Penetration Testing Basics - Questions and Answers

# 1. What is Penetration Testing?

Penetration testing is a simulated cyber attack on a system, network, or application to find security vulnerabilities that could be exploited by attackers.

# 2. Why is Penetration Testing Important?

It helps identify weaknesses, ensure compliance, improve security posture, and protect sensitive data from real threats.

# 3. What are the Types of Penetration Testing?

Types include Black Box (no prior knowledge), White Box (full knowledge), and Gray Box (partial knowledge) testing.

# 4. What is the Penetration Testing Life Cycle?

It includes: Planning & Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Analysis & Reporting.

# 5. What Tools are Commonly Used in Penetration Testing?

Popular tools include Nmap, Metasploit, Burp Suite, Wireshark, and Nikto.

# 6. What is the Difference Between Vulnerability Scanning and Penetration Testing?

Vulnerability scanning identifies known weaknesses, while penetration testing exploits them to assess actual risks.

# 7. What are the Legal and Ethical Considerations?

Pen testing must be authorized and follow legal guidelines to avoid unauthorized access and data breaches.

# 8. What Skills are Needed for a Penetration Tester?

Skills include networking, operating systems, scripting, security protocols, and knowledge of hacking tools and techniques.

# 9. What is a Zero-Day Vulnerability?

A zero-day is a previously unknown vulnerability that is exploited before the vendor has issued a fix.

# 10. What Certifications Help in Becoming a Penetration Tester?

Certifications include CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), and CompTIA PenTest+.