

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.

```
> nmap -sV 192.168.42.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 22:14 IST
Nmap scan report for 192.168.42.162
Host is up (0.000049s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp   open  mysql   MySQL (unauthorized)
5000/tcp   open  rtsp
7000/tcp   open  rtsp
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port5000-TCP:V=7.95%I=7%D=2/12%Time=67ACCFE5%P=arm-apple-darwin24.1.0%r
SF:(GetRequest,90,"HTTP/1.1\x20403\x20Forbidden\r\nContent-Length:\x200\r
SF:\nServer:\x20AirTunes/835\19\5\r\nX-Apple-ProcessingTime:\x200\r\nX-A
SF:pple-RequestReceivedTimestamp:\x20112482859\r\n\r\n")%r(RTSPRequest,90,
SF:"RTSP/1.0\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20Ai
SF:rTunes/835\19\5\r\nX-Apple-ProcessingTime:\x201\r\nX-Apple-RequestRec
SF:eivedTimestamp:\x20112482884\r\n\r\n")%r(HTTPOptions,90,"HTTP/1.1\x204
SF:03\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/835\19\
SF:5\r\nX-Apple-ProcessingTime:\x201\r\nX-Apple-RequestReceivedTimestamp:
SF:\x20112487885\r\n\r\n")%r(FourOhFourRequest,90,"HTTP/1.1\x20403\x20Fo
SF:rbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/835\19\5\r\nX-A
SF:pple-ProcessingTime:\x201\r\nX-Apple-RequestReceivedTimestamp:\x2011248
SF:7889\r\n\r\n")%r(SIPOptions,A2,"RTSP/1.0\x20403\x20Forbidden\r\nConten
SF:t-Length:\x200\r\nServer:\x20AirTunes/835\19\5\r\nCSeq:\x2042\x200PTI
SF:IONS\r\nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp
SF:p:\x20112487893\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port7000-TCP:V=7.95%I=7%D=2/12%Time=67ACCFEA%P=arm-apple-darwin24.1.0%r
SF:(RTSPRequest,91,"RTSP/1.0\x20403\x20Forbidden\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/835\19\5\r\nX-Apple-ProcessingTime:\x2010\r\nX
SF:Apple-RequestReceivedTimestamp:\x20112482848\r\n\r\n")%r(GetRequest,90
SF:,"HTTP/1.1\x20403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20A
SF:rTunes/835\19\5\r\nX-Apple-ProcessingTime:\x201\r\nX-Apple-RequestRe
SF:eivedTimestamp:\x20112487849\r\n\r\n")%r(HTTPOptions,90,"HTTP/1.1\x20
SF:403\x20Forbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/835\19
SF:5\r\nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp
SF::\x20112487863\r\n\r\n")%r(FourOhFourRequest,90,"HTTP/1.1\x20403\x20Fo
SF:rbidden\r\nContent-Length:\x200\r\nServer:\x20AirTunes/835\19\5\r\nX-
SF:Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestamp:\x201124
SF:87867\r\n\r\n")%r(SIPOptions,A2,"RTSP/1.0\x20403\x20Forbidden\r\nConte
SF:t-Length:\x200\r\nServer:\x20AirTunes/835\19\5\r\nCSeq:\x2042\x200PT
SF:IONS\r\nX-Apple-ProcessingTime:\x200\r\nX-Apple-RequestReceivedTimestam
SF:p:\x20112487870\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.27 seconds
```

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
3306/tcp  open  mysql
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.