ALLSAFE ACADEMY

Junior Penetration Tester Path (JrPT)

WWW.ALLSAFEACADEMY.COM

INFO@ALLSAFEACADEMY.COM

Module 1 : Introduction to Penetration Testing

- Penetration testing is a proactive approach to identify and exploit vulnerabilities in computer systems, networks, and applications in order to improve their security.
- Ethical considerations are essential, and penetration testers must operate within legal boundaries and obtain proper authorization for testing.
- The penetration testing methodology typically includes five phases: reconnaissance, scanning, enumeration, exploitation, and reporting.

Module 2 : Information Gathering and Reconnaissance

- Information gathering involves collecting data about the target system, including IP addresses, domain names, and employee information.
- Passive reconnaissance techniques involve gathering information from public sources, such as search engines, social media, and online forums.
- Active reconnaissance techniques involve direct interaction with the target system, such as port scanning, network mapping, and service enumeration.

Module 3 : Vulnerability Assessment and Exploitation

- Vulnerability assessment aims to identify vulnerabilities in target systems through various methods, such as vulnerability scanning and manual inspection.
- Exploiting vulnerabilities involves taking advantage of identified weaknesses to gain unauthorized access or control over the target system.
- Common vulnerabilities include misconfigurations, weak passwords, software vulnerabilities, and insecure network protocols.

Module 4 : Network Penetration Testing

- Network penetration testing focuses on assessing the security of network infrastructure, including routers, switches, firewalls, and network services.
- Techniques such as port scanning, service enumeration, and network sniffing help identify potential entry points and vulnerabilities.
- Post-exploitation activities involve maintaining access, escalating privileges, and pivoting within the network.

Module 5 : Web Application Penetration Testing

- Web application penetration testing aims to identify vulnerabilities in web-based applications, such as SQL injection, cross-site scripting (XSS), and command injection.
- Manual and automated scanning techniques, using tools like Burp Suite and OWASP ZAP, help identify common web vulnerabilities.
- Exploiting web vulnerabilities can lead to unauthorized data access, session hijacking, defacement, or remote code execution.

Module 6 : Wireless Network Penetration Testing

- Wireless network penetration testing focuses on assessing the security of Wi-Fi networks and related protocols.
- Techniques include wireless network scanning, capturing and analyzing network traffic, and identifying weak encryption mechanisms.
- Exploiting wireless network vulnerabilities may involve cracking WEP or WPA/WPA2 encryption, conducting rogue access point attacks, or exploiting misconfigurations.

THANK YOU