# CREST CPSA

## CREST Practitioner Security Analyst Certification Questions & Answers

Exam Summary – Syllabus –Questions

**CPSA**

**[CREST Practitioner Security Analyst (CPSA)]**

**120 Questions Exam – 60% Cut Score – Duration of 120 minutes**

## Table of Contents:

# Know Your CPSA Certification Well:

The CPSA is best suitable for candidates who want to gain knowledge in the CREST Penetration Testing. Before you start your CPSA preparation you may struggle to get all the crucial Practitioner Security Analyst materials like CPSA syllabus, sample questions, study guide.

But don't worry the CPSA PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the CPSA syllabus?
- How many questions are there in the CPSA exam?
- Which Practice test would help me to pass the CPSA exam at the first attempt?

Passing the CPSA exam makes you CREST Practitioner Security Analyst (CPSA). Having the Practitioner Security Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

# CREST CPSA Practitioner Security Analyst Certification Details:

| | |
|---|---|
| Exam Name | CREST Practitioner Security Analyst (CPSA) |
| Exam Code | CPSA |
| Exam Price | $400 (USD) |
| Duration | 120 mins |
| Number of Questions | 120 |
| Passing Score | 60% |
| Books / Training | Cyberskills Training<br>ICSI – CREST Approved Training Provider<br>PGI Cyber Academy – CREST Approved Training Provider<br>QA – CREST Approved Training Provider |
| Schedule Exam | Pearson VUE |
| Sample Questions | CREST Practitioner Security Analyst Sample Questions |
| Practice Exam | **CREST CPSA Certification Practice Exam** |

# CPSA Syllabus:

| Topic | Details |
|---|---|
| Soft Skills and Assessment Management | - Engagement Lifecycle<br>• Benefits and utility of penetration testing to the client.<br>• Structure of penetration testing, including the relevant processes and procedures.<br>• Concepts of infrastructure testing and application testing, including black box and white box formats.<br>• Project closure and debrief.<br>- Law & Compliance<br>• Knowledge of pertinent UK legal issues:<br>- Computer Misuse Act 1990<br>- Human Rights Act 1998<br>- Data Protection Act 1998<br>- Police and Justice Act 2006<br>• Impact of this legislation on penetration testing activities.<br>• Awareness of sector-specific regulatory issues.<br>- Scoping<br>• Understanding client requirements.<br>• Scoping project to fulfil client requirements.<br>• Accurate timescale scoping.<br>• Resource planning.<br>- Understanding Explaining and Managing Risk<br>• Knowledge of additional risks that penetration testing can present.<br>• Levels of risk relating to penetration testing, the usual outcomes of Such risks materialising and how to mitigate the risks.<br>• Effective planning for potential DoS conditions.<br>- Record Keeping, Interim Reporting & Final Results<br>• Understanding reporting requirements.<br>• Understanding the importance of accurate and structured record keeping during the engagement. |
| Core Technical Skills | - IP Protocols<br>• IP protocols: IPv4 and IPv6, TCP, UDP and ICMP.<br>• Awareness that other IP protocols exist.<br>- Network Architectures<br>• Varying network types that could be encountered during a penetration test:<br>- CAT 5 / Fibre<br>- 10/100/1000baseT<br>- Token ring<br>- Wireless (802.11)<br>• Security implications of shared media, switched media and VLANs.<br>- Network Mapping & Target Identification<br>• Analysis of output from tools used to map the route between the engagement point and a number of targets. |

| Topic | Details |
|---|---|
|  | • Network sweeping techniques to prioritise a target list and the potential for false negatives.<br>- Interpreting Tool Output<br>• Interpreting output from port scanners, network sniffers and other network enumeration tools.<br>- Filtering Avoidance Techniques<br>• The importance of egress and ingress filtering, including the risks associated with outbound connections.<br>- OS Fingerprinting<br>• Remote operating system fingerprinting; active and passive techniques.<br>- Application Fingerprinting and Evaluating Unknown Services<br>• Determining server types and network application versions from application banners.<br>• Evaluation of responsive but unknown network applications.<br>- Network Access Control Analysis<br>• Reviewing firewall rule bases and network access control lists.<br>- Cryptography<br>• Differences between encryption and encoding.<br>• Symmetric / asymmetric encryption<br>• Encryption algorithms: DES, 3DES, AES, RSA, RC4.<br>• Hashes: SHA1 and MD5<br>• Message Integrity codes: HMAC<br>- Applications of Cryptography<br>• SSL, IPsec, SSH, PGP<br>• Common wireless (802.11) encryption protocols: WEP, WPA, TKIP<br>- File System Permissions<br>• File permission attributes within Unix and Windows file systems and their security implications.<br>• Analysing registry ACLs.<br>- Audit Techniques<br>• Listing processes and their associated network sockets (if any).<br>• Assessing patch levels.<br>• Finding interesting files. |
| Background Information Gathering and Open Source | - Registration Records<br>• Information contained within IP and domain registries (WHOIS).<br>- Domain Name Server (DNS)<br>• DNS queries and responses<br>• DNS zone transfers<br>• Structure, interpretation, and analysis of DNS records:<br>- SOA<br>- MX<br>- TXT<br>- A |

