TOP TIPS – CREST Certified Tester (CCT) – Practical Exam

Purpose

The primary aim of any CREST exam is to assess your knowledge, skills and experience in a particular discipline and determine your ability to carry out activities that may present themselves during real-world engagements.

The 'Practical' examination is not only designed to assess your technical proficiency but also to evaluate your grasp of penetration testing tools, techniques, and the capacity to address common issues through troubleshooting or adapting your approach.

The new **CCT INF/APP Practical** exam is designed to evaluate these skills albeit in an artificial environment and within specified time constraints. We have worked hard to ensure the exam is set at the right technical level and is achievable in terms of the time allocated, provided that you have prepared well and have the appropriate hands on experience.

Pro tip: Kali Linux is the main platform provided to candidates in the exam. To help you prepare for your exam, CREST provided a copy of the candidate virtual machine online. Download a copy and make sure you are familiar with the interface, available tooling and behaviour of the environment. Detailed information is available on **CREST CCT** web pages:

- CREST Certified Tester - Infrastructure
- CREST Certified Tester - Application

Strategy

At the beginning of the exam, you will be provided with time to understand what is in scope and **read through the questions** provided, so you can formulate a strategy. You should:

- Identify the modules you feel most comfortable with and plan the order in which to tackle these. However, factor in all modules in case you need to change tactic or to tackle some of the initial questions for extra marks.
- Although it is fine to tackle each module in the order you prefer, note that you should answer the questions within each module in the order that they appear as they follow a logical sequence and usually relate to the previous question.
- Allocate your time following the principial of one mark a minute. Be aware that not all modules are equal in number of marks (each exam has four modules with 30 marks and one with 60 marks)
- Identify and execute tasks that can be run in parallel, e.g. port scans, enumeration, or brute-forcing. Do not watch and wait for these to finish!
- Consider your tooling. Ensure that you not only understand and feel comfortable with a task, but that you are comfortable with the tooling that is available on the candidate testing platform.

Pro tip: Prepare and practise your strategy in advance and amend on the day to meet the specific challenges.

Time constraints

One of the main challenges in any exam is managing the limited time available to you. Real-world engagements are also time-bound, albeit there is usually a longer period to complete the work.

CREST have developed the exam rigs with this in mind. While individual modules and challenges reflect the vulnerabilities and insecure configurations that you might encounter during an engagement, the complexity and number of issues have been scaled down. When developing the challenges and assigning available marks, **one mark per minute** has been used.

When preparing and taking the exam you should keep this in mind when designating time to each module and question. Try to get a sense of the time it will take to do a specific task or action.

Pro tip:

- In advance of the exam **practice under timed conditions**. Not only of a full rig, but of individual tasks, such as enumerate users from Active Directory or configure an exploit in Metasploit. There is not enough time to learn new techniques during the exam; you should be comfortable with common tasks.
- **Avoid rabbit holes**. This is easier said than done, however be disciplined and move on to another task if you are stuck.
- **Keep an eye on the time**. Time flies when you're having fun 😉

Tools and notes

The new CCT INF/APP – Practical exam does not allow candidates to bring their own laptops into the test centre. Instead, candidates have access to a fully functioning virtual machine running Kali Linux, which is equipped with a wide array of standard tools.

Be comfortable with a range of tooling, and be able to digest and apply help and man pages on the fly. Most modules will require common tools and by this stage in your career you should be familiar with nearly all the tools that you will require to solve the challenges.

Ensure you are comfortable with Bash and be ready to generate or modify lists for enumeration and cracking.

The exam version of Kali Linux can be accessed via the CCT exams web pages. This image reflects the version that is available during the exam and contain all the tools that will be needed to complete the challenges. **You are strongly advised to familiarise yourself with this image and its tools.**

Prior to the exam, test various capabilities of available tools including their commonly and less commonly used parameters and capabilities, and find alternative ways to achieve a similar outcome if possible (e.g. using a different tool or method). It may also help your learning process to reproduce steps manually.

