Chapter 3

Port Scanning

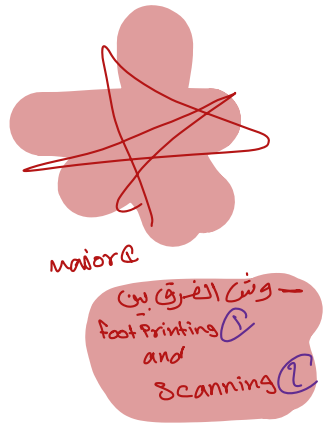
Dr. Ahmed Redha
PSU

Learning Objective

- Identify common information-gathering tools and techniques.

Key Concepts

- Determining the network range
- Identifying active machines
- Mapping open ports
- Operating system (OS) fingerprinting
- Network mapping



Overview of Network Scanning

- Scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques.

جمع معلومات الهدف قبل الهجوم بدون ما تحس الضحية

- Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network.
- It is one of the most important phases of intelligence gathering for an attacker which enables him/her to create a profile of the target organization.

- The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and keep track of the ones that are responsive or useful to an attacker's particular needs.

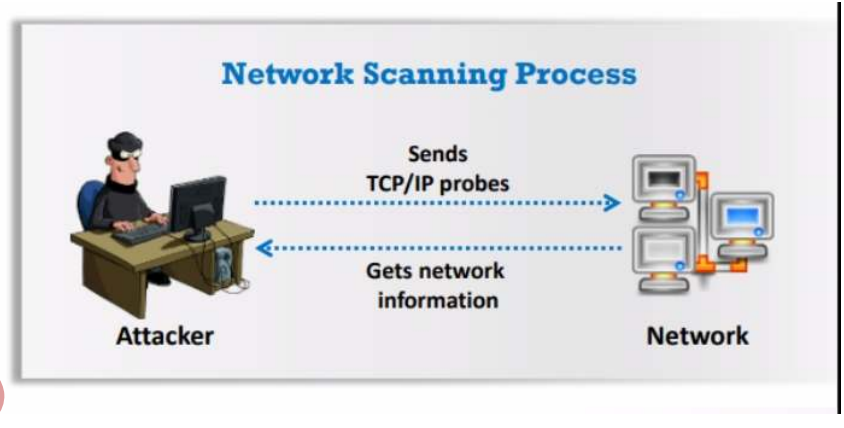
- In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more about the target system to find out if there are any configuration lapses in it.

The attacker then uses the information obtained during the scan to develop an attack strategy.

Types and Objectives of Scanning

The more the information at hand about a target organization, the greater the chances of knowing a network's security loopholes and consequently, for gaining unauthorized access to it. The followings are types used for scanning a network:

1. **Port Scanning**
2. **Network Scanning**
3. **Vulnerability Scanning**



1- Port Scanning – Lists the open ports and services:

By sending a sequence of messages to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state. The listening state provides information about:

- The operating system and system architecture of the target. This is also known as fingerprinting. An attacker can formulate an attack strategy based on the operating system's vulnerabilities.
- Discover the services running/listening on the target system. Doing so gives the attacker an indication of vulnerabilities (based on the service) exploitation for gaining access to the target system. Sometimes, active services that are listening may allow unauthorized user access to misconfigure systems or to run software with vulnerabilities.
- Identify specific applications or versions of a particular service.

2- Network Scanning (Lists IP addresses): Discover the network's live hosts, IP addresses, and open ports of live machines. Using open ports, the attacker will determine the best means of entry into the system.

3- Vulnerability Scanning (Shows the presence of known weaknesses): Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The catalog includes a list of common files with known vulnerabilities and common exploits for a range of servers.

A vulnerability scanner may, for example, look for backup files or directory traversal exploits.

Communicatio method depends on 3-handshake

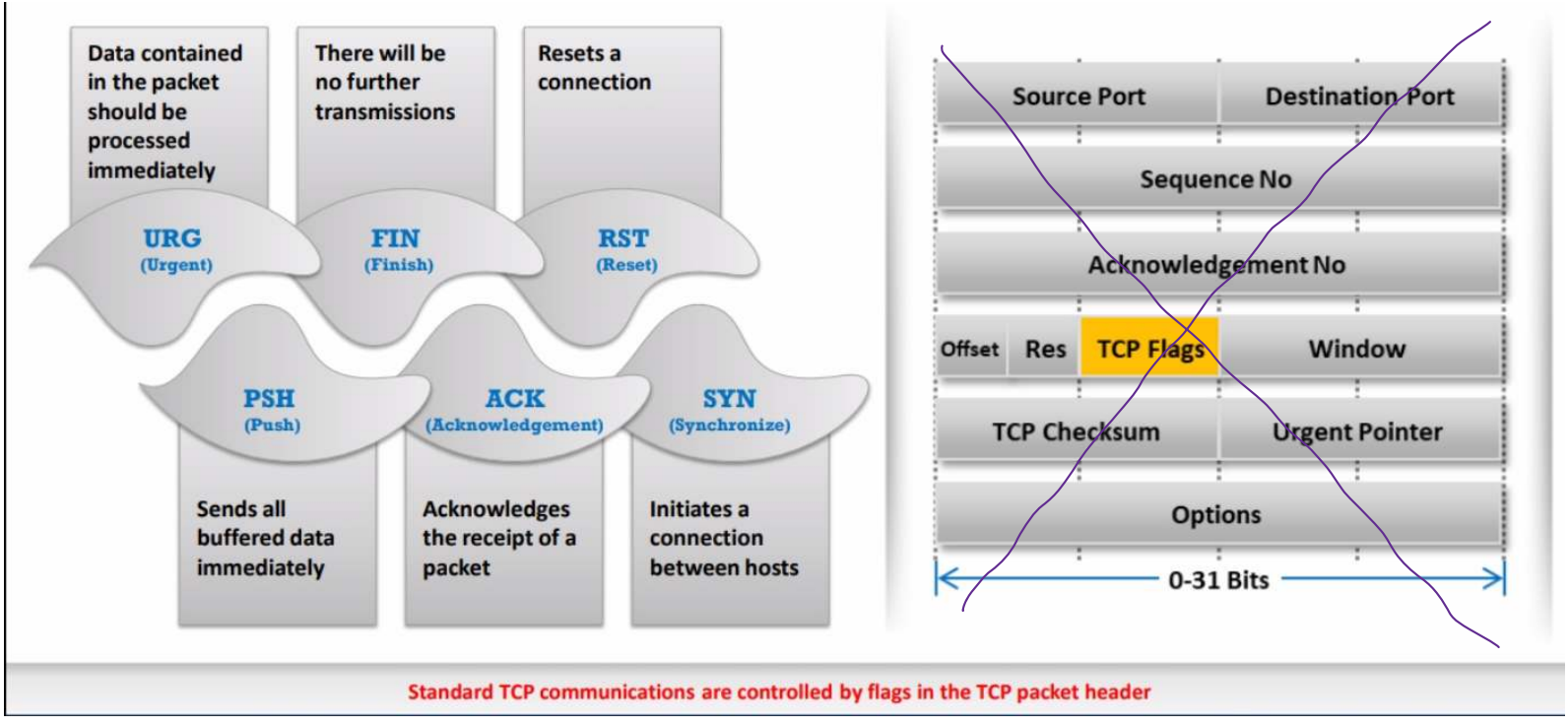
*what does the flag do? → controls the transmission ↙ manage the connection.

