Cryptography, Network & Software Security

Jaspreet Singh

Project Engineer
E-Security
CDAC, Hyderabad

Hyderabad Centre

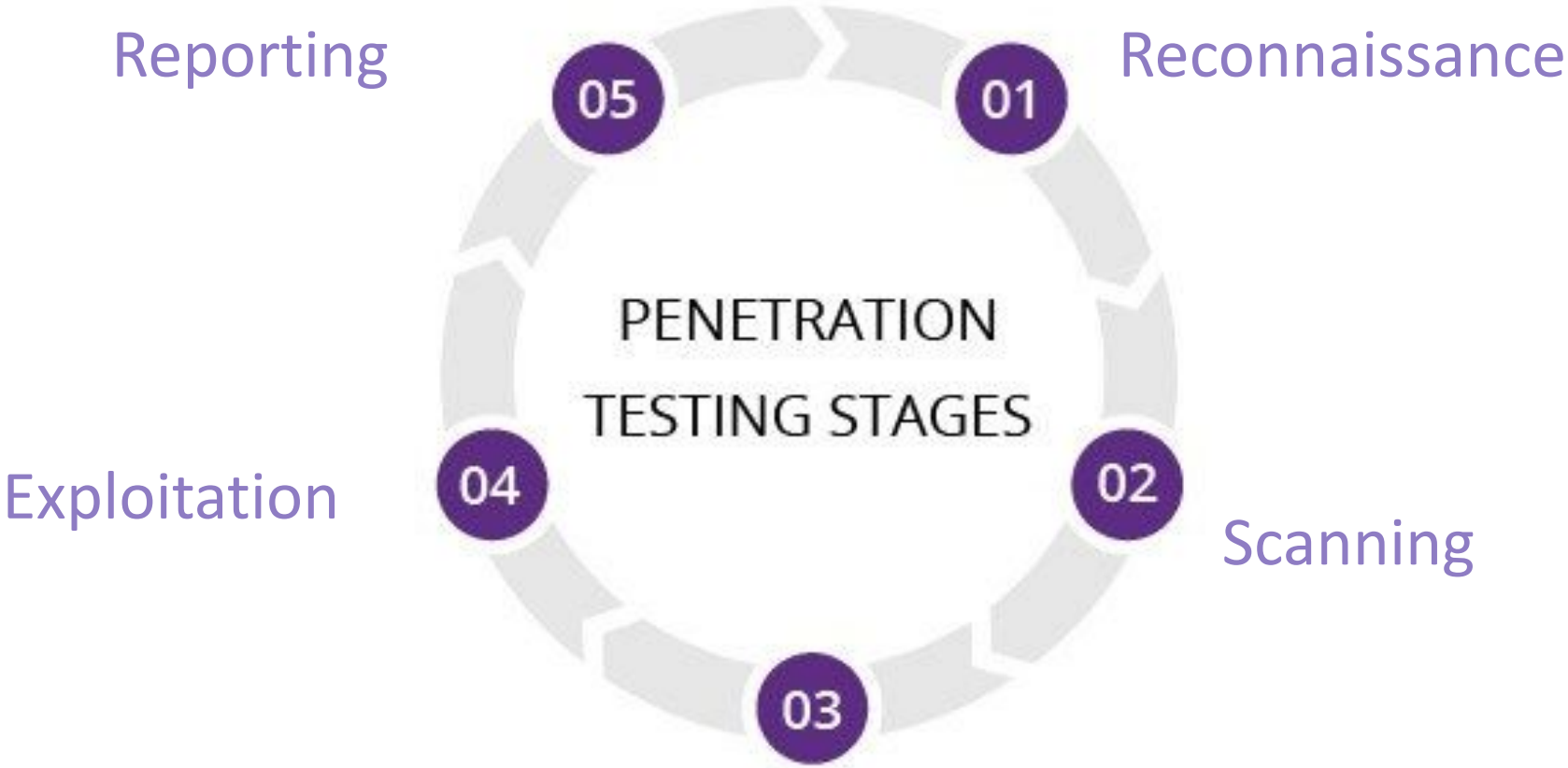
Overview

- Penetration Testing
- Nmap
- Nmap-Scans
- Nmap LAB

Penetration Testing

- **Definition:** Penetration Testing is a simulated cyber attack against your computer system to check for exploitable vulnerabilities.
    - **Importance:** Identifies security weaknesses, helps in enhancing security measures, and ensures compliance with regulations.

