



The University of Fiji



SCHOOL OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE / INFORMATION TECHNOLOGY

FINAL EXAMINATION SEMESTER II, 2015

SECURITY AND SUPPORT IN IT

ITC263

Time Allowed: Three hours (3 hours)

(An extra ten minutes is allowed for reading this paper)

INSTRUCTIONS

- 1.0 Write **all** your answers in the **Answer Book** provided.
- 2.0 There are seven (7) pages of questions in this Question Booklet (excluding the Cover Page)
- 3.0 Write your **Student Identification Number** on the front page of the **Answer Book**.
- 4.0 If you use extra sheets of paper, be sure to show clearly the question number(s) being answered and to tie each sheet securely in your Answer Book at the appropriate place.
- 5.0 There are **three** sections in this paper; **Section A** consists of 20 multiple choice and is worth 20 marks, **Section B** consists of 23 short answer questions and is worth 60 marks, **Section C** consists of 4 scenario-based questions and is worth 20 marks.
- 6.0 **Programmable calculators** are not allowed.

SECTION A: MULTIPLE CHOICE QUESTIONS**20 MARKS**

Write the question number and the letter representing the best answer in the Answer Book.

1. You can use the upgrade installation method when upgrading from Windows Vista Business to which of the following?
 - A. Windows 7 Home Basic
 - B. Windows 7 Home Premium
 - C. Windows 7 Professional
 - D. Windows 7 Business
2. Which of the following is not an account type in Windows 7?
 - A. Guest
 - B. Limited user
 - C. Standard user
 - D. Administrator
3. Which of the following is not a UAC notification level?
 - A. Always notify me
 - B. Notify me only when users try to access my files
 - C. Notify me only when programs try to make changes to my computer
 - D. Never notify me of installations or changes
4. What do you call the process of disabling unneeded services and ports to make a system more secure?
 - A. Reducing the surface attack area
 - B. Mitigating a Trojan Horse
 - C. Security avoidance
 - D. Defense in depth
5. Where do you configure security zones in Internet Explorer 9?
 - A. Internet Options Security tab
 - B. Internet Options Privacy tab
 - C. Safety menu
 - D. Tracking Protection window
6. Why would you use a minimum password age?
 - A. To ensure that someone does not guess a password
 - B. To stop someone from trying over and over to guess a password
 - C. To make sure a user does not reset a password multiple times until he or she can reuse his or her original password
 - D. To automatically reset a password

7. Which of the following do you access to enter Safe Mode the next time the computer starts?
- A. The General tab
 - B. The Boot tab
 - C. The Start-up tab
 - D. Services console
8. What authorizes a user to perform certain actions on a computer?
- A. Permission
 - B. Encryption Algorithm
 - C. Right
 - D. Authentication Protocol
9. At which layer of the OSI model does routing occur?
- A. Physical
 - B. Network
 - C. Data link
 - D. Transport
10. What is the maximum disk size NTFS can handle?
- A. 32GB
 - B. 256GB
 - C. 32TB
 - D. 256TB
11. BitLocker can use a chip, found on some computers, to protect BitLocker encryption keys. What is the name of the chip?
- A. Trusted Platform Module
 - B. Trusted Protection Module
 - C. Encryption Platform Module
 - D. Trusted Hard Drive Module
12. When using Microsoft's free cloud storage solutions, which solution requires software to be installed on the client computer?
- A. Windows Live SkyDrive
 - B. Windows Live Mesh
 - C. OneNote to SkyDrive
 - D. Hotmail

13. Which of the following are password-based attacks?
- A. Replay Attacks
 - B. Man-in-middle attacks
 - C. Network sniffer attacks
 - D. Dictionary attacks
14. After you compress a folder in *Windows Explorer*, in what color is it displayed in Windows 7?
- A. Blue
 - B. Green
 - C. Black
 - D. Red
15. When your peer-to-peer network has a mix of Windows 7, Windows Vista, and Windows XP computers, which of the following should be used for file sharing?
- A. Public folders
 - B. HomeGroup
 - C. A workgroup
 - D. A domain
16. Which system does Microsoft Forefront Endpoint Protection require?
- A. Windows Server 2008 R2
 - B. Windows Server 2008 R2 or later versions
 - C. System Center Configuration Manager 2007
 - D. Windows 7
17. The process of eliminating a risk by choosing not to engage in an action or activity describes which of the following?
- A. Mitigation
 - B. Residual risk
 - C. Avoidance
 - D. Acceptance
18. Which of the following requires its own power connector?
- A. eSATA
 - B. USB
 - C. FireWire
 - D. USB 2.0

