

## NETWORK SCANNING

The purpose of each scanning process is given below:

**Port Scanning** - detecting open ports and services running on the target.

**Network Scanning** - IP addresses, Operating system details, Topology details, trusted routers information etc

**Vulnerability scanning** - scanning for known vulnerabilities or weakness in a system

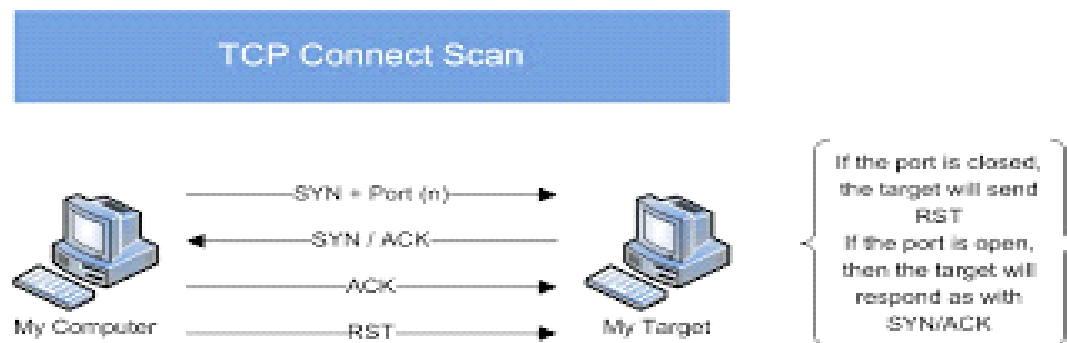
### SCANNING METHODOLOGIES



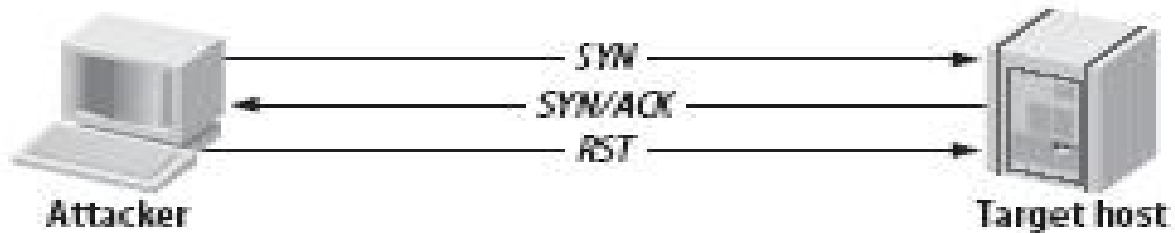
- **Check for Live Systems:** Ping scan checks for the live system by sending **ICMP echo request packets**. If a system is alive, the system responds with **ICMP echo reply packet containing details of TTL, packet size** etc.
- **Check for Open Ports:** Port scanning helps us to find out open ports, services running on them, their versions etc. Nmap is the powerful tool used mainly for this purpose.


**We have various types of scan:**

**Connect scan:** Identifies open ports by establishing a TCP handshake with the target.



**Half-open scan** otherwise known as **Stealth scan** used to scan the target in a stealthy way by **not completing the TCP handshake by abruptly resetting the communication.**



**XMAS scan:** This is also called as *inverse TCP scanning*. This works by sending packets set with PSH, URG, FIN flags. The targets do not respond if the ports are open and send a reset response if ports are closed. 



