COURSE OUTLINE

ETHICAL HACKING
Certified Wireless Security Analyst (CWSA)

●●●○ **CORE-LEVEL COURSE** Cost: **£1,300.00** + VAT Duration: **2 days**

This two-day course is for people involved in a variety of wireless network-related roles. It is designed to give you the skills you need to develop a more secure infrastructure around critical data and applications, and defend systems from unauthorised wireless attacks.

"An essential course for those designing and configuring all aspects of wireless networking."
CWSA Delegate
New Vision Group Ltd

COURSE OVERVIEW

As wireless technologies become ever more pervasive, the need to consider the risks they present should form part of any information security policy. This course gives you the knowledge of how hackers bypass wireless security as well as an understanding of the principles of wireless cryptography. Once able to identify and exploit vulnerabilities, you will be introduced to a range of defensive countermeasures, allowing you to complete the final exercise of building a secure wireless network to protect information assets.

THE SKILLS YOU WILL LEARN

- Learn how hackers and auditors alike test wireless networks for vulnerabilities
- Discover the latest security standards and practices in WiFi
- Understand the threats to wireless networks, including rogue access points, denial of service (DoS) attacks and client-side (i.e. non Access Point) threats
- In-depth coverage of a comprehensive series of wireless security measures and their weaknesses, including WEP and WPA/WPA2 (i.e. TKIP/CCMP) and 802.1X authentication (although WEP is outdated, understanding its flaws helps to understand why the replacements are better as well as introducing principles that underpin other security protocols).
- Understand how enterprise WiFi networks need not rely on pre-shared keys

KEY BENEFITS

This course will give you:

- A thorough understanding of how hackers target wireless networks and how to protect wireless networks (and clients) from attack in the real world
- A safe classroom environment to experiment with the tools
- Delegates leave with knowledge they can apply outside the world of WiFi, such as how public key cryptography works
- The course culminates in a hands-on exercise to create a secure wireless network using digital certificates for authentication
- Valuable preparation for the CREST Registered Penetration Tester (CRT) examination

WHO SHOULD ATTEND

Anyone with responsibility for, or an interest in, the security of wireless networks and Wi-Fi enabled devices, including:

- IT managers
- Systems/network administrators
- IT security professionals
- Forensic/network investigators

PREREQUISITES

Basic understanding of TCP/IP networking:

- Are you familiar with the OSI model? Can you name a layer 2 and layer 3 protocol?
- Can you describe how a request reaches a web server through Ethernet, IP and TCP?

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

COURSE OUTLINE

ETHICAL HACKING
Certified Wireless Security Analyst (CWSA)

●●●○ **CORE-LEVEL COURSE** | **Cost: £1,300.00 + VAT** | Duration: **2 days**

- What function does ARP perform?
- How does a system know whether or not a gateway is required?

Basic 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 display network configuration information etc.?

If you are planning to do both the CSTA and CWSA courses, we recommend you take CSTA first.

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Wireless Security Analyst (CWSA) qualification.

SYLLABUS

1. WiFi Networks
a. Standards
b. Components
c. WiFi Station Modes
d. Channels
e. Architectures
f. Frames and Types

2. WiFi Threats
a. Monitor mode
b. Wardriving
c. Wardriving Stations
d. Eavesdropping
e. ARP poisoning
f. Denial of Service
g. Rogue Access Points
h. Rogue Stations
i. WiFi Connection Software

3. WiFi Security
a. SSID broadcast
b. MAC filtering
c. Stream ciphers
d. WEP and WEP flaws
e. Shared Key Authentication
f. Café Latte attack

4. 802.11I
a. TKIP
b. TKIP Key Management
c. 4-way handshake
d. Key mixing
e. TKIP attacks
f. Client-side dictionary attack
g. Block ciphers
h. CCMP
i. CCMP attacks
j. WiFi Protected Setup (WPS)

5. WiFi Enterprise Security
a. The trouble with pre-shared keys
b. EAP
c. 802.1X
d. RADIUS
e. EAP methods
f. Public key cryptography
g. Certificates
h. TLS weaknesses
i. PEAP weaknesses

6. Conclusions
a. Summary
b. Further WiFi defences

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

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