INVALUABLE ADVICE FROM A CREST ASSESSOR WHEN TAKING AN EXAM

The purpose of this document is to offer insight into the different CREST penetration test examinations, highlighting common areas where candidates struggle.

This article includes common themes across all of the examinations.

Purpose

The key purpose of CREST examinations is to measure the extent to which a candidate can perform tasks expected of them in a 'real life' engagement in a timely manner.

It is worth being aware that one of the most important skills of a penetration tester is being able to troubleshoot and very rapidly understand and apply their practice to new environments. The exams are set up, in varying degrees, to test this. For example, an exam question that relates to a specific operating system (for example, Solaris) is arguably less about the specifics of Solaris but more about the penetration tester's general knowledge of UNIX based operating systems and the ability to quickly identify attack vectors. Following this example, a privilege escalation vector based on abuse of 'sudo' is not usually operating system specific; the same underlying technique and theory would apply regardless of whether the OS was FreeBSD, Ubuntu or any other UNIX based operating system.

Time

One of the most common frustrations with CREST examinations expressed by candidates is time pressure. It is often felt that, in 'real life', there is more time available.

One of the considerations here is that the successful candidate is expected to be able to work in a timely manner. For example, a candidate who is technically able to perform a portscan of a single host but takes 10 minutes to correctly construct an *nmap* command is not working at a rate expected of an advanced infrastructure tester. The exam is not just measuring technical ability in isolation; it is measuring overall familiarity with tools, ability to troubleshoot common problems.

Marks

It is understandable that many candidates attempt to apply a level of 'exam technique', but this can be slightly problematic when it changes the way that you approach the environment. We often remind candidates to treat this, as much as possible, as a 'real life' scenario, the point being that there is often an expectation of parallel activity. For example, on an open scope infrastructure penetration test, you would not scan each host individually; background scans would be set up.

The marks allocated to the question are reflective of the time and effort needed to complete that question, which includes recognising the ability to use information obtained in previous questions.

Our advice is not to try and second-guess the mark scheme, but take the questions at face value. I have seen some candidates agonise over marks believing that the question is more complicated than it actually is.

Candidates are informed that the questions are built on a 'one minute per mark' principle. Remember that this is assuming that candidates will achieve full marks. The pass mark, depending on the exam, of our practical exams is between 60 and 67%, implying that a successful candidate actually has more than one minute per mark.

We also understand that candidates will have areas of strengths and weaknesses; this is a reflection of individual experiences which will be different for everyone. This is why there is such a variance across all of the certified penetration testing exams; for

example, the Web Applications examination tests a number of different web application vulnerabilities across a number of technologies, and the infrastructure exam tests everything – including locked down environments, UNIX machines, Windows networks and network infrastructure. You will have different areas of strength and weakness, and it is quite normal that you will complete some areas with ease and struggle with others. The ability to work quickly in one area can 'make up' for a lack of familiarity in other areas, and that is reflective of real life tests. If you struggle in all areas, it gives you an indication of the areas of work to brush up on before taking the exam.

Lastly with respect to time, it is worth highlighting that whilst you have 'more time' on a client engagement, the environments are also proportionally more complicated. For example, a week long penetration test may have several thousand hosts which may or may not be vulnerable to something; you only have a few hours during the exam, but the environment is proportionally smaller.

Documentation

Several years ago, the certified penetration testing (web applications and infrastructure) exams included a report writing section, which takes the form of a build review. This is something that was requested of CREST, because the ability to quickly document findings and present them in a clear way to clients has been highlighted as being particularly important and relevant to the industry.

Most candidates score extremely well at the vulnerability writeup section, although the candidates who score most highly write up vulnerabilities in a very clear and non-ambiguous way.

The other traditional sections of a report, including the management summary (executive summary) and technical summary are where some candidates struggle more than others. The key requirement here, as with real life, is to be able to translate technical findings into business impact; a board member is highly unlikely to understand the relevance of 'cross site scripting' but will often have explained where the key risk to the organisation is. For example, a very common concern is the loss of personal information which brings with it both legislative and reputational risks. The successful candidate is able to show the extent to which the technical results could result in those risks being realised. Candidates who produce reporting or documentation in this manner score extremely highly in this section.

Accuracy and Understanding

It is of course extremely important that all written material is accurate and has been applied to the scenario that is given. A common example of this is legislation; where relevant legislation is quoted (common examples in the UK include the Computer Misuse Act 1990 and the Data Protection Act 2018), it must be factually correct, but successful candidates are able to show how that legislation applies to the situation that they are presented with. Simply including it verbatim will attract far less marks than showing how it is relevant and its effect.

This is true of real life. For example, during a simulated attack, an understanding of the criminal and civil legislation is very important, but being able to factually recall it is not enough. You may have to make a decision about whether a phishing campaign is appropriate, or a particular technique is appropriate for a client. You need to be able to take the meaning of the legislation (and any established best practice), not just recite it out of context in order to obtain full marks. You aren't expected to quote it word for word from memory, but you are expected to have a good understanding of the meaning and effect of legislation.

