Assessors Panel

CREST Intrusion Analysis Certification Examinations – Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	C-IAM-CN01
Version Number	3.7
Status	Public Release
Issue Date	6 June 2019
Review Date	August 2019

Table of Contents

1. INTRODUCTION

1.1 Examination

The CREST Practitioner Intrusion Analyst (CPIA) examination has one component: a multiple choice written question section.

The CREST Registered Intrusion Analyst examination has one component: a multiple choice practical question section. All candidates must hold a valid CPIA certification to be eligible to sit this examination.

The CREST Certified Intrusion Analyst examinations have two components: a written component and a practical component.

There are three parallel tracks of the CREST Intrusion Analyst Certification examinations. Practitioner and Registered examinations cross all three syllabus areas while Certified examinations specialise in one track. Candidates can only sit one examination track at a time.

For all tracks, the qualification is valid for three (3) years. Success at the one of the examinations above will confer upon candidates the status of one of the following:

1.1.1 CREST Practitioner Intrusion Analyst (CPIA)

The (CPIA) examination tests a candidates' knowledge across all 3 specialist subject areas at a basic level below that of the CREST Registered examination.

1.1.2 CREST Registered Intrusion Analyst (CRIA)

The (CRIA) examination tests a candidates' knowledge across all 3 specialist subject areas at an intermediate level. A valid CPIA certification is a prerequisite to this examination.

1.1.3 CREST Certified Network Intrusion Analyst (CCNIA)

The (CCNIA) examination tests candidates' knowledge and expertise in analysing data sources for evidence relating to potential network compromise.

1.1.4 CREST Certified Host Intrusion Analyst (CCHIA)

The (CCHIA) examination tests candidates' knowledge of analysing Windows hosts for evidence of potential compromise.

1.1.5 CREST Certified Malware Reverse Engineer (CCMRE)

The (CCMRE) examination tests candidate's ability to reverse engineer malware, particularly remote access trojans.

1.2 Confidentiality

CREST takes the confidentiality of all examinations very seriously. The retention or dissemination of data relating to the CREST examinations (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: along with their booking forms, candidates must also send a signed Non-Disclosure Agreement to this effect or be prepared to sign a Non-Disclosure Agreement in the morning before they start the examination. It should be noted that prior knowledge of specific examination configurations will be of little use to candidates, as the examination is constantly updated and revised.

2. EXAMINATION DETAILS (CPIA)

2.1 Format

The CREST Practitioner Intrusion Analyst examination is delivered at Pearson Vue Centres. Please visit www.pearsonvue.com and follow the on-screen instructions to schedule your chosen examination. Note the logistical requirements for exams conducted at a Pearson Vue centre are defined by Pearson Vue and candidates must ensure they adhere to all the necessary requirements as listed on their website. CREST candidates are not exempt from any of the standard requirements.

The CPIA examination comprises one hundred and twenty (120) multiple choice questions, all of which the candidate must complete Details of the areas covered can be found in the Syllabus document.

2.2 Timings

The examination lasts 2 hours.

Note that the permitted maximum session time at Pearson Vue is 2.5 hours in total, allowing time to read the Code of Conduct and also to provide feedback following the examination.

2.3 Open Book/Closed Book

The exam 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.

3. EXAMINATION DETAILS (CRIA)

3.1 Format

The CREST Registered Intrusion Analyst exam is a practical examination delivered at CREST Examination Centres comprising multiple-choice questions weighted according to difficulty.

Stages and tasks are designed to examine fundamental intrusion analyst testing skills; 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 provided files.

All candidates must hold a valid CPIA certification. Exam success in addition to valid CPIA certification will confer CREST Registered Intrusion Analyst status to the individual.

3.2 Timings

The examination lasts 2.5 hours in total.

3.3 Open Book /Closed Book

The examination is an open book test: candidates will be permitted to use reference material and Internet access will be available

4. EXAMINATION DETAILS (CCNIA / CCHIA / CCMRE)

4.1 Written Component – CCNIA / CCHIA / CCMRE

4.1.1 Format

These CREST Certified-level examinations are delivered at CREST Examination Centres.

