



CREST. Representing the technical information security industry

Technical Committee and Assessors Panel

CREST Certified Tester Technical Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	SYL_CCT_V2.0
Version Number	2.2
Status	Public Release

This document and any information therein are confidential property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Contents

1. Introduction.....	4
2. Certification Examination Structure	4
3. Syllabus Structure	4
Appendix A: Soft Skills and Assessment Management	5
Appendix B: Core Technical Skills.....	7
Appendix C: Background Information Gathering & Open Source	9
Appendix D: Networking Equipment	11
Appendix E: Microsoft Windows Security Assessment	13
Appendix F: Unix Security Assessment	15
Appendix G: Web Technologies	18
Appendix H: Web Testing Methodologies.....	21
Appendix I: Web Testing Techniques	24
Appendix J: Databases	27



1. Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Certification Examinations. There are two alternate Certification Examinations for the Crest Certified Tester (CCT) certification.

Crest Certified Web Application Tester (CCT)

The (CCT) Web Application Certification Examination tests candidates' knowledge and expertise in assessing web applications.

The Certification Examination covers a common set of core skills and knowledge; success will confer CREST Certified Tester status to the individual.

2. Certification Examination Structure

Crest Certified Tester (CCT)

The Certification Examination has two components: a written paper and a practical assessment. The written paper consists of one section: a set of multiple choice questions. The practical assessment tests candidates' hands-on penetration testing methodology and skills against reference networks, hosts and applications.

The *Notes for Candidates (CCT)* document for the Certification Examinations provides further information regarding the Certification Examinations in general and the skill areas that will be assessed within the practical components.

3. Syllabus Structure

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

For each skill area, CREST has indicated where and how the area will be assessed: in which component (Written Multiple Choice or Practical).

Within the tables, the following acronyms apply:

CCT APP Application Certification Examination

MC Written Multiple Choice

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



P Practical

Appendix A: Soft Skills and Assessment Management

ID	Skill	Details	How Examined
			CCT APP
A1	Engagement Lifecycle	<p>Benefits and utility of penetration testing to the client.</p> <p>Structure of penetration testing, including the relevant processes and procedures.</p> <p>Concepts of infrastructure testing and application testing, including black box and white box formats.</p> <p>Project closure and debrief</p>	MC
A2	Law & Compliance	<p>Knowledge of pertinent UK legal issues:</p> <p>Computer Misuse Act 1990 Human Rights Act 1998 Data Protection Act 1998 Police and Justice Act 2006</p> <p>Impact of this legislation on penetration testing activities.</p> <p>Awareness of sector-specific regulatory issues.</p>	MC
A3	Scoping	<p>Understanding client requirements.</p> <p>Scoping project to fulfil client requirements.</p> <p>Accurate timescale scoping.</p>	MC

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



		Resource planning.	
A4	Understanding Explaining and Managing Risk	<p>Knowledge of additional risks that penetration testing can present.</p> <p>Levels of risk relating to penetration testing, the usual outcomes of such risks materialising and how to mitigate the risks.</p> <p>Effective planning for potential DoS conditions.</p>	MC
A5	Record Keeping, Interim Reporting & Final Results	<p>Understanding reporting requirements.</p> <p>Understanding the importance of accurate and structured record keeping during the engagement.</p>	<p>MC</p> <p>P</p>

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



Appendix B: Core Technical Skills

ID	Skill	Details	How Examined
			CCT APP
B1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. Awareness that other IP protocols exist.	MC
B2	Network Architectures	Varying networks 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.	MC
B3	Network Routing	Network routing protocols RIP, OSPF, and IGRP/EIGRP.	MC
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.	MC P
B5	Interpreting Tool Output	Interpreting output from port scanners, network sniffers and other network enumeration tools.	MC
B6	Filtering Avoidance Techniques	The importance of egress and ingress filtering, including the risks associated with outbound connections.	MC

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



B7	Packet Crafting	Packet crafting to meet a particular requirement: Modifying source ports Spoofing IP addresses Manipulating TTL's Fragmentation Generating ICMP packets	MC
B8	OS Fingerprinting	Remote operating system fingerprinting; active and passive techniques.	MC
ID	Skill	Details	How Examined CCT APP
B9	Application Fingerprinting and Evaluating Unknown Services	Determining server types and network application versions from application banners. Evaluation of responsive but unknown network applications.	MC
B10	Network Access Control Analysis	Reviewing firewall rule bases and network access control lists.	MC
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	MC P
B12	Applications of Cryptography	SSL, IPsec, SSH, PGP Common wireless (802.11) encryption protocols: WEP, WPA, TKIP	MC

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



B13	File System Permissions	File permission attributes within Unix and Windows file systems and their security implications. Analysing registry ACLs.	MC
B14	Audit Techniques	Listing processes and their associated network sockets (if any). Assessing patch levels. Finding interesting files.	MC

Appendix C: Background Information Gathering & Open Source

ID	Skill	Details	How Examined
			CCT APP
C1	Registration Records	Information contained within IP and domain registries (WHOIS).	MC
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	MC

