Penetration Tester

Program Details

This certificate program provides the skills and knowledge to simulate cyber attacks on web-based systems, networks and applications with the intention to secure them. With these skills, you can work in a diverse set of industries and sizes of organizations.

While you can work as an inhouse expert in these organizations, it is more likely that you will be working with a consulting or risk management organization to help your clients mitigate these risks.

Location	At the iWIL Pro training centre near you
Mode of Delivery	Hybrid
Mode of Assessment	Online (from the training centre)
Duration	40 hours (weekday/weekend batches)
Prerequisite / Entry Requirements	• Graduate (or pursuing graduation) • Desirable: 1-3 years of IT work experience/ Python programming
Possible occupational outcomes	Information Security Analyst, Security Analyst, Certified Ethical Hacker (CEH), Security Consultant, (Computing / Networking / Information Technology), Penetration Tester
Tuition fee	Rs. 35,000 (plus GST)
Fees Includes	Training + Exam + Certificate (iWIL CSP)
Fee Excludes	Fees for external certificates (if applicable)

Units to Study

Operating Systems (Windows, UNIX and Linux)
An introductory understanding of the popular Operating Systems to help in detecting security-related issues.

Languages (C, C++, C#, Java, ASM, PHP, PERL)
A sufficient working knowledge about various computing languages to be able to write complex programs and diagnose any errors in a written code.

Networking and hardware
A knowledge of various network servers and networking tools (e.g. Nessus, nmap, Burp, etc.) and the related computer hardware and software systems is critical to understand the failure points in any security attack.

Web-based applications
The applications hosted on cloud are most vulnerable to cyber attacks due to the interplay of multiple systems like server, hosting service, applications and user interfaces. This unit covers concepts of SQL injection, scripting errors etc in this context.

Security frameworks
A knowledge of frameworks like ISO 27001/27002, NIST, HIPPA, SOX, etc. is important to be able to dive deeper into the underlying security protocols and how a hacker might be able to exploit them.

Security tools and products
There are various tools like Fortify and AppScan that are used to secure the software applications from external attacks. This unit deals with comparative analysis of these tools and products to be able to advise on the best options to an organization.

Vulnerability analysis and reverse engineering
A tester needs to be proficient in analysing the vulnerability of a system and use the right framework to communicate this to the end users in simple words. This is the most important output expected from this role.

Metasploit framework
Metasploit Framework, the Metasploit Project's best-known creation, is a software platform for developing, testing, and executing exploits. It can be used to create security testing tools and exploit modules and also as a penetration testing system.

Forensics tools
A hands-on working on industry-standard tools like SIFT, CrowdStrike, FTK Imager etc gives tremendous confidence to a Penetration Tester about penetrating a live site used for this purpose.

Cryptography principles
A theoretical understanding of Kerckhoff's principle and others is needed to guage a system's strength in authentication of critical information.