Scanning

TOPICS

- Overview of Network Scanning
- Detecting Live Hosts
- Checking for Open Ports
- OS Fingerprinting
- Banner Grabbing
- Countermeasures

RECALL – PHASES OF HACKING

NETWORK SCANNING

- A set of procedures of identifying hosts, open ports and services in a network
- One of the components of intelligence gathering an attacker uses to profile a target
- Objectives
  - Discover live hosts and their open ports
  - Discover running services on hosts
  - Discover operating systems on live hosts

TYPES OF SCANNING

- Host scanning
  - Checking for live hosts on the network
- Port scanning
  - Checking for the open ports on live hosts in the network
- OS and Vulnerability scanning
  - Checking for vulnerabilities present on the system

DETECTING LIVE HOSTS – ARP SCANNING

- Address Resolution Protocol
  - ARP requests can determine host MAC addresses if a corresponding ARP reply is returned
- ARP Scanning
  - Examines ARP messages from the local network to determine live hosts
  - Works only on the local network

DETECTING LIVE HOSTS – ARP SCANNING

Who is 192.168.1.1?

I am 192.168.1.1
My MAC address is ….

Who is 192.168.1.2?

I am 192.168.1.2
My MAC address is ….

Live hosts:
192.168.1.1
192.168.1.2
192.168.1.4

Who is 192.168.1.3?

Who is 192.168.1.4?

I am 192.168.1.1
My MAC address is ….

ARP SCAN TOOL: NETDISCOVER

- Active Scan (Default)
  - Sends a series of ARP requests to a specified range to generate ARP replies
  - netdiscover –i <interface> –r <subnet>
- Passive Scan:
  - Only collects ARP requests sent by live hosts
  - Does not send its own ARP requests
  - netdiscover –i <interface> –p

DETECTING LIVE HOSTS – ICMP SCANNING

- Ping
  - ICMP echo requests can identify live hosts if a corresponding echo reply is returned
  - Determine if ICMP passes through firewalls

    Note: No reply doesn't necessarily mean that the host is not live

PING SWEEP

- Used to determine live hosts from a range of IP addresses
- Consists of ICMP echoes sent to multiple hosts
- Creates an inventory of live systems on the subnet

PING SWEEP

Live hosts:
192.168.1.1
192.168.1.2
192.168.1.4

Echo is 192.168.1.1

Echo reply

Echo: 192.168.1.2

Echo reply

Echo: 192.168.1.3?

Echo 192.168.1.4?

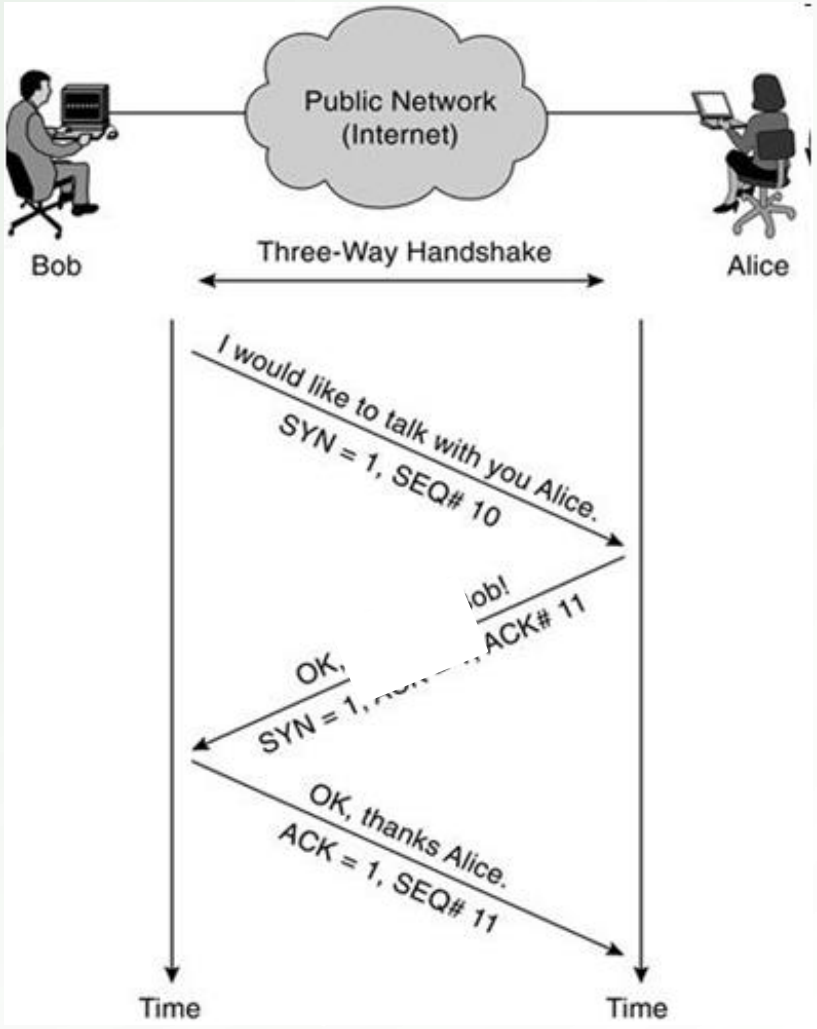
Echo reply

PING SWEEP TOOLS:

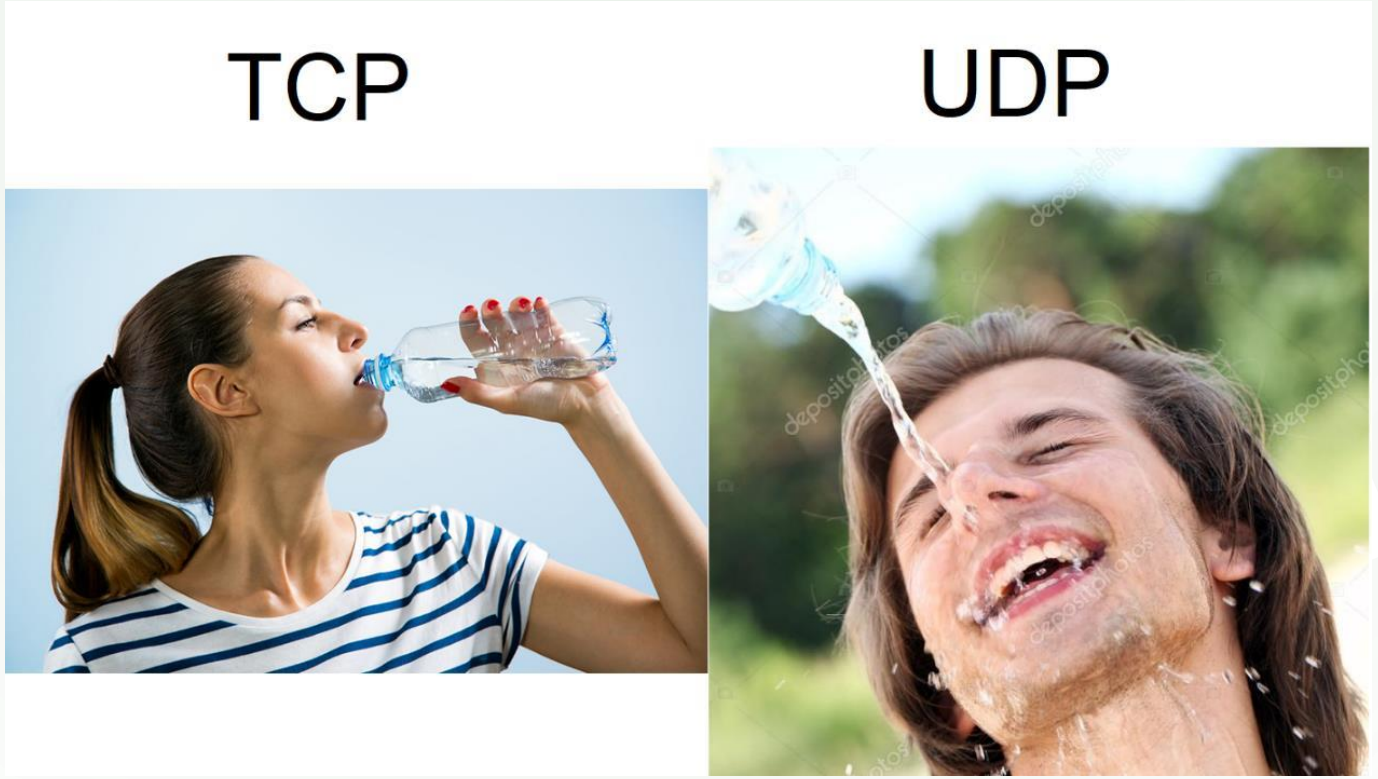
- Nmap
  - Network scanning tool with ping sweep functionality
  - Has a GUI called Zenmap
  - **nmap –sn <subnet>**

REVIEW: TCP CONNECTION ESTABLISHMENT

- Step 1: Bob initiates a connection with Alice with the SYN flag set
- Step 2: Alice replies with a packet where both SYN and ACK flags are set
- Step 3: Bob responds with an ACK flag



TCP VS UDP



REVIEW: TCP COMMUNICATION FLAGS

SYN (Synchronize)	• Initiates a connection between hosts
RST (Reset)	• Resets a connection
ACK (Acknowledgment)	• Acknowledge received data
FIN (Finish)	• No more transmissions
PSH (Push)	• Sends all buffered data immediately
URG (Urgent)	• Data in packet should be processed ASAP

CHECKING FOR OPEN PORTS – PORT SCANS

- Identifies open ports on a target server or host on the network
- Often used by admins to verify security policies and by hackers to determine running services
- Recall: Each TCP or UDP port number is often associated with a specific type of application

COMMON PORTS

Port	Service
TCP 20, 21	FTP
TCP 22	SSH
TCP 23	Telnet
TCP 25	SMTP
TCP and UDP 53	DNS
UDP 67	DHCP server
UDP 69	TFTP
TCP 80	HTTP
TCP 443	HTTPS