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



		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.	MC P
C4	Google Hacking and Web Enumeration	Effective use of search engines and other public data sources to gain information about a target.	MC
C5	NNTP Newsgroups and Mailing Lists	Searching newsgroups or mailing lists for useful information about a target.	MC
C6	Information Leakage from Mail & News Headers	Analysing news group and e-mail headers to identify internal system information.	MC

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



Appendix D: Networking Equipment

ID	Skill	Details	How Examined
			CCT APP
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	MC
D2	Network Traffic Analysis	Techniques for local network traffic analysis. Analysis of network traffic stored in PCAP files.	MC
D3	Networking Protocols	Security issues relating to the networking protocols: ARP DHCP CDP HSRP VRRP VTP STP TACACS+	MC
D4	IPSec	Enumeration and fingerprinting of devices running IPSec services.	MC
D5	VoIP	Enumeration and fingerprinting of devices running VoIP services. Knowledge of the SIP protocol.	MC
D6	Wireless	Enumeration and fingerprinting of devices running Wireless (802.11) services.	MC

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



		Knowledge of various options for encryption and authentication, and the relative methods of each. WEP TKIP WPA/WPA2 EAP/LEAP/PEAP	
ID	Skill	Details	How Examined
			CCT APP
D7	Configuration Analysis	Analysing configuration files from the following types of Cisco equipment: Routers Switches Interpreting the configuration of other manufacturers' devices.	MC

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



Appendix E: Microsoft Windows Security Assessment

ID	Skill	Details	How Examined
			CCT APP
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	MC
E2	User Enumeration	Identifying user accounts on target systems and domains using NetBIOS, SNMP and LDAP.	MC
E3	Active Directory	Active Directory Roles (Global Catalogue, Master Browser, FSMO) Reliance of AD on DNS and LDAP Group Policy (Local Security Policy)	MC
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)	MC P

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



ID	Skill	Details	How Examined
			CCT APP
E5	Windows Vulnerabilities	<p>Knowledge of remote windows vulnerabilities, particularly those for which robust exploit code exists in the public domain.</p> <p>Knowledge of local windows privilege escalation vulnerabilities and techniques.</p> <p>Knowledge of common post exploitation activities:</p> <ul style="list-style-type: none"> 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 	MC P
E6	Windows Patch Management Strategies	<p>Knowledge of common windows patch management strategies:</p> <ul style="list-style-type: none"> SMS SUS WSUS MBSA 	MC
E7	Desktop Lockdown	<p>Knowledge and understanding of techniques to break out of a locked down Windows desktop / Citrix environment.</p> <p>Privilege escalation techniques.</p>	MC
E8	Exchange	<p>Knowledge of common attack vectors for Microsoft Exchange Server.</p>	MC
E9	Common Windows Applications	<p>Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available.</p>	MC

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



Appendix F: Unix Security Assessment

ID	Skill	Details	How Examined
			CCT APP
F1	User enumeration	<p>Discovery of valid usernames from network services commonly running by default:</p> <ul style="list-style-type: none"> rusers rwho SMTP finger <p>Understand how finger daemon derives the information that it returns, and hence how it can be abused.</p>	MC
F2	Unix vulnerabilities	<p>Recent or commonly-found Solaris vulnerabilities, and in particular those for which there is exploit code in the public domain.</p> <p>Recent or commonly-found Linux vulnerabilities, and in particular those for which there is exploit code in the public domain.</p> <p>Use of remote exploit code and local exploit code to gain root access to target host</p> <p>Common post-exploitation activities:</p> <ul style="list-style-type: none"> exfiltrate password hashes crack password hashes check patch levels derive list of missing security patches reversion to previous state 	MC
F3	FTP	<p>FTP access control</p> <p>Anonymous access to FTP servers</p> <p>Risks of allowing write access to anonymous users.</p>	MC

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



F4	Sendmail / SMTP	Valid username discovery via EXPN and VRFY Awareness of recent Sendmail vulnerabilities; ability to exploit them if possible Mail relaying	MC
-----------	-----------------	---	----

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



ID	Skill	Details	How Examined
			CCT APP
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.	MC
F6	R* services	Berkeley r* service: access control (/etc/hosts.equiv and .rhosts) trust relationships Impact of poorly-configured trust relationships.	MC
F7	X11	X Windows security and configuration; host-based vs. user-based access control.	MC
F8	RPC services	RPC service enumeration Common RPC services Recent or commonly-found RPC service vulnerabilities.	MC
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	MC

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



Appendix G: Web Technologies

ID	Skill	Details	How Examined
			CCT APP
G1	Web Server Operation	How a web server functions in terms of the client/server architecture. Concepts of virtual hosting and web proxies.	MC
G2	Web Servers & their Flaws	Common web servers and their fundamental differences and vulnerabilities associated with them: IIS Apache (and variants)	MC P
G3	Web Enterprise Architectures	Design of tiered architectures. The concepts of logical and physical separation. Differences between presentation, application and database layers.	MC
G4	Web Protocols	Web protocols: HTTP, HTTPS, SOAP. All HTTP web methods and response codes. HTTP Header Fields relating to security features	MC P
G5	Web Mark-up Languages	Web mark-up languages: HTML and XML.	MC
G6	Web Programming Languages	Common web programming languages: JSP, ASP, PHP, CGI based Perl and JavaScript.	MC

