Day 25: Exploitation on Metasploitable Machine

Topics Covered:

- Intro to Metasploitable Machine
- Basic Exploitation with Metasploit
- Nmap scanning
- Wireshark tool

Metasploitable Overview

- A **UNIX-based** OS for testing vulnerabilities.
- Uses only **Command-Line Interface (CLI)**.
- Runs services like **PostgreSQL** (an open-source database) in a virtual environment.

Accessing Metasploitable from Kali Linux

Use Kali Linux as the attack machine:

1. **Start Metasploit Framework:** `msfconsole -q`
2. **Scan Metasploitable for FTP (Port 21) with Nmap:** `nmap -sV -p 21 <target_IP>`
3. **Start Exploitation Console (if closed):** `msfconsole -q`
   Use different **Metasploit modules** based on what services and vulnerabilities you find.

Wireshark

A network protocol analyzer used by security analysts and pentesters for:

- Capturing and analyzing live network traffic
- Filtering traffic
- Finding suspicious things like FTP logins, DNS queries, and unencrypted HTTP.
  To launch: `wireshark`. Then pick your network interface (e.g., eth0).

Vulnerable Websites for Practice

- textphp
- ocunefix
- Global ERP
  These are vulnerable web apps for ethical hacking and VAPT practice.