Assessors Panel

CREST Certified Tester (CCT)
Penetration Testing Examinations
Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	AP_0508-CN02_ANZ
Version Number	1.8
Status	Public Release
Issue Date	2 August 2016

Table of Contents

Version History

Version	Date	Authors	Status
1.0	4 December 2007	Technical Committee and Assessors Panel	Public Release
1.1	14 May 2008	Technical Committee and Assessors Panel	Public Release
1.2	12 November 2009	Technical Committee and Assessors Panel	Public Release
1.3	12 January 2010	Technical Committee and Assessors Panel	Public Release
1.4	11 May 2011	Technical Committee and Assessors Panel	Public Release
1.5	17 October 2013	Technical Committee and Assessors Panel	Public Release
1.6	09 December 2015	Technical Committee and Assessors Panel	Public Release
1.8	02 August 2016	Technical Committee and Assessors Panel	Public Release

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board

1 Introduction

1.1 Examination

There are two parallel tracks of the CREST Penetration Testing Certification (CCT) Examination:

- The Infrastructure Certification Examination, which assesses a candidate's capabilities in the field of general infrastructure and operating system security assessments.
- The Application Certification Examination, which assess a candidate's capabilities in the field of 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 Certified Tester (Infrastructure), or
- CREST Certified Tester (Application)

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

1.2 Confidentiality

CREST takes the confidentiality of its examinations very seriously. The retention or dissemination of data relating to the examination (other than what is contained in the Notes for Candidates and Technical Syllabus documentation that is available from the CREST Australia New Zealand web site http://www.crestaustralia.org/) is not permitted.

Along with their booking forms, candidates must also bring both a signed Non-Disclosure Agreement to this effect and also a signed Code of Conduct document, or be prepared to sign a both documents on the morning before they start the examination.

Both of these documents are provided by the CREST Administrator as part of the booking process. The Code of Conduct for Individuals is also available on the CREST Australia New Zealand website.

It should be noted that prior knowledge of specific CREST examination configurations will be of little use to candidates, as the Examination is constantly updated and revised and many of the answers are randomised tokens generated uniquely for each candidate.

2 Examination Details

The CREST Certified Tester (CCT) has two components: a written component and a practical component.

2.1 Written Component

2.1.1 Format

The written component of both tracks of the CREST CCT Certification Examination will comprise of ninety (90) multiple choice questions, all of which the candidate must complete. In addition the candidate will be presented with four (4) long form questions, of which the candidate must choose and complete three (3) that are worth 15 marks each.

2.1.2 Timings

The written component will last 2½ hours in total.

2.1.3 Open Book / Closed Book

The entire written component of the exam will be conducted as a closed book exercise. This applies to both multiple choice and long form sections.

2.2 Practical Component

2.2.1 Format

The practical component of both tracks of the CREST Certified Tester Examinations will comprise a series of stages, split into structured tasks to be carried out against the CREST Certification Network 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 is 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.

The CCT level exams also include one scenario question where a candidate is expected to identify security related problems on a specific set of infrastructure/application and then document the findings.

2.2.2 Timings

The practical component will last 3½ hours. However, candidates will be given the practical component worksheet fifteen (15) minutes before the start, to allow its perusal before the examination starts.

Candidates should take great care to note that the breakdown of marks approximates to one mark per minute throughout each phase of the exam. If a candidate spends significantly more time than suggested by the marks for any one section or question then they are potentially missing out on marks that could have been obtained more quickly later in the paper. Where candidates are struggling with a particular question or section they are strongly advised to move on and return later in the session if remaining time permits.

2.2.3 Open Book / Closed Book

The practical component is an open book test with candidates permitted to use reference material they have brought along. Although the CREST certification network is not connected to the Internet, a dedicated Internet PC will be made available if required.

2.2.4 Integrity Protection

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

It is the candidates’ responsibility to ensure their test laptop is fully prepared prior to attending the exam and it is their responsibility to bring all necessary tools, software, applications and relevant updates with them.

Note particularly that external media players are not permitted in the Certification examination, unless candidates are prepared to have these wiped (as with any other media used during the examination). If you’d like to listen to music, put it on your hard drive.

2.2.5 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:

- 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.
- Assessing common installed application services

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
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
B13	File system permissions
B14	Audit techniques
E5	Windows vulnerabilities
E7	Desktop lockdown

For further information, consult the Technical Syllabus.

2.2.6 Web Application Assessment Details

The application assessment consists of a number of applications; candidates will be presented with multiple small applications selected from a larger pool at random, each being designed to test specific vulnerability type knowledge.

The applications are based on common internet and web application technologies hosted on a mixture of both Windows and Unix platforms. No specific server technology is included or excluded.

The 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
A5	Record keeping, interim reporting & final results
C3	Customer web site analysis
E4	Windows passwords
E5	Windows vulnerabilities
G2	Web servers and their flaws
G4	Web Protocols
G7	Web Application Servers
G8	Web APIs
G9	Web Sub-Components
H3	Information gathering from web mark-up
H4	Authentication Mechanisms
H5	Authorisation Mechanisms
H6	Input Validation
H9	Use of Cross Site Scripting Attacks
I1	Web site structure discovery
I2	Cross-site scripting attacks
I3	SQL injection
I4	Session ID attacks
I5	Fuzzing
I6	Parameter manipulation
I7	Data confidentiality & integrity
I8	Directory traversal
I9	File uploads
I10	Code injection
I11	CRLF attacks
I12	Application logic flaws
J1	Microsoft SQL server
J3	Web / App / Database connectivity

Candidates will be expected to exploit these issues as directed by their candidate 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 the exam systems.

