Assessors Panel

CREST Certified (CC)
Simulated Attack Specialist & Manager Examinations

Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	NFC_CCSAS/M
Version Number	1.12
Status	Release
Issue Date	24 October 2019

Table of Contents

Version History

Version	Date	Authors	Status
0.1	28 March 2014	Technical Committee and Assessors Panel	Internal Release
1.0	23 May 2014	Technical Committee and Assessors Panel	Public Release
1.1	27 May 2014	Technical Committee and Assessors Panel	Public Release
1.2	3 June 2014	Technical Committee and Assessors Panel	Public Release
1.3	18 June 2014	Technical Committee and Assessors Panel	Public Release
1.4	27 June 2014	Technical Committee and Assessors Panel	Public Release
1.5	09 December 2015	Technical Committee and Assessors Panel	Public Release
1.6	15 September 2016	Technical Committee and Assessors Panel	Public Release
1.7	24 March 2017	Technical Committee and Assessors Panel	Public Release
1.8	3 April 2017	Technical Committee and Assessors Panel	Public Release
1.9	26 April 2018	Operations Manager	Public Release
1.10	17 September 2018	Operations Manager/Assessors	Public Release
1.11	5 June 2019	Operations Manager/Assessors	Public Release
1.12	24 October 2019	Operations Manager	Public Release

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board
Ops Manager	CREST Operations Manager

1 Introduction

1.1 Examination

1.1.1 CREST Certified Simulated Attack Manager (CCSAM)

The CREST Certified Simulated Attack Manager (CCSAM) has three components: a multiple-choice examination, a number of long form questions, and a scenario question. The examination is delivered in two parts at a Pearson Vue Centre.

Success at the Certification Examination will confer upon candidates the status of:

- CREST Certified (Simulated Attack Manager)

The CREST Certification qualification is valid for three (3) years.

1.1.2 CREST Certified Simulated Attack Specialist (CCSAS)

The CREST Certified Simulated Attack Specialist (CCSAS) has two components: a written section compromising of a multiple-choice examination and a number of long form questions, and a practical component. The written component is taken at a Pearson Vue centre; the practical component is taken at a CREST examination centre. All candidates wishing to sit the CCSAS examination must have a valid certificate for the CREST Certified Infrastructure qualification as this exam is considered a specialism to the existing CREST Certified Infrastructure certification. Whilst it is acknowledged that there is significant overlap with the existing Certified Infrastructure exam syllabus this examination is set at a significantly higher level of detail in a number of areas.

Success at the Certification Examination will confer upon candidates the status of:

- CREST Certified (Simulated Attack Specialist)

The CREST Certification qualification is valid for three (3) years.

It should be noted that these exams do not confer any status under the NCSC CHECK scheme and are not recognised for the purposes of equivalency with any other schemes. Candidates are required to hold both CCT INF and CCSAS qualifications in order to operate under the CREST STAR scheme.

1.2 Confidentiality

CREST takes the confidentiality of its examinations very seriously. The retention or dissemination of data relating to the 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.

Along with their booking forms, candidates must also bring both a signed Non-Disclosure Agreement to this effect and also a signed Code of Conduct document, or be prepared to sign a both documents on the morning before they start the examination.

Both of these documents are provided by the CREST Administrator as part of the booking process. The Code of Conduct for Individuals is also available on the CREST website.

It should be noted that prior knowledge of specific CREST examination configurations will be of little use to candidates, as the Examinations are constantly updated and revised and many of the answers are randomised tokens generated uniquely for each candidate.

2 Examination Details (CCSAM)

2.1 Written Component (CCSAM)

The CREST Certified Simulated Attack Manager examination contains only written components – there is no practical element to this exam. There are three elements to the written component, multiple choice questions, long form questions and a more detailed scenario question.

The CC SAM examination is delivered in two separate sessions as a Pearson Vue Centre. The Sessions are identified as SAM 1 and SAM 2. SAM 1 must be taken before SAM 2 and SAM 2 must be taken within three months of SAM 1. The award of CC SAM certification will not be made until both SAM 1 and SAM 2 have been taken and passed

2.1.1 Multiple Choice Questions (SAM 1)

The Multiple Choice Questions will comprise one hundred and fifty (150) questions, all of which the candidate must complete. There is no negative marking in use in the CREST Multiple Choice exam components so the candidate is advised to attempt every question.

2.1.2 Long Form Questions (SAM 1)

The candidate will be presented with one (1) compulsory long form question on the subject of legal matters

2.1.3 Long Form & Scenario Questions (SAM 2)

The candidate will be presented with three (3) long form questions of which the candidate must choose and complete two (2) in addition to the one (1) scenario based question The Scenario question is similar in nature to the Long Form questions, although more detail is expected and more time is allocated as a result.

