Network Scanning

Strathmore
UNIVERSITY

Outline

SESSION	CONTENT
1	Describe the network Scanning Concepts
2	Use various Scanning Tools
3	Perfom Scanning to check live systems
4	Perfom scanning by using Various Scanning Techniques
5	Perfom Scanning Penetration Testing

Why do Network Scanning

- To discover live hosts, Ip address, and open ports of live hosts
- To discover OS and system architecture
- To find the services running
- To discover vulnerabilities

Network flags

- SYN – to initiate the connection
- ACK – receipt of the package
- PSH – (Push)send immediately
- RST- (Reset) reset connection
- FIN – (finish) termination of communication
- URG – (urgently) process immediately

Network Scanning

- Scanning is the process of gathering additional information about the target by using reconnaissance techniques.

- Network Scanning Refers to a set of procedures used for identifying hosts, ports and services on a network.

cont

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 needs.

Scanning Types

Port Scanning- Lists the open ports and services.

Network Scanning - Lists IP addresses

Vulnerability Scanning- Shows the presence of known weaknesses.

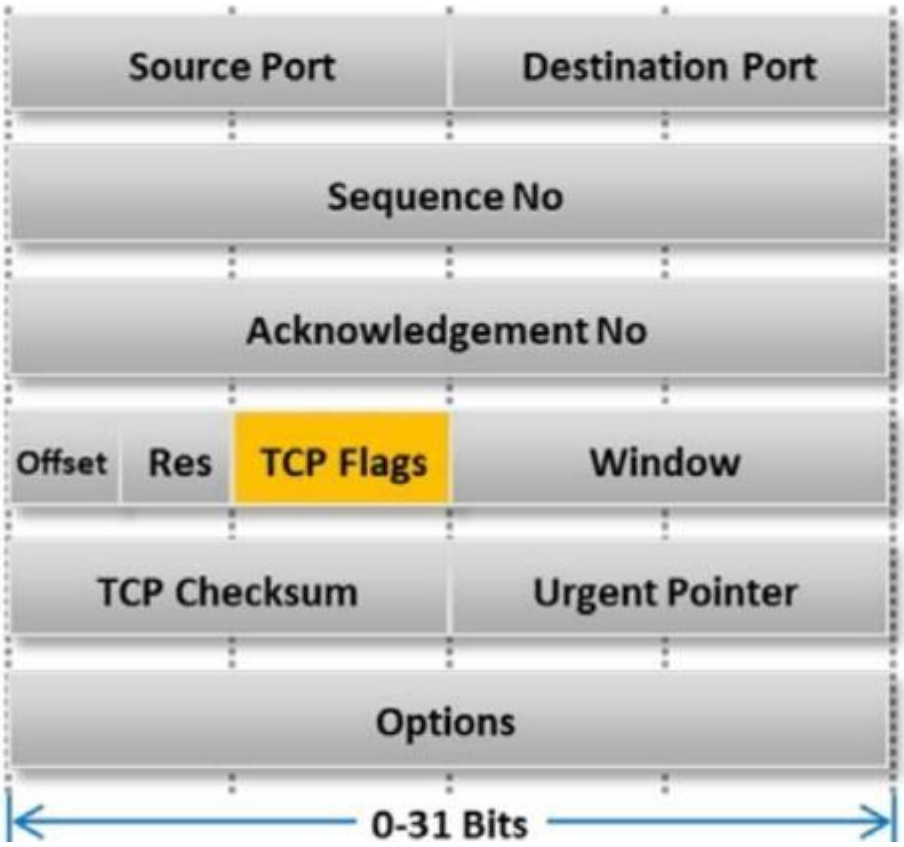
TCP/IP Communication

- TCP is connection-oriented, which prioritizes connection establishment before data transfer between applications.

- This type of communication between protocols is possible because of the three way handshake

Tcp header

TCP header contains various flags that control the transmission of data across a TCP connection.



