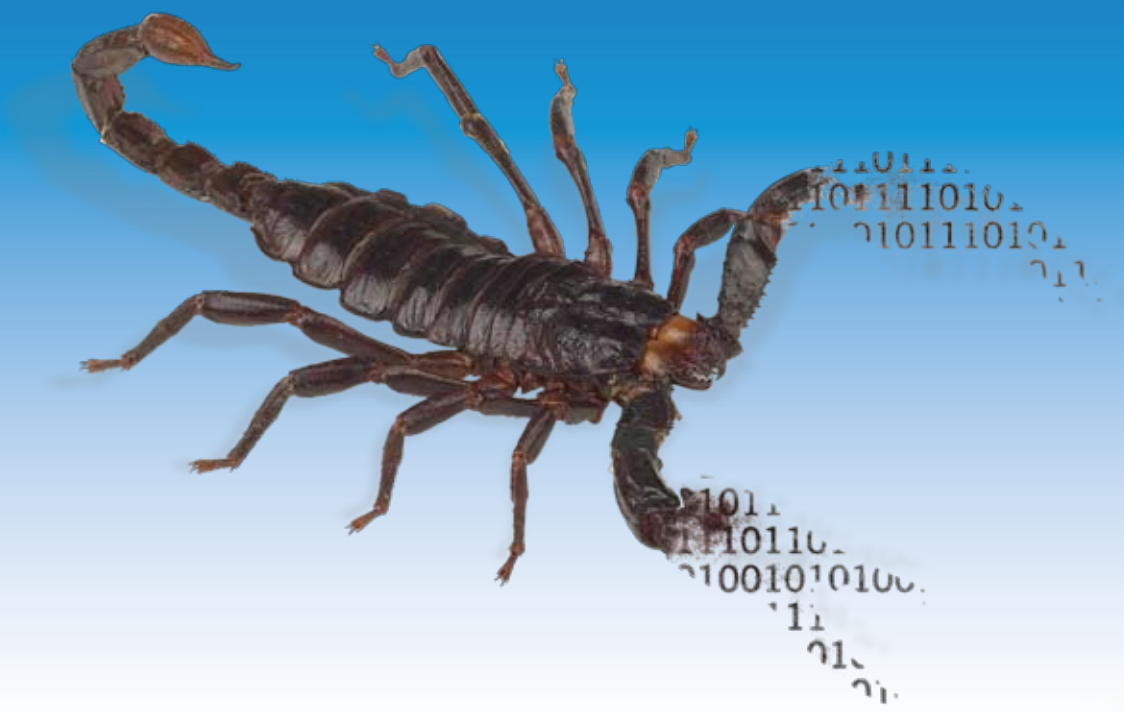
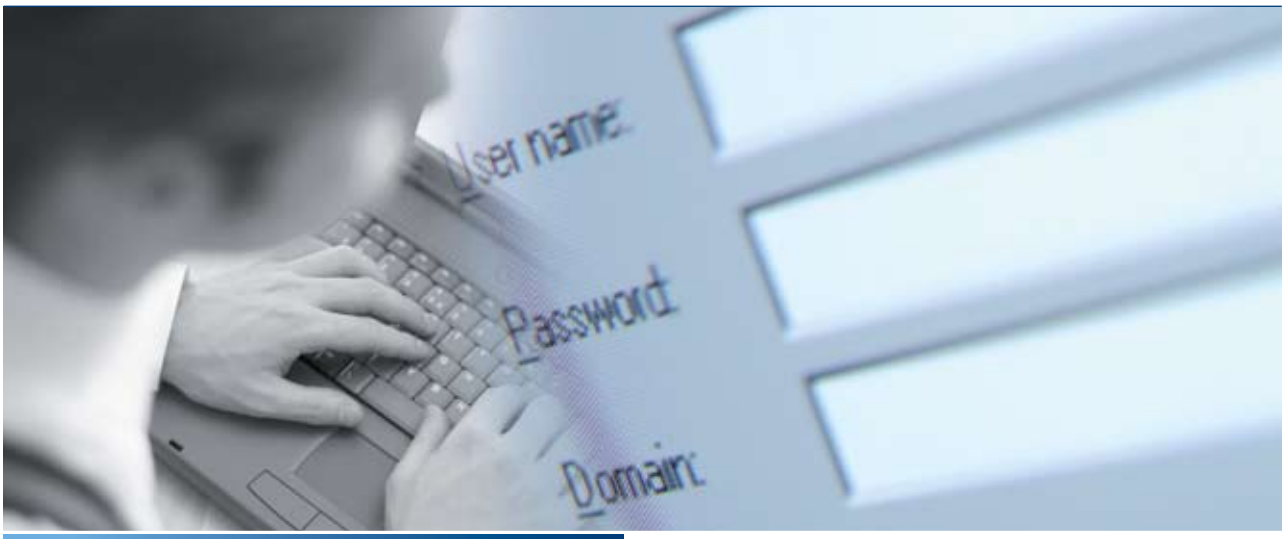
CSTA Ethical Hacking: Hands-On

7safe training

Course Outline



CSTA Ethical Hacking: Hands-On



The CSTA training course provides a comprehensive grounding in the methodology, techniques and culture of ethical hacking.

It takes delegates on a practical journey through the various stages and elements of a penetration test, from initial information discovery and target scanning through to exploitation, privilege escalation, and retaining access.

The course also explores the usage of Trojans and Root kits, which have become increasingly important elements of the ethical hacking arena.

