Infrastructure Sample
Assault Course

CREST Certification Examination – Example Examination Paper

Infrastructure – Assault Course

This is an example of a CREST Certified Tester (Infrastructure) examination paper, designed to give candidates an understanding of the structure of the Assault Course component of the CCT Infrastructure examination.

Candidates should use this to aid examination preparation, but should **not** use this as an indication of the technical content and capability required. Candidates should refer to the syllabus to understand the breadth and depth of the required knowledge and capability.

Table of Contents

1 Introduction

You will be given 15 minutes before the assessment starts to read through the requirements for this part of the exam. You are not permitted to perform active attacks during this time.

The practical component lasts for 3½ hours. This is your time for you to manage as you see fit; that said, we have given suggested timings for each section which you may use as you wish, which will leave you with a little spare time at the end. Periodically, the invigilator will let you know how much time you have left.

We appreciate that there is a lot to do in the practical component; be careful not to spend too much time on one task so that you are forced to rush through others.

There is no requirement to complete individual sections in the order that they are given in this worksheet; feel free to complete them as you wish, provided that you do so within the allotted time.

Each phase of the test clearly states the deliverable required. Only deliverables provided in the format specified can be assessed so ensure that you carefully read the deliverable section and comply with the deliverable requirements.

In some sections, we have given hints to help direct you to the specifically vulnerable parts of individual hosts or subnets so that you do not waste time fruitlessly; **we advise that you follow these hints**, although you are free to ignore them. We also suggest that you maximise your available time by running time-consuming operations (e.g. port scans or bulk vulnerability assessment scans) in parallel with other tasks.

Many deliverables are passwords that you will need to recover (if they are in a reversible format) or crack (if they are in a hashed format). Precise details of password length and character set are given in the introduction of the specific section; **you may want to configure your password cracking tools accordingly**. You should answer "Blank Password" or words to that effect if you believe a password is blank. No marks will be awarded if the answer box is left blank. Where passwords or other credentials are case-sensitive on the target system, your answer must use the correct case.

2 Examination Paper

This examination paper is to be electronically completed and uploaded, in PDF format, before the end of the examination to **\\crestanswers\Practical**.

Some questions require additional evidence to be saved; this should be saved to **\\crestanswers\Practical**.

3 Rules of Engagement / Other Information

The rules and information below are designed to help you during the practical test, and prevent you from attacking the wrong targets or wasting time on hosts that will be much more difficult to attack successfully.

- You should be able to obtain an IPv4 address by DHCP in the range **172.30.253.150-159** and you must not attack systems outside **172.30.252.0/23** unless the question explicitly states otherwise.
- You should be able to obtain an IPv6 address using stateless address autoconfiguration.
- You may need to configure your DNS server manually to **172.30.253.10**.
- You may need to configure your DNS suffix manually to **crest.elements**.
- You may make any legitimate DNS queries to **172.30.253.10**.

All systems in the range 172.30.253.120-150 have been designated as business critical systems which are out of scope for ALL of your activities and MUST be excluded from scans, attacks and interaction.

Up to 10 marks may be deducted if ANY traffic (except legitimate DHCP broadcast traffic) from you is detected on these hosts. No tasks depend on them and there is no benefit in scanning, attacking or interacting with them. There are no further reminders of this requirement.

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. For example, you may need to exploit a vulnerability to gain normal user access before using a local privilege escalation vulnerability to gain root access. In these situations, **if you are unable to carry out the first step, ask the Invigilator, who will be able to give you the information you need**. You will not receive any marks for that task, but should be able to carry on further.

If it is not clear which hosts you are to attack for each of the sections, ask the Invigilator, who will be able to guide you.

4 Router / Network Assessment (35 marks, 35 minutes)

You have been asked to conduct a review of the networks and systems that are accessible on your network over both IPv4 and IPv6.

