TOP TIPS – CREST Registered Tester (CRT) 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 in real-world engagements.

The 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 CRT 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 you have prepared well and are focussed on answering the question.

Pro tip: Kali Linux is the main platform used in the exam, which is openly available. Download a copy and make sure you are familiar with the interface and behaviour of the environment. Detailed information is available on CREST CRT web page.

Time constraints

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

Exams are scaled down to replicate specific components of what you might encounter during an engagement, and this also allows you to apply the strategy of allocating one minute per mark as you progress through the questions. Tasks with a higher mark are likely to require that you spend a bit more time working through the problem to identify the flag, or there may be several steps involved in the process.

Similarly to a real-world engagement, it is important to balance expected results with the time available and apply an iterative approach to your activities. Make sure that you stay focused on what the task requires you to do, and only go as far as you need to get the flag; for example, do not spend time enumerating a range of services on a host if the task clearly only requires you to focus on a single protocol.

Pro tip: use grep or open your port scan outputs in a text editor to quickly search through large amounts of output. You can also use text editors to take notes and build a pool of information about your targets.

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. Once the exam time begins, it is usually a good idea to initiate bulk activities such as port scanning and vulnerability scanning that are known to take a certain amount of time.

Whilst these processes are running in the background, identify tasks that are straightforward to complete, so no time is lost whilst you wait on the scan results to come through.

A common mistake is to approach the exam as if it were a "capture the flag" style event with isolated vulnerabilities. Taking this approach to the exam, where each question is addressed individually in sequence, does not reflect real-life methodology. Therefore, if you adopt this approach, you are more likely to run out of time during the exam.

Everyone will come with different strengths and weaknesses, reflecting individual experiences. Your ability to work swiftly in one area may compensate for a lack of familiarity in others. The questions do not need to be taken in any particular order, and success in one area does not hinge on success in others. Once you have decided on a task, try to see it through, however if you are at risk of getting stuck, it may be prudent to move on to the next item. Whatever your chosen method, make best use of the time available, keeping overhead to a minimum.

Pro tip: use a new terminal for each new host, so all relevant output is in one place. You can also log the output of your terminal to search through it later.

Marks

Within the environment, you will encounter locked-down desktops, network awareness scenarios, vulnerability assessments, Windows domain environments, simple exploitations, routing manipulations, and vulnerable web applications. Certain tasks may come with additional background information, for added context. Be sure to take these into account.

You can collect up to a **total of 160 marks**, which are distributed as follows:

Infrastructure (100 marks)

- Network Awareness, 20 marks
- Vulnerability Assessment, 20 marks
- Simple Exploitation, 20 marks
- Desktop Lockdown, 20 marks
- Routing Manipulation, 20 marks

Web Application (60 marks)

Once you have acquired the appropriate flags, all you need to do is enter the flag text or required value in the designated space next to the question.

Pro tip: Burp Suite Professional (without extensions) will be available on the Kali machine. Practice combining Burp with tools with command line tools on Hack The Box or local virtual machines to automate certain activities.

Tools and notes

The new CRT exam does not allow candidates to bring their own testing machines into the test centre or use their own notes. Instead, candidates have access to a fully functioning virtual machine running Kali Linux, which is equipped with a wide array of standard tools. The exam version of Kali Linux can be accessed via the CRT Web Page.

Make sure to have a good understanding on how these tools work. You are strongly advised to familiarise yourself with the tools, which are entirely sufficient to successfully complete the exam. Any other tools available in Kali can also be used.

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 (eg using a different tool or method). It may also help your learning process to reproduce steps manually.

Pro tip: more importantly 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.

Final tips

Our best advice is that you apply the same approach to your exam as you would to a penetration testing engagement. If you have never been on a project before, this means understanding the scope and limitations of the environment, work through the tasks with a clear strategy in mind, and apply an iterative method to obtaining your results.

Also make sure that you are able to:

- **Scan a network** to identify live hosts, host names, and understand what makes your scans run quicker or slower, and what level of information you should expect to see (it may help to run several different scans which all produce different outcomes)
- **Identify network services** and protocols, including when they may be running on non-standard ports, understand what weaknesses may apply to the version identified, and whether they are encrypted or not
- **Enumerate available information** from network shares, web servers, web applications, operating systems, Windows domains and other available sources
- **Run an automated Vulnerability Assessment**, and interpret the results (blue findings may contain hidden gems)
- **Exploit** weaknesses and vulnerabilities (default passwords are sometimes just as effective as a reliable exploit). It may be required to change default parameters in exploit modules to get them working properly
- **Break password hashes** through the use of password crackers or password lists
- **Understand web applications**, including how the technology stack influences the vulnerabilities they are susceptible to, the role of cookies, various input validation weaknesses, and how to get the underlying web server to execute your commands

Obtaining flags in the desktop lockdown / kiosk environment do not require any external tools. Similarly to modern day attackers, all you need to do is embrace the "living off the land" approach.

Pro tip: Metasploit has a secondary superpower beyond exploitation of vulnerabilities; it can connect to a large number of services to act as a client, enumerate information, and can be used to brute-force credentials. Don't be afraid to experiment!

We hope that you found this guidance useful, remember to stay focused, and believe in yourself.

Best of luck with your CRT exam!