NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF CYBER SECURITY

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE in CYBER SECURITY	
QUALIFICATION CODE: 07BCCY, 07BCCS	**LEVEL:** 7
COURSE: OPERATING SYSTEMS SECURITY	**COURSE CODE:** OS711S
DATE: JUNE 2023	**SESSION:** 1
DURATION: 3 Hours	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER (S)	MR. ISAAC NHAMU
MODERATOR	DR. NALINA SURESH

THIS EXAM QUESTION PAPER CONSISTS OF 6 PAGES

(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions on the answer scripts.
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. None.

Section A (Multiple Choice)   [15 marks]

1. A buffer-overflow attack can gain access to a system's memory. (True or false)

2. A smart card is an authentication example using the something you know factor. (True or false)

3. If users forget their password, they can reset the password with a _____, as long as they created it before forgetting their password.

4. Permissions assigned at the drive level are inherited by all root folders on the drive. (True or false)

5. Permissions are retained when you move a file within the same partition. Any other time you move or copy files, the original permissions are lost. (True or false)

6. MBSA can detect weak passwords for accounts on Microsoft systems. (True or false)

7. In Linux systems, regular (non-administrator) users can view the *etcpasswd* file. (True or false)

8. What is meant by reducing the attack surface of a system?
    A. Disabling the anti-virus
    B. Removing unneeded protocols
    C. Keeping a system up to date
    D. Disabling the firewall

9. Elizabeth is a member of the Finance group and the Budget group. The Finance group is granted Modify permission for an NTFS folder called Funding. The Budget group is granted Read permission for the same folder. What is Maria's permission to the Funding folder?
    A. Impossible to determine.
    B. Read
    C. Modify
    D. Full Control

10. Which Audit Policy selection records any time a user logs onto a local system?
    A. Logon Events
    B. Account Logon Events
    C. System Events
    D. Process Tracking

11. Which of the following choices can be used to automatically collect events on a single server from multiple servers?
    A. Process Tracking Events auditing
    B. MBSA
    C. Automatic archiving
    D. Event subscriptions

12. Which one of the following is not a valid use of a digital certificate?
    A. Authentication
    B. Encryption
    C. Digital signatures
    D. Virus detection

13. What is known as sandbox?
    A. It is a program which can be molded to do desired task.
    B. It is program that is controlled or emulated section of OS
    C. It is a special mode of antivirus
    D. None of the mentioned

14. Why is a one-time password safe?
    A. It is easy to generate.
    B. It cannot be shared.
    C. It is different for every access.
    D. It is a complex encrypted password.

15. What does the value 7 represent in the following line from the *etcshadow* file?

    `sync:*:16484:0:99999:7:::`

    A. The date of last password change field
    B. The minimum password age field
    C. The maximum password age field
    D. The password warning period field

Section B (Structured Questions)   [55 marks]

Question 1

a.   Explain the suitability or unsuitability of the following passwords:

    i.   Rachel123

    ii.   Windhoek

    iii.   tv9cartoon#

    iv.   oneloveafrica   [4]

b.   While trying to improve the security of an organisation through an operating system, explain what the problem could be of;

    i.   Increasing the complexity of a password

    ii.   Setting the password age to one month

    iii.   Enforcing a password history policy that sets the value larger than 24?[6]

Question 2

a.   State **three** threats that result from a process running with administrator or root privileges on a system.   [6]

b.   List **two** ways in which security misconfigurations can occur during operating systems installation.   [2]

a.   Give an example each, of weaknesses/vulnerabilities that may affect the operating system that are caused by;

    i.   Software   [1]

    ii.   Policy/Procedures.   [1]

Question 3

Figure 1 below shows the architecture of Type I and Type II virtual machine systems. From a security perspective outline **three** advantages of Type I virtual machine systems over Type II systems and **two** advantages of Type II virtual machine systems over Type I systems.
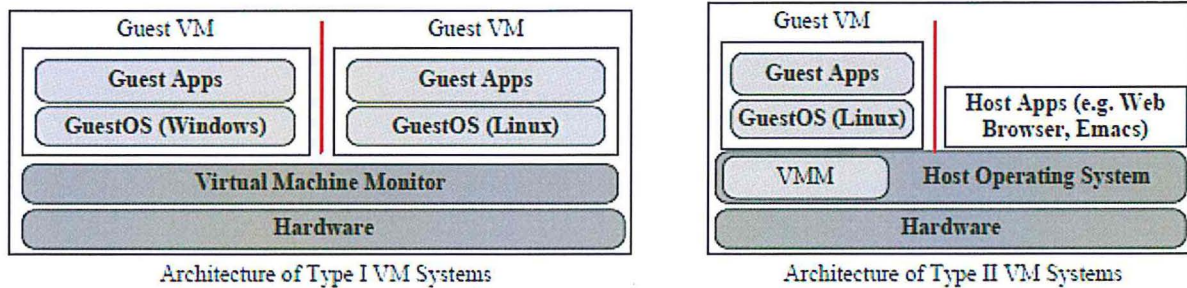
[10]

Figure 1: Architecture of Type I and Type II Virtual Machine Systems

Question 4

One way to implement security in an operating system is by way of assigning permissions on objects to subjections. Figure 2 illustrates a relationship between permissions.
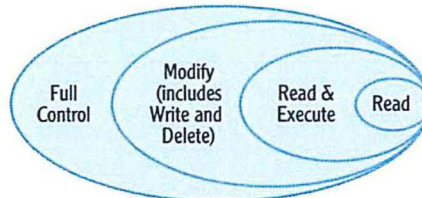

Figure 2: Relationship between permissions in an NTFS system

a. What can a user given **Full Control** do to an object that one given **Modify** cannot do?