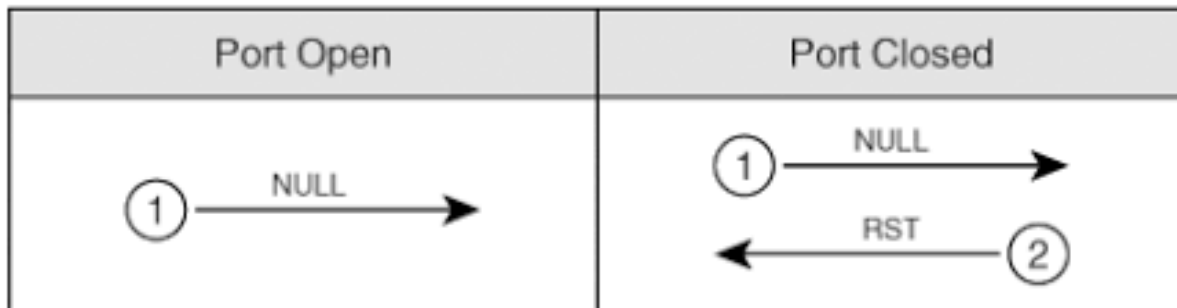
**FIN scan:** Fin flag is set in the TCP packets sent to the target. open ports do not respond while closed ports send a reset response.



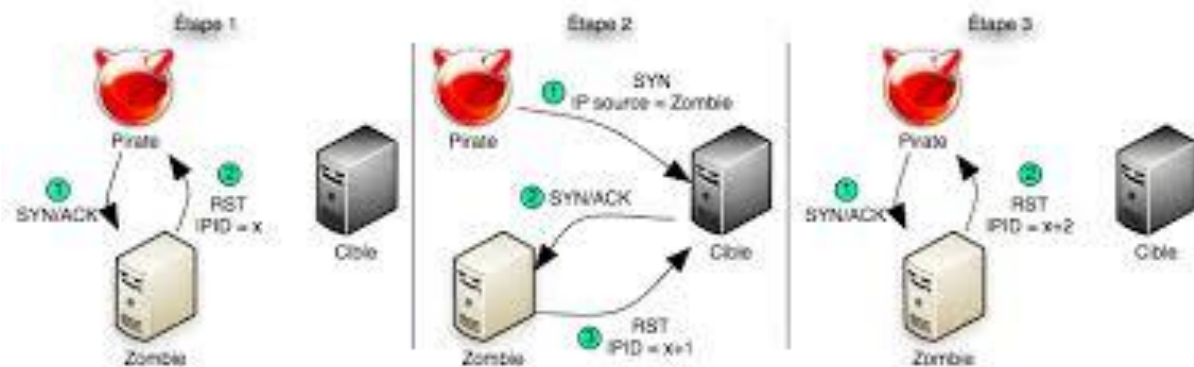
**ACK scan:** Here the attacker sets the ACK flag in the TCP header and the target's port status is gathered based on window size and TTL value of RESET packets received from the target.



**Null Scan:** Works by sending TCP packets with no flags set to the target. Open ports do not respond while closed ports respond with a RESET packet.



**Idle Scan:** Here the **attacker tries to mask his identity uses an idle machine** on the network to probe the status details of target ports.



## Banner Grabbing

Banner grabbing is a process of **collecting information like operating system details, the name of the service running with its version number** etc.

## Vulnerability scanning:

Mainly automated tools are used for this purpose. These automated scanners **scan the target to find out vulnerabilities or weakness in the target organization** which can be exploited by the attackers. Vulnerabilities **include application vulnerabilities, configuration vulnerabilities, network vulnerabilities, operating system vulnerabilities** etc.

Some examples include operating system is **not updated, default passwords used, plain text protocols used, vulnerable protocols** running etc.

**Tools: Nessus, Acunetix**

## **Draw Network Diagrams**

With the information gathered, **the attacker can come up with a network diagram which might give him information about network** and architecture of the target organization helping him to identify the target easily

**Tools: Network View, Opmanager etc**

## **Prepare Proxies**

Proxies can use **to maintain the anonymity of the attacker by masking the IP address.** It can capture information passing through it since it acts as an intermediary between client and server and the attacker can access the resources remotely using the proxies.

**Eg: TOR browsers, Onion sites etc, Proxify, Psiphon etc**

## **Countermeasures:**

- Configure IDS and firewall to block probes.
- Keep firewall, routers, IDS firmware update
- Run port scanners to verify the security of the target.
- Add rules in firewall restricting access to ports.
- Disable ICMP based scanning at firewall.