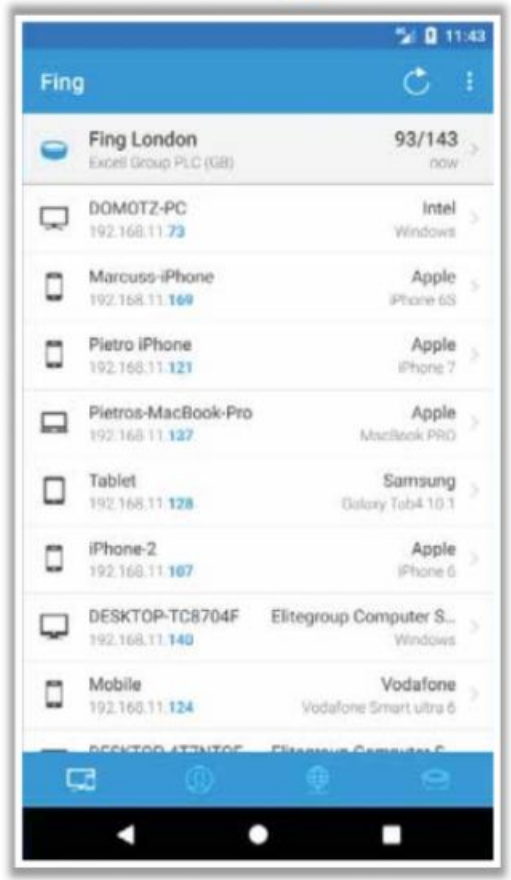
Scanning Tools for Mobile

IP Scanner



https://10base-t.com

Fing



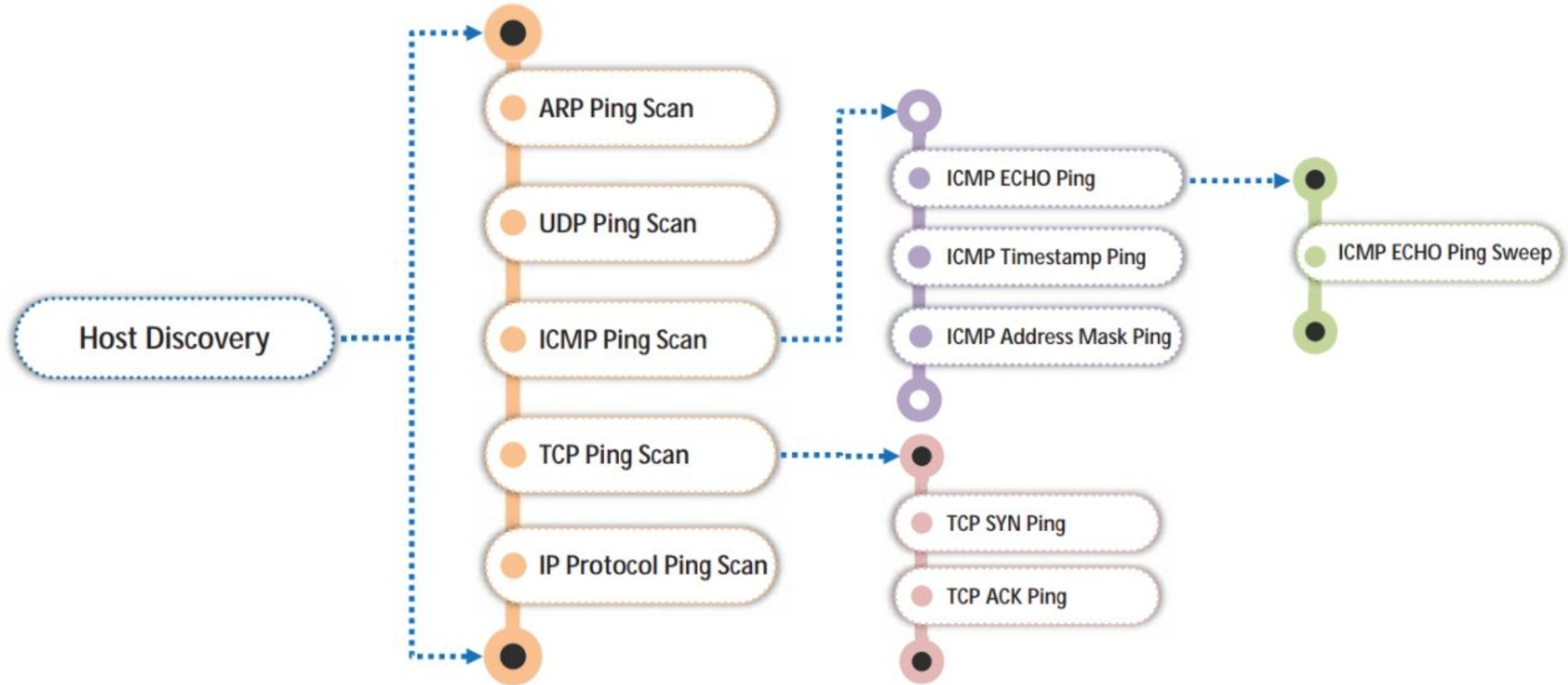
https://www.fing.io

Network Scanner

https://play.google.com

Host Discovery Techniques

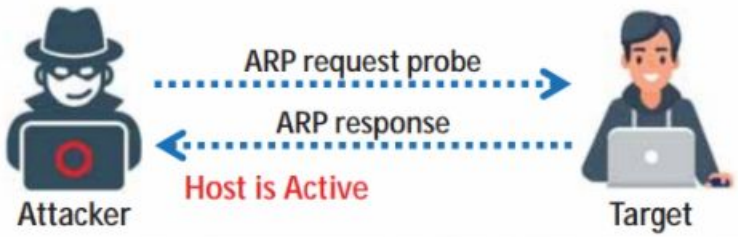
- Host discovery techniques are used to identify the active/live systems in the network

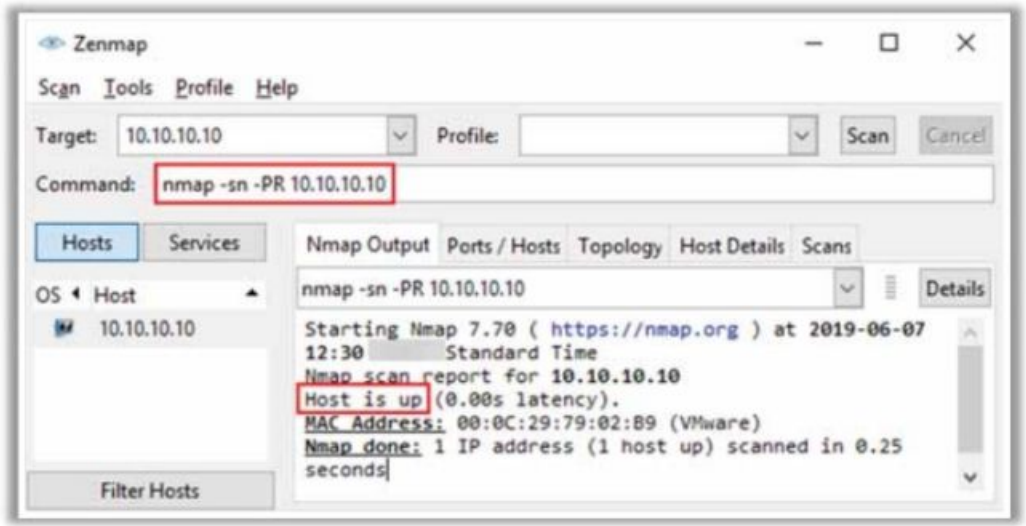


ARP Ping Scan and UDP Ping Scan

ARP Ping Scan

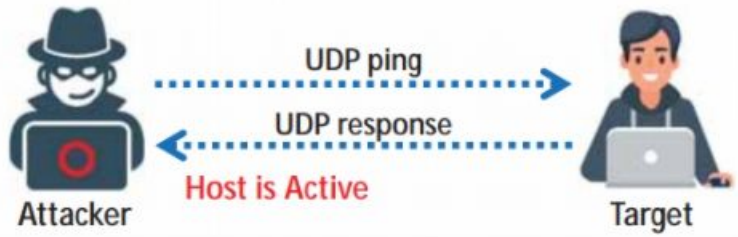
- Attackers send ARP request probes to target hosts, and an ARP response indicates that the host is active

