



PENETRATION TESTING OF INFORMATION SYSTEMS

COURSE DESCRIPTION

The ability of an organization to proactively test its own defenses is quickly becoming more a requirement than a luxury. Penetration testing (Pentesting) is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, and known and/or unknown hardware or software flaws. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

THE STUDENT WILL LEARN:

- + How to analyze their organizations network as a potential intruder would
- + How to scan and launch attacks against encountered vulnerabilities
- + How to gain access and escalate privileges without being detected
- + How to recover from a successful intrusion

PREREQUISITES:

- + General understanding of computer networks and networking protocols
- + A fundamental understanding of computer security (Security+ recommended)
- + General knowledge of computer and operating system fundamentals is recommended

COURSE INFORMATION:

5 days, MF, 40 hours. A certificate of completion will be given at the end of the course. Each student will be provided with a preconfigured laptop with all course training software.