COURSE OUTLINE

ETHICAL HACKING
Certified Security Testing Associate (CSTA)

●●●○ **CORE-LEVEL COURSE** Cost: **£3,250.00** + VAT Duration: **5 days**

This infrastructure ethical hacking course is our most popular core-level technical course for people from a wide variety of network related and security roles across all industry sectors looking to develop their own capability to support their organisation's in-house cyber team.

> *I found it all very interesting, the hardware and software system was excellent; everything worked as planned. The content was extremely relevant to our organisation."*
> ***CSTA Delegate***
> ***SuperWebs Ltd***

Assured Training in association with the National Cyber Security Centre

Assured Service Provider
in association with National Cyber Security Centre
Training Course

APMG International

COURSE OVERVIEW

Our five-day ethical hacking training course is a hands-on journey into the hacking mind-set, examining and practically applying the tools and techniques that an external threat may use to launch "infrastructure" attacks on your organisation.

The various stages of that attack, or equally a penetration test, are explored from initial information gathering, target scanning and enumeration through to gaining access, exploitation, privilege escalation and retaining access. Practical in-depth hands-on exercises using various tools reinforce the theory as you experiment with a Windows 2012 domain (server and workstation) plus a Linux server.

The course demonstrates cyber-attack techniques but this is always done with defence in mind and countermeasures are discussed throughout, enabling delegates to identify the threats and understand the strategies, techniques and policies required to defend their critical information.

THE SKILLS YOU WILL LEARN

- You will learn a series of attack methodologies and gain practical experience using a range of tools to undertake an infrastructure penetration test across a multi-OS environment
- Once you are able to identify and exploit vulnerabilities in a safe manner, you will be introduced to a range of defensive countermeasures, allowing you to protect your network and respond to cyber threats

KEY BENEFITS

This course will provide you with the following:

- An understanding of the risks and how to mitigate them
- Learn a number of methodologies for undertaking an infrastructure penetration test
- Acquire effective techniques to identify exploits and vulnerabilities
- Improve your ability to respond effectively to cyber threats
- Valuable preparation and hands-on practice in preparation for the CREST Registered Penetration Tester (CRT) examination

WHO SHOULD ATTEND

The course is ideally suited to anyone looking to improve their career prospects or transitioning into a cyber security role, including:

- Network engineers
- Systems administrators
- Systems architects or developers
- IT security officers
- Information security professionals
- Budding penetration testers

PREREQUISITES

Basic understanding of TCP/IP networking

- Are you familiar with the OSI model?
- Can you name a layer 2 and layer 3 protocol?
- What function does ARP perform?
- Can you describe at a high-level how a request reaches a web server through Ethernet, IP and TCP?
- How does a system know whether or not a gateway is required?
- What is a TCP port?

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com

PA

COURSE OUTLINE

ETHICAL HACKING
Certified Security Testing Associate (CSTA)

●●●○ **CORE-LEVEL COURSE** **Cost: £3,250.00 + VAT** Duration: **5 days**

Be comfortable with Windows and Linux command line. As a guideline, you should be able to tick off the following (without heavy recourse to Google):

- Understand how switches change the way commands work
- How does adding > affect a command?
- Understand the difference between cd /folder/file and cd folder/file (i.e. what does / at the front of the path do?)
- Understand the difference between ../file and ./file
- Understand how to pull up built-in help for a command

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Security Testing Associate (CSTA) qualification.

PA Consulting
Global Innovation & Technology Centre Back
Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
www: cybereducation.paconsulting.com

SYLLABUS

1. Introduction
- a. Motivations behind hacking
- b. The hacking scene
- c. Methodology

2. Networking Refresher
- a. Sniffing Traffic – Wireshark, Ettercap

3. Information Discovery
- a. Information Gathering – wget, metadata, pdfinfo and extract
- b. DNS – dig, zone transfers, DNSenum and Fierce

4. Target Scanning
- a. Host Discovery – Nmap and Netdiscover
- b. Port Scanning with Nmap – Connect, SYN and UDP scans, OS detection
- c. Banner Grabbing – Amap, Netcat, Nmap, Nmap scripts (NSE)

5. Vulnerability Assessment
- a. Nikto
- b. Nessus

6. Attacking Windows
- a. Windows Enumeration – (SNMP, IPC$)
- b. Enum4linux
- c. RID Cycling – Enum4linux, Cain
- d. Metasploit
- e. Client-side Exploits – Internet Explorer, Metasploit Auxiliary modules

7. Privilege Escalation – Windows
- a. Information Gathering with Meterpreter – Stuxnet exploit, Meterpreter scripts
- b. Privilege Escalation – Keylogging, Service Configuration
- c. Password Cracking – John The Ripper, Cain, Rainbow tables
- d. Brute-Force Password Attacks
- e. Attacks on Cached Domain Credentials
- f. Token Stealing – PsExec, Incognito, local admin to domain admin
- g. Pass the Hash

8. Attacking Linux
- a. Linux User Enumeration
- b. Linux Exploitation without Metasploit
- c. Online Password Cracking – Medusa
- d. User Defined Functions
- e. ARP Poisoning Man in the Middle – clear-text protocols, secured protocols

9. Privilege Escalation – Linux
- a. Exploiting sudo through File Permissions
- b. Exploiting SUID and Flawed Scripts – logic errors
- c. Further Shell Script Flaws – command injection, path exploits
- d. Privilege Escalation via NFS
- e. Cracking Linux Passwords

10. Pivoting the Connection
- a. Pivoting with Meterpreter
- b. Port Forwarding

11. Retaining Access
- a. Netcat as a Backdoor
- b. Dark Comet RAT – Metasploit Handlers, a full end-to-end attack

12. Covering Tracks
- a. Alternative Data Streams
- b. Dark Comet

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com