TCP/UDP SCANS

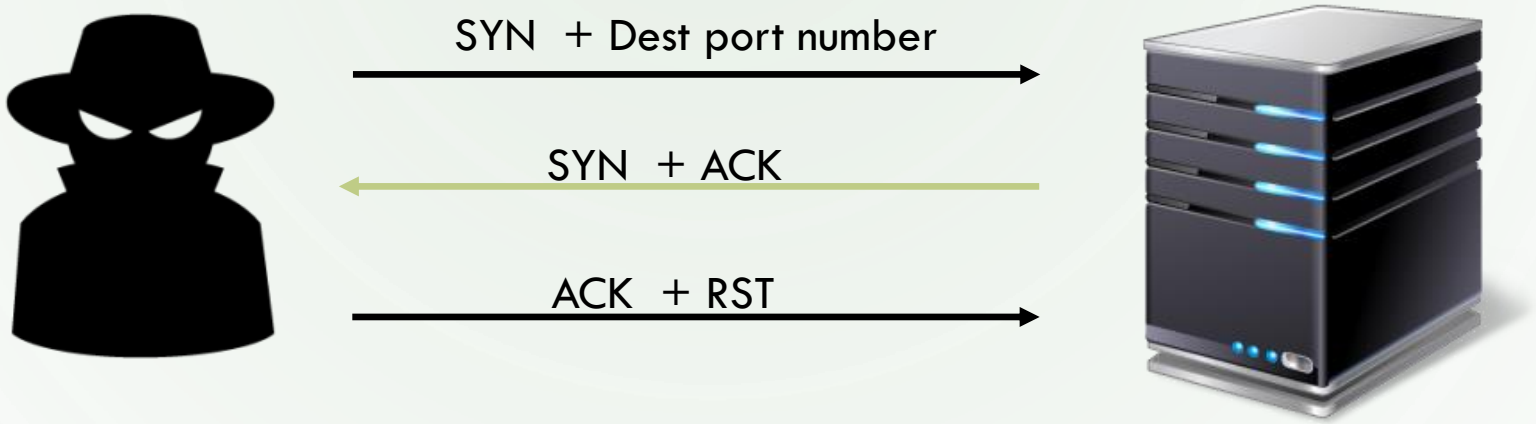
- TCP Connect Scan
- Stealth Scans
  - TCP SYN (Half-open) Scan
  - Xmas Scan
  - FIN Scan
  - Null Scan
- TCP ACK Scan
- UDP Scan

TCP CONNECT SCAN

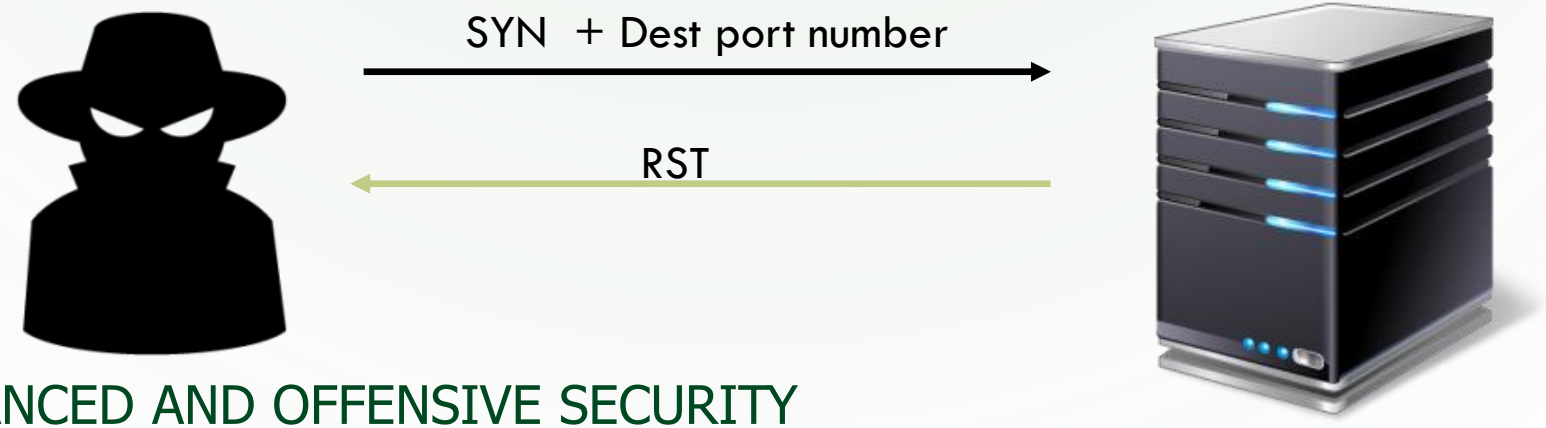
- One of the most reliable methods of port scanning
- Host attempts to establish a connection with a target port. If this succeeds, port is open
- Easy to detect and filter
- Could be logged by the target host
- Nmap

TCP CONNECT SCAN

- Scan result if open:



- Scan result if closed:

