



## Assessors Panel

# CREST Certification Examinations Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	AP_1207-CN01
Version Number	1.0
Status	Public Release
Issue Date	4 December 2007
Review Date	By 4 November 2008

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.



## Table of Contents

1	Introduction .....	4
1.1	Examination .....	4
1.2	Confidentiality .....	4
2	Examination Details.....	5
2.1	Written Component.....	5
2.1.1	Format .....	5
2.1.2	Timings.....	5
2.1.3	Open Book /Closed Book.....	5
2.2	Practical Component .....	5
2.2.1	Format .....	5
2.2.2	Timings.....	5
2.2.3	Integrity Protection.....	5
2.2.4	Infrastructure Assessment Details.....	6
2.2.5	Web Application Assessment Details.....	6
2.3	Invigilation.....	6
3	Marking Scheme / Pass Mark.....	6
4	Examination Logistics.....	6
4.1	Location .....	6
4.2	Timing.....	6
4.3	Communication of Results .....	6
4.4	Testing Platform Options .....	6
4.4.1	Introduction.....	6
4.4.2	Option 1: Use own laptop testing platform (recommended).....	6
4.4.3	Option 2: Use own VMware images .....	6
4.4.4	Option 3: Use CREST's VMware images .....	6
5	Example questions (written component).....	6
5.1	Multiple choice .....	6
5.1.1	Question .....	6
5.1.2	Answer .....	6
5.1.3	Marking scheme .....	6
5.2	Long form .....	6
5.2.1	Question .....	6
5.2.2	Model answer .....	6



## Version History

Version	Date	Authors	Status
1.0	4 December 2007	Technical Committee and Assessors Panel	Public Release

## Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board



# 1 Introduction

## 1.1 Examination

The CREST Certification Examination has two components: a written component and a practical component. Components will be sat consecutively, with an hour break for lunch, and the overall examination will last a day.

There are two parallel tracks of CREST Certification Examination:

- The Infrastructure Certification Examination, which assesses a candidate's capabilities in the field of general infrastructure and operating system security assessments; and
- The Web Application Certification Examination, which assess a candidate's capabilities in the field of web application security assessments.

Candidates can only sit one examination track at a time.

Success at the Certification Examination will confer upon candidates the status of either:

- CREST Consultant (Infrastructure), or
- CREST Consultant (Web Applications)

For both tracks, the CREST Certification qualification is valid for three (3) years.

## 1.2 Confidentiality

CREST takes the confidentiality of the Certification Examination very seriously. The retention or dissemination of data relating to the CREST Certification Examination (other than what is contained in the Notes for Candidates and Technical Syllabus documentation that is available from the CREST web site <http://www.crest-approved.org/>) is not permitted: along with their booking forms, candidates must also send a signed Non-Disclosure Agreement to this effect.



## 2 Examination Details

### 2.1 Written Component

#### 2.1.1 Format

The written component of both tracks of the CREST Certification Examination will comprise ninety (90) multiple choice questions, all of which the candidate must complete. In addition the candidate will be presented with five (5) longer form questions, of which the candidate must choose and complete three (3).

#### 2.1.2 Timings

The written component will last 2½ hours in total.

#### 2.1.3 Open Book /Closed Book

The multiple choice part is a closed book test: candidates will not have access to reference material or the Internet for its duration. The longer form questions are an open book test: candidates will be permitted to use reference material and Internet access will be available.

In order to allow candidates maximum flexibility as to how to manage their time, initially the written component will be conducted as a closed book test: we expect candidates to answer the multiple choice questions at this point. As soon as candidates notify the Invigilator that they wish to use the Internet or make use of reference material, the multiple choice answer sheet will be collected from the candidate; the written component will then be conducted as an open book test, **but the candidate will not be able to make any changes to their multiple choice answers.**

### 2.2 Practical Component

#### 2.2.1 Format

The practical component of both tracks of the CREST Certification Examination will comprise a series of stages, split into structured tasks to be carried out against the CREST Certification Network (CCN) and the target hosts, infrastructure and applications that it comprises. Please note that the practical components are not designed as replicas of “real world” security assessment engagements: rather, they are examinations whose aim to test the skills and knowledge that security consultants and penetration testers will need to carry out effective security assessment engagements.

As noted above, stages and tasks are designed to examine fundamental infrastructure or web application penetration testing skills; candidates will be required to complete all of them. Success at each question or task is based on an item or items of information that the candidate must retrieve, acquire or derive from the target applications or infrastructure. The practical components have, wherever possible, been designed so that success at each question or task should *generally* not depend on success at other questions or tasks, however in some cases where system compromise is required before access can be gained, limited “task chaining” will occur.