TCP Communication Flags

- TCP header contains various flags that control the transmission of data across a TCP connection. Six TCP control flags manage the connection between hosts and give instructions to the system.
- Four of these flags (namely: SYN, ACK, FIN, and RST) govern the establishment, maintenance, and termination of a connection.
- The other two flags (namely: PSH and URG) provide instructions to the system. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1", that flag is automatically turned on.

TCP Communication Flags

SYN → Start message
Ack → I received your message
FIN → close connection
RST → Force close
PSH → send data now
URG → high Priority data

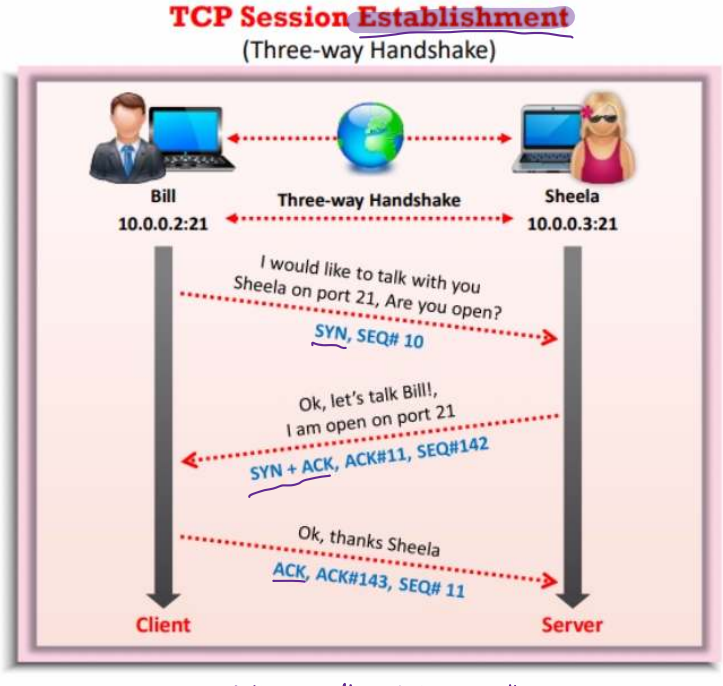


Standard TCP communications are controlled by flags in the TCP packet header

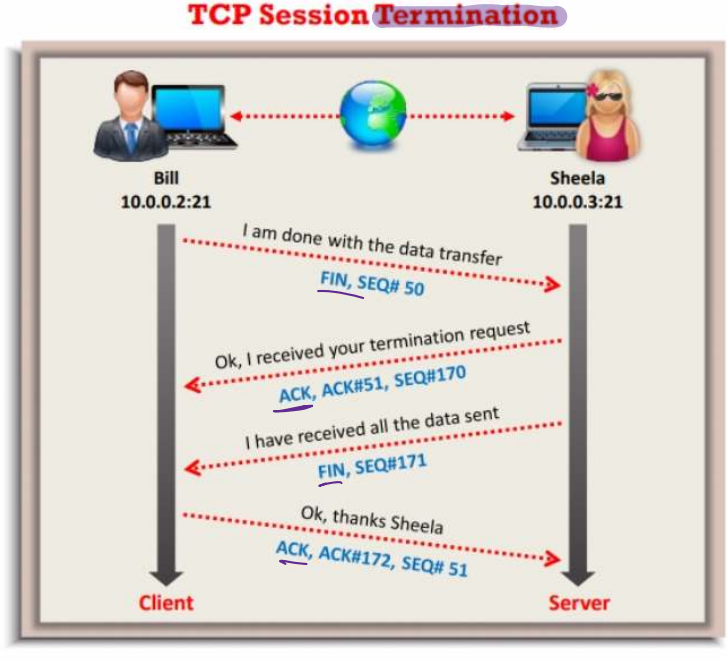


```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: c2:01:0c:b4:00:00 (c2:01:0c:b4:00:00), Dst: c2:02:13:98:00:00 (c2:02:13:98:00:00)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
Transmission Control Protocol, Src Port: 41417 (41417), Dst Port: 23 (23), Seq: 0, Len: 0
    Source Port: 41417 (41417)
    Destination Port: 23 (23)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 24 bytes
    .... 0000 0000 0010 = Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
    Window size value: 4128
    [Calculated window size: 4128]
    Checksum: 0xe46a [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Urgent pointer: 0
    Options: (4 bytes), Maximum segment size
        Maximum segment size: 1460 bytes
            Kind: Maximum Segment Size (2)
            Length: 4
            MSS Value: 1460
```

TCP/IP Communication

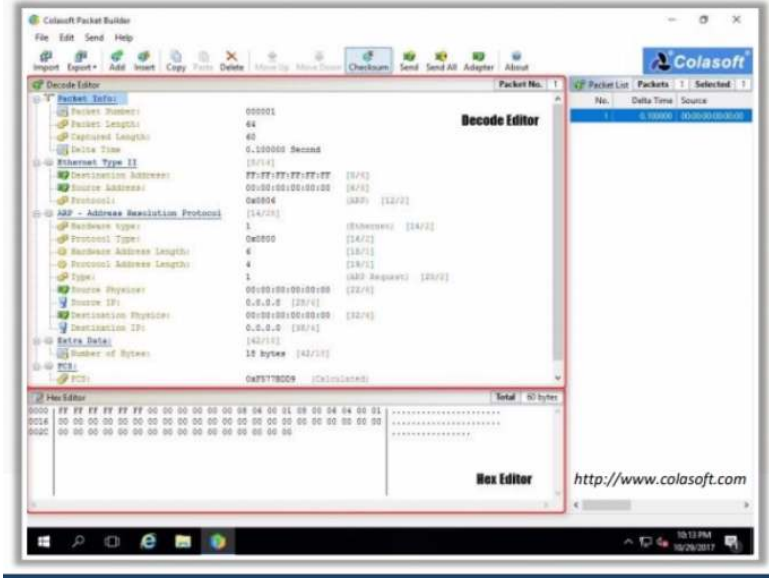


SYN , SYN+Ack , Ack



Creating Custom Packet Using TCP Flag

- Colasoft Packet Builder enables the creation of custom network packets to **audit networks for various attacks**
- Attackers can also use it to create fragmented packets to **bypass firewalls and IDS systems** in a network



Packet Crafting Tools

- NetScanTools Pro (*https://www.netscantools.com*)
- Ostinato (*http://ostinato.org*)
- WAN Killer (*http://www.solarwinds.com*)
- Packeth (*http://packeth.sourceforge.net*)
- LANforge FIRE (*http://www.candelatech.com*)

→ help attacker identify open ports on targeted system
→ Administrators use it to verify Policies of their network.