| Topic | Details |
|---|---|
| | - NS<br>- PTR<br>- HINFO<br>- CNAME<br>- Customer Web Site Analysis<br>• Analysis of information from a target web site, both from displayed content and from within the HTML source.<br>- Google Hacking and Web Enumeration<br>• Effective use of search engines and other public data sources to gain information about a target.<br>- NNTP Newsgroups and Mailing Lists<br>• Searching newsgroups or mailing lists for useful information about a target.<br>- Information Leakage from Mail & News Headers<br>• Analysing news group and e-mail headers to identify internal system information. |
| Networking Equipment | - Management Protocols<br>• Weaknesses in the protocols commonly used for the remote management of devices:<br>- Telnet<br>- Web based protocols<br>- SSH<br>- SNMP (covering network information enumeration and common attacks against Cisco configurations)<br>- TFTP<br>- Cisco Reverse Telnet<br>- NTP<br>- Network Traffic Analysis<br>• Techniques for local network traffic analysis.<br>• Analysis of network traffic stored in PCAP files.<br>- Networking Protocols<br>• Security issues relating to the networking protocols:<br>- ARP<br>- DHCP<br>- CDP<br>- HSRP<br>- VRRP<br>- VTP<br>- STP<br>- TACACS+<br>- IPSec<br>• Enumeration and fingerprinting of devices running IPSec services.<br>- VoIP<br>• Enumeration and fingerprinting of devices running VoIP services.<br>• Knowledge of the SIP protocol.<br>- Wireless |

| Topic | Details |
|---|---|
|  | • Enumeration and fingerprinting of devices running Wireless (802.11) services.<br>• Knowledge of various options for encryption and authentication, and the relative methods of each.<br>• WEP<br>• TKIP<br>• WPA/WPA2<br>• EAP/LEAP/PEAP<br>- Configuration Analysis<br>• Analysing configuration files from the following types of Cisco equipment:<br>- Routers<br>- Switches<br>• Interpreting the configuration of other manufacturers' devices. |
| Microsoft Windows Security Assessment | - Domain Reconnaissance<br>• Identifying domains/workgroups and domain membership within the target network.<br>• Identifying key servers within the target domains.<br>• Identifying and analysing internal browse lists.<br>• Identifying and analysing accessible SMB shares<br>- User Enumeration<br>• Identifying user accounts on target systems and domains using NetBIOS, SNMP and LDAP<br>- Active Directory<br>• Active Directory Roles (Global Catalogue, Master Browser, FSMO)<br>• Reliance of AD on DNS and LDAP<br>• Group Policy (Local Security Policy)<br>- Windows Passwords<br>• Password policies (complexity, lockout policies)<br>• Account Brute Forcing<br>• Hash Storage (merits of LANMAN, NTLMv1 / v2)<br>• Offline Password Analysis (rainbow tables / hash brute forcing)<br>- Windows Vulnerabilities<br>• Knowledge of remote windows vulnerabilities, particularly those for which robust exploit code exists in the public domain.<br>• Knowledge of local windows privilege escalation vulnerabilities and techniques.<br>• Knowledge of common post exploitation activities:<br>- obtain password hashes, both from the local SAM and cached credentials<br>- obtaining locally stored clear-text passwords<br>- crack password hashes<br>- check patch levels<br>- derive list of missing security patches<br>- reversion to previous state |