Penetration Testing



Penetration Testing

Reconnaissance

- **Objective:** Gather as much information about the target system as possible.
- **Methods:**
  - **Passive Reconnaissance:** Gathering information from publicly available resources without directly interacting with the target.
  - **Active Reconnaissance:** Interacting directly with the target to gather information, such as scanning networks and systems.

Scanning

- **Objective:** Identify open ports, services running on those ports, and potential entry points.
- **Tools:** Utilize tools to scan for open ports and services (e.g., Nmap).
- **Importance:** Provides a foundational understanding of the target's network topology and potential vulnerabilities.

Penetration Testing

Vulnerability Assessment

- **Objective:** Analyze gathered data to identify and assess vulnerabilities.
- **Resources:** Use databases like the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) to rate vulnerabilities based on severity (using CVSS).
- **Integration:** Combines information from reconnaissance and scanning to pinpoint weaknesses that could be exploited.

Exploitation

- **Objective:** Attempt to exploit identified vulnerabilities to gain access to the target system.
- **Caution:** Requires careful execution to avoid compromising or damaging the system.
- **Tools:** Tools like Metasploit are often used to simulate real-world attacks and test the security defenses of the system.

Penetration Testing

Reporting

- **Objective:** Document findings and provide actionable recommendations.
- **Contents of Report:** Includes detailed descriptions of vulnerabilities (with CVSS scores), business impact assessment, technical risk briefing, and remediation advice.
- **Purpose:** Helps organizations understand their security posture and prioritize improvements

Popular Penetration Testing Tools

Nmap

- Network scanning tool
- Detects open ports and services
- Identifies vulnerable applications

Metasploit

- Vulnerability exploitation tool
- Contains a library of exploits for various OS and software
- Assists in exploiting known vulnerabilities

Wireshark

- Network analysis tool
- Captures and decodes packet data
- Useful for detecting malicious traffic and analyzing network behavior

Burp Suite

- Web application security testing tool
- Scans websites for vulnerabilities
- Manipulates requests and intercepts traffic between client and server

Nikto

- Web server vulnerability scanner
- Scans for outdated software, vulnerabilities, and misconfigurations
- Identifies potential security issues in web servers and applications

What is NMAP?

Step 4: Exploitation

- Exploit identified vulnerabilities to gain privileged access.
- Conduct simulated attacks carefully to avoid system damage.

Step 5: Post Exploitation

- Document sensitive data, configuration settings, communication channels, and network relationships.
- Set up methods for future access.

Step 6: Reporting

- Create a comprehensive report of findings.
- Document vulnerabilities and provide remediation suggestions to improve security.

Features of NMAP

- Versatile scanning options
- Scriptable with Nmap Scripting Engine (NSE)
- Rich output options
- Extensive documentation and community support

Installation and Setup

Windows:

- Download from the NMAP official site
- Run the installer

Linux:

- Use package managers: `sudo apt-get install nmap` (Debian-based),
- `sudo yum install nmap` (Red Hat-based)

MacOS:

- Use Homebrew: `brew install nmap`

Basic Commands and Usage

- **Basic Scan:** `nmap <target>`
- **Scan Specific Ports:** `nmap -p 22,80 <target>`
- **Service Version Detection:** `nmap -sV <target>`
- **Operating System Detection:** `nmap -O <target>`
- **Save Output to File:** `nmap -oN output.txt <target>`
- **Aggressive Scan:** `nmap -A <target>`

Stealth Scan (SYN Stealth)

Definition: A SYN scan is a type of port scan that sends TCP SYN packets to determine the status of ports.

Alias: Also known as "half-open" scanning because it doesn't complete the TCP handshake.

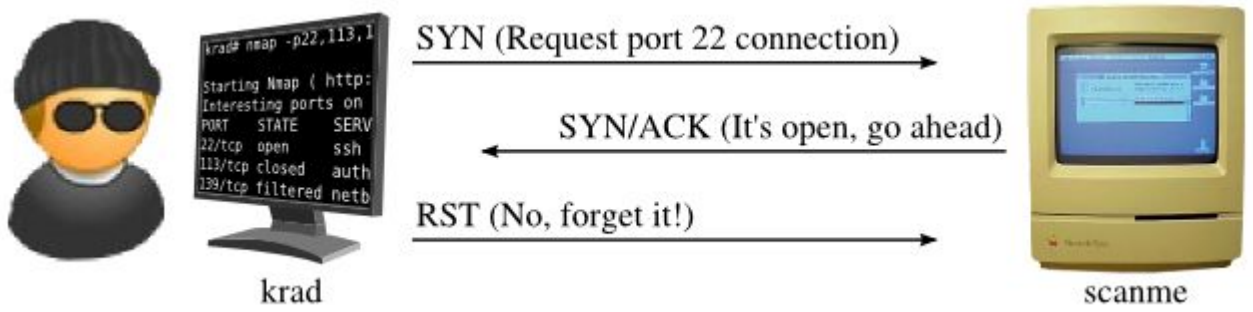
Benefits of SYN Scans

- **Stealthy:** Less likely to be logged by the target system.
- **Efficient:** Fast and effective in identifying open ports.
- **Widely Supported:** Works on most systems and networks.

Stealth Scan (SYN Stealth)

Process:

- NMAP sends a SYN packet to the target port.
- If the port is open, the target responds with a SYN-ACK packet.
- NMAP then sends an RST packet to reset the connection.
- If the port is closed, the target responds with an RST packet.
- If the port is filtered, there is no response or an ICMP unreachable error.



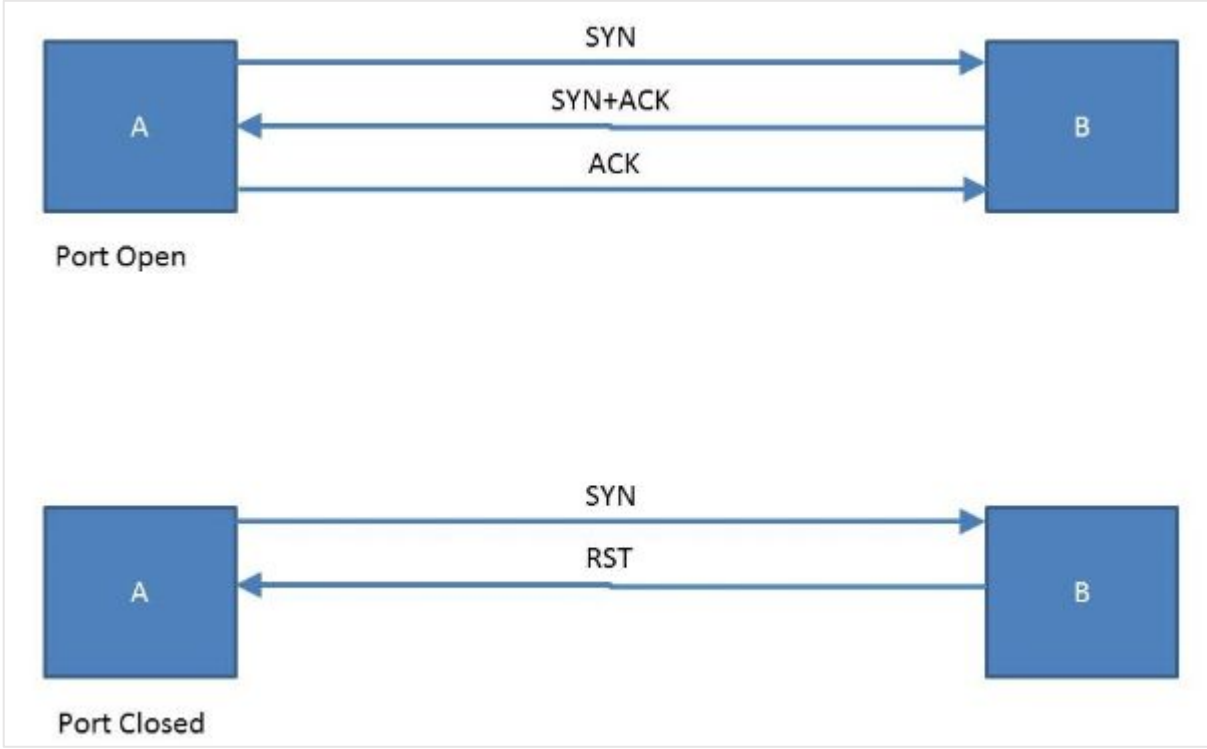
Example of a SYN Scan

```
┌──(vixen㉿Vixen)-[~/Downloads]
└─$ sudo nmap -sS 10.244.9.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 15:17 IST
Nmap scan report for 10.244.9.35
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
902/tcp  open  iss-realsecure
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.62 seconds
```

Full TCP Connect Scan

- **Purpose:** Completes the TCP three-way handshake for each port to determine open ports.
- **Command:** `nmap -sT <target>`
- **Example:** `nmap -sT 192.168.1.1`
- **Output Explanation:**
    - Provides a full connection to each port, more reliable but less stealthy.



Ping Sweep (ICMP Echo Scan)

Purpose: Determines live hosts by sending ICMP echo requests (ping).

Command: `nmap -sn <target>`

Example: `nmap -sn 192.168.1.0/24`

Output Explanation:

- Lists live hosts without performing port scans.

Decoy Scan

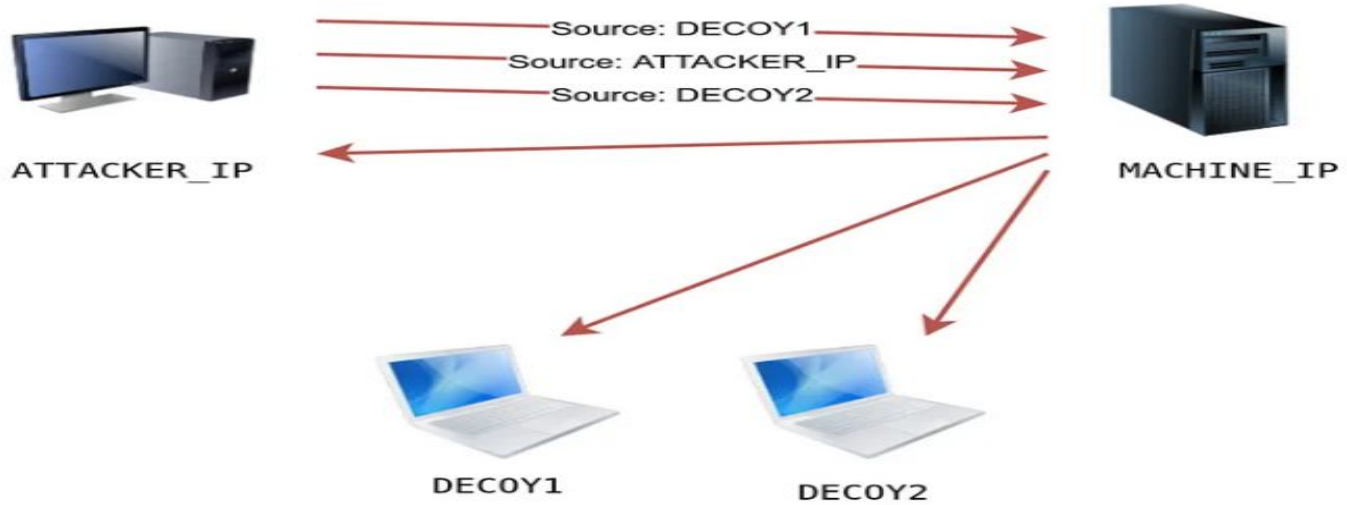
Purpose: Spoofs the source IP address to hide the identity of the real scanner.

Command: `nmap -sS -D <decoy1,decoy2,...,me> <target>`

Example: `nmap -sS -D 192.168.1.100,192.168.1.101,192.168.1.102,192.168.1.1`

Output Explanation:

- Sends packets from multiple decoy IPs to confuse target logging systems.