2.1.4 Timings

The CREST Certified Simulated Attack Manager is delivered in two separate sessions at a Pearson Vue Centre. The Sessions are identified as SAM 1 and SAM 2. SAM 1 must be taken before SAM 2. The award of CC SAM certification will not be made until both SAM 1 and SAM 2 have been taken and passed.

SAM 1 will consist of multiple choice and compulsory long form papers of 2½ hours; SAM 2 will consist of a 3½ hour examination to encompass both the long form and scenario sections. Note that your permitted maximum session time at Pearson Vue is 3 hours in total for SAM 1 and 4 hours in total for SAM 2, allowing you time to read the Code of Conduct and also to provide feedback following each examination.

Candidates should take great care to note that the breakdown of marks approximates to one mark per minute throughout each phase of the exam. If a candidate spends significantly more time than suggested by the marks for any one section or question, they are potentially missing out on marks that could have been obtained more quickly later in the paper. Where candidates are struggling with a particular question or section they are strongly advised to move on and return later in the session if remaining time permits.

2.1.5 Open Book /Closed Book

The whole CCSAM exam is a closed book exam; candidates will not have access to reference material or the Internet for its duration.

2.2 Invigilation (CCSAM)

An invigilator will be present throughout the assessment. The Invigilator is not there to assess candidates' capabilities: all assessment is via the objective written components which will be blind marked by a number

of qualified assessors following the exam. However, the Invigilator will be able to answer any procedural questions that candidates may have during the day.

3 Examination Details (CCSAS)

3.1 Written Component (CCSAS)

3.1.1 Format

The written component of the CC SAS examination is delivered at a Pearson Vue centre of your choice. Please visit www.pearsonvue.com and follow the on-screen instructions to schedule your chosen examination:

The written component of the CREST Certified Simulated Attack Specialist examination will comprise ninety (90) multiple choice questions, all of which the candidate must complete. In addition the candidate will be presented with four (4) longer form questions, of which the candidate must choose and complete three (3).

3.1.2 Timings

The written component will last 2½ hours in total.

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.

3.1.3 Open Book /Closed Book

The entire written component of the exam will be conducted as a closed book exercise. This applies to both multiple choice and long form sections.

Please note that candidates are required to achieve a pass in the written component BEFORE they can sit the practical component.

3.2 Practical Component (CCSAS)

3.2.1 Format

The practical component of the CREST Certified Simulated Attack Specialist examination is delivered at a CREST Examination Centre.

The practical component of the CREST Certified Simulated Attack Specialist examination will comprise a series of stages, split into structured tasks to be carried out against the CREST Certification Network and the target hosts, infrastructure and applications that it comprises. Please note that the practical components are not designed as exact 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 simulated attack 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 target applications or infrastructure. 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.

This exam is intended to simulate a number of real world attack situations. For this reason a candidate will need to be familiar with and to have tools capable of performing client side exploitation attacks, pivoting and traversal attacks, workstation and browser enumeration, server exploitation and also application level exploitation. Some use of basic antivirus software and intrusion detection solutions should be expected

within the environment and the candidate is expected to have the appropriate tools and techniques to operate in this kind of environment.

3.2.2 Timings

The practical component will last 3½ hours. However, candidates will be given the practical component worksheet fifteen (15) minutes before the start, to allow its perusal before the examination starts.

Candidates should take great care to note that the breakdown of marks approximates to one mark per minute throughout each phase of the exam. If a candidate spends significantly more time than suggested by the marks for any one section or question then they are potentially missing out on marks that could have been obtained more quickly later in the paper. Where candidates are struggling with a particular question or section they are strongly advised to move on and return later in the session if remaining time permits.

3.2.3 Open Book / Closed Book

The practical component is an open book test with candidates permitted to use reference material they have brought along. Although the CREST certification network is not connected to the Internet, a dedicated Internet PC will be made available if required.

3.2.4 Practical Assessment Details

The practical examination for the infrastructure assessment 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 of:

- Enumeration of information pertinent to a simulated attack
- The various techniques required to deliver an attack (e.g. Trojan delivery)
    - *The exam rigs host 'bots' simulating real users - following embedded links and opening certain email attachments that are successfully delivered into the organisation. Users' workstations are also simulated in a virtual environment, again following links and rendering HTML and other active content.*
    - *No user/automated interaction with launched applications will be conducted. Files will be opened by their associated default application – you should assume no further interaction (e.g. accepting security warning messages) once the application has been launched and craft any attacks accordingly.*
- Exploitation of client-applications
- Exploitation of embedded and peripheral devices
- Implant creation
    - *NB: Candidates will not be expected to develop an implant during the exam, but will be expected to bring a functional custom implant with at least the following capabilities:*
        - *HTTP proxy aware C&C implant with file upload/download functionality*
        - *Ability to run on x64 Microsoft operating systems*
        - *Ability to evade detection by typical signature based antivirus products*
        - *Full logging/auditing capabilities*
- Command and control channels
- IDS and antivirus evasion
- Egress of information out of a network
    - *NB: Strict egress filtering will be enforced during the exam (e.g. only the perimeter proxy will be authorised to use HTTP as an outbound protocol)*

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.

