



Call us on...  
**0113 257 8955**



## Ethical Hacking and Countermeasures

### Part of the Sec-1 Training Programme

#### Course Overview

The Ethical Hacking and Countermeasures Course has been developed to provide you with the skills, tools and techniques to effectively assess the threat to your organisations network security.

#### Course Outcomes

During this engaging one day module, you will advance your knowledge of network security attacks through a series of instructor-led modules.

You will:

- Learn the theory of Hacking, including the ways in which Malicious Intruders gather information on network vulnerabilities
- Be taught to utilise the methodology and tools an unauthorised intruder would use to gain access to a network
- Put your knowledge to the test in a series of hands-on labs, attempting to hack our simulated network

#### Key Benefits

This training module provides attendees with the following benefits:

- The skills, tools and techniques required to effectively assess the threat to your organisations network security
- Free Trial of the AppCheck Web Application and Infrastructure Scanner
- Free Toolkit, a collection of the latest scanning, hacking and cracking tools
- 8 CPE Credits

#### What do our other clients say about us?

*I thoroughly enjoyed my day with Sec-1; the course was a real eye opener. It showed how online tools are readily available for hackers to use, which has led me to take preventative steps to ensure this doesn't happen to our network. Overall an informative day which I would actively recommend to others...*

IT Manager  
Local Regional Government

#### Accreditations



## Course Schedule

### 09:00 Hacking Overview

- 4 Steps to Intrusion
- Footprinting the Target
- Enumerating the Application
- Port Scanning
- Vulnerability Exploitation

### 10:00 Attack Methods

- Protocol Attacks
- Man In The Middle Attack
- ARP Cache Poison Attack
- Hijacking Connections Using MITM Attacks
- IP Spoofing
- Application Attacks
- Stack Overflows
- Heap Overflows
- Input Validation Attacks
- Stack Overflow Details
- Hijacking the Return Address
- Buffer Overflow Exploitation
- Vulnerability Scanners

### 11:45 Attack LAB 1

- Install the Sec-1 Exploit Arsenal
- ARP Cache Poison Attack
- Hijack a Connection
- Steal Confidential Data

### 12:00 Bypassing Perimeter Defences

- Firewall Technologies
- Common Firewall Misconfigurations
- Advanced Bypassing Techniques

### 12:30 Password Cracking

- FTP, POP3, HTTP,IMAP
- Windows Passwords
- Time-Memory Trade Off cracking
- Using latest Cracking tools

### 13:00 Lunch

### 14:00 Attack LAB 2

- Identify a Vulnerable Web Server
- Using a CGI Scanner
- Using Sec-1 Exploit Arsenal to gain administrator Access
- Install 2 Backdoors
- Crack OS passwords

### 15:00 Attack LAB 3

- Using 0-day Exploits
- Exploit a SMTP Server
- Install a Dynamic Packet Sniffer
- Capture Email and Passwords

### 16:00 Advanced Hacking

- Bespoke Applications
- Input Validation
- SQL Injection

### 16:30 Attack LAB 4

- SQL Injection
- Bypassing Authentication Forms
- Executing Stored Procedures

### 17:00 Intrusion Prevention

- Firewall Configuration
- Patch Deployment
- IDS Systems
- Web Site Design

### 17:00 Q&A

### 17:30 Finish

## Who Should Attend

Sec-1's Ethical Hacking and Countermeasures Course is designed for IT Professionals responsible for or with an interest in their organisations network security

## Prerequisites

Attendees should have a working knowledge of TCP/IP and common networking technologies

## About the Sec-1 Training Programme

Sec-1 has developed a training programme to provide IT professionals a structured approach to learning.

The training programme is constantly under development.

Other courses include:

- Securing Web Applications
- Wireless Hacking and Countermeasures

