Infrastructure Sample Scenario

CREST Certification Examination – Example Examination Paper

Infrastructure – Scenario

This is an example of a CREST Certified Tester (Infrastructure) examination paper, designed to give candidates an understanding of the structure of the Scenario 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

Infrastructure Sample Scenario

1 Introduction

You will be given **15 minutes** before the examination starts to read through the requirements for this part of the exam. This is purely for you to get familiar with the requirements of the scenario component of the Infrastructure Certification Examination; no examination activities are permitted during this time.

The infrastructure examination comprises two parts; this is the first and requires you to complete a scenario question which involves practical work and reporting, based on the concept of a build review. The second part, which you will attempt after this one, is based on a practical penetration test. You must achieve the minimum pass mark in both parts.

There is no requirement to complete the 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.

You should upload your deliverables to **\\crestanswers\written** before the end of the examination, and are advised to save your work as you go along.

1.1 Marking

Written answers to these questions should be of a similar quality to a report supplied as a client deliverable by a CREST company. Candidates should be aware that the following will not attract marks:

- Lack of a form and style of writing appropriate to purpose, or appropriate to the audience.
- Unclear or ambiguous answers.
- Incorrect technical information (e.g. incorrect findings or incorrect terminology)
- Poor sentence construction.
- An excessive number of spelling or grammatical errors, or casual language which would not be suitable in a professional report.
- Overly vague, generic, incorrect or irrelevant content included as part of the answer which adds no meaningful value to the report.
- An absence of contextualisation of the findings.

1.2 Late Delivery Penalty

You have 150 minutes to complete the scenario portion of this exam including delivery of your output. It is suggested you ensure that you can deliver the output as required prior to the end of the 150 minutes.

Output submitted after the 150 minutes elapses is subject to a penalty (5 marks per minute overdue). You may also lose access to **\\crestanswers\written** after this time, so ensure that any deliverables have been correctly saved in good time.

2 Rules of Engagement

2.1 Infrastructure

The purpose of the rules and information below is to help you during the examination, 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 – this will be in the range **172.29.240.0/20** and you must **not** attack systems outside this range.
- You may need to configure your DNS server manually to **172.29.253.254**.
- You may need to configure your DNS suffix manually to **elements.crest**.
- You may make any legitimate DNS queries to **172.29.253.254**.
- The examination answers host (**\\crestanswers**) is provided for you to upload your responses. There is nothing to be gained by attempting to compromise this host; no correct answers are stored on it. It is simply a file share designed for electronic submission of your examination answers.

For this part, you may ONLY interact with:

- The DHCP server (legitimate DHCP traffic only)
- The DNS server (legitimate DNS queries only)
- The host that you have been specifically asked to review.
- The examination answers share (\\crestanswers) - legitimate requests only.

No interaction is permitted with ANY other system or IP address.

Any other interaction may result in immediate termination of your examination.

3 Scenario Question (150 marks, 150 minutes)

3.1 Background

Zenicarna, a fictional pharmaceuticals company, have engaged you to conduct a build review against one of their corporate laptops for compliance purposes. All systems are reportedly built in an identical manner from a "Gold" image and are configured with identical software and policies. These images were built and configured quickly in response to the pandemic in 2020, with Zenicarna having to quickly adopt a 'working from home' model in which the laptop connects to the corporate network over a VPN. As these laptops are in widespread use and have been since 2020, Zenicarna would like to urgently understand their current level of risk.

Employees are not given administrative access to the laptop; they are provided with low privilege user accounts.

3.2 Test Objectives

Zenicarna would like a review of one of their workstations which is based on their Gold image. They are particularly concerned that compromise of one of these systems could allow attacks against their wider corporate environment, especially because these laptops will be connected to domestic or otherwise untrusted networks. Specifically, Zenicarna would like to understand if compromise of a corporate laptop would facilitate or allow a malicious user to:

- Gain local administrative privileges to the laptop;
- Gain access to the laptop remotely (for example from an employee's home network); or
- Gain access to information which could allow wider attacks against the internal environment.

Zenicarna understand that, due to the timescales and notice, a full security review is not viable. In order to help you focus your efforts, they have informed you that vulnerabilities exist in the areas below and would like to understand more about them. They will need technical investigation and contextualisation to enable Zenicarna to fully understand their impact.

- Excessive network services which are available to other hosts on the network.
- A lack of regular patching.
- System service binaries whose ACLs are overly permissive.
- Weak configurations issues relating to the VPN client in use.
- Credentials being stored in an insecure manner.

