# Scanning

INTRODUCTION

DURATION : 0’30

# Network scanning

- **Network Scanning** means discovering systems on the network (can be hosts, switches, servers, routers, firewalls and so on) and looking at what ports are open as well as applications/services and their respective versions that may be running.
- In general network scanning have three main objectives:

1. Scanning for live devices, OS, IPs in use.
   - Server at 192.168.60.30
2. Looking for Ports open/closed.
   - The server 192.168.60.30 have TCP port 23 (Telnet) running
3. Search for vulnerabilities on services scanned.
   - The Telnet service is cleartext and have many vulnerabilities published

- Connectionless Communication - UDP packets are sent without creating a connection. Examples are TFTP, DNS (lookups only) and DHCP.
- Connection-Oriented Communication - TCP packets require a connection due to the size of the data being transmitted and to ensure deliverability.

# Scanning Methodology

- **Check for live systems :** Ping or other type of way to determine live hosts
- **Check for open ports :** Once you know live host IPs, scan them for listening ports
- **Scan beyond IDS :** If needed, use methods to scan beyond the detection systems; evade IDS using proxies, spoofing, fragmented packets and so on
- **Perform banner grabbing :** Grab from servers as well as perform OS fingerprinting (versions of the running services)
- **Scan for vulnerabilities :** Use tools to look at the vulnerabilities of open systems
- **Draw network diagrams :** Shows logical and physical pathways into networks
- **Use proxies :** Obscures efforts to keep you hidden
- **Pentest Report :** Document everything that you find

