Tec Train Cyber Security

Course Details

Duration – 4 Days
09:00am till 17:00pm
Location – Crewe or Uxbridge

Course Format

The training will start with a recap of knowledge the candidates are expected to have in order to contextualise elements of the course. This will include a good balance of practical activity, covering theory and legal elements to ensure that the correct methodology for a penetration test is undertaken each time.

To maintain flexibility, the course is broken down into modules that can be moved around to take into account the potential for mixed abilities in the classroom.

Assessment

You will be assessed throughout the course through interactive activities and verbal feedback. Any areas for further development are discussed with the candidates at the earliest opportunity. On the assessment module, candidates will complete a practical scenario followed by the requirement to write a written report of findings. This will be scored and discussed with the candidate so that they are aware of their areas for further development.

The skills gained from undertaking the course should allow the candidate to sit an external certified exam.

The Tec-Train Ltd,
Cerco House, Southmere Court
Crewe, Cheshire, CW1 6GU

www.tec-train.co.uk 01270 212951
enquiries@tec-train.co.uk

Course Contents

Penetration Testing Methodology

- The purpose of a penetration test
- Scoping the test
- Authority to test (customer, suppliers)
- Compliance requirements (if any)

Legal framework

- Relevant legislation (these will be amended accordingly post Brexit)
  - Computer Misuse Act 1990
  - Communications Act 2003
  - General Data Protection Regulation 2016
  - Official Secrets Act 1989

Networking and enumeration fundamentals

- Network architecture types
- Common protocols and services
- Network fingerprinting
- Identification and exploitation of services

Exploitation

- Common vulnerabilities
- Bug bounties
- CVE
- Responsible disclosure

Cryptography

- Common cryptography methods
- Deprecated but often used cryptography methods

Wireless

- Wireless networking protocols
- Packet sniffing
- Packet injection
- Key cracking

Social Engineering

- Common social engineering / fraud attack vectors
- Reconnaissance
- Execution
- Education / Awareness

Website applications

- Common scripting languages
- OWASP Top 10
- APIs
- Assessment tools

Mobile applications

- Android, iOS environments
- Common vulnerabilities
- Security assessment basics

Reporting of findings

- Structuring a penetration test report
- Articulating technical findings in non-technical language
- Proposed remediation
- Scoring of risk against the CIA model

Continued Professional Development (CPD)

- Low to no cost options
- Recommended reading
- Premium options