# Scanning Phase

## 1. 🚂Checking for live System:

- Ping -
  - It involves sending an ICMP ECHO request to the host.
  - [Packet InterNet Groper].
  - Useful for locating active devices or determining if ICMP passes through a firewall.


- Ping Sweep -
  - Used to determine live host from a range of IPs.
  - Attackers calculate subnet masks using Subnet Mask Calculators to identify the number of hosts.
  - Attackers then use ping sweep to create an inventory of live systems in the subnet.

```
ping -c3 192.168.1.1
```

🛠️ Tools:

- Angry IP Scanner

---

ℹ️ **Note**

TCP Communication Flag

- **URG** (Urgent): Data contained in the packet should be processed immediately. Out of order
- **FIN** (Finish): There will be no more transmissions
- **RST** (Reset): Resets a connection
- **PSH** (Push): Send all buffered data immediately. In order
- **ACK** (Acknowledgment): Acknowledges the receipt of a packet
- **SYN** (Synchronize): Initiates a connection between hosts

---

## 2. ⛳Port Scanning:

Gathering attack surfaces for the victim against whom you want to launch an attack or gathering loopholes in your system.

▼ States of Ports

- **Open:** Actively accepting TCP connections, UDP datagram, or SCTP associations
- **Filtered:** Packet filtering is enabled (firewall, router rules, etc.) and cannot determine open or closed.
- **Closed:** Accessible (it receives and responds to probe packets), but there is no application listening on it

## ***Scanning TCP Network Services:***

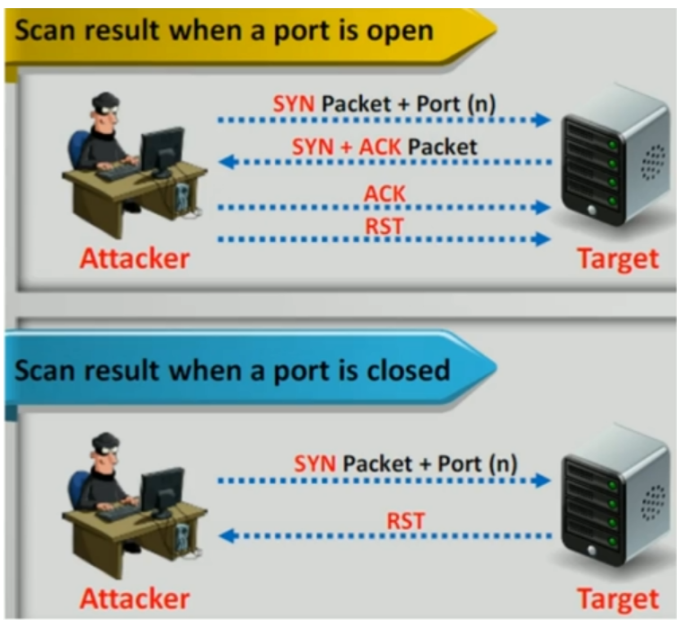
- Open TCP Scanning Methods
  - TCP Connect  / Full Open Scan
- Stealth TCP Scanning Methods
  - Half-open Scan
  - Inverse TCP Flag Scanning
    - XMAS Scan
    - FIN Scan
    - NULL Scan
  - ACK Flag Probe Scanning
- Third-Party and Spoofed TCP Scanning Methods
  - IDLE / IP ID Header Scanning

🛠️ Tools:

- Nmap
- hping2 / hping3

1. **TCP Connect / Full Open Scan (-sT)**

- TCP Connect scan detects when a port is open by 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 a superuser.