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



G7	Web Application Servers	Vulnerabilities in common application frameworks, servers and technologies: .NET, J2EE, Coldfusion, Ruby on Rails and AJAX.	MC P
G8	Web APIs	Application interfaces: CGI, ISAPI filters and Apache modules.	MC P

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



ID	Skill	Details	How Examined
			CCT APP
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 Decompilation of client-side code	MC P

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



Appendix H: Web Testing Methodologies

ID	Skill	Details	How Examined
			CCT APP
H1	Web Application Reconnaissance	<p>Benefits of performing application reconnaissance.</p> <p>Discovering the structure of web applications.</p> <p>Methods to identify the use of application components defined in G1 to G9.</p>	MC
H2	Threat Modelling and Attack Vectors	<p>Simple threat modelling based on customer perception of risk.</p> <p>Relate functionality offered by the application to potential attack vectors.</p>	MC
H3	Information Gathering from Web Mark-up	<p>Examples of the type of information available in web page source that may prove useful to an attacker:</p> <ul style="list-style-type: none"> Hidden Form Fields Database Connection Strings Credentials Developer Comments Other included files Authenticated-only URLs 	MC P
H4	Authentication Mechanisms	Common pitfalls associated with the design and implementation of application authentication mechanisms.	MC P
H5	Authorisation Mechanisms	Common pitfalls associated with the design and implementation of application authorisation mechanisms.	MC P
H6	Input Validation	The importance of input validation as part of a defensive coding strategy.	MC P

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



		How input validation can be implemented and the differences between white listing, black listing and data sanitisation.	
H7	Application Fuzzing	<p>Fuzzing and its relevance within web-app penetration testing.</p> <p>The use of fuzz strings and their potential effects.</p> <p>Potential dangers of fuzzing web applications.</p>	MC P
ID	Skill	Details	How Examined
			CCT APP
H8	Information Disclosure in Error Messages	How error messages may indicate or disclose useful information.	MC
H9	Use of Cross Site Scripting Attacks	<p>Potential implications of a cross site scripting vulnerability.</p> <p>Ways in which the technique can be used to benefit an attacker.</p>	MC P
H10	Use of Injection Attacks	<p>Potential implications of injection vulnerabilities:</p> <p>SQL injection LDAP injection Code injection XML injection</p> <p>Ways in which these techniques can be used to benefit an attacker.</p>	MC P
H11	Session Handling	Common pitfalls associated with the design and implementation of session handling mechanisms.	MC P

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



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	MC P
H13	Source Code Review	Common techniques for identifying and reviewing deficiencies in the areas of security.	MC P

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



Appendix I: Web Testing Techniques

ID	Skill	Details	How Examined
			CCT APP
I1	Web Site Structure Discovery	<p>Spidering tools and their relevance in a web application test for discovering linked content.</p> <p>Forced browsing techniques to discover default or unlinked content.</p> <ul style="list-style-type: none"> •Identification of functionality within client-side code 	P
I2	Cross Site Scripting Attacks	<p>Arbitrary JavaScript execution.</p> <p>Using Cross Site Scripting techniques to obtain sensitive information from other users.</p> <p>Phishing techniques.</p>	P
I3	SQL Injection	<p>Determine the existence of an SQL injection condition in a web application.</p> <p>Determine the existence of a blind SQL injection condition in a web application.</p> <p>Exploit SQL injection to enumerate the database and its structure.</p> <p>Exploit SQL injection to execute commands on the target server.</p>	P
I4	Session ID Attacks	<p>Investigate session handling within a web application.</p> <p>Harvest and analyse a number of session identifiers for weaknesses.</p>	P
I5	Fuzzing	The concept of fuzzing within a web application testing methodology.	P

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



		Common fuzzing tools.	
16	Parameter Manipulation	Parameter manipulation techniques, particularly the use of client side proxies.	P

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



ID	Skill	Details	How Examined
			CCT APP
I7	Data Confidentiality & Integrity	Identifying weak (or missing) encryption. Identifying insecure SSL configurations. Identify insecure use of encoding techniques	P
I8	Directory Traversal	Identifying directory traversal vulnerabilities within applications.	P
I9	File Uploads	Identifying common vulnerabilities with file upload capabilities within applications.	P
I10	Code Injection	Investigate and exploitation of code injection vulnerabilities within web applications	P
I11	CRLF Attacks	Assessment of web applications for CRLF vulnerabilities	P
I12	Application Logic Flaws	Assessing the logic flow within an application and the potential for subverting the logic.	P

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



Appendix J: Databases

ID	Skill	Details	How Examined
			CCT APP
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.	MC P
J2	Oracle RDBMS	Derivation of version and patch information from hosts running Oracle software. Default Oracle accounts.	MC P
J3	Web / App / Database Connectivity	Common databases (MS SQL server, Oracle, MySQL and Access) and the connection and authentication methods used by web applications.	MC P

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