ICSI

INTERNATIONAL CYBERSECURITY INSTITUTE

Course Outline: Web Application Penetration Testing and Ethical Hacking

Certification: ICSI | CPT Certified Penetration Tester

Required Courses and Exams:

Course	Exam
a) Network Infrastructure Penetration Testing and Ethical Hacking (5 Days)	CPT-INF
b) Web Application Penetration Testing and Ethical Hacking (3 Days)	**CPT-WEB**

Note: You need to pass both exams to become an ICSI | CPT Certified Penetration Tester.

Duration: 3 Days

Candidate Prerequisites:
Basic understanding of web application technologies.

Overview:
You'll gain insight into the insecurities, vulnerabilities and exploits that lie within web applications so you can reduce the risk this poses to your business. This course is based on OWASP Top 10 2017 and along with course Network Infrastructure Penetration Testing and Ethical Hacking will help students prepare for the CREST CRT examination.

Who Should Attend:
Those responsible for developing, managing, testing or maintaining web based applications or anyone with an interest in the security of their web presence.

What is Included:

- eBook
- Lab Guide
- 6 months 24x7 remote access to a virtual lab
- 1 exam voucher - Online Exam Proctoring
- Certificate of Attendance (Digital)

Module 1: HTTP Protocol overview

- Important HTTP methods
- Cookies
- Web Application Architecture
- OWASP TOP 10

Module 2: Web Vulnerability Scanners and Proxies

- Burp proxy
- OpenVas
- Nikto, Wapiti

Module 3: Profiling the Web server

- Nmap
- Metasploit Auxiliary Modules

Module 4: Injection

- Command injection
- SQL Injection
- Blind SQL Injection
- Sqlmap
- Mitigation of Injection

Module 5: Broken Authentication

- Authentication Protocols and weaknesses
- Brute forcing credentials using Hydra
- Mitigation of Broken Authentication and Session Management

Module 6: Sensitive Data Exposure

- Examples
- Scanning for Sensitive Data Exposure Issues
- Mitigation of Sensitive Data Exposure

Module 7: XML External Entities (XXE)

- XML External Entities XXE
- Exploiting an XML External Entity Injection
- Mitigation of XML External Entities (XXE)

Module 8: Broken Access Control

- Directory Traversal Overview
- Mitigation of Broken Access Control

Module 9: Security Misconfiguration

- Understanding Security Misconfiguration
- Using Burp to detect security misconfiguration
- Mitigation of Security Misconfiguration

Module 10: Cross-Site Scripting (XSS)

- Types of cross-site scripting
- Using Burp to test for XSS vulnerabilities
- Mitigation of cross-site scripting (XSS)

Module 11: Insecure Deserialization

- Examples
- Searching for vulnerabilities
- Mitigation of Insecure Deserialization

Module 12: Using Components with Known Vulnerabilities

- Examples
- Searching for Vulnerabilities
- Mitigation of using components with Known Vulnerabilities

Module 13: Insufficient Logging and Monitoring

- Examples
- Mitigation of Insufficient Logging and Monitoring

Module 14: Capture the Flag workshop

In this workshop you will apply skills acquired during the course to conduct a full web penetration test in an isolated environment.

Exam:
The CPT-WEB practical certification exam covers Hands-On material from all 13 modules. The exam duration is 2 hours. Passing Grade = 70%.