The written component will comprise one hundred and fifty (150) multiple choice questions, all of which the candidate must complete.

A pass in the written component of the examination is a pre-requisite to taking the practical component.

4.1.2 Timings

The written examination will last 2.5 hours and you should attempt to answer all questions within this time.

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

4.1.3 Open Book / Closed Book

The entire written component of the CCHIA exam will be conducted as a closed book exercise.

4.2 Practical Component - CCNIA / CCHIA / CCMRE

4.2.1 Format

The practical component the CREST Certification Examination will comprise a series of stages, split into structured tasks to be carried out. Please note that the practical components are not designed as replicas of “real world” intrusion analysis 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 intrusion analysis engagements.

4.2.2 Timings

The practical component will last 4.5 hours

4.2.3 Open Book/Closed Book

The practical is an open book test: candidates will be permitted to use reference material, and, although the CREST Certification Network is not directly connected to the Internet, Internet access will be made available if required. Candidates will be given the practical component worksheet fifteen (15) minutes before the start, to allow its perusal before the examination starts.

5. SUBJECT SPECIFIC NOTES

5.1 CREST Practitioner Intrusion Analyst

The CPIA assessment covers areas from all three syllabus areas at a basic level below that of the CREST Registered examination.

5.2 CREST Registered Intrusion Analyst

The CRIA assessment covers areas from all three syllabus areas highlighted above at intermediate level and is aimed to show a breadth of knowledge as opposed to a depth of knowledge in a subject.

5.3 CREST Network Intrusion Analysis (NIA) Examination

The NIA assessment been designed to provide the candidate with a series of generic network intrusions to find, assess and understand.

Candidates will be expected to demonstrate knowledge and expertise in the following areas:

Syllabus area	Syllabus area description
A2	Incident Chronology
A4	Record Keeping, Interim Reporting & Final Results
B4	OS Fingerprinting
B5	Application Fingerprinting
C2	DNS
C4	Extraction of Document Meta Data
D1	Network Traffic Capture
D2	Data Sources and Network Log Sources
D3	Network Configuration Security Issues
D4	Unusual Protocol Behaviour
D5	Beaconing
D6	Encryption
D7	Command and Control Channels
D8	Exfiltration of Data
D9	Incoming Attacks
D10	Reconnaissance
D11	Internal Spread and Privilege Escalation
D12	Web Based Attacks
D13	False Positive Acknowledgement

For further information see the full Technical Syllabus.

Candidates will be expected to analyse network traffic covering these areas as directed by their candidate's worksheet, providing the results onto the supplied media for later review by the Invigilator.

5.4 CREST Host Intrusion Analysis (HIA) Examination

The practical examination for the HIA assessment provides controlled example test scenarios of host and artefact analysis.

Given the time constraints of the examination, there are no requirements to image any device, to perform complex string searches on large images or otherwise perform complex file carving.

The areas of the Technical Syllabus that are covered in the Practical assessment are as follows:

Syllabus Area	Syllabus Area Description
A1	Engagement Lifecycle Management
A2	Incident Chronology
A5	Threat Assessment
Appendix B	Generic Knowledge
Appendix C	Generic Knowledge
Appendix D	Generic Knowledge
E1	Host-based Data Acquisition
E2	Live Analysis Laboratory Set-up
E3	Windows File System Essentials
E4	Windows File Structures
E5	Application File Structures
E6	Windows Registry Essentials
E7	Identifying Suspect Files
E9	Memory Analysis
E10	Infection Vectors
E11	Malware Behaviours and Anti-Forensics
E12	Rootkit Identification
E13	Live Malware Analysis
E14	Linux OS File Structures

For further information see the full Technical Syllabus.

