Assessors Panel

CREST Certified Tester (CCT)

Penetration Testing Examinations

Notes for Candidates

Contents

1. Introduction

1.1. Examination

The There are two disciplines in the CREST Certified Penetration Testing Certifications (CCT):

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

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

- • CREST Certified Tester (Infrastructure) (CCT Inf), or
- • CREST Certified Tester (Application) (CCT App)

For either discipline, the CREST 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 web site http://www.crest-approved.org/) is not permitted.

Along with their booking forms, candidates must 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 Examinations Administrator as part of the booking process. The Code of Conduct for Individuals is also available on the CREST website.

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 the CCT examinations are delivered at a Pearson Vue centre of your choice. Please visit www.pearsonvue.com and follow the on-screen instructions to schedule your chosen examination:

Note the logistical requirements for exams conducted at a Pearson Vue centre are defined by Pearson Vue and candidates must ensure they adhere to all of the necessary requirements as listed on their web site. CREST candidates are not exempt from any of the standard requirements.

The written component of both disciplines of the CREST CCT Certification Examinations will comprise one hundred and fifty (150) multiple choice questions, all of which the candidate must complete.

2.1.2 Timings

The written examination will last 2.5 hours and you should attempt to answer all questions within this time.

Note that your permitted maximum session time at Pearson Vue is 3 hours in total, allowing you time to read the Code of Conduct and to provide feedback following the examination.

2.1.3 Open Book / Closed Book

The entire written component of the exam will be conducted as a closed book exercise.

2.2. Practical Component

2.2.1 Overview

The practical component of both disciplines 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. This is designed to mimic the skills required to perform a 'build review' and author a client report on the findings.

2.2.2 Timings

The practical component is split up into two sections which are conducted sequentially.

Section	Time
Scenario Question	150 minutes (2½ hours)
Assault Course	210 minutes (3½ hours)

In total, the practical components will last 6 hours, but the examination is conducted in two sections with a break in between. However, candidates will be given the practical component question papers fifteen (15) minutes before the start, to allow 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   Format

The structure of the examination day is shown below:

Activity	Description	Time
Candidate Arrival	Candidates arrive, complete initial paperwork, ID checks and all other administrative activities.	-
Scenario Question	Candidates attempt the scenario question; they are given 15 minutes to read the question paper. At the end of this section, their answers will be collected and saved. <u>No further answers or modifications to this section will be accepted</u>	15 minutes reading time 150 minutes (2½ hours)
Lunch	Candidates may leave for lunch.	1 hour
Assault Course	Candidates attempt the practical assault course; they are given 15 minutes to read the question paper.	15 minutes reading time 210 minutes (3½ hours)

For example, if the candidates arrive at 0930, it is likely that they will have completed all of the activities required by 1730/1745. This is because of the extra time taken for administrative purposes (for example, removing hard disks or completing paperwork).

2.2.4   Open Book / Closed Book

The entire practical component is an open book test with candidates permitted to use reference material they have brought along. Candidates will also have Internet access though the CREST certification network; however, this is restricted browse down solution that does not allow copy and paste and logs all access.

2.2.5   Integrity Protection

Any attempt to connect the candidate's test platform to a network other than the CREST Certification Network 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.

<u>External media players are not permitted in the examination room, unless candidates are prepared to have these wiped (as with any other media used during the examination). Candidates may listen to music, providing it does not disturb others, through headphones connected to their laptop.</u>

2.2.6   Infrastructure Examination Assessment Details

The practical examination for the Certified Infrastructure examination 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 IP networks, such as network mapping, switches and routers;
- Assessing hosts running Windows operating systems;
- Assessing hosts running Unix (both commercial and open source) operating systems;
- Assessing the effectiveness of a Windows desktop lockdown environment.
- 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.

2.2.7   Guidance

The CREST Assessors panel regularly identifies common themes and consolidates common questions and answers from candidates and from the industry in relation to the CREST certification examinations. Candidates are advised to familiarise themselves with these, although they are free to disregard them if they wish. The latest information can be accessed at https://www.crest-approved.org/professional-qualifications/examination-faqs/index.html.

CREST recommend that candidates familiarise themselves with the content at https://crest-approved.org/ufaqs/do-you-have-any-technique-advice-for-the-practical-exams/index.html which has been created specifically for those attempting a practical examination.

Sample Papers

Sample papers for both the Scenario and Assault Course are available on the website at https://www.crest-approved.org/certification-careers/crest-certifications/crest-certified-infrastructure-tester/ .

These sample papers are to provide information about the structure of the exam, as well as to give some indication of timings and general expectations.

These are not intended to help revision in terms of breadth and depth of the technical contact. For that consult the Technical Syllabus.

Tools

These are some general notes about tools.

- This is an advanced exam. Do not expect a single tool or source to provide all the exploits you might need.
- Have multiple tools for each task you might want to perform.
- Have tools that use different approaches for task. As an example, if you were to be enumerating users from a Windows host have tools that can do this over SMB, and one that can work over SNMP, as well as other possible options.
- Learn how to use tools before the exam. There will generally not be time during the exam to learn how to use a tool for the first time.
- Some tasks may require custom scripts. Prepare templates that can be used for a variety of common tasks.
- Be prepared to perform tasks on networks or hosts that you don't have direct access to e.g. pivoting, jump boxes, or routed networks.

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
B	Core Technical Skills
D	Networks
E	Network Services

For further information, consult the Technical Syllabus.

Linux / Unix stage

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

Syllabus area	Syllabus area description
B	Core Technical Skills
D	Networks
E	Network Services
G	Linux / UNIX Security Assessment
I	Databases
K	Containerisation

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
B	Core Technical Skills
D	Networks
E	Network Services
F	Microsoft Windows Security Assessment
I	Databases
K	Containerisation

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
B	Core Technical Skills
D14	TCP
E9	Desktop Access
F	Microsoft Windows Security Assessment

For further information, consult the Technical Syllabus.

2.2.8   Web Application Examination Assessment Details

The Certified Web Application Examination 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 **Note: Taken in a Pearson Vue examination centre**	150 Multiple Choice Questions (1 mark each)	150
Practical Component	1 Scenario Question	150
	Application: A number of mini applications – each with a set of questions. **Infrastructure:** Sub sections of the key infrastructure elements.	210
Total		**510**

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

- at least **100 marks** from the **written component** (possible total: 150 marks), and
- at least **100 marks** from the **scenario component** (possible total: 150 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 if they achieved a lower mark than 67%.

4. Examination Logistics & Timing

4.1. Location & Timing

Specific logistical information relating to the practical examination centres in each Region can be found on the Examination Preparation page of your chosen examination location.

Please note that the written section is performed at a Pearson Vue centre and the practical completed at the CREST assessment centre.

Before the Examination starts

Before the examination starts, Candidates will:

- Need to show suitable office ID (e.g. 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. CREST makes every effort to email candidates with their result letter within 30 days of the examination being taken. Digitally signed certificates, where appropriate, will be emailed to candidates

4.3. Testing Platform

As noted in sections **Error! Reference source not found.** and 2.2.5, 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.

In line with the CREST Terms and Conditions of Examinations, 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 passwords (e.g. hardware encryption) 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 (e.g. Bit locker etc) from the disks as this will simply be overwritten.

If the disk is not a standard SATA, NVMe 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 memory stick 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 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.