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: OSS711S**
DATE: JUNE 2024	**SESSION: 1**
DURATION: 3 HOURS	**MARKS: 100**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER (S)	**MR. ISAAC NHAMU**
MODERATOR	**MS. KLAUDIA UUZOMBALA**

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. What is not good practice for user administration?
   - A. Isolating a system after compromise
   - B. Using telnet and FTP for remote access
   - C. Granting privileges on a per host basis
   - D. Performing random audit checks

2. Why is one time password safe?
   - A. It is easy to generate.
   - B. It is generated once.
   - C. It is different for every access.
   - D. It is a complex encrypted password.

3. 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

4. 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

5. The Light Directory Access Protocol (LDAP) does NOT store?
   - A. Users
   - B. Passwords
   - C. Security keys
   - D. Address

6. What is not a best practice for password policy?
   - A. Deciding maximum age of password.
   - B. Removing retired employees from the system.
   - C. Password encryption.
   - D. All of the above.

7. Which feature is commonly used to enhance the security of user accounts on Windows operating systems?
   - A. sudo
   - B. BitLocker
   - C. SELinux
   - D. User Account Control (UAC)

8. The operating system's role in the protection of the system from physical threats involves:
   - A. providing tools to enable system backups and restoration of the OS itself, files, programs and data.
   - B. triggering denial of service attacks to prevent malicious users from using the system.
   - C. providing tools to enable system firewall deployment.
   - D. providing port scanning mechanisms.

9. What is the primary purpose of the SELinux (Security-Enhanced Linux) feature in Linux operating systems?
    A. File encryption
    B. Enhancing access control through mandatory access controls (MAC)
    C. User authentication
    D. Network traffic monitoring

10. Which file system is commonly used in Linux for enhanced security features, including file permissions and access control lists?
    A. NTFS
    B. ext4
    C. FAT32
    D. HFS+

11. What is the purpose of the sudo command in Unix-based operating systems like Linux?
    A. Authorisation
    B. System restore
    C. User authentication
    D. Elevated privileges for specific commands

12. Which security measure is commonly used in Windows operating systems to encrypt entire volumes and protect against unauthorized access?
    A. BitLocker
    B. Full Disk Encryption (FDE)
    C. User Account Control (UAC)
    D. Windows NTFS Encryption File System (EFS)

13. Which security measure is designed to protect against buffer overflow attacks in operating systems?
    A. Firewall
    B. Antivirus software
    C. Data Execution Prevention (DEP)
    D. Virtual Private Network (VPN)

14. 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

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

Section B (Structured Questions) [60 marks]

Question 1

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

i. OSSEXAM123

ii. Windhoek@40_Ye@rs

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

Describe what each of the following Linux commands can be used for in the security of an operating system and in turn to secure the system. Give an example implementation of each command.

(e.g. the `kill` linux command is used to kill or stop a process that is hanging or taking too long to execute, example usage `kill 15` will terminate a process with process ID (PID) 15.

a. sudo [2]

b. usermod [2]

c. chmod [2]

d. lsof [2]

e. passwd [2]

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]

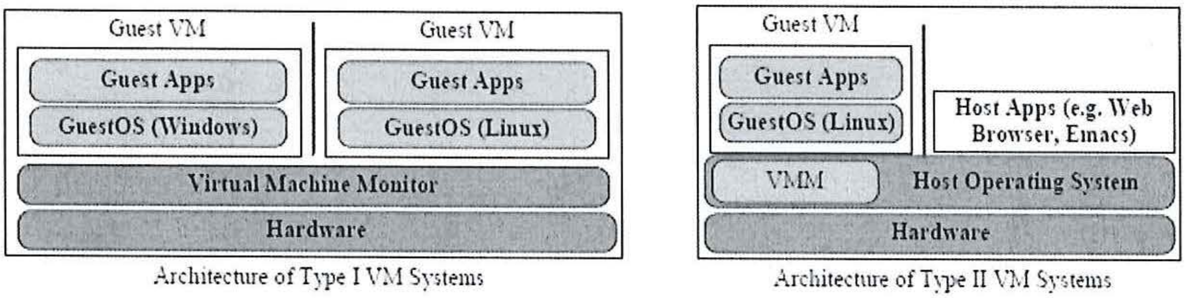

Figure 1: Architecture of Type I and Type II Virtual Machine Systems

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.

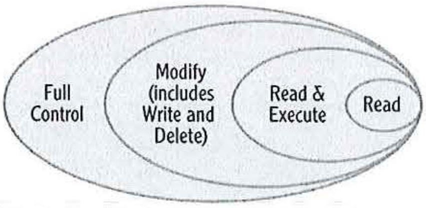

Figure 2: Relationship between permissions in an NTFS system

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

Figure 3 below shows the security architecture diagram for iOS.

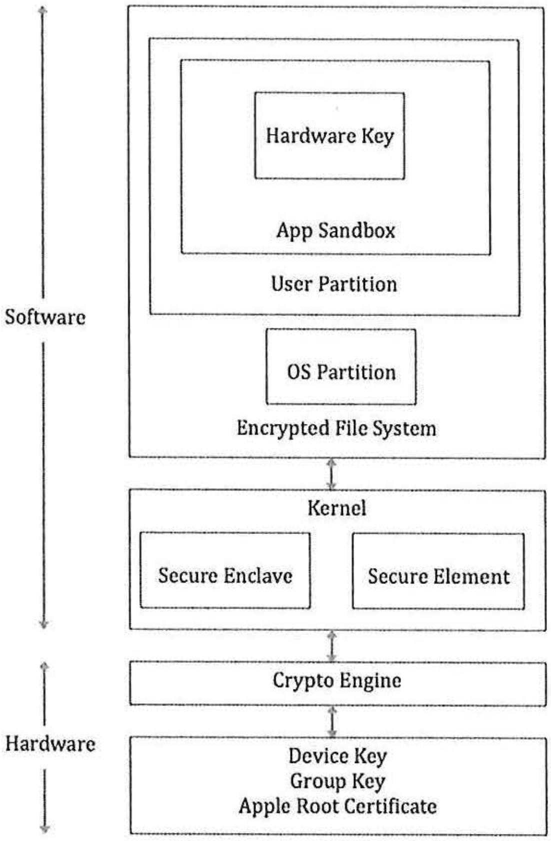

Figure 3: Security architecture diagram for iOS

a. What file system does iOS use? Give two key features that makes this file system more secure than others. [3]

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

c. What is the advantage of sandboxing? 2]

d. Describe iOS's Secure boot process (how does it protect the system?) [3]

e. What is iOS's Secure Enclave? [2]

f. Explain the Application revie and code signing concept used on IOS devices as a form of security. [2]

g. What is jailbreaking an iOS device? What is the risk of jailbreaking an iOS device? [4]

Section A (Scenarios and Practice) **[25 marks]**

Question 6

According to Kaspersky, many businesses are converting their hardware assets to virtual. The main business goal in most cases is almost certainly to gain maximum efficiency from IT infrastructure. Running several virtual machines (VMs) together on a single computer instead of using dedicated servers, all demanding their own power, cooling and maintenance, makes for a convincing argument. Multiple virtualized nodes powered by a single physical server creates business savings. The economic effect of virtualization can be amazingly powerful. However, whenever new technology emerges there are pros and cons of its utilisation.

In terms of operating systems security, Outline at least **five** security concerns and **five** security benefits of adapting virtualisation. [20]

Question 7

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. State at least five reasons why devices running iOS are considered better than those running Android.

[5]

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