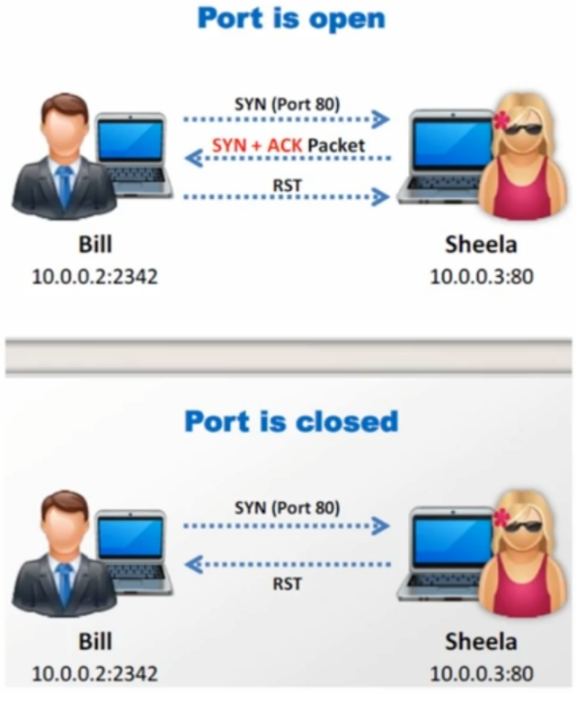



2. **Stealth Scan (Half-open Scan) (-sS)**

- Resetting the TCP connection between client and server abruptly before completion of three-way handshake signals making the connection half open.
- Stealth Scan Process:
  - The client sends a single SYN packet to the server on the appropriate port.
  - If the port is open then the server responds with a SYN+ACK packet.
  - If the server responds with **RST**, then the port is closed

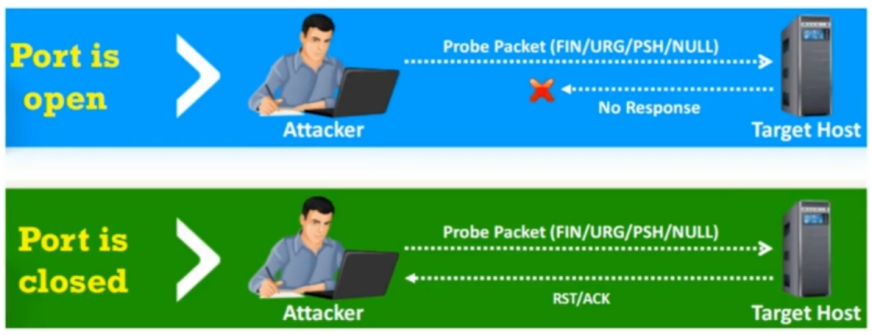
- If the client sends the **RST** before a connection ever be established, it is open.

**[ ROOT privileges required. ]**



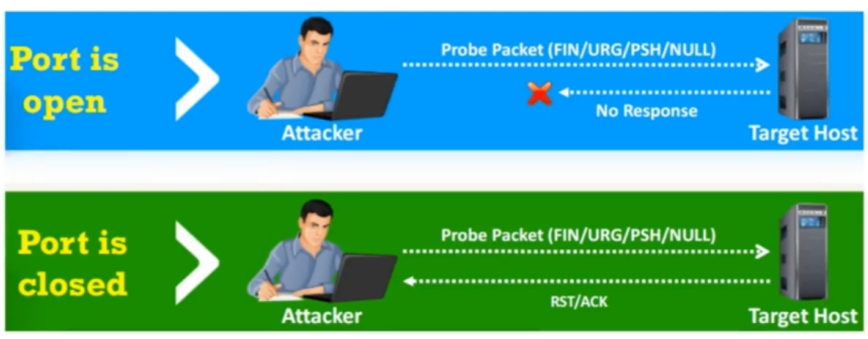

3. **Inverse TCP Flag Scanning (-sF, -sN)**

- TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, no response means the port is open and RST means the port is closed.
- It may give false positive responses.
- Linux can provide this type of scan.




4. **Xmas Scan (-sX)**

- In an Xmas scan, attackers send a TCP frame to a remote device with FIN, URG, and PUSH flags set.




5. **ACK Flag Probe Scanning (-sA)**

- The attacker sends TCP probe packets with the ACK flag set to a remote device and then analyzes the header information (TTL and WINDOW field) of received RST packets to find **whether the port is open or closed**.
- If the **TTL** value of the RST packet is less than the boundary value of 64, we consider it as open.
- If the WINDOW value of the RST packet on a particular port has a non-zero value, then that port is open.
- ACK probe packet with random sequence number, no response mean port filtered.
- ICMP unreachable error also gives us a filtered port.