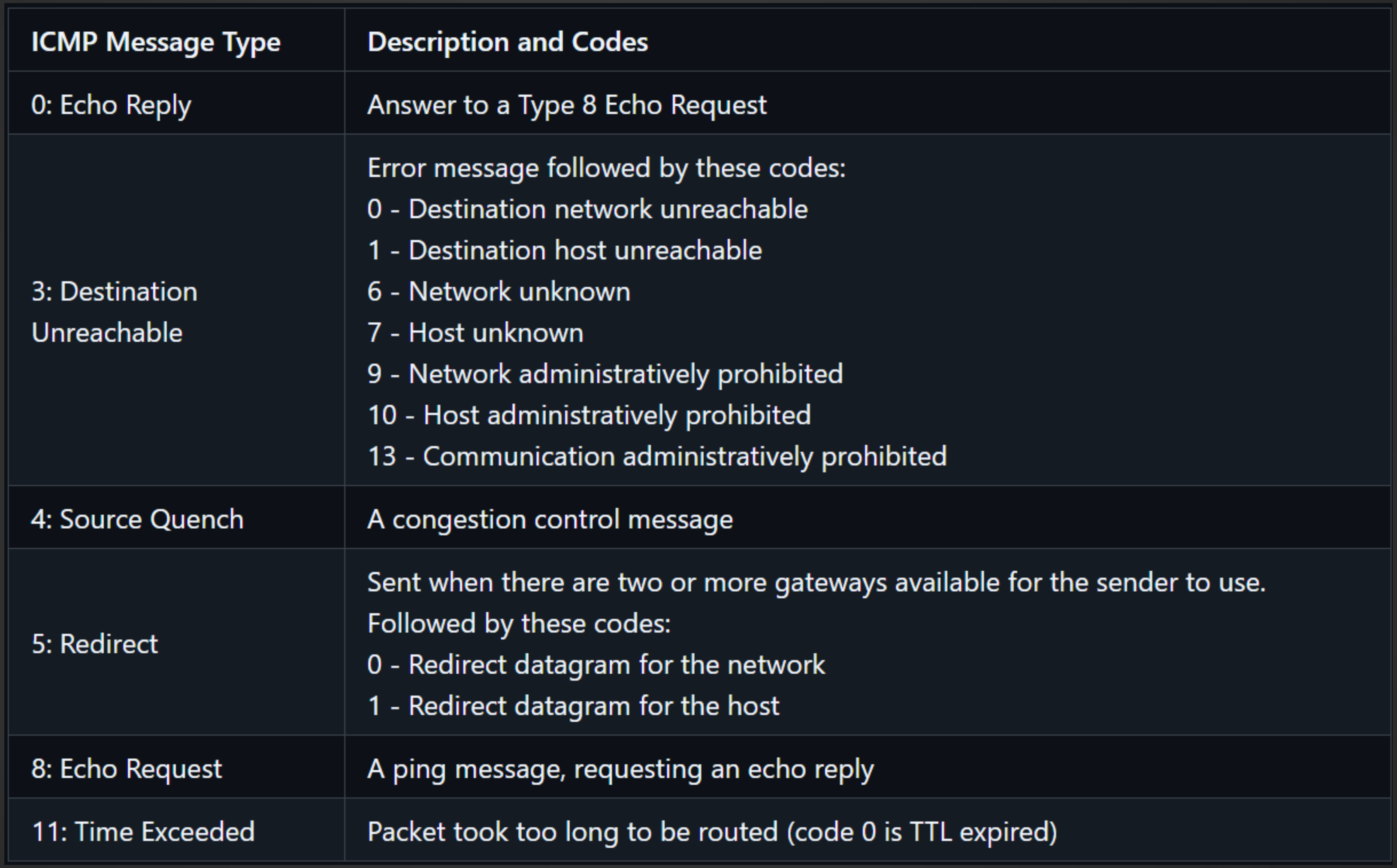
# Identifying Targets

- The easiest way to scan for live systems is through ICMP.
- **Payload of an ICMP message can be anything** : RFC never set what it was supposed to be.
- **Ping sweep :** easiest method to identify multiple hosts on subnet. You can automate ping sweep with scripting language like Bash Script (Linux) or PowerShell (Windows) or use softwares like Advanced IP Scanner, Angry IP Scanner, Nmap, etc.
- **ICMP Echo scanning :** sending an ICMP Echo Request to the network IP address.
- An ICMP return of type 3 with a code of 13 indicates a poorly configured firewall.

# Identifying Targets with ping tools

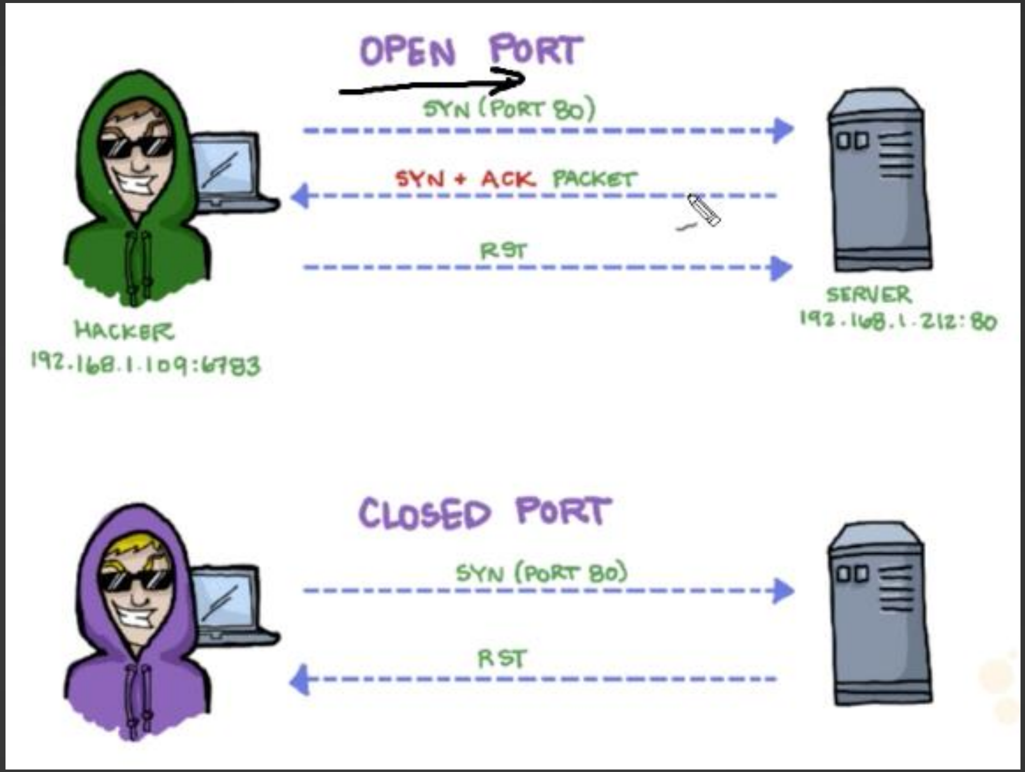
- Nmap (virtually always does a ping sweep with scans unless you turn it off)
  - nmap -sn 192.168.1.0/24
  - This command uses -sn flag (ping scan). This will perform a ping sweep on 256 IP addresses on this subnet in seconds, showing which hosts are up.
- hping3
  - hping -1 10.0.0.x --rand-dest -I eth0
    - -1 --> ICMP mode
    - --rand-dest --> random destionation address mode
    - -I <interface> --> network interface name
- Angry IP Scanner
- Solar-Winds Engineer Toolkit
- Advanced IP Scanner
- Pinkie

