

NAMIBIA UNIVERSITY

OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE				
QUALIFICATION CODE: 07BACS	LEVEL: 6			
COURSE CODE: ISS610S	COURSE NAME: IT Systems Security			
DATE: JUNE 2019	PAPER: THEORY			
DURATION: 3 HOURS	MARKS: 100			

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER				
EXAMINER(S)	MR. EDWARD NEPOLO			
	MR. ATTLEE GAMUNDANI			
	MR. JULIUS SILAA			
	MRS. UAKOMBA MBASUVA			
	MS. JOVITA MATEUS			
	MR. ISAAC NHAMU			
MODERATOR:				

INSTRUCTIONS		
	1.	Answer ALL the questions.
	2.	Write clearly and neatly.
	3.	Number the answers clearly.
	4.	When answering questions you should be guided by the allocation of
		marks in (). Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. Non programmable Scientific Calculator.

THIS QUESTION PAPER CONSISTS OF 4 PAGES (Excluding this front page)

Question 1 True or False [10 Marks]

- 1. Information Technology System objects of value include Data, Hardware, and Software. (True / False)
- 2. Harm is a desired outcome of an actualized threat, or an attack. (True / False)
- 3. DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale. (True / False)
- 4. Types of control can either be Physical, Procedural, and Technical. (True / False)
- 5. WEP uses RC4 encryption algorithm, which has cryptographic flaws, due to it's key length and design. (True / False)
- 6. A denial-of-service, or DoS, attack is an attempt to defeat availability, the third of the three basic properties to be preserved in computer security. (True / False)
- 7. With End-to-End Encryption, Data is encrypted just before the system places them on the physical communications link. In this case, encryption occurs at layer 1 or 2 in the OSI model. (True / False)
- 8. In 1999, the Internet Engineering Task Force upgraded SSL 3.0 and named the upgrade TLS, for transport layer security. TLS 1.0, which is sometimes also known as SSL 3.1 (True / False)
- 9. A firewall implements a security policy, that is, a set of rules that determine what traffic can or cannot pass through the firewall. (True / False)
- 10. A community cloud deployment model is shared by the general public, is owned by an organization that sells cloud services. (True / False)

Question 2 Multiple Choice [10 Marks]

- 1. The user interacts with the database through a program called:
- A. DB Control

C. System Controller

B. Database Manager

- D. Database Administration
- 2. The logical structure of a database is called a:
- A. Logic

C. Logical DB

B. Syntax

D. Schema

fields and recor	ct with databases through commands to the DBMS that retrieve, modify, add, or delete on the database. These commands are called: C. Queries D. XSS				
	Data means analysis of massive amounts of, often collected from different different data formats.				
	C. Protocols D. Intrusions				
	es statistics, machine learning, mathematical models, pattern recognition, and other iscover patterns and relations on large datasets.				
A. Data Mining	C. Machine Learning				
B. Cloud Compu					
harm.	System, is a technology with built-in protective response to try and block or stop C. Detention D. Proactive				
	cks generally seek to obtain sensitive information like:				
	C. Name and Surname				
B. Data	D. Passwords				
8. A	is a function which records or keystrokes on a computer.				
	C. keylogger				
B. Keyrecorder	D. Loggerkey				
9. To describe b	oth fault and failure, Security Engineers use the term				
A. Flaw	C. Fault				
B. Flow	D. Floor				
10. A program t	hat appears to be useful but has undocumented hidden malicious features.				
A. Trojan Horse	C. Tricky Horse				
R Malware	D Spyware				

i. Explain what is meant by (a) Vulnerability (b) Threat (c) Harm.	(6)
ii. How is Denial of Service (DoS) different from Distributed Denial of Service (DDoS)?	(2)
iii. Mention and explain the 3 principles of the CIA Triad.	(6)
iv. The CIA Triad has two additional principles. (a) Mention and (b) explain how those two principles help in IT Systems Security.	(4)
Question 4 [12 Marks] i. How is Authentication different from Authorization in IT Systems security?	(4)
ii. Authentication is the first step in access control, and there are three common factors used fo authentication. Name and explain the three authentication mechanisms.	r (6)
iii. Discuss the concept of Single-Sign-On (SSO).	(2)
Question 5 [8 Marks] i. Vitjitua is a System Administrator for Matisa Travel Agency CC. She created a file that runs an application through the company's website. She needs to share it with group members but wan make sure that only she has full rights over the file, while her group members should only be abread and modify the file, other users should only be able to execute. Give the permissions that Vitjitua must assign to that file using a Debian operating system.	its to
#mkdir Files #touch Files/information.exe #chmod Files/information.exe	
ii. Vitjitua realises that a modification was made to the file, which led to a compromise of the or application on the website. No one will admit to the modification, and there was no external int into the system. Vitjitua decided to view the record of events recorded for that file.(a) What document/file must she view to get those records?(b) Which principle of the CIA triad will Vitjitua be addressing?	
Question 6 [11 Marks] i. What is asymmetric encryption?	(2)
ii. What is symmetric encryption?	(2)
iii. Give one example of an asymmetric encryption algorithm, and one example of symmetric encryption algorithm.	(2)
iv. Web Browsers are trusted with sensitive information, making them a target of malicious atta What are the three Web Browser attack vectors?	cks. (3)
v. Explain what is meant by Buffer overflow.	(2)

i. Name and explain the three cloud computing service models.	(6)
ii. You are the Security Administrator of a certain company. The company deals with forensics investigations and the company would like to seek for cloud services to store data, as this data i confidential.	s highly
(a) Which cloud computing deployment model would you recommend the company to use in or ensure that the risk of leaking confidential information is kept to minimum.	der to
(b) Explain how your recommendation will help with the objective set in (a).	(2)
Question 8 [9 Marks] i. Name any command line tool that is useful in troubleshooting DNS services.	(1)
ii. What is the role of a DNS server on a network?	(2)
iii. What is an "A Record" and what is a "PTR Record" in DNS?	(4)
iv. What could happen if the DNS server stopped working on the network?	(2)
Question 9 [Marks] i. Why is a Self-Signed certificate not trusted, and what would be the alternative to Self-Signed certificates?	(4)
ii. Privacy is controlled disclosure, in what the subject chooses what personal data to give out, w and to whom. There are 8 Privacy Principles and Policies. One of them is Data Quality. What does this Privacy Principle/Policy say?	hen,
Question 10 [8 Marks]	(0)
i. Explain what is meant by risk analysis in IT Systems security.	(2)
ii. List the 6 steps of Risk Analysis	(6)

----End of Question Paper----