Source Port | Destination Port

Sequence No

Acknowledgement No

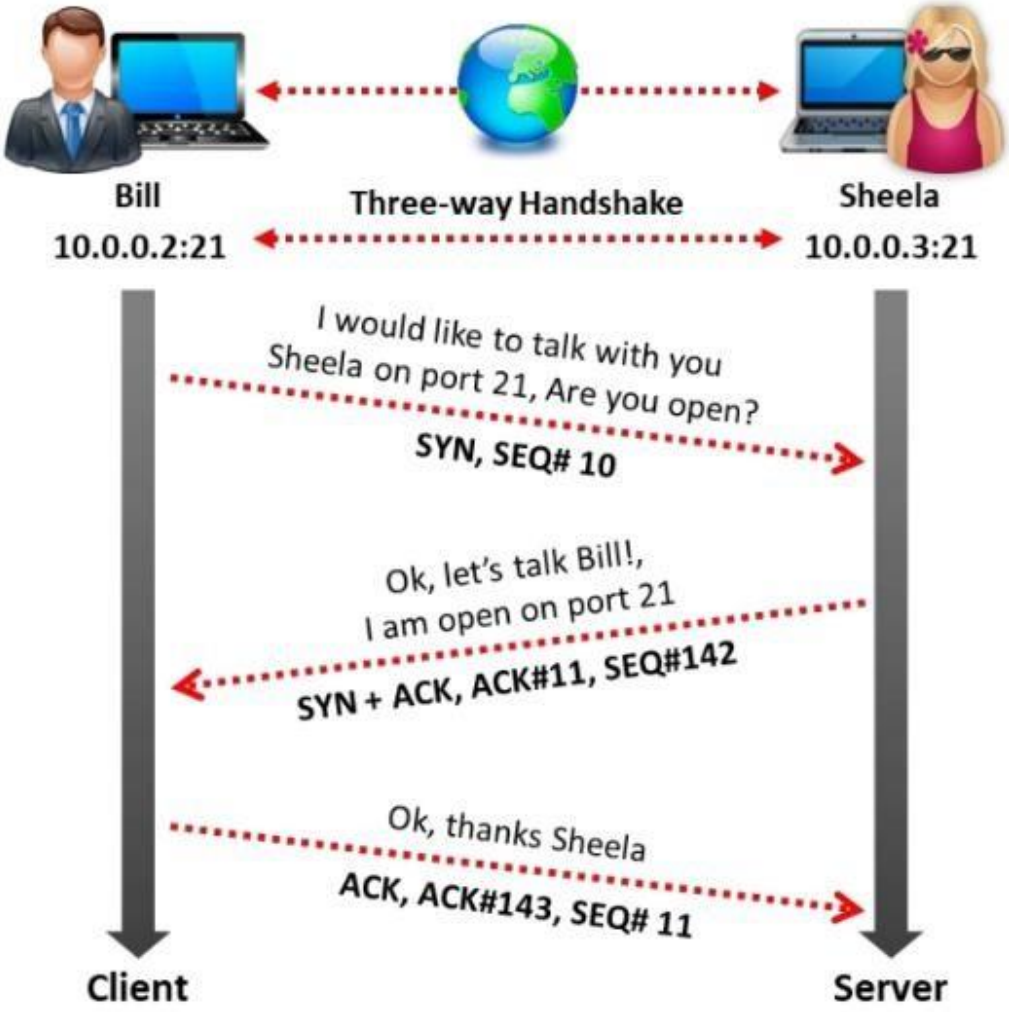
Offset | Res | TCP Flags | Window

TCP Checksum | Urgent Pointer

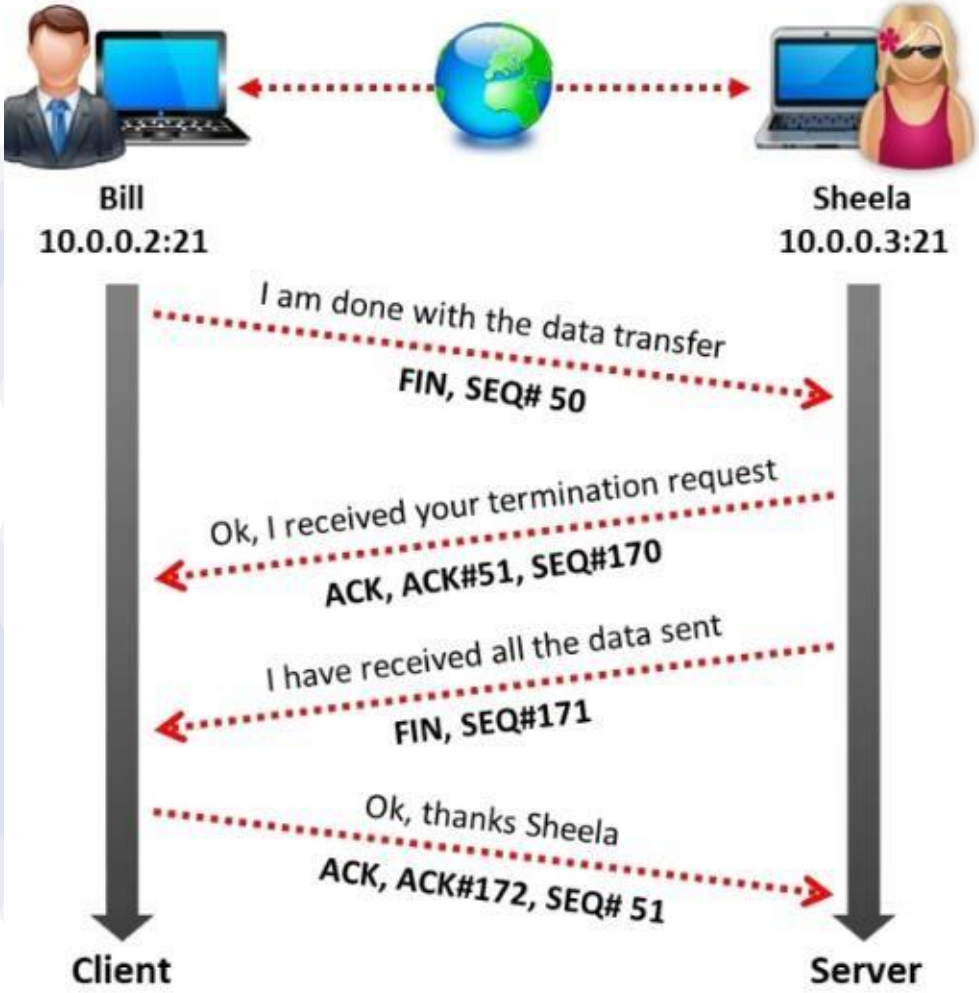
Options

0-31 Bits

Session Establishment



Session termination



Scanning Tools

Scanning tools scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info and information about all TCP/IP, UDP open ports

Nmap

Nmap is a security scanner for network exploration and hacking. It allows you to discover hosts and services on a computer network, thus creating a "map" of the network.

It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal.

Hping2/Hping3

- ICMP ping hping3 -1 <ip address>
- ACK scan on port 80 hping –A <ipaddress> -p 80
- UDP scan on por 80 hping3 -2 <ipaddress> -p80
- Collecting

NETSCAN

- Allows you to troubleshoot, monitor, discover and detect devices on your network.

Benefits

- Produce reports on web browser
- Info gathering is simpler

Scanning tools for mobile

- IP scanner-Used for IOS scan in local area network to determine identity of machines
- Fing-Discovers all devices connected to a WiFi network, Displays MAC address and device manufacturer.etc

