CREST Practitioner Security Analyst

Learn via: **Classroom**

Duration: **5 Day**

https://bilginc.com/en/training/crest-practitioner-security-analyst-639-training/

Overview

QA are an approved CREST training provider. The CPSA course leads to the CREST Practitioner Security Analyst (CPSA) examination, which is an entry level qualification that tests a candidate's knowledge in assessing operating systems and common network services at a basic level below that; of the main CRT and CCT qualifications.

Delegates are provided with a Pearson Vue exam voucher for the CPSA examination as part of the course fee. The CPSA examination also includes an intermediate level of web application security testing and methods to identify common web application security vulnerabilities. The examination covers a common set of core skills and knowledge that assess the candidate's technical knowledge. The candidate must demonstrate that they are able to perform basic infrastructure and web application testing and interpret the results to locate security vulnerabilities. Success will confer the CREST Practitioner status to the individual. This qualification is a pre-requisite for the CREST Registered Penetration Tester (CRT) examination and comprises a multiple-choice examination. CRT is not currently available due to the recent syllabus change, we advise learners to seek the OffSec OSCP (PEN-200) class, which has equivalency with the CRT.

Target Audience

- Aspiring information security personnel who wish to be part of a Pen Test team
- System administrators who are responding to attacks
- Incident handlers who wish to expand their knowledge into Penetration Testing and Digital Forensics
- Corporations and Government departments who wish to raise and baseline skills across all security teams
- Law enforcement officers or detectives who want to expand their investigative skills
- Information security managers who would like to brush up on the latest techniques and processes in order to understand information security implications
- Anyone who is considering a career in Penetration Testing

Prerequisites

A good appreciation of the technical concepts is advised, Security Fundamentals is recommended.

Outline

Day 1

- Intro
- What is Cybersecurity
- Security Concepts
- Risk
- VA & Pen Testing
- Threat Modelling
- Law & Compliance
- Module Summary

Day 2

- Network Overview
- Networking Models
- Network Types & Topologies
- Networking Devices
- Network Addresses & Protocols
- Internet Protocol Suite
- Module Summary

Day 3

- Assessing Logical Ports
- Organisational Security

- Assessing Operating Systems
- Windows
- Module Summary

Day 4

- Application Exploits
- Web Server Exploits
- Web Browser Exploits
- Secure Application Design
- Secure Coding
- Auditing Applications
- Module Summary

Day 5

- Cryptography Application
- Identity and Access Management
- Cryptocurrency
- Module Summary