香 港 銀 行 學 會
The Hong Kong Institute of Bankers

Certified Cyber Attack Simulation Professional

Handbook 2017

Syllabus, Regulations and General Information

CCASP CCASP

Certified Cyber Attack Simulation Professional (CCASP)

CCASP CCASP

Table of Contents

1. Introduction

1.1 Pursuing a Professional Identity

The HKMA is working with Hong Kong Institute of Bankers (HKIB) and Hong Kong Applied Science and Technology Research Institute (ASTRI) to develop a localized certification scheme – Certified Cyber Attack Simulation Professional (CCASP) and training programme for cybersecurity professionals.

CCASP is supported by the Council of Registered Ethical Security Testers (CREST) International.

1.2 Learning Path

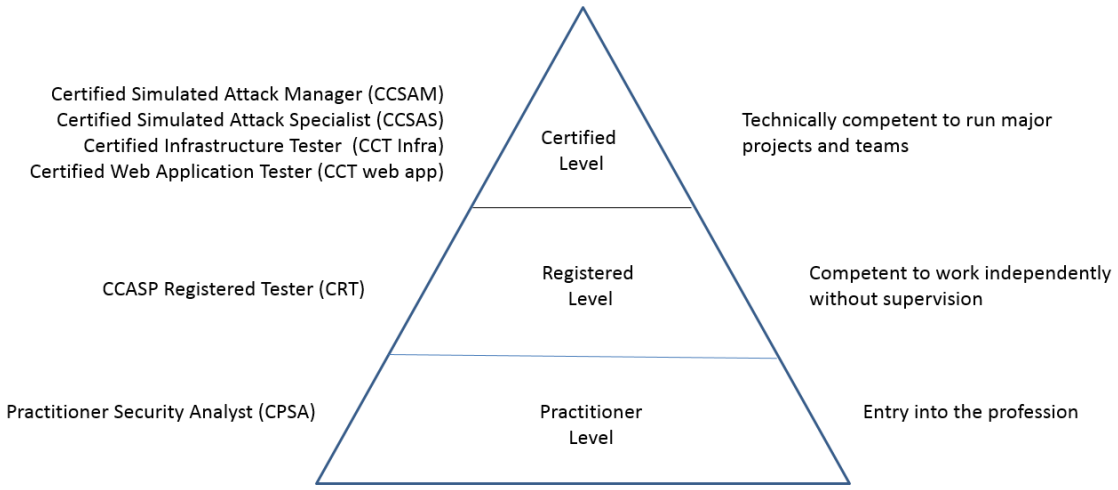
The programme is classified into Practitioner level, Registered level and Certified level.

1.3 Three-level programme

The CCASP Practitioner exams are the entry level exams and are aimed at individuals with around 2,500 hours relevant and frequent experience.

The CCASP Registered Tester examinations are the next step and by passing this you are demonstrating your commitment as an information security tester. Typically, candidates wishing to sit a Registered Tester examination should have at least 6,000 hours (three years or more) relevant and frequent experience.

The CCASP Certified Tester examinations are designed to set the benchmark for senior testers: These are the certifications to which all testers aspire. By gaining the CCASP Certified Tester certification you are recognizably at the top of your game as an information security specialist.



1. Introduction

1.4 Designations

After passing the respective examination, candidate will be awarded with both CCASP and CREST certifications of that examination.

	Designation
CCASP Practitioner Security Analyst	Certificate for CCASP Practitioner Security Analyst Certificate for CREST Practitioner Security Analyst
CCASP Registered Tester	Certificate for CCASP Registered Tester Certificate for CREST Registered Tester
Certified Infrastructure Tester	Certificate for CCASP Certified Infrastructure Tester Certificate for CREST Certified Infrastructure Tester
Certified Web Application Tester	Certificate for CCASP Certified Web Application Tester Certificate for CREST Certified Web Application Tester
Certified Simulated Attack Manager	Certificate for CCASP Certified Simulated Attack Manager Certificate for CREST Certified Simulated Attack Manager
Certified Simulated Attack Specialist	Certificate for CCASP Certified Simulated Attack Specialist Certificate for CREST Certified Simulated Attack Specialist

1.5 Training Classes

Candidates are recommended to complete CCASP training classes before sitting for the examinations but not mandatory.

	Duration (days)
CCASP Practitioner Security Analyst	2
CCASP Registered Tester	2
Certified Infrastructure Tester	3
Certified Web Application Tester	3
Certified Simulated Attack Manager	TBC
Certified Simulated Attack Specialist	TBC

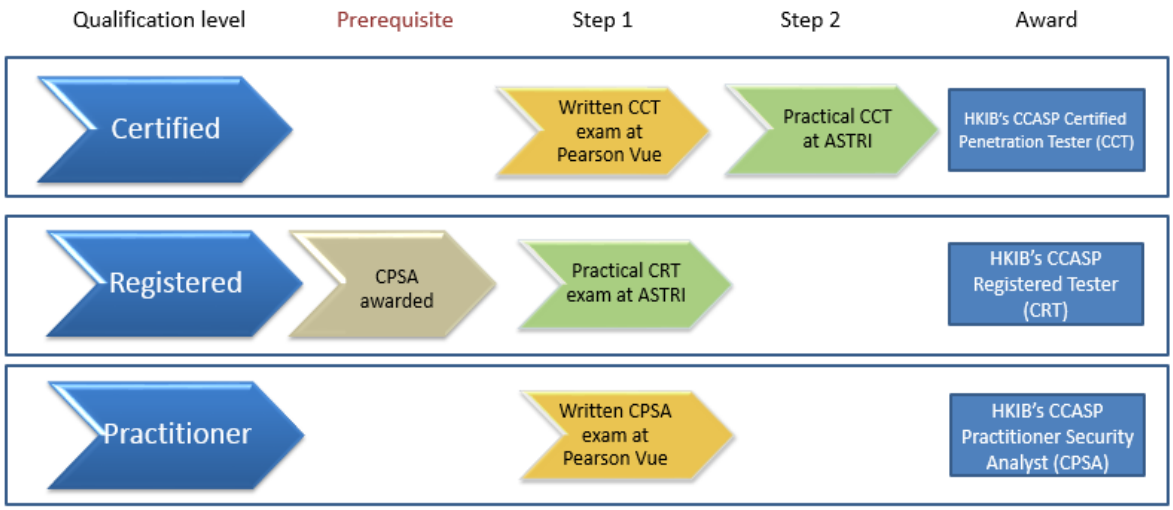
Training Class:

- Classroom based training class
- Content base training by CCASP/CREST certified professional
- Training methodologies:
  - Group discussion
  - Lecture with handouts
  - Group exercise