#### 2.2.2 Timings

The practical component will last 3½ hours, and is an open book test: candidates will be permitted to use reference material, and, although the CCN is not directly connected to the Internet, Internet access will be made available if required. Candidates will be given the practical component worksheet fifteen (15) minutes before the start, to allow its perusal before the examination starts.

#### 2.2.3 Integrity Protection

Candidates will not be permitted to connect their test platforms to CREST's Internet connection, and any data transfer between the CCN and the Internet will be by means of a USB flash drive supplied by the Invigilator. Any attempt to connect the candidates test platform to the Internet via any means will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. Any attempt to retain data relating to the CREST Certification Examinations either locally or by remote



upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. No refund of fees will be considered in these situations.

#### 2.2.4 Infrastructure Assessment Details

The practical examination for the infrastructure assessment contains sample equipment that would typically be found in a real world test of a medium to large size organisation. Candidates will be expected to demonstrate their capabilities in and competency at:

- Network mapping
- Assessing network devices such as switches and routers
- Assessing hosts running Windows operating systems
- Assessing hosts running Unix (both commercial and open source) operating systems
- Assessing Windows desktop lockdowns

Knowledge gained will need to be used in an intelligent manner to demonstrate a good understanding of the technologies in use and their implications as well as simply being able to run tools and scripts.

##### *Network mapping and network device assessment stage*

The areas of the Technical Syllabus that are covered in the network mapping and network device assessment stage are as follows:

Syllabus area	Syllabus area description
A5	Record keeping, interim reporting & final results
B1	IP protocols
B2	Network architectures
B3	Network routing
B4	Network mapping & target identification
B5	Interpreting tool output
B6	Filtering avoidance techniques
C2	Domain name server (DNS)
D1	Management protocols
D2	Network traffic analysis
D3	Networking protocols

For further information, consult the Technical Syllabus.

##### *Unix stage*

The areas of the Technical Syllabus that are covered in the Unix stage are as follows:

Syllabus area	Syllabus area description
A5	Record keeping, interim reporting & final results
B5	Interpreting tool output
B8	OS fingerprinting
B9	Application fingerprinting and evaluating unknown services
B13	File system permissions



Syllabus area	Syllabus area description
B14	Audit techniques
F1	User enumeration
F2	Unix vulnerabilities
F3	FTP
F4	Sendmail / SMTP
F5	Network File System (NFS)
F6	R* services
F7	X11
F8	RPC services
F9	SSH
G2	Web servers and their flaws
G4	Web protocols

For further information, consult the Technical Syllabus.

#### *Windows stage*

The areas of the Technical Syllabus that are covered in the Windows stage are as follows:

Syllabus area	Syllabus area description
A5	Record keeping, interim reporting & final results
B5	Interpreting tool output
B8	OS fingerprinting
E1	Domain reconnaissance
E2	User enumeration
E3	Active Directory
E4	Windows passwords
E5	Windows vulnerabilities
E8	Exchange
E9	Common Windows applications
G2	Web servers and their flaws
G4	Web protocols
J1	Microsoft SQL Server

For further information, consult the Technical Syllabus.

#### *Windows desktop lockdown stage*

The areas of the Technical Syllabus that are covered in the Windows desktop lockdown stage are as follows:

Syllabus area	Syllabus area description
A5	Record keeping, interim reporting & final results



Syllabus area	Syllabus area description
<b>B13</b>	File system permissions
<b>B14</b>	Audit techniques
<b>E5</b>	Windows vulnerabilities
<b>E7</b>	Desktop lockdown

For further information, consult the Technical Syllabus.

### 2.2.5 Web Application Assessment Details

The application assessment consists of two web applications, both configured as two-tier architectures. The web applications will be based on common web application technologies hosted on Windows and Unix platforms.

Both applications have been designed to provide the candidate with a series of generic vulnerabilities to find, assess and exploit.