ID	Task	Deliverable
1	Identify an SNMP service running on one of the discovered hosts that makes use of an insecure community string.	Write down the IP addresses that responds to SNMP queries and the community string identified. *(2 marks)*
		IP Address
		Community String
2	Identify a router that can be used to access the subnet 10.2.2.0/24.	Provide the IP address of the router in the space below. *(5 marks)*
		Answer

ID	Task	Deliverable
3	Identify all active IPv4 hosts in the 10.2.2.0/24 subnet.	Provide the IP addresses of all IPv4 hosts that respond to ping. *(4 marks)*
		Answer
4	Identify IPv6 router traffic	Write down the router and advertised routes in the space below. *(6 marks)*
		Router
		Routes
5	After adding the appropriate route, retrieve the trophy from a web service running on saturn.crest.elements.	Write the trophy in the space below. *(8 marks)*
		Trophy

ID	Task	Deliverable
6	Actively intercept network traffic.	Obtain the trophy value from traffic between **moses.crest.elements** and **noah.crest.elements**. *(9 marks)*
		Trophy

5 Windows Desktop Privilege Escalation (35 marks, 35 minutes)

Zenicarna have developed a new desktop solution to allow third-party contractors to complete safety training associated with instruments and chemicals that are present in their labs. This training solution is referred to as IODINE and comprises a Microsoft Windows system which is executing a training application. When a contractor arrives onsite, they are given an initial briefing, provided with temporary credentials and then tasked with completing a compliance e-learning exercise using the IODINE training application. Contractors should not be able to interact with any other aspect of the desktop other than the training application.

Zenicarna have tasked you with a review of the IODINE solution to ensure that contractors are appropriately restricted and cannot access native Windows functionality. In order to provide a true assessment of the solution, they have provided the account below which has representative permissions of a typical training account provided to a contractor.

Username: `user` **Password:** `password` **IP:** `172.30.253.101`

ID	Task	Deliverable
1	Access the local file system.	Provide the volume label of the **D:\** drive. *(5 marks)* **Trophy**
2	Obtain the filename and path of the IODINE training executable file.	Write down the name and path of the binary file running the IODINE training application. *(4 marks)* **Path & Filename**

ID	Task	Deliverable
3	Identify the remote server and TCP port to which the IODINE application connects. .	Write down the active TCP connection established below. *(6 marks)*
		Server IP Address
		TCP Port
4	Gain control over the operating system	List all **enabled** administrative users on the host who are also members of the local group **PISTACHIO**. *(4 marks)*
		Users
5	Elevate privileges	Provide the last 6 characters of the password hash of the 'crest' user. *(10 marks)*
		Password Hash

ID	Task	Deliverable
6	Obtain the cleartext password from the above hash, which is in the format **/^[a-z][0-9]{5}$/** (one lowercase letter followed by 5 digits).	Write down the cleartext password. *(6 marks)*
		Password

6 Windows Host Assessments (70 marks, 1 hour 10 mins)

Zenicarna are in the process of acquiring a smaller research company. In order to allow researchers at both companies to share research efficiently, it has been decided that the networks of both companies should be integrated. In order to ensure that this does not undermine the security posture of the existing Zenicarna network, you have been tasked with reviewing the third-party network.

All hosts within scope of this assessment are located on the **172.30.252.0/25** range.

6.1 Initial Host

ID	Task	Deliverable
1	Identify valid credentials by responding to NBNS / LLMNR traffic on the network. **If you are unable to do this, you can request a valid set of credentials, but you will lose all 10 marks for Q1 regardless of any answers written down.**	Write down the username and plaintext password associated with the account. *(7 marks)*
		Username
		Password
2	Identify a system which accepts the credentials from Q1. Remember to attempt to authenticate using a variety of management protocols.	Write down the IP address and hostname of the system. *(8 marks)*
		IP Address
		Hostname

ID	Task	Deliverable
3	Identify patch levels.	Write down the date that the most recent operating system patch was applied to the host. (*3 marks*)
		Date
4	Elevate privileges using the above information.	Write down the last six characters of the hashed password associated with the user 'crest'. *(9 marks)*
		Hash Value

6.2 Second Host

ID	Task	Deliverable
5	Identify another Windows host which can be accessed using the hashes recovered from Q4. Remember to attempt to authenticate using a variety of management protocols. **If you are unable to do this, you can request the IP address and a valid set of credentials, however, you will lose all 17 marks for Q4 and Q5 regardless of any answers written down.**	Write down the username and IP address of the system which can be accessed *(4 marks for the IP address, 4 marks for username)*
		IP Address
		Username