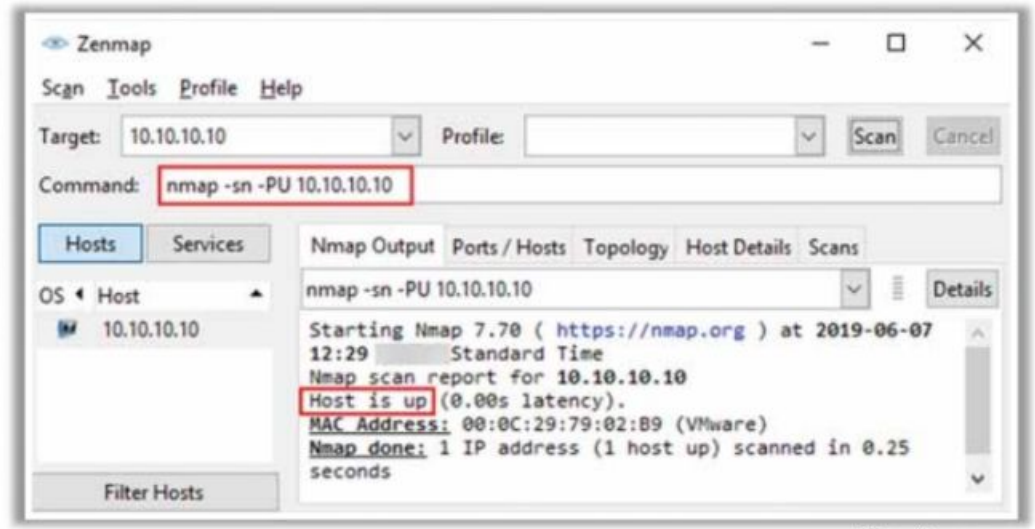




UDP Ping Scan

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



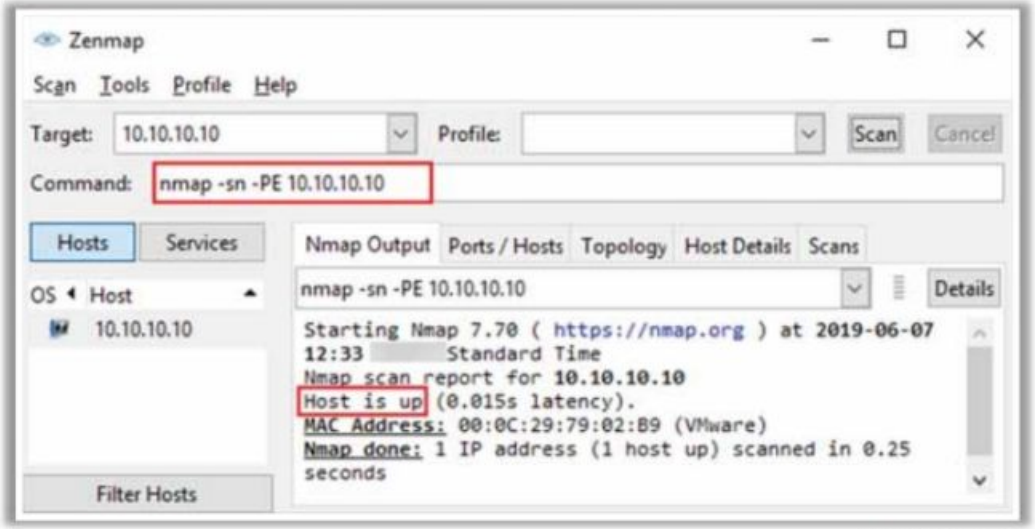


https://nmap.org

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

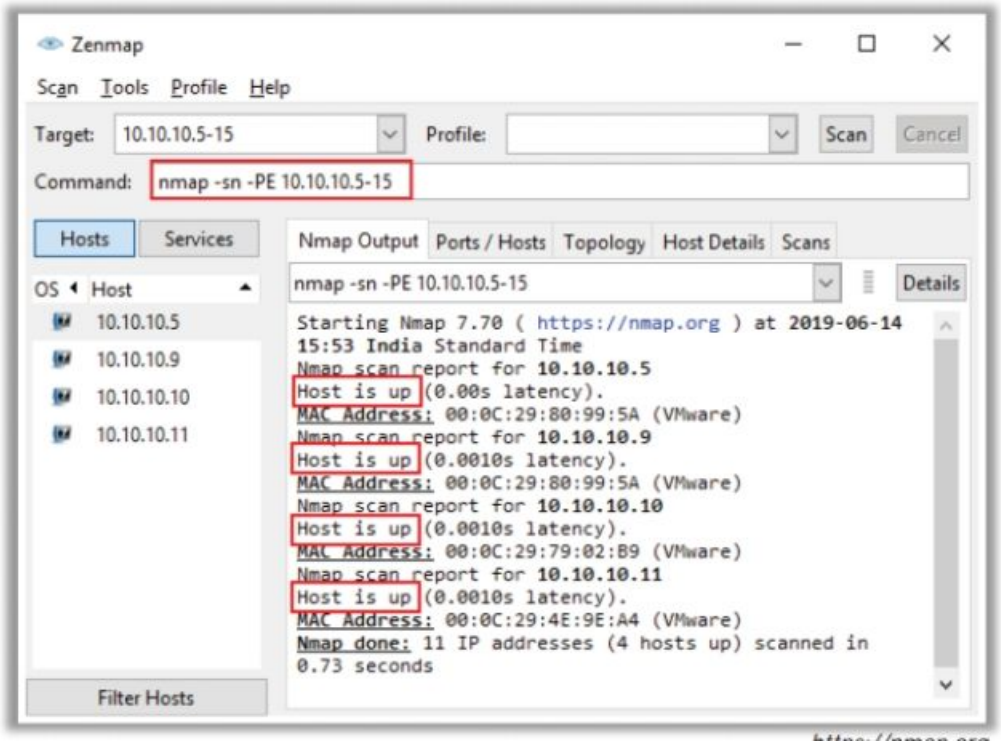
ICMP Echo ping scan outputusing Zenmap

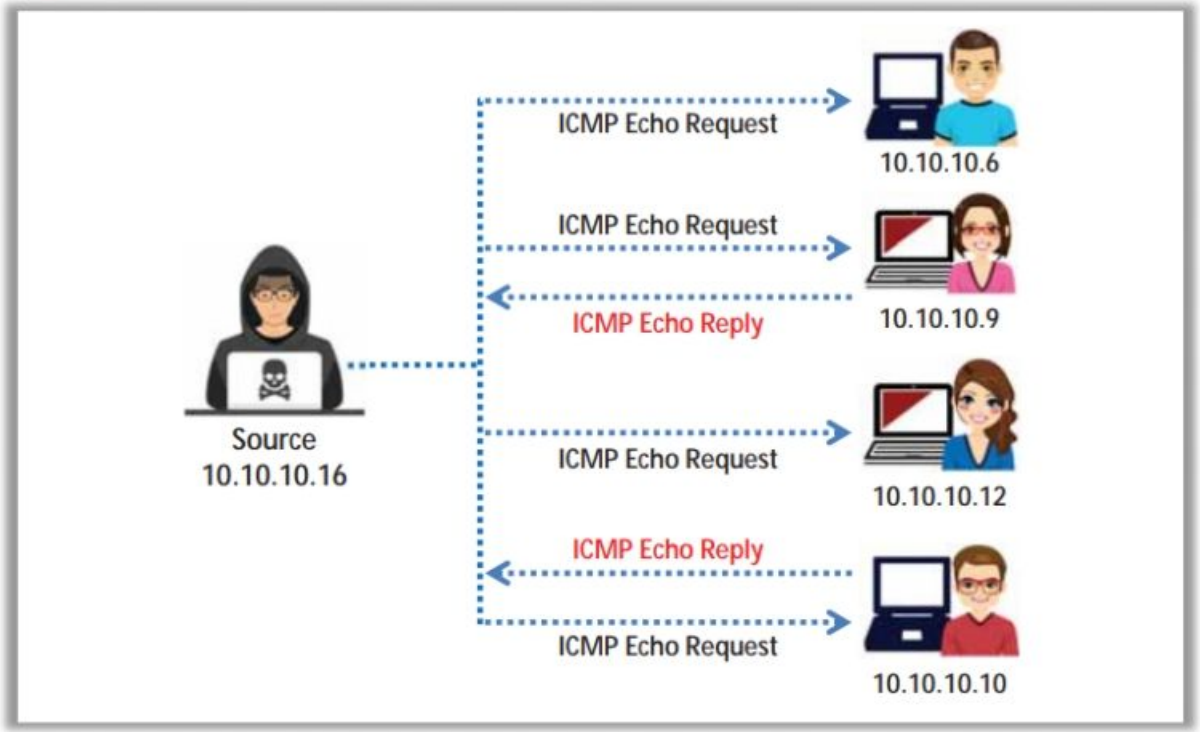


https://nmap.org

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





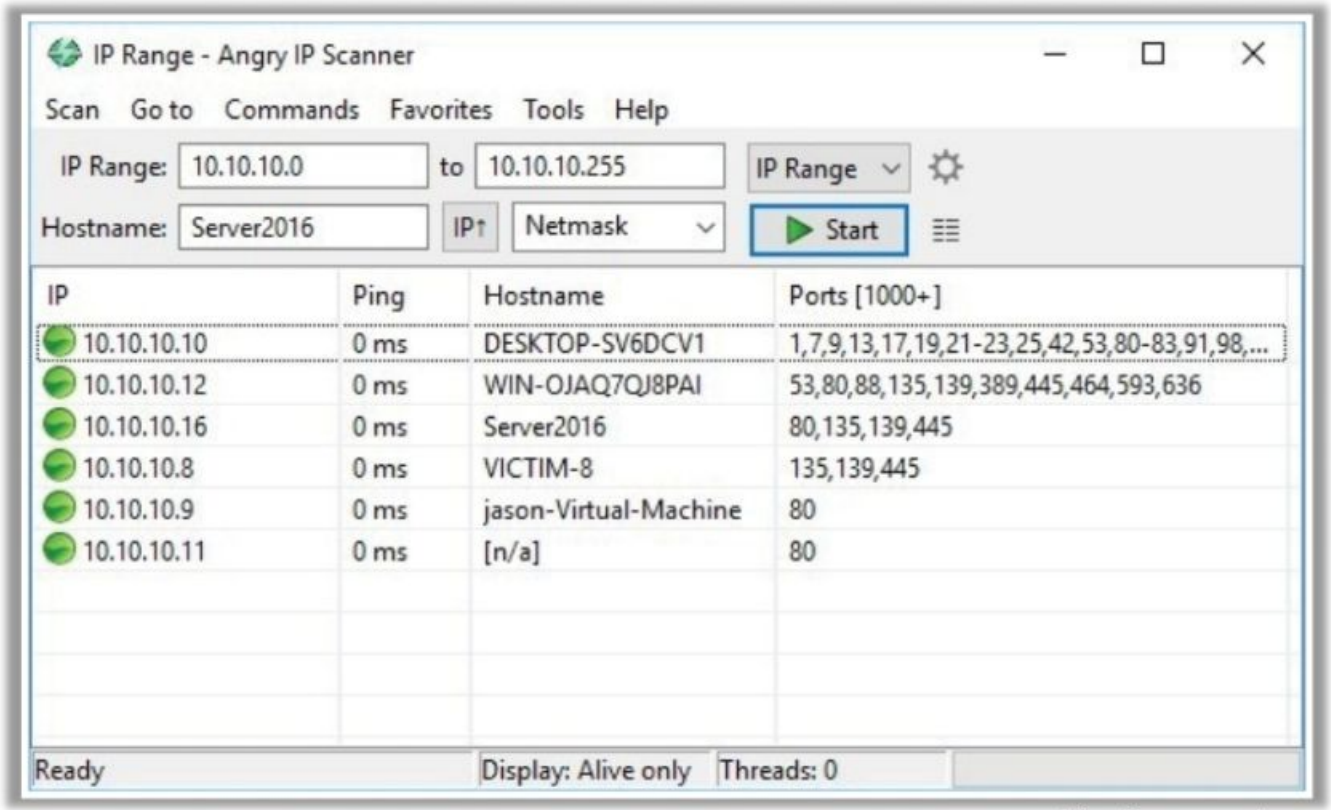
Ping Sweep Tools

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*)