# Important ICMP codes



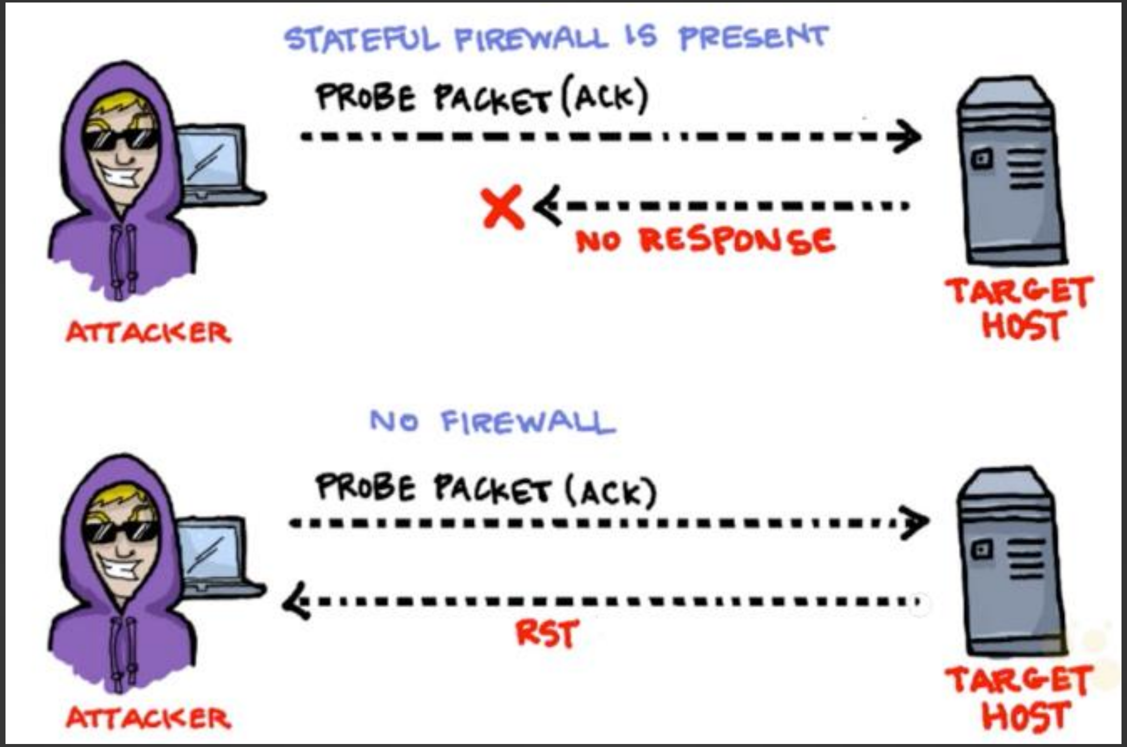
| ICMP Message Type | Description and Codes |
|---|---|
| 0: Echo Reply | Answer to a Type 8 Echo Request |
| 3: Destination Unreachable | Error message followed by these codes:<br>0 - Destination network unreachable<br>1 - Destination host unreachable<br>6 - Network unknown<br>7 - Host unknown<br>9 - Network administratively prohibited<br>10 - Host administratively prohibited<br>13 - Communication administratively prohibited |
| 4: Source Quench | A congestion control message |
| 5: Redirect | Sent when there are two or more gateways available for the sender to use. Followed by these codes:<br>0 - Redirect datagram for the network<br>1 - Redirect datagram for the host |
| 8: Echo Request | A ping message, requesting an echo reply |
| 11: Time Exceeded | Packet took too long to be routed (code 0 is TTL expired) |

