

Ethical Hacker Associate

Our **five day** course covers current techniques and associated skills used for ethical hacking and penetration testing. The course allows you to learn and practice current techniques used by industry qualified cyber-security penetration testers when conducting engagements in real world environments. The course includes the theory, as well as immersive, hands-on demonstrations and exercises of security assessment skills in four days, with the fifth day dedicated to assessments.

Aim

Increase knowledge of current ethical hacking techniques and practice using hands-on penetration testing skills in a safe environment. By completing the course you will be on your way to becoming a security consultant, knowing how to liaise with technical and non-technical clients.

Who Should Attend?

- IT professionals who wish to understand ethical hacking techniques and perform tasks in vulnerable environments

Prerequisites

It is recommended that you have an in-depth knowledge of networking and the TCP protocol, as well as some familiarity or experience using the command line and Linux.

Learning Objectives

- Understand information security in the corporate world
- Develop an understanding of ethics and criminal law in relation to ethical hacking
- Network enumeration and network mapping
- Network device management and exploitation
- Service enumeration
- Service topology/dependency mapping
- Service management and exploitation
- Application enumeration and profiling
- Application and operating system management
- Application and operating system exploitation and manipulation
- Conducting penetration testing engagements
- The professionalism, communication skills, ethics and the law associated with penetration testing
- Risk management
- Required critical thinking when conducting security testing.