3.2.5 Practical Components

The areas of the Technical Syllabus that are covered in the practical examination are listed in the syllabus.

It is essential that all candidates are fully familiar with the contents of the Technical Syllabus prior to preparing for and taking the exam.

3.3 Testing Platform Options (CCSAS)

As noted in sections 1.2 and 3.4, CREST takes the confidentiality of the content of its examinations seriously: candidates are reminded that any attempt to retain data relating to the CREST Examinations either locally or by remote upload will be considered a breach of the CREST 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 that have been connected to the CREST Certification Network 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 is the candidate's responsibility to remove any disk IDE / SATA passwords prior to handing the disk over for erasure – if this is not done then the drive will remain locked and cannot be accessed and thus cannot be returned. There is no requirement to remove software encryption (e.g. Bit locker etc.) from the disks as this will simply be overwritten.

It should be noted that CREST are **UNABLE** to accept responsibility for candidate laptops and only the bare drive will be retained. It is the candidate's responsibility to ensure they are competent to remove the disk.

3.3.1 Option 1: Use own laptop testing platform

There is currently only one option available for test platforms.

Candidates will bring their own testing platform (e.g. laptop with appropriate software toolkit) to the CREST offices. It must have an RJ45 Ethernet connection capable of running at 100Mbps, configured to obtain an IP address via DHCP. Additionally, it must be capable of reading from and writing to a USB key formatted with a FAT file system.

The operating systems and tools used must be capable of conducting a simulated attack: candidates may use any software tools they deem appropriate, but are responsible for ensuring that any tools used are appropriately licensed and function correctly.

It is important to note that candidates using 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 within approximately two weeks of completion of the certification examination providing no disk access or other technical issues arise.

3.4 Integrity Protection (CCSAS)

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 Examination rules and will result in an instant fail decision. Any attempt to retain data relating to the CREST 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.

It is the candidates' responsibility to ensure their test laptop is fully prepared prior to attending the exam and it is their responsibility to bring all necessary tools, software, applications and relevant updates with them.

Note that external media players are not permitted in the 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 and ensure that headphone volume levels do not disturb other candidates.

3.5 Invigilation (CCSAS)

A CREST assessor will be present throughout the day 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 the exam systems.

4 Marking Scheme / Pass Mark

4.1 CREST Certified Simulated Attack Manager (CCSAM)

The marking scheme is given in the table below:

Component	Number of questions	Total Marks
Written (multiple choice)	150: – 1 mark each	150
Written (long form)	3: – 30 marks each.	90
Scenario Questions	1. – 120 marks	120

Successful candidates must score 70% of the available marks in each component. That is:

- at least **105 marks** from the **Multiple Choice** (possible total: 150 marks), and
- at least **63 marks** from the **Long Form** (possible total: 90 marks), and
- at least **84 marks** from the **Scenario component** (possible total: 120 marks).

This represents an overall pass mark of approximately 70%, 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 each component where less than two-thirds of the marks were attained, along with feedback as to the general areas in which they fell short.

4.2 CREST Certified Simulated Attack Specialist (CCSAS)

Candidates are required to hold a pass in the written component before they can sit the practical component.

The marking scheme is given in the table below:

Component	Number of questions	Total Marks
Written (multiple choice) Note: Taken in a Pearson Vue centre	90: – 1 mark each	90
Written (long form) Note: Taken in a Pearson Vue centre	3: – 15 marks each.	45
Practical	The exact breakdown of marks and number of questions varies per exam	210

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

- at least **90 marks** from the **written component** (possible total: 135 marks), and
- at least **140 marks** from the **practical component** (possible total: 210 marks).

This represents an overall pass mark of approximately 67%, but note **that candidates must score the minimum number of marks in both the combined written section and also the practical 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 each examination component (multiple choice/long form/practical) where less than two-thirds of the marks were attained. Due to the nature of the CC SAS and CC SAM examinations, detailed feedback cannot be provided and candidates should refer to the examination FAQs available on the website for further information to help them (www.crest-approved.org)

The award of CC SAS certification will not be made until both written and practical components have been passed.

