NFSU

विद्या अमृतं अश्नुते

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Penetration Testing

Top 50 Questions and Answers

Placement Cell, NFSU Goa
January 31, 2025

Penetration Testing - Top 50 Questions

1. **What is penetration testing, and why is it important?**
   Penetration testing simulates a cyberattack to identify vulnerabilities. It is crucial for strengthening security by finding weaknesses before malicious hackers do.

2. **What are the different types of penetration tests?**
   Types include external, internal, web application, wireless, social engineering, and physical penetration tests, each targeting different areas of a system.

3. **What is the difference between white-box, black-box, and gray-box testing?**
   White-box testing involves full access to systems, black-box testing simulates an attack with no internal knowledge, and gray-box testing is a combination of both.

4. **What is a vulnerability assessment, and how does it differ from penetration testing?**
   A vulnerability assessment identifies security flaws without exploitation, while penetration testing actively exploits vulnerabilities to assess their impact.

5. **What are some common penetration testing tools you use?**
   Common tools include Metasploit, Burp Suite, Nmap, Wireshark, and Nessus for scanning, exploiting, and analyzing vulnerabilities.

6. **Can you explain the OSI model and its relevance to penetration testing?**
   The OSI model defines seven layers of networking; understanding it helps testers identify where vulnerabilities exist, from physical to application layers.

7. **What is network sniffing, and how is it used in penetration testing?**
   Network sniffing captures and analyzes packets on a network, helping to identify unencrypted sensitive data or misconfigurations.

8. **What is the importance of information gathering (reconnaissance) during a penetration test?**
   Information gathering helps identify attack vectors by collecting publicly available data, such as domain names and server details.

9. **What are the key differences between TCP and UDP, and how do they impact penetration testing?**
   TCP is connection-oriented and more reliable, while UDP is faster and connectionless. These differences affect how attacks are launched and detected.

10. **What is SQL Injection, and how do you defend against it?**
    SQL Injection occurs when malicious SQL code is inserted into input fields. Defense includes input validation, prepared statements, and parameterized queries.

11. **How do you conduct a brute-force attack?**
    A brute-force attack tries all possible password combinations. Tools like Hydra or Burp Suite can automate this process for web applications.

12. **What is Cross-Site Scripting (XSS), and how do you prevent it?**
    XSS injects malicious scripts into webpages. It can be prevented by validating inputs, encoding outputs, and using Content Security Policy (CSP).

Penetration Testing - Top 50 Questions

13. **What is a man-in-the-middle (MITM) attack, and how can you prevent it?**
MITM attacks intercept communication between two parties. Use encryption (TLS/SSL), VPNs, and secure protocols to prevent such attacks.

14. **What is the purpose of a reverse shell in penetration testing?**
A reverse shell allows an attacker to remotely control a compromised system. It is often used in post-exploitation to maintain access.

15. **What is the role of Metasploit in penetration testing?**
Metasploit is a framework for developing and executing exploit code against a target, making it a powerful tool for automating attacks and testing vulnerabilities.

16. **What is the difference between a vulnerability scan and a penetration test?**
A vulnerability scan identifies weaknesses without exploitation, while penetration testing actively tries to exploit those vulnerabilities.

17. **What is social engineering, and how can it impact penetration testing?**
Social engineering manipulates individuals to gain access to systems. It is often used in penetration tests to test employee awareness and security protocols.

18. **What is port scanning, and what tools do you use for it?**
Port scanning detects open ports on a system. Tools like Nmap and Netcat are commonly used to identify exposed services.

19. **How do you identify and avoid false positives in penetration testing?**
By verifying vulnerabilities through manual testing and using multiple tools, penetration testers can minimize false positives.

20. **What is a zero-day vulnerability?**
A zero-day vulnerability is a previously unknown security flaw that is exploited by attackers before a patch is made available.

21. **What is privilege escalation, and how do you achieve it during penetration testing?**
Privilege escalation is the process of gaining higher access levels. It is achieved by exploiting vulnerabilities to move from a low-level account to an admin account.

22. **What is a keylogger, and how do you defend against it?**
A keylogger records keystrokes, capturing sensitive data. It can be defended against by using endpoint protection, encryption, and educating users about phishing.

23. **What is the difference between active and passive reconnaissance?**
Active reconnaissance involves directly interacting with a target system (e.g., scanning), while passive reconnaissance collects information without direct contact.

24. **What are DNS attacks, and how can they be mitigated?**
DNS attacks involve manipulating domain name system data. They can be mitigated by using DNSSEC and securing DNS configurations.