19. Which type of malware copies itself onto other computers without the owner's consent and will often delete or corrupt files?
- A. Virus
 - B. Worm
 - C. Trojan horse
 - D. Spyware
20. Say that you receive an email stating that your account has just expired and asking you to log in to a legitimate-looking website to fix the problem. What is this an example of?
- A. Phishing
 - B. Pharming
 - C. Phaking
 - D. IP address spoofing

SECTION B: SHORT ANSWER QUESTIONS**60 MARKS**

All questions in this section are compulsory

1. Computing can be divided in 32-bit and 64-bit computing. What does 32-bit and 64-bit signify. Describe a major difference between a 32-bit and a 64-bit computer.
[2 Marks]
2. Describe the process of Zero Touch Installation (ZTI).
[2 Marks]
3. What is a system Image from a Windows point of view and what is it used for?
[2 Marks]
4. What is the User Account Control (UAC) feature of Windows 7? List 6 actions that can trigger a UAC.
[4 Marks]
5. The bottom portion of the Ease of Access Center window includes other accessibility options you can configure for visually or hearing impaired users. List at least 4 accessibility options that are provided.
[2 Marks]
6. Explain the process of pinning a website from Internet Explorer to Windows 7 taskbar.
[2 Marks]

7. Define Group Policy, Group Policy Objects and Active Directory. Briefly describe the relationship between the three.
[4 Marks]
8. Compare and Contrast between Encrypting File System (EFS) and BitLocker Drive Encryption feature of Windows.
[2 Marks]
9. List the three broad categories of network locations in Windows 7 and identify the most restrictive network location.
[2 Marks]
10. What is Windows Registry and what are the 3 components that make up the windows registry?
[3 Marks]
11. Explain the "*Principle of Least Privilege*" in security fundamentals.
[1 Mark]
12. List the three methods that are used for authentication with examples of each method of authentication.
[3 Marks]
13. List and briefly explain the two types of permissions used in NTFS.
[2 Marks]
14. Explain the difference between a dictionary attack and a Brute Force attack.
[2 Marks]
15. Let's say you have a PIN that is four digits long. Each digit can be 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9, giving you a total of 10 possible digits. How many different PINs are possible?
[2 Marks]
16. List and briefly describe the three common types of protocol spoofing?
[3 Marks]
17. What Social Engineering. Provide an example to support your answer.
[2 Marks]
18. List and briefly describe the 7 layers of the OSI model?
[7 Marks]

19. Compare and contrast between intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

[2 Marks]

20. In computer networking, a DMZ (*demilitarized zone*) is a firewall configuration used to secure hosts on a network segment. What are the two typical DMZ configurations you may encounter in production?

[2 Marks]

21. Define what is a firewall and how does it work?

[2 Marks]

22. Malware can be divided into several categories. List the 6 categories you have learnt.

[3 Marks]

23. List 8 common symptoms of malware infection.

[4 Marks]

SECTION C: CASE BASED QUESTIONS

20 MARKS

All questions in this section are compulsory

1. You are the Security Manager for a medium-sized bank. You have been asked to design a security solution to keep intruders out of the bank after hours. The three areas of the bank you need to secure are the parking lot, the building perimeter, and the vault. List the technologies you would use in each of these areas.

Note: List 5 security technologies each for the three areas (Parking lot, building perimeter and vault)

[6 Marks]

2. You are the IT administrator for the Contoso Corporation. Your CIO wants you to investigate the possible use of biometrics for security purposes. The CIO understands what biometrics is and how this technology can be used, but he does not understand the potential disadvantages of using biometrics. What should you tell him?

Note: List at least 3 points and discuss thoroughly.

[5 Marks]

3. Imagine that you work for the Contoso Corporation. Your CIO tells you that he just got a message on his computer saying that he has to change his password. He wants to know why he must not only use such a relatively long password, but also why he must change that password on a regular basis. What should you tell him?

Note: Discuss each point in the question thoroughly explaining the importance and threats.

[4 Marks]

4. You were hired as an IT administrator for the ABC Company. Across from your desk, there is a table with seven physical servers. You go to your boss and ask why the servers are out in the open and not locked up. He says there are located on the table so that they can be easily monitored and watched. How should you respond to your boss?

Note: Discuss at least 3 threats thoroughly.

[5 Marks]

THE END