Penetration Testing Basics

1. What is Penetration Testing?

Penetration Testing (Pen Testing) is a controlled and authorized process of simulating cyber attacks on a system, network, or application to identify security vulnerabilities before attackers can exploit them.

2. Why is Penetration Testing Important?

Penetration testing helps organizations:

- Identify security weaknesses
- Prevent data breaches
- Validate security controls
- Meet compliance requirements
- Improve overall security posture

3. Types of Penetration Testing

- Black Box Testing – Tester has no prior knowledge of the system.
- White Box Testing – Tester has full knowledge of the system.
- Grey Box Testing – Tester has partial knowledge of the system.

4. Penetration Testing Phases

- Planning and Reconnaissance
- Scanning and Enumeration
- Gaining Access
- Maintaining Access
- Analysis and Reporting

5. Difference Between Vulnerability Assessment and Penetration Testing

Vulnerability Assessment identifies and lists vulnerabilities, while Penetration Testing actively exploits vulnerabilities to assess their real-world impact.

6. Common Penetration Testing Tools

- Nmap – Network scanning
- Metasploit – Exploitation framework
- Burp Suite – Web application testing
- Nessus – Vulnerability scanning

7. Legal and Ethical Aspects of Penetration Testing

Penetration testing must always be conducted with written permission. Unauthorized testing is illegal and considered hacking. Ethical guidelines ensure safe and responsible testing.

8. Web Application Penetration Testing

It focuses on testing web applications for issues such as SQL Injection, XSS, authentication flaws, and insecure configurations.

9. Network Penetration Testing

Network penetration testing evaluates network devices, firewalls, servers, and services to find misconfigurations and vulnerabilities.

10. Reporting in Penetration Testing

A penetration testing report includes identified vulnerabilities, risk levels, proof of concept, and remediation recommendations.