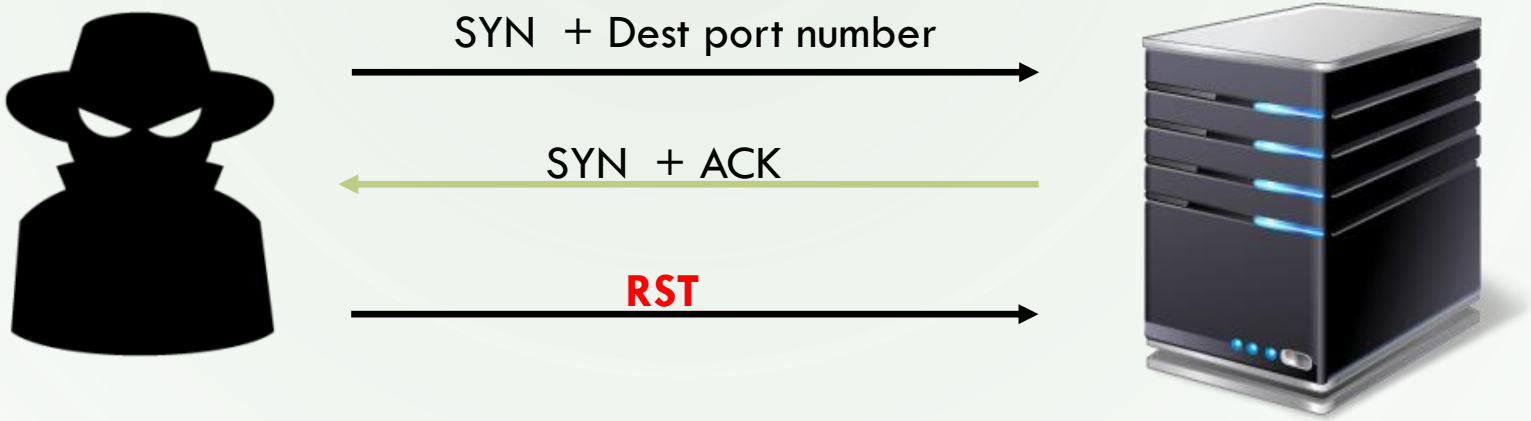


TCP SYN (HALF-OPEN) SCAN

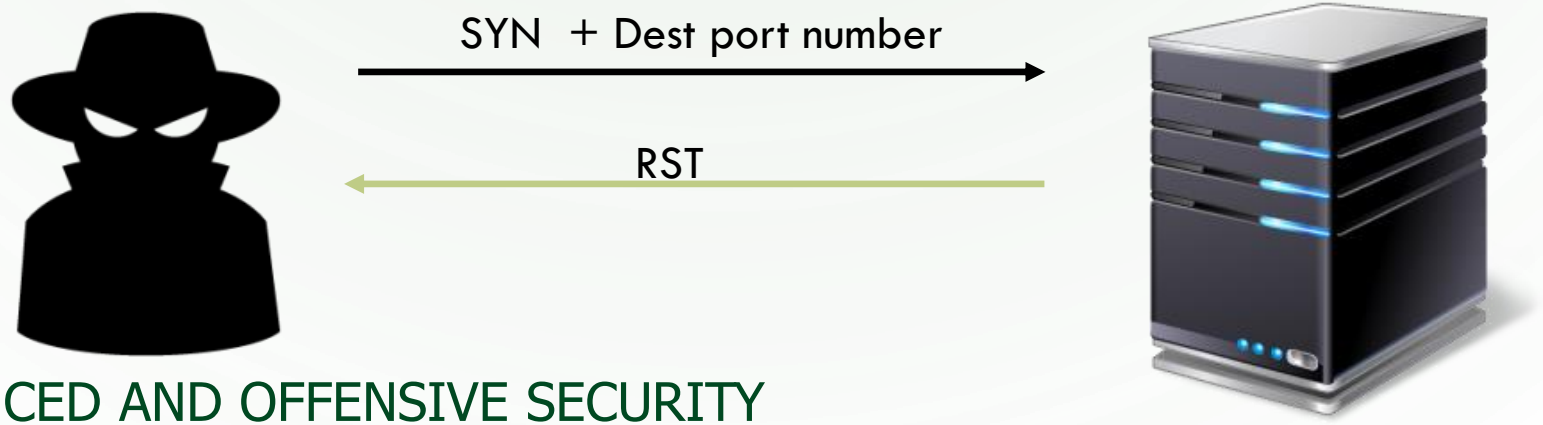
- Sends only a single packet
- Performs only a partial 3-way handshake; so no connection established
- Is considered a stealth scan because service is not notified of a connection

TCP SYN SCAN

- Scan result if open:



- Scan result if closed:

