Application Sample
Assault Course

CREST Certification Examination – Example Examination Paper

Application – Assault Course

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

Application Sample Assault Course

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.

Some 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 trophies 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 172.30.253.120-149 inclusive 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 Slough Admirers Society (50 marks, 50 minutes)

This question requires you to review the application security of the following application:
https://sloughadmirers.crest.elements

ID	Task	Deliverable
1	Application Crawling	Provide a site map of the application. Save the file to **\\crestanswers\sloughadmirers.txt** *(2 marks)*
2	Identify Authentication opportunities	Identify all login interfaces and list them below *(5 marks)*
		Login Interfaces:

ID	Task	Deliverable
3	Identify valid users in the application	Identify a weakness in the login interfaces and provide a list of valid usernames. *Note: usernames are all lowercase and up to a maximum of 3 characters long.* *(5 marks)*
		Interface(s) with vulnerabilities: **Name of vulnerability:** **Valid Users Discovered:**
4	Compromise an account	List any weak account credentials discovered *(5 marks)*
		Credentials discovered (username/password):

ID	Task	Deliverable
5	Identify a vulnerability in the application	Log into the application, test the security of the application and identify a vulnerability. (10 marks)
		Name of vulnerability: **Name and location of vulnerable field:** **Rating / Severity of vulnerability:** **Evidence to confirm vulnerability:**
6	Exploit the vulnerability to obtain further access	Use the vulnerability you have identified to confirm how passwords are stored in the database. *(8 marks)*
		How passwords are stored:

ID	Task	Deliverable
7	Escalating Privileges	Using the vulnerability you identified as an entry point, retrieve the contents of the file located at C:\CREST\Trophy.txt and write it below. (15 marks)
		Trophy:

5 Super Sweep (15 marks, 15 minutes)

This question requires you to review the application security of the following application:

https://bargainsforall.crest.elements

ID	Task	Deliverable
1	Identify the infrastructure in use	Identify the web server technology running as well as the underlying operating system in use. *(5 marks)*
		Web Server: **Underlying Server OS:**
2	Vulnerability identification	Identify a vulnerability in the application and note the relevant details below. *(5 marks)*
		Name of vulnerability: **Steps to exploit the vulnerability:**

ID	Task	Deliverable
3	Exploit the vulnerability	Using the identified vulnerability, execute an action which results in money being sent to you and write the trophy provided on confirmation screen below. *(5 marks)*
		Trophy:

6 X Rated (70 marks, 1 hour 10 mins)

This question requires you to review the application security of the following application:

https://x-rated.crest.elements

ID	Task	Deliverable
1	Identify the port the application listens on. **If you are unable to do this, you can request the answer, but you will lose all 2 marks for Q1 regardless of any answers written down.**	Write down the port number the application is running on below. *(2 marks)* **Port:**
2	Discover valid credentials for the application. **If you are unable to do this, you can request the answer, but you will lose all 3 marks for Q2 regardless of any answers written down.**	Examine the web application pre-authentication and retrieve a valid set of credentials, noting them below. *(3 marks)* **Username:** **Password:** **Location Identified:**

ID	Task	Deliverable
3	Login and identify a vulnerability **If you are unable to do this, you can request the answer, but you will lose all 10 marks for Q3 regardless of any answers written down.**	Identify a vulnerability in the application and note the relevant details below. *(10 marks)*
		Name of vulnerability: **Name and location of vulnerable field:** **Evidence to confirm vulnerability:**
4	Obtain a file on the local system using the identified vulnerability.	Using the identified vulnerability retrieve the contents of /crest/trophy.txt and write it below. *(10 marks)*
		Trophy:
5	Obtain interactive access using the identified vulnerability.	Using the identified vulnerability, retrieve the trophy in the environment variable of the server named "CREST_Trophy", writing it below. (20 marks)
		Trophy:

ID	Task	Deliverable
6	Identify the user the web server is running as.	Using the access obtained, identify the user the web server is running as and write it below. (5 marks)
		User:
7	Password hash retrieval and cracking The password set meets the following regex: **/^[A-Z][a-z][a-z]\d\d$/** One uppercase character followed by 2 lowercase characters followed by 2 digits.	Using the access obtained, retrieve the password hash of the user the server is running as, identifying the hash type and obtain the user's plaintext password. (10 marks)
		Hash: **Hash type:** **Plaintext Recovered Password:**

ID	Task	Deliverable
	Analyse the source code of the application	Using the obtained access to the server hosting the application, locate the source code and identify what language the application is written in, writing the answers below. (10 marks)
		Directory hosting source code: **Language application written in:**

7 Who Am I (35 marks, 35 minutes)

This question requires you to review the application security of the following application:

https://identifyme.crest.elements

ID	Task	Deliverable
1	Login using the credentials below, and evaluate session security **User: pineapple** **Password: pizza**	Identify the cookies used in authenticating the user post authentication. (2 marks)
		Authentication Cookie name:
2	Obtain access as another user	Identify a vulnerability in the cookie creation process, exploit this to login as the user *pepperoni*, retrieving the trophy from the welcome page returned. *(8 marks)*
		Name of vulnerability: **Trophy:** **Exploitation steps:**

ID	Task	Deliverable
3	Gather information on the pineapple user.	When authenticated as the pineapple user, review their profile page and obtain the information requested below. *(5 marks)*
		Where was Pineapple's profile photo taken? **What device was Pineapple's profile photo taken with?** **What's Pineapple's printer name?**
4	Steal the session of an unknown user	Craft a URL which exploits a session vulnerability to obtain access to a third party's session. Write down the user who has been compromised below. *(10 marks)*
		Username of compromised session:

ID	Task	Deliverable
5	Obtain unauthorised access to the API	Interact with the API, identify how the authentication works and gain access. Write the trophy down below. *(10 marks)*
		Authentication technology: **Trophy:**

8 Deployed and Landed (40 marks, 40 minutes)

This question requires you to review the application security of the following application:

https://bracebracebrace.crest.elements

ID	Task	Deliverable
1	Identify a code injection vulnerability **If you are unable to do this, you can request the answer, but you will lose all 10 marks for Q1 regardless of any answers written down.**	Describe the vulnerability. *(10 marks)* **Name of vulnerability:** **Name and location of vulnerable field:** **Evidence to confirm vulnerability:**

ID	Task	Deliverable
2	Exploit the vulnerability and circumvent any defences	Exploit the identified vulnerability to retrieve /etc/passwd on the server, noting any defence mechanisms that had to be overcome. (10 marks)
		/etc/passwd output: **Defensive mechanisms encountered:** **Bypass technique:**
3	Compromise another user	Using the access obtained, compromise the session of another user, browse to their welcome page and write down the trophy below. (20 marks)
		Trophy: