



# The University of Fiji

## School of Science and Technology

Department of Computer Science/ Information Technology

### ITC263 Security and Support in IT

FINAL EXAMINATION - SEMESTER 2, 2013

#### QUESTION PAPER

Time Allowed: 3 Hours (+10 Minutes For Reading the Paper)  
Weighting: 50%  
Total Marks: 100 marks.

| Section | Question Type                | Marks Allocation |
|---------|------------------------------|------------------|
| A       | 40 Multiple Choice           | 20 marks         |
| B       | 30 Short-Answers\Descriptive | 80 marks         |

#### Instructions

- Answer All Questions in the ANSWER BOOKLET provided.
- Answer Multiple Choice questions in the Grid provided and attach it to the Answer Booklet.
- Show your answers clearly in each question to gain maximum marks.
- You may ask for extra sheets from the supervisors if the need arises.
- Do not forget to write your name and ID number on all the extra sheet(s) attached.

## Section A – 40 Multiple Choice Questions (20 marks)

Circle the letter representing the best answer in the Multiple Choice Grid in the Answer Booklet.

1. Each of the following is a reason why it is difficult to defend against today's attackers except \_\_\_\_\_.
  - a. speed of attacks
  - b. greater sophistication of attacks
  - c. complexity of attack tools
  - d. delays in patching hardware and work software products
2. A(n) \_\_\_\_\_ is a person or thing that has the power to carry out a threat.
  - a. vulnerability
  - b. threat agent
  - c. exploit
  - d. risk factor
3. Utility companies, telecommunications, and financial services are considered prime targets of \_\_\_\_\_ because attackers can significantly disrupt business and personal activities by destroying a few targets.
  - a. cyberterrorists
  - b. kiddie scripters
  - c. computer spies
  - d. blue hat hackers (BHH)
4. A(n) \_\_\_\_\_ is a program that secretly attaches itself to a carrier such as a document or program and then executes when that document is opened or program is launched.
  - a. virus
  - b. worm
  - c. rootkit
  - d. Trojan
5. \_\_\_\_\_ is a technique used by spammers to horizontally separate words so they are not trapped by a filter yet can still be read by the human eye.
  - a. Word splitting
  - b. Word layering
  - c. Parsing
  - d. Speckling

6. Attackers use \_\_\_\_\_ to remotely control zombies.
- Google
  - e-mail
  - spam
  - Internet Relay Chat (IRC)
7. A(n) \_\_\_\_\_ is a general software security update intended to cover vulnerabilities that have been discovered.
- service pack
  - hotfix
  - patch
  - critical update
8. A cookie that was not created by the Web site that attempts to access it is called a(n)
- first-party cookie
  - second-party cookie
  - third-party cookie
  - fourth-party cookie
9. A(n) \_\_\_\_\_ is a program that does not come from a trusted source.
- ActiveX Controller Entity
  - signed JavaScript application
  - JavaScript applet
  - unsigned Java applet
10. A(n) \_\_\_\_\_ is an account on a device that is created automatically to aid in installation and should be deleted once that is completed.
- default account
  - back door
  - User Installation Account (UIA)
  - privilege account
11. A man-in-the-middle attack \_\_\_\_\_.
- can be defeated by using the TCP/IP protocol
  - intercepts legitimate communication and forges a fictitious response
  - is only found on a wireless network
  - are always passive

12. A group of Bluetooth piconets in which connections exist between different piconets is called a(n) \_\_\_\_\_.
- a. scatternet
  - b. OPNET
  - c. double piconet (DP)
  - d. slavenet
13. Which of the following is not true regarding a demilitarized zone (DMZ)?
- a. It contains servers that are only used by internal network users
  - b. It typically has an e-mail or Web server
  - c. It can be configured to have one or two firewalls
  - d. provides an extra degree of security
14. Each of the following can be used to hide information about the internal network except \_\_\_\_\_.
- a. Network address translation (NAT)
  - b. Proxy server
  - c. subnetting
  - d. protocol analyzer
15. A honeypot is used for each of the following except \_\_\_\_\_.
- a. Deflect attention away from real servers
  - b. Filter packets before they reach the network
  - c. Provide early warning of new attacks
  - d. Examine attacker techniques
16. The Service Set Identifier (SSID) \_\_\_\_\_.
- a. serves as the network name for a WLAN
  - b. is only used on IEEE 802.11g networks
  - c. is optional on all networks
  - d. is used only with closed system authentication
17. The two models for personal wireless security developed by the Wi-Fi Alliance are Wi-Fi Protected Access (WPA) and \_\_\_\_\_.
- a. Protected Wireless Security (WPS)
  - b. IEEE 802.11x
  - c. Postshared Key Protection (PKP)
  - d. Wi-Fi Protected Access 2 (WPA2)