# Port Discovery - Basic Concepts (1/2)



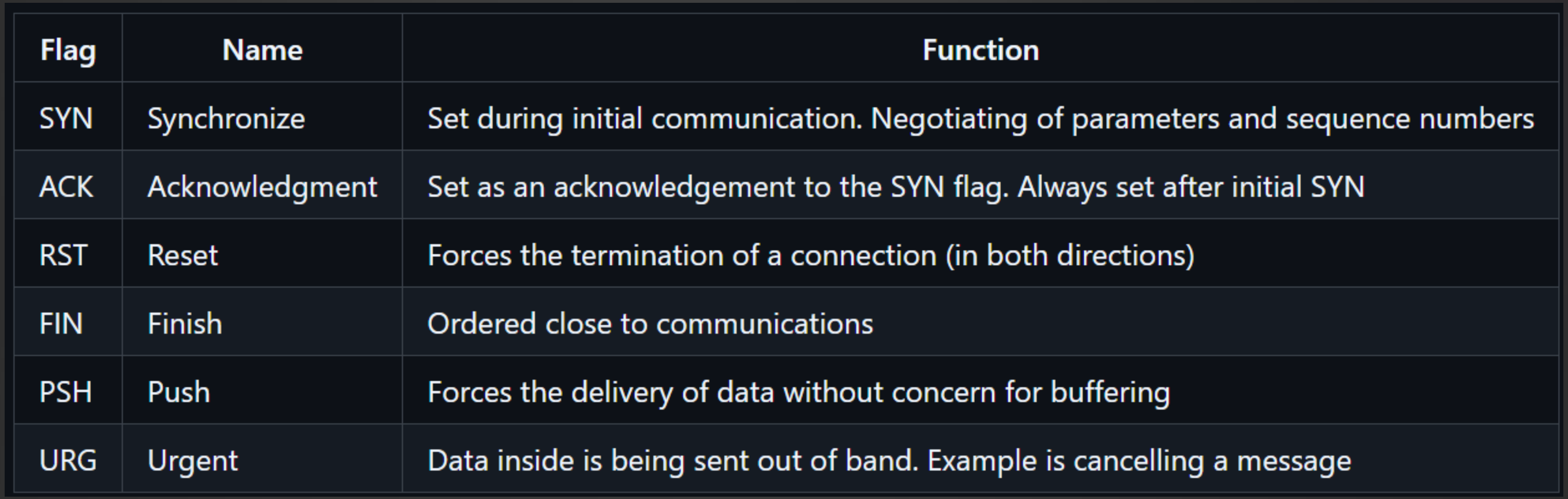
- The hacker above sends a SYN packet to port 80 on the server.
  - If server returns SYN-ACK packet = the port is open
  - If server returns RST (reset) packet = the port is closed

# Port Discovery - Basic Concepts (2/2)



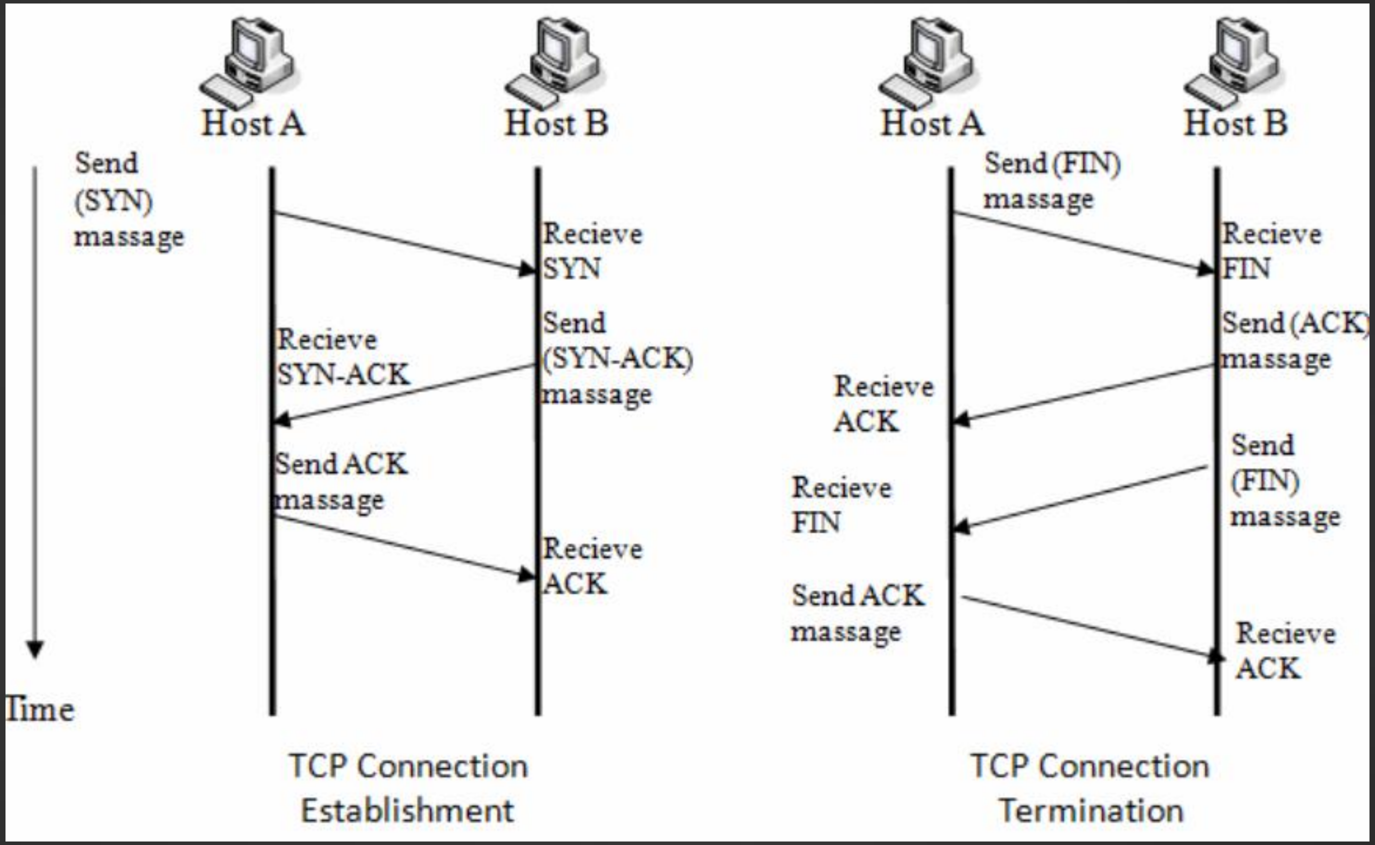
- The hacker above sends an ACK segment/packet on the first interaction (without three-way handshake).
  - If server returns no response means that might have a stateful firewall handling proper sessions
  - If server returns RST packet means that have no stateful firewall

