CREST Practitioner Security Analyst

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

Overview

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.

The CPSA examination (booked directly with CREST) 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 available as a separate course.

Target Audience

- Aspiring information security personnel who wish to be part of a PenTest 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 inorder to understand information security implications
- Anyone who is considering a career in Penetration Testing

Prerequisites

A good appreciation of the technical aspects of ICT. QAFCCS and or CISMP is recommmended.

Outline

MODULE 1 - Soft Skills and Assessment Management

- Engagement Lifecycle
- Law & Compliance
- Scoping
- Understanding Explaining and Managing Risk
- Record Keeping, Interim Reporting & Final Results

MODULE 2 - Core Technical Skills

- IP Protocols
- Network Architectures
- Network Mapping & Target Identification
- Interpreting Tool Output
- Filtering Avoidance Techniques
- OS Fingerprinting
- Application Fingerprinting and Evaluating
- Unknown Services
- Network Access Control Analysis
- Cryptography
- Applications of Cryptography
- File System Permissions
- Audit Techniques

MODULE 3 - Networking Equipment

- Registration Records
- Domain Name Server (DNS)
- Customer Web Site Analysis
- Google Hacking and Web Enumeration
- NNTP Newsgroups and Mailing Lists
- Information Leakage from Mail & News Headers

MODULE 4 - Management Protocols

- Network Traffic Analysis
- Networking Protocols
- IPSec
- VoIP
- Wireless
- Configuration Analysis
- Information Gathering & Open Source

MODULE 5 - Microsoft Windows Security Assessment

- Domain Reconnaissance
- User Enumeration
- Active Directory
- Windows Passwords
- Windows Vulnerabilities
- Windows Patch Management Strategies
- Desktop Lockdown
- Exchange
- Common Windows Applications

MODULE 6 - Unix Security Assessment

- User Enumeration
- Unix Vulnerabilities
- FTP
- Sendmail / SMTP
- Network File System (NFS)
- R* services X11
- RPC services
- SSH

MODULE 7 - Web Technologies

- Web Server Operation
- Web Servers & their Flaws
- Web Enterprise Architectures
- Web Protocols
- Web Mark-up Languages
- Web Programming Languages
- Web Application Servers
- Web APIs
- Web Sub- Components

MODULE 8 - Web Testing Methodologies

- Web Application Reconnaissance
- Threat Modelling and Attack Vectors
- Information Gathering from Web Mark-up
- Authentication Mechanisms
- Authorisation Mechanisms
- Input Validation
- Information Disclosure in Error Messages
- Use of Cross Site Scripting Attacks
- Use of Injection Attacks
- Session Handling
- Encryption

- Source Code Review

MODULE 9 - Databases

- Microsoft SQL Server
- Oracle RDBMS
- Web / App / Database Connectivity

MODULE 10 - Preparation for the CPSA and CRT exams

- Examination guidance
- Mock exam