**[ Here our main objective is to analyze the rule of firewall ]**

6. **UDP Scanning (-sU)**

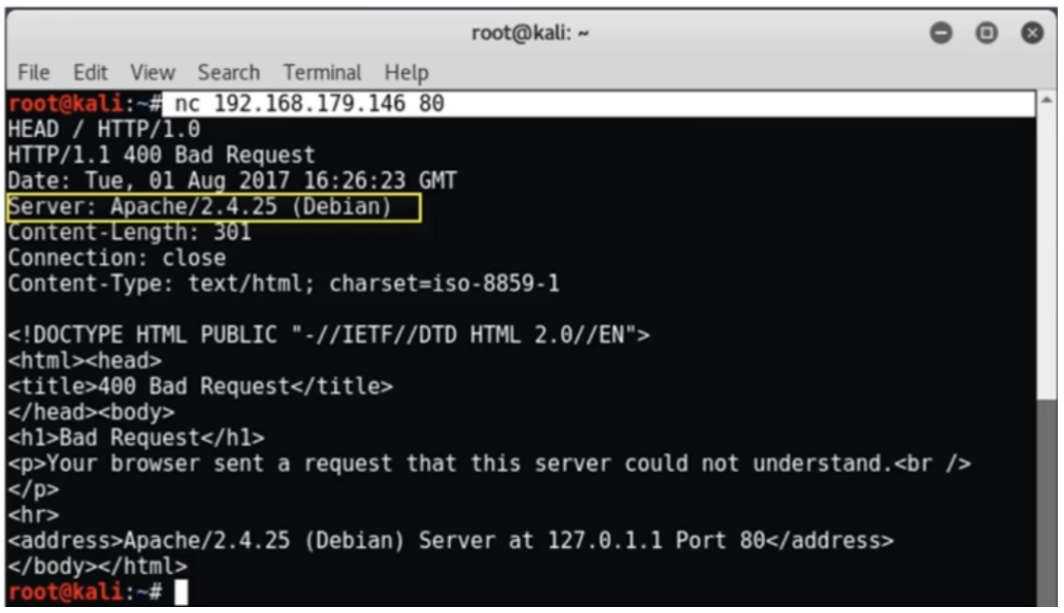
- UDP open
  - There is no three-way handshake
  - No response in return from the server.
  - Majorly gives you false positive
- UDP closed
  - If a UDP packet is sent to a closed port, the system responds with ICMP port unreachable message (type 3, code 3).
  - Spyware, Trojan horses, and other malicious application use UDP ports.


> 🛠️ Tools:
>
> - Colasoft  [Creating custom packet]

---

## 3. 📬Banner Grabbing:

- Also called OS fingerprinting.  Banners are used to tell the server what we like and recommend products according to that. Two types:
  - Active
  - Passive
- Identifying the OS used on the target host allows an attacker to figure out the vuln the system possess and the exploits that might work on a system to further carry out additional attacks.




3.1. **Active Banner Grabbing**

- 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.
- Response from different OS varied due to differences in TCP/IP stack implementation.

