THE STATE UNIVERSITY OF ZANZIBAR

SCHOOL OF COMPUTING, COMMUNICATION AND MEDIA
DEPARTMENT OF COMPUTER SCIENCE
END OF SEMESTER EXAMINATION
SEMESTER 2

PRINCIPLES OF COMPUTER AND NETWORK SECURITY – CS 2216

Date: 02- 08- 2024 **Time: 02:00 PM – 05:00 PM**

INSTRUCTIONS

1. This paper consists of **TWO** sections, **A** and **B** which carries 24 and 36 marks respectively.
2. Answer all questions from section A, and any THREE questions from section B.
3. Cellular phones and any other unauthorized materials are NOT allowed in the examination room.
4. **ANSWER EACH QUESTION ON SEPERATE SHEET**
5. This exam consists of six (6) printed pages, including cover page

SECTION A [24 Marks]

Answer all Questions from this Section

1 Choose the correct answer and write the letter of result beside the question number **[10 marks]**

a. What is the primary goal of information security?
   A) To protect the physical components of a computer system.
   B) To ensure confidentiality, integrity, and availability of data.
   C) To facilitate confidentiality, integrity, and availability of data to everyone.
   D) To enhance the speed of network connections.

b. A security incident refers to:
   A) Breach of security policy that poses a threat to information assets.
   B) A new update to antivirus software that poses a strength to information assets.
   C) An increase in secured network speed over unsecured network.
   D) Regular maintenance of hardware components.

c. In risk management, what is the purpose of a risk mitigation strategy?
   A) To completely eliminate all risks.
   B) To accept all risks and move on.
   C) To reduce the impact or likelihood of a risk.
   D) To ignore risks and focus on profits.

d. Which protocol is commonly used for secure remote access?
   A) FTP
   B) HTTP
   C) Telnet
   D) SSH

e. An Intrusion Detection System (IDS) primarily:
   A) Prevents unauthorized access to network resources and services.
   B) Detects and monitors unauthorized access or attacks.
   C) Repairs damaged network hardware and software.
   D) Increases network bandwidth.

f. A Denial of Service (DoS) attack aims to:
   A) Steal confidential information.
   B) Encrypt files for ransom.
   C) Make a service unavailable to its intended users.
   D) Redirect traffic to a malicious website.

g. Which type of malware is designed to spread without user intervention?
   A) Virus
   B) Trojan
   C) Worm
   D) Spyware

h. In the context of digital forensics, "slack space" refers to:
   A) Unused space in a file cluster.
   B) The time delay between data transfers.
   C) The unused capacity of a hard drive.
   D) The amount of data that can be compressed.

i. Which of the following best describes the concept of "chain of custody" in digital forensics?
   A) A sequence of network protocols used for secure data transfer.
   B) A process ensuring that digital evidence is stored securely and remains untampered.
   C) A method for compressing digital files to save space.
   D) A technique for encrypting digital communications.

j. The GDPR primarily aims to:
   A) Improve internet speeds across Europe.
   B) Protect personal data and privacy of individuals in the EU.
   C) Enhance the capabilities of digital forensic tools.
   D) Develop new encryption algorithms.

2 ***Write short notes on the following questions*** ***[10 marks]***

a. What is the deference between information security and cybersecurity?

b. Explain the concept of a digital signature.

c. How is risk differ from a threat or vulnerability?

d. What are some best practices for securing remote access to corporate networks?

e. What is disaster recovery planning in the context of information security?

3 Decrypt the message "FRQJUDWXODWLRQV BRX PDGH LW" using the Caesar shift of 3 substitution cipher. ***[4 marks]***

SECTION B [36 Marks]

Answer only three (3) questions from this Section.

