Day 109

Topic: System Hacking

Objective: To compromise a system by exploiting identified vulnerabilities using the Metasploit Framework.

Theoretical Concepts:
This is the "Exploitation" phase. We introduced **Metasploit**, a massive framework for developing and executing exploit code. We discussed the components: Exploits (the code that breaks in), Payloads (the code that runs after break-in, e.g., Meterpreter), and Encoders (to hide from AV).

Practical Work:
We targeted the "vsftpd 2.3.4" backdoor vulnerability on our Metasploitable lab machine. 1. Launched *msfconsole*. 2. Searched for the exploit: *search vsftpd*. 3. Configured the payload and target IP: *set RHOSTS*. 4. Executed the attack: *exploit*. We gained a root shell on the target system. We also practiced using **Netcat** to listen for reverse shell connections.

Tools Used: Metasploit Framework, Netcat.

Outcome: Successfully gained unauthorized root access to a vulnerable system in a controlled environment.