CYTAD

Pentration Testing Checklist

FOLLOW

IMPORTANT

Penetration testing, a vital component of cybersecurity, is a powerful tool for identifying vulnerabilities in a system.

It's crucial to emphasize that while conducting penetration tests, **both legal and ethical considerations must be at the forefront.**

These tests should only be performed with proper authorization and in compliance with the law. **Unauthorized or unethical penetration testing can lead to legal consequences, privacy breaches, and reputational damage. Maintaining transparency, obtaining consent, and adhering to best practices are essential to ensure the responsible and ethical use of penetration testing.**

1. Did you gather information about the target, such as domain names, IP addresses, and employee names?

☐ Yes ☐ No ☐ N/A

Remarks :

2.Did you perform open-source intelligence (OSINT) gathering?

☐ Yes ☐ No ☐ N/A

Remarks :

3.Did you use tools like WHOIS, Shodan, and Google Dorking to find publicly available

☐ Yes ☐ No ☐ N/A

Remarks :

4. Did you enumerate services to gather version information?

☐ Yes ☐ No ☐ N/A

Remarks :

5. Did you use automated tools like Nessus, OpenVAS, or Qualys to identify known vulnerabilities?

☐ Yes ☐ No ☐ N/A

Remarks :

6. Did you manually analyze and confirm vulnerabilities using techniques like source code review, configuration file analysis, and protocol inspection?

☐ Yes ☐ No ☐ N/A

Remarks :

7. Did you use tools like Hydra or Medusa to test for weak or default credentials for authentication?

☐ Yes ☐ No ☐ N/A

Remarks :

8. Did you employ password-cracking tools such as John the Ripper or Hashcat?

☐ Yes ☐ No ☐ N/A

Remarks :

9. Did you check password complexity and expiration policies manually?

☐ Yes ☐ No ☐ N/A

Remarks :

10. Did you use web vulnerability scanners like OWASP ZAP, Burp Suite, or Acunetix to test for common web application vulnerabilities like XSS, SQL injection, and CSRF?

☐ Yes ☐ No ☐ N/A

Remarks :

11. Did you use tools like Nmap, Hping, or Firewalk to check for misconfigured firewalls or attempt to bypass them?

☐ Yes ☐ No ☐ N/A

Remarks :

12. Did you use tools like Snort or Suricata to test if the IDS can be bypassed?

☐ Yes ☐ No ☐ N/A

Remarks :

13. Did you use tools like Aircrack-ng or Wireshark for wireless network security and evil twin attacks?

☐ Yes ☐ No ☐ N/A

Remarks :

14. Did you utilize tools like Ubertooth and BlueZ for Bluetooth security?

☐ Yes ☐ No ☐ N/A

Remarks :

15. Did you use tools like GoPhish for phishing simulations?

☐ Yes ☐ No ☐ N/A

Remarks :

16. Did you attempt social engineering tactics like tailgating or impersonation?

☐ Yes ☐ No ☐ N/A

Remarks :

17. Did you use lock picking tools for physical access control testing?

☐ Yes ☐ No ☐ N/A

Remarks :

18. Did you employ tools like Proxmark for access badge cloning?

☐ Yes ☐ No ☐ N/A

Remarks :

19. Did you assess IoT device security using tools like Shodan or specific IoT vulnerability scanners?

☐ Yes ☐ No ☐ N/A

Remarks :

20. Did you use malware analysis tools like Cuckoo Sandbox or VirusTotal?

☐ Yes ☐ No ☐ N/A

Remarks :

21. Did you use tools like Metasploit for delivering and testing payloads?

☐ Yes ☐ No ☐ N/A

Remarks :

22. Did you assess API security using tools like Postman, Insomnia, or OWASP Amass?

☐ Yes ☐ No ☐ N/A

Remarks :

23. Did you employ fuzzing tools like American Fuzzy Lop (AFL) or Burp Suite for web application fuzzing?

☐ Yes ☐ No ☐ N/A

Remarks :

24. Did you use OpenSSL or GnuPG for cryptography analysis?

☐ Yes ☐ No ☐ N/A

Remarks :

25. Did you evaluate the strength of encryption algorithms using tools like John the Ripper, Hashcat, or Cryptool?

☐ Yes ☐ No ☐ N/A

Remarks :

26. Did you assess cloud infrastructure and configurations for security issues using tools like AWS Trusted Advisor or Azure Security Center?

☐ Yes ☐ No ☐ N/A

Remarks :

27. Did you assess the security of IoT devices for vulnerabilities with specialized IoT scanning tools?

☐ Yes ☐ No ☐ N/A

Remarks :

28. Did you use tools like PowerSploit or Empire for privilege escalation and post-exploitation?

☐ Yes ☐ No ☐ N/A

Remarks :

29. Did you use tools like data loss prevention (DLP) solutions or network monitoring tools for data exfiltration attempts?

☐ Yes ☐ No ☐ N/A

Remarks :

30. Did you check if the system logs events and whether they can be exploited using log analysis tools like ELK Stack or Splunk?

☐ Yes ☐ No ☐ N/A

Remarks :

31. Did you use reporting tools like Dradis, Faraday, or Microsoft Word to create a detailed report outlining findings, vulnerabilities, and recommendations for remediation?

☐ Yes ☐ No ☐ N/A

Remarks :

32. Did you use tools and methods to verify that identified vulnerabilities have been properly patched, such as vulnerability scanners and manual retesting?

☐ Yes ☐ No ☐ N/A

Remarks :

33. Did you ensure proper authorization and legal documentation for the penetration test, and followed relevant standards and regulations?

☐ Yes ☐ No ☐ N/A

Remarks :

34. Did you use cleanup tools and procedures to remove test artifacts and restore the system to its original state?

☐ Yes ☐ No ☐ N/A

Remarks :

35. Did you conduct a post-test debriefing to discuss what went well and what could be improved?

☐ Yes ☐ No ☐ N/A

Remarks :

36. Are you keeping up-to-date with the latest tools, techniques, and vulnerabilities through ongoing training and education, such as attending courses, conferences, or webinars?

☐ Yes ☐ No ☐ N/A

Remarks :

Follow CYTAD on Linkedin for security advisories, checklists, mentoring, services, insights and much more