Day 25: Exploitation on Metasploitable Machine

Date: July 17, 2025

Topics Covered:

- Introduction to Metasploitable Machine
- Basic Exploitation using Metasploit
- Nmap scanning
- Wireshark tool

Metasploitable Overview

- Metasploitable is a **UNIX-based** operating system specifically designed for vulnerability testing and exploitation practice.
- It is completely **Command-Line Interface (CLI)** based.
- When booted in a virtual environment (such as VMware), it runs multiple services, including **PostgreSQL**.
    - PostgreSQL is an open-source relational database management system.

Accessing Metasploitable from Kali Linux

Use Kali Linux as the attacker machine. The following steps demonstrate a basic workflow:

1. **Start the Metasploit Framework**

   msfconsole -q

2. **Scan Metasploitable for FTP (Port 21) Using Nmap**

   nmap -sV -p 21 <target_IP>

3. **Start the Exploitation Console Again (If Closed)**

   msfconsole -q

Use various **Metasploit modules** depending on the detected services and vulnerabilities.

Wireshark

Wireshark is a widely used network protocol analyzer. It is commonly utilized by Security Operations Center (SOC) analysts and penetration testers for:

- Capturing and analyzing live network traffic
- Filtering traffic using custom expressions

- Identifying suspicious activities such as FTP login attempts, DNS queries, and unencrypted HTTP requests

To launch Wireshark:

```
wireshark
```

Then select the appropriate network interface (e.g., eth0) for capturing traffic.

Vulnerable Websites for Practice

- textphp
- ocunefix
- Global ERP

These names refer to vulnerable web applications commonly found in lab setups or training networks used for ethical hacking and VAPT practice.