Candidates will be expected to demonstrate knowledge of the following types of application vulnerability:

Syllabus area	Syllabus area description
<b>A5</b>	Record keeping, interim reporting & final results
<b>C3</b>	Customer web site analysis
<b>E4</b>	Windows passwords
<b>E5</b>	Windows vulnerabilities
<b>G2</b>	Web servers and their flaws
<b>H3</b>	Information gathering from web mark-up
<b>I1</b>	Web site structure discovery
<b>I2</b>	Cross-site scripting attacks
<b>I3</b>	SQL injection
<b>I4</b>	Session ID attacks
<b>I5</b>	Fuzzing
<b>I6</b>	Parameter manipulation
<b>I7</b>	Data confidentiality & integrity
<b>I8</b>	Directory traversal
<b>I9</b>	File uploads
<b>I10</b>	Code injection
<b>I11</b>	CRLF attacks
<b>I12</b>	Application logic flaws
<b>J1</b>	Microsoft SQL server
<b>J3</b>	Web / App / Database connectivity

Candidates will be expected to exploit these issues as directed by their candidate's worksheet, providing the results onto the supplied media for later review by the Invigilator.



## 2.3 Invigilation

A CREST assessor will be present throughout the day as Invigilator. The Invigilator is not there to assess candidates' capabilities: all assessment is via the objective written and practical components. However, the Invigilator will be able to answer any procedural questions that candidates may have, and assist in troubleshooting.

## 3 Marking Scheme / Pass Mark

The marking scheme is given in the table below:

Component	Marks per question	Number of questions	Total Marks	Weight (%)
Written (multiple choice)	1	90	90	26.1%
Written (long form)	15	3	45	13.0%
Practical	35	6	210	60.9%
<b>Total</b>			<b>345</b>	<b>100.0%</b>

**Successful candidates must score two-thirds of the available marks in each component.** That is:

- at least **90 marks** from the **written component** (possible total: 135 marks), and
- at least **140 marks** from the **practical component** (possible total: 210 marks).

This represents an overall pass mark of approximately 67%, but note **that candidates must score the minimum number of marks in each section: candidates who score very well in one component but not the other will not pass.**

Unsuccessful candidates will be told their final scores in the written and practical components, along with feedback as to the general areas in which they fell short.

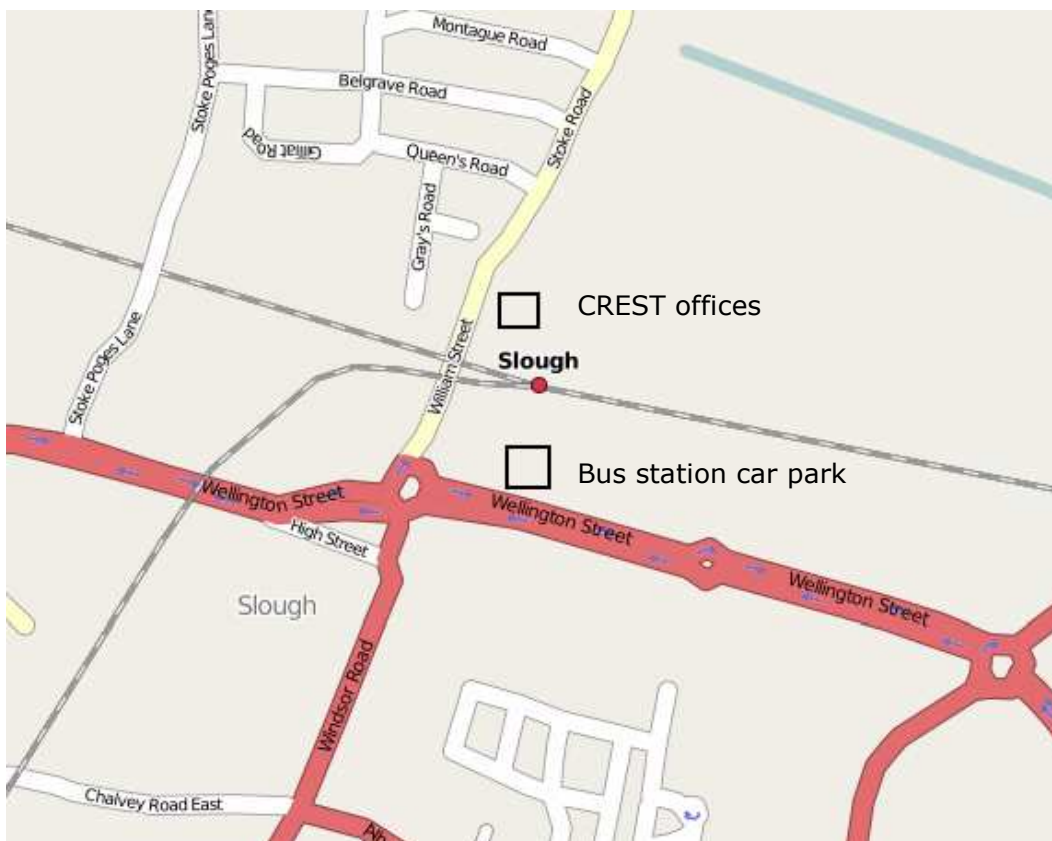


## 4 Examination Logistics

### 4.1 Location

The Certification Examination will take place at CREST's offices in Slough:

CREST (GB) Ltd  
Abbey Business Centres  
18-24 Stoke Road  
SLOUGH  
Berkshire  
SL2 5AG



CREST's offices are approximately 10 minutes' walk from Slough train station: come out of the North entrance (from platform 5; not the main entrance), turn left on Railway Terrace and walk up to the main road, Stoke Road. Then turn right, cross over Stanley Cottages, and the CREST offices are in front of you on the right hand side.

Parking is available in the car park above the bus station on the corner of Wellington Street and William Street: it costs £7 per day, **payable in coins only: the machine does not accept notes or credit/debit cards.**

Full directions can be found online at <http://www.abbeyoffices.com/ourlocations/slough/map/>, or via Google Maps UK at <http://maps.google.co.uk/maps?q=SL2+5AG>.



## 4.2 Timing

The general timings of a typical CREST Certification Examination day are as follows, although these should be taken as a guideline only. The only hard time limits are, as laid out above, 2½ hours for the written component and 3½ hours for the practical component.

Candidates will be informed in advance whether they have been assigned the Candidate 1 or Candidate 2 designation.

Candidate 1	Candidate 2
0900: Arrive	0900: Arrive
0915: Read through worksheet	
0930: Start Practical Component	0930: Start Written Component
	1200: Finish Written Component
1300: Finish Practical Component	1200-1315: Lunch
1300-1400: Lunch	
1300-1330 Invigilator reconfigures network	
	1315: Read through worksheet
	1330: Start Practical Component
1400 Start Written Component	
1630: Finish Written Component	
	1700: Finish Practical Component

Lunch will not be provided, but there are several options close by within 5-10 minutes' walk. We allow at least an hour for lunch.

## 4.3 Communication of Results

All written and practical component examination scripts will be marked independently by two CREST assessors: this will be completed within five working days of the examination and where possible by the end of the week in which the candidate sits the examination. Results will be communicated by letter to the candidate.

A list of all current CREST Consultants in good standing will be available from the CREST web site, <http://www.crest-approved.org/>.

## 4.4 Testing Platform Options

### 4.4.1 Introduction

As noted in section 1.2, CREST takes the confidentiality of the content of the CREST Certification Examinations seriously: candidates are reminded that any attempt to retain data relating to the CREST Certification Examinations either locally or by remote upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision.

In order to help CREST maintain this confidentiality, we do not permit candidates to remove hard disks and writeable media that have been connected to the CREST certification network (CCN) unless they have been securely wiped: we have the facility to do this.

Consequently, CREST offers three testing platform options for candidates sitting Certification Examinations, which are described below. **We strongly recommend that candidates plan to use their own testing**

Version: 1.0 (Public Release)	Page 11 of 14	Date: 4 December 2007
-------------------------------	---------------	-----------------------



**platform (option 1), as this will be what they are most familiar with**, but we offer two alternative options in addition.

#### **4.4.2 Option 1: Use own laptop testing platform (recommended)**

Candidates will bring their own testing platform (e.g. laptop with appropriate software toolkit) to the CREST offices. It must have an RJ45 Ethernet connection capable of running at 100Mbps, configured to obtain an IP address via DHCP. Additionally, it must be capable of reading from and writing to a USB key formatted with a FAT filesystem.

The operating systems and tools used must be capable of conducting an infrastructure or web application test: candidates may use any software tools they deem appropriate, but are responsible for ensuring that any tools used are appropriately licensed and function correctly.

It is important to note that candidates choosing to use their own testing platform **must surrender their hard disk and any other writeable media for wiping at the end of the assessment process**. Hard disks, once wiped, will be returned to the candidates: we envisage that this will be within two weeks of completion of the certification examination.

#### **4.4.3 Option 2: Use own VMware images**

Candidates will bring their own testing platforms as VMware images, either burned on to a DVD or on an external hard drive. These will be copied to a CREST machine running VMware Server 1.0.4, and candidates will use them from there. VMware images should be configured with a bridged interface that is configured to obtain an IP address via DHCP.