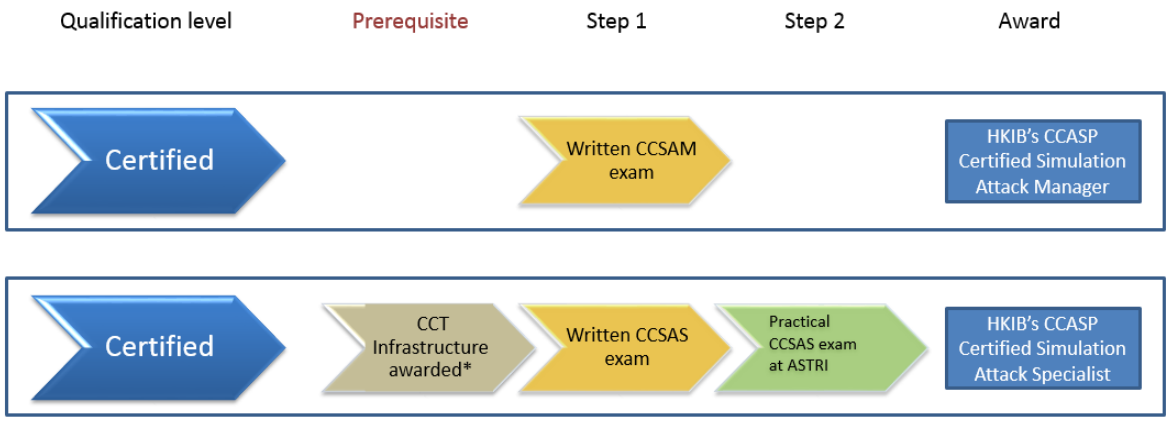
2. Examination Structure and Awards

2.1 CCASP Examination Structure and Awards

Route to HKIB's CCASP Qualification – Penetration Tester



Route to HKIB's CCASP Qualification – Simulation Target Attack and Response (STAR)



*A valid CCT Infrastructure qualification. All HKIB's CCASP examinations are valid for 3 years

STAR courses are being planned for Q4 of 2017. Exact dates are to be confirmed

2. Examination Structure and Awards

To achieve HKMA's iCAST requirement, candidates can consider to participate the following programmes :

Role for HKMA's iCAST	Certification Requirement
iCAST Manager	CCASP – Certified Simulated Attack Manager *OR* CREST Certified Simulated Attack Manager (CCSAM)
iCAST Specialist	CCASP – Certified Simulated Attack Specialist *OR* CREST Certified Simulated Attack Specialist (CCSAS)
iCAST Tester (IT infrastructure)	CCASP – Certified Infrastructure Tester *OR* CREST Certified Infrastructure Tester (CCT Infrastructure)
iCAST Tester (Web Application)	CCASP – Certified Web Applications Tester *OR* CREST Certified Web Application Tester (CCT Web Application)
For general security practitioners in the banking industry	CCASP Registered Tester (CRT)
Compulsory for taking CRT	CCASP Practitioner Security Analyst (CPSA)

Other equivalent qualifications are available on HKMA website.

2.2 Entry Requirement for the CCASP training programme

Participants should possess a minimum of at least three (3) years of experience in IT, security area.

The course is ideally suited to anyone looking to improve their career prospects or transitioning into a cyber security role, including:

- Network engineers
- Systems administrators
- Systems architects or developers
- IT security officers
- Information security professionals
- Budding penetration tester

2. Examination Structure and Awards

2.3 Exemption

OSCP/OSCE/CRT Equivalency

CREST and Offensive Security have entered a partnership to allow Offensive Security OSCP and OSCE certified individuals to be granted CREST Registered Penetration Tester equivalency, subject to various conditions and exclusions. If successfully granted, equivalency will be valid for six months during which time candidates must sit a top-up examination which will grant them the CREST Registered Penetration Tester qualification for a maximum of four years from the date on which the OSCP certification was officially awarded or three years after the equivalence was issued, whichever occurs first. Full information on eligibility, exclusions, process and fees is available on the CREST website at http://www.crest-approved.org/professional-qualifications/oscp-and-crt-equivalency/index.html.

2. Examination Structure and Awards

2.4 Examination Format

Subject	Examination Question Format	Passing Mark for each question format
Certified Simulated Attack Manager	Multiple Choice Questions Long Form Questions Scenario Questions	70%
Certified Simulated Attack Specialist	Multiple Choice Questions Long Form Questions Scenario Questions	67%
Certified Infrastructure Tester (CCT ICE)	Multiple Choice Questions Long Form Questions Practical Questions	67%
Certified Web Application Tester (CCT APP)	Multiple Choice Questions Long Form Questions Practical Questions	67%
CREST Registered Tester (CRT)	Prerequisite: CPSA pass Multiple Choice Questions Practical Questions	60%
CREST Practitioner Security Analyst (CPSA)	Multiple Choice Questions	60%

2.5 Learning Effort

Candidates are suggested to take the training by CCASP accredited training providers before taking the exam. However, the training lessons are not compulsory for the exam.

2.6 Grading

No specific grading for each examination. The result is either Pass or Fail.

Certified Cyber Attack Simulation Professional (CCASP)

Certified Level

Certified Simulated Attack Specialist (CCSAS)

Certified Level

Certified Simulated Attack Manager (CCSAM)

⇧

Certified Level

Certified Infrastructure Tester (CCT Infra)	**Certified Web Application Tester (CCT Web App)**

Certified Infrastructure Tester (CCT Infra) is the **prerequisite of Certified Simulated Attack Specialist (CCSAS)*

⇧

Registered Level

CCASP Registered Tester (CRT)

*Individuals should possess **at least 3 years or more***

IT and security related and frequent experience

⇧

Practitioner Level

CCASP Practitioner Security Analyst (CPSA)

*Individuals with around **2,500 hours***

IT and security related and frequent experience

*CCASP Practitioner Security Analyst (CPSA) is the **prerequisite** of CCASP Registered Tester*

3. Regulations

A. General Examination Regulations

1. Payments for examinations must be received in advance of a candidate sitting the examination. CCASP/CREST reserves the right to withhold the results of the examination until payment in full is received.
2. Cancellations must be made in writing to CCASP/CREST (GB) Ltd at the address on this form at least 21 days before the date of the examination in order to obtain a full refund. Email notification is accepted. Another delegate may be substituted once at no extra cost.
3. No refund will be made for cancellations received less than 21 days before the date of the examination.
4. CCASP/CREST (GB) Ltd reserves the right to amend or cancel any examination and will endeavour to give adequate notice. A full refund of the examination fee will be given in the event of examination cancellation in these circumstances.
5. CCASP/CREST (GB) Ltd reserves the right to apply an administration charge if payment of the examination fee has not been received by the date of the exam.
6. Hard Disk Drive Wiping Policy:
    - 6.1. Hard disk drives ("disk" or "disks"), pen drives and removable media are required to be handed to the examination Assessor for wiping (erasure) or destruction at the end of the examination.
    - 6.2. Erased disks will usually be returned to the candidate within two weeks of the examination to the address identified on the Exam Candidate HD Return Form that will be given to the candidate for completion prior to the examination commencing.
    - 6.3. It is the responsibility of the candidate to ensure that their disk is left in an accessible manner for wiping, specifically without SATA BIOS passwords or similar security mechanisms enabled. (Note: software encryption products such as Bitlocker, Becrypt, Truecrypt, LUKS, etc. do NOT need to be disabled).
    - 6.4. Where all-in-one devices are used, candidates must either:
        a. Surrender the internal disks AND also provide a caddy allowing them to be accessed using either standard SATA or USB under Debian Linux; or
        b. Surrender the internal disks for destruction – CREST will not be liable for the cost of the lost devices; or
        c. Provide a bootable CD/DVD drive with the laptop and ensure that it can be booted from a Debian Linux CD. It can then be left with CCASP/CREST overnight (at the candidate's risk) and erased for collection the following day.
    - 6.5. Where a disk cannot be wiped because it is inaccessible or faulty, CCASP/CREST reserves the right to mechanically destroy the disk and return its remains to the candidate for audit purposes. CCASP/CREST will not be liable for the cost of replacement disks in these circumstances.