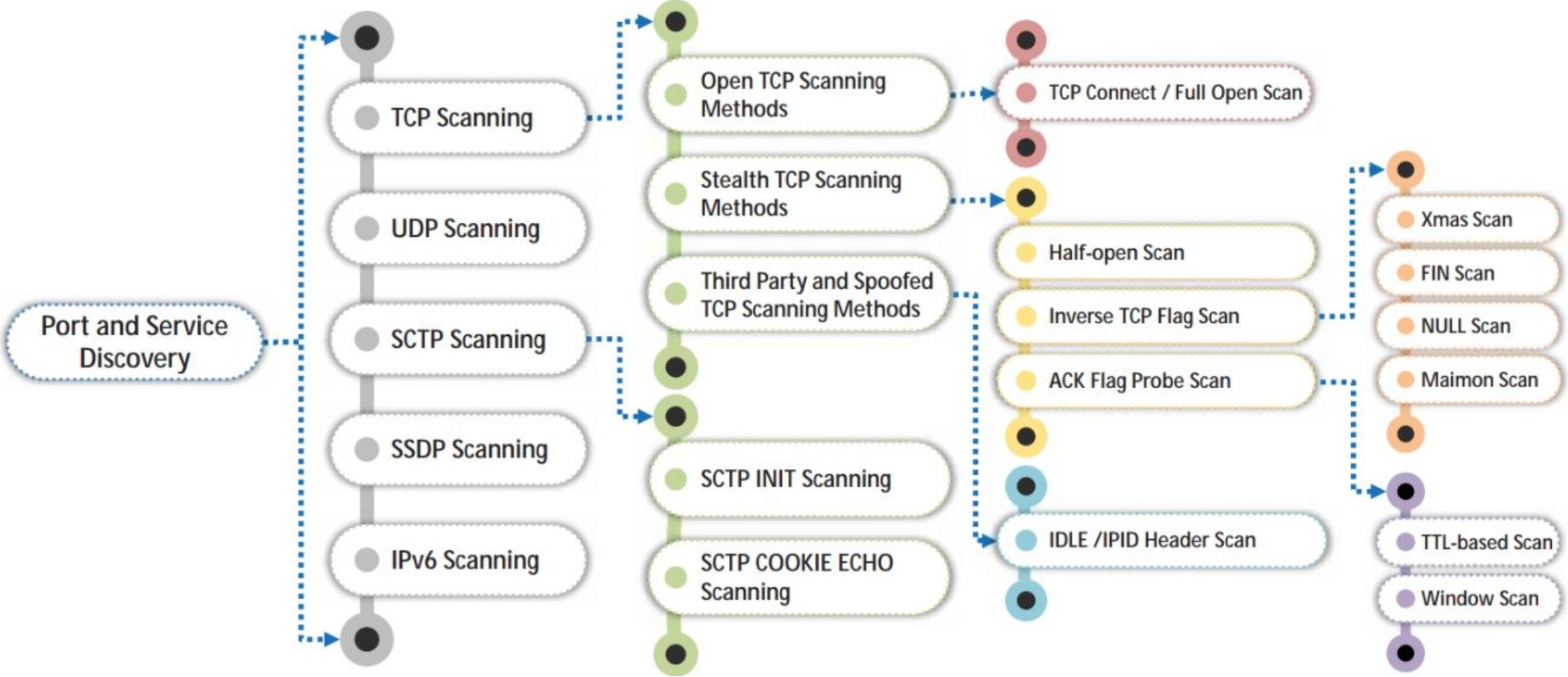
https://www.angryip.org

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

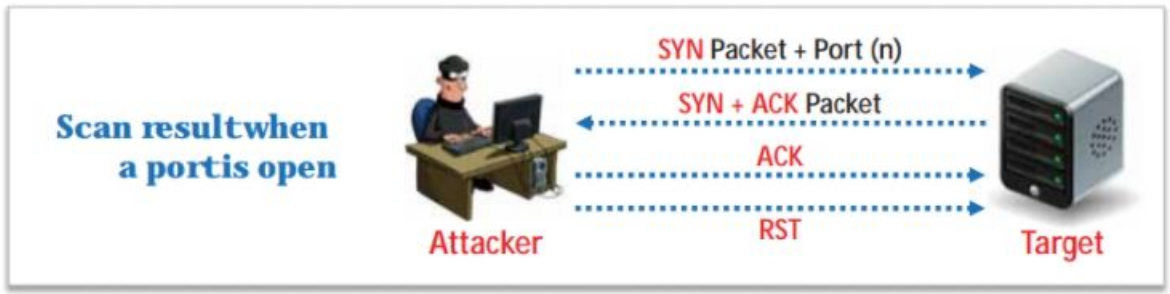
Port Scanning Techniques

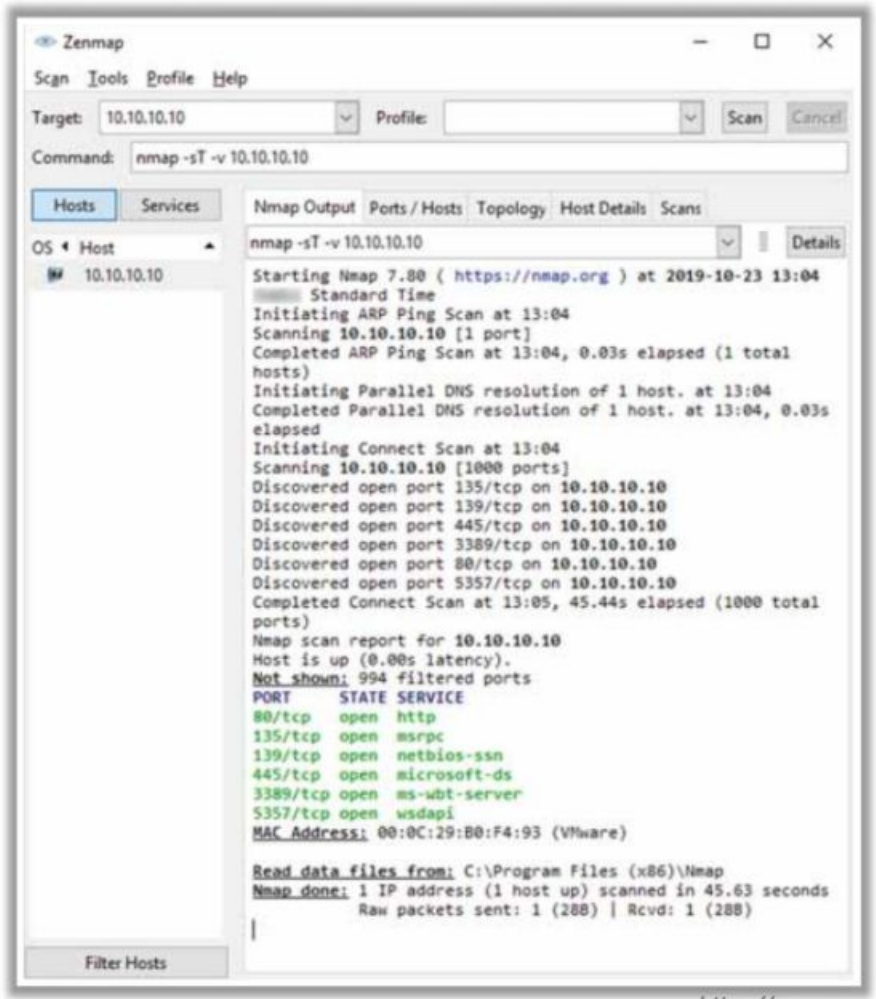
- The port scanning techniques are categorized according to the type of protocol used for communication



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



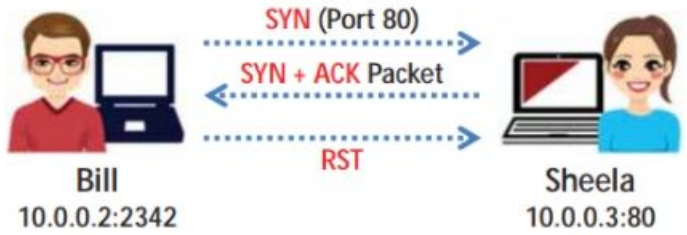


https://nmap.org

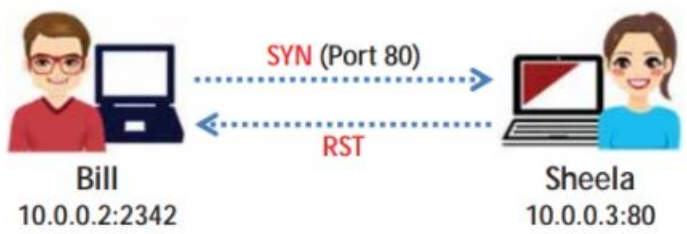
Stealth Scan (Half-open Scan)

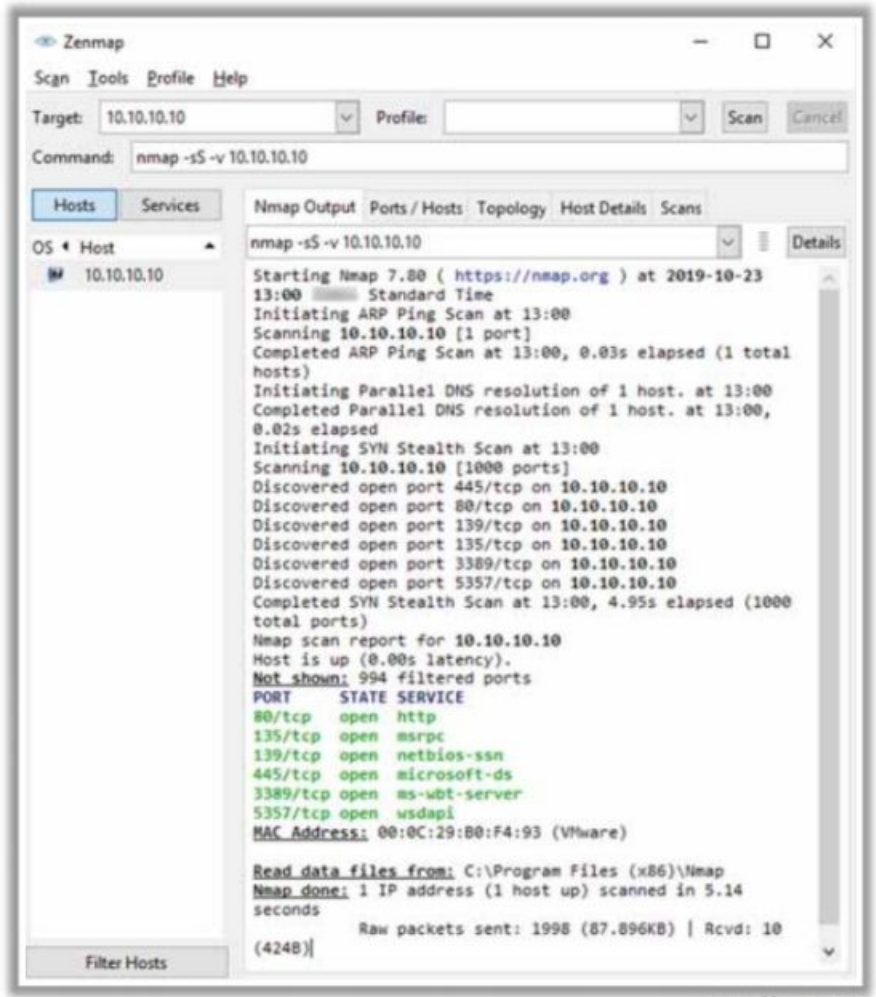
- Stealth scanning involves abruptly resetting the TCP connection between the client and server before the completion of three-way handshake signals, thus leaving the connection half-open
- Attackers use stealth scanning techniques to bypass firewall rules as well as logging mechanisms, and hide themselves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