5 Examination Logistics

5.1 Location and Timing

Specific logistical information relating to the practical examination centres in each region can be found at the following location:

http://www.crest-approved.org/examination-logistics.pdf

Before the Examination starts

Before the examination starts, Candidates will:

- Need to show suitable office ID (eg 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.

5.2 Communication of Results

CC SAM
Candidates will receive the overall result of their examination on completion of SAM 2. No results will be released after completion of SAM 1.

CC SAS
All written and practical component examination scripts will be marked independently by CREST Invigilators.

CREST makes every effort to email candidates with their result letters (only) within 14 days of the examination being taken. However, examinations that require second marking may take up to 30 working days for the results to be sent to candidates. This is to ensure both probity and accuracy of results. CREST will make every effort to reduce this period where possible

Results will be communicated by email PDF letter to the candidate to the specified email address at booking.

6 Example questions (written component)

6.1 Multiple choice

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

6.1.1 Question

Which of the following is NOT a valid DNS record type?

A. *SOA – Start of Authority*

B. *NWS – News Server*

C. *CNAME – Canonical Name*

D. *MX – Mail eXchange*

E. *PTR - Domain Name Pointer*

Candidates should clearly indicate their answer by circling the appropriate letter in their test script.

6.1.2 Answer

The correct answer is (B).

6.1.3 Marking scheme

Each multiple choice answer is worth one (1) mark. No points are deducted for incorrect answers.

6.2 Long form

An example long form question is given below, along with a model answer. Each long form question is worth a total of fifteen (15) marks. Note that long form questions on IPsec will not be asked (see technical syllabus): this is an example question only.

6.2.1 Question

During a penetration test, you have discovered an IPsec VPN server at IP address 10.0.0.1, and have determined that it supports the following transform attribute sets for IKE Phase-1:

Encryption Algorithm	Hash Algorithm	Authentication Method	Diffie-Hellman Group
DES	SHA1	RSA Signature	1
AES/256	SHA1	RSA Signature	2
3DES	SHA1	RSA Signature	2

a) *Identify the issue and write an issue description for the customer. The issue description should contain a risk level, detail of the issue, implications and recommendations for ways to mitigate the risk.*

[9 marks]

b) After presenting your findings to the customer, you conduct a de-brief with the customer and their IT supplier. During the de-brief, they mention that the VPN is used for remote access and they only use one VPN client. During IKE Phase-1 negotiations, this client sends a single proposal containing the following six transforms in the order shown:

Transform No.	Encryption Algorithm	Hash Algorithm	Authentication Method	Diffie-Hellman Group
1	3DES	SHA1	RSA Signature	2
2	3DES	MD5	RSA Signature	2
3	AES/256	SHA1	RSA Signature	2
4	AES/256	MD5	RSA Signature	2
5	AES/128	SHA1	RSA Signature	2
6	AES/128	MD5	RSA Signature	2

b) What IKE Phase-1 transform attributes will be negotiated when this client initiates a connection to the VPN server that you discovered? Describe why these particular attributes will be chosen.

[4 marks]

c) Assuming that only this VPN client is used, and the client transform set cannot be altered by the user, does this affect the risk level in practice? Does it make the risk higher or lower?

[2 marks]

6.2.2 Model answer

a) Issue: VPN Server supports weak encryption

Risk Level: Low or Medium

The VPN Server at address 10.0.0.1 supports both strong and weak encryption algorithms for IKE Phase-1. This could allow the VPN to use a weak encryption method for the ISAKMP SA, which could permit an attacker with access to the VPN traffic to crack the encryption and observe the clear-text traffic passing over this SA.

The weak encryption algorithms are DES, which uses a 56-bit symmetric key, and Diffie-Hellman group 1, which uses a 768-bit prime. Best practice dictates that you should use at least 128 bits for symmetric keys, and 1024 bits for Diffie-Hellman prime moduli.

You should disable both DES and Diffie-Hellman group 1 on the server, so that there is no possibility of them being used. However, before doing so, you should check that they are not required by connecting VPN peers, as some older clients only support weak encryption.

b) The transform attributes that would be negotiated are:

- Encryption: 3DES
- Hash: SHA1
- Authentication: RSA Signature
- Diffie Hellman Group: 2

These attributes will be chosen because during IKE Phase-1 negotiation, the transform chosen is the first transform in the initiator's proposal that is acceptable to the responder. In this situation, the VPN client is acting as the initiator, and the VPN server as the responder. The first acceptable client transform is number 1, which has the attributes shown above.

c) Using only this VPN client will reduce the risk level, because it will ensure that the weak encryption algorithms that are supported by the server are not used in practice.