3. Regulations

6.6. It is the responsibility of the candidate to ensure that the disk is adequately labelled with their full name prior to handing it over to CCASP/CREST.

6.7. In all cases, the decision of the Assessor regarding the appropriate action to take for a candidate supplied disk is final.

7. If a candidate leaves behind a laptop after their examination, it is the responsibility of the candidate to collect the said laptop in person at a mutually convenient time to CCASP/CREST which may be up to 72 hours after the end of the examination. In such circumstances, CCASP/CREST will not be held liable for loss or theft during this period.

8. CCASP/CREST (GB) Ltd undertakes that information provided on this form will not be passed to third parties and no details provided on this form will be used by organizations other than CCASP/CREST (GB) Ltd. subject to the provisions of paragraph 11 below.

9. By signing the form, the candidate agrees to the pass/fail result (not scores) being passed on to agreed third parties (see Booking Form FAQ 9).

10. Candidates' mobile numbers will only be used to contact them in the case of an emergency.

11. Re-take policy

11.1. Candidates can sit the written aspects of CCASP/CREST examinations once in a seven day period. If a candidate fails the written examination, they must wait seven days before attempting to rebook the examination.

If a candidate fails the practical examination, they must wait three months between attempts.

4. Certified Cyber Attack Simulation Professional

4.1 Certified Cyber Attack Simulation Professional

CCASP Practitioner Security Analyst (CPSA) Duration: 2 days

Objective

- The course aims to provide candidates with knowledge in assessing operating systems and common network services at a basic level.
- The course also includes intermediate level of web application security testing and methods to identify web application security vulnerabilities

Learning Outcomes

- Acquire a common set of core skills and knowledge, including: (please see appendix for details)
  - Soft Skills and Assessment Management
  - Core Technical Skills
  - Background Information Gathering & Open Source
  - Networking Equipment
  - Microsoft Windows Security Assessment
  - Unix Security Assessment
  - Web Technologies
  - Web Testing Methodologies
  - Web Testing Techniques
  - Database
- Perform basic infrastructure and web application vulnerability scan
- Interpret the results to locate security vulnerabilities

Assessment Method

- Examination: **120 Multiple Choice questions**
- Passing mark for this subject is **60%**
- Time allowed: **2 hours**
- Open/Closed book: The written multiple choice 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.

Example Question

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

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.

Answer The correct answer is (B).

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

Exam Logistics

Location

These examinations are delivered at a Pearson Vue centre but the booking of the exam is via the HKIB

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 from the automated process are provided to the candidate at the end of the exam session.

Examination scripts will be reviewed within fifteen working days of the examination and formal certificates produced where appropriate and posted to the candidate in hard copy

Recommended Readings

- Network Security Assessment (by O'Reilly, 2nd edition)
- Hacking Exposed Linux
- Red Team Field Manual (RTFM) (by Ben Clarke)
- Nmap Network Scanning: The Official Nmap Project (by Gordon Lyon)
- Guide to Network Discovery and Security Scanning

CCASP Registered Tester (CRT) Duration: 2 days

Objective

The course aims to provide candidates with a thorough understanding of knowledge in assessing operating systems and common network services at an intermediate level. It also provides an intermediate level of web application security testing and methods to identify common web application security vulnerabilities.

- Understand the techniques used in basic ethical hacking activities.
- Provide candidates with understanding of knowledge in assessing host and common network services.
- Gain hands on experience with a variety of basic tools applicable to all phases of an ethical hacking engagement.
- Gain valuable insight into CCASP certifications.

Learning Outcomes

- This course will cover penetration testing techniques against Windows and Linux networks. It will cover the penetration testing lifecycle.
- Understand what types of security vulnerability may exist on a network. Learn how to use a vulnerability scanner quickly find issues.
- The course will introduce participants to methodologies and tools used throughout the phases of a penetration test and how to use them effectively.
- The content of this programme is designed to help participants prepare for the CCASP CRT exam and will cover a significant portion of the syllabus.

Topic

- Recap on basic networking technologies and protocols.

➢ Network mapping
  - Host identification on local and remote networks
  - Port scanning
  - Common tools used for network mapping

➢ Service enumeration and discussion of common services
  - Using tools to quickly identify services running on hosts
  - Identifying operating systems

➢ Using informational services on a network
  - Information available from network services

- Using tools to gather information from Windows systems

- Assessing the network for security vulnerabilities
  - What is a security vulnerability?
  - Software defects
  - Configuration weaknesses
    - Authentication
    - Encryption
    - Authorization
    - Segregation or other non-authentication restrictions
    - Network security defenses
- Vulnerability scanning
  - Introduction to vulnerability scanners
  - Common vulnerability scanning tools
- Using a vulnerability scanner
- Limitations of vulnerability scanners
  - Issues that scanners will miss
  - False positives
  - Workarounds
  - Exploitability and prioritization of findings.
- Discuss significant vulnerabilities caused by software defects
  - Windows operating system vulnerabilities
  - Linux kernel vulnerabilities
  - Commonly found vulnerabilities in applications
  - Client-side vulnerabilities
- Explore configuration weaknesses common to a number of services
  - Weak or non-existent authentication
  - Default passwords or other credentials
  - Authorisation weaknesses or overly broad permissions
- Discuss services commonly found on networks and common weaknesses
  - Remote access services (RDP, SSH)
  - Applications (Email, web, databases)
  - File sharing (NFS, SMB, NetBIOS)
  - Network management (DNS, SNMP, NTP)
- Exploiting vulnerabilities caused by software defects
  - Introduction to exploit frameworks focusing on Metasploit
  - Common issues encountered when using Metasploit
- Attacking passwords
  - Online password brute forcing
  - Generating wordlists
  - Offline password brute forcing

(There may be minor change on topic depending on trainer)

Assessment Method

The CCASP Registered Tester exam is a multiple-choice practical assessment where the candidate will be expected to find known vulnerabilities across common network, application and database technologies aimed at assessing the candidate's technical knowledge of penetration testing methodology and skills against reference networks, hosts and applications.

A pass at CPSA level is a pre-requisite for the Registered Tester examination and success at both CPSA and CRT will confer the CCASP Registered status to the individual.

- Practical assessment which is examined using multiple choice answers
- Passing mark for this subject is 60%
- Time allowed: 2.5 hours
- Open/closed Book: The practical component is conducted as an open book test, reference material or access to the Internet is permitted. Although the CREST CRT Certification Network is not directly connected to the Internet, Internet access will be made via a dedicated computer.

Example Question

Example (1 Mark Question)
An example 1 mark multiple choice question is given below, along with the answer.

Question (1 Mark)
Which version of operating system is installed on the host xx.xx.xx.xx ?
A. Solaris 9 (x86)
B. Solaris 9 (SPARC)
C. Solaris 10 (x86)
D. Ubuntu 9.01
E. CentOS 5.1

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

Example (5 Mark Question)

An example 5 mark multiple choice question is given below, along with the answer.

Question (5 Mark) Identify the Crest Trophy String in the file 'Crest-Trophy' using the XXXX service and a common security misconfiguration issue on the host xx.xx.xx.xx?

A. RandomStringA
B. RandomStringB
C. RandomStringC
D. RandomStringD
E. RandomStringE

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

Exam Logistics

Location

All practical examinations are being held at Cyber Range, ASTRI, Science Park

Before the Certification Examination starts

Before the Certification 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.
- Need to show suitable official ID (e.g. HKID card)

Communication of results

Examination scripts will usually be marked within 10 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 and letter to the candidate.

Recommended Readings

- Network Security Assessment (by O'Reilly, 2nd edition)
- Hacking Exposed Linux
- Red Team Field Manual (RTFM) (by Ben Clarke)
- Nmap Network Scanning: The Official Nmap Project (by Gordon Lyon)
- Guide to Network Discovery and Security Scanning
- Web Application Hacker's Handbook (1st & 2nd Editions)
- Grey Hat Hacking (by Allen Harper, Shon Harris & Jonathan Ness)

CCASP Certified infrastructure tester (CCT infra) Duration: 3 days

Objective

- Understand the techniques used in advanced ethical hacking activities.
- Gain hands on experience with a variety of advanced tools applicable to all phases of an ethical hacking engagement.
- Identify common issues encountered during different phases of an ethical security test and ways to work around them.
- Test yourself against a real-life vulnerable network in a network challenge.
- Gain valuable insight into CCASP certifications.

Learning Outcomes

- This course will cover advanced penetration testing techniques against Windows and Linux networks.
- It will cover the penetration testing lifecycle.
- Understand exploitation of software vulnerabilities.
- Identify the phases of post-exploitation. Understand potential countermeasures that can be deployed against post-exploitation tasks.
- Describe some common post-exploitation tasks on Windows and Linux systems.
- Describe vulnerabilities and issues on network protocols and common networking devices.
- The content of this programme is designed to help participants prepare for the CCASP CCT Infra exam and will cover a significant portion of the syllabus.

Topic

- Penetration testing lifecycle
  - Reconnaissance
  - Foot-printing
  - Vulnerability assessment
  - Exploitation
  - Post-exploitation
  - Using information obtained to gain further access
- Revisiting exploitation
  - Types of software defect
  - Shellcode
  - Protections deployed against exploitation (StackGuard, DEP, ASLR)

- Using Metasploit through a firewall
- Other sources of exploits

- What happens once a vulnerability has been exploited
  - Privilege levels on operating systems
  - Local system reconnaissance
  - Information to look for on compromised systems
- Theory behind post-exploitation on Windows
  - Security accounts on Windows
  - Password storage (NT and LM hashes)
  - Authentication in Windows
- Local reconnaissance on Windows
  - Identifying your privilege level
  - Finding missing patches
  - Service enumeration
- Privilege escalation
  - Known kernel exploits
  - Service configuration weaknesses
  - File system permissions
  - User Account Control
- Looting
  - Hash dumping
  - Memory dumping for passwords
  - LSA secrets
  - Application passwords
- Reusing Loot
  - Cracking Windows hashes
  - Pass-the-Hash
  - Password reuse
- Theory behind post-exploitation on Linux
  - Users and groups
  - File system permissions
  - Authentication and PAM
- Local reconnaissance on Linux
  - Running processes
  - File system permissions
  - Missing patches
- Privilege escalation on Linux
  - Weak file system permissions
  - Cron and other program launchers
  - SUID bits
  - Kernel exploits

- Looting
  - Password hashes
  - Kerberos caches
  - SSH keys
- Reusing loot
  - Cracking Linux hashes
  - Using SSH keys
- Introduction to relay attacks
  - Techniques for intercepting traffic
    - ARP spoofing
    - NBNS
    - WPAD
- Protocols vulnerable to relay attacks
  - SMB
  - HTTP/S
- Layer 2 protocols and devices
  - VLANs and 802.1q
  - Cisco networking devices
  - HSRP and VRRP

(There may be minor change on topic depending on trainer)

Assessment Method

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A hands-on practical examination
- A multiple choice technical examination
- A long form 'essay style' written paper.

To pass the exam, the candidate must pass all three sections. The written elements of the examination are delivered at **Pearson Vue test centres**; the practical element is delivered at a CCASP/CREST examination center

Written Examination: 120 Multiple Choice questions (2 out of 3 longer form questions)
Passing mark for this subject is = 67%
Time allowed: 3 hours

Open/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.

Practical Examination: Sub section of infrastructure elements

Passing mark for this subject is = 67%

Time allowed: 4.5 hours

Open/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.

Example question

Example questions (written component)

Multiple choice

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.

Answer The correct answer is (B).

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

Long form

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.

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]

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]

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.

Exam Logistics

Location & Timing

All practical examinations are being held at Cyber Range, ASTRI, Science Park

Please note that the written section is performed at a Peason Vue centre and the practical completed at the Crest assessment centre.

Before the Examination starts

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.

Communication of Results

All written and practical component examination scripts will be marked independently by CREST Invigilators: this will be completed within fifteen 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 and also a hard copy will be sent via the post.

Recommended Readings

- Network Security Assessment (by O'Reilly/McNab)
- The Art of Exploitation (by O'Reilly)
- Unix in a Nutshell (by O'Reilly)
- Red Team Field Manual (RTFM) (by Ben Clarke)
- Hacking Exposed 7: Network Security Secrets and Solutions (by Stuart McClure/Joel
- Scambray/George Kurtz)
- The Oracle Hacker's Handbook: Hacking and Defending Oracle (by David Litchfield)
- Red Hat Linux Networking and System Administration (by Terry Collings)
- TCP/IP Illustrated (vol.1, 2nd edition) (by Kevin Fall/W.Richard Stevens)
- The Art of Software Security Assessment (by Mark Dowd/John McDonald/Justin Schuh)
- Grey Hat Hacking (by Allen Harper/Shon Harris/Jonathan Ness)

- Network Warrior (by Gary A. Donahue)
- Hackers Playbook (by Peter Kim)
- Metasploit – The Penetration Tester's Guide (by David Kennedy)

CCASP Certified Web application tester (CCT web app)

Duration: 3 days

Objective

- Understand the techniques used in both basic and advanced ethical hacking activities against web applications.
- Gain hands on experience with a variety of tools applicable to all phases of an ethical hacking engagement.
- Identify common issues encountered during different phases of an ethical security test and ways to work around them.
- Test yourself against a real-life vulnerable network in a network challenge.
- Gain valuable insight into CCASP/CREST certifications.

Learning Outcomes

- This course will cover advanced penetration testing techniques against bespoke web-based applications and associated technologies, including web services and applications.
- It will cover common phases of penetration testing against custom web applications from enumeration and profiling, through identifying weaknesses and then exploiting those weaknesses.
- It will introduce you to methodologies and tools used throughout the phases of a penetration test and how to use them effectively.
- Look at common issues you might encounter and how to work around them.

Topic

- Introduction to Web Application security
- An introduction to common testing tools and process
- Understand Application Design problems
- Mapping and Analyzing an Application
- Using Automation
- Bypassing Client Controls
- Assessing Authentication Mechanisms
- Assessing Session Management
- About application Logic and how it can be bypassable
- Learn and exploit SQL Injection
- Breaking Access Controls

- Logic Flaws
- SQL Injection
- Advanced SQL Injection
- Other Injection types: Attacking Data Stores
- Attacking Backend Components
- Learn attacks against XML, JavaScript, PHP, Filesystem, Network components
- Understand attacks against other application users
- Cross Site Scripting
- Other Attacks against Users

(There may be minor change on topic depending on trainer)

Assessment Method

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A hands-on practical examination
- A multiple choice technical examination
- A long form 'essay style' written paper.

To pass the exam, the candidate must pass all three sections. The written elements of the examination are delivered at **Pearson Vue test centres**; the practical element is delivered at a CCASP/CREST examination center.

Written Examination: 120 Multiple Choice questions (2 out of 3 longer form questions)
Passing mark for this subject is = 67%
Time allowed: 3 hours

Open/Closed book; Open/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.

Practical Examination: A number of mini applications – each with a set of questions
Passing mark for this subject is = 67%
Time allowed: 4.5 hours

Open/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.

Example question

Please see CCT infrastructure in the previous section

Exam Logistics

Location & Timing

All practical examinations are being held at Cyber Range, ASTRI, Science Park

Please note that the written section is performed at a Peason Vue centre and the practical completed at the Crest assessment centre.

Before the Examination starts

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.

All written and practical component examination scripts will be marked independently by CREST Invigilators: this will be completed within fifteen 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 and also a hard copy will be sent via the post.

Recommended Readings

- Web Application Hacker's Handbook (1st & 2nd Editions)
- The Browser Hacker's Handbook
- Hacking Exposed 7: Network Security Secrets and Solutions (by Stuart McClure/Joel Scambray/George Kurtz)
- The Oracle Hacker's Handbook: Hacking and Defending Oracle (by David Litchfield)
- SQL Injection: Attacks and Defence (by Justin Clarke)
- Network Warrior (by Gary A Donahue)

Certified Simulated Attack Manager (CCSAM)

Duration: TBC

Objective

The course aims to provide candidates with a thorough understanding of leading a team expertizes in Simulated Attacks/Target Attacks. After the training, a candidate should have an overall knowledge including penetration tests, target attack and incidents management. A candidate should have the proven exercises on all the related area as well. This training material should help the candidate build up the ability of simulating a target attack in order to understand the details of the potential threads in the real world. The course will ensure that the candidates learn the related intelligence and be able to response reasonable when surrender the target attack in order to minimize the risk against the attack.

Learning Outcomes

- A candidate should possess the well knowledge in all related areas of target attack including penetration tests, incidents management and target attack exercise.
- A candidate should have a proven experience of simulated attack after training and be able to simulate the target attacks in a realistic, legal and safe manner.
- A candidate should be able to response reasonably and immediately under the thread of target attack.

Assessment Method

- Examination: 150 **Multiple Choice questions, long form questions and scenario question**
- Passing mark for this subject is **70%**.
- Time allowed: **6 hours**.
- Open/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.

Exam Logistics

Location & Timing

Both written and practical examinations are being held at Cyber Range, ASTRI, Science Park

Before the Examination starts 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

Communication of results

All written and practical component examination scripts will be marked independently by 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 and also a hard copy will be sent via the post.

Timing of exam

09:00	Arrive – exam induction and preparation
09:30	Start Multiple Choice and compulsory Long Form written component
12:00	Finish morning session
12:00-13:00	Lunch
13:15	Read through questions
13:30	Start Long Form & Scenario Component
17:00	Finish Long Form & Scenario Component

Recommended Readings

- Targeted Cyber Attacks (by Syngress)

Certified Simulated Attack Specialist (CCSAS) Duration: TBC

Objective

- Understand how to perform a red-team simulated attack exercise from planning, through execution to delivery and lateral movement.
- Identify the tools that you will need to successfully run a simulated attack exercise.
- Consider the risks to client's systems from executing a simulated attack and be able to list some measures you can take to minimize these risks.
- Learn how to identify and exploit weaknesses on the internal network whilst minimizing the chance of discovery.
- Test yourself against a real-life exercise.

Learning Outcomes

- This course is designed to introduce you to the techniques used to simulate advanced attacks against client's networks.
- The focus will be on executing the tactics used by real threat groups in the wild such as spear-phishing and browser based attacks, followed by operating covertly within a client's network.
- These simulations are sometimes referred to as "red-teaming".
- It covers exploitation of the human factor to gain a foothold on clients networks, how to establish communications in modern corporate networks and how to exploit weaknesses within internal networks from outside the perimeter.
- The course will focus primarily on corporate Windows networks with common security controls in place, including detective and monitoring controls.

Assessment Method

Please note that candidates are required to hold the CCASP Certified Infrastructure Tester qualification alongside the Certified Simulated Attack Specialist examination in order to operate under the STAR scheme.

The CCSAS Examination has two components: a written paper and a practical assessment.

The written paper consists of two sections: a set of multiple choice questions and a selection of long form questions that will require written answers.

The practical assessment tests candidates' hands-on simulated attack skills against reference networks, hosts and applications.

To pass the exam, the candidate must pass all sections in the written examination and practical examination.

Written Examination: 90 Multiple Choice questions (3 longer form questions:45 marks)

Passing mark for this subject is = 67%

Time allowed: 2.5 hours

Open/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.

Practical Examination: it comprises a series of stages, split into structured tasks to be carried out against the CCASP Certification Network and the target hosts, infrastructure and applications that it comprises. (210 marks)

Passing mark for this subject is: 67%

Time allowed: 3.5 hours

Open/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.