Scanning Techniques

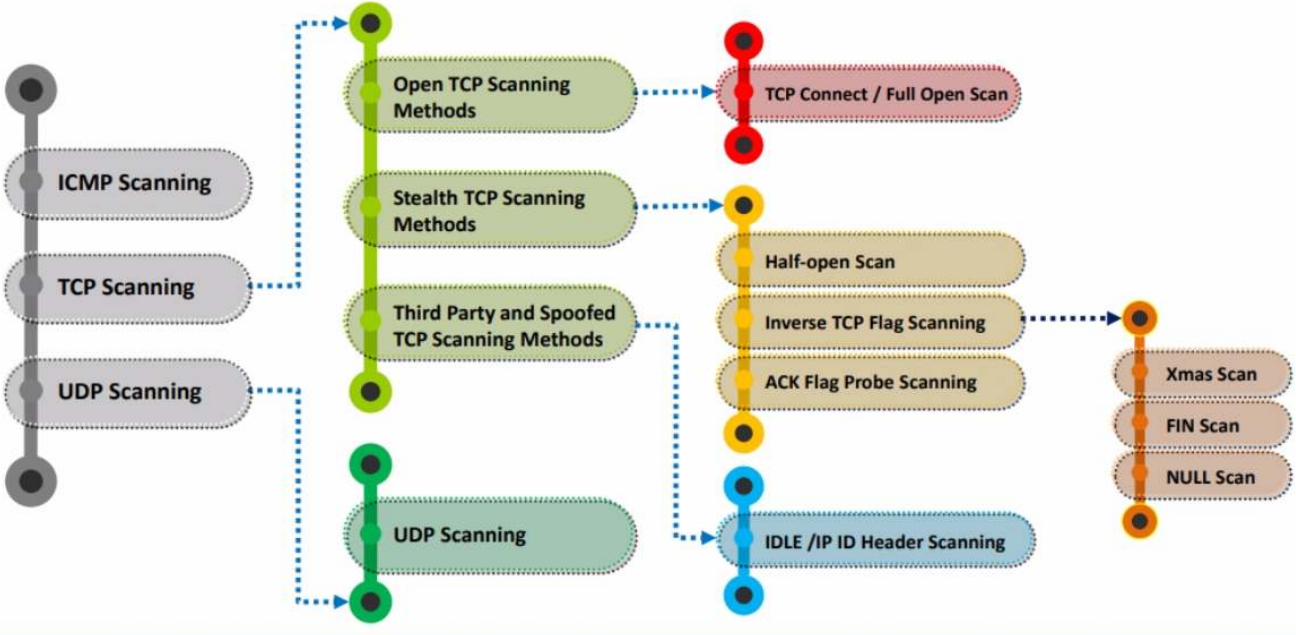
- Scanning is the process of gathering information about systems that are "alive" and responding on the network. **Port scanning techniques help an attacker to identify the open ports on a targeted server or host.** Administrators often use port scanning techniques to verify security policies of their networks, whereas attackers use them to identify running services on a host with the intent of compromising the network. The first step in scanning networks is to check for live systems.
- Once the attackers detect live systems in the target network, they try to find open ports in the discovered live systems. Sometimes users unknowingly keep unnecessary open ports on their systems. Attacker takes advantages of such open ports to launch attacks.

Port Scanning: Common Port Numbers

PORT	SERVICE	PROTOCOL
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

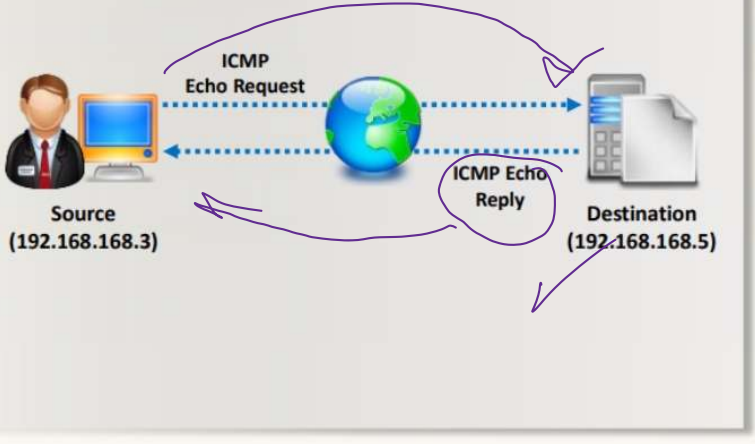
Scanning Techniques

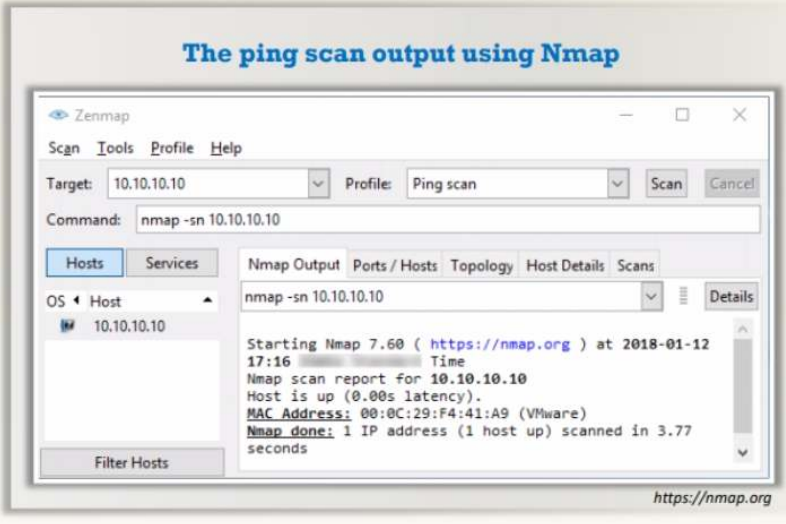
- The scanning techniques are categories according to the type of protocol used for communication



ICMP Scanning - Checking for Live Systems

- Ping scan involves sending ICMP ECHO requests to a host. If the host is alive, 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





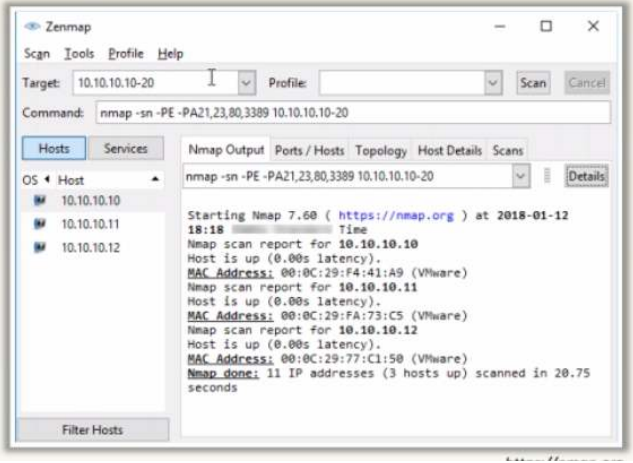
2

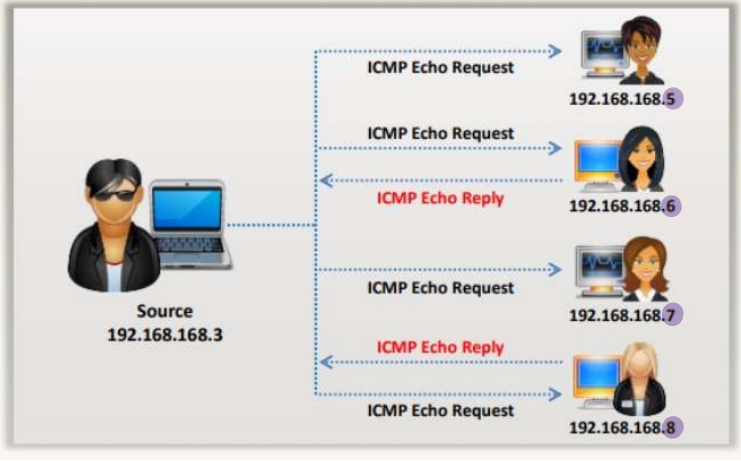
they use IP address to see live host (Alive)

Ping Sweep-Checking for Live Systems

- 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 the Subnet Mask Calculators to identify the number of hosts that are present in the subnet
- Attackers subsequently use ping sweep to create an inventory of live systems in the subnet

The ping sweep output using Nmap





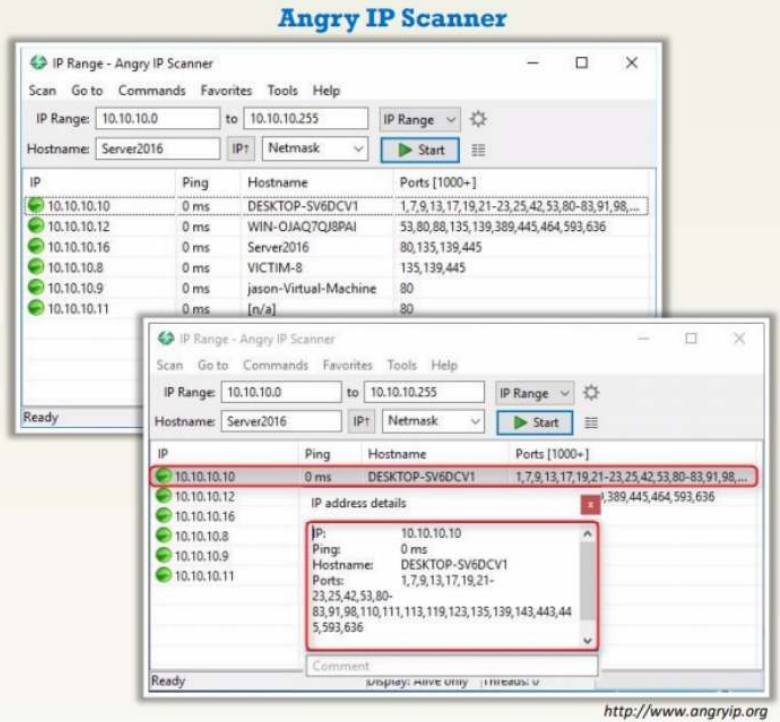
Ping Sweep Tools

Angry IP Scanner

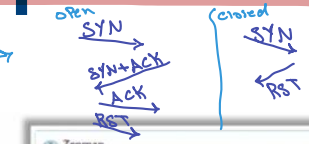
Angry IP Scanner pings each IP address to check if they are alive, then it optionally resolves its hostname, determines the MAC address, scans ports, etc.

Ping Sweep Tools

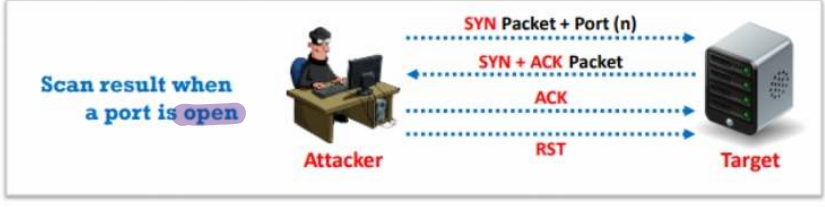
- SolarWinds Engineer's Toolset (*http://www.solarwinds.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Colasoft Ping Tool (*http://www.colasoft.com*)
- Visual Ping Tester (*http://www.pingtester.net*)
- OpUtils (*https://www.manageengine.com*)

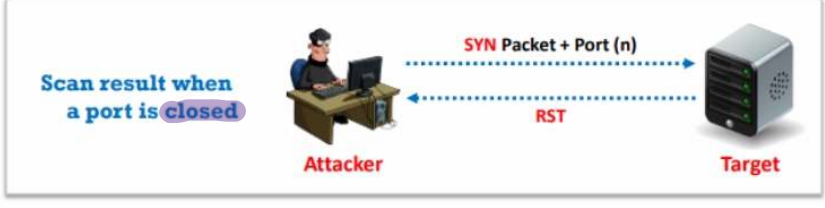


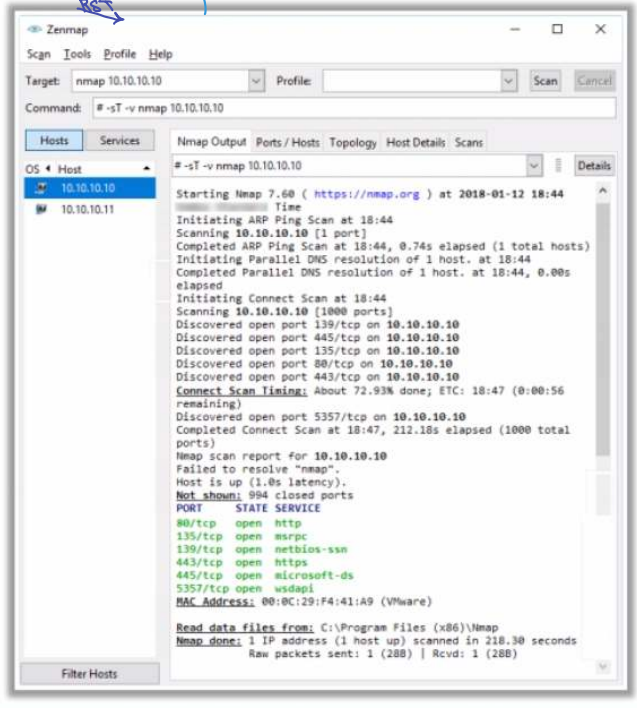
TCP Connect / Full Open Scan



- The TCP Connect scan detects when a port is open after completing the three-way handshake
- TCP Connect scan establishes a full connection and tears it down by sending an RST packet
- It does not require the super user privileges







4

Stealth Scan (Half-open Scan)

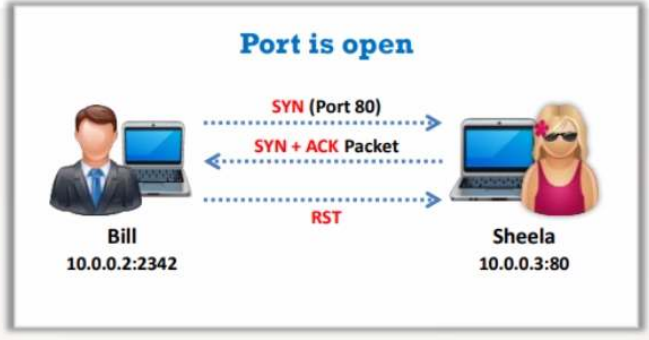
↳ because, it sends SYN but never complete the connection

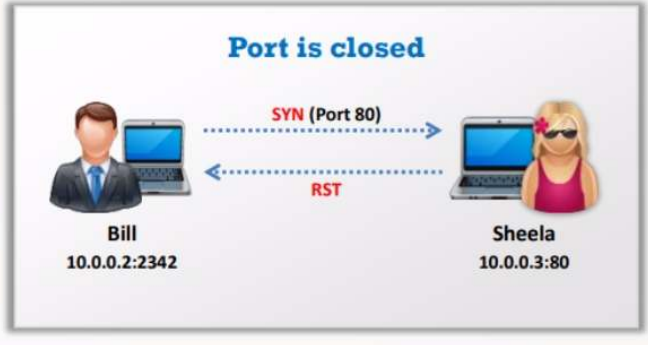
- The Stealth scan involves resetting the TCP connection between the client and server abruptly before completion of **three-way handshake signals**, hence, making the connection half open
- Attackers use stealth scanning techniques to **bypass firewall rules**, **logging mechanism**, and hide themselves as usual under network traffic

why ? ① ② ③

Stealth Scan Process

The client sends a single **SYN** packet to the server to the appropriate port	**01**
If the port is open, subsequently, the server will responds with an **SYN/ACK** packet	**02**
If the server responds with an **RST** packet, then the remote port is in the "closed" state	**03**
The client sends the **RST** packet to close the initiation before a connection can ever be established	**04**





B

(called null Flag)

Inverse TCP Flag Scanning

send unusual flags to confuse the system
example: (URG, FIN, Null, PSH)

No response → open
RST → closed

01

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

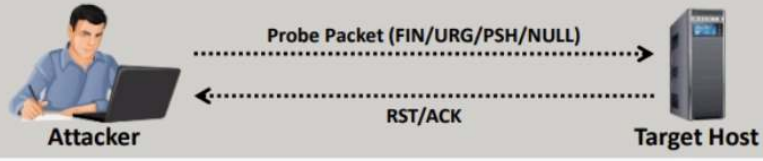
02

Port is open



03

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

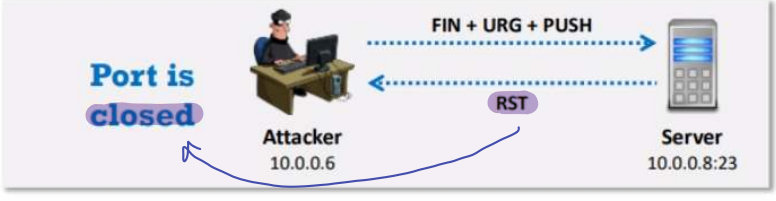
6

Xmas Scan

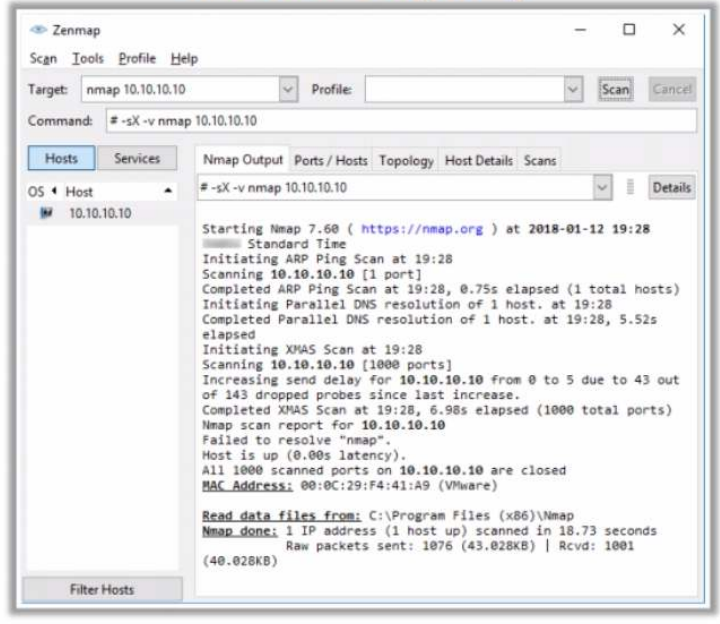
if open or not
↓ response ↓ no response

- In Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set
- FIN scan works only with OSes with RFC 793-based TCP/IP implementation
- It will not work against any current version of Microsoft Windows





Xmas Scan Using Nmap



7

use TTL or window size

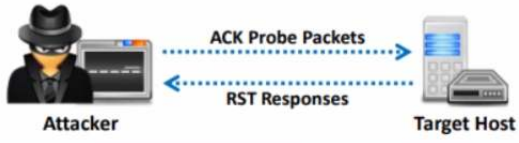
ACK Flag Probe Scanning

→ Analyze to see if it's open or closed
know this by TTL and window field

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

< 64

TTL based ACK flag probe scanning



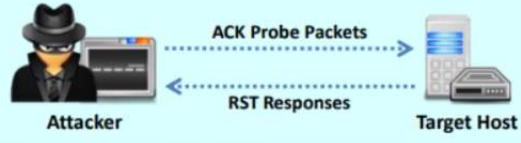

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

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

< 64 → open
> 64 → closed

non zero

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
```

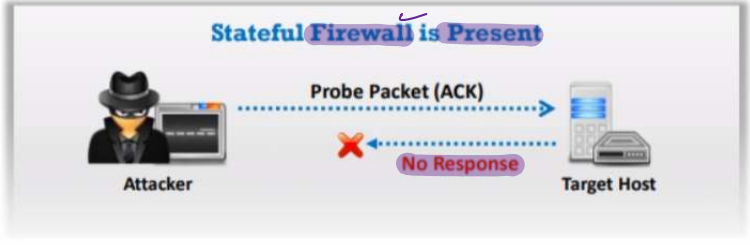
If the **WINDOW value of RST packet** on a particular port has a **non zero value**, then that **port is open**

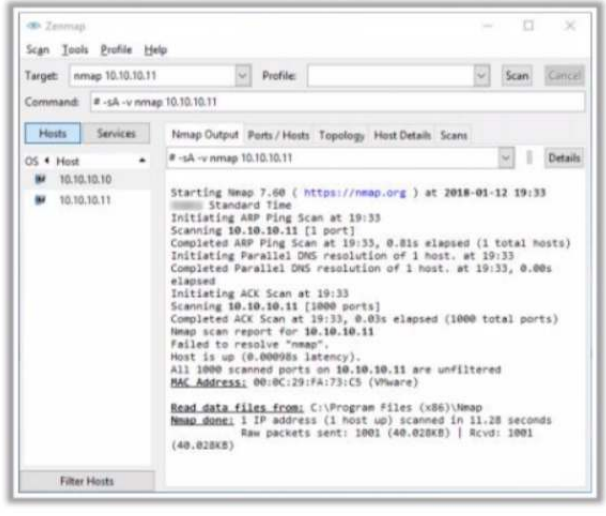
0 → open
any other number → closed

ACK Flag Probe Scanning (cont..)

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

there's firewall





IDLE/IPID Header Sca

Aim to find out if the Port is open or closed based on the IPID & use Zombie to Protect (himself) attacker

Attacker checks the IPID to see if it's open or close because OS increase the IPID when Packet is sent

- Every IP packet on the Internet has a fragment identification number (IPID); 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 **RST packet**, disclosing the IPID. However, always analyse the RST packet from the zombie machine to **extract IPID**
3. Send 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 **SYN+ACK Packet** to the zombie and in response the zombie will send an RST to the target
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. IPID increased by **2 will indicate an open port** whereas **1 will indicate a closed port**

Attacker & target

one device only attacker

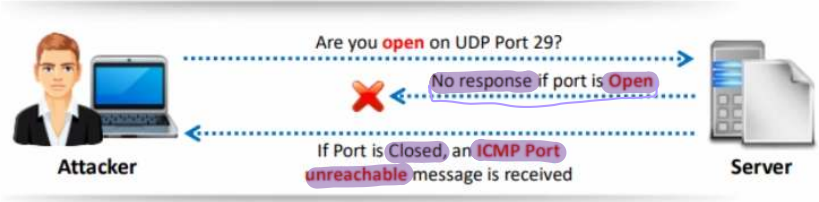


- Faster
- No 3-handshake

UDP Scanning

No response → open
unreachable message → closed

UDP

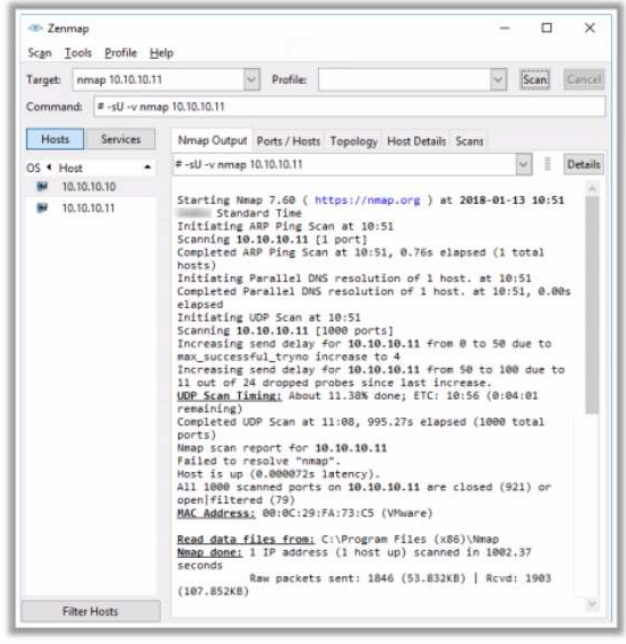


UDP Port Open

- There is no three-way TCP handshake for UDP scan
- 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



Port Scanning Countermeasures

01 Configure firewall and IDS rules to detect and block probes

02 Run the port scanning tools against hosts on the network to determine whether the firewall properly detects the port scanning activity

03 Ensure that the mechanism used for routing and filtering at the routers and firewalls respectively cannot be bypassed using a particular source ports or source-routing methods

04 Ensure that the router, IDS, and firewall firmware are updated to their latest releases/version

05 Use custom rule set to lock down the network and block unwanted ports at the firewall

06 Filter all ICMP messages (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the firewalls and routers

07 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

08 Ensure that the anti scanning and anti spoofing rules are properly configured

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 the system posses and the exploits that might work on a system to further carry out additional attacks

Active Banner Grabbing

needs to interact with the target

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



Passive Banner Grabbing

No need to interact with the target

like 404 error

- 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

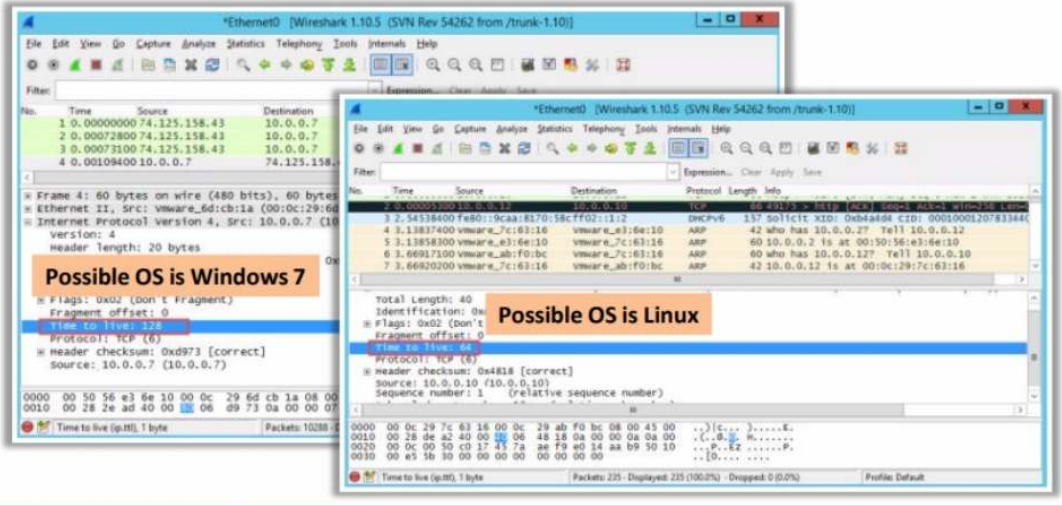
  Looking for an extension in the URL may assist in determining the application's version.

  Example: .aspx => IIS server and Windows platform

How to Identify Target System OS

each OS has a value of TTL (time to live) & window size

- Attacker 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 by using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields

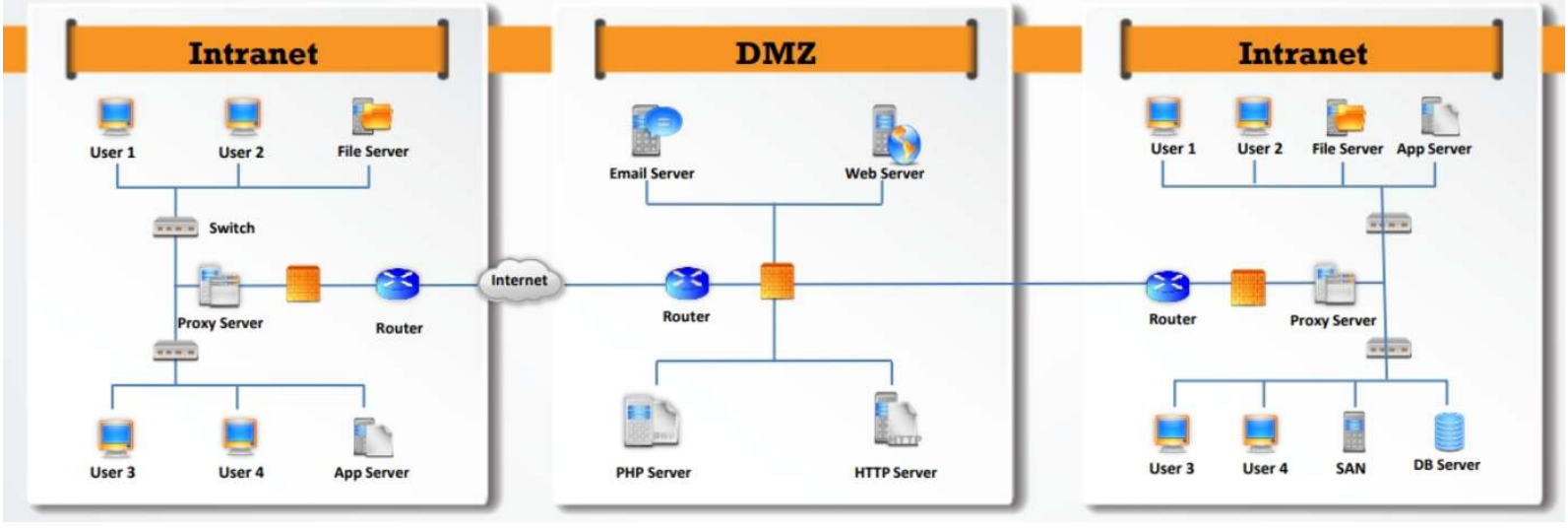


Values for the Operating Systems

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

Drawing Network Diagrams

- Drawing target's network diagram gives valuable information about the network and its architecture to an attacker
- Network diagram shows logical or physical path to a potential target



Scanning Pen Testing

- The network scanning penetration test helps to determine the network's **security posture** by identifying **live systems**, discovering **open ports**, associating **services**, and grabbing **system banners** from a remote location to simulate a network hacking attempt

- The penetration testing report will help the **system administrators** to:

Close **unused ports** 1



Disable **unnecessary services** 2



Hide or customize banners 3



Troubleshoot service configuration errors 4



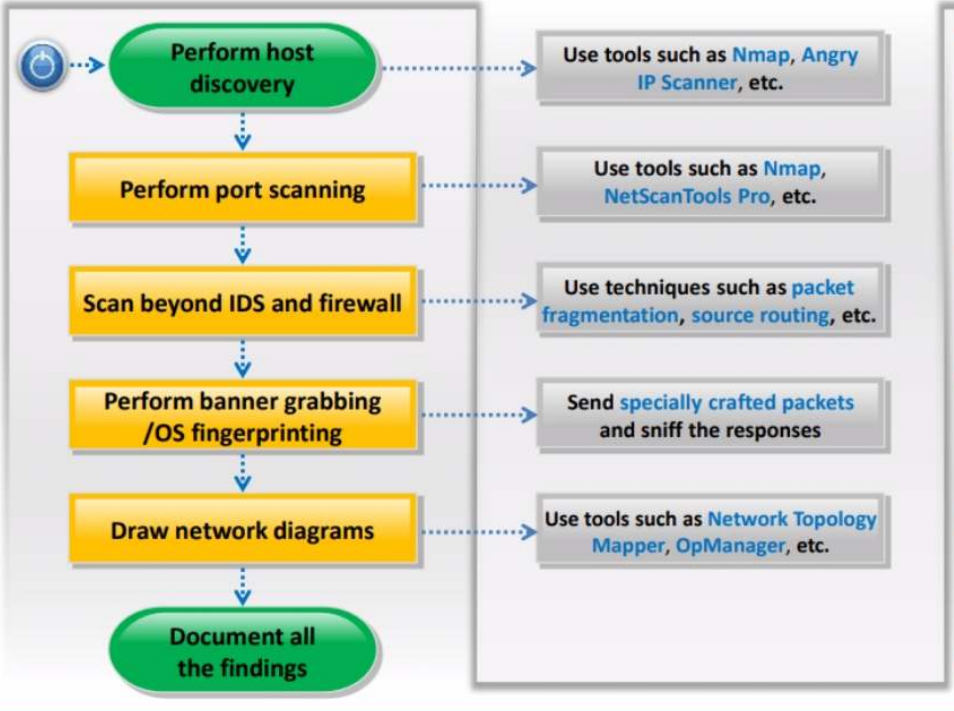
Calibrate **firewall rules** 5



Scanning Pen Testing (cont'd)

it will come as a scenario

how to identify the target sys. or



- Check for the live hosts using tools such as **Nmap**, **Angry IP Scanner**, **SolarWinds Engineer's toolset**, **NetScanTools Pro**, etc.
- Check for open ports using tools such as **Nmap**, **NetScanTools Pro**, **Hping3**, **PRTG Network Monitor**, **SuperScan**, etc.
- Scan beyond IDS and firewall using techniques such as **packet fragmentation**, **source routing**, **IP address spoofing**, etc.
- Perform banner grabbing/OS fingerprinting by sending **specially crafted packets** to the targeted machine and then comparing the responses with the database
- Draw network diagrams of the vulnerable hosts using tools such as **Network Topology Mapper**, **OpManager**, **The Dude**, **NetSurveyor**, **NetBrain**, etc.
- Document all the findings

Nmap

- Nmap (Network Mapper)
  - One of the most widely used security tools
  - Is a port scanner with capability to perform a number of different scan types
  - Available in Windows, Linux, MacOS, and others
  - Command-line application and graphical user interface (GUI) version (Zenmap)
- To perform an Nmap scan at Windows command prompt:

```
nmap <IP address> <options>
```

how to write (maybe mcqs)

	NMAP COMMAND	SCAN PERFORMED
1	-sT	TCP connect scan
2	-sS	SYN scan
3	-sF	FIN scan
4	-sX	XMAS tree scan
5	-sN	NULL scan
6	-sP	Ping scan
7	-sU	UDP scan
8	-sO	Protocol scan
9	-sA	ACK scan

Nmap (Cont.)



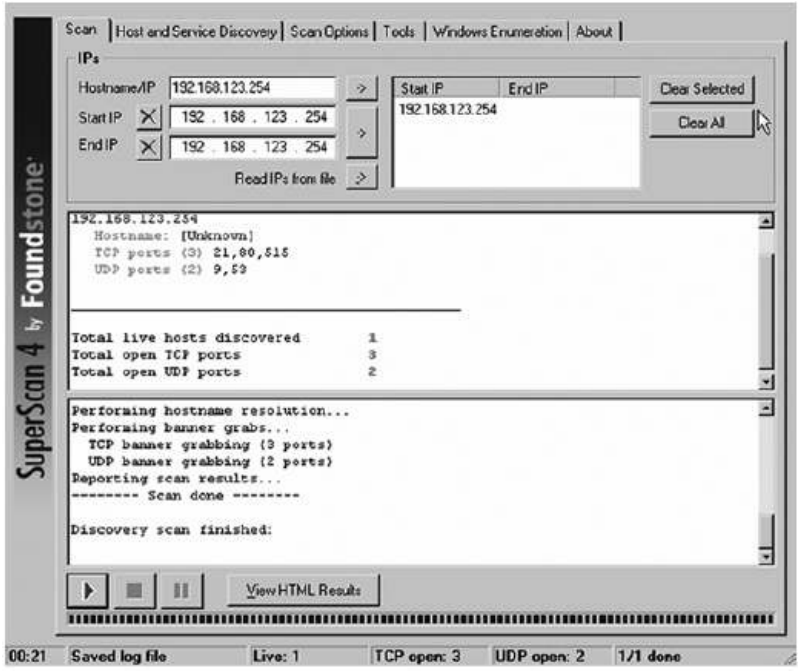
- Example: `nmap -sT 192.168.123.254`
- Response:

```
Starting Nmap 7.60 (http://nmap.org) at 2017-10-17 10:37
Central Daylight Time
Interesting ports on 192.168.123.254:
Not shown: 1711 filtered ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
2601/tcp open zebra
2602/tcp open ripd
MAC Address: 00:16:01:D1:3D:5C (Linksys)
Nmap done: 1 IP address (1 host up) scanned in 113.750
seconds
```

Using Nmap

- Results display status of port in one of three states:
  - **Open:** Target device is accepting connections on the port
  - **Closed:** Port is not listening or accepting connections
  - **Filtered:** Firewall, filter, or other network device is monitoring the port and preventing full probing to determining its status

SuperScan



SuperScan is a Windows-based port scanner designed to scan TCP and UDP ports, perform ping scans, run Whois queries, and use Traceroute.

Scanrand

- Scanning tool
- Can scan a single host or large-scan networks
- Scans ports in parallel using technique known as stateless scanning
- Used when large numbers of IP addresses need to be scanned quickly

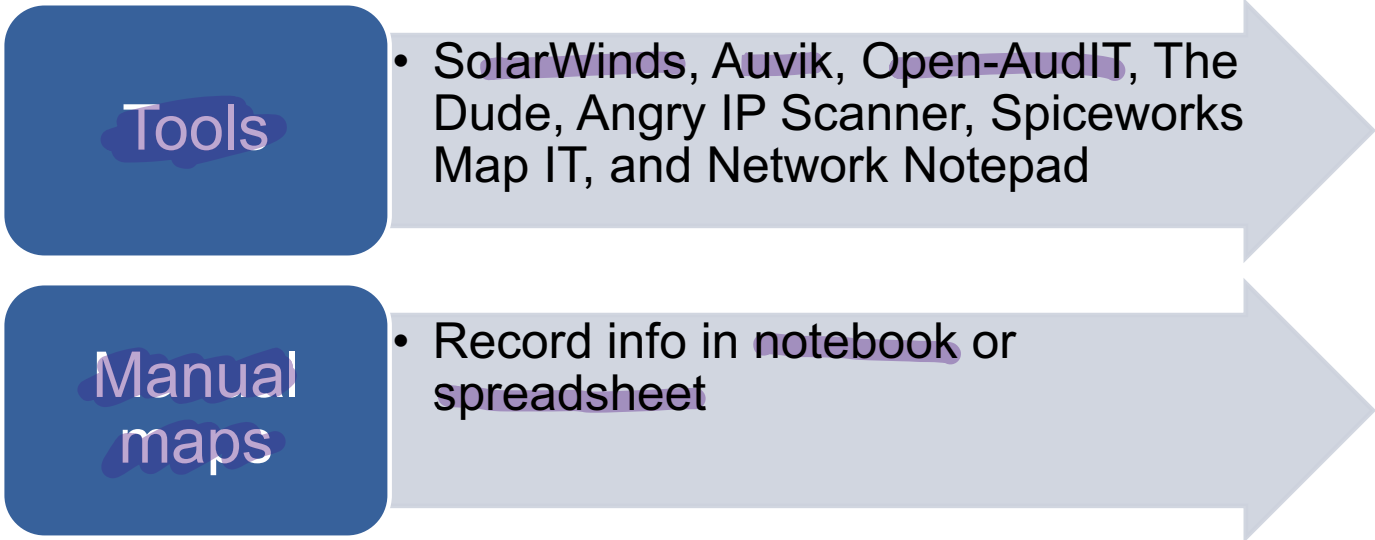
THC-Amap

THC-Amap (The Hacker's Choice – Another Mapper)

- Stores a collection of normal responses that can be provided to ports to elicit a response when scanning services that use encryption
- Allows security professionals the ability to find services that have been redirected from standard ports

Mapping the Network

- Create a network diagram to show vulnerable or potentially vulnerable devices on target network



Analyzing the Results

1. Analyze the services that have been revealed.
2. Explore vulnerabilities for each service or system.
3. Research and locate any potential exploits that can be used to attack the system.

The attacker can use a search engine to gather information about potential attacks by searching the OS and exploits.

Summary

- Identification of target systems
- Port and vulnerability scanning techniques
- Network mapping tools