| Topic | Details |
|---|---|
|  | - Windows Patch Management Strategies<br>• Knowledge of common windows patch management strategies:<br>- SMS<br>- SUS<br>- WSUS<br>- MBSA<br>- Desktop Lockdown<br>• Knowledge and understanding of techniques to break out of a locked down Windows desktop / Citrix environment.<br>• Privilege escalation techniques<br>- Exchange<br>• Knowledge of common attack vectors for Microsoft Exchange Server.<br>- Common Windows Applications<br>• Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available. |
| Unix Security Assessment | - User enumeration<br>• Discovery of valid usernames from network services commonly running by default:<br>- rusers<br>- rwho<br>- SMTP<br>- finger<br>• Understand how finger daemon derives the information that it returns, and hence how it can be abused.<br>- Unix vulnerabilities<br>• Recent or commonly found Linux vulnerabilities, and in particular those for which there is exploit code in the public domain.<br>• Use of remote exploit code and local exploit code to gain root access to target host.<br>• Common post-exploitation activities:<br>- exfiltrate password hashes<br>- crack password hashes<br>- check patch levels<br>- derive list of missing security patches<br>- reversion to previous stat<br>- FTP<br>• FTP access control.<br>• Anonymous access to FTP servers.<br>• Risks of allowing write access to anonymous users.<br>- Sendmail / SMTP<br>• Valid username discovery via EXPN and VRFY.<br>• Awareness of recent Sendmail vulnerabilities; ability to exploit them if possible.<br>• Mail relaying<br>- Network File System (NFS) |

| Topic | Details |
|---|---|
| | • NFS security: host level (exports restricted to particular hosts) and file level (by UID and GID).<br>• Root squashing, nosuid and noexec options.<br>• File access through UID and GID manipulation.<br>- R* services<br>• Berkeley r* service:<br>- access control (/etc/hosts.equiv and .rhosts)<br>- trust relationships<br>• Impact of poorly configured trust relationships.<br>- X11<br>• X Windows security and configuration; host-based vs. user-based access control.<br>- RPC services<br>• RPC service enumeration.<br>• Common RPC services.<br>• Recent or commonly found RPC service vulnerabilities.<br>- SSH<br>• Identify the types and versions of SSH software in use.<br>• Securing SSH.<br>• Versions 1 and 2 of the SSH protocol.<br>• Authentication mechanisms within SSH. |
| Web Technologies | - Web Server Operation<br>• How a web server functions in terms of the client/server architecture.<br>• Concepts of virtual hosting and web proxies.<br>- Web Servers & their Flaws<br>• Common web servers and their fundamental differences and vulnerabilities associated with them:<br>- IIS<br>- Apache (and variants)<br>- Web Enterprise Architectures<br>• Design of tiered architectures.<br>• The concepts of logical and physical separation.<br>• Differences between presentation, application, and database layers.<br>- Web Protocols<br>• Web protocols: HTTP, HTTPS, SOAP.<br>• All HTTP web methods and response codes.<br>• HTTP Header Fields relating to security features.<br>- Web Mark-up Languages<br>• Web mark-up languages: HTML and XML.<br>- Web Programming Languages<br>• Common web programming languages: JSP, ASP, PHP, CGI based Perl and JavaScript.<br>- Web Application Servers<br>• Vulnerabilities in common application frameworks, servers and technologies: .NET, J2EE, Coldfusion, Ruby on Rails and AJAX.<br>- Web APIs |

| Topic | Details |
|---|---|
| | - Application interfaces: CGI, ISAPI filters and Apache modules.<br>- Web SubComponents<br>- Web architecture sub-components: Thin/Thick web clients, servlets and applets, Active X.<br>- Flash Application Testing.<br>- .NET Thick Clients.<br>- Java Applets.<br>- De-compilation of client-side code. |
| Web Testing Methodologies | - Web Application Reconnaissance<br>- Benefits of performing application reconnaissance.<br>- Discovering the structure of web applications.<br>- Methods to identify the use of application components defined in G1 to G9.<br>- Threat Modelling and Attack Vectors<br>- Simple threat modelling based on customer perception of risk.<br>- Relate functionality offered by the application to potential attack vectors.<br>- Information Gathering from Web Mark-up<br>- Examples of the type of information available in web page source that may prove useful to an attacker:<br>- Hidden Form Fields<br>- Database Connection Strings<br>- Credentials<br>- Developer Comments<br>- Other included files<br>- Authenticated-only URLs<br>- Authentication Mechanisms<br>- Common pitfalls associated with the design and implementation of application authentication mechanisms.<br>- Authorisation Mechanisms<br>- Common pitfalls associated with the design and implementation of application authorisation mechanisms.<br>- Input Validation<br>- The importance of input validation as part of a defensive coding strategy.<br>- How input validation can be implemented and the differences between white-listing, black-listing, and data sanitisation.<br>- Information Disclosure in Error Messages<br>- How error messages may indicate or disclose useful information.<br>- Use of Cross Site Scripting Attacks<br>- Potential implications of a cross site scripting vulnerability.<br>- Ways in which the technique can be used to benefit an attacker.<br>- Use of Injection Attacks |