5.5 CREST Malware Reverse Engineering (MRE) Examination

The practical examination for the malware reverse engineering assessment contains examples of Windows malware that might typically be found on a compromised system. Candidates will be expected to demonstrate their capabilities in and competency at:

- Static binary analysis of unknown samples
- Behavioural analysis of malware on target
- Reverse engineering of binary executables
- Identifying important functionality efficiently
- Process debugging
- Identifying and inspecting network command and control protocols
- Binary unpacking and modification

The areas of the Technical Syllabus that are covered in the malware reverse engineer assessment are as follows:

Syllabus area	Syllabus area description
D6	Network Traffic Analysis
F1	Windows Anti-Reverse Engineering
F2	Functionality Identification
F6	Cryptographic Techniques
F7	Processor Architectures
F8	Windows Executable File Formats
F11	Binary Obfuscation
F12	Behavioural Analysis

For further information see the full Technical Syllabus.

Pre-Requisites
To successfully perform the assessment the following key pre-requisite should be met by the candidate, along with the relevant too/software prerequisites:

- Access to a Microsoft Windows client operating system, Windows XP SP2 and above, Vista, Windows 7 or Windows 10. Note: This can be a virtualised environment; all samples are expected to operate correctly if run within a virtual machine.

To aid the assessment process, the candidate might also find the following information useful to have localised access to (Internet access will be limited):

- Windows API Reference
- X86 Assembly Language Reference
- Programming tools
- Microsoft Windows public symbol repository

5.6 Recommended Tools

This following provides guidance on the areas that the technical exams cover, with some examples of tools that perform specific functions that maybe useful in the exams. Note that the tools and areas may not apply to all exams.

PCAP

- Wireshark: https://www.wireshark.org/download.html
- NetworkMiner: https://www.netresec.com/?download=NetworkMiner

Log Analysis

- Highlighter: https://www.fireeye.com/services/freeware/highlighter.html
- grep: *nix distributions
- sift: https://github.com/svent/sift/releases

Malicious File Analysis:

- oledump: https://blog.didierstevens.com/programs/oledump-py/
- olefile: http://www.decalage.info/python/olefileio
- OfficeMalScanner: http://www.reconstructer.org/code/OfficeMalScanner.zip

WMI Analysis

- flare-wmi: https://github.com/fireeye/flare-wmi
- WMI_Forensics: https://github.com/davidpany/WMI_Forensics

Memory Analysis

- volatility: http://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_win64_standalone.zip
- rekall: https://github.com/google/rekall/releases

Active Directory (NTDS.at)

- ntdsxtract: https://github.com/csababarta/ntdsxtract

Browser History

- sqlitebrowser: http://sqlitebrowser.org

SHIM Cache

- AppCompatCacheParser: https://github.com/EricZimmerman/AppCompatCacheParser/releases

Event Logs

- python-evtx: https://github.com/williballenthin/python-evtx

PE Files

- pestudio: https://www.winitor.com/binaries.html

MFT

- mft2csv: https://github.com/jschicht/Mft2Csv
- analyzeMft: https://github.com/dkovar/analyzeMFT
- sleuthkit: https://www.sleuthkit.org/sleuthkit/download.php

File Carving

- foremost: http://foremost.sourceforge.net
- scapel: https://github.com/sleuthkit/scalpel
- BulkExtractor: http://downloads.digitalcorpora.org/downloads/bulk_extractor

Windows Registry

- Registry Explorer: https://ericzimmerman.github.io
- regripper: https://github.com/keydet89/RegRipper2.8

Linux Logins

- last: *nix distributions

Misc

- Python: https://www.python.org/downloads

Image Mounting

- Arsenal Image Mounter: http://arsenalrecon.com/downloadsregistration

Debugger
Web Server
PE Modification
Hex Editor
String dumper
Process dumper
Disassembler

When selecting software please note CREST policy on media and USB sticks - removable media are required to be handed to the examination Assessor for wiping (erasure) or destruction at the end of the examination.

5.7 Integrity Protection

Candidates will not be permitted to connect their test platforms to CREST's Internet connection, and any data transfer between the CREST Certification Network and the Internet will be by means of a USB flash drive supplied by the Invigilator. Any attempt to connect the candidate's test platform to the Internet via any means will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. Any attempt to retain data relating to the CREST Certification Examinations either locally or by remote upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. No refund of fees will be considered in these situations.

