Nmap

1. Nmap

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It helps administrators and security professionals identify devices on a network, discover open ports, and determine what services and versions are running. In this assignment, we explore three types of scans: Basic Scan, Service Detection, and Aggressive Scan using the IP address 192.168.42.162.

—> to install nmap in macOS just write

```
brew install nmap
```

2. Basic Scan

Command Used:

```
nmap 192.168.42.162
```

The basic scan checks which ports are open on the target system. It sends TCP packets to the specified IP and waits for responses, identifying open ports.

```
❯ nmap 192.168.42.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 22:13 IST
Nmap scan report for 192.168.42.162
Host is up (0.000046s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3306/tcp open  mysql
5000/tcp open  upnp
7000/tcp open  afs3-fileserver

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Purpose and Usage:

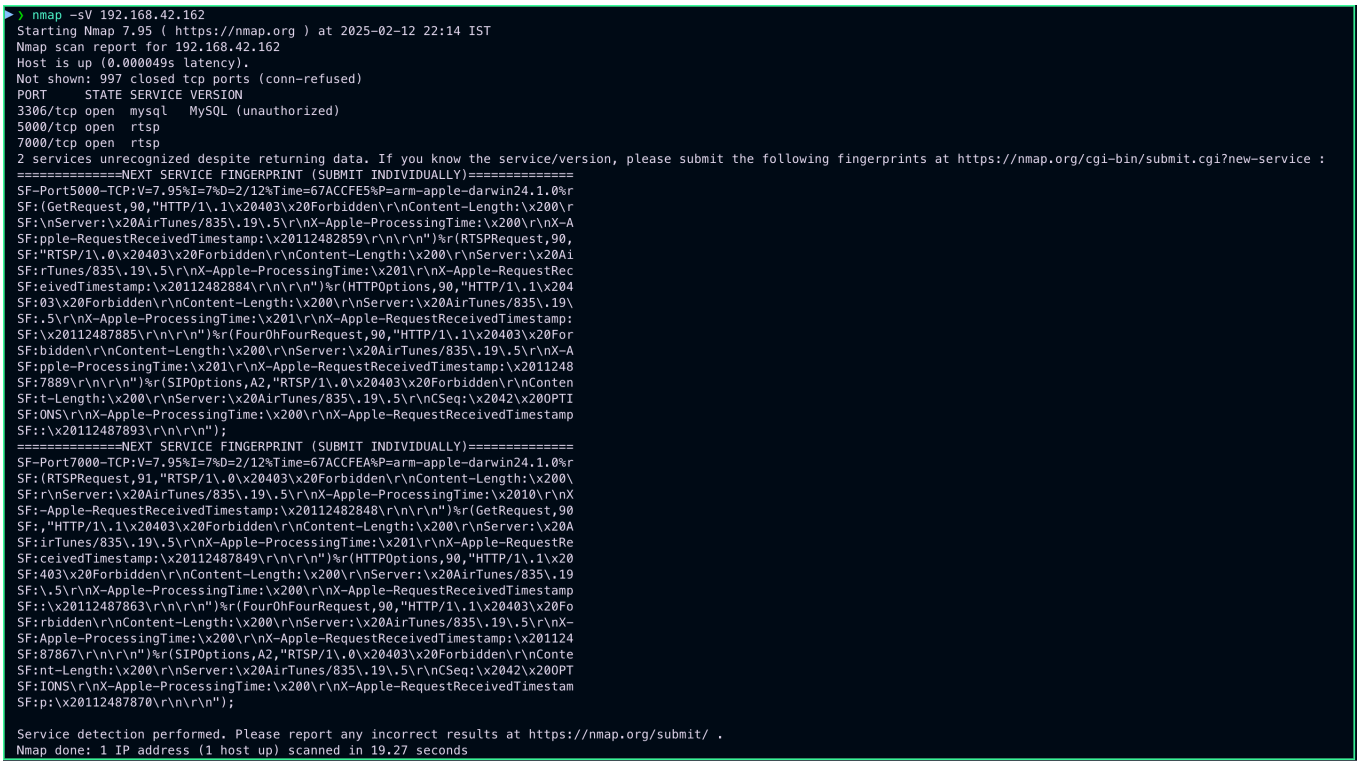
This scan is typically used for initial reconnaissance. It provides an overview of accessible services but does not reveal detailed information about them.

3. Service Detection Scan

Command Used:

```
nmap -sV 192.168.42.162
```

Service detection identifies the version of services running on open ports. This scan sends packets to open ports and analyzes the responses to determine the service name and version.



Purpose and Usage:

This scan is useful for vulnerability assessments, as identifying specific versions of services can help in locating potential security flaws or outdated software.

4. Aggressive Scan

Command Used:

```
nmap -A 192.168.42.162
```

The aggressive scan provides a detailed analysis of the target, including OS detection, version detection, script scanning, and traceroute. It gathers extensive information, making it ideal for comprehensive network audits.

```
❯ nmap -A 192.168.42.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 22:15 IST
Nmap scan report for 192.168.42.162
Host is up (0.000046s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
5000/tcp open  rtsp
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/835.19.5
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 112543376
|   GetRequest:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/835.19.5
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 112538342
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/835.19.5
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 112543369
|   RTSPRequest:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/835.19.5
|     X-Apple-ProcessingTime: 0
|     X-Apple-RequestReceivedTimestamp: 112538364
|   SIPOptions:
|     RTSP/1.0 403 Forbidden
|     Content-Length: 0
|     Server: AirTunes/835.19.5
|     CSeq: 42 OPTIONS
|     X-Apple-ProcessingTime: 0
|_    X-Apple-RequestReceivedTimestamp: 112543381
7000/tcp open  rtsp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 26.84 seconds
```

Purpose and Usage:

This scan is typically used when detailed insights about a target are required. However, it is more intrusive and can be easily detected by network security systems.