It is important to note that candidates choosing this option will themselves be responsible for getting the VMware images running properly. Any CDs or DVDs used must be destroyed at the end of the certification examination, and CREST will provide a shredder for this purpose.

#### **4.4.4 Option 3: Use CREST's VMware images**

Candidates will be provided with both a pre-built Linux Fedora Core 7 and a Windows XP Professional SP2 system onto which a number of tools have been loaded: the toolkit provided should be sufficient for the candidate to achieve a pass mark in Certification Examination practical components. Candidates may bring in CDs or DVDs containing any additional tools, code or other reference material they see fit for loading on to these images. Any CDs or DVDs used must be destroyed at the end of the certification examination, and CREST will provide a shredder for this purpose.



## 5 Example questions (written component)

### 5.1 Multiple choice

An example multiple choice question is given below, along with the answer.

#### 5.1.1 Question

Which of the following is NOT a valid DNS record type?

- A. SOA – Start of Authority
- B. NWS – News Server
- C. CNAME – Canonical Name
- D. MX – Mail eXchange
- E. PTR - Domain Name Pointer

Candidates should clearly indicate their answer by circling the appropriate letter in their test script.

#### 5.1.2 Answer

The correct answer is (B).

#### 5.1.3 Marking scheme

Each multiple choice answer is worth one (1) mark. No points are deducted for incorrect answers.

### 5.2 Long form

An example long form question is given below, along with a model answer. Note that long form questions on IPsec will not be asked (see technical syllabus): this is an example question only.

#### 5.2.1 Question

During a penetration test, you have discovered an IPsec VPN server at IP address 10.0.0.1, and have determined that it supports the following transform attribute sets for IKE Phase-1:

Encryption Algorithm	Hash Algorithm	Authentication Method	Diffie-Hellman Group
DES	SHA1	RSA Signature	1
AES/256	SHA1	RSA Signature	2
3DES	SHA1	RSA Signature	2

a) Identify the issue and write an issue description for the customer. The issue description should contain a risk level, detail of the issue, implications and recommendations for ways to mitigate the risk.

[9 marks]

b) After presenting your findings to the customer, you conduct a de-brief with the customer and their IT supplier. During the de-brief, they mention that the VPN is used for remote access and they only use one VPN client. During IKE Phase-1 negotiations, this client sends a single proposal containing the following six transforms in the order shown:

Transform No.	Encryption Algorithm	Hash Algorithm	Authentication Method	Diffie-Hellman Group
1	3DES	SHA1	RSA Signature	2
2	3DES	MD5	RSA Signature	2



3	AES/256	SHA1	RSA Signature	2
4	AES/256	MD5	RSA Signature	2
5	AES/128	SHA1	RSA Signature	2
6	AES/128	MD5	RSA Signature	2

b) What IKE Phase-1 transform attributes will be negotiated when this client initiates a connection to the VPN server that you discovered? Describe why these particular attributes will be chosen.

[4 marks]

c) Assuming that only this VPN client is used, and the client transform set cannot be altered by the user, does this affect the risk level in practice? Does it make the risk higher or lower?

[2 marks]

### 5.2.2 Model answer

a) Issue: VPN Server supports weak encryption

Risk Level: Low or Medium

The VPN Server at address 10.0.0.1 supports both strong and weak encryption algorithms for IKE Phase-1. This could allow the VPN to use a weak encryption method for the ISAKMP SA, which could permit an attacker with access to the VPN traffic to crack the encryption and observe the clear-text traffic passing over this SA.

The weak encryption algorithms are DES, which uses a 56-bit symmetric key, and Diffie-Hellman group 1, which uses a 768-bit prime. Best practice dictates that you should use at least 128 bits for symmetric keys, and 1024 bits for Diffie-Hellman prime moduli.

You should disable both DES and Diffie-Hellman group 1 on the server, so that there is no possibility of them being used. However, before doing so, you should check that they are not required by connecting VPN peers, as some older clients only support weak encryption.

b) The transform attributes that would be negotiated are:

Encryption: 3DES

Hash: SHA1

Authentication: RSA Signature

Diffie Hellman Group: 2

These attributes will be chosen because during IKE Phase-1 negotiation, the transform chosen is the first transform in the initiator's proposal that is acceptable to the responder. In this situation, the VPN client is acting as the initiator, and the VPN server as the responder. The first acceptable client transform is number 1, which has the attributes shown above.

c) Using only this VPN client will reduce the risk level, because it will ensure that the weak encryption algorithms that are supported by the server are not used in practice. Marking scheme

Each long form question is worth a total of fifteen (15) marks.