Penetration Testing Phases

Phase 1: Reconnaissance and Information Gathering

- Initial step in penetration testing.
- Collect public information about the organization.
- Identify potential vulnerabilities.
- Formulate a strategy for further testing.
- Passive information gathering minimizes detection risk.
- Open-Source Intelligence (OSINT) uses public sources.
    - Web Scraping
    - Google Dorking
    - Social media profiling
- Tools: host, nslookup, dig, whois, knockpy, netdiscover, traceroute, whatweb, theHarvester, sherlock, wfw00f, Google Dorking, OSINT framework.

Phase 2: Scanning and Vulnerability Analysis

- Discover open ports, services, OS versions, etc.
- Identify vulnerabilities, weaknesses, and misconfigurations.
- Active information gathering.
- Requires written permission from the system owner.
- Tools: nmap, searchsploit, nessus, OpenVAS, MSF.

Phase 3: Exploitation and Gaining Access

- Exploit identified weaknesses.
- Gain unauthorized initial entry.
- Methods:
    - Exploit known vulnerabilities.
    - Exploit default configurations and stolen credentials.
    - Brute Force weak credentials.
    - Launch social engineering attacks.
    - Launch phishing attacks.
- Tools: MSF, Exploit DB, Burp Suite, SQLmap, BeEF, Social Engineering Toolkit, Cobalt Strike, PowerSploit.
- Focus: Metasploit Framework

Key Terms: Vulnerability, Malware, Exploit, Payload, and Shellcode

Vulnerability

- Weakness in software, OS, hardware, or system configurations.
- Can be exploited to compromise CIA Triad (Confidentiality, Integrity, Availability).
- Example: CVE-2017-0144 (Microsoft SMBv1).

Malware

- Self-contained executable.
- Designed to harm, steal, or disrupt a system.
- Delivered via phishing, malicious websites, or USBs.
- Requires execution by the end-user.
- Example: WannaCry ransomware.

Exploit

- Code or technique that takes advantage of a vulnerability.
- Gains unauthorized access, escalates privileges, or executes arbitrary code.
- Requires a vulnerability to exist.
- Delivered as a script or crafted input.
- Example: EternalBlue.

Shellcode vs. Payload

| Feature | Shellcode | Payload | | ---------- | ---------- | ---------- | | Definition | Small piece of standalone executable code | Piece of code delivered via exploit to perform a specific action | | Purpose | Typically spawn a shell or execute commands | Can perform a variety of tasks, including data exfiltration and malware installation | | Complexity | Usually compact and self-contained | Can be complex and may include multiple components | | Execution Context | Executed within a vulnerable application | Delivered to the target system through various means | | Types | Local and remote shellcode | Command execution, information gathering, RATs, downloaders, ransomwares |

Environment Setup

1. Kali Linux (Attacker Machine)
2. Metasploitable 2 (Linux based target)
3. Metasploitable 3 (Windows based target)