| Topic | Details |
|---|---|
| | • Potential implications of injection vulnerabilities:<br>- SQL injection<br>- LDAP injection<br>- Code injection<br>- XML injection<br>• Ways in which these techniques can be used to benefit an attacker.<br>- Session Handling<br>• Common pitfalls associated with the design and implementation of session handling mechanisms.<br>- Encryption<br>• Common techniques used for encrypting data in transit and data at rest, either on the client or server side.<br>• Identification and exploitation of Encoded values (e.g. Base64) and Identification and exploitation of Cryptographic values (e.g. MD5 hashes).<br>• Identification of common SSL vulnerabilities.<br>- Source Code Review<br>• Common techniques for identifying and reviewing deficiencies in the areas of security. |
| Web Testing Techniques | - Web Site Structure Discovery<br>• Spidering tools and their relevance in a web application test for discovering linked content.<br>• Forced browsing techniques to discover default or unlinked content.<br>• Identification of functionality within client-side code.<br>- Cross Site Scripting Attacks<br>• Arbitrary JavaScript execution.<br>• Using Cross Site Scripting techniques to obtain sensitive information from other users.<br>• Phishing techniques.<br>- SQL Injection<br>• Determine the existence of an SQL injection condition in a web application.<br>• Determine the existence of a blind SQL injection condition in a web application.<br>• Exploit SQL injection to enumerate the database and its structure.<br>• Exploit SQL injection to execute commands on the target server.<br>- Parameter Manipulation<br>• Parameter manipulation techniques, particularly the use of client-side proxies. |
| Databases | - Microsoft SQL Server<br>• Knowledge of common attack vectors for Microsoft SQL Server.<br>• Understanding of privilege escalation and attack techniques for a system compromised via database connections. |

| Topic | Details |
|---|---|
| | - Oracle RDBMS<br>• Derivation of version and patch information from hosts running Oracle software.<br>• Default Oracle accounts.<br>- Web / App / Database Connectivit<br>• Common databases (MS SQL server, Oracle, MySQL and Access) and the connection and authentication methods used by web applications. |

# CREST CPSA Sample Questions:

## Question: 1

**Which file, when misconfigured, can allow passwordless login using RSH or RLOGIN?**

a) /etc/shadow
b) /etc/hosts.deny
c) /etc/passwd
d) .rhosts

**Answer: d**

## Question: 2

**In which part of a web application is DOM-based XSS typically executed?**

a) Within client-side JavaScript execution
b) In the HTML meta tags
c) In the server-side script
d) Inside CSS stylesheets

**Answer: a**

## Question: 3

**What is the purpose of the DBMS_METADATA.GET_DDL function in Oracle?**

a) Deletes user accounts from the database
b) Dumps full contents of a database table
c) Retrieves the DDL (schema) for database objects
d) Encrypts stored procedures

**Answer: c**

Question: 4

**You review an Nmap scan output and observe port 80/tcp is open with a service name "http-proxy." What does this imply?**

a) The web server is using port forwarding
b) A proxy service (such as Squid) is running on that port
c) The port is misconfigured and should be closed
d) SSL encryption is enforced on that port

**Answer: b**

Question: 5

**What is a key security consideration in a three-tier web architecture (presentation, application, and database layers)?**

a) Only the presentation layer requires access control
b) All tiers should use the same credentials
c) The application tier should validate all input before passing to the database
d) SSL is only necessary between users and the database

**Answer: c**

Question: 6

**Which of the following fields in an IPv4 header is used for packet fragmentation and reassembly?**

a) Header Checksum
b) Time to Live (TTL)
c) Protocol
d) Identification

**Answer: d**

Question: 7

**What HTTP response header can help mitigate XSS by instructing the browser not to execute scripts from unauthorized origins?**

a) Content-Type
b) X-XSS-Protection
c) Content-Security-Policy (CSP)
d) Referrer-Policy

**Answer: c**

## Question: 8

**Why is enabling the xp_cmdshell stored procedure a critical security concern in SQL Server?**

a) It allows command execution on the operating system level
b) It disables SQL logging
c) It grants SA privileges to all users
d) It leaks encryption keys from the master database

**Answer: a**

## Question: 9

**During traffic analysis, which layer of the OSI model would reveal source and destination MAC addresses?**

a) Layer 3 – Network
b) Layer 5 – Session
c) Layer 2 – Data Link
d) Layer 7 – Application

**Answer: c**

## Question: 10

**Which of the following techniques is most effective for discovering unlinked web content?**

a) DNS zone transfer
b) Directory brute-forcing with a wordlist
c) Traceroute mapping
d) SSL certificate inspection

**Answer: b**

# Study Guide to Crack CREST Practitioner Security Analyst CPSA Exam:

- Getting details of the CPSA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CPSA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CREST provided training for CPSA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CPSA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CPSA practice tests is must. Continuous practice will make you an expert in all syllabus areas.