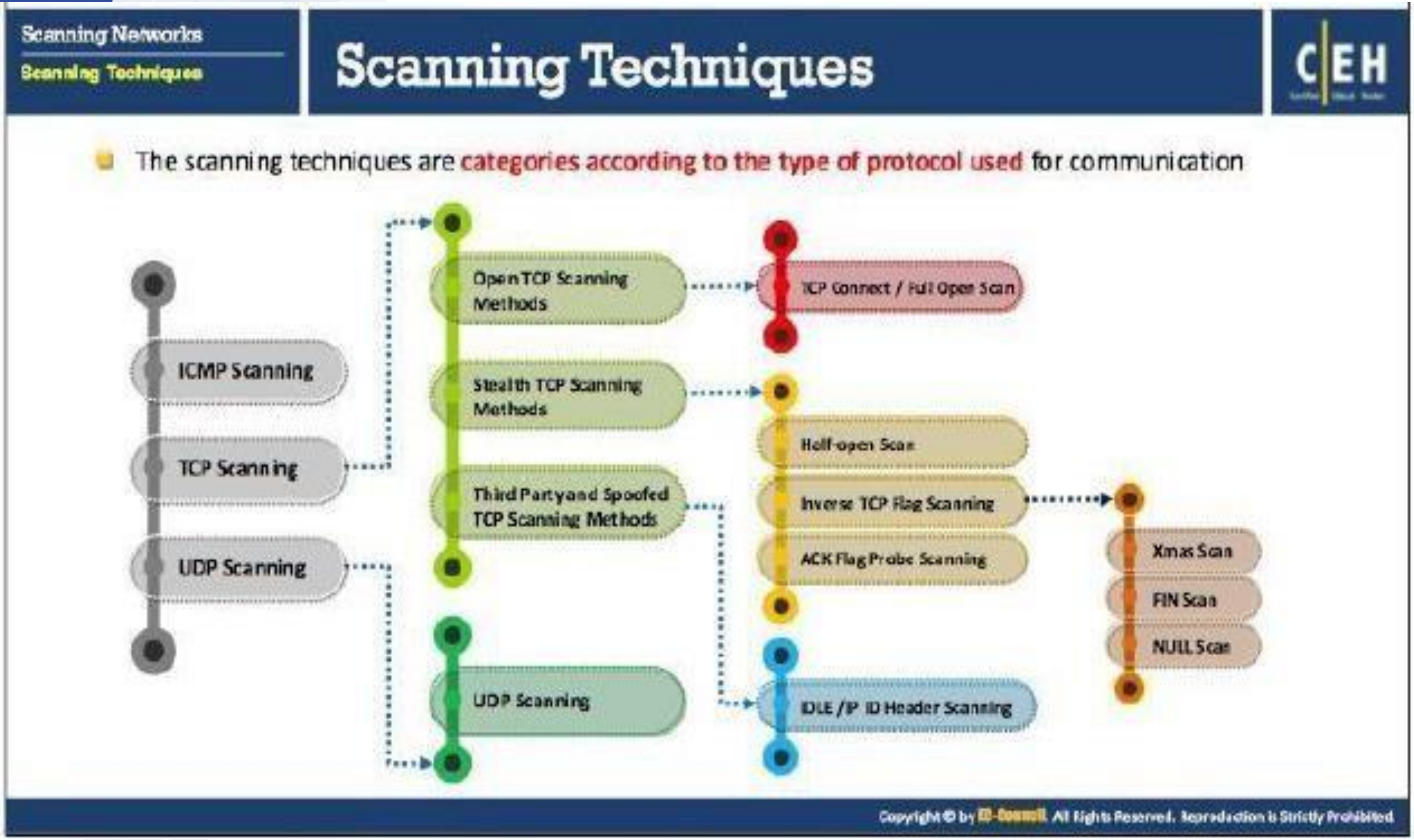
Scanning techniques

- Scanning-Gather info about systems that are alive and responding to the network.
- Port scanning helps an attacker identify open ports on a targeted machine

Scanning Techniques

- Ping Sweep – ICMP Scanning
- TCP scan
- Half open Scan – Stealth Scan
- Inverse TCP Scans – Using FIN, URG, OSH flags
- Xmas scan
- ACK flag scan
- UDP scan