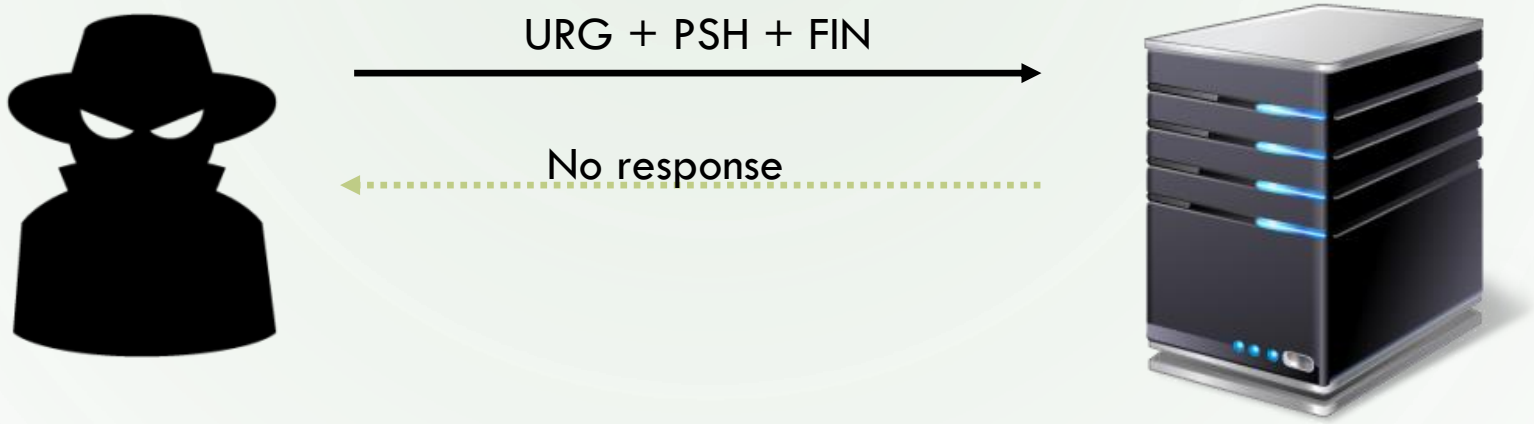


XMAS SCAN

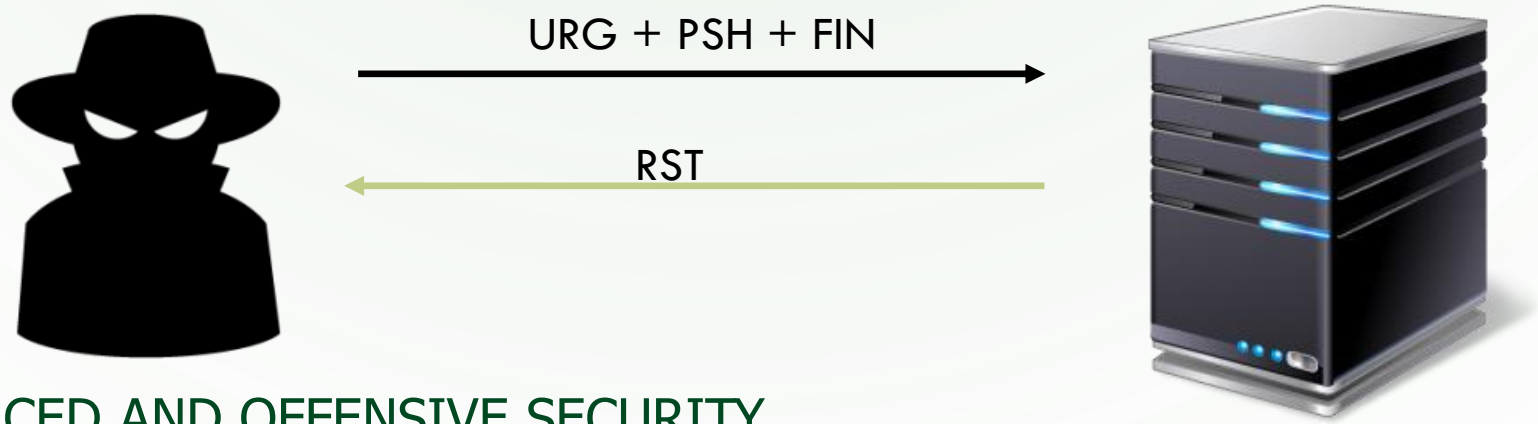
- A type of scan that sets all 6 flags in the TCP header
- Can cause some systems to hang
- Usually a variation that uses only URG-PSH-FIN is used
- Works only on Unix platforms – shows all ports as open if used against Windows

XMAS SCAN

- Scan result if open:



- Scan result if closed:

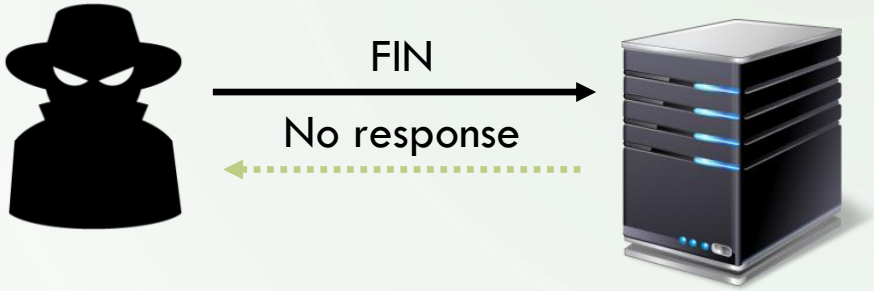


FIN AND NULL SCANS

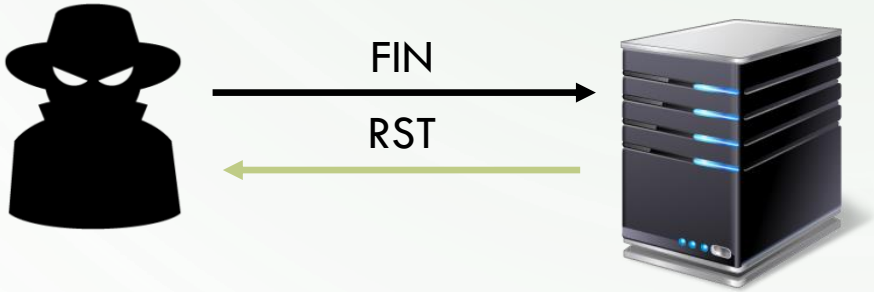
- Attacker sends a packet with only the FIN flag or no flags (null) set in the TCP header
- Target replies only if port is closed
- Works only against Unix platforms

FIN SCAN

- Scan result if open:

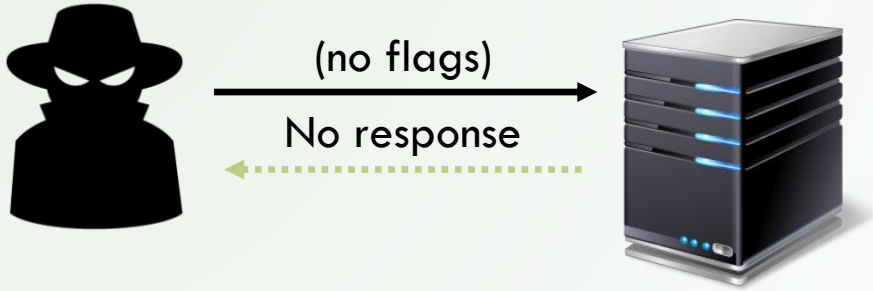


- Scan result if closed:

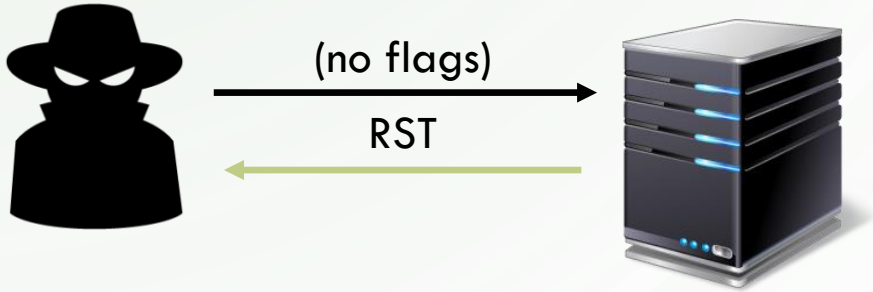


NULL SCAN

- Scan result if open:



- Scan result if closed:



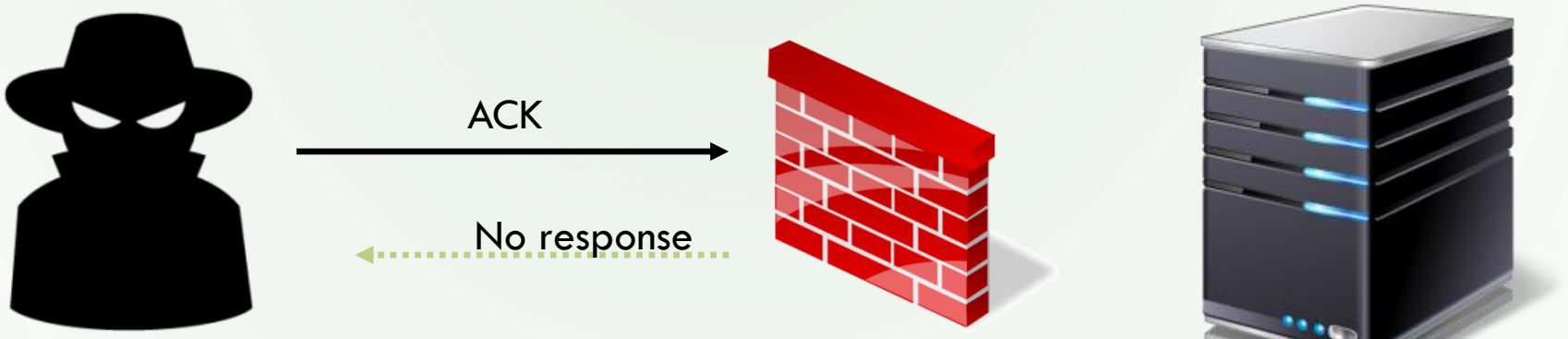
ACK SCAN

- A type of scan that is used to check for the presence of a firewall

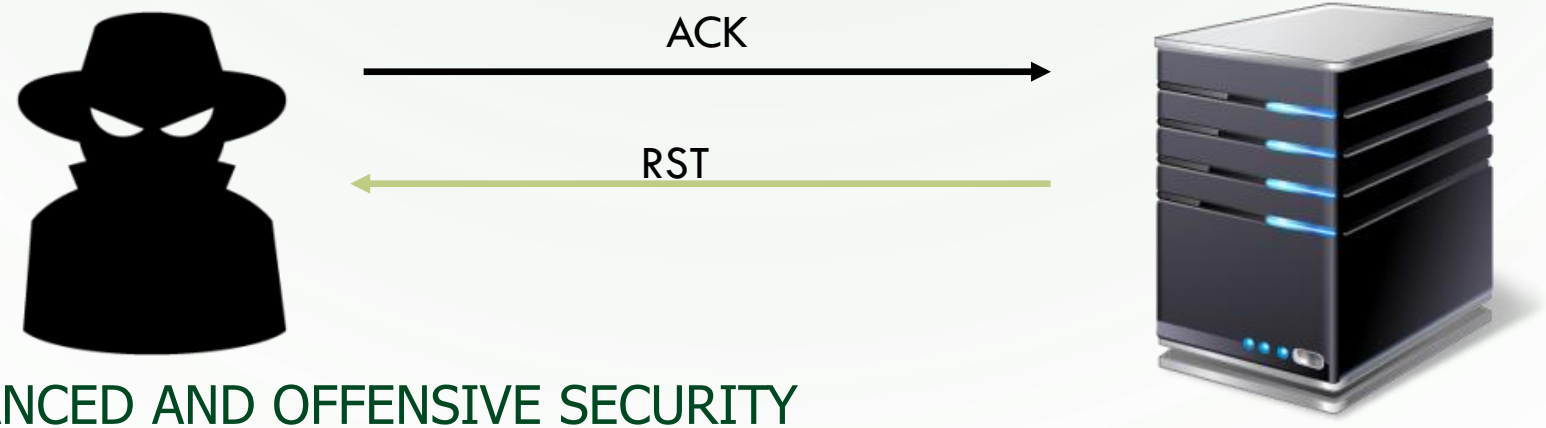
- Firewalls normally block an ACK with no previous SYN

ACK SCAN

- Scan result if there is a firewall:



- Scan result if there is no firewall:

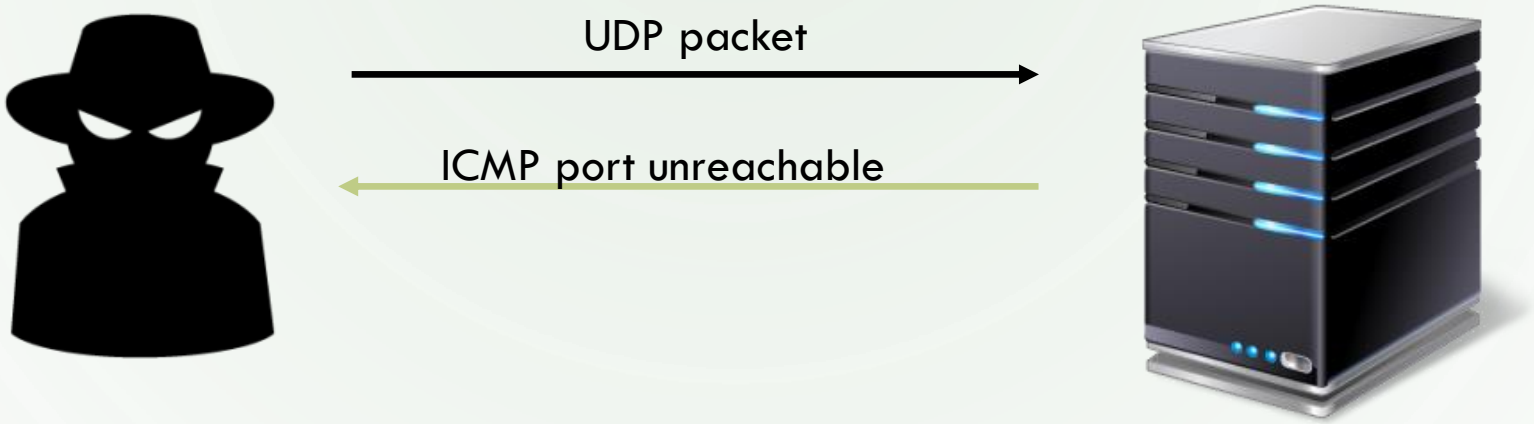


UDP SCAN

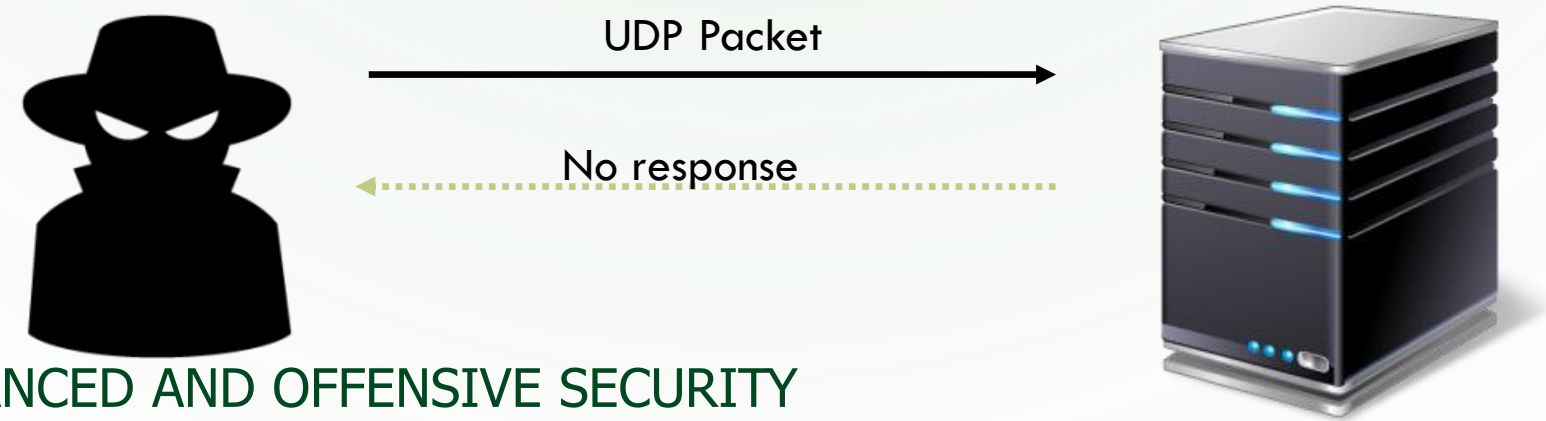
- Checks for closed UDP ports
- Cannot always distinguish between open and filtered ports
- Closed ports return an ICMP port unreachable message if probed

UDP SCAN

- Scan result if closed:



- Scan result if open or filtered by a firewall:



PORT SCAN TOOL: NMAP

- Syntax: **nmap <scan option> <target>**
- Scan options
  - **-sT** : Connect scan
  - **-sS** : SYN scan
  - **-sA** : ACK scan
  - **-sN, -sF** or **-sX** : Null / FIN / Xmas scan
  - **-sT** : SYN scan
  - **-sU** : UDP scan

IDENTIFY THE TYPE OF SCAN, PORT BEING TESTED, AND CONCLUSION OF THE TEST (E.G. OPEN, CLOSE, OPEN OR FILTERED, FILTERED, UNFILTERED, ETC.)

```
0.163866 192.168.1.100 -> 192.168.1.104 TCP 59079 > 67 [SYN] Seq=0 Len=0
MSS=1460 TSV=18703363 TSER=0 WS=2

0.163956 192.168.1.104 -> 192.168.1.100 TCP 67 > 59079 [RST, ACK] Seq=0
Ack=1 Win=0 Len=0
```

TCP Connect or TCP SYN scan

67

closed

Example from midnightresearch.com

IDENTIFY THE TYPE OF SCAN, PORT BEING TESTED, AND CONCLUSION OF THE TEST (E.G. OPEN, CLOSE, OPEN OR FILTERED, FILTERED, UNFILTERED, ETC.)

```
0.425238 192.168.1.100 -> 69.89.27.228 TCP 63851 > www [ACK] Seq=0 Ack=0
Win=2048 Len=0

0.459511 69.89.27.228 -> 192.168.1.100 TCP www > 63851 [RST] Seq=0 Len=0
```

TCP ACK Scan
80
Unfiltered port

Example from midnightresearch.com

IDENTIFY THE TYPE OF SCAN, PORT BEING TESTED, AND CONCLUSION OF THE TEST (E.G. OPEN, CLOSE, OPEN OR FILTERED, FILTERED, UNFILTERED, ETC.)

```
0.695056 192.168.1.100 -> 72.14.207.99 TCP 59002 > www [SYN] Seq=0
Len=0 MSS=1460

0.844707 72.14.207.99 -> 192.168.1.100 TCP www > 59002 [SYN, ACK] Seq=0
Ack=1 Win=8190 Len=0 MSS=1460

0.844736 192.168.1.100 -> 72.14.207.99 TCP 59002 > www [RST] Seq=1
Len=0
```

TCP SYN Scan
80
open port

Example from midnightresearch.com

OS FINGERPRINTING

- Used to determine the type of OS installed on a target system
- Takes advantage of the fact that different OS implement the TCP/IP stack differently

  Examples:

	Default TTL	Initial Window
Windows	128	65535
Linux	64	5720
Cisco IOS	254	4128

OS FINGERPRINTING

- Methods:
  - Active: sends packets to target and guess OS based on response characteristics
  - Passive: sniffs packets from the network to check for differences and provides clues to OS

- Using Nmap: **nmap –O <target>**

BANNER GRABBING

- Examining banners can sometimes give clues about the software servicing a particular port

VULNERABILITY SCANNING

- Identifies weaknesses and vulnerabilities in order to determine how it can be exploited

- Tools
  - Nessus
  - OpenVAS

COUNTERMEASURES

- Ping Sweeps
  - Filter inbound ICMP messages and outbound ICMP unreachable messages at routers / firewalls
- Port Scanning:
  - Configure firewalls and IDS to block probes to ports that should not be publicly accessible
- Banner grabbing
  - Use fake banners
  - Disable or change banner information