ID	Task	Deliverable
6	Gain interactive access to the operating system.	Locate a text file containing the phrase 'TROPHY' on the local hard disk. *(5 marks)*
		Path
		Filename
6	Elevate privileges.	Obtain the filename of the KeePass file which is saved in the Administrator user's Documents folder. *(9 marks)*
		Filename
7	Crack the decryption password, which is in the format **/^[0-9]{7}$/** (7 digits). **If you are unable to do this, you can request the file and password, but you will lose all 19 marks for Q6 and Q7 regardless of any answers written down.**	Obtain the password to decrypt the KeePass file. *(6 marks)*
		Password

6.3 Third Host

ID	Task	Deliverable
8	Use the contents of the KeePass file from Q7 to locate a domain controller which accepts one of the sets of credentials. Remember to attempt to authenticate using a variety of management protocols.	Write down the IP address of the domain controller and the username which accepts those credentials. *(10 marks)*
		IP Address
		Username
9	Position for further compromise.	Provide the last 6 characters of the **RC4** **krbtgt** hash. *(5 marks)*
		Krbtgt hash (last 6 characters)

7 Unix Host: RADIUM (35 marks, 35 minutes)

You have been asked to assess a UNIX host, accessible at **radium.crest.elements.**

Unless otherwise specified, passwords to be cracked will be **6 numeric characters** (**/^[0-9]{6}$/**).

ID	Task	Deliverable
1	Obtain access as a non-root user.	Obtain valid credentials that allow interactive access to be gained, and identify the management protocol used to interact with the host. *(5 marks for username, 5 marks for password, 2 marks for protocol)*
		Username
		Password
		Protocol
2	Identify a non-standard binary which can be run by any user at an elevated level of privilege.	Provide the path and filename of the binary. *(5 marks)*
		Path & Filename

ID	Task	Deliverable
4	Locate a file.	Obtain the name of a file containing the case sensitive phrase ‘CRESTCREST’. *(4 marks)*
		Path & Filename
5	Elevate privileges.	Provide the contents of /root/trophy.txt. *(10 marks)*
		File Contents
6	Identify password reuse.	Provide a list of local users who all share the same operating system password. *(4 marks)*
		Usernames

8 Unix Host: SULFUR (35 marks, 35 minutes)

You have been asked to assess a UNIX host, accessible at **SULFUR.crest.elements.**

Unless otherwise specified, passwords to be cracked on SULFUR will be **5 lowercase alphabet characters** (**/^[a-z]{5}$/**).

ID	Task	Deliverable
1	Enumerate and identify accessible network services.	Perform a **full** TCP port scan of the server. Save the file to **\\crestanswers\sulfur.nmap** *(2 marks)*
2	Gain operating system access. **If you are unable to do this, you can request valid credentials, but you will lose all 12 marks for Q1 and Q2 regardless of any answers written down.**	Obtain the contents of '~/trophy.txt', and write down the username of the user who owns the file. *(5 marks for username, 5 marks for trophy)*
		Username
		Trophy
3	Elevate privileges **If you are unable to do this, you can request valid root credentials, but you will lose all 20 marks for Q1, Q2 and Q3 regardless of any answers written down.**	Obtain the last 6 characters of the root password hash. *(8 marks)*
		Filename

ID	Task	Deliverable
4	Hijack another user's privileges. **If you accidentally delete the keys from the keyserver, inform the invigilator who will be able to reload them for you.**	Identify another user who is running an SSH agent with keys that are loaded, and provide the number of keys that are loaded. *(3 marks)*
		Username
		Number of keys loaded
5	Identify opportunities for further compromise.	Authenticate with another UNIX host using one of the keys. *(7 marks)*
		IP Address
		Key Thumbprint
6	Using **all available** operating system credentials from SULFUR, authenticate with the management service accessible on 127.0.0.1 of the other UNIX host.	Provide the trophy value embedded in the service output. *(5 marks)*
		Trophy