Candidates will also have access to CRESTDrive, a new functionality that enables candidates to securely upload files which can then be accessed during your exam. There are no restrictions to the types of files that can be uploaded as long as it does not exceed the total 100MB size limit per exam and that these files are solely intended to support candidates with their exam.

Pro tip: More important than remembering every command option and parameter by heart, practice locating the information you need in an offline environment using the manual or help sections of command line tools.

Password cracking and online brute forcing

There may be challenges in the exam which require you to perform an online password guessing or offline password crack. When approaching these challenges you should consider the following:

- Read the question! Some questions may direct you to a particular file or password dictionary, or hint at potential username or password formats.
- Be realistic with time – Within the exam context an online attack or offline crack should take less than a minute and no more than a few.

Pro-tip: Password-cracking or online password guessing **should take up to a few minutes max**. Any longer and you should stop and re-evaluate your method.

Answer input

Answers will require you to select an option or enter a string. When entering a string do so carefully! An incorrect string will not be awarded any marks.

Challenge types

CCT INF

The modules and questions will be aligned with the CCT INF syllabus, and all are achievable using the toolset available. The types of challenges you may face include:

Windows Active Directory – These modules involve multiple hosts that are members of an Active Directory domain. In these challenges you will need to gain a foothold on a system, enumerate users and privileges, move laterally, and escalate privileges.

Linux OS – The Linux challenges mix OS level configuration issues with insecure third-party software. You should be familiar with typical services that support applications, databases, and workloads in a Linux enterprise environment. In addition, the candidate should be familiar with common configuration weaknesses that could provide privilege escalation vectors.

Windows Lockdown – The lockdown or breakout modules drop you into an environment which has been locked down using Windows native security controls. Candidates should be familiar with common strategies to implement application restrictions, bypass techniques, the Windows command line, and common privilege escalation weaknesses. .

Network Configuration – Be prepared to enumerate network configurations and exploit vulnerabilities to bypass network restrictions.

Some modules combine different platforms and services, such as Linux or Windows with AWS or Azure. Where this is the case, any relevant challenge that requires a movement between these services will be highlighted, however be prepared to pivot between these.

CCT APP

The modules and questions will be aligned with the CCT APP syllabus, and are all achievable using the toolset available. The type of challenges you may face include:

Web Apps(!) - Of course this will be the bulk of the exam, browser or thick client, website or API, any common server stack or backend.

Databases – Where the application uses a data store further exploitation of this will be expected. Relational, NoSQL or Query, these questions will assess your capability in breaking through a web application to compromise the data store, fully, as well.

Injection Attacks – Can you change how the web app operates? Be prepared to bypass filters and ensure your injection payloads can be weaponised to extract data or elevate access & privileges.

Authentication Attacks – Bypassing authentication, assessing poorly implemented authentication models or elevating privileges are all common web application testing elements.

Cloud – Be prepared to exploit SaaS and other cloud services that may be used to deliver a web app

Some questions will cover multiple syllabus topics; be prepared to pivot across services and use an initial vulnerability to leverage further compromise and answer a module fully.

Final tips

The CREST CCT **INF/APP** is without a doubt a tough challenge; however, it is achievable! Our final tips to get exam ready are:

- **Plan ahead.** Have a strategy before you enter the exam room and adapt when you see the questions.
- **Be flexible.** Be able to adapt your methods and be comfortable with a variety of tools.
- **Read the question** and **respond** to the information and vulnerabilities you discover in each of the challenges.
- **Mind the time!** Think one mark a minute and allow a contingency.
- **Avoid the rabbit holes.** If you find yourself entering one take a step back and review the question.
- **Practise** the skills and methods detailed in the syllabus using the sample virtual candidate machine (Kali image and tooling).
- **Enjoy the experience** – Perhaps easier to say now than when you have 30 minutes left on the clock, however, make the most of your exam experience.
- **Have confidence** that with hard work and preparation you can pass the CREST CTT INF/APP exam.

Good luck!