Scanning techniques



Scanning Networks

Scanning Techniques

Scanning Techniques

C|EH

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

ICMP Scanning

TCP Scanning

UDP Scanning

Open TCP Scanning Methods

Stealth TCP Scanning Methods

Third Party and Spoofed TCP Scanning Methods

UDP Scanning

TCP Connect / Full Open Scan

Half-open Scan

Inverse TCP Flag Scanning

ACK Flag Probe Scanning

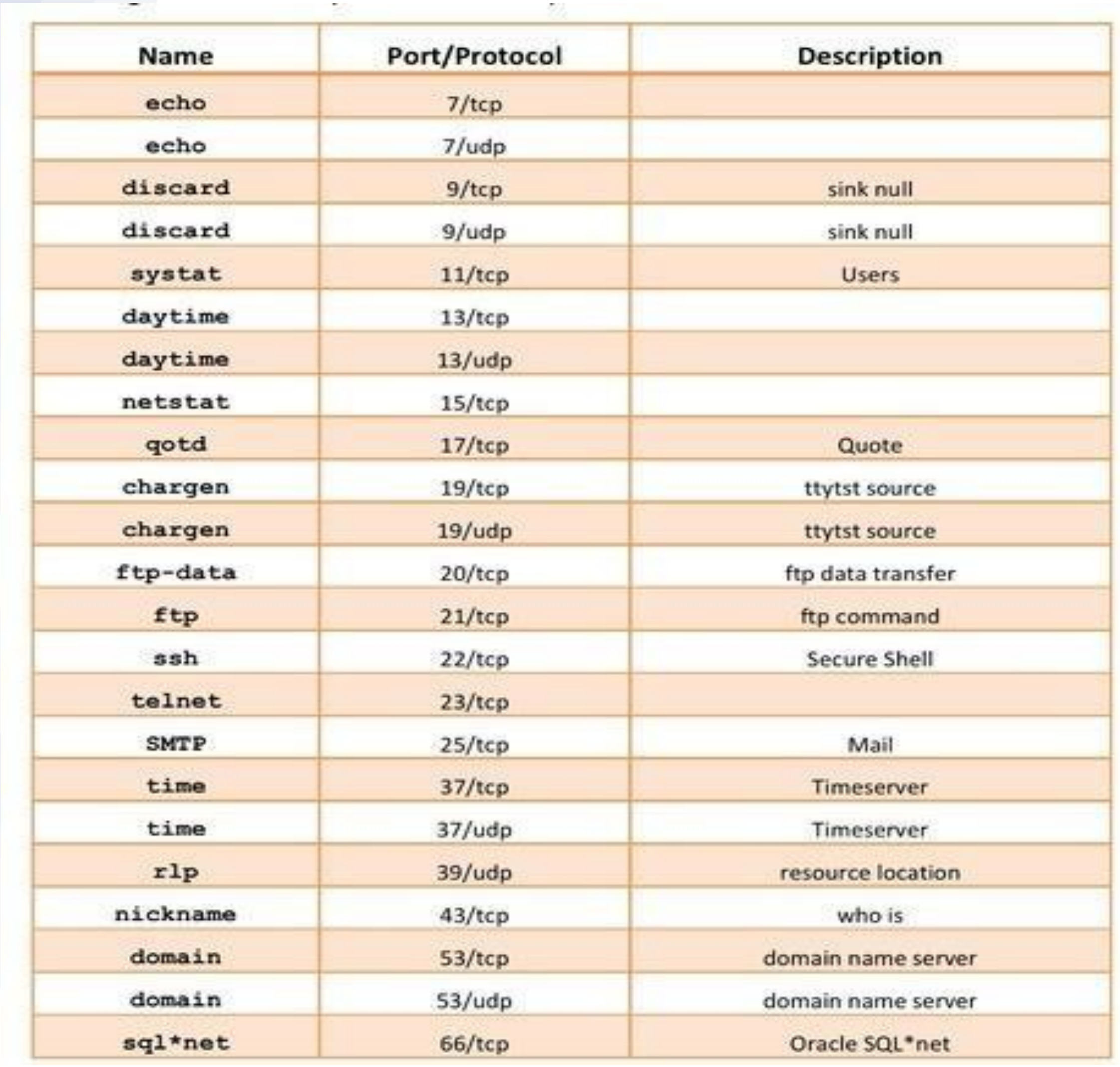
IDLE / IP ID Header Scanning

Xmas Scan

FIN Scan

NULL Scan

Ports



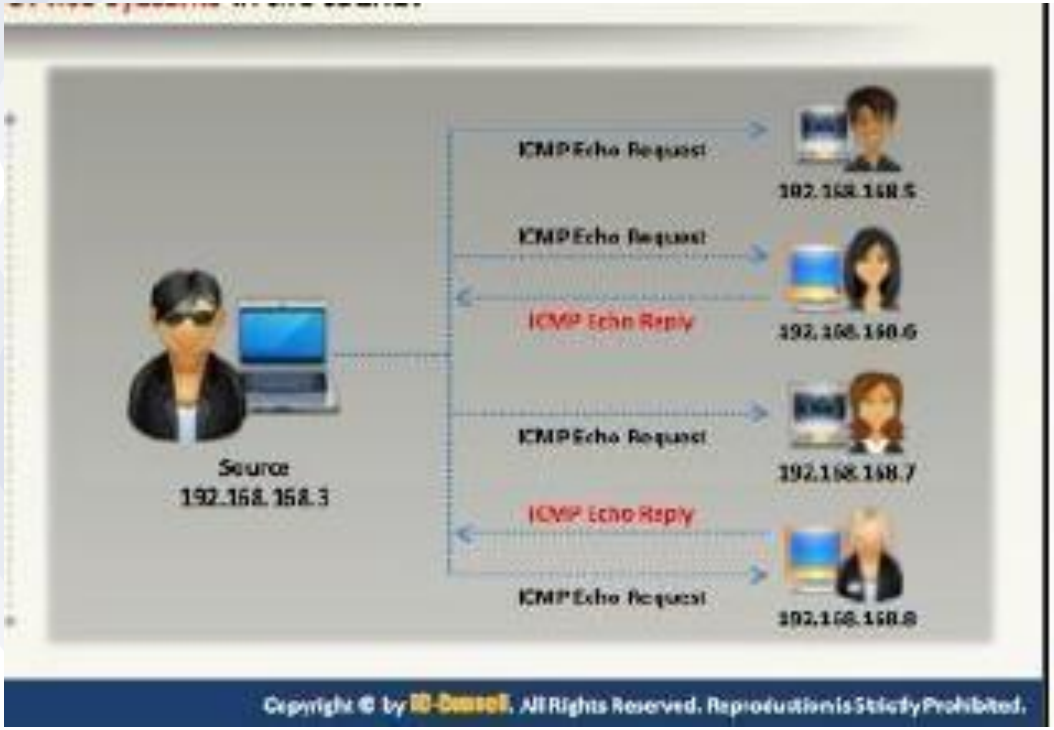
Name	Port/Protocol	Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	
daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
SMTP	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nickname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net

ICMP Scanning

- Ping scan involves sending ECHO request to a host and it replies with an ICMP ECHO reply.
- Useful to locate active devices or determine if ICMP is passing through a firewall.