Scan result when a port is open



Scan result when a port is closed



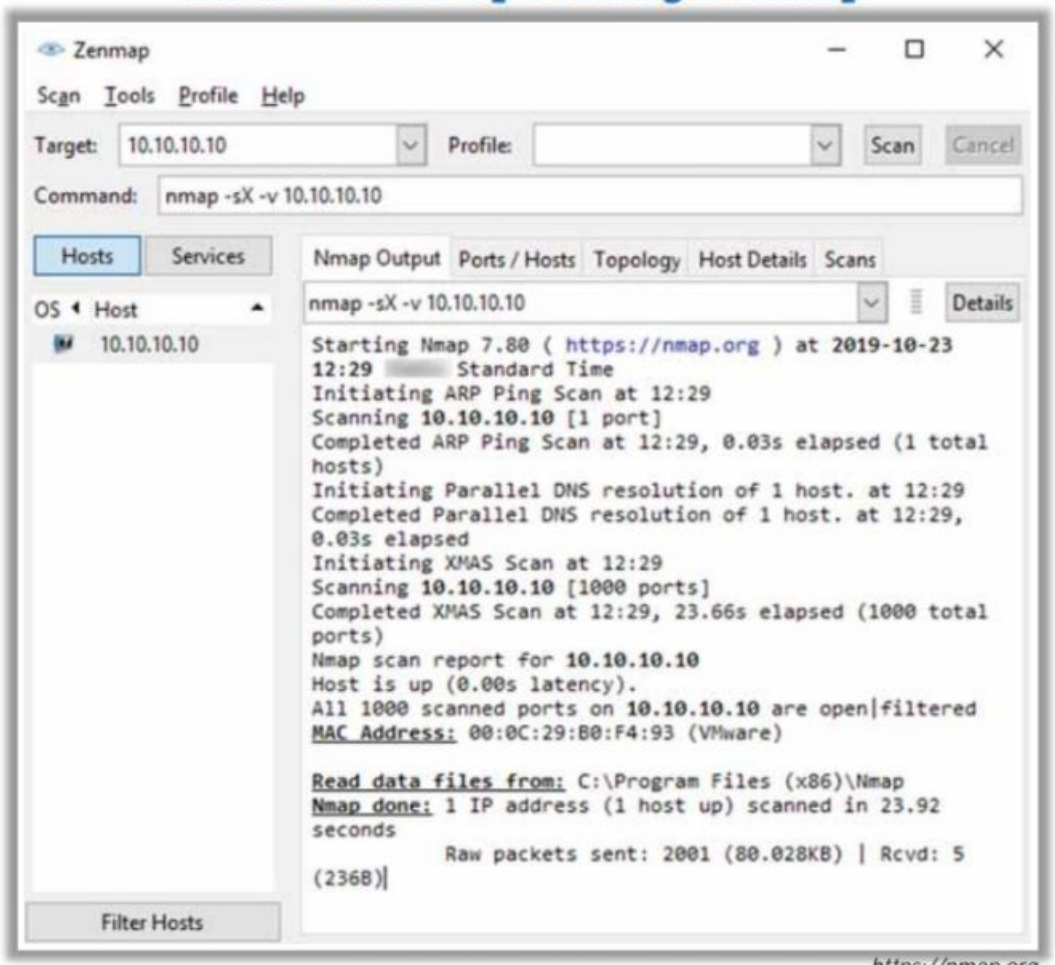


https://nmap.org

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

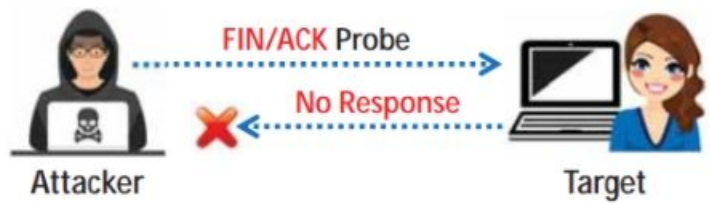
Xmas scan output using Zenmap

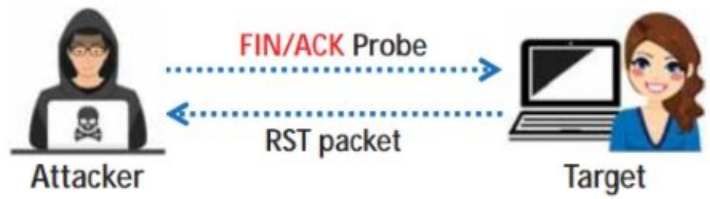


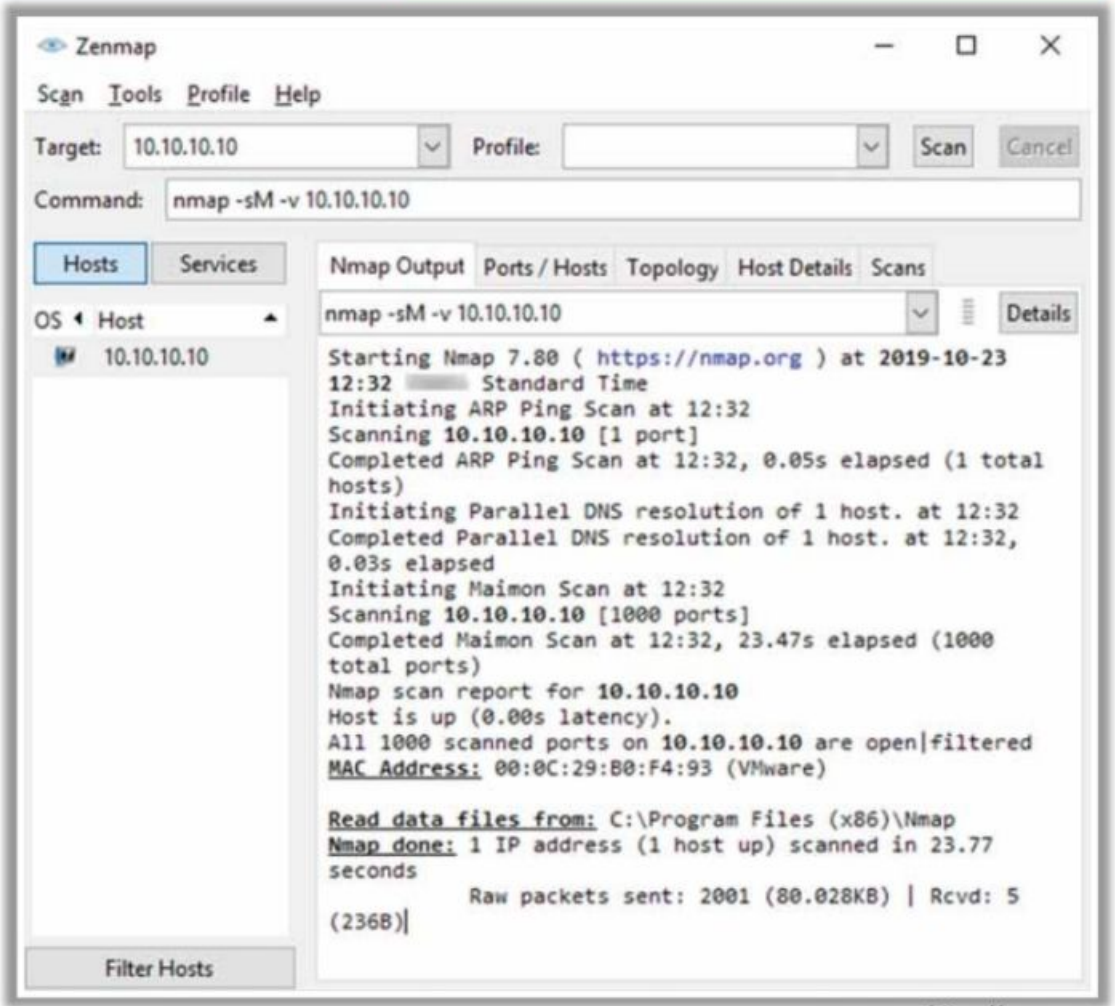
https://nmap.org

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





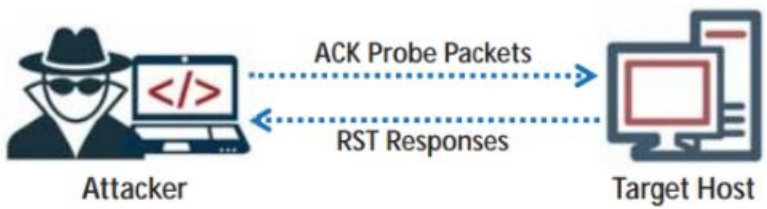


https://nmap.org

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

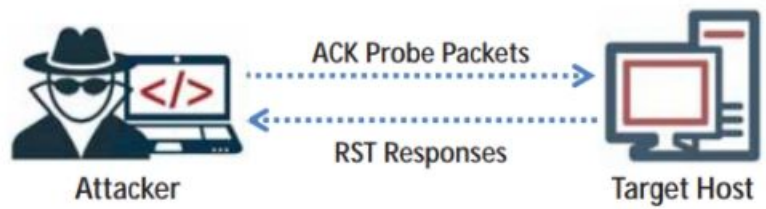
TTL-based ACK Flag Probe scanning




```
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

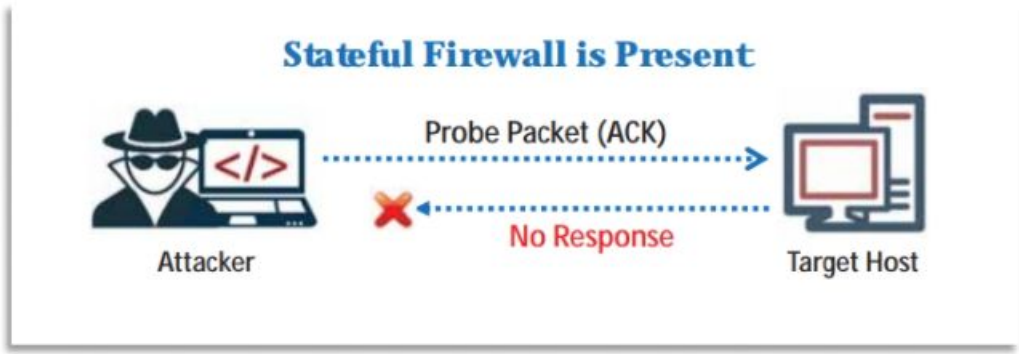


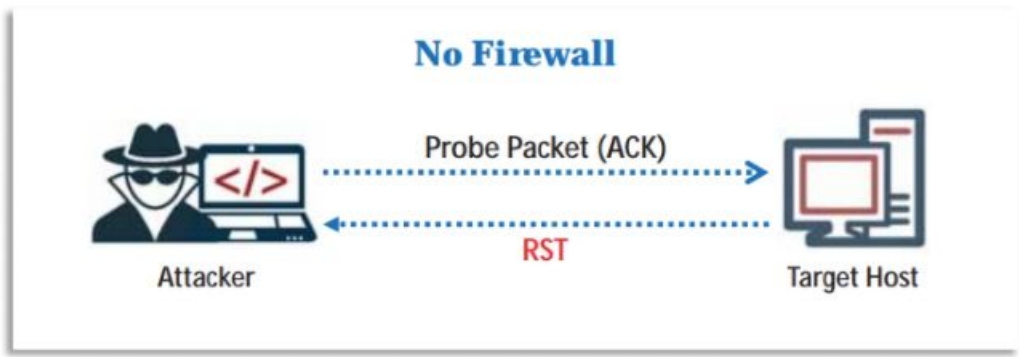

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

