CREST

CREST. Representing the technical information security industry

Technical Committee and Assessors Panel

CREST Practitioner Security Technical Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	SYL_CPSA
Version Number	2.5
Status	Public Release

Contents

1. Introduction 3

2. Certification Examination Structure 3

3. Exam Format 3

4. Syllabus Structure 3

Appendix A: Soft Skills and Assessment Management 4

Appendix B: Core Technical Skills 5

Appendix C: Background Information Gathering and Open Source 7

Appendix D: Networking Equipment 8

Appendix E: Microsoft Windows Security Assessment 10

Appendix F: Unix Security Assessment 12

Appendix G: Web Technologies 14

Appendix H: Web Testing Methodologies 15

Appendix I: Web Testing Techniques 17

Appendix J: Databases 18

1. Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the CREST Practitioner Security Analyst (CPSA) examination.

The (CPSA) Crest Practitioner Security Analyst examination tests candidates' knowledge in assessing operating systems and common network services at a level below that of the CRT and main CCT qualifications.

Success will confer CREST Practitioner Security Analyst status to the individual.

2. Certification Examination Structure

The CPSA Examination has one component: a written paper. The written paper consists of a set of multiple choice questions.

The *Notes for Candidates (CPSA)* document for the Certification Examinations provides further information regarding the Certification Examinations in general.

3. Exam Format

The CPSA is a written multiple-choice examination.

4. Syllabus Structure

The syllabus is divided into ten knowledge groups (Appendices A to J below), each of which is subdivided into specific skill areas.

Appendix A: Soft Skills and Assessment Management

ID	Skill	Details
A1	Engagement Lifecycle	Benefits and utility of penetration testing to the client. Structure of penetration testing, including the relevant processes and procedures. Concepts of infrastructure testing and application testing, including black box and white box formats. Project closure and debrief.
A2	Law & Compliance	Knowledge of pertinent UK legal issues: Computer Misuse Act 1990 Human Rights Act 1998 Data Protection Act 1998 Police and Justice Act 2006 Impact of this legislation on penetration testing activities. Awareness of sector-specific regulatory issues.
A3	Scoping	Understanding client requirements. Scoping project to fulfil client requirements. Accurate timescale scoping. Resource planning.
A4	Understanding Explaining and Managing Risk	Knowledge of additional risks that penetration testing can present. Levels of risk relating to penetration testing, the usual outcomes of such risks materialising and how to mitigate the risks. Effective planning for potential DoS conditions.
A5	Record Keeping, Interim Reporting & Final Results	Understanding reporting requirements. Understanding the importance of accurate and structured record keeping during the engagement.

Appendix B: Core Technical Skills

ID	Skill	Details
B1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. Awareness that other IP protocols exist.
B2	Network Architectures	Varying network types that could be encountered during a penetration test: CAT 5 / Fibre 10/100/1000baseT Token ring Wireless (802.11) Security implications of shared media, switched media and VLANs.
B4	Network Mapping & Target Identification	Analysis of output from tools used to map the route between the engagement point and a number of targets. Network sweeping techniques to prioritise a target list and the potential for false negatives.
B5	Interpreting Tool Output	Interpreting output from port scanners, network sniffers and other network enumeration tools.
B6	Filtering Avoidance Techniques	The importance of egress and ingress filtering, including the risks associated with outbound connections.
B8	OS Fingerprinting	Remote operating system fingerprinting; active and passive techniques.
B9	Application Fingerprinting and Evaluating Unknown Services	Determining server types and network application versions from application banners. Evaluation of responsive but unknown network applications.
B10	Network Access Control Analysis	Reviewing firewall rule bases and network access control lists.

ID	Skill	Details
B11	Cryptography	Differences between encryption and encoding. Symmetric / asymmetric encryption Encryption algorithms: DES, 3DES, AES, RSA, RC4. Hashes: SHA1 and MD5 Message Integrity codes: HMAC
B12	Applications of Cryptography	SSL, IPsec, SSH, PGP Common wireless (802.11) encryption protocols: WEP, WPA, TKIP
B13	File System Permissions	File permission attributes within Unix and Windows file systems and their security implications. Analysing registry ACLs.
B14	Audit Techniques	Listing processes and their associated network sockets (if any). Assessing patch levels. Finding interesting files.