What you will learn

- How to use the tools, techniques and methodologies employed by hackers, in 7Safe's purpose-built lab environment
- How hackers can accurately collect and assimilate information about an organisation's infrastructure whilst avoiding detection
- Measures to secure and protect information against hacker attacks
- Limitations of firewalls and the tools used to bypass them
- Which tools can be used to leverage access on a system
- How information may be used to assess weaknesses and subsequently launch an attack against a target
- How hackers conceal their tracks and the route through which access to a target may be maintained
- The implications of flawed web applications security
- How web users are at threat

Benefits

- Delegates will learn about the hacker mindset and become familiar with the tools used to attack systems
- Our state of the art class environment covers Windows and UNIX operating systems and associated server software
- Includes examination, successful completion of which earns delegates the CSTA certification, a prerequisite for the CSTP certification
- Around 40 hands-on practical exercises are featured, using a wide range of hacking tools

Who should attend

Those responsible for the security of IT systems, including but not limited to: System/Network Administrators, Crime Prevention & Protection Offices, Auditors, Security Officers, Information Security Professionals & Penetration Testers.

Course style

The course is a hands-on journey into the hacking mindset, examining and practically applying the tools and techniques that hackers use. Delivery is in an interactive format with the use of multimedia and practical hands-on workshops. Open group discussion is strongly encouraged. The course is designed to educate for the purpose of properly defending systems from hacking attacks.

Level & Prerequisites

A familiarity of TCP/IP and a background in Microsoft Windows and/or UNIX is desirable.

Course content highlights

HACKING – AN INTRODUCTION

- A history and cultural overview of hacking
- Insights into the hacker mindset
- Hacker genres

COMMUNICATION PROTOCOL BASICS

Provides a fundamental understanding of communication protocols

- An overview of TCP/IP & Networking
- An introduction to ports and protocols
- Sniffing and intercepting traffic
- Man in the middle attacks

METHODOLOGY OVERVIEW

A practical exploration of hacking/penetration testing methods

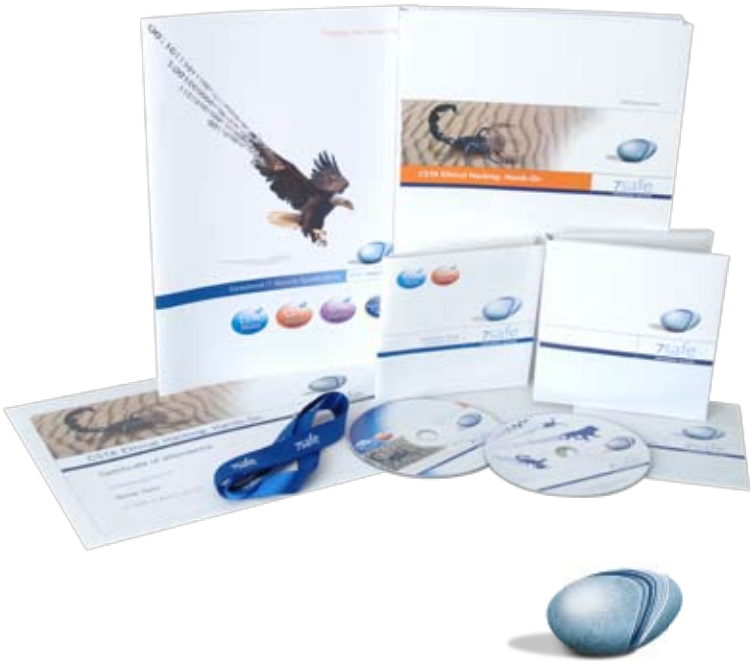
- Information Discovery
  - How information about a target may be gathered discreetly
  - Target profiling
  - Using public databases to reveal sensitive information
  - Social engineering
  - Target scanning & system detection
  - Examining the target landscape
  - Operation system detection
  - Port scanning to reveal openings in the system
  - Use of bespoke tools for enumerating banners
- Vulnerability Assessment (VA)
  - How attackers probe and test for weaknesses
  - Setup and configuration of VA tools
- Exploitation & Privilege Escalation
  - How access may be gained & privilege escalated to achieve full control of Windows & Unix systems
- Trojans, Back-Doors & Root Kits
  - Practical hands-on use of 'Trojan horses' & 'back doors'
  - Working with root kits to hide the presence of a hacker at the application & kernel level
- Firewall & IDS Evasion
  - How attacks may traverse a firewall
  - The role of intrusion detection & how it may be evaded using advanced techniques
- Hacking prevention
  - Security policy, system integrity, hardening & monitoring
  - Security tools, vulnerability assessment & penetration testing
- Sample of featured tools
  - Cane and Abel
  - Wireshark
  - Nmap
  - Amap
  - Netcat
  - Nessus/NeWT
  - Nikto

Duration

3 days

Cost

£1498.50+VAT



7safe | information security services

University Accredited Training

The CSTA Ethical Hacking: Hands-On training course, Certified Security Testing Associate (CSTA) certification and university-accredited CSTA+ qualification have proven to be increasingly important to individuals working within the area of penetration testing.
The latter also forms part of 7Safe's Masters-level education programme.

- Penetration Testing
- Education
- Computer Forensics
- Payment Card Industry DSS
- ISO 27001 Consulting

t +44 (0)870 600 1667
e contact@7safe.com
w www.7safe.com

CPE Credits: 24

PgC Credits: 15

MSc Credits: 15