Zenicarna have created a 'pentest' account with administrative privileges, and a 'user' account with permissions representative of a standard employee. These accounts have been created with a simple password to facilitate the assessment and will be disabled at the end of the engagement.

3.3 Reporting

Zenicarna expect a report in PDF format to be delivered at or before the deadline containing the sections below:

- A management summary, intended for Zenicarna's Head of Compliance (HOC). This role ultimately owns and is accountable for Zenicarna's risk. The HOC would like to understand the strategic themes and requires the technical findings to be translated into business risk. In particular, she would like to understand the extent to which the vulnerabilities would allow achievement of the objectives, and the underlying root causes. She is **not** a technical specialist and is very keen that the entire report is contextualised to Zenicarna's situation.
- A technical summary, intended for Zenicarna's Desktop Team Lead, who has a technical background and is responsible for the overall delivery of the Gold images. A description of any attack paths, explaining how a combination of vulnerabilities could form a path which results in systemic compromise or achievement of the objectives, would be extremely welcome.
- Vulnerability descriptions, intended for Zenicarna's system administrators, who will need a clear technical understanding of any issues that you discover. They require clear instructions on how to replicate and exploit any issues that you discover and specific recommendations. The content must be sufficiently detailed to allow a technically competent individual who does not have prior knowledge of this particular issue to be able to understand and reproduce it.

3.4 Answer

Your answers should be delivered as a single client report which contains, as a minimum, each of the deliverables detailed in section 3.6, and should be uploaded to **\\crestanswers\written** before the end of the examination as **scenario.pdf**.

A report template layout which is detailed in section 3.7. If you use report generation software or have corporate reporting templates, you may use them as long as the output is presented in a similar format and meets all criteria. Additional unrelated content included due to the reporting software or template will be disregarded without penalty as long as it is possible to easily identify the elements that are requested section 3.6.

You must present your report as an **A4 PDF** which does not include active scripting or other dynamic content. No other format will be accepted.

3.5 Server Details

Server Type	Remote Desktop Service
Server FQDN	workstation.zenicarna.com
Admin Username	pentest
Admin Password	pentest
Employee Username	user
Employee Password	user
Management method	RDP (TCP port 3389)

3.6 Tasks (145 marks)

ID	Task	Marks
1	Identify two separate 'high risk' vulnerabilities and document them. Your documentation for each issue should include: • A technical description of the issue. • Reproduction instructions. • Supporting evidence (e.g. screenshots or code output with the relevant part clearly marked) • Recommendations or remedial action.	50 marks (25 marks each)
2	Identify one 'medium risk' vulnerability and document it. Your documentation for each issue should include: • A technical description of the issue. • Reproduction instructions. • Supporting evidence (e.g. screenshots or code output with the relevant part clearly marked) • Recommendations or remedial action.	25 marks
3	Identify one 'low risk' vulnerability and document it. Your documentation should include: • A technical description of the issue. • Reproduction instructions. • Supporting evidence (e.g. screenshots or code output with the relevant part clearly marked) • Recommendations or remedial action.	25 marks
4	Provide a technical summary of your findings. Simply duplicating the answers to tasks 1-3 will not attract high marks.	20 marks
5	Provide a management summary (an executive summary) of your findings. Simply duplicating the answers to tasks 1-4 will not attract high marks.	25 marks

3.7 Report Deliverables (5 marks)

This section provides an example of the report format that is required. You are free to use any reporting software or adjuncts provided that the output is generated in the format and structure below. Key requirements for the report include:

- The report must contain page numbers.
- The author must be named on the report.
- There must be clear sections that relate to the tasks and deliverables in section 3.4.
- There must be a table which allows the documentation for each vulnerability to be clearly identified. This can be by using a unique section number or a page number, but it must be possible to quickly and intuitively cross-reference or find specific vulnerabilities.
- It must be exported in PDF format and uploaded to **\\crestanswers\written** before the end of the examination as **scenario.pdf**. It cannot be dynamic (i.e. it cannot include or rely on active scripting).

Infrastructure Sample Scenario

An example of the report structure required is shown below. Note that the spacing between each of the sections **is not indicative of the level of detail or length of answer required**:

Page 1 of 2 Candidate Name

Contents

Management Summary

Answer here.

Technical Summary

Answer here.

Name	Rating	Page
Vulnerability 1 Name	HIGH	2
Vulnerability 2 Name	HIGH	2
Vulnerability 3 Name	MEDIUM	2
Vulnerability 4 Name	LOW	2

Vulnerability 1 Name (High Risk)

Vulnerability 2 Name (High Risk)

Vulnerability 3 Name (Medium Risk)

Vulnerability 4 (Low Risk)