Null Scan

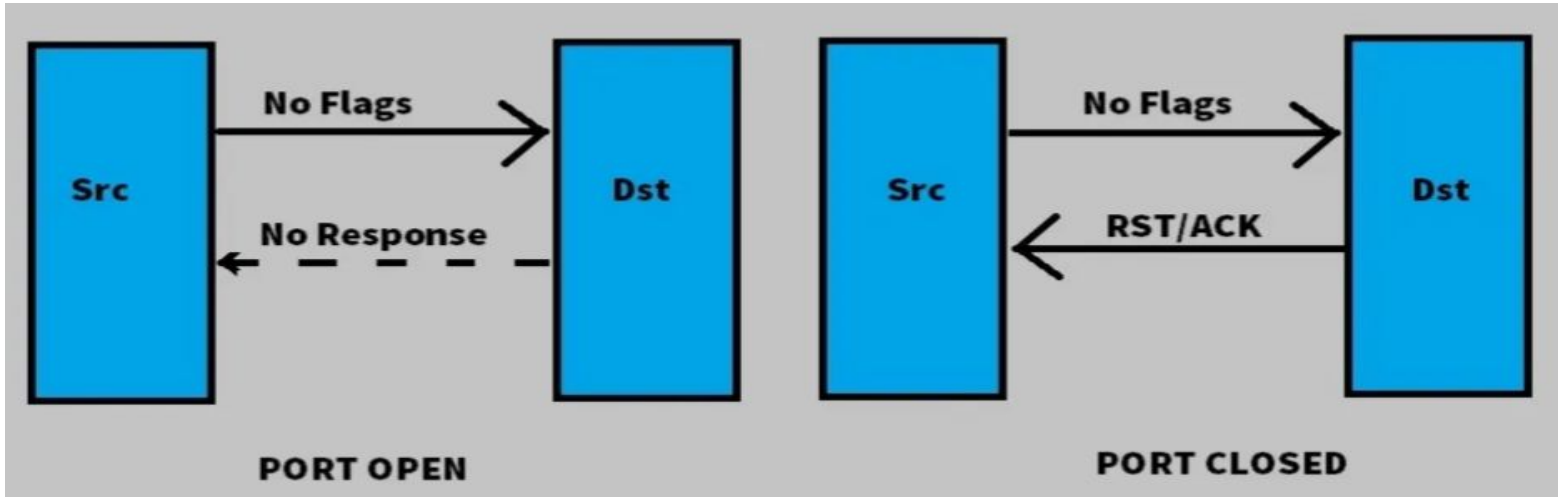
Purpose: Sends TCP packets with no flags set (Null packets).

Command: `nmap -sN <target>`

Example: `nmap -sN 192.168.1.1`

Output Explanation:

- Used to determine firewall filtering rules or stealthily map out a network.



TCP ACK Scan

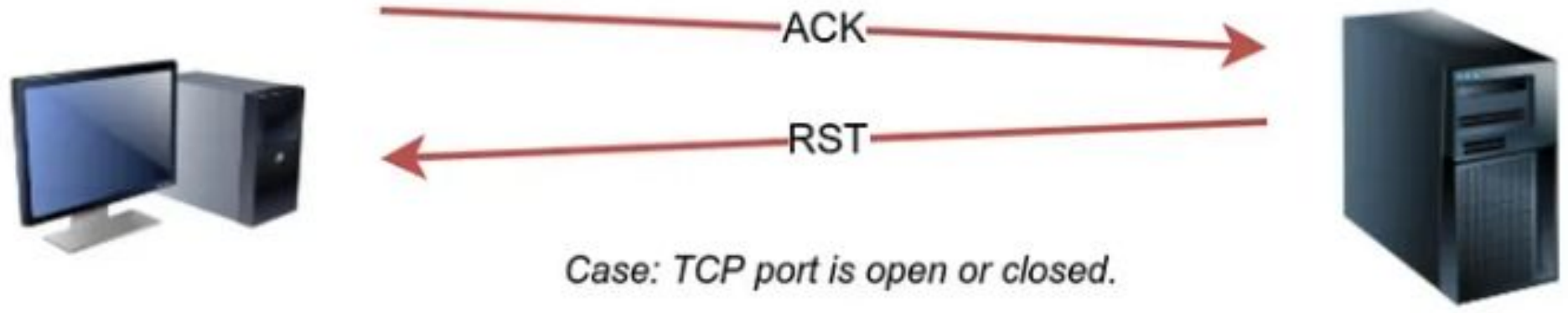
Purpose: Sends TCP ACK packets to determine firewall rulesets.