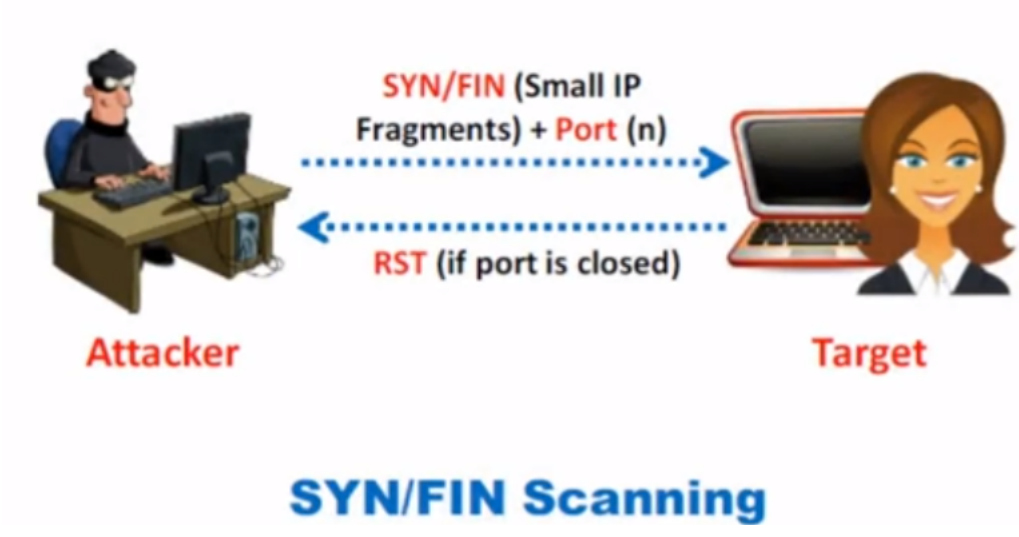
3.2. **Passive Banner Grabbing**

- Banner grabbing from error messages: They provide info such as the type of server, os, and SSL tool used by the target remote system.[404]
- Sniffing the network traffic: Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system.
- Page extension: looking for an extension in the URL may assist in determining the application version.[ .aspx > IIS Server and Windows platform. ]

> 🛠️ Tools:
>
> 1. IDserve
> 2. Netcraft
> 3. netcat

### Evading IDS, Firewalls

- Use of fragmented IP packets.
- Spoof IP when launching attack and sniff responses from the server.
- Use source routing
- Connect to a proxy server or compromised trojan machine to launch an attack.




---

## 4. 🎯Vulnerability Scanning

Identifying vulnerabilities and weaknesses of a system and network in order to determine how a system can be exploited.

- Network Vuln
- Open ports and running services
- Application and services vuln
- Application and services configuration errors

> 🛠️ Tools:
>
> - Nessus
> - NMAP
> - Nikto
> - OpenVas [gvm]
> - Wpscan

> ℹ️ **Note**
>
> CVE : Common Vulnerabilities and Exposure

### NMAP

- Nmap Scripting Engine (/usr/share/nmap/scripts)

```
nmap -sC -p- target
```

- [Manual]

```
nmap --scripts=ssh-brute.nse target
```

### Nikto

- Web Vulnerability Scanner [ **OSVDB header** ]

```
nikto -h domain -o vuln_scan -F txt -p 80
```

---

## 6. 🗺️Mapping the Network

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

> 🛠️ Tools:
>
> - LANSurveyor
> - Network Topology Mapper
> - OpManager
> - NetworkView

---

## 7. Countermeasures

- Install firewall and IDS to your network.
- Configure firewall and IDS rules to detect and block probes.
- Run the port scanning tools against hosts on the network to determine whether the firewall properly detects the port scanning activity.
- Ensure that the mechanism used for routing and filtering at the router and firewall respectively cannot be bypassed using particular source ports or source-routing methods.
  - For example: Do not allow frame size of more than 64-bit. But with fragmentation, it can be bypassed. To avoid that manually add value to the header.
- Ensure that the anti-scanning and anti-spoofing rules are configured.

### 7.1. **Port Scanning Countermeasures**:

- Ensure updation in the router, IDS, and firewall firmware.

- Use a custom ruleset to lock the network and block unwanted ports at the firewall.
- Filter all ICMP messages [ Ensure not allow UDP scanning ]
- Perform TCP and UDP scanning with ICMP probes to check the network configuration and its availability.

**7.2. Banner Grabbing Countermeasures**:

Disable or Changing of Banners

- Display false banner to misguide attacker.
- Turn off unnecessary services on the network host to limit information disclosure. [ Try disabling verbose output ]
- Use ServerMask tools to disable or change banner information.
- Use a directive in httpd.conf file to change banner information.
- Alternatively, change the ServerSignature line to ServerSignature off in the httpd.conf file.

Hide File Extension from Web Pages

- File extension reveals information about the underlying technology
- Hide file extension to mask the web technology.
- Change application mappings such as .asp with .thm or .foo, etc. to disguise the identity of servers.
- Apache users can use mod negotiation directives
- IIS users use tools such as PageXchanger[tool] to manage file extensions.
- It is even better if the file extension is not at all used.