25. **What are the most common security misconfigurations in web servers?**
Common misconfigurations include default credentials, unnecessary services running, and misconfigured access controls.

26. **What is an SSL/TLS handshake, and why is it important in penetration testing?**
    The SSL/TLS handshake is the process that establishes a secure connection. Testing its implementation ensures that data transmission is encrypted.

27. **What is a shellcode, and how is it used in penetration testing?**
    Shellcode is a small piece of code used to exploit vulnerabilities and execute commands on a target system. It is commonly used in buffer overflow attacks.

28. **What is a buffer overflow, and how do you exploit it?**
    A buffer overflow occurs when data exceeds the allocated memory space. It is exploited to overwrite memory and execute arbitrary code.

29. **How do you test a website for Cross-Site Request Forgery (CSRF)?**
    CSRF tests involve simulating unauthorized actions by a user on a vulnerable site. It can be mitigated using anti-CSRF tokens and same-origin policies.

30. **What is the purpose of a Web Application Firewall (WAF)?**
    A WAF protects web applications by filtering and monitoring HTTP traffic to block malicious requests such as SQL injection and XSS.

31. **What is session hijacking, and how can you prevent it?**
    Session hijacking involves stealing a session token to impersonate a user. It can be prevented by using HTTPS, secure cookies, and session expiration mechanisms.

32. **What is a red team engagement?**
    A red team engagement simulates an adversary's attack to test an organization's security measures and incident response capabilities.

33. **What are some examples of network-based attacks?**
    Examples include DDoS, DNS spoofing, man-in-the-middle attacks, and ARP poisoning.

34. **How would you test for weak passwords during a penetration test?**
    Weak passwords can be tested using brute-force or dictionary attacks with tools like Hydra or John the Ripper.

35. **What is the difference between session fixation and session hijacking?**
    Session fixation involves setting a known session ID, while session hijacking steals an active session ID from a victim.

36. **What is the difference between exploitation and post-exploitation?**
    Exploitation involves gaining unauthorized access, while post-exploitation involves maintaining access and performing further actions after a successful breach.

37. **What is the role of a penetration tester in securing cloud environments?**
    Penetration testers assess cloud infrastructures for vulnerabilities, misconfigurations, and weaknesses to ensure the security of cloud-hosted applications and data.

38. **What is the importance of logging and monitoring in penetration testing?**
    Logging and monitoring help detect and analyze suspicious activities, providing critical information for identifying potential security breaches.

39. **What are some methods of protecting against password cracking?**
Protect against password cracking by using strong, complex passwords, multi-factor authentication, and account lockout policies.

40. **What is a pivot in penetration testing?**
Pivoting is a technique where a tester moves from a compromised system to others within the network to expand the scope of the attack.

41. **What is the role of vulnerability scanning in a penetration test?**
Vulnerability scanning identifies potential weaknesses in a system, which are then manually tested and exploited during the penetration testing process.

42. **What is an exploit, and how do you use it during penetration testing?**
An exploit is code or a method used to take advantage of a vulnerability. During penetration testing, exploits are used to verify the existence and impact of vulnerabilities.

43. **What is the purpose of a fuzzing test in penetration testing?**
Fuzzing involves sending random or malformed data to a program or system to identify vulnerabilities like crashes, memory leaks, or unexpected behavior.

44. **What is the importance of ethical hacking in penetration testing?**
Ethical hacking follows legal and ethical guidelines to identify vulnerabilities and improve system security without causing harm to the organization.

45. **How do you test for privilege escalation in a penetration test?**
Testing for privilege escalation involves exploiting system weaknesses to gain higher privileges, such as administrative or root access.

46. **What is the purpose of conducting a post-exploitation phase in penetration testing?**
The post-exploitation phase focuses on maintaining access, expanding control, and gathering valuable data after initial access is gained.

47. **How would you conduct a wireless penetration test?**
A wireless penetration test involves assessing Wi-Fi networks for vulnerabilities like weak encryption, improper access controls, or misconfigured routers.

48. **What is the significance of buffer overflow attacks in penetration testing?**
Buffer overflow attacks exploit programming errors by overflowing buffers, allowing attackers to overwrite memory and execute arbitrary code on a system.

49. **What is a Rootkit, and how do you detect it during a penetration test?**
A Rootkit is a malicious software that allows an attacker to maintain privileged access to a system while hiding its presence. Detection involves using anti-rootkit tools and monitoring system integrity.

50. **What is the difference between a vulnerability scan and a penetration test?**
A vulnerability scan identifies potential vulnerabilities, while a penetration test actively exploits those vulnerabilities to determine their severity and impact.