Exam Logistics

Location & Timing

Both written and practical examinations are being held at Cyber Range, ASTRI, Science Park

Before the Examination starts 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

Communication of results

All written and practical component examination scripts will be marked independently by 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 and also a hard copy will be sent via the post.

Timing of exam

09:00	Arrive – exam induction and preparation
09:30	Start Written Component
12:00	Finish Written Component
12:00-13:00	Lunch
13:15	Read through worksheet
13:30	Start Practical Component
17:00	Finish Practical Component

Recommended Readings

- Red Team Field Manual (RTFM) (by Ben Clarke)
- Hacking Exposed 7: Network Security Secrets and Solutions (by Stuart McClure/Joel Scambray/George Kurtz)
- Metasploit Unleashed Guide
- Hackers Playbook (by Peter Kim)
- Network Security Assessment (by O'Reilly, 2nd edition)
- Targeted Cyber Attacks (by Syngress)
- Metasploit – The Penetration Tester's Guide (by David Kennedy)

5. Programme Enrollment

A. *Programme Schedule*

For the latest information about the programme enrollment period and programme schedule, please contact HKIB staff or refer to HKIB website at http://www.hkib.org/.

B. Training Duration

Subject	Training Duration (Days)
CCASP Practitioner Security Analyst	2
CCASP Registered Tester	2
Certified Infrastructure Tester	3
Certified Web Application Tester	3
Certified Simulated Attack Manager	TBC
Certified Simulated Attack Specialist	TBC

C. *Programme Enrollment*

- Applicants can obtain the application form: (i) from the HKIB website; or (ii) in person from the counter of HKIB Head Office during office hours.
- The information provided on the application form must be true and clear. Completed application forms can be returned by fax or email, by hand or by registered mail (to avoid being lost in transit) on or before the corresponding enrolment deadline. Attention should be paid to the application deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee will be charged.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paid the programme fee.
- Each applicant should submit only ONE application form for each programme.
- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received the application form, NO alterations to the programme arrangement will be allowed.
- HKIB reserves the right to change the programme dates and the enrolment deadlines at any time.
- Applicants are advised to retain a copy of the completed application form for their own records.

6. Examination Enrollment

A. Examination Schedule

For the latest information about the examination enrollment period and examination schedule, please contact HKIB staff or refer to HKIB website at http://www.hkib.org/.

B. Examination Mode and Format

Subject	Examination Format	Passing Mark
CCASP Practitioner Security Analyst	Multiple Choice Questions Long Form Questions Scenario Questions	70%
CCASP Registered Tester	Multiple Choice Questions Long Form Questions Scenario Questions	67%
Certified Infrastructure Tester	Multiple Choice Questions Long Form Questions Practical Questions	67%
Certified Web Application Tester	Multiple Choice Questions Long Form Questions Practical Questions	67%
Certified Simulated Attack Manager	Prerequisite: CPSA Pass Multiple Choice Questions Practical Questions	60%
Certified Simulated Attack Specialist	Multiple Choice Questions	60%

C. Examination Enrollment

- Applicants can obtain: (i) from the HKIB website; or (ii) in person from the counter of HKIB Office during office hours.
- The information provided on the application form must be true and clear. Applicants should submit the completed and signed application form, together with the appropriate examination fee, to HKIB Head Office on or before the corresponding application deadline.
- Application forms can be returned by fax or email, by hand or by registered mail (to avoid being lost in transit). Attention should be paid to the application

deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee will be charged.

- Inaccurate or incomplete enrolment applications may not be accepted even if the applicant has paid the examination fee.
- Each applicant should submit only ONE application form for each examination.
- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received the application form, NO alterations to the examinations and examination arrangements will be allowed.
- HKIB reserves the right to change the examination dates and the application deadlines at any time.
- Applicants are advised to retain a copy of the completed application form for their own records.

7. Study Guide - Planning your study

A. Preparation

To prepare your study programme, you are advised to:

1. plan your study realistically
2. list the topics you will have to study
3. learn and revise until the examination
4. allow sufficient time for revision per subject
5. discipline yourself to stick to the study periods you set aside
6. set your study targets and make efforts fully to meet them

B. Study Techniques

The followings are some efficient ways of learning:

1. writing short notes
2. underlining key words or phrases
3. relating what you are reading to real-life examples or experiences are efficient ways of learning

C. CCASP Handbook

The CCASP Handbook lists out the syllabus and requirements of the examinations. You should study the parameters of the examination syllabus of the subjects you will take, and keep the syllabus requirements in sight as your study progresses towards the examination date.

D. Training Classes

Enrolment for training classes is not compulsory but recommended for CCASP learning programme. For details on the programme schedule, please refer to the HKIB website or contact HKIB staff.

8. Addendums and Changes

HKIB reserves the right to make changes and additions to the examination regulations, the enrolment procedures, the information in this handbook and any policies relating to the examination without prior notice. HKIB shall bear no responsibility for any loss to candidates caused by any change or addition made to the aforementioned subjects.

9. Contact Information

HKIB Head Office Address

3/F Guangdong Investment Tower, 148 Connaught Road Central, Hong Kong

General Enquiries

Tel.: (852) 2153 7800 Facsimile: (852) 2544 9946
Email: hkib@hkib.org

Membership Enquiries

Tel.: (852) 2153 7879 Email: membership@hkib.org

Training Programme Enquiries

Tel.: (852) 2153 7877 Email: programme@hkib.org

Office Service Hours

Monday – Friday: 09:00 - 18:00

Saturday, Sunday & Public Holiday: Closed

Syllabus and Examination Mapping

MC- Multiple Choice
SC - Written Scenario Questions
LF - Written Long Form
P- Practical

ID	Skill	Practitioner	CRT	CCT-Web	CCT-Infra	CSAM
A1	Engagement Lifecycle	MC		MC	MC	MC, LF, SC
A2	Law & Compliance	MC		MC	MC	MC, LF, SC
A3	Scoping			MC	MC	MC, LF, SC
A4	Understanding Explaining and Managing Risk	MC		MC	MC	MC, LF, SC
A5	Record Keeping, Interim Reporting & Final Results	MC		MC, P	MC, P	MC, LF, SC
A6	Client Communications					MC, LF, SC
A7	Operations Security (OpSec)					MC, LF, SC
A8	Social Engineering Attacks					MC, LF, SC
A9	Physical Security					MC, LF, SC
A10	Kill Chain					MC, LF, SC
B1	IP Protocols	MC		MC	MC	MC
B2	Network Architectures	MC		MC	MC	MC
B3	Network Routing				MC	MC, LF, SC
B4	Network Mapping & Target Identification	MC	P	MC, P	MC, LF, P	MC
B5	Interpreting Tool Output	MC	P	MC	MC	MC, LF, SC