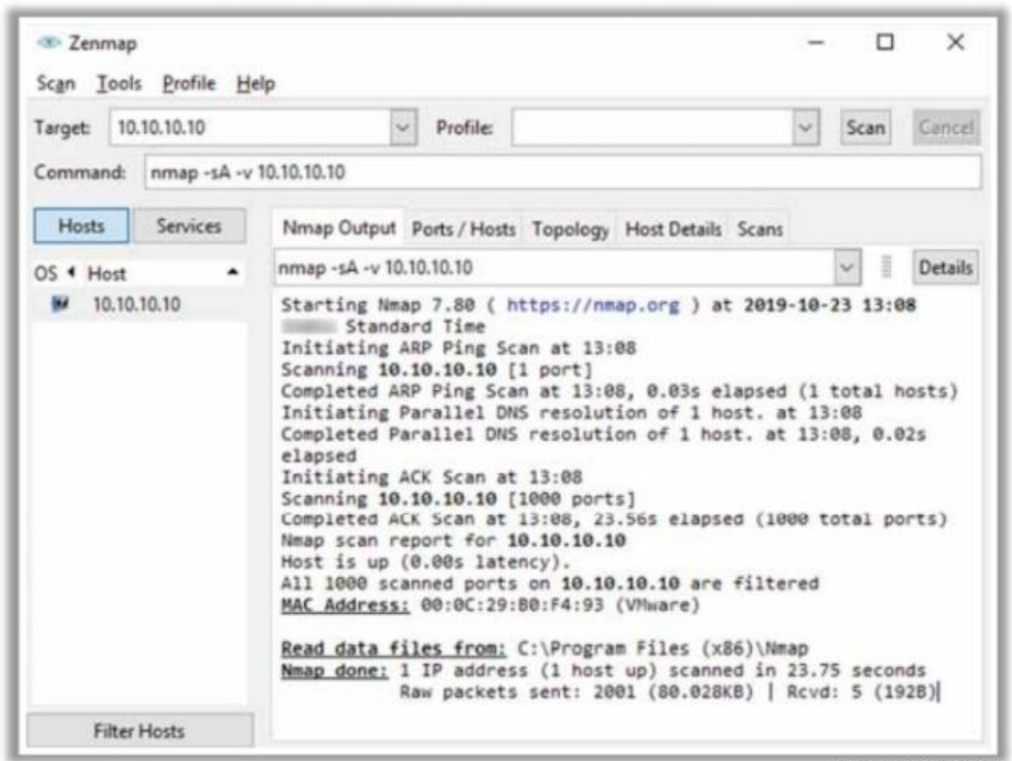
If the window value of the RST packet on a particular port has a non-zero value, then that port is open

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

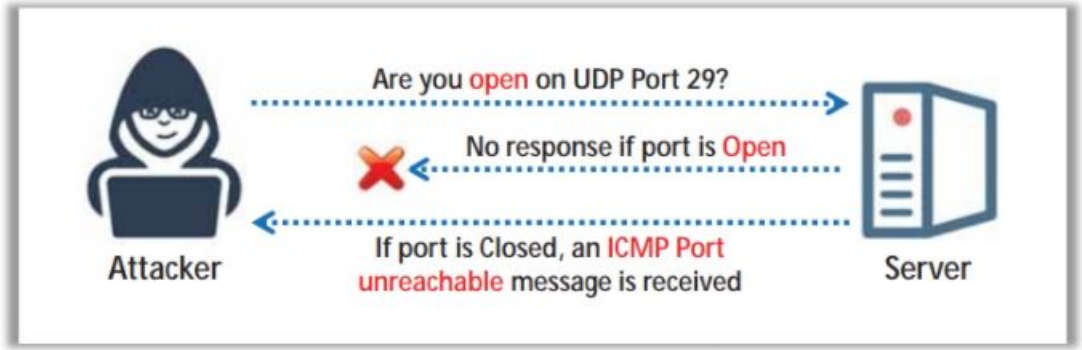






https://nmap.org

UDP Scanning

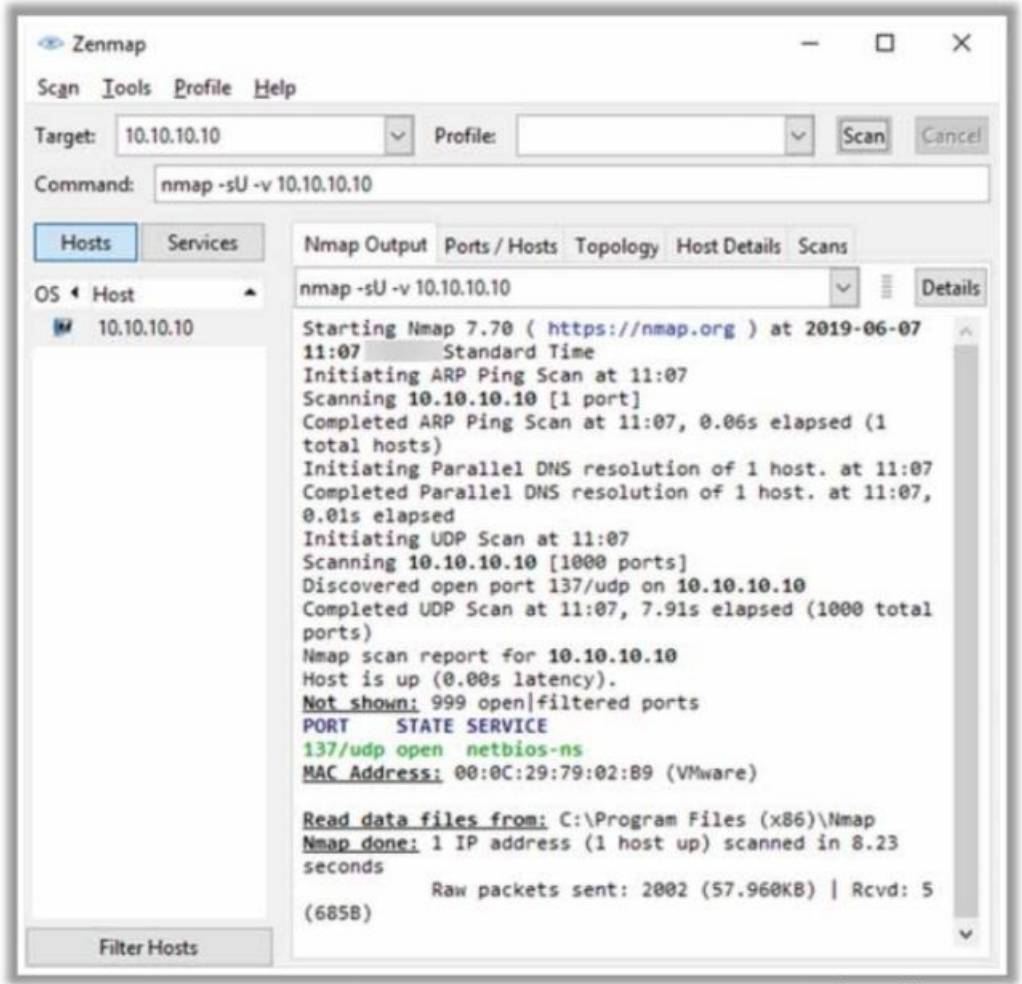


UDP Port Open

- 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

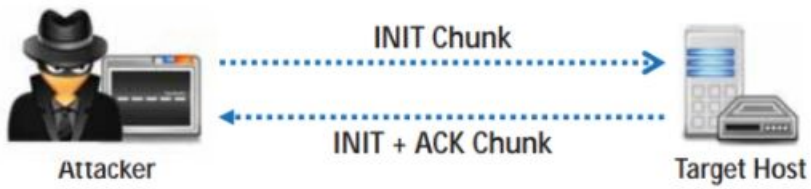


https://nmap.org

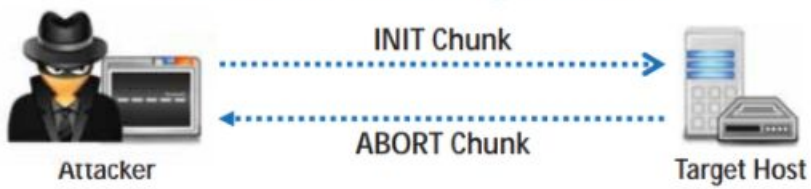
SCTP INIT Scanning

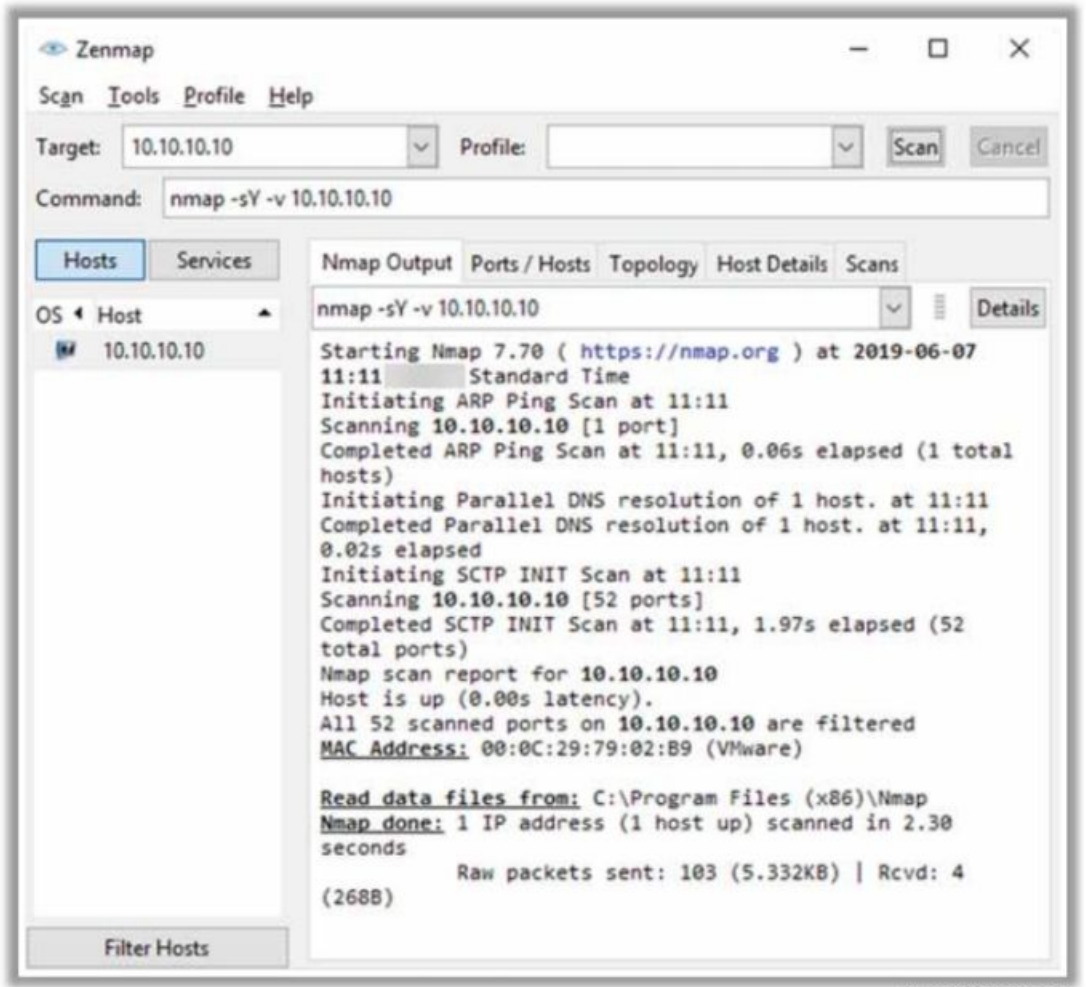
- Attackers send an INIT chunk to the target host, and an INIT+ACK chunk response implies that the port is open, whereas an ABORT Chunk response means that the port is closed
