



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, 2012

QUESTION PAPER

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

Section	Question Type	Marks Allocation
A	20 Multiple Choice	20 marks
B	27 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—Multiple Choice Questions(20 marks)

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

1. An example of a(n) _____ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password.
 - a. vulnerability
 - b. threat
 - c. threat agent
 - d. asset exploit (AE)

2. _____ is exploiting a vulnerability in the software to gain access to resources that the user would normally be restricted from obtaining.
 - a. Vulnerability assessment
 - b. Software threat release (STR)
 - c. Hardware virus
 - d. Privilege escalation

3. A(n) _____ is a cumulative package of all security updates plus additional features.
 - a. service pack
 - b. update
 - c. update rollup
 - d. hotfix patch

4. War driving exploits _____, which is the wireless access point sending out information about its presence and configuration settings.
 - a. scanning
 - b. beaconing
 - c. location frame stamping
 - d. SGP mapping

5. 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
6. Each of the following can be used to monitor airwaves for traffic except a(n) _____.
- a. dedicated probe
 - b. access point probe
 - c. resource monitor probe
 - d. wireless device probe
7. 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
8. Creating a pattern of when and from where a user accesses a remote Web account is an example of _____.
- a. computer footprinting
 - b. Time-Location Resource Monitoring (TLRM)
 - c. cognitive biometrics
 - d. keystroke dynamics
9. _____ is a method of evaluating the security of a computer system or network by simulating a malicious attack.
- a. Probing
 - b. Hacker simulation
 - c. Vulnerability assessment
 - d. Penetration testing

10. When permissions are assigned to a folder, any current subfolders and files within that folder _____.
- a. inherit the same permissions
 - b. can be deleted only by the administrator
 - c. are available to the currently logged-in user
 - d. cannot be accessed
11. Data that is to be encrypted by inputting into an algorithm is called _____.
- a. clear text
 - b. open text
 - c. ciphertext
 - d. plaintext
12. A cryptographic transport protocol for FTP is _____.
- a. RAS-256
 - b. MIME
 - c. UNIX Remote Shell encryption (UNIX-RSE)
 - d. Secure Sockets Layer
13. 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
14. A(n) _____ defines the actions users may perform while accessing systems and networking equipment.
- a. acceptable encryption policy
 - b. information sensitivity policy
 - c. email policy
 - d. acceptable use policy

15. The _____ is primarily responsible for design, configuration, installation, and maintenance of technical security equipment.
- a. Chief Information Security Officer (CISO)
 - b. security manager
 - c. security administrator
 - d. security technician
16. The TCP/IP protocol _____ handles incoming mail.
- a. Post Office Protocol (POP)
 - b. Simple Mail Transfer Protocol (SMTP)
 - c. IMAP4
 - d. Microsoft Mail Transport (MMT)
17. _____ is pretending to be someone or something else by presenting false information.
- a. replay
 - b. Denial of service
 - c. man in the middle
 - d. spoofing
18. _____ create a large pre-generated data set of hashes from nearly every possible password combination.
- a. LM hashes
 - b. NTLM databases
 - c. Dictionary tables
 - d. Rainbow tables
19. 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

20. In RAID _____ data is written twice to separate drives.

- a. Level 0
- b. Level 1
- c. Level 2
- d. Level 5

Section B - Short Answers/Descriptive (80 marks)

Introduction to Security [6 marks]

21. Define *information security*.

[2 marks]

22. Discuss four reasons why it is difficult to defend against today's attacks.

[1+1+1+1marks]

Systems Threats and Risks [7 marks]

23. Explain one difference between the infecting malware *virus* and *worm*.

[2 marks]

24. Discuss the concealing malware *Trojan horse*.

[2 marks]

25. Malware with a profit motive includes *spam*, *spyware*, and *botnets*.D

[1+1+1 marks]

Protecting Systems [8 marks]

26. Discuss the statement, "Hardening the operating system to resist attacks is often a three-pronged approach."

[1+1+1 marks]

27. "Along with hardening the operating system to resist attacks, it is important to protect systems from attacks that come through the Web browser. These attacks involve using cookies, JavaScript, Java, ActiveX, and cross-site scripting."

What are the defenses against each (cookies, JavaScript, Java, ActiveX, and cross-site scripting)?

[1+1+1+1+1 marks]

Network Vulnerabilities and Attacks [7 marks]

28. "Monitoring network traffic for media based vulnerabilities is an important task for a network administrator. It helps to identify and troubleshoot network problems, such as a network interface card (NIC) adapter that is defective and is sending out malformed packets. Monitoring traffic can be done in two ways."
Discuss these two ways.

[2+2 marks]

29. Explain three characteristics of a weak password.

[1+1+1 marks]

Network Defenses [6 marks]

30. Explain at least three advantages of subnetting.

[1+1+1 marks]

31. "The basis of a firewall is a rule base. The rule base establishes what action the firewall should take when it receives a packet."

Explain the three typical options in a firewall rule base?

[1+1+1 marks]

Wireless Network Security [7 marks]

32. List the two types of device authentication supported by the 802.11 standard.

[2 marks]

33. List the 5-steps of 802.1x authentication procedure in enterprise wireless security.

[5marks]

Access Control Fundamentals [5 marks]

34. List the basic steps in access control.

[2 marks]

35. Discuss at least three physical access control methods.

[3 marks]

Authentication[5 marks]

36. Explain the authentication model “Single Sign-on (SSO)”, with an example. [1+1marks]

37. “AAA (Triple A) stand for three key elements in security.”
Discuss each element. [1+1+1 marks]

Performing Vulnerability Assessment [7 marks]

38. Define “risk management”. [2 mark]

39. Discuss the five risk identification actions and the steps in each. [5 marks]

Risk Identification Action	Steps

Conducting Security Audits [5 marks]

40. Discuss one type of “security application log”. [2 marks]

41. Discuss “signature-based monitoring”. [3 marks]

Basic Cryptography [5 marks]

42. "The simplest type of stream cipher is substitution cipher."
Using an example, explain how monoalphabetic substitution cipher works.

[1+1 marks]

43. "There are five basic protection that cryptography can provide for information security. The first three characteristics are confidentiality, integrity, and availability."
Describe the protection provided by the remaining two characteristics.

[1 ½ + 1 ½ marks]

Characteristic	Description	Protection

Applying Cryptography [6 marks]

44. What is Public Key Infrastructure (PKI)?

[2 marks]

45. "The life cycle of a digital certificate is typically divided into four parts".
Briefly explain each part.

[1+1+1+1 marks]

Business Continuity [6 marks]

46. What is "Van Eck phreaking"?

[2 marks]

47. List and describe the four types of data backups.

[1+1+1+1 marks]

Type of backup	Description

THE END