Command: `nmap -sA <target>`

Example: `nmap -sA 192.168.1.1`

Output Explanation:

- Checks how a firewall responds to different TCP flags without actually establishing a full connection.



FIN Scan

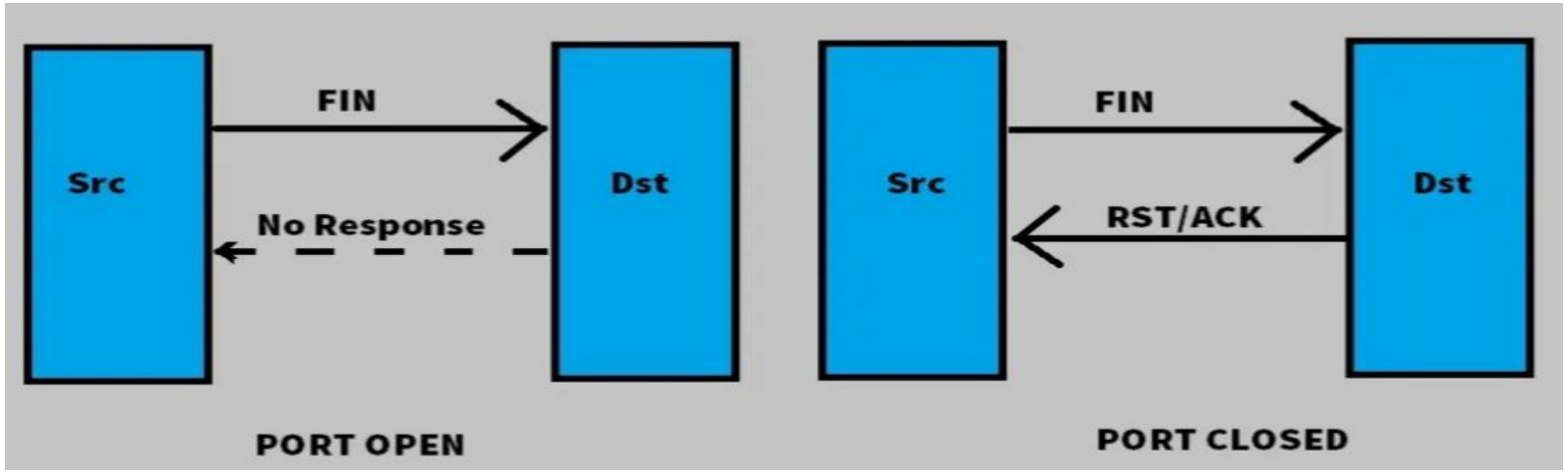
Purpose: Sends TCP packets with only the FIN flag set.

Command: `nmap -sF <target>`

Example: `nmap -sF 192.168.1.1`

Output Explanation:

- Used similarly to Null scan to probe firewall configurations.