- No response from the target, or a response of an ICMP unreachable exception indicates that the port is a Filtered port

Port is listening (Open)



Port is not listening (Closed)

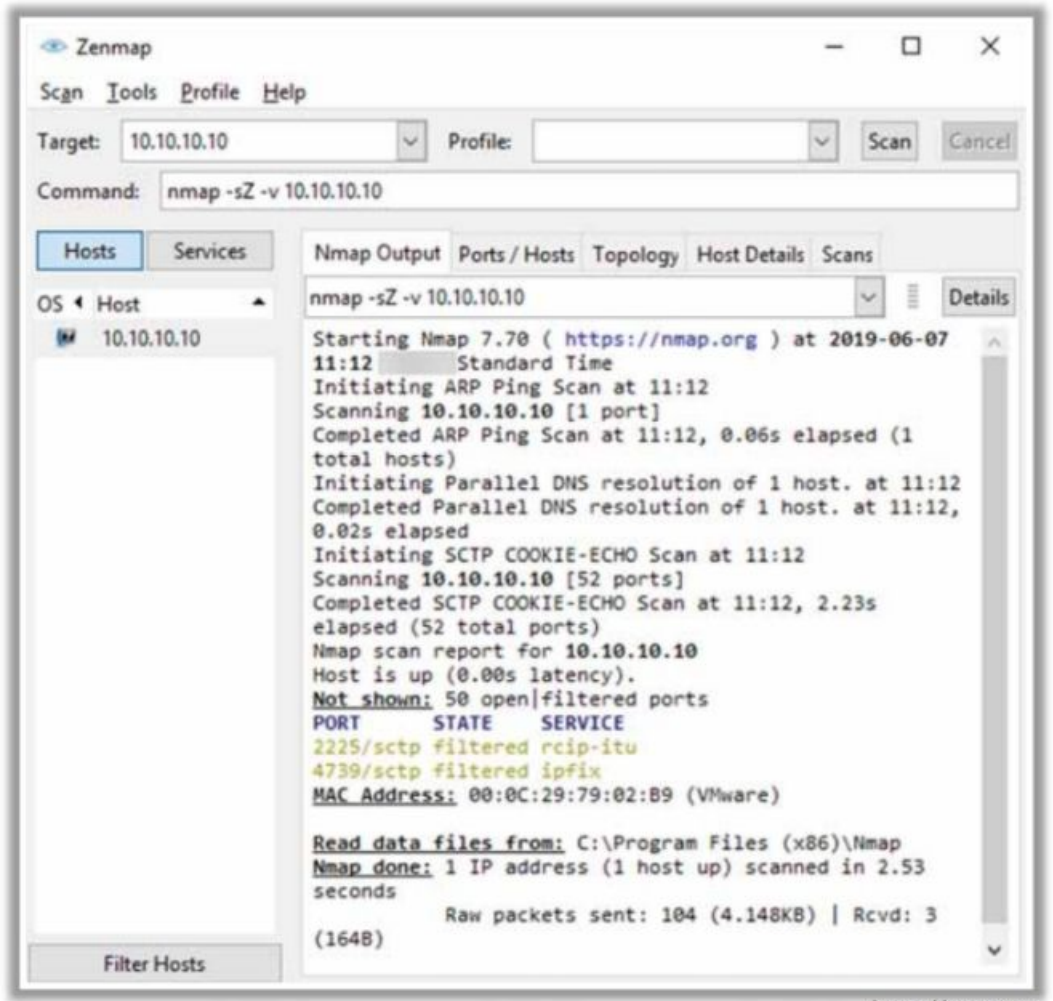




https://nmap.org

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

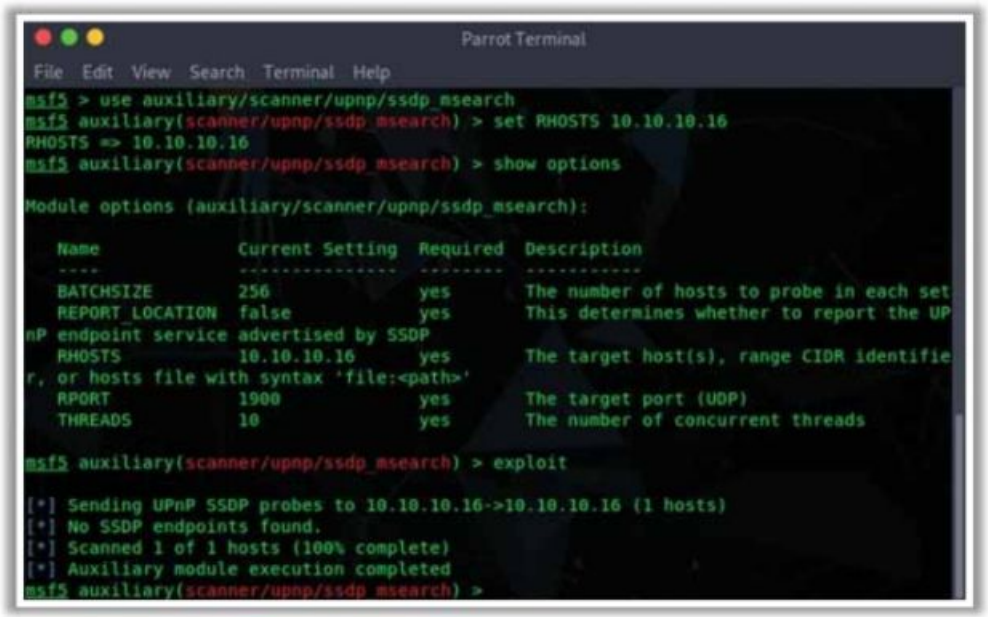


https://nmap.org

SSDP and List Scanning

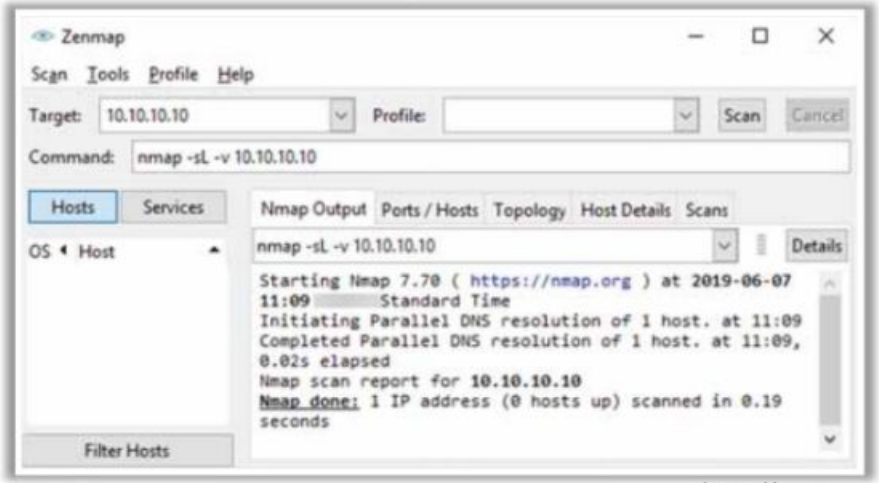
SSDP Scanning

- 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



ListScanning

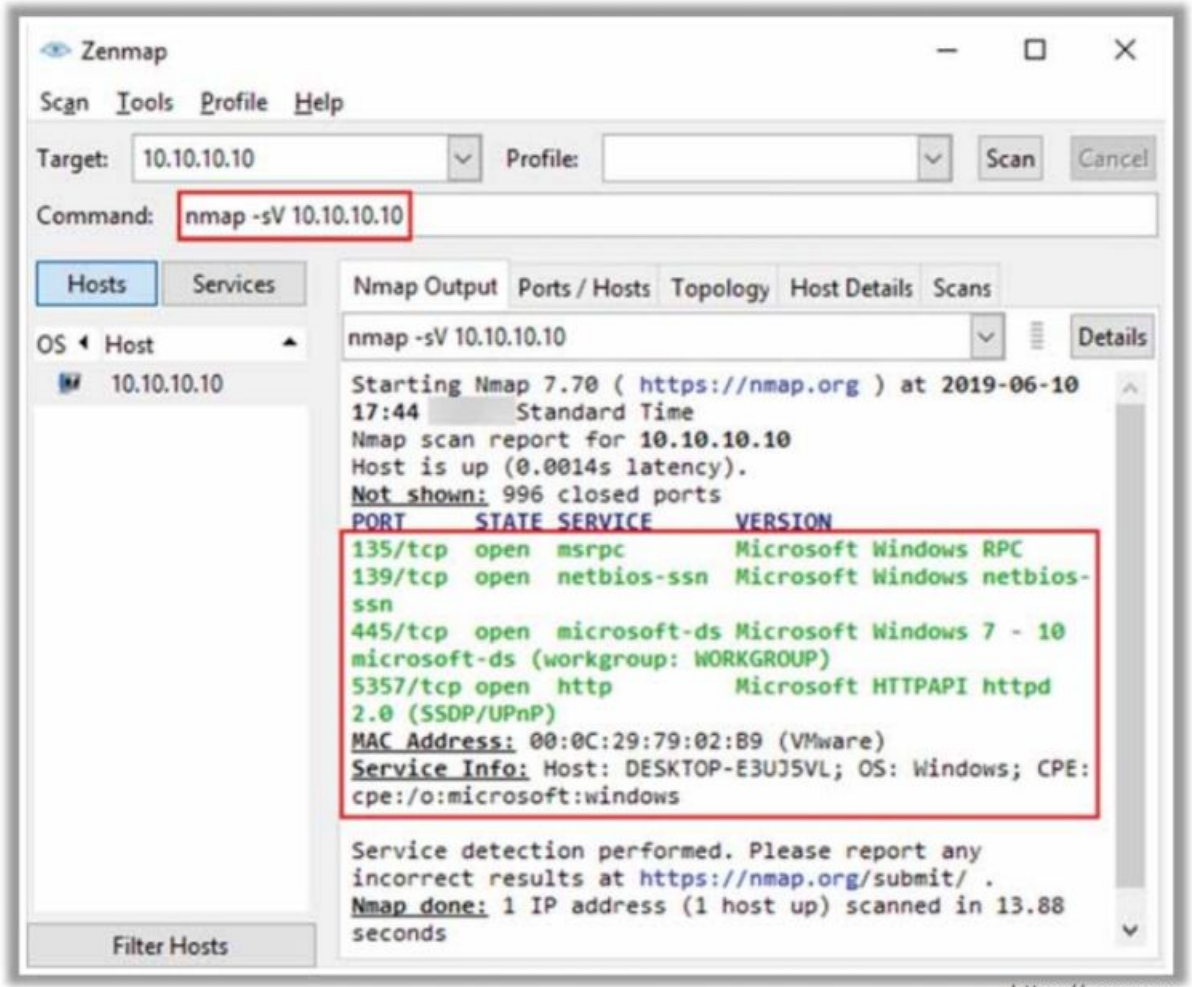
- This type of scan simply generates and prints a list of IPs/Names without actually pinging them
- A reverse DNS resolution is performed to identify the host names



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



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

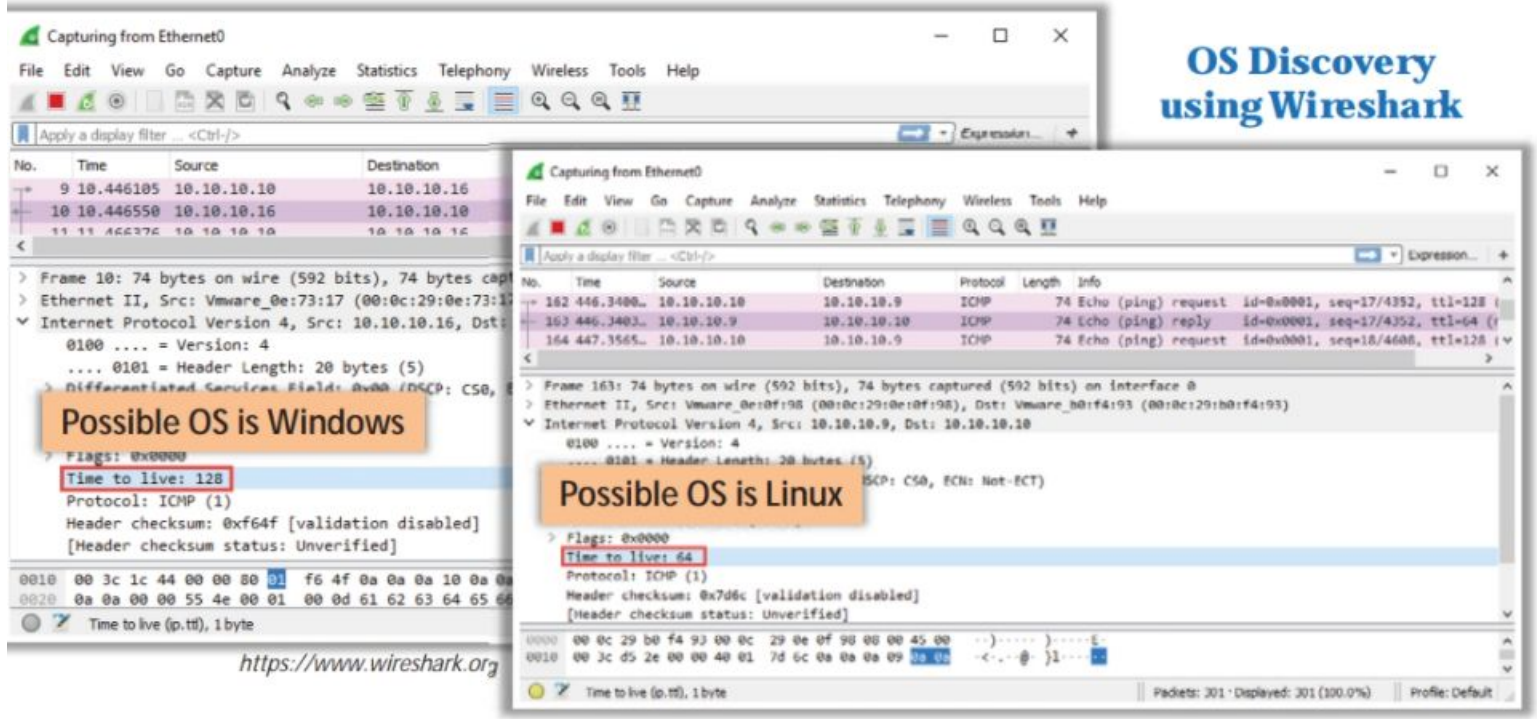
  Looking for an extension in the URL may assist in determining the application's version.

  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



https://www.wireshark.org

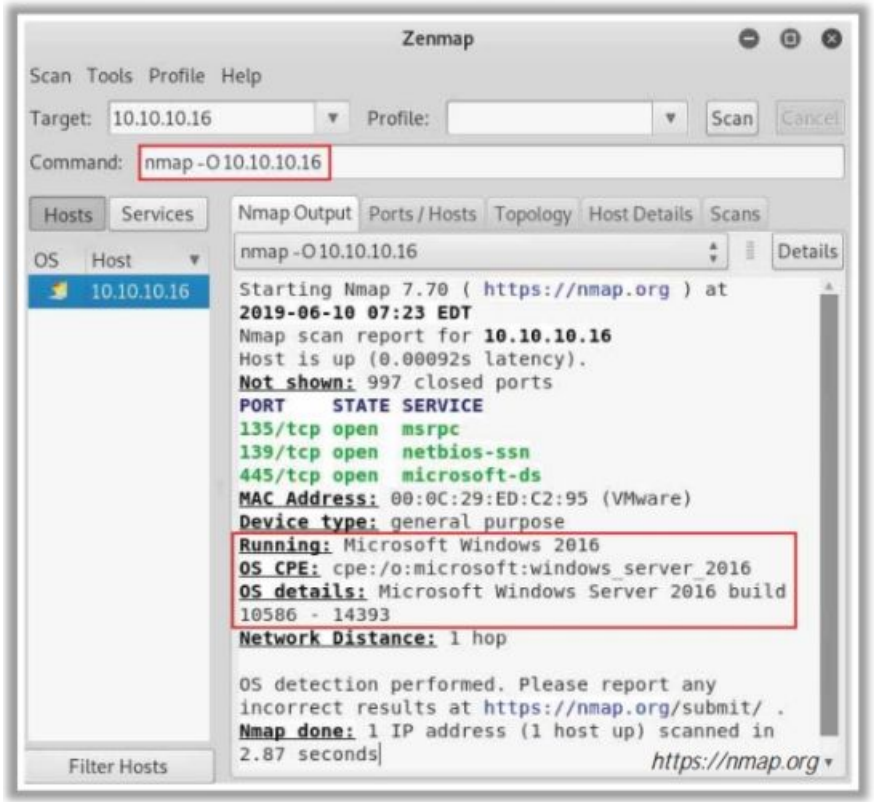
OS Discovery using Wireshark

Window size values for OS

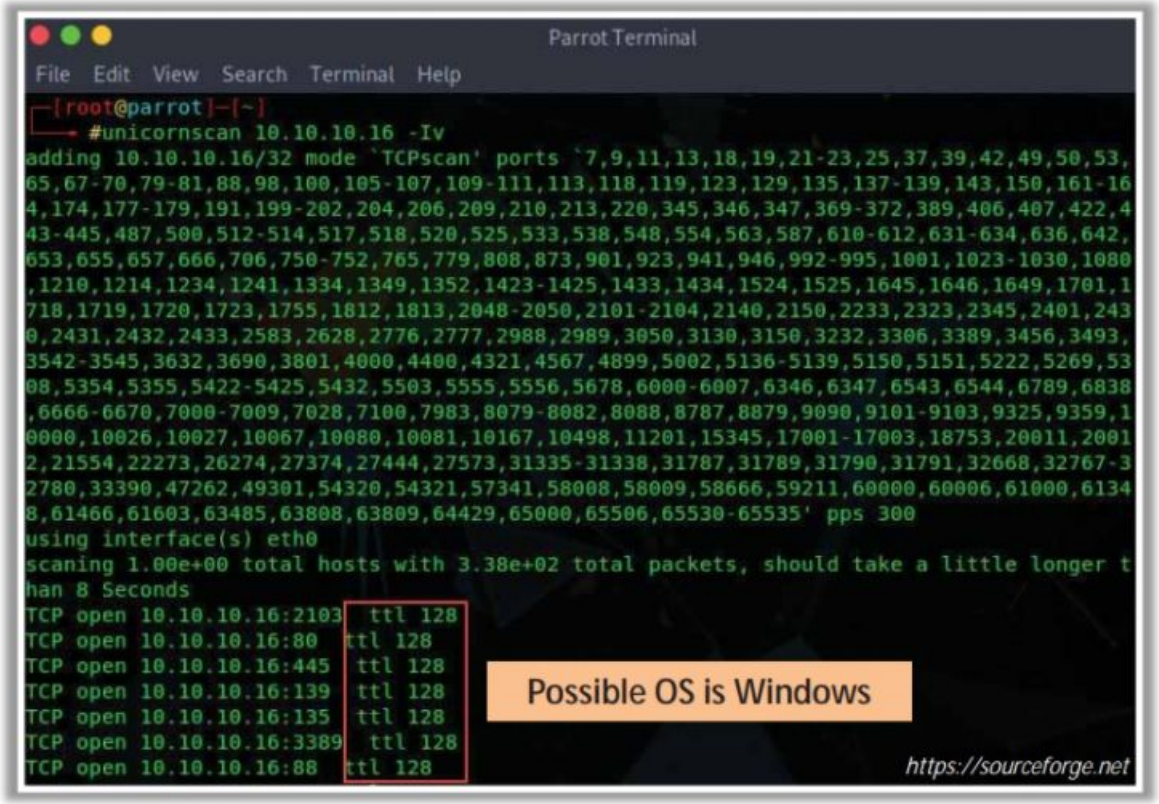
Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX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

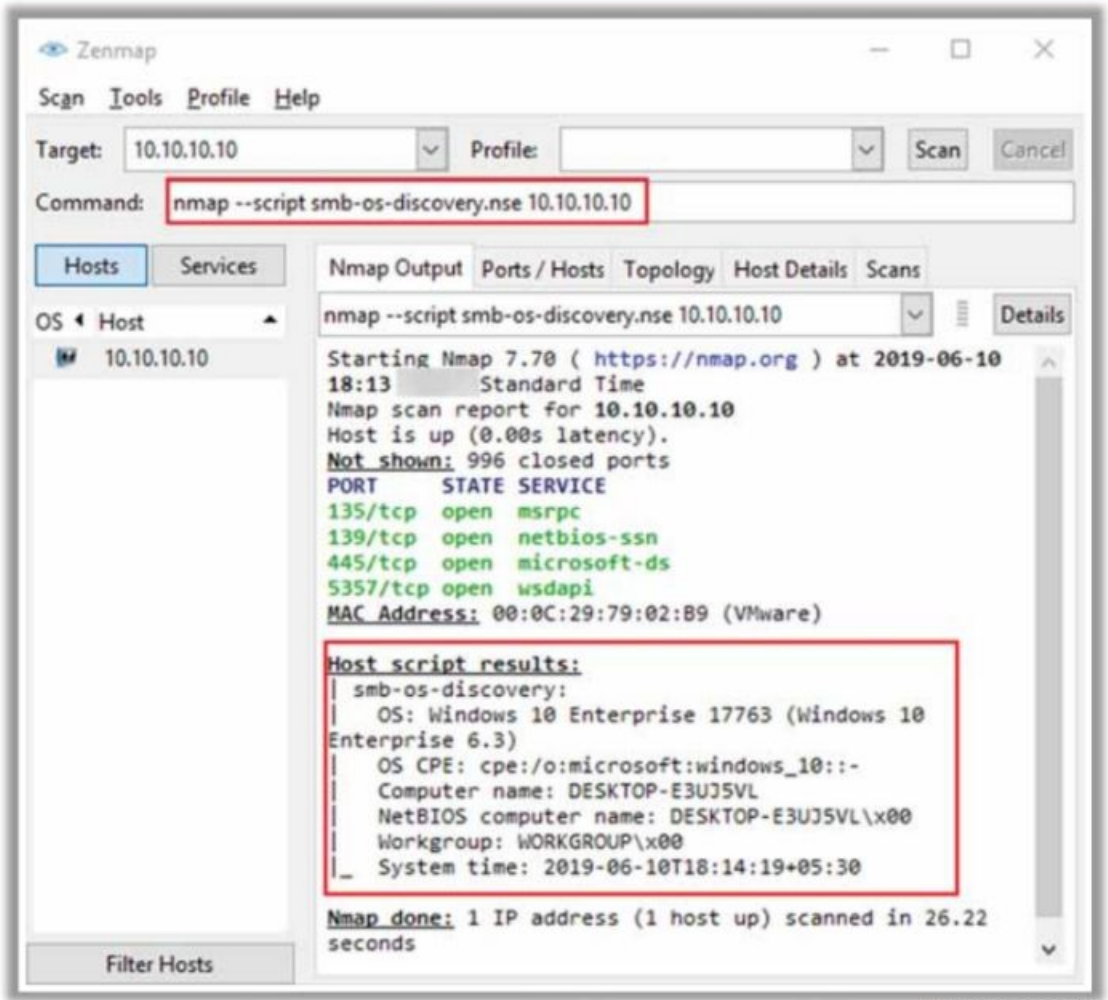


- In **Unicornscan**, the OS of the target machine can be identified by observing the TTL values in the acquired scan result



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



https://nmap.org

Anonymizers

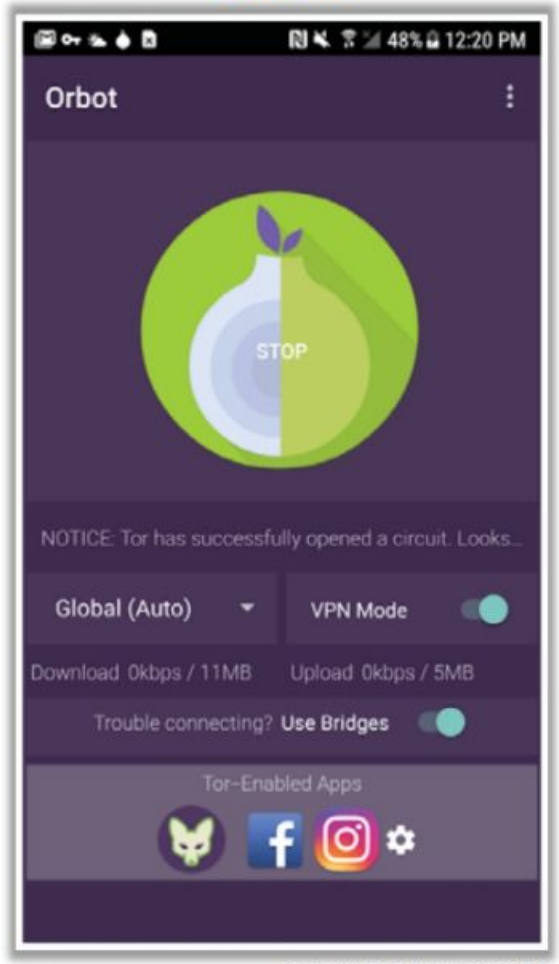
- An anonymizer removes all identity information from the user's computer while the user surfs the Internet