Tooling

It is long established that you need to be familiar with tools, and being familiar with a tool is not the same thing as having used it once in a lab. Familiarity includes being able to troubleshoot common problems and being able to adapt it to a given situation. For example, the infrastructure exams often expect the ability to exploit known, publicly disclosed vulnerabilities. This should not be mistaken for being a 'metasploit exam', even though this is the tool that the majority choose to use.

The exams focus on outcomes (regardless of how they are achieved). Tool failure or unexpected behaviour is part of life, and the successful candidate will have performed all of these techniques in different environments, will understand pitfalls and be able to troubleshoot or debug them.

On a related subject, rebuilding your laptop for the exam is not a sensible idea. The reason you bring your own platform is so that you can do what you do in real life. Use an operating system and build that you know works, with the tools installed where you expect them to be.

Dechaining

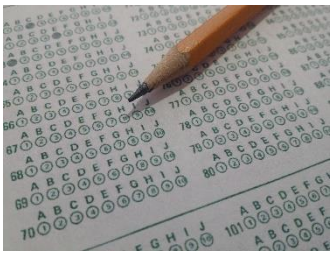
In the current certified examinations, it is unavoidable that a candidate will need to complete a first step in order to progress; an example would be obtaining code execution in an application before interacting with the underlying host.

In these situations, there is often an opportunity to 'dechain'; this refers to sacrificing the marks for the first question in order to progress.

This is one area where exam technique is important. If the first question is worth 10 marks (suggesting 10-15 minutes of time maximum) and you are struggling with it, it is worth 'dechaining' so that you can move on with the question to obtain the marks.

Nobody will 'know' whether you have dechained or not, and it is not a failing on your part. Sometimes the ego of penetration testers, along with the interest in problem solving, can be reasons why some are reluctant to. In this case, as with real life, it is important to prioritise time.

Question Paper



This may sound like a typical school phrase, but RTFQ (read the *full* question). There is nothing here to trick you, but some candidates don't answer the question that is being asked.

You have reading time before the exam starts for a reason!

With all practical exams, the exam paper needs to be downloaded from and uploaded to an SMB share, and needs to be electronically completed. It is assumed that every candidate will be able to configure their system to be able to do this. It is not part of the exam per se, but it is reasonable to expect everyone is of a technical level sufficient to read and write to a standard SMB/CIFS share.

Context

At certified level, most of the questions have some background information associated with them. This is to mirror 'real life' engagements; it is rare that a security review would be conducted without a client scope which contains within it boundaries (ie. areas to

avoid) and an understanding of what the client wants out of the engagement.

This is not designed to mislead or waste time, but to help you get into the mindset that is intended for that particular question.

Trick questions

For complete doubt avoidance, there are no trick questions or intentional traps. Most hosts start off as default configurations, with vulnerability pathways constructed as would be expected in real life. A common mistake is to treat the examination as a 'capture the flag' style event with isolated vulnerabilities. This is not really true of real life.

CRT

This is a practical examination that is designed to test network reconnaissance, infrastructure and application skills. There is a level of guidance in the examination as to the route to take and vulnerability scanners are of some help.

A common mistake is to treat each question in isolation; on a real network, you would scan the whole network and quickly parse the scan results when you needed them. Approaching the exam in serial (ie. treating each question individually and solving them in a serial manner) is not representative of any real life methodology, which is why you will more than likely run out of time during the exam if you take this approach.

CCT APP / INF / CCSAS

There is less guidance around the methodology to follow with these exams; for example, you may be asked to compromise a host but will not be told explicitly how to. Not every host on the network contains vulnerabilities.

This is not unreasonable; on real engagements, you would be presented with a network where some, but definitely not all, hosts will be vulnerable. Part of this is trusting your tool output, which means understanding how the tool works.

Tool failures are never intentional; there is nothing in the exam intended nor designed to catch you out or otherwise frustrate you. If a tool does not work properly, it is quite likely that this is related to the way the tool is being used.

Every question is solvable, in the time given.

CCSAM

This exam is all about risk assessment. A common approach by highly technical candidates is to approach each question as you would a technical exam.

In reality, this exam is about managing a STAR engagement. It is about understanding risk (to everyone involved). Knowledge of legislation is important, but it is as important to understand the effect of that legislation in the context of the question. For example, the exam expects you to be able to apply the Data Protection Act to a scenario and explain how it changes or affects the risk involved, not just factually recall it.

Key takeaways

- Read the full question, including the background information that is given.
- Understand how your tools work. Performing a technique once, in one CTF lab, is unlikely to be enough.
- Be aware of time; don't be afraid to 'dechain' or move on to another question. This is true in real life too; you have time constraints on real jobs.
- Don't try to second-guess the mark scheme. There's no tricks, just answer the questions as they appear.