CREST. Representing the technical information security industry

Assessors Panel

CREST Registered Security Analyst Certification Examination

Notes for Candidates

This document and any information therein are confidential property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retain the right to alter the document at any time unless a written statement to the contrary has been appended..

Contents

1. Introduction

1.1. Examination

The CREST Registered Security Analyst (CRSA) examination tests candidates' knowledge in assessing operating systems and common network services at an intermediate level below that of the main penetration testing Certified qualifications. The CRSA examination also includes an intermediate level of web application security testing and methods to identify common web application security vulnerabilities.

The examination covers a common set of core skills and knowledge. The candidate must demonstrate that they can perform an infrastructure and web application vulnerability scan using commonly available tools and interpret the results to locate security vulnerabilities.

Exam success, in addition to valid CPSA certification, will confer CREST Registered Security Analyst status to the individual.

The CREST Registered Security Analyst qualification is valid for three (3) years.

The Examination has one component: a practical assault course. The practical assessment tests candidates' hands-on penetration testing methodology and skills against reference networks, hosts and applications.

1.2. Confidentiality

CREST takes the confidentiality of the Examination very seriously. The retention or dissemination of data relating to the CREST Examination (other than what is contained in the Notes for Candidates and Technical Syllabus documentation that is available from the CREST web site http://www.crest-approved.org/) is not permitted: candidates will be required to accept a Non-Disclosure Agreement to this effect at the start of the Examination.

2. Examination Details

2.1. Examination Timings

The examination will last 2.5 hours.

Note that the permitted maximum session time at Pearson Vue is 3 hours in total, allowing time to read the Code of Conduct and also to provide feedback following the examination.

2.2. Practical Assault Course

2.2.1 Open Book / Closed Book

The practical assault course is conducted as a completely closed book process, reference material or access to the Internet is not permitted. Interactive chat or message systems are not permitted.

2.2.2 Format

The practical component of the CRSA Examination will comprise a series of stages, split into structured tasks to be carried out against the CREST CRSA Network and the target hosts, infrastructure and applications that it comprises. Please note that the practical components are not designed as replicas of “real world” security assessment engagements; rather, they are examinations whose aim is to test the skills and knowledge that security consultants and penetration testers will need to carry out effective security assessment engagements.

As noted above, stages and tasks are designed to examine fundamental infrastructure and web application penetration testing skills at an intermediate level below that of the main Certified level qualifications; candidates will be required to complete all of them. Success at each question or task is based on an item or items of information that the candidate must retrieve, acquire or derive from the target applications or infrastructure in order to establish the correct answer. The practical components have been designed so that success at each question or task does not depend on success at other questions or tasks.

The assault course is split into the following sections:

- 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

2.2.3 Candidate Platform

During the exam candidates will be provided with desktop access to a virtual machine running Kali Linux that can be used to perform the required tasks. This machine has a large number of tools installed including licensed versions of Nessus Professional and BurpSuite Professional.

A version of this virtual machine without the commercial licenses can be downloaded by candidates so they can familiarise themselves with the platform prior to the exam. This can be downloaded from the following location:

https://candidate-downloads.crest-approved.org/crsa/kali

2.2.4 Infrastructure Assessment Details

The practical assault course contains sample equipment that would typically be found in a real-world test of a medium to large size organisation. Candidates will be expected to demonstrate their capabilities in and competency at:

- Assessing network devices such as switches and routers
- Assessing hosts running Windows operating systems
- Assessing hosts running Unix and Linux (both commercial and open source) operating systems
- Assessing locked down desktop environments
- Assessing IP networks

Knowledge gained will need to be used in an intelligent manner to demonstrate a good understanding of the technologies in use and their implications as well as simply being able to run tools and scripts.

For further information on the skills being assessed, consult the Technical Syllabus.

The subsections that are covered in the infrastructure stage are as follows:

Network Awareness

Candidates will be required to identify hosts and services on an IP network, to enumerate basic information, and to interact with basic services.

Vulnerability Assessment

Candidates will be required to find vulnerabilities that might typically be identified by vulnerability scanners and exploit them to extract related information.

Simple Exploitation

Candidates will be required to exploit systems and services in order to obtain key pieces of data, such as emails, passwords, or data from a database.

Desktop Lockdown

Candidates will be given access to a restricted desktop environment. They will be required to bypass the restrictions in order to collect specific data.