Xmas Scan

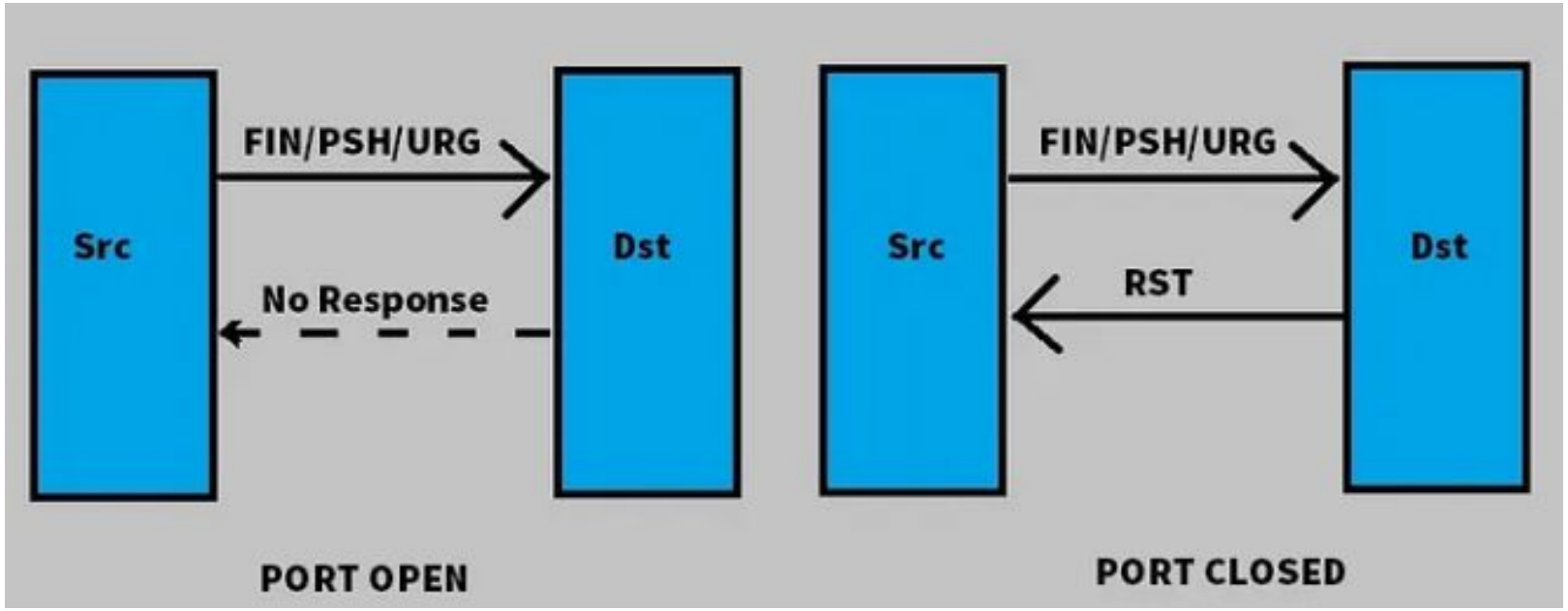
Purpose: Sends TCP packets with the FIN, URG, and PSH flags set.

Command: `nmap -sX <target>`

Example: `nmap -sX 192.168.1.1`

Output Explanation:

- Used to detect firewall filtering rules.



Examples:

- Scan a single host: `nmap 192.168.1.1`
- Scan a range of IPs: `nmap 192.168.1.1-20`
- Scan a subnet: `nmap 192.168.1.0/24`
- UDP Scan: `nmap -sU 192.168.1.1`
- Intense Scan Plus UDP: `nmap -sS -sU 192.168.1.1`
- OS Detection: `nmap -O 192.168.1.1`
- Aggressive Scan: `nmap -A 192.168.1.1`
- Stealth Scan: `nmap -sS -Pn 192.168.1.1`
- Ping Sweep: `nmap -sn 192.168.1.0/24`
- Xmas Scan: `nmap -sX 192.168.1.1`
- Full TCP Connect Scan: `nmap -sT 192.168.1.1`
- Decoy Scan: `nmap -sS -D 192.168.1.100,192.168.1.101,192.168.1.102,192.168.1.1`
- Null Scan: `nmap -sN 192.168.1.1`
- ACK Scan: `nmap -sA 192.168.1.1`
- FIN Scan: `nmap -sF 192.168.1.1`

Summary

- Recap of Key Points:
  - Symmetric and Asymmetric Key Cryptography
  - Diffie-Hellman Key Exchange & Man-in-the-Middle Attack
  - Setting up CA with OpenSSL
  - Stream Ciphers & Block Ciphers, RSA
  - Hash Functions, MAC, HMAC

Q&A

Reference

- EC-Council
  - https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/
- nmap
  - https://nmap.org/
- Security Metrics
  - https://www.securitymetrics.com/
- OKTA
  - https://www.okta.com/identity-101/hmac/

Thank you