CYHUB ARMENIA Microsoft Innovation Center

Course Title: Hacking 101

Duration: 80 hours, 40 lessons

Introduction to Penetration Testing

1. What is Pentest, red teaming. Planning and scoping of Pentest, rules of engagement, pentest phases

Information Gathering

2. Information gathering, passive information gathering,
3. Open-source intelligence /OSINT/ (Google dorks, social media, various services and tools)
4. Active information gathering, port scanning
5. Service fingerprinting and enumeration, vulnerability scanning
6. Web scanning
7. Vulnerability analysis, preparing information for Pentest

Engagement and post exploitation

8. Non-technical tests; Social engineering and physical security
9. Network tools
10. Network and network services Pentest
11. Web Pentest: mapping
12. Exploitation
13. Lateral movement
14. Post exploitation

Vulnerabilities

15. Authentication vulnerabilities
16. Authorization vulnerabilities
17. Cross Site Scripting /XSS/
18. SQL injection
19. Cross-Site Request Forgery /CSRF/
20. File and directory traversal attacks
21. Server-side request forgery /SSRF/
22. Business logic vulnerabilities
23. OS specific vulnerabilities

24. Privilege escalation attack

Other types of pentest

25. Wi-Fi Pentest
26. Mobile application Pentest

Reporting and Remediation

27. Reporting, recap