# Reminder : TCP Flags



| Flag | Name | Function |
|---|---|---|
| SYN | Synchronize | Set during initial communication. Negotiating of parameters and sequence numbers |
| ACK | Acknowledgment | Set as an acknowledgement to the SYN flag. Always set after initial SYN |
| RST | Reset | Forces the termination of a connection (in both directions) |
| FIN | Finish | Ordered close to communications |
| PSH | Push | Forces the delivery of data without concern for buffering |
| URG | Urgent | Data inside is being sent out of band. Example is cancelling a message |

# Reminder : TCP Three-way handshake



# Banner Grabbing

- Banner grabbing can be used to get information about OS or specific server info (such as web server, mail server, etc.).
  - **Active :** sending specially crafted packets and comparing responses to determine OS
  - **Passive :** reading error messages, sniffing traffic or looking at page extensions
  - Easy way to banner grab is connect via **telnet** on port (e.g. 80 for web server)
  - Netcat is another tool
    - Provides all sorts of control over a remote shell on a target
    - Connects via **nc -e <IP address> <Port>**
    - From attack machine **nc -l -p 5555** opens a listening port on 5555
    - Can connect over TCP or UDP, from any port
    - Offers DNS forwarding, port mapping and forwarding and proxying
    - Netcat can be used to banner grab:
      - **nc <IP address or FQDN> <port number>**

# Windows System Basics

- Everything runs within context of an account
- Security Context - user identity and authentication information
- Security Identifier (SID) - identifies a user, group or computer account
- The end of the SID indicates the user number
  - Example SID (500 is Administrator account) : S-1-5-21-3874928736-367528774-1298337465-500
  - Command to get SID of local user : wmic useraccount where name='username' get sid
- Regular Accounts - start with a SID of 1000
- SAM Database : file where all local passwords are stored and encrypted (**C:\Windows\System32\Config**)
- **Windows SysInternals** is a website and suite that offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor.
  - https://docs.microsoft.com/en-us/sysinternals/downloads/
  - Lots of resources for enumerating, windows administration tools, etc.

# NetBIOS Enumeration

- NetBIOS provides mainly name servicing and connectionless communication.
- You can use nmap or zenmap to check which OS the target is using, and which ports are open : **nmap -O <target>**
- If theres any UDP port 137 or TCP port 138/139 open, we can assume that the target is running some type of NetBIOS service.
- On Windows you can also used **nbtstat** command.

# Linux System Basics

- Linux Systems used user IDs (UID) and group IDs (GID). Found in /etc/passwd
- Enum4linux is a tool for enumerating information from Windows and Samba systems:
  - `enum4linux -u admin -p Pa$$w0rd -U 10.0.2.23`
  - -u Username, -p Password, -U users information