4 An employee at a bank is suspected of altering financial records to conceal unauthorized transactions. The IT security team has detected unusual activity in the database logs, and a forensic investigation is launched.

a. Explain the steps involved in conducting a forensic investigation to detect data tampering. **[4 marks]**

b. Propose measures to prevent data tampering in the future. **[4 marks]**

c. Discuss the legal implications of data tampering for both the employee and the bank. **[4 marks]**

5 A hospital's network is infected with ransomware, encrypting patient records and disrupting medical services. The attackers demand a ransom in cryptocurrency. The hospital must decide whether to pay the ransom and how to restore operations.

a. Analyze the ethical considerations involved in deciding whether to pay the ransom. **[4 marks]**

b. Outline the forensic steps taken to identify the ransomware variant and trace its origins. **[4 marks]**

c. Discuss the long-term measures the hospital should implement to prevent future ransomware attacks. **[4 marks]**

6 In a medium-sized organization, the IT department consists of several teams, each responsible for different aspects of IT management. You need to delegate administrative tasks to team members without giving them full administrative rights. How would you set up RBAC in Windows to accomplish this? **[12 marks]**

Note that:

i. The Help Desk team should be able to reset user passwords and unlock accounts.

ii. The Network team should manage DNS and DHCP settings but not have access to user accounts.

iii. The Server team should manage server configurations and perform system updates but should not modify network settings or user accounts.

7 You have a project directory *'/project'* that needs to be shared among members of the 'developers' group. However, only the owner (a user named alice) should have write access, while others should have read-only access. Additionally, only the root user should be able to modify the permissions of this directory. Explain how would you configure this? **[12 marks]**

8 You are a cybersecurity expert working for a financial institution. One day, you receive an urgent call from the Chief Information Security Officer (CISO) reporting that the bank's online banking system has been compromised. Customers are complaining about unauthorized transactions, and there is a significant amount of money missing from several accounts. Initial investigations suggest that the attack was conducted using a sophisticated phishing campaign combined with malware to capture login credentials and execute unauthorized transactions.

a. Describe the steps you would follow to conduct a thorough investigation of the cybercrime. **[4 marks]**

b. How would you determine the entry point and the attack vectors used by the cybercriminals? **[4 marks]**

c. What are the legal implications of this cybercrime, and how should you collaborate with law enforcement agencies during the investigation? **[4 marks]**

WISH YOU ALL THE BEST

THE STATE UNIVERSITY OF ZANZIBAR
SCHOOL OF COMPUTER, COMMUNICATION & MEDIA STUDIES (SCCM)
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
FINAL EXAMINATION
SEMISTER II – 2022/2023

CS/INF 2216 - Principles of Computer & Network Security

Date: 21, July, 2023 **Time:** 2:00 pm – 05:00 pm

---

1. This paper consists of Two Section, Section A and Section B. Answer ALL question from Section A and any 3 questions from section B.
2. Sections A and B carries 24 marks and 36 marks, respectively.
3. Cellular phones and any other unauthorized materials are **NOT allowed** in the examination room
4. Make sure that the points you make are not repetitive within your answer. Also, each question addresses a different issue. If you find yourself repeating the same information as you answer different questions, you may be on the wrong track.
5. Answer each question in separate page. Any attempt to answer more than questions required will not be entertained
6. This exam consists of printed 5 pages, including cover page.

Answer all questions in this section.

This Section carries 24 marks.

Question One: Choose a correct answer from multiple answers by writing a letter to the corresponding question. (12 marks, 1 mark each)

I. Digital certificates used in Transport Layer Security (TLS) support which of the following?
   A. Information input validation
   B. Non-repudiation controls and data encryption
   C. Multi-Factor Authentication (MFA)
   D. Server identity and data confidentially

II. Which protocol uses the SSL?
   A. SSH
   B. HTTPS
   C. HTTP
   D. Telnet

III. If a message between a client and server is comprised of several back and forth exchanges (think of an email to a friend and their reply back to you), the _____ keeps the entire communication thread secure.
   A. Digital certificate
   B. Message authentication code
   C. Message (sometimes called record) protocol
   D. Cryptography

IV. Ali wants to send Bahati an email that includes sensitive information, and he does not trust the network that he is connected to. Bahati gives him the idea of using PGP. What should Ali do to communicate correctly using this type of encryption?
   A. Use his own private key to encrypt the message.
   B. Use his own public key to encrypt the message.
   C. Use Bahati's private key to encrypt the message.
   D. Use Bahati's public key to encrypt the message

