# 🛡️ Day 5 – Ethical Hacking

## 🔍 Topic: Active Reconnaissance & Nmap Scanning

Active reconnaissance involves direct interaction with the target system to gather information. Unlike passive reconnaissance, active recon is noisy and detectable—it can trigger alerts on intrusion detection systems (IDS) or firewalls.

Examples of Active Reconnaissance:

- Port Scanning  
- OS Detection  
- Service Enumeration  
- Vulnerability Scanning

Tools commonly used: Nmap, Netcat, Hping, and others.

## 📌 What are Ports?

A port is a virtual point where network connections start and end. Think of it as a doorway for communication between devices.

|  |  |  |
| --- | --- | --- |
| Port | Service | Common Use |
| 20 | FTP Data Transfer | Transfers files |
| 21 | FTP Command | Controls FTP sessions |
| 22 | SSH | Secure remote access |
| 25 | SMTP | Email transfer |
| 53 | DNS | Domain resolution |
| 80 | HTTP | Web traffic (non-secure) |
| 443 | HTTPS | Secure web traffic |

## 🔗 What are Protocols?

A protocol defines the rules for data exchange between devices. It ensures that data is sent, received, and interpreted correctly.

- TCP (Transmission Control Protocol): Reliable, connection-based  
- UDP (User Datagram Protocol): Fast, connectionless, no guarantee of delivery

## 🧾 Table Explanation (From Image)

Based on the uploaded table, here is the summary:

|  |  |  |  |
| --- | --- | --- | --- |
| Record Type | Protocol | Service Name | Use |
| 20 | TCP | FTP Data Transfer | Transferring files |
| 21 | TCP | FTP Command Control | FTP session commands |
| 22 | TCP | SSH | Secure login and command execution |
| 25 | TCP | SMTP | Sending emails |
| 53 | UDP | DNS | Resolving domain names to IPs |
| 80 | TCP | HTTP | Viewing websites |
| 443 | TCP | HTTPS | Secure communication between browser and server |

## 🛠️ Practical – Using Nmap Tool

Nmap (Network Mapper) is a powerful open-source tool for network discovery and security auditing.

Capabilities of Nmap:

- Host discovery (live systems)  
- Port scanning (open, closed, filtered)  
- Service enumeration (version info)  
- OS fingerprinting  
- Vulnerability detection (with scripts)

## ⚙️ Command Used Today:

sudo nmap -sS -sV -sC -O scanme.nmap.org

Explanation of Flags:

|  |  |
| --- | --- |
| Flag | Description |
| -sS | TCP SYN Scan – Stealthy and fast, sends SYN packets |
| -sV | Version Detection – Detects versions of services running |
| -sC | Default Scripts – Runs default NSE scripts for service detection and basic vulns |
| -O | OS Detection – Tries to identify the operating system of the target |

## 🔁 Shorter Version:

sudo nmap -A scanme.nmap.org

-A Flag = Aggressive Scan (combines -O, -sV, -sC, traceroute)

## 🧪 More Common Nmap Flags

|  |  |
| --- | --- |
| Flag | Description |
| -Pn | Treat all hosts as online, skip ping check |
| -p | Scan specific ports (e.g., -p 80,443) |
| -T4 | Set timing to faster scan |
| -F | Fast scan (scans fewer ports) |
| -v | Verbose mode – more output |
| --top-ports | Scan top N commonly used ports |
| -sU | UDP Scan |
| -sT | TCP Connect scan (used if no root) |
| -oN | Output to a file (normal text) |
|  |  |

## ✅ Conclusion – Day 5 Summary

Today’s lesson helped you understand:  
- What ports and protocols are  
- How active reconnaissance works  
- Introduction to powerful scanning with Nmap  
- How to use specific flags (-sS, -sV, -sC, -O, -A)  
- How to interpret service-port relationships using the provided table