Security Testing: Theory and Practice
IYM016 (Option)

Aims

This course provides the foundation and theoretical underpinning which aims to give an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system. This foundation forms the basis of a methodical approach to surveying and auditing systems, and prepares candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.

Pre-requisites
IYM003 Network Security and IYM004 Computer Security (or equivalent industry experience or certifications)

Essential Reading


Included as study material once registered on the course.

Assessment

This module is assessed by a two hour unseen written examination.

Learning Outcomes

On completion of the module students will have:

• Gained an understanding of common approaches and methodologies used for carrying out and managing security and penetration testing, as well as an understanding of the legal aspects involved in such audits.
• Gained a detailed understanding of some typical network protocols, relevant computer system architectures, and web application systems.
• Gained an understanding of the vulnerabilities in some existing protocols, systems, and applications, and some common forms of attack; in addition, an understanding of the security technologies designed to mitigate these vulnerabilities.
• Gained practical experience of how these vulnerabilities may be exploited in practice to penetrate a system.
**Syllabus**

*Topic 1 – Security testing Management and Methodology*
  - Introduction to the module – discussion on security testing, management issues, frameworks and methodologies
  - OSSTM (Open Source Security Testing Methodology)

*Topic 2 – Network based Security Testing*
  - Introduces network based testing
  - TCP/UDP/IP/ICMP, etc., ping and traceroute, network devices and theoretical basis for vulnerabilities
  - ISSAF approach and methodology, information gathering and network mapping
  - DNS, WHOIS, tools such as nmap for reconnaissance, vulnerability identification and verification (CVE)

*Topic 3 – System Based Security Testing*
  - Operating systems, access control in Windows and Unix-like systems
  - Host based intrusion detection
  - Escalation of privileges and how to exploit these vulnerabilities in practice
  - System hardening

*Topic 4 – Web Application Security Testing*
  - Internet based applications, web services, protocols and languages
  - Example exploits such as SQL injection, cross site scripting or similar
  - Exploiting vulnerabilities
  - Registry database
  - Vulnerability mitigation

*Topic 5 – Pen testing Lab Sessions*
  - A set of exercise sheets covering elements of the module, such as
    - nmap – reconnaissance and port scanning
    - The Metasploit framework and scanning
    - Exploiting a system in practice

*Topic 6 – Legal Aspects*
  - An overview of the legal aspects involved when doing penetration testing.

*Topic 7 – Revision*
  - Course review and exam questions practice

**Key module coverage:**

* Professional Security Testing: management and methodologies
* Overview of Planning and Initiating Processes
* Security Testing Execution Processes:
  - Information Gathering
  - Network Mapping
  - Vulnerability Identification
  - Penetration: vulnerability exploitation
  - Privilege Escalation and Further Compromise
  - Maintaining Access and Covering the Tracks
* Web Application Security Testing
* Closing Processes, Reporting and Testing Data Handling
* Legal Aspects in Security Testing