V. Handshake protocol refers to
   A. Confirming that one of the many lines of communication between the sending client and receiving server is not already in use.
   B. Sending an electronic key attached to the message so that the receiving server can be unlocked as the message is coming in.
   C. Verifying that the message sender and message receiver have available communication channels that intersect in the middle.
   D. Establishing a secure communications path between the message sender and received

VI. A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?
   A. Shoulder surfing
   B. Phishing
   C. Insider Accomplice
   D. Vishing

VII. James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf
B. Trinoo
C. Fraggle
D. SYN flood

VIII. War driving attack is an attempt to exploit what technology?

A. Fiber optic networks whose cable often run along roads and bridges
B. Cellular telephone
C. The public switched te4lephone network
D. Wireless networks

IX. Malicious code that is set to execute its payload on a specific date or at a specific time is known as

A. Logic bomb
B. Trojan horse
C. Virus
D. Time bomb

X. Update software loaded on non-volatile storage devices such as ROM is called

A. Buffer overflows
B. Firmware updates
C. Hotfix
D. Service pack

XI. You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of the lack of space, casting is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

A. Transference
B. Mitigation
C. Avoidance
D. Acceptance

XII. ARP and RARP are used to map which of the following?

A. MAC address to DNS host
B. MAC address to IP addresses
C. IP addresses to DNS hostnames
D. DNS hostname to MAC address

Question Two (6 marks)

a) Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Outline five (5) components of risk when collecting and analyzing data (2.5 marks)

b) Write three basic activities of risk assessment process. (1.5 marks)

c) What are the two *conditions/factors* influence the management of organization to accept certain level of risk (2 marks)

Question Three (6 marks)

a) Use Caesar's Cipher (substitution cipher) to encrypt the following plaintext SECURITY AND PRIVACY, using the below cipher pattern (3 marks).
Note: Every character in the first row *is replaced with the character three* slots to the right

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	J	K	I	L	M	N	O	P	O	R	S	T	U	V	W	X	Y	Z	A	B	C

b) Brute force attack is the hacking method that uses *trial and error* to crack passwords, login credentials, and encryption keys.
   i. Write three signs that can be observed during and/or after brute force attacks in computer systems (1.5 marks)
   ii. Outline three tools that can be used to perform brute force attacks in window and Linux platforms. (1.5 marks)
   - kasheat
   - aircrack
   - Nmap
   - John the ripper

Section B: Answer any THREE (3) questions.
This Section consists of 36 marks, each question carries equal mark.

Question Four (12 marks)

a) Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Briefly describe four types of malicious codes that could take forms of software that have been design to enhance web pages and/or email applications (4 marks)
b) Suppose you are concerned that your browser has malicious code running within it, though you are confident that your operating system has not been compromised. You type *www.projectsuza.ac.tz* into your browser's address bar to take you to the SUZA project site. Briefly describe two steps/actions you could take (which could involve additional effort on your part) to check whether your browser sent any information to *www.projectsuza.ac.tz* via cookies as part of that request (4 marks)
c) Define the term 'spoofing' as far as security of Individual's email box in the organization is concerned. (1 mark)
d) Mention two reasons why would someone spoof an email of individual in the organization (3 marks)

Question Five (12 marks)

a) What is the primary goal of TLS/SSL? Describe three properties provided by TLS/SSL (4 marks)
b) Describe two components of TLS/SSL (3 marks)
c) Outline five steps involving in TLS/SSL communication between server and client (5 marks)

Question Six (12 marks)

a) Pretty good privacy (PGP) is an open source and freely available software package for email security. Mention four (4) aspects of security in which PGP is guarantee to provide during email transferring between server and client. (2 marks)

b) Using sketch diagram, write 5 steps taken
   i. By the sender when decides to secure email using PGP software (5 marks)
   ii. By receiver when receiving email message which has been prepared using PGP software (5 marks)

Question Seven (12 marks)

a) Briefly describe the term 'disaster recovery' (1 mark)

b) With example in each, define three types of backup facilities which are normally used during disaster in the organization. (3 marks)

c) What are the three basic questions have to be asked during Business Impact Analysis? (3 marks)

d) Briefly describe why it's important to conduct a testing of developed disaster recovery plan? (2 marks)

e) Differentiate between disaster recovery and business continuity planning (3 marks)

Question Eight (12 marks)

a) With example in each, define the following terms which have been frequently used in computer security (3 marks)
   i. Identification
   ii. Authentication
   iii. Authorization

b) With example differentiate between biometric identification and biometric authentication (3 marks)

c) On your own word, briefly describe the limitations of biometric technology (2 marks)

d) What is access control? Define three models/methods of handling access control (4 marks)

Many thanks

The State University of Zanzibar
School of Computing, Communication and Media Studies
Department of Computer Science and Information Technology
Midterm Test ONE - Principles of Computer Security (CS 2216): 11/05/2023

Answer ALL Questions - 20 Marks (45 min)

Question One (5 marks, each 0.5)

I. The CIA of security includes;
   A. Confidentiality, integrity authentication
   B. Confidentiality, integrity, availability
   C. Certificates, integrity, availability
   D. Confidentiality, inspection, authentication

II. Which of the following concepts requires users and system processes to use the minimal amount of permission necessary to function?
   A. Layer defence
   B. Diversified defence
   C. Single security rule
   D. Least privilege

III. Hiding information to prevent disclosure is an example of
   A. Security through obscurity
   B. Certificate-based security
   C. Discretionary data security
   D. Defence in-depth

IV. The concept of blocking an action unless it is specifically authorized is
   A. Implicit deny
   B. Least privilege
   C. Simple security rule
   D. Hierarchical defence model

V. Which of the following is a physical security threat?
   A. Cleaning crews are allowed unsupervised access because they have contract
   B. Employees undergo background criminal checks before being hired
   C. All data is encrypted before being backed up
   D. All of the above

VI. What device should be used by organization to protect sensitive equipment form fluctuations in voltage?
   A. A surge protector
   B. An uninterruptible power supply
   C. A backup power generator
   D. A redundant array of inline-batteries

VII. Reserve social engineering involves
   A. Contacting the target, eliciting some sensitive information, and convincing them that nothing out of the ordinary has occurred

B. Contacting the target in an attempt to obtain information that can be used in a second attempt with a different individual

C. An individual lower in the chain of command convincing somebody at a higher level to divulge information that the attacker is not authorised to have

D. An attacker attempting to somehow convince the target to initiate contact in order to avoid questions about authenticity

VIII. What are the three types of event logs generated by Microsoft Window OSs

A. Event, Process and Security

B. Application, User and Security

C. User, Event and security

D. Application, System and Security

IX. Which of the following is not a capability of network-based IDS?

A. Can detect denial of service attacks

B. Can decrypt and read encrypted traffic

C. Can decode UDP and TCP packets

D. Can be tuned to a particular network environment

X. Honeypot are used to

A. Monitoring network usage by employees

B. Process alarms from other IDSs

C. Attract customers to e-commerce sites

D. Attract attackers by simulating systems with open network services

Question Two (5 marks)

a) Briefly describe why operational model of computer security acknowledgements the fact that, **prevention technologies are not sufficient** to protect computer infrastructure and networks? **(2 marks)**

b) Social engineering is the process of convincing an authorized individual to provide confidential information. Briefly describe two reasons, why ***social engineering*** activities have been very successful in modern era**. (3 marks)**

Question Three (5 marks)

a) Briefly describe why insiders (inside attacks) are considered to possess a great threat to the organization infrastructure **(2 marks)**

b) With at least one example, briefly describe why the strategy/approach of implementing **'security in depth/layered security', when planning security actions in organization,** is considering a good approach to protect computer and network infrastructure. **(3 marks)**

Question Four (5 marks)

a) Intrusion detection system (IDS) can be categorised in terms of **deployment** and **the way they are detecting the malicious behaviour** in the networks. Briefly describe **the later with its types. (3 marks)**

b) Briefly describe why organization needs to deploy IDS in the networks, while Firewalls are perfectly working in blocking malicious traffics in the networks? **(2 marks)**