Curtin College

Mock Test 1 - Trimester 1, 2020

Subject: **Fundamental Concepts of Data Security**

Index No.: FCDS2001

Name:………………………………………………………….

Student ID:……………………………………………………..

This test is OPEN BOOK.

Time Allowed: 1 HOUR
Total Marks: 100

Multiple choice questions (2 points each)

□ Indicates a single or multiple answers.

○ Indicates a single answer.

1. The concept Availability is about:

□ The ability to come back to normal after a disruption

□ The ability to correct errors

□ Functionality and performance are as expected or as per service-level agreements

□ Data moving over the Internet is secure

□ None of the above

2. **What is the top-down approach in information security?**

○ An approach that focuses on matters of highest priority first

○ An approach that tackle all matters

○ An approach that receives the initiatives, direction, and support from senior management

○ An approach that addresses concerns of all staff

○ None of the above

3. **Which security principle is about providing information systems with adequate functionality, predictable manner, acceptable performance, and ability to recover quickly from disruptions?**

○ Availability

○ Integrity

○ Confidentiality

○ All Availability, Confidentiality, and Integrity

○ None of the above

4. **The distributed nature of modern computing poses security challenges because**

○ Information is often sent via insecure channels

○ There are a large number of hackers

○ Many people do not have sufficient security training

○ There are many types of communication channels

○ None of the above

5. **An intrusion detection system is an example of what type of countermeasure?**

○ Preventive

○ Corrective

○ Subjective

○ Detective

○ Postulative

6. **Examples of security management responsibilities are**

□ Help achieve business goals

□ Develop security policies and guidelines

□ Perform risk analysis and security audits

□ Ensure compliance

□ None of the above

7. **Security baselines are**

○ Implementations to achieve the minimum security levels that are deemed acceptable industry-wide

○ Recommendations of security practices

○ Basic hardware and software to achieve security goals

○ General security advice to all staff

○ None of the above

8. **What can be said about substitution and shuffling**

○ Substitution is a form of shuffling

○ Shuffling is a form of substitution

○ Shuffling and substitution are not related

○ Substitution is the same as shuffling

○ None of the above

9. **Storage area networks easily scale well with data size**

○ True

○ False

10. Which solutions can address Distributed Denial-of-Service attacks (Select all that apply)

□ Encryption of Internet traffic

□ Strengthening access control

□ Provisioning of network bandwidth

□ Redundant servers

□ Network monitoring

11. The third rule of the Bell-Lapadulla implies that

○ A user cannot have both read and write access to a data object

○ Each group of data objects are only fully accessible (read+write) by a group of subjects

○ If a data object has multi classification labels then no one can both read and write the object

○ If a user has different clearances then that user cannot read and write any data object at the same time

○ None of the above

12. The Bell-Lapadulla is said to be a multi-level security model. Multi-level means

○ There are different mechanisms to access data

○ Data have different classifications and users have different clearances

○ Subjects access data using a top-down approach

○ Subjects access data using a bottom-up approach

○ None of the above

13. A full backup typically makes a copy of all files

○ True

○ False

14. Phishing attacks aiming at specific individuals or companies are called

○ Advanced persistent threats

○ Whaling

○ Spear phishing

○ Clone phishing

○ None of the above

15. A media sanitization process that involves executing firmware secure erasure commands belongs to which category (as per NIST SP800-80)

○ Clearing

○ Destroying

○ Disposal

○ Purging

○ None of the above

16. In the Clark-Wilson model, the transformation procedures (TPs) deal with all types of data

○ True

○ False

17. "No write up, No read down" are the two rules of which model?

