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: JULY 2023	**SESSION:** 2
DURATION: 3 Hours	**MARKS:** 100

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

THIS EXAM QUESTION PAPER CONSISTS OF 5 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. You can enforce a password policy through Group Policy. (True or false)

2. Any permission explicitly assigned to an object is retained when you remove inherited permissions. (True or false)

3. If you want to audit all access to a folder, all you have to do is enable Object Access auditing in the Audit Policy. (True or false)

4. If you want to ensure that an audit-log entry records each time a system is shut down, you should enable Successful entries for _____________ auditing.

5. You can secure audit logs with WORM media. (True or false)

6. If files are encrypted on a server using EFS, they're automatically encrypted when a user uses offline folders. (True or false)

7. Fill in the missing option so the user of the bob account can't change his password:

   passwd _____ 99999 -M 99998 bob

8. What tool can you use to create a comprehensive security policy as an XML file on a Windows Server system?
   A. Microsoft Baseline Security Analyzer (MBSA)
   B. System Center Configuration Manager (SCCM)
   C. Security Configuration Wizard (SCW)
   D. Windows Server Update Services (WSUS)

9. What is the difference between identification and authentication?
   A. Nothing. They're the same.
   B. Identification proves an identity.
   C. Authentication proves an identity.
   D. Identification authenticates an individual, and authentication provides authorization.

10. Of the following choices, what isn't a valid use of a RADIUS server?
    A. Authenticate VPN clients.
    B. Authenticate wireless clients.
    C. Provide port-based authentication.
    D. Provide authentication for 802x database servers.

11. Which Audit Policy selection records modifications to Active Directory?
    A. Privilege Use
    B. Account Management Events
    C. Directory Service Access
    D. Policy Change

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

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

14. Which of the following is a security-based Linux distribution?
    A. Fedora
    B. CentOS
    C. Debian
    D. Kali

15. Which command can be used to find users who have no password?
    A. find
    B. grep
    C. passwd
    D. search

Section B (Structured Questions) [55 marks]

Question 1

One of the important tasks when securing an operating system is to manage passwords. Outline five different way passwords can be attacked. For each of the attacks you state, provide a mechanism that can be used to protect against such attacks. [10]

Question 2

Giving examples, explain how each of the following access control models work and give two advantages of each.

a. Discretionary Access Control. [4]

b. Mandatory Access Control. [3]

c. Role Based Access Control. [3]

Question 3

For each of the security goals below give two ways/techniques that an operating system can use to enforce each one of them. [10]

a. Confidentiality

b. Integrity

c. Availability

d. Non-repudiation

e. Privacy

Question 4

Figure 1 below illustrates a buffer overflow vulnerability.

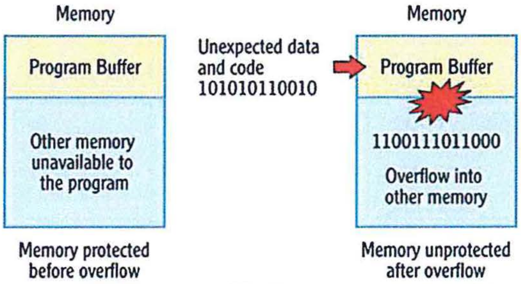

Memory
Program Buffer
Other memory unavailable to the program
Memory protected before overflow
Unexpected data and code 101010110010
Memory
Program Buffer
1100111011000
Overflow into other memory
Memory unprotected after overflow

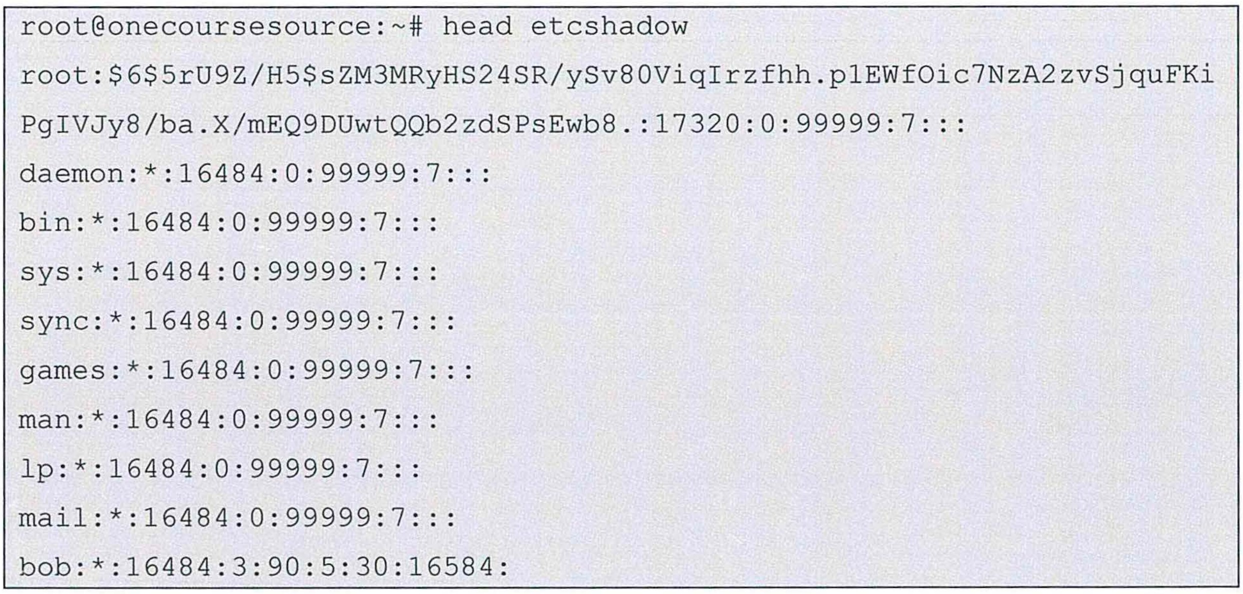
Figure 1: Illustration of buffer overflow vulnerability.

a. Using the illustration above, explain what a buffer overflow attack is. [4]

b. Give **three** ways by which buffer overflow attack can be mitigated. [6]

Question 5

a. In Linux compare what the ***etcshadow*** file and the ***etcpasswd*** file store. [2]
b. Is the ***etcshadow*** file viewable by non- administrative users? [1]
c. Below is a demonstration of part of a typical ***etcshadow*** file.



```
root@onecoursesource:~# head etcshadow
root:$6$5rU9Z/H5$sZM3MRyHS24SR/ySv80ViqIrzfhh.p1EWfOic7NzA2zvSjquFKi
PgIVJy8/ba.X/mEQ9DUwtQQb2zdSPsEwb8.:17320:0:99999:7:::
daemon:*:16484:0:99999:7:::
bin:*:16484:0:99999:7:::
sys:*:16484:0:99999:7:::
sync:*:16484:0:99999:7:::
games:*:16484:0:99999:7:::
man:*:16484:0:99999:7:::
lp:*:16484:0:99999:7:::
mail:*:16484:0:99999:7:::
bob:*:16484:3:90:5:30:16584:
```

using the **bob:*:16484:3:90:5:30::16584** line as an example describe the information each field holds. [7]

Question 6

Describe five way of securing audit logs in an operating system. [5]

Section A (Scenarios and Practice) **[30 marks]**

Question 7

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 8

Outline at least **five** security problems that may hamper the provisioning of services on the cloud. [10]

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