18. The IEEE standard for wireless security is known as \_\_\_\_\_.  
a. IEEE 803.x  
b. IEEE Wi-Fi Protected Access  
c. IEEE 802.11i  
d. IEEE PSK
19. In the \_\_\_\_\_ model, the end user cannot change any security settings.  
a. Discretionary Access Control  
b. Mandatory Access Control  
c. Security Access Control  
d. Restricted Access Control
20. A(n) \_\_\_\_\_ uses buttons that must be pushed in the proper sequence to open the door.  
a. keyboard lock  
b. user bolt lock (UBL)  
c. pad lock  
d. cipher lock
21. Each of the following make up the AAA elements in network security except \_\_\_\_\_.  
a. determining user need (analyzing)  
b. controlling access to network resources (authentication)  
c. enforcing security policies (authorization)  
d. auditing usage (accounting)
22. \_\_\_\_\_ is an authentication protocol available as a free download and runs on Microsoft Windows Vista, Windows Server 2008, Apple Mac OS X, and Linux.  
a. IEEE 802.1x  
b. RADIUS  
c. Kerberos  
d. LDAP
23. Using one authentication to access multiple accounts or applications is known as \_\_\_\_\_.  
a. credentialization  
b. identification authentication  
c. federal login  
d. single sign-on

24. \_\_\_\_\_ is a current snapshot of the security of an organization.
- a. Risk evaluation
  - b. Threat mitigation
  - c. Asset liability
  - d. Vulnerability appraisal
25. The \_\_\_\_\_ is the proportion of an asset's value that is likely to be destroyed by a particular risk.
- a. Annualized Rate of Occurrence (ARO)
  - b. Annualized Loss Expectancy (ALE)
  - c. Single Loss Expectancy (SLE)
  - d. Exposure Factor (EF)
26. Each of the following is a state of a port that can be returned by a port scanner except \_\_\_\_\_.
- a. Busy
  - b. Open
  - c. Closed
  - d. Blocked
27. Client request and server responses are found in which type of logs?
- a. System event logs
  - b. Risk security logs
  - c. User application logs
  - d. Security alert logs
28. \_\_\_\_\_ refers to a methodology for making changes and keeping track of those changes, often manually.
- a. Change management
  - b. Resource logging
  - c. Assessment auditing
  - d. Vulnerability scanning
29. Each of the following is a monitoring mechanism except \_\_\_\_\_.
- a. Anomaly-based monitoring
  - b. Signature-based monitoring
  - c. Risk-based monitoring
  - d. Behavior-based monitoring

30. Data that is to be encrypted by inputting into an algorithm is called \_\_\_\_\_.  
a. clear text  
b. open text  
c. ciphertext  
d. plaintext
31. Each of the following is an example of how hashing is used except \_\_\_\_\_.  
a. bank automatic teller machine (ATM)  
b. verifying a user password entered on a Linux system  
c. determining the integrity of a message  
d. encrypting and decrypting e-mail attachments
32. When Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, which key does he use to encrypt the message?  
a. Bob's public key  
b. Alice's public key  
c. Bob's private key  
d. Alice's private key
33. Which of the following asymmetric cryptographic algorithms is the most secure?  
a. RSA  
b. B.MD-17  
c. SHA-2  
d. ERFGA
34. A digital certificate associates \_\_\_\_\_.  
a. the user's identity with their public key  
b. a user's private key with the public key  
c. a digital signature with a user  
d. a private key with a digital signature
35. What is the cryptographic transport protocol that is used most often to secure Web transactions?  
a. HTTPS  
b. SHTTP  
c. PPPTPoE  
d. MD-17