- Anonymizers make activity on the Internet untraceable
- Anonymizers allow you to bypass Internet censors

Why use an Anonymizer?

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

Anonymizers for Mobile

Orbot



https://guardianproject.info

Psiphon

https://psiphon.ca

OpenDoor

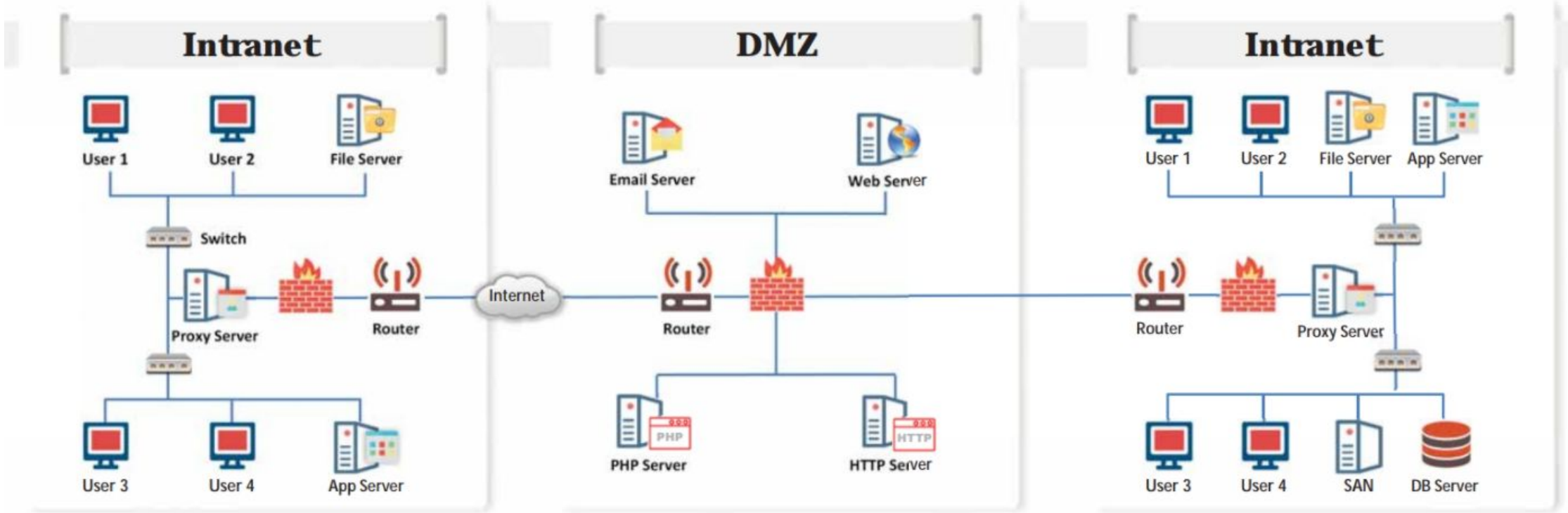
https://www.apple.com

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

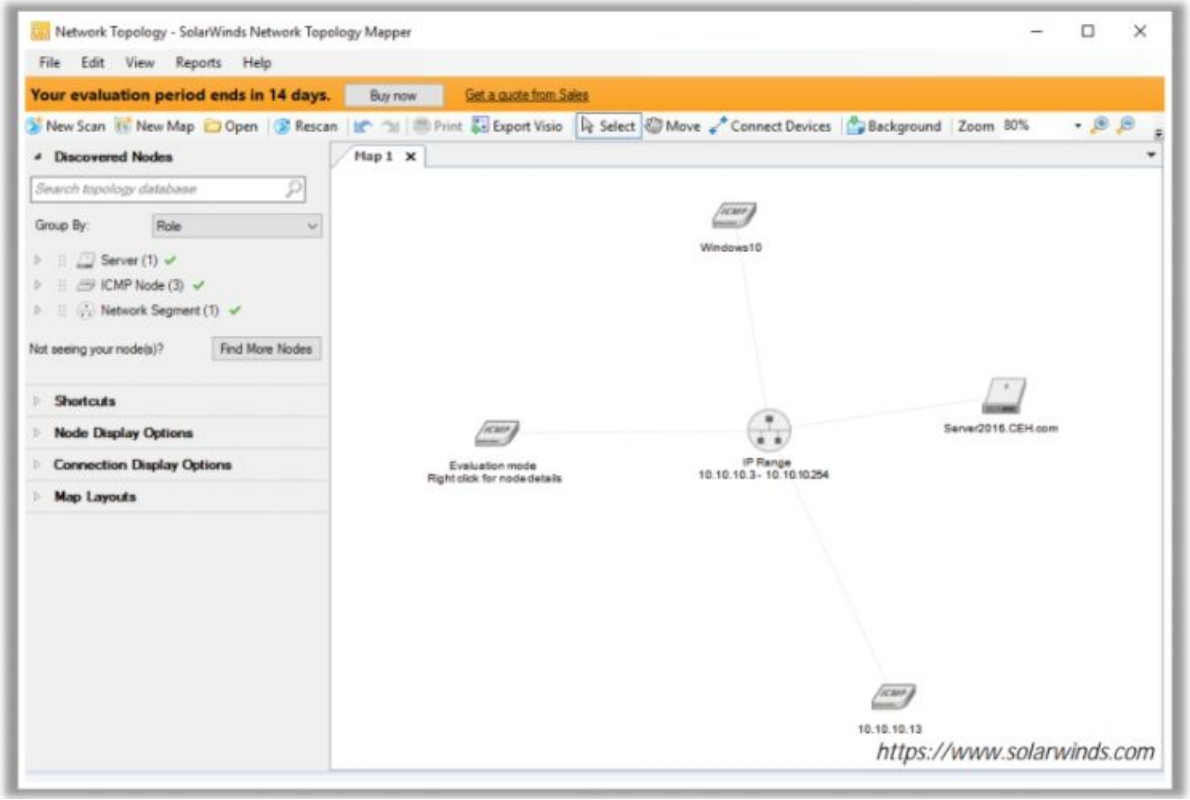
- A diagram of a target network provides an attacker with valuable information about the network and its architecture
- Network diagrams show logical or physical paths to a potential target



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

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