B6	Filtering Avoidance Techniques	MC		MC	MC	MC
B7	Packet Crafting			MC	MC	MC
B8	OS Fingerprinting	MC	P	MC	MC, P	MC
B9	Application Fingerprinting and Evaluating Unknown Services	MC	P	MC	MC, P	MC
B10	Network Access Control Analysis	MC		MC	MC, LF, P	MC
B11	Cryptography	MC		MC, P	MC	MC
B12	Applications of Cryptography	MC		MC	MC, LF	MC
B13	File System Permissions	MC	P	MC	MC, P	MC
B14	Audit Techniques	MC		MC	MC, P	MC
B15	Unix/Linux Vulnerabilities					MC
B16	Wireless Networks					MC, LF
B17	Automation and Scripting					MC
B18	Directory Services					MC
B19	VPN TECHNOLOGIES					MC
C1	Registration Records	MC		MC	MC	MC, LF, SC
C2	Domain Name Server (DNS)	MC	p	MC	MC, P	MC, LF, SC
C3	Customer Web Site Analysis	MC		MC, P	MC	MC, LF, SC
C4	Google Hacking and Web Enumeration	MC		MC	MC	MC, LF, SC
C5	NNTP Newsgroups and Mailing Lists	MC		MC	MC	MC, LF, SC
C6	Information Leakage from Mail & News Headers	MC		MC	MC	MC, LF, SC
C7	DOCUMENT METADATA					MC, LF, SC

D1	Management Protocols	MC	p	MC	MC, LF, P	
D2	Network Traffic Analysis	MC			MC, LF, P	
D3	Networking Protocols	MC			MC, P	
D4	IPSec	MC			MC, P	
D5	VoIP	MC			MC, P	
D6	Wireless	MC			MC	
D7	Configuration Analysis	MC			MC, LF, P	
E1	Domain Reconnaissance	MC	P	MC	MC, LF, P	
E2	User Enumeration	MC	P	MC	MC, P	
E3	Active Directory	MC	P	MC	MC, P	
E4	Windows Passwords	MC	P	MC, P	MC, LF, P	
E5	Windows Vulnerabilities	MC	P	MC, P	MC, LF, P	
E6	Windows Patch Management Strategies	MC			MC, P	
E7	Desktop Lockdown	MC			MC, P	
E8	Exchange	MC			MC	
E9	Common Windows Applications	MC	P		MC, P	
F1	User enumeration	MC	P		MC, P	
F2	Unix vulnerabilities	MC	P		MC, LF, P	
F3	FTP	MC	P		MC, P	
F4	Sendmail / SMTP	MC	P		MC, LF, P	
F5	Network File System (NFS)	MC	P		MC, P	
F6	R* services	MC	P		MC, P	
F7	X11	MC	P		MC, LF, P	
F8	RPC services	MC	P		MC, P	
F9	SSH	MC	P		MC, P	
G1	Web Server Operation	MC		MC	MC	
G2	Web Servers & their	MC	P	MC, P	MC, P	

	Flaws					
G3	Web Enterprise Architectures	MC		MC	MC	
G4	Web Protocols	MC	P	MC, P	MC, P	
G5	Web Mark-up Languages	MC		MC	MC	
G6	Web Programming Languages			MC	MC	
G7	Web Application Servers			MC, P		
G8	Web APIs			MC, P	MC	
G9	Web Sub-Components			MC, P		
H1	Web Application Reconnaissance			MC, LF	MC	
H2	Threat Modelling and Attack Vectors			MC	MC	
H3	Information Gathering from Web Mark-up	MC		MC, LF, P	MC	
H4	Authentication Mechanisms	MC		MC, LF, P	MC	
H5	Authorization Mechanisms	MC		MC, LF, P	MC	
H6	Input Validation	MC		MC, LF, P	MC	
H7	Application Fuzzing			MC, LF, P		
H8	Information Disclosure in Error Messages	MC		MC	MC	
H9	Use of Cross Site Scripting Attacks	MC		MC, LF, P	MC	
H10	Use of Injection Attacks	MC		MC, LF, P	MC	
H11	Session Handling	MC		MC, LF, P	MC	
H12	Encryption	MC		MC, P	MC	
H13	Source Code Review	MC		MC, LF, P	MC	
I1	Web Site Structure Discovery		P	P		
I2	Cross Site Scripting		P	P		

	Attacks					
I3	SQL Injection		P	P		
I4	Session ID Attacks			P		
I5	Fuzzing			P		
I6	Parameter Manipulation		P	P		
I7	Data Confidentiality & Integrity			P		
I8	Directory Traversal		P	P		
I9	File Uploads		P	P		
I10	Code Injection		P	P	MC	
I11	CRLF Attacks			P	MC	
I12	Application Logic Flaws			P	MC	
J1	Microsoft SQL Server	MC	P	MC, P	MC, P	
J2	Oracle RDBMS	MC	P	MC, P	MC, P	
J3	Web / App / Database Connectivity	MC	P	MC, P	MC, P	
CSAM Specific Attacks						
D1	Enumeration of hosts					MC
D2	Enumeration of users					MC, LF, SC
D3	Enumeration of Operating Systems					MC
D4	Enumeration of software packages					MC, LF, SC
D5	Enumeration of missing security updates					MC, LF
D6	Enumeration of sensitive files					MC
D7	Enumeration of registry and configuration settings					MC

E1	Email Spoofing					MC, LF, SC
E2	Anti-Spoofing Countermeasures					MC, LF
E3	Web Site Seeding					MC, SC
E4	Trojanised Legitimate Binaries					MC
F1	Exploitation of common document formats					MC, LF, SC
F2	Exploitation of client web browsers					MC, LF, SC
F3	Exploitation of rich content					MC, LF, SC
F4	Exploitation of underlying operating system vulnerabilities					MC, LF, SC
F5	Exploitation of Cross-site scripting vulnerabilities					MC, LF, SC
G1	Identification and exploitation of embedded devices					MC, LF, SC
G2	Identification and remote control of peripheral devices					MC, LF, SC
G3	Key Logging					MC, LF, SC
H1	Implant Design					MC, SC
H2	Win32 Implant Creation					MC
H3	VBA Macro Creation					MC
H4	Operating System Bootstrap					MC, LF
H5	USB "Autorun"					MC, LF
H6	Physical Implants					MC, LF
I1	Antivirus Detection Evasion					MC, LF

I2	Disable/Re-enable Antivirus					MC
I3	Port Scanning					MC, LF
I4	Operating System Defenses					MC, LF
I5	Perimeter Controls					MC, LF
I6	IDS Evasion					MC, LF
J1	Outbound Firewall Rules					MC, LF
J2	Reverse Shell					MC
J3	Tunneling					MC, LF, SC
J4	Attack Source Obfuscation					MC, LF, SC
J5	Secure Egress					MC, LF, SC

Bad Weather Arrangements

In the event of bad weather on the training class/ examination day, candidates should visit the HKIB website at www.hkib.org for announcements about the latest arrangements, and should pay attention to radio/ television broadcasts about the weather conditions.

