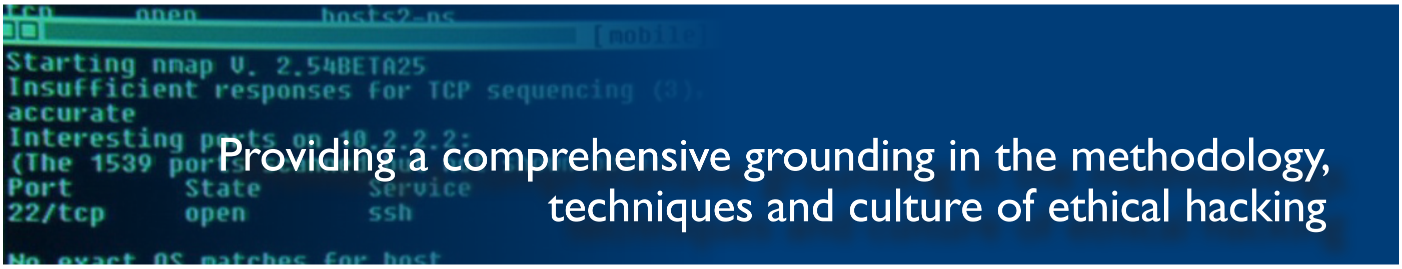
Ethical Hacking: Hands-On



```
tcp         open          hosts2-ns
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3).
accurate
Interesting ports on 10.2.2.2:
(The 1539 por
Port         State        Service
22/tcp       open         ssh
No exact OS matches for host
```

Providing a comprehensive grounding in the methodology, techniques and culture of ethical hacking

CSTA takes delegates on a journey through the various stages of a hacking attack, or equally a penetration test, from initial information discovery and target scanning through to exploitation, privilege escalation and retaining access.

On this course, practical exercises reinforce theory with each delegate having access to a Windows 2008 domain (server and workstation) along with a Linux server. Although the course demonstrates current hacking techniques, this is always done with defence in mind and countermeasures are discussed throughout. The CSTA exam (theory based) is included at the end of the course.

The course is ideally suited to anyone with responsibility for, or with an interest in, the security of IT systems, such as: system administrators, auditors, IT security officers, information security professionals and budding penetration testers.

To Book Call:

+353 1 685 4942

Duration: 4 days
Cost: €2100.00

Prerequisites

A basic understanding of TCP/IP networking, e.g.

- Can you describe at a high-level how a request reaches a web server through Ethernet, IP and TCP?
- What function does ARP perform?
- How does a system know whether or not a gateway is required?
- What is a TCP port?

Familiarity with the Windows or Linux command line, e.g.

- What's the difference between a command and its switches?
- Can you navigate the file system using commands?
- Can you extract and display basic network configuration information, etc?

Together with CSTP helps prepare you for the CREST Registered Tester qualification

CPE Credits: 32

MSc Credits: 15

Course Content

A full list of practical exercises is available on our website: www.7safe.com/csta

Introduction

- Motivations behind hacking
- The hacking scene
- Methodology

Networking Refresher

- Sniffing traffic

Information Discovery

- Useful information
- Sources – websites, metadata, search engines, DNS, social engineering

Target Scanning

- Host discovery
- Port scanning techniques
- Banner grabbing

Vulnerability Assessment

- Causes of vulnerabilities
- The classic buffer overflow
- Vulnerability tracking
- Scanning
- Client-side vulnerabilities

Attacking Windows

- Windows enumeration
- Metasploit
- Client-side exploits

Privilege Escalation – Windows

- Local information gathering
- Metasploit's Meterpreter
- Keyloggers
- Password storage
- Password extraction
- Password cracking techniques
- Cached Domain Credentials
- Windows network authentication
- Access tokens
- Pass the hash

Attacking Linux

- Exploitation
- Web shells
- Pivoting the attack
- Online password cracking
- ARP Poisoning Man in the Middle

Privilege Escalation – Linux

- Standard streams
- Privilege escalation by exploit
- Commercial penetration testing tools
- Password storage
- Password cracking
- Permission errors
- Sudo
- SUID
- Flawed shell scripts

Retaining Access

- Backdoors
- Trojan Horses
- Delivery mechanisms
- Botnets
- Bypassing client-side security

Covering Tracks

- Hiding backdoors
- Simple obfuscation
- Rootkits
- Anti-forensics
- Log manipulation
- Connection laundering

Conclusions

CSTA Exam