Assessors Panel

CREST Registered Tester Certification Examination Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	**AP_0508_CN07_ANZ**
Version Number	2.0
Status	Public Release
Issue Date	2nd August 2016
Review Date	

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

Version History

Version	Date	Authors	Status
0.1	10 January 2010	Technical Committee and Assessors Panel	Beta Release
1.0	25 March 2010	Technical Committee and Assessors Panel	Public Release
1.1	15 April 2010	Technical Committee and Assessors Panel	Public Release
1.2	11 May 2011	Technical Committee and Assessors Panel	Public Release
1.3	1 May 2015	Technical Committee and Assessors Panel	Public Release
2.0	2 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

The (CRT) Crest Registered Tester examination tests candidates’ knowledge in assessing operating systems and common network services at an intermediate level below that of the main CCT qualifications. The CRT examination also includes an intermediate level of web application security testing and methods to identify common web application security vulnerabilities.

The examination covers a common set of core skills and knowledge. The candidate must demonstrate that they can perform an infrastructure and web application vulnerability scan using commonly available tools and interpret the results to locate security vulnerabilities.

The CREST Registered Tester Certification qualification is valid for three (3) years.

The Certification Examination has two components: a multiple choice written question section and a practical assessment which is also examined using multiple choice answers. The practical assessment tests candidates’ hands-on penetration testing methodology and skills against reference networks, hosts and applications.

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 Australia New Zealand web site http://www.crestaustralia.org/) is not permitted: along with their booking forms, candidates must also send a signed Non-Disclosure Agreement to this effect, or be prepared to sign a Non-Disclosure Agreement in the morning before they start the Certification Examination.

It should be noted that prior knowledge of specific Certification Examination configurations will be of little use to candidates, as the Examination is constantly updated and revised.

2 Examination Details

2.1 Written Component

2.1.1 Open Book / Closed Book

The written multiple choice part is a closed book test: candidates will not have access to reference material or the Internet for its duration.

2.1.2 Format

The written component of the CRT Examination will comprise of one hundred and twenty (120) multiple choice questions, all of which the candidate must complete.

- The first 20 relate to fundamental knowledge of IT Security
- The next 20 relate to Infrastructure Security Testing
- The next 20 relate to Application Security Testing
- The final 60 are a mix of Infrastructure and Application Security questions

2.1.3 Timings

There are 3½ hours available in total for the exam. It is the candidate's responsibility for managing their own time during the exam, however it is recommended that approximately one hour is spent on the written component.

2.2 Practical Component

2.2.1 Open Book / Closed Book

The practical component is conducted as an open book test, reference material or access to the Internet is permitted. Although the CREST CRT Certification Network is not directly connected to the Internet, Internet access will be made via a dedicated computer.

2.2.2 Format

The practical component of the CRT Examination will comprise a series of stages, split into structured tasks to be carried out against the CREST CRT 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 and web application penetration testing skills at an intermediate level below that of the main CCT qualifications; 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 in order to establish the correct multiple choice answer. The practical components have been designed so that success at each question or task does not depend on success at other questions or tasks.

- There are 10 Marks available for identifying settings and configuring network address settings, the answers to this section will be verified by the assessor at the start of the assessment to ensure the candidate can successfully attempt the practical component.
- The first set of questions in the practical section relate to fundamental knowledge of IT Security Infrastructure.
- The next set relate to Windows Infrastructure Security Testing.
- The next set relate to Unix Infrastructure Security Testing.
- The final set relate to Application Security Testing.

There are 5 possible answers for each question. Only one is correct. If multiple answers are given your answer will be marked as incorrect.

2.2.3 Timings

There are 3½ hours available in total for the exam. It is the candidate's responsibility for managing their own time during the exam, however it is recommended that approximately 2½ hours are spent on the practical component.

It is recommended that any relevant network scans to be conducted are started at the beginning of the exam against the whole network, so as to save time later when they can be used as a reference.

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 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.

Note: external media players are specifically prohibited during the Certification Examination. If you would like to listen to music, please put it on your hard drive and use headphones during the exam. The volume of the music you listen to must not distract other candidates.

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

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
B4	Network mapping & target identification
B5	Interpreting tool output
B6	Filtering avoidance techniques
C2	Domain Name System (DNS)
D1	Management protocols
D2	Network traffic analysis

Syllabus area	Syllabus area description
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

Syllabus area	Syllabus area description
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.

2.2.6 Web Application Assessment Details

The application assessment consists of multiple single page web applications. The web applications will be based on common web application technologies hosted on Windows and Unix platforms.

Pages 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
G2	Web servers and their flaws
H3	Information gathering from web mark-up
I1	Web site structure discovery
I2	Cross-site scripting attacks
I3	SQL injection
I6	Parameter manipulation
I7	Data confidentiality & integrity
I8	Directory traversal
I9	File uploads
I10	Code injection
I12	Application logic flaws
J1	Microsoft SQL server
J3	Web / App / Database connectivity

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	Total Marks
Written (multiple choice)	120
Practical	100

Successful candidates must score 60% of the available marks in each component. That is:

- at least **72 marks** from the **written component** (possible total: 120 marks); and
- at least **60 marks** from the **practical component** (possible total: 100 marks)

This represents an overall pass mark of approximately 60%, 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 Testing Platform Options

4.1 Introduction

As noted in sections 1.2 and 2.2.4, 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 unless they have been securely wiped: we have the facility to do this. Candidates must surrender the internal disks AND also provide a caddy allowing them to be accessed using either standard SATA or USB under Debian Linux

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 should be noted that CREST are **UNABLE** to accept responsibility for candidate laptops and only the bare drive will be retained. It is the candidates responsibility to ensure they are competent to remove the disk. Any disk security passwords within the IDE BIOS must be removed.

There is currently only one option available for test platforms.

4.2 Option 1: Use own laptop testing platform

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.

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

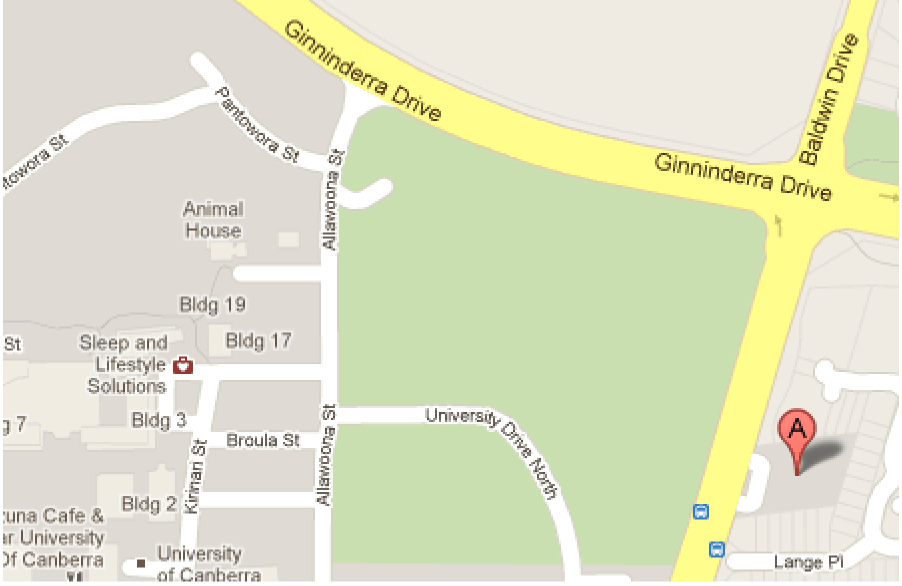
It is important to note that candidates choosing to use their own testing platform **must surrender their hard disk and any other writeable media for wiping at the end of the assessment process**. Hard disks, once wiped, will be returned to the candidates: we envisage that this will be **at the latest**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

5 Examination Logistics

5.1 Location

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

5.2 Before the Certification Examination starts

Before the Certification Examination starts, candidates will:

- **Have to sign an NDA**. This is to help us maintain the confidentiality of the Examination.
- Have to sign the **CREST Code of Conduct**.
- **Need to show suitable official ID** (eg military ID, driver's license or passport)

5.3 Communication of Results

Examination scripts will usually be marked 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 communicated by letter to the candidate.

6 Example questions

6.1 Example 1 Mark Question

An example 1 mark multiple choice question is given below, along with the answer.

6.1.1 Question (1 Mark)

Which version of operating system is installed on the host xx.xx.xx.xx ?

A. Solaris 9 (x86)

B. Solaris 9 (SPARC)

C. Solaris 10 (x86)

D. Ubuntu 9.01

E. CentOS 5.1

6.1.2 Answer

The correct answer is (x).

6.1.3 Marking scheme

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

6.2 Example 5 Mark Question

An example 5 mark multiple choice question is given below, along with the answer.

6.2.1 Question (5 Mark)

Identify the Crest Trophy String in the file 'Crest-Trophy' using the XXXX service and a common security misconfiguration issue on the host xx.xx.xx.xx ?

A. RandomStringA

B. RandomStringB

C. RandomStringC

D. RandomStringD

E. RandomStringE

6.2.2 Answer

The correct answer is (x).

6.2.3 Marking scheme

Each multiple choice answer is worth five (5) marks. No points are deducted for incorrect answers.