[2]

b. Give an example of an **Execute** operation. [2]

c. What is the difference between **Write** and **Modify**? [2]

d. What is the advantage of using **Groups** to manage permissions and what is one disadvantage? [4]

Question 5

a. State **five** ways in which a systems administrator can harden an organisation's operating system. [5]

b. Name any three tools that can be used to perform audit log in an operating system. [3]

c. Using an example define Role Based Access control. [2]

Question 6

Figure 3 below shows the security architecture diagram for iOS.
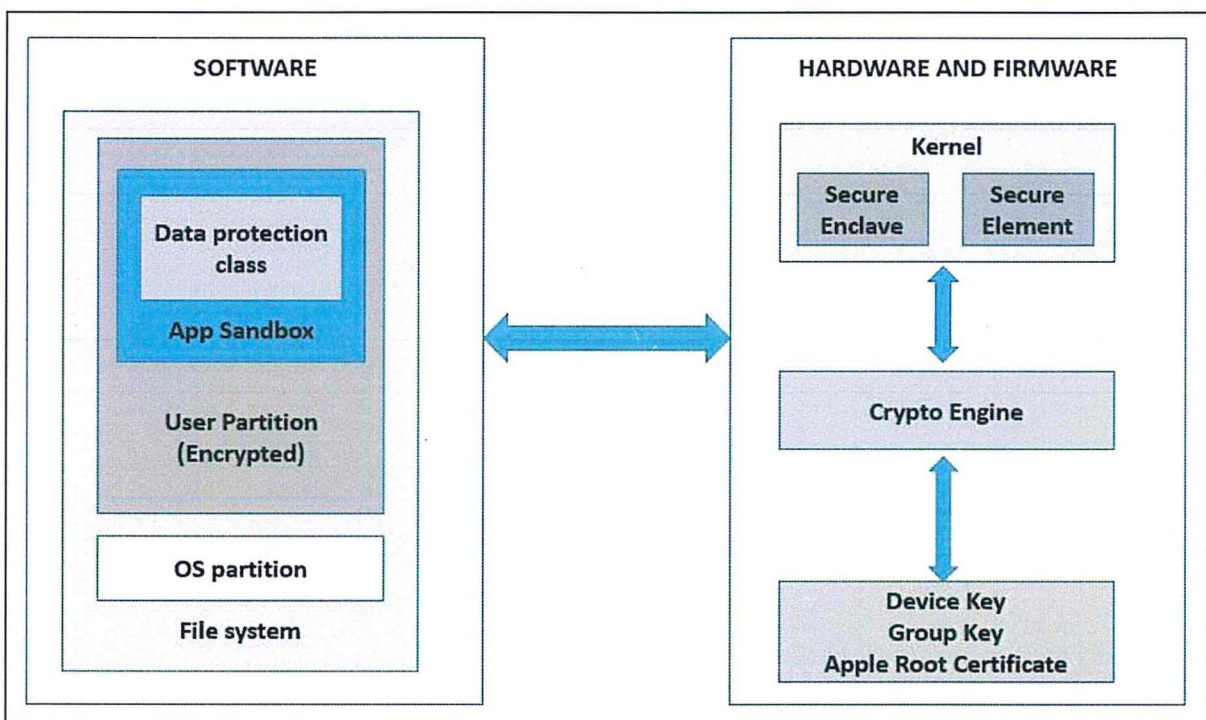

Figure 3: Security architecture diagram for iOS

a. What file system does iOS use? [1]

b. With reference to iOS, what is sandboxing? [2]

c. What is the advantage of sandboxing? [2]

Section A (Scenarios and Practice)   [30 marks]

Question 7

A university has realized that they do not have sufficient ICT resources to cater for their ever-increasing population of students. They have decided to allow staff and students at the university to bring they own devices (BYOD) to complement their limited resources so as to facilitate a more conducive teaching and learning environment.

Outline at least **ten** policy items that systems administrators should enforce at the operating systems level to protect the university's production system from the BYOD phenomenon, as well as to protect the staff/students' devices.   [20]

Question 8

According to Android Authority, an independent online publication that is a voice for the world of Android & technology,

> *"Whether iOS is better than Android in security is now up for debate, but the consensus still gives Apple the upper hand."* ... making it harder for attackers to target iOS users.

Based on the argument above and from an operating systems perspective. Outline at least five reasons why devices running iOS are considered better than those running Android.   [10]

<<<<<<<< END >>>>>>>>