Penetration Testing: Fundamentals

Duration: 2 days (16 hrs)

1: Fundamentals and Key Processes

Module 1: Overview of Penetration Testing

- **Introduction to Penetration Testing**
  - Definition and purpose
  - Importance in enhancing organizational cybersecurity
  - Ethical and legal considerations
- **The Penetration Testing Lifecycle**
  - Pre-engagement activities
  - Active testing phases
  - Reporting and post-testing actions
- **Connection to Defensive Cybersecurity**
  - How Pen Testing strengthens defensive measures

Module 2: Information Gathering and Vulnerability Analysis

- **Reconnaissance Techniques**
  - Open-source intelligence (OSINT)
  - Passive vs. active reconnaissance
- **Identifying Vulnerabilities**
  - Tools and methodologies (e.g., Nmap, Nessus, Burp Suite)
  - Overview of OWASP Top 10 vulnerabilities and examples:
    - Injection flaws
    - Broken authentication
    - Security misconfigurations

Module 3: Web and Application Security Testing

- **Understanding Rich-Thin Applications**
  - Definitions and architecture overview
  - Security challenges unique to each
- **Testing Web Applications**

- OWASP Top 10 examples:
    - Cross-Site Scripting (XSS)
    - Insecure Direct Object References (IDOR)

- **Testing Post-Application and Cloud Security**
    - Identifying cloud-specific risks

2: Advanced Techniques and Reporting

Module 4: Exploitation and Mitigation Strategies

- **Exploitation Basics**
    - Crafting and executing exploits
    - Demonstrating impact (without full-scale exploitation)
    - Case studies from recent incidents
- **Defensive Measures and Hardening**
    - Mitigating risks identified in OWASP Top 10
    - Strengthening application, cloud, and system security

Module 5: Reporting and Post-Engagement Activities

- **Effective Reporting Techniques**
    - Structuring penetration test reports
    - Highlighting critical vulnerabilities
    - Suggesting actionable remediations
- **Post-Engagement Activities**
    - Debriefing stakeholders
    - Planning for remediation

Module 6: Awareness and Practical Applications

- **Enhancing Defensive Security Through Awareness**
    - Key insights for cybersecurity experts
    - Proactive measures based on penetration testing results
- **Final Discussion**
    - Q&A session and feedback