36. A digital certificate that turns the address bar green is a(n) \_\_\_\_\_.  
a. Extended Validation SSL Certificate  
b. Web Server Advanced Certificate  
c. Personal Web-Client Certificate  
d. Internet Standard Certificate
37. "RAID" is an abbreviation of \_\_\_\_\_.  
a. Resilient Architecture for Interdependent Discs  
b. Redundant Array of Independent Drives  
c. Redundant Array of IDE Drives  
d. Resistant Architecture of Inter-related Data Storage
38. Which of the following is NOT a characteristic of a disaster recovery plan (DRP)?  
a. It is a private document only used by top-level administrators for planning.  
b. It is written.  
c. It is detailed.  
d. It is updated regularly.
39. When an unauthorized event occurs, the first duty of the computer forensics response should be to \_\_\_\_\_.  
a. log off from the server  
b. secure the crime scene  
c. back up the hard drive  
d. reboot the system
40. Each of the following is what a security policy must do except \_\_\_\_\_.  
a. State reasons why the policy is necessary  
b. Be able to implement and enforce it  
c. Be concise and easy to understand  
d. Balance protection with productivity
-

## Section B - Short Answers/Descriptive (80 marks)

### Introduction to Security [7 marks]

1. Discuss the five steps of an attack. [5 marks]
2. Multiple defenses may be necessary to withstand any attack. Explain at least two fundamental security principles on which defenses should be based. [2 marks]

### Systems Threats and Risks [7 marks]

3. State three primary objectives of *malware*. [3 marks]
4. Explain at least three effects of *spyware*. [3 marks]
5. State two techniques used by image spammers. [1mark]

### Application and Network Attacks [6 marks]

6. List four common web application attacks. [2 marks]
7. What does the attacker do in ARP poisoning and DNS poisoning attacks? [2 marks]
8. Explain persistent *cookie* and a *secure cookie*? [2 marks]

Vulnerability Assessment and Mitigating Attacks [7 marks]

9. List the step(s) for each *Risk Identification Action*.

[5.5 marks]

| Risk Identification Action | Steps          |
|----------------------------|----------------|
| 1. Asset identification    | A.<br>B.<br>C. |
| 2. Threat identification   | A.<br>B.       |
| 3. Vulnerability appraisal | A.<br>B.       |
| 4. Risk assessment         | A.<br>B.<br>C. |
| 5. Risk mitigation         |                |

10. Explain the three types of *penetration testing*: *black box*, *white box*, and *grey box testing*.  
[1.5 marks]

Host, Application and Data Security [5 marks]

11. List at least five recommended *key management procedures*.

[2.5 marks]

12. List five-step process for protecting operating systems.

[2.5 marks]

Network Security [5 marks]

13. State at least four functions of a *network switch*.

[2 marks]

14. "OSI model breaks networking step into seven layers. Each layer has a separate networking task and corporates with adjacent layers"  
State the name of *layer 4* and its function.

[1.5 marks]

15. State at least three advantages of *Proxy Server*.

[1.5 marks]

Administrating a Secure Network [7 marks]

16. State at least four configuration tasks to secure a router. [2 marks]
17. List the six steps of 802.1x authentication process [3 marks].
18. State two enhanced security features provided by IPv6. [2 mark]

Wireless Network Security [3.5 marks]

19. "Attacks using Access Points include *Rouge Access Points* and *Evil Twins*". Explain each. [2 marks]
20. Explain the three steps of Open-System authentication. [1.5 marks]

Access Control Fundamentals [8 marks]

21. Give *descriptions* and *computer processes* of the four basic steps (*actions*) in access control. [6 marks]
22. List at least four best-practices for access control. [2 marks]

Authentication and Account Management [5.5 marks]

23. List the three kinds of authentication credentials, with examples. [3 marks]
24. State at least five password management practices. [2.5 marks]

Basic Cryptography [6.5 marks]

25. State the three categories of cryptographic algorithms. [1.5 marks]
26. "There are five basic protections that cryptography can provide for information security. List and describe each. [5 marks]

Advanced Cryptography [5.5 marks]

27. "The life cycle of a Public Key Infrastructure (PKI) digital certificate is typically divided into four parts". List and briefly explain each part. [4 marks]
28. What are the three classes of digital certificates? [1.5 marks]

Business Continuity [7 marks]

29. Compare characteristics of a cold site, warm site, and hot site. [3 marks]
30. Describe the four common RAID levels (0, 1, 5, 0+1). [4 marks]

**THE END**