Appendix C: Background Information Gathering and Open Source

ID	Skill	Details
C1	Registration Records	Information contained within IP and domain registries (WHOIS).
C2	Domain Name Server (DNS)	DNS queries and responses DNS zone transfers Structure, interpretation, and analysis of DNS records: SOA MX TXT A NS PTR HINFO CNAME
C3	Customer Web Site Analysis	Analysis of information from a target web site, both from displayed content and from within the HTML source.
C4	Google Hacking and Web Enumeration	Effective use of search engines and other public data sources to gain information about a target.
C5	NNTP Newsgroups and Mailing Lists	Searching newsgroups or mailing lists for useful information about a target.
C6	Information Leakage from Mail & News Headers	Analysing news group and e-mail headers to identify internal system information.

Appendix D: Networking Equipment

ID	Skill	Details
D1	Management Protocols	Weaknesses in the protocols commonly used for the remote management of devices: Telnet Web based protocols SSH SNMP (covering network information enumeration and common attacks against Cisco configurations) TFTP Cisco Reverse Telnet NTP
D2	Network Traffic Analysis	Techniques for local network traffic analysis. Analysis of network traffic stored in PCAP files.
D3	Networking Protocols	Security issues relating to the networking protocols: ARP DHCP CDP HSRP VRRP VTP STP TACACS+
D4	IPSec	Enumeration and fingerprinting of devices running IPSec services.
D5	VoIP	Enumeration and fingerprinting of devices running VoIP services. Knowledge of the SIP protocol.
D6	Wireless	Enumeration and fingerprinting of devices running Wireless (802.11) services. Knowledge of various options for encryption and authentication, and the relative methods of each. WEP TKIP WPA/WPA2 EAP/LEAP/PEAP

ID	Skill	Details
D7	Configuration Analysis	Analysing configuration files from the following types of Cisco equipment: Routers Switches Interpreting the configuration of other manufacturers’ devices.

Appendix E: Microsoft Windows Security Assessment

ID	Skill	Details
E1	Domain Reconnaissance	Identifying domains/workgroups and domain membership within the target network. Identifying key servers within the target domains. Identifying and analysing internal browse lists. Identifying and analysing accessible SMB shares
E2	User Enumeration	Identifying user accounts on target systems and domains using NetBIOS, SNMP and LDAP.
E3	Active Directory	Active Directory Roles (Global Catalogue, Master Browser, FSMO) Reliance of AD on DNS and LDAP Group Policy (Local Security Policy)
E4	Windows Passwords	Password policies (complexity, lockout policies) Account Brute Forcing Hash Storage (merits of LANMAN, NTLMv1 / v2) Offline Password Analysis (rainbow tables / hash brute forcing)
E5	Windows Vulnerabilities	Knowledge of remote windows vulnerabilities, particularly those for which robust exploit code exists in the public domain. Knowledge of local windows privilege escalation vulnerabilities and techniques. Knowledge of common post exploitation activities: obtain password hashes, both from the local SAM and cached credentials obtaining locally stored clear-text passwords crack password hashes check patch levels derive list of missing security patches reversion to previous state
E6	Windows Patch Management Strategies	Knowledge of common windows patch management strategies: SMS SUS WSUS MBSA

ID	Skill	Details
E7	Desktop Lockdown	Knowledge and understanding of techniques to break out of a locked down Windows desktop / Citrix environment. Privilege escalation techniques
E8	Exchange	Knowledge of common attack vectors for Microsoft Exchange Server.
E9	Common Windows Applications	Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available.

Appendix F: Unix Security Assessment

ID	Skill	Details
F1	User enumeration	Discovery of valid usernames from network services commonly running by default: rusers rwho SMTP finger Understand how finger daemon derives the information that it returns, and hence how it can be abused.
F2	Unix vulnerabilities	Recent or commonly found Linux vulnerabilities, and in particular those for which there is exploit code in the public domain. Use of remote exploit code and local exploit code to gain root access to target host. Common post-exploitation activities: exfiltrate password hashes crack password hashes check patch levels derive list of missing security patches reversion to previous state
F3	FTP	FTP access control. Anonymous access to FTP servers. Risks of allowing write access to anonymous users.
F4	Sendmail / SMTP	Valid username discovery via EXPN and VRFY. Awareness of recent Sendmail vulnerabilities; ability to exploit them if possible. Mail relaying
F5	Network File System (NFS)	NFS security: host level (exports restricted to particular hosts) and file level (by UID and GID). Root squashing, nosuid and noexec options. File access through UID and GID manipulation.

ID	Skill	Details
F6	R* services	Berkeley r* service: access control (/etc/hosts.equiv and .rhosts) trust relationships Impact of poorly configured trust relationships.
F7	X11	X Windows security and configuration; host-based vs. user-based access control.
F8	RPC services	RPC service enumeration. Common RPC services. Recent or commonly found RPC service vulnerabilities.
F9	SSH	Identify the types and versions of SSH software in use. Securing SSH. Versions 1 and 2 of the SSH protocol. Authentication mechanisms within SSH.

Appendix G: Web Technologies

ID	Skill	Details
G1	Web Server Operation	How a web server functions in terms of the client/server architecture. Concepts of virtual hosting and web proxies.
G2	Web Servers & their Flaws	Common web servers and their fundamental differences and vulnerabilities associated with them: IIS Apache (and variants)
G3	Web Enterprise Architectures	Design of tiered architectures. The concepts of logical and physical separation. Differences between presentation, application, and database layers.
G4	Web Protocols	Web protocols: HTTP, HTTPS, SOAP. All HTTP web methods and response codes. HTTP Header Fields relating to security features.
G5	Web Mark-up Languages	Web mark-up languages: HTML and XML.
G6	Web Programming Languages	Common web programming languages: JSP, ASP, PHP, CGI based Perl and JavaScript.
G7	Web Application Servers	Vulnerabilities in common application frameworks, servers and technologies: .NET, J2EE, Coldfusion, Ruby on Rails and AJAX.
G8	Web APIs	Application interfaces: CGI, ISAPI filters and Apache modules**.**
G9	Web Sub-Components	Web architecture sub-components: Thin/Thick web clients, servlets and applets, Active X. Flash Application Testing. .NET Thick Clients. Java Applets. De-compilation of client-side code.

Appendix H: Web Testing Methodologies

ID	Skill	Details
H1	Web Application Reconnaissance	Benefits of performing application reconnaissance. Discovering the structure of web applications. Methods to identify the use of application components defined in G1 to G9.
H2	Threat Modelling and Attack Vectors	Simple threat modelling based on customer perception of risk. Relate functionality offered by the application to potential attack vectors.
H3	Information Gathering from Web Mark-up	Examples of the type of information available in web page source that may prove useful to an attacker: Hidden Form Fields Database Connection Strings Credentials Developer Comments Other included files Authenticated-only URLs
H4	Authentication Mechanisms	Common pitfalls associated with the design and implementation of application authentication mechanisms.
H5	Authorisation Mechanisms	Common pitfalls associated with the design and implementation of application authorisation mechanisms.
H6	Input Validation	The importance of input validation as part of a defensive coding strategy. How input validation can be implemented and the differences between white-listing, black-listing, and data sanitisation.
H8	Information Disclosure in Error Messages	How error messages may indicate or disclose useful information.
H9	Use of Cross Site Scripting Attacks	Potential implications of a cross site scripting vulnerability. Ways in which the technique can be used to benefit an attacker.

ID	Skill	Details
H10	Use of Injection Attacks	Potential implications of injection vulnerabilities: SQL injection LDAP injection Code injection XML injection Ways in which these techniques can be used to benefit an attacker.
H11	Session Handling	Common pitfalls associated with the design and implementation of session handling mechanisms.
H12	Encryption	Common techniques used for encrypting data in transit and data at rest, either on the client or server side. Identification and exploitation of Encoded values (e.g. Base64) and Identification and exploitation of Cryptographic values (e.g. MD5 hashes). Identification of common SSL vulnerabilities.
H13	Source Code Review	Common techniques for identifying and reviewing deficiencies in the areas of security.

Appendix I: Web Testing Techniques

ID	Skill	Details
I1	Web Site Structure Discovery	Spidering tools and their relevance in a web application test for discovering linked content. Forced browsing techniques to discover default or unlinked content. Identification of functionality within client-side code.
I2	Cross Site Scripting Attacks	Arbitrary JavaScript execution. Using Cross Site Scripting techniques to obtain sensitive information from other users. Phishing techniques.
I3	SQL Injection	Determine the existence of an SQL injection condition in a web application. Determine the existence of a blind SQL injection condition in a web application. Exploit SQL injection to enumerate the database and its structure. Exploit SQL injection to execute commands on the target server.
I4	Parameter Manipulation	Parameter manipulation techniques, particularly the use of client-side proxies.

Appendix J: Databases

ID	Skill	Details
J1	Microsoft SQL Server	Knowledge of common attack vectors for Microsoft SQL Server. Understanding of privilege escalation and attack techniques for a system compromised via database connections.
J2	Oracle RDBMS	Derivation of version and patch information from hosts running Oracle software. Default Oracle accounts.
J3	Web / App / Database Connectivity	Common databases (MS SQL server, Oracle, MySQL and Access) and the connection and authentication methods used by web applications.

CREST

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press / Public Relations: media@crest-approved.org

www.crest-approved.org