Reconnaissance & scanning

Using tools like Nmap and Netdiscover to gather information about a target network.

Nmap (Network Mapper) - Report

Introduction

Nmap (short for **Network Mapper**) is a **free and open-source** network scanning tool used for **network discovery and security auditing**. Originally written by **Gordon Lyon** (also known by his pseudonym **Fyodor**), Nmap is a powerful utility that helps administrators map networks, discover hosts and services, and detect vulnerabilities.

Purpose of Nmap

Nmap is primarily used to:

- Discover hosts and devices on a network
- Identify open ports and services
- Detect operating systems and software versions
- Assess network security
- Detect misconfigured or vulnerable devices

Key Features

- ✅ **Host Discovery** – Detect live hosts on a network
- ✅ **Port Scanning** – Identify open TCP/UDP ports
- ✅ **Service Detection** – Determine what services (e.g., HTTP, FTP) are running and their versions

- ✅ **OS Detection** – Detect the target system's operating system and hardware details

- ✅ **Scriptable Interaction** – Use the **Nmap Scripting Engine (NSE)** to perform advanced tasks like vulnerability detection, malware scanning, etc.

- ✅ **Flexible Output** – Supports normal, XML, grepable, and JSON output formats for reporting and integration

How Nmap Works

Nmap sends specially crafted packets to target hosts and then analyzes the responses. Depending on the flags and scan types used, Nmap can perform a variety of scans

Follows Commands:

```
nmap <target IP>
nmap -sV <target IP> # Detects service versions
nmap -O <target IP> # Detects operating system
nmap -p 1-65535 <target IP> # Scans all ports
```

```
netdiscover -r 192.168.1.0/24
```