Course: CREST CPSA Exam Preparation

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.

Audience Profile:

- Penetration Tester
- Ethical hackers
- Red Team members
- Vulnerability Tester
- Security Analyst
- Vulnerability Assessment Analyst
- Network Security Operations

Candidate Prerequisites:

Basic familiarity with Information Security.

Accreditation:

CREST Approved Training

Duration:

5 Days (40 Hours)

Exam Details:

Exam Code: CPSA (The exam is delivered at Pearson VUE test centres)
Type of questions: Multiple choice
Duration: 2 Hours and 30 minutes
Passing Score: 60%

Course Outline:

Module 1: Soft Skills and Assessment Management

Lessons:

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

Review Questions

Module 2: Core Technical Skills

Lessons:

- IP Protocols
- Network Architectures
- Network mapping and Target Identification
- Filtering Avoidance Techniques
- OS Fingerprinting
- Application Fingerprinting and Evaluating Unknown Services
- Cryptography
- Applications of Cryptography
- File System Permissions
- Audit Techniques

Review Questions

Module 3: Background Information Gathering and Open Source

Lessons:

- Registration Records
- Domain Name Server (DNS)
- Google Hacking and Web Enumeration
- Information Leakage from Mail Headers

Review Questions

Module 4: Networking Equipment

Lessons:

- Management Protocols
- Network Traffic Analysis
- Networking Protocols
- IPsec
- VoIP
- Wireless
- Configuration Analysis

Review Questions

Module 5: Microsoft Windows Security Assessment

Lessons:

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

Review Questions

Module 6: UNIX Security Assessment

Lessons:

- User Enumeration
- UNIX/Linux Vulnerabilities
- FTP
- RPC Services
- Sendmail/SMTP
- Network File System (NFS)
- R-Services
- SSH

Review Questions

Module 7: Web Technologies

Lessons:

- Web Server Operation & Web Servers and Their Flaws
- Web Enterprise Architectures
- Web Protocols
- Web Markup Languages
- Web Programming Languages
- Web Application Servers
- Web APIs
- Web Sub-Components

Review Questions

Module 8: Web-Testing Methodologies

Lessons:

- 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 (XSS)
- Use of Injection Attacks
- Session Handling
- Encryption
- Source Code Review

Review Questions

Module 9: Web Testing Techniques

Lessons:

- Web Site Structure Discovery
- SQL Injection
- Cross Site Scripting Attack
- Parameter Manipulation

Review Questions

Module 10: Databases

Lessons:

- Databases
- Microsoft SQL Server
- Oracle RDBMS
- MySQL

Review Questions