Ping sweep/ICMP sweep

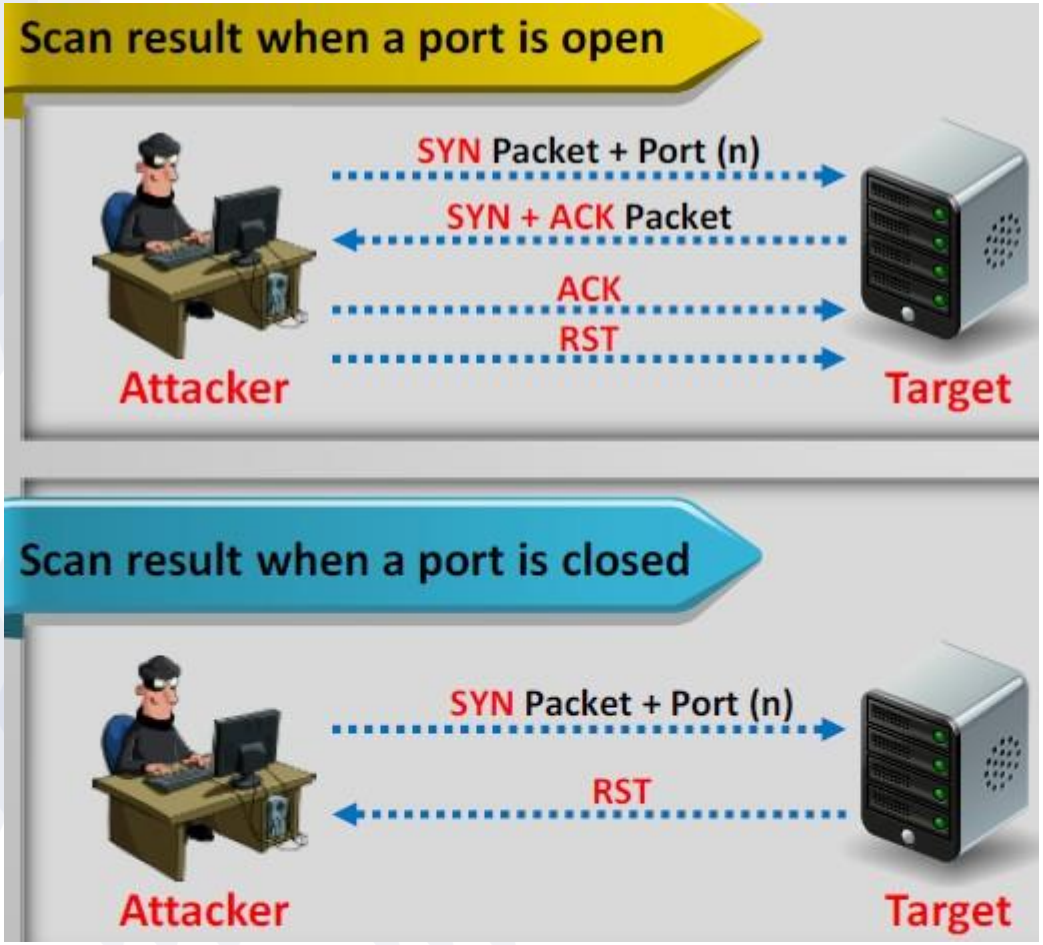
- Determines live hosts from a range of IP addresses by sending ICMP ECHO request to multiple hosts.



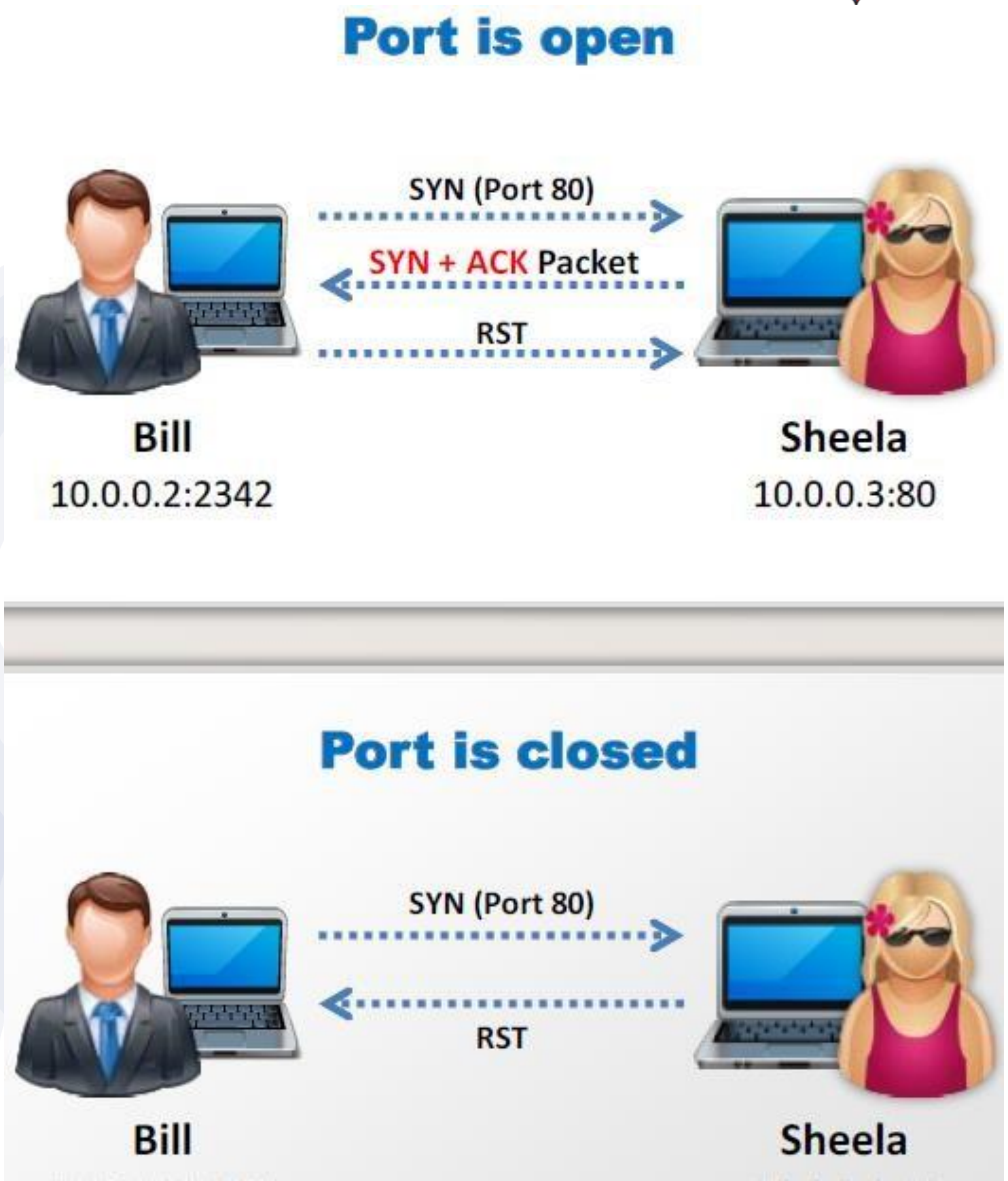
Ping sweep Tools

- Angry IP scanner-scans a range of IP addresses and ports present. Pings to check if they are alive. Can show NET BIOS information
- Visual Ping Tester
- Advanced IP Scanner
- MegaPing