Routing Manipulation

Candidates will be required to understand and interact with IP networks in order to access systems and services that would otherwise be inaccessible.

2.2.5 Web Application Assessment Details

The application assessment consists of multiple simple web applications. The web applications will be based on common web application technologies hosted on Windows and Unix platforms.

Pages have been designed to provide the candidate with a series of generic vulnerabilities to find, assess and exploit.

2.3. Invigilation

An invigilator will be present throughout the examination. The invigilator is not there to assess candidates' capabilities; all assessment is via the objective written and practical components. However, the invigilator will be able to answer any procedural questions that candidates may have, and assist in troubleshooting.

3. Marking Scheme / Pass Mark

The marking scheme is given in the table below:

Component	Total Marks
Practical Assault Course – Infrastructure	100
Practical Assault Course – Web Application	60
Total	160

Successful candidates must score 60% of the available marks in each component. That is:

at least **60 marks** from the **Assault Course – Infrastructure** (possible total: 100 marks), and

at least **36 marks** from the **Assault Course – Web Application** (possible total: 60 marks).

This represents an overall pass mark of approximately 60%, but note **that candidates must score the minimum number of marks in each section: candidates who score very well in one component but not the other will not pass.**

Unsuccessful candidates will be told their final scores in the Infrastructure and Web Application components, if they achieved a lower mark than 60%.

4. Examination Logistics

4.1. Location

These examinations are delivered at a Pearson Vue centre that meets the technical requirements for this examination, of your choice. Please visit www.pearsonvue.com and follow the on-screen instructions to schedule your examination.

4.2. Before the Examinations starts

Before the Examination starts, candidates will:

- **Have to sign an NDA**. This is to help us maintain the confidentiality of the Examination.
- Have to sign the **CREST Code of Conduct**.

Communication of Results

Examination results will be emailed to the candidate within 30 working days of the examination. Digitally signed certificates, where appropriate, will be emailed to candidates.

5. Example questions

5.1. Example Network Awareness Question

An example question is given below, along with the answer.

5.1.1 Question (2 Marks)

Find the box named jaguar and identify what domain it resides in.

Provide the NetBIOS domain name.

5.1.2 Answer

The correct answer is “bigcats”.

5.1.3 Marking scheme

Each answer is worth one (1) or two (2) marks. No points are deducted for incorrect answers.

5.2. Example Vulnerability Assessment Question

An example question is given below, along with the answer.

5.2.1 Question (2 Marks)

Identify a valid user on the host named monkey that is also in the /home/kali/Desktop/Candidate/wordlist.txt file.

5.2.2 Answer

The correct answer is “janet”.

5.2.3 Marking scheme

Each answer is worth two (2) marks. No points are deducted for incorrect answers.

5.3. Example Simple Exploitation Question

An example question is given below, along with the answer.

5.3.1 Question (5 Marks)

Exploit 10.0.1.27 and provide the trophy value from a file with 'trophy' or 'secret' in its name.

5.3.2 Answer

The correct answer is “trophy-12345”.

5.3.3 Marking scheme

Each answer is worth five (5) marks. No points are deducted for incorrect answers.

5.4. Example Desktop Lockdown Question

An example question is given below, along with the answer.

5.4.1 Question (10 Marks)

Find the 'zenicarna' file and provide the trophy value.

5.4.2 Answer

The correct answer is “trophy-54321”.

5.4.3 Marking scheme

Each answer is worth ten (10) marks. No points are deducted for incorrect answers.

5.5. Example Routing Question

An example question is given below, along with the answer.

5.5.1 Question (10 Marks)

Attempt to access the telnet server on 172.20.31.10 via 172.17.89.254 and obtain the value in the service banner.

5.5.2 Answer

The correct answer is “trophy-98765”.

5.5.3 Marking scheme

Each answer is worth ten (10) marks. No points are deducted for incorrect answers.

5.6. Example Web Application Question

An example question is given below, along with the answer.

5.6.1 Question (10 Marks)

Zenicarna has deployed a new authentication mechanism to replace the previously unsecured portal.

Host: 10.0.1.180 Port: 8080

Attempt to gain access and provide the trophy value presented upon successful authentication.

5.6.2 Answer

The correct answer is “trophy-11122”.

5.6.3 Marking scheme

Each answer is worth from two (2) to fifteen (15) marks. No points are deducted for incorrect answers.

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press / Public Relations: media@crest-approved.org

www.crest-approved.org