- If the typhoon signal No. 8 or above, or the black rainstorm signal, is hoisted or still in force on the day of a training class, the below arrangements will apply:

Signal in force	Programme(s) cancelled
6:30 am	Morning Session (8:30 am – 1:59 pm) will be cancelled.
12:00 noon	Afternoon Session (2:00 – 5:59 pm) will be cancelled.
3:00 pm	Evening Session (6:00 – 10:00 pm) will be cancelled.

- If the typhoon signal No. 8 or above, or the black rainstorm signal, is hoisted or still in force on the day of an examination at the following times, the below arrangements will apply:

Signal in force	Examination cancelled
At or after 6 am but before 10 am	Examination(s) starting at or after 8am but before 1pm will be cancelled.
At or after 10 am but before 2 pm	Examination(s) starting at or after 1pm but before 5pm will be cancelled.
At or after 2 pm	Examination(s) starting at or after 5pm will be cancelled.

  - If the typhoon signal No. 8 or above, or the black rainstorm signal, is hoisted or still in force while the training class/ examination is in progress, the training class/ examination will continue as scheduled.
  - If a training class/ examination is rescheduled, HKIB will notify candidates of the new training class/ examination date and time by email within **one week** of the originally scheduled training class/ examination date. Under such circumstances, candidates are not required to re-register for the training class/ examination. Applications for a refund and/or transfer of the training class/ examination fee(s) will NOT be allowed.

HKIB reserves the right and absolute sole discretion to postpone, cancel and/or reschedule any training class/ examination.

Policy of Personal Data Protection

When HKIB collects information from participants in our activities, training programmes and/or examinations ("Participants"), it is our policy to meet fully the requirements of the Ordinance, which regulates the treatment of personal data. Throughout this policy, the meaning of the term "personal data" is as defined in the Ordinance. In dealing with personal data, we will ensure compliance by our staff with the standards of security and confidentially prescribed under the Ordinance.

1. All information of a personal nature obtained by HKIB is for the purposes of administering our services, which may include, but are not limited to: training, examinations and other activities organised wholly or in part by HKIB; conducting subsequent performance assessments; and handling related irregularities, if any.

The personal data is supplied either by Participants themselves or from external sources, including, but not limited to: employers, service or learning providers; third parties that are otherwise affiliated to the service in which Participants are involved, and, who may provide HKIB with relevant information on their employees, members and/or students; and members of the public.

After the data obtained from Participants have been captured, processed and checked, hard copies – for example, of Participants' information checklists or Attendance Notices – may be produced for all HKIB services in order to ensure the accuracy of the data. Some data may also be used for the following purposes during registration and/or payment:

- To verify Participants' identities;
- To fulfill Participants' specific requests, applications or enrolments relating to our services;
- To administer and deliver information about the service;
- To maintain and process examination marks and results, if any;
- To process and handle Participants' complaints, enquiries, feedback or irregularities, if any;
- To maintain Participants' records;
- To conduct research or statistical analysis;
- To release information to relevant third parties on whose behalf HKIB administers, conducts or organises services, and to any third party that HKIB engages to administer and/or conduct services for and on behalf of HKIB;

- To promote and provide various HKIB member services to Participants;
- To serve other purposes as permitted by law; and
- To serve any other purposes as may be agreed between the Participants and HKIB.

2. HKIB will keep the personal data of Participants' confidential. Nevertheless, as part of its operations, HKIB may compare, transfer or exchange their data with the data already in HKIB's possession, or obtained hereafter by HKIB, for these or any other purposes.

3. HKIB is also professionally obliged to process the personal data fairly, confidentially and lawfully.

4. The provision of personal data or any information is voluntary. However, failure to provide the requested personal data may result in HKIB being unable to process Participants' requests, perform its statutory functions or deliver its services to Participants.

5. HKIB may contact a Participant if we require confirmation of his/her identity, or further information about the data requested that may assist HKIB to locate his/her personal data before complying with his/her request.

6. HKIB will only use the data for specifically or directly related purposes, as outlined on its enrolment form and the accompanying explanatory notes, if any. No exception to this rule is permitted without the express permission of HKIB.

7. HKIB recognises the sensitive and highly confidential nature of much of the personal data that it handles, and maintains a high level of security in its work. HKIB has well-established guidelines and procedures for maintaining the security of all personal data, both as hard copies and in computer-readable form.

8. HKIB will do its best to ensure compliance with the Ordinance by providing guidelines to and monitoring the compliance of the relevant parties. However, HKIB cannot control how third parties use Participants' personal information and assumes no responsibility for the privacy protection provided by such third parties.

9. The means of Participants' communications with HKIB, including online, by email, by text message (SMS), via HKIB's customer hotline or otherwise, may be recorded and retained for training and record-keeping purposes. Records may be used to monitor the quality of the assistance given and to verify the matters discussed.

Personal data protection in regions outside Hong Kong would be subject to the requirements of these jurisdictions.

Responsibility and Rights of Candidates

Participants are required to keep HKIB informed of any changes in their personal data once they have enrolled as Participants for services offered by HKIB or for an examination, and until such time as the service is completed or Participants have completed the examination. HKIB has well-established procedures to verify and to process the amendment of Participants' particulars. After the data obtained from the enrolment forms have been captured, processed and checked, hard copies – for example, of Participants' information checklists or Attendance Notices – may be produced for all services offered by HKIB in order to ensure the accuracy of the personal data.

Participants may have the right, under the Ordinance, to request access to, or correction of any data provided by them as per the manner and limitations prescribed therein. As the Ordinance allows, HKIB has the right to charge a reasonable fee for processing any request for data access.

Participants who request access to data or the correction of their data should do so in writing to HKIB. Participants should also write to HKIB if they do not want to receive any information on services offered by HKIB.

Data Retention

Unless otherwise agreed, hard copies of any documents containing Participants' personal data that they have provided to HKIB become the property of HKIB. HKIB will destroy any documents it holds in accordance with its internal policy and applicable laws.

Personal data will be retained only for such period as may be necessary for carrying out the purposes stated in this policy or as otherwise specified at the time of collection. In some circumstances, HKIB may retain certain records for other legitimate reasons, including to resolve any potential disputes, cross-check against future examination enrolment, if applicable, and to comply with other reporting and retention obligations.

Transfer of Personal Data Outside of Hong Kong

At times it may be necessary and prudent for HKIB to transfer certain personal data to places outside Hong Kong SAR, in order to carry out the purposes, or directly related purposes, for which the personal data were collected. Where such a transfer is performed, it will be done in compliance with the requirements of the Ordinance.

Amendments

HKIB reserves the right to change or modify its privacy policy at any time and without prior notice. Any such change or modification shall be effective immediately upon posting of the changes and modification on this website.

Enquiry

All access/ correction requests and any enquiries about this privacy policy statement should be directed to HKIB at the address and telephone numbers below:

The Hong Kong Institute of Bankers
3/F Guangdong Investment Tower
148 Connaught Road Central
Hong Kong
Tel.: (852) 2153 7800
Facsimile: (852) 2544 9946
Email: hkib@hkib.org (General Enquiries)
pdp-enquiry@astri.org (Technical Enquiries)