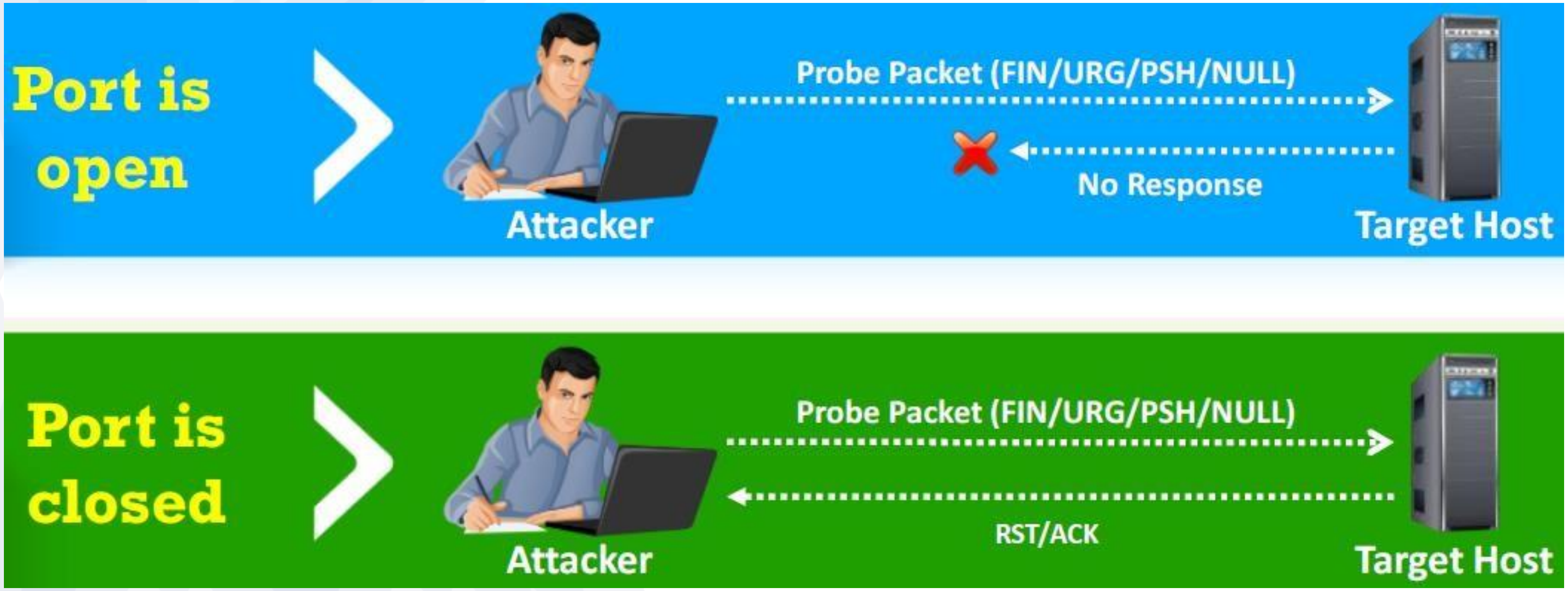
TCP Connect/Full Open Scan



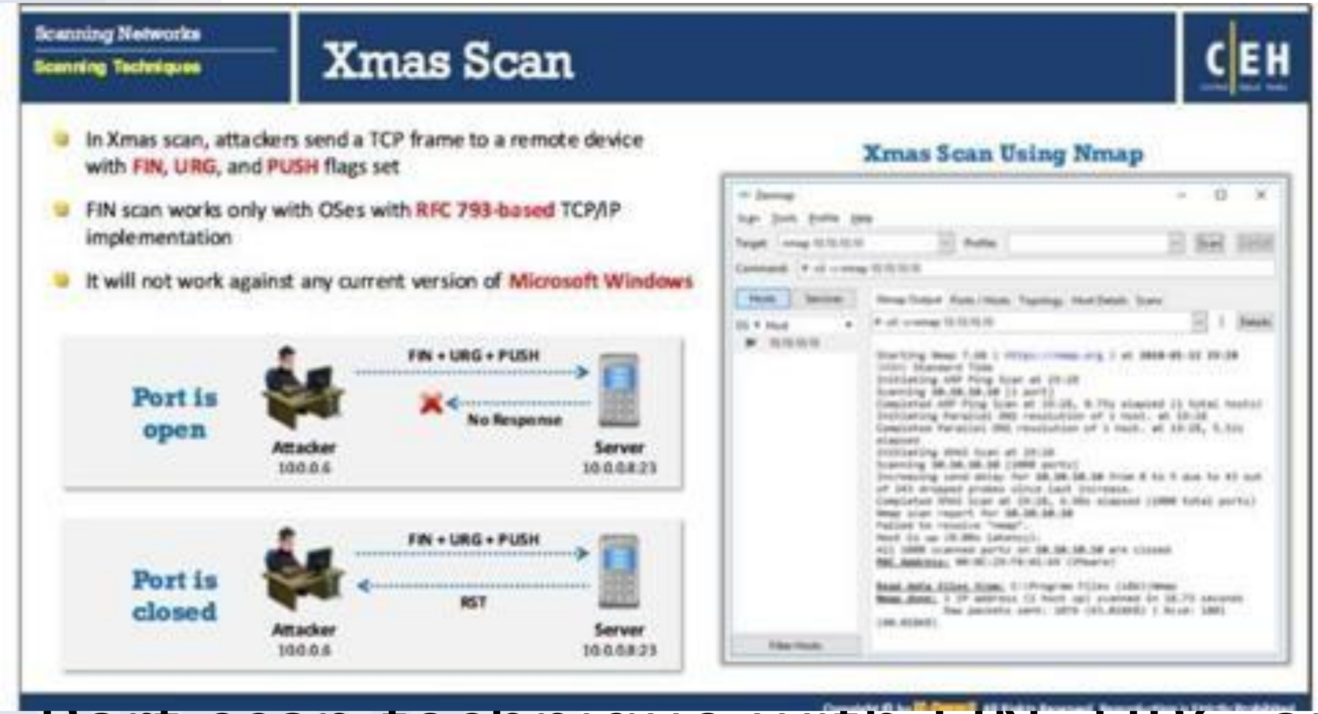
Stealth scan(Half open scan)



