CCCA
CHARTERED COMPLIANCE AND CYBER ANALYST

CYBER SECURITY OPERATIONS
SAMPLE QUESTIONS

SECTION A

1. Information sources for measuring cybercrime include all of the following except:

A.Police-recorded crime statistics;
B. Victim reporting initiatives
C. Population-based and business surveys
D. Yellow book

2. Criminal tools of choice for these crimes, such as botnets, have global reach. More than one million unique ……..addresses globally functioned as command and control servers for botnets.

A. IP
B. Spam
C. Trojan
D. Phishing

3. A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in …….. .

A. United Nation principles
B. Council of Europe Cybercrime Convention
C. The Basel Accord
D. Palermo Accord

4. ……is concerned with recovering – often volatile and easily contaminated – information that may have evidential value.

A. Digital analysis
B. Digital mining
C. Data analysis
D. Digital forensics

5. International law provides for a number of bases of jurisdiction over cybercrime acts, primarily including forms of territory- and nationality-based jurisdiction.
A. True B. False

6.Which of the following services have been characterized as 'infrastructure-as-a-service,' 'softwareas-a-service,' and 'platform-as-a-service,' covering the provision of 'virtual' machines over the internet, the provision of software applications, and the provision of a whole network, server system, operating system and storage, respectively.

A. Cloud computing
B. Cloud forensics
C. Computer forensics
D. Computer Security

7. Acts hindering the functioning of a computer system, as well as to acts involving damage, deletion, deterioration, alteration or suppression of computer data without authorization or justification are termed

A. Illegal data interference
B. Hacking
C. Penetration
D. Stalking

8. The use of a computer system to process, disseminate, obtain, or access personal information in violation of data protection provisions is termed.
A. Breach of privacy
B. Intrusion
C. Cyber laundering
D. Penetration

9. A digital signature is one of the most important methods to ensure the authenticity of digital information. How is a digital signature created from the digital fingerprint (hash) of the information?

A. The hash is encrypted with the session key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with a corresponding session key.

B. The hash is encrypted with the public key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding private key.
C. The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.
D. The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding public key.

10. Biometric has become ever more important as a means to verify the identity of users. Which feature of biometrics represents a major consideration for organizations that want to implement it?

A. The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are equal.
B. The way users swipe their tablet or smart phone can be used as a behavioral mechanism for biometrics.
C. The so-called crossover error rate, which is the rate at which both acceptance and rejection errors are within acceptable levels.
D. Face recognition cannot be used as a biometric mechanism, because it is very inaccurate.

11. Hackers and cyber criminals usually perform their activities according to a well-structured plan. What is the best order in which these activities are performed within a well-structured plan?
A. Enumeration, foot printing, getting access, privilege escalation, erasing tracks
B. Reconnaissance, enumeration, getting access, privilege escalation, erasing tracks
C. Reconnaissance, scanning, getting access, privilege escalation, maintaining access
D. Scanning, enumeration, getting access, privilege escalation, maintaining access

12. A consultant is hired by a company that wants advice on how to organize and implement patch management. He recommends that:
1. Patches should be tested first.
2. Patches should be implemented as soon as possible after they are released.

What additional recommendation should he make?
A. Critical systems should be patched before the less critical ones.
B. Both critical systems and less critical systems should be patched at the same time.
C. Less critical systems should be patched before the critical ones.

13. What characteristic makes the internet so attractive?
A. the 'secure' surroundings within which it is implemented
B. the ability to provide an open, easy-to-use network
C. it eliminates the need for firewalls
D. you don't require a fast computer to use the internet

14.Why is it important for the internet to implement protocols?
A. to provide a universal data 'platform' for all connections to use
B. so that nobody gets confused

C. to enable the use of cryptographically techniques
D. to prevent the use of viruses

15. The acronym **COBIT** stands for:
A .Central Objectives for Information and Related Technology
B. Centre for Optimizing Objectives for Information and Related Technology
C. Control Objectives for Information and Related Technology
D. Control Objectives for Information and Related Tools
16. What must exist for cyber stalking to be illegal in a state or territory?
A. Specific laws against cyber stalking in that state or territory.
B. Specific laws against cyber stalking in that nation.
C. Nothing; existing stalking laws can apply.
D. Nothing; existing international cyber stalking laws apply.

17. What is a cookie?

A. A piece of data that web servers gather about you.
B. A small file made that contains data and then is stored on your computer.
C. A piece of data that your web browser gathers about you.
D. A small file made that contains data and then is stored on the web server.

18. What can you do on your local computer to protect your privacy?

A. Install a virus scanner.
B. Install a firewall.
C. Set your browser's security settings.
D. Set your computer's filter settings.

19**.** If you are posting anonymously in a chat room and another anonymous poster threatens you with assault or even death, is this person's post harassment?

A. Yes, any threat of violence is harassment.
B. Probably not, because both parties are anonymous, so the threat is not credible.
C. Yes, chat room threats are no different than threats in person.
D. Probably not, because making a chat room threat is not the same as making a threat in person.

20. What will law enforcement officials usually require of the victim in order to pursue harassment allegations?

A. A verifiable threat of death or serious injury
B. A credible threat of death or serious injury
C. A verifiable threat of harm
D. A credible threat of harm

SECTION B

ATTEMPT ALL QUESTIONS

1. You receive the following email from the Help Desk:
Dear CCCA Email User, beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

*Name (first and last):
*Email Login:
*Password:
*Date of birth:
*Alternate email:
Please contact the Webmail Team with any questions. Thank you for your immediate attention.
As a cyber-analyst, how will you address the case above?

2. One of the staff members in **IBM** subscribes to a number of free **IT** magazines. Among the questions she was asked in order to activate her subscriptions, one magazine asked for her month of birth, a second asked for her year of birth, and a third asked for her mother's maiden name. What do you think might be going on here?

3.(i) What is a password manager?
(ii) Discuss the operations of a password manager.

4. Discuss the content of the Council of Europe Convention on Cybercrime (2001).