3 Marking Scheme / Pass Mark

The marking scheme is given in the table below:

Component	Number of questions	Total Marks
Written Component	90 Multiple Choice Questions (1 mark each) 3 x Long form questions (each worth 15 marks)	135
Practical Component	**Application:** A number of mini applications – each with a set of questions. 1 Scenario Question **Infrastructure:** Sub sections of the key infrastructure elements. 1 Scenario Question	210
Total		**345**

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.**

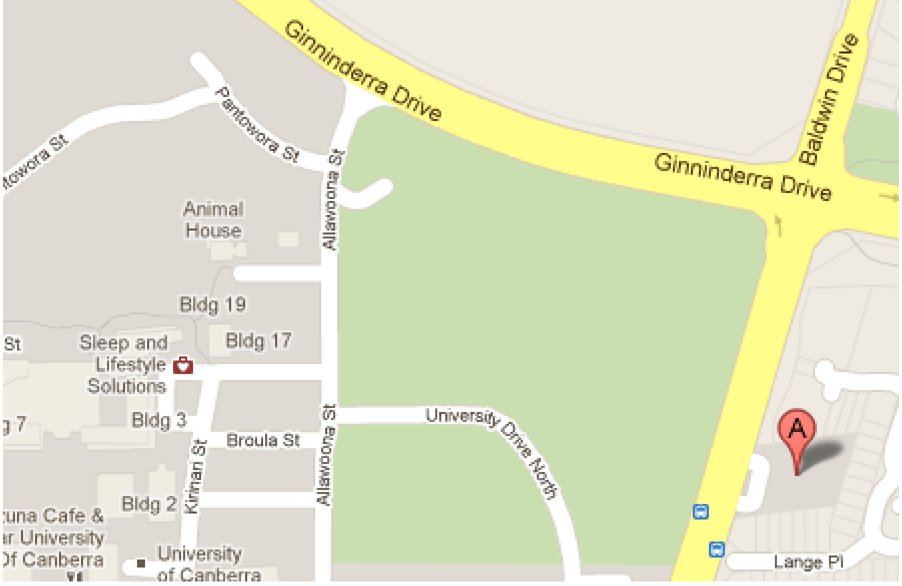
Unsuccessful candidates will be told their final scores in the written and practical components, along with feedback as to the general areas in which they fell short.

4 Examination Logistics & Timing

4.1 Location & Timing

The Certification Examination will take place at Canberra University:

Building 18, 170 Haydon Drive
Canberra University
Bruce
ACT (Australian Capital Territory)



The University of Canberra is approximately 15 minutes' drive from Canberra Central.

Follow the directions below:

1. Head east on Vernon Circle/Tourist Drive 1 toward Northbourne Ave/National Route 23
2. Continue to follow Tourist Drive 1 900 m
3. Continue onto Northbourne Ave/National Route 23 3.5 km
4. Turn left onto Mouat St/Tourist Drive 4 1.0 km
5. Turn left onto Ginninderra Drive/Tourist Drive 4
6. Continue to follow Ginninderra Drive 3.4 km
7. Turn left onto Haydon Drive, Destination will be on the left 280 m

Full directions can be found online at http://www.canberra.edu.au/maps/buildings-directory/building-18 or via Google Maps AU at https://goo.gl/maps/9BygUysjSDp

Before the Examination starts

Before the examination starts, Candidates will:

- Need to show **suitable office ID** (eg military ID, driver's license or passport)
- Have their **NDAs** collected. This is to help us maintain the confidentiality of the examination.
- Have their **Codes of Conduct** collected.

Candidates should have read and signed both of these documents in advance.

4.2 Communication of Results

All written and practical component examination scripts will be marked independently by CREST Invigilators: this will be completed within fifteen 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.

4.3 Testing Platform

As noted in sections 1.2 and 2.2.4, CREST takes the confidentiality of the content of its examinations seriously: candidates are reminded that any attempt to retain data relating to the CREST Examinations either locally or by remote upload will be considered a breach of the CREST 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 unless they have been securely wiped: we have the facility to do this.

Consequently, CREST requires all candidates to be able (and equipped) to remove their internal hard disk at the end of the exam so that it can be retained by CREST for erasure. It is the candidate’s responsibility to remove any disk IDE / SATA passwords prior to handing the disk over for erasure – if this is not done then the drive will remain locked and cannot be accessed and thus cannot be returned. There is no requirement to remove software encryption (eg BitLocker etc) from the disks as this will simply be overwritten.

If the disk is not a standard SATA or USB connection then the candidate is required to provide a suitable adaptor plate or cable to allow the disk to be wiped.

It should be noted that CREST are **UNABLE** to accept responsibility for candidate laptops and only the bare drive will be retained. It is the candidate’s responsibility to ensure they are competent to remove the disk.

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 least 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 file system.

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 **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 approximately two weeks of completion of the certification examination providing no disk access or other technical issues arise.

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