Note particularly that external media players such as iPods are not permitted in the Certification Examination, unless candidates are prepared to have these wiped (as with any other media used during the Examination). If you'd like to listen to music, put it on your hard drive.

5.8 Invigilation

An invigilator will be present throughout the examination as Invigilator. 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.

6 MARKING SCHEME / PASS MARKS

The marking scheme is given in the tables below.

6.1 Practitioner Intrusion Analyst

	Marks per question	Number of questions	Total Available Marks	Pass Mark
Written (multiple choice)	1	120	120	72

6.2 Registered Intrusion Analyst

	Marks per question	Number of questions	Total Available Marks	Pass Mark
Practical	Various	Various	150	90

6.3 Network Intrusion Analysis

Component	Marks per question	Number of questions	Total Available Marks	Pass Mark
Written (multiple choice)	1	150	150	100
Practical	Various	Various	250	167

6.4 Host Intrusion Analysis

Component	Marks per question	Number of questions	Total Available Marks	Pass Mark
Written (multiple choice)	1	150	150	100
Practical	Various	Various	250	167

6.5 Malware Reverse Engineering

Component	Marks per question	Number of questions	Total Available Marks	Pass Mark
Written (multiple choice)	1	150	150	100
Practical	Various	Various	250	167

Successful "CREST Practitioner" or "CREST Registered" candidates must score 60% of the available marks in each component. That is:

- CPIA
  - at least **72 marks** (possible total: 120 marks)
- CRIA
  - at least **90 marks** (possible total: 150 marks)

Successful "CREST Certified" candidates must score two-thirds of the available marks in each component. That is:

- CCNIA / CCHIA / CCMRE /
  - at least **100 marks** from the **written component** (Multiple Choice) (possible total: 150 marks), and
  - at least **167 marks** from the **practical component** (possible total: 250 marks).

- This represents an overall pass mark of approximately 67% 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 others will not pass.**

Unsuccessful candidates will be told their final scores in the written and practical components, along with feedback as to the general areas in which they fell short.

7 EXAMINATION LOGISTICS

7.1 Location and Timings

Specific logistical information relating to the examination centres in each region can be found can be found in the Examination Preparation pages for your country of choice at http://www.crest-approved.org/. This includes examination timings.

7.2 Before the Certification Examinations starts

Before the Certification Examination starts, candidates will:

Before the examination starts, Candidates will:

- Need to show **suitable office ID** (e.g. military ID, driver's license or passport)
- Have their **NDAs** collected. This is to help us maintain the confidentiality of the examination.
- Have their **Codes of Conduct** collected.

Candidates should have read and signed both of these documents in advance.

7.3 Communication of Results

All written and practical component examination scripts will be marked independently by two CREST Invigilators: this will be completed within five working days of the examination and where possible by the end of the week in which the candidate sits the examination. Results will be communicated by email PDF letter to the candidate to the specified email address at booking.

7.4 Analysis Platform Options

7.4.1 Introduction

CREST takes the confidentiality of the content of the CREST Certification Examinations seriously: candidates are reminded that any attempt to retain data relating to the CREST Certification Examinations either locally or by remote upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision.

In order to help CREST maintain this confidentiality, we do not permit candidates to remove hard disks and writeable media from the examination room unless they have been securely wiped: we have the facility to do this.

Consequently, CREST requires all candidates to be able (and equipped) to remove their internal hard disk at the end of the exam so that it can be retained by CREST for erasure.

It should be noted that CREST is **UNABLE** to accept responsibility for candidate laptops and only the bare drive will be retained. It is the candidates' responsibility to ensure they are competent to remove the disk. Any disk security passwords within the IDE BIOS must be removed.

Candidates must bring their own analysis platform(s) (e.g. laptop with appropriate software toolkit) to the CREST offices.

Additionally, any analysis platform must be capable of reading from and writing to a USB key formatted with a FAT file system.

It is important to note that candidates choosing to use their own testing platform **must surrender their hard disk and any other writeable media for wiping at the end of the assessment process**. Hard disks, once wiped, will be returned to the candidates: we envisage that this will be **at the latest** within two weeks of completion of the certification examination.