Inverse TCP Flag Scanning



XMAS scan



Scanning Networks

Scanning Techniques

Xmas Scan

- 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

```
Starting Nmap 7.[illegible] ( https://nmap.org ) at [illegible]
[illegible] Standard Time
Initiating ARP Ping Scan at [illegible]
Scanning [illegible] [1 port]
Completed ARP Ping Scan at [illegible], [illegible] elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at [illegible]
Completed Parallel DNS resolution of 1 host. at [illegible], [illegible]
elapsed
Initiating XMAS Scan at [illegible]
Scanning [illegible] [1000 ports]
Increasing send delay for [illegible] from 0 to 5 due to [illegible] out
of [illegible] dropped probes since last increase.
Completed XMAS Scan at [illegible], [illegible] elapsed (1000 total ports)
Nmap scan report for [illegible]
Failed to resolve "nmap".
Host is up ([illegible] latency).
All 1000 scanned ports on [illegible] are closed
MAC Address: [illegible] (VMware)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in [illegible] seconds
           Raw packets sent: [illegible] | Rcvd: [illegible]
([illegible])
```

- Port scan technique with FIN, URG and PUSH flags set to send a TCP frame to a remote device.

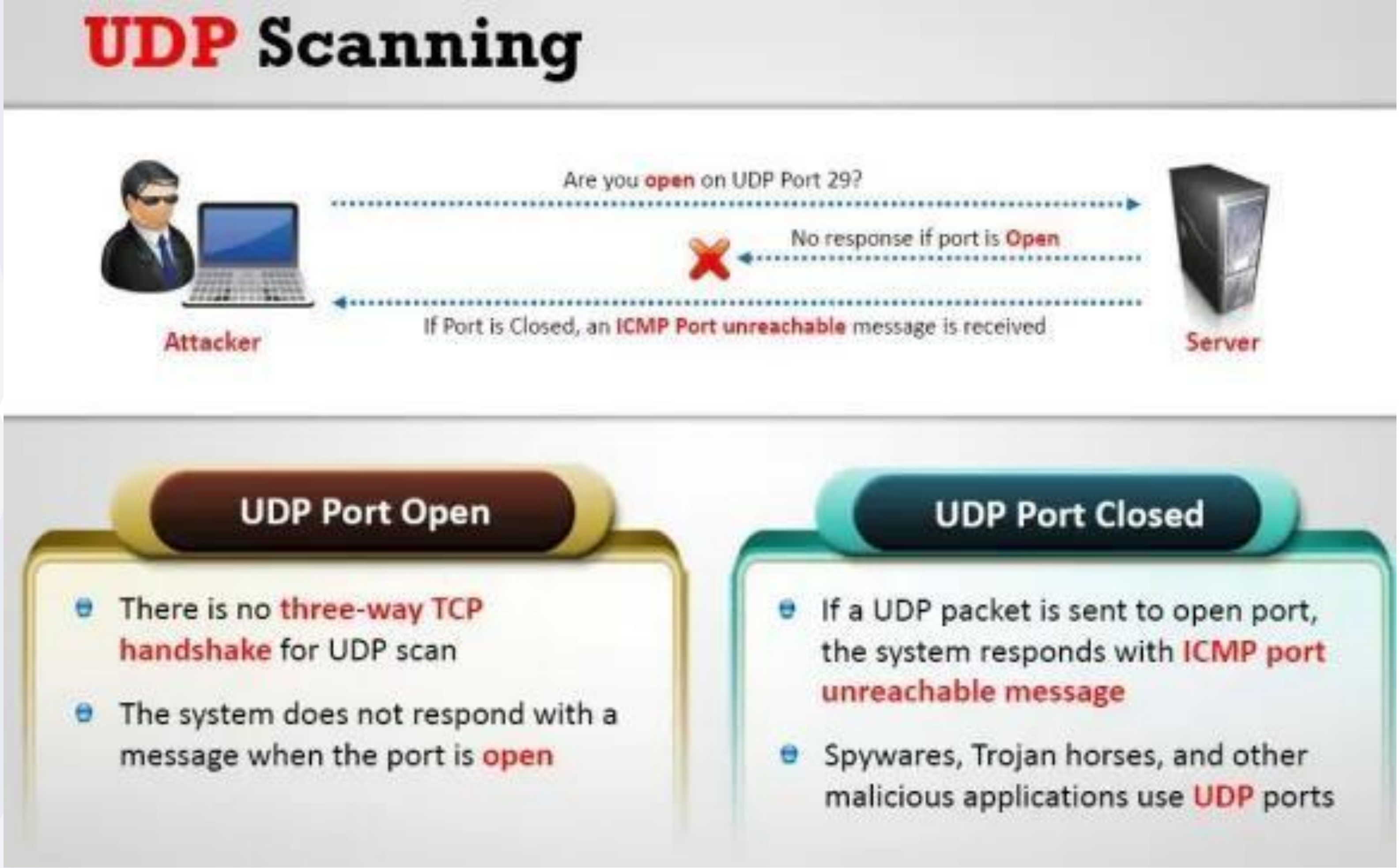
ACK Flag Probe Scanning

- Attackers send TCP probe packets with ACK flag to a remote device then analyzes the header information of received RST packets to find if a port is open or closed.
- Used to check filtering system of a target.Attacker sends random sequence number,no response implies that port is not filtered.

Categories of ACK Flag Probe scanning

- TTL based ACK Flag probe scanning- Send ACK probe packtes to different TCP ports then amalyze TTL field valueof RST packets received. I f a port has a boundary less than 64 then the port is open.
- Window BASED ACK flag probe scanning-Send an ACK probe packet to different TCP ports then analyze window field value of received RST packets.
- Advantage-Evades IDS
- Disadvantage-Slow and can exploit older OS

UDP scanning



UDP Scanning

Are you open on UDP Port 29?

No response if port is Open

If Port is Closed, an ICMP Port unreachable message is received

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 open port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports

SSDP and LIST Scanning

- List Scanning- Generates and prints a list of IP’s names without scanning hosts without pinging.
- Advantages
- List scan perform a sanity check.
- List scan detects incorrectly identified IP addresses on command line.

SSDP Scanning(Simple Service Discovery Protocol)

- This is a network protocol that communicates with machines when querying tem within a routable IPv4 or IPV6 multicast address.
- Vulnerabilities allow attackers to launch buffer overflows or DOS.

Port Scanning Countermeasures

- Configure firewall and IDS to detect and block probes.
- Run port scanning tools on host to determine whether firewall detects any port scanning actively.
- Update router,IDS and firewall firmware
- Ensure there are anti spoofing and anti scanning rules configured.

IDS/Firewall Evasion Technique

- Packet Fragmentation-Send fragments probe packets to intended server that reassembles after receiving fragments.
- Source Routing-Specify routing path for malformed packet to reach intended server
- IP Address Spoofing –Change source IP address of decoy so firewall doesnt trace ip address
- Proxy server-Hide actual source of scan and evade IDS restrictions

Banner Grabbing/OS Fingerprinting

- Method used to determine the operating system running on a remote target system.
- Identifying an OS you know what vulnerabilities are present on a system.

Active Banner Grabbing

- Special crafted packets are sent to a remote OS and responses are noted. Responses are compared to DB.

Passive Banner grabbing

- Banner Grabbing from error messages-Error messages provide info on type of OS
- Sniff network-Capture and analyze packets to know more about the target.
- Banner grabbing from page extension-URL

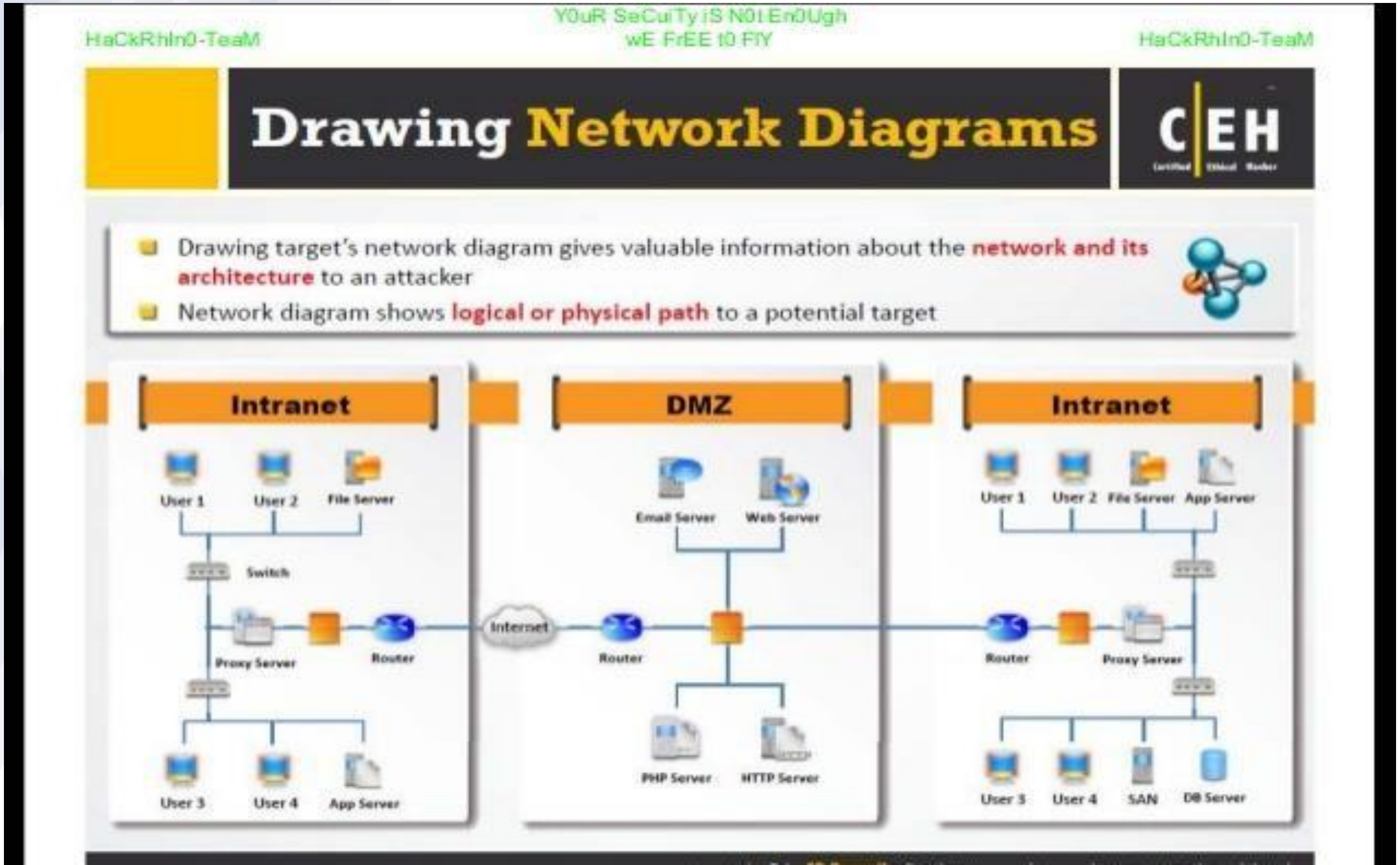
Banner Grabbing Countermeasures

- Disable or change the banner
  - Display false banners to mislead attackers.
  - Turn off unnecessary services on the network host.
  - Use Server Masks
  - Change ServerSignature line to ServerSignature Off in http.conf

- Hiding File extensions from Web Pages
  - File extensions reveal technology used.
  - Hide file extensions to mask web technology.
  - Change application mappings ie .asp
  - Apache users can use mod_negotiation directives.

Draw Network Diagrams

- Helps in analyzing complete network topology/architecture.



Drawing Network Diagrams

C|EH Certified Ethical Hacker

- 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

Network Discovery & Mapping tools

- Network Topology Mapper
- The Dude
- LANState
- InterMApper

Network Discovery tools for mobile

- Scany
- Network “Swiss-Army-Knife”
- Fing
- Network Mapper

Countermeasures

- Firewall and IDS Rules to detect and block probes
- Check router, IDS, firewalls are updated to its latest
- Use custom rule set to block unwanted ports
- Filter all ICMP messages at firewalls and routers
- Anti Spoofing Rules are properly configured or not

Thank you!

Any Questions?