○ Biba

○ Bell Lapadulla

○ Clark Wilson

18. An IT environment consisting of IT components and processes that enable the delivery of on-demand computing resources via the Internet or private network is called

○ Virtualisation

○ Cloud computing

○ Platform-as-a-service

○ IT hub

○ None of the above

19. In the Clark-Wilson model, data are categorised into

○ Confidential data items and non-confidential data items

○ Unconstrained data items and constrained data items

○ Only one type of data

○ Public data items and private data items

○ None of the above

20. Which rule of the Biba model prevents the use of "dirty" data?

○ No write up rule

○ No read down rule

○ Service request rule

○ None of the above

21. Data masking is the same as encryption

○ True

○ False

22. How should an organisation demonstrate uniform of enforcement of a policy

○ Making sure everyone understands the penalty

○ Providing mechanisms to detect and prosecute any violations of policy regardless of status

○ Asking law enforcement agency to review policy on a regular basis

○ Performing system audits regularly

○ None of the above

23. What is a computer crime?

○ Any attack specifically listed in your security policy

○ Any illegal attack that compromises a protected computer

○ Any violation of a law or regulation that involves a computer

○ Failure to practice due diligence in computer security

○ None of the above

24. A company needs to make employees be aware that discrimination in the workplace can be caught. What should the company do? (select all that apply)

□ Having a website to report discrimination

□ Introduce severe penalty in the policy

□ Publication of previous cases

□ Having specific roles in the organisation to deal with discrimination

□ None of the above

25. Professional organisations have no role in promoting ethical behaviour at work, it is solely the organisation's responsibility

○ True

○ False

26. It is advised that you should acknowledge the authors of open-source libraries that you use for your software project. This is part of which section of the ACS code of conduct

○ Professionalism

○ Honesty

○ Competence

○ Professional development

○ None of the above

27. Do security policies and guidelines help improve ethical behaviour?

○ Yes

○ No

28. A student claims that changing few words and reordering sentences of a copied paragraph and presenting as own work does not constitute plagiarism. As per Curtin policy, is this claim accepted

○ Yes, because it is not original

○ No, because it is still not the student's work.

○ It depends on a case-by-case basis, hard to tell

Written response questions

29. You are writing ICT guidelines for students in a university to make them aware of recommended security practices. For each of the general security goals (Availability/Integrity/Confidentiality), give one (1) example of what they should do, and one (1) example of they should not do. **(10 pts)**

30. On Wednesday February 28, 2018, the largest ever distributed denial-of-service (DDoS) attack peaking 1.35 terabits per second was launched against the software development platform GitHub. This was an amplification attack wherein the attacker sent IP spoofed requests to many memcached database servers which then forwarded a huge amount of reply traffic to the victim machine. For a period of time during the attack, GitHub users were unable to access the server.

    Which security goal (Availability/Integrity/Confidentiality) was compromised by this DDoS attack? Briefly explain your reasoning**. (6 pts)**

31. USB thumb drives are very convenient portable storage, however they also pose security risks. Identify two (2) security problems that may arise from the use of USB thumbdrives, and suggest two (2) solutions that can mitigate the risk whilst still allowing staff to have the convenience of these portable storage devices. **(10 pts)**

32. After studying the Bell-Lapadulla and the Biba security models, a student concludes that it is impossible to address both Confidentiality and Integrity simultaneously because of the first two rules of these models. Explain the reason why the student comes to that conclusion, and whether or not you agree with the student's finding. **(10 pts)**

33. Max works in a large state department of alcoholism and drug abuse. The agency administers programs for individuals with alcohol and drug problems, and maintains a huge database of information on the clients who use their services. Some of the data files contain the names and current addresses of clients. Max has

been asked to take a look at the track records of the treatment programs. He is to put together a report that contains the number of clients seen in each program each month for the past five years, length of each client' s treatment, number of clients who return after completion of a program, criminal histories of clients, and so on. In order to put together this report, Max has been given access to all files in the agency's mainframe computer. After assembling the data into a file that includes the clients' names, he downloads it to the computer in his office. Under pressure to get the report finished by the deadline, Max decides he will have to work at home over the weekend in order to finish on time. He burns the information onto a CD and takes it home. After finishing the report he leaves the CD at home and forgets about it. Identify three (3) relevant clauses of the ACS Professional Code of Conduct for this case study. For each clause, briefly explain the particular ethical issue in this case study. **(8 pts)**