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: JULY 2024	SESSION: 2
DURATION: 3 HOURS	MARKS: 100

SUPPLEMENTARY/SECOND OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER (S)	MR. ISAAC NHAMU
MODERATOR	MS. KLAUDIA UUZOMBALA

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/True or False) [20 marks]

True/False and Fill in Questions

1. 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)

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

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

4. You can enforce a password policy through Group Policy. (True or false)

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

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

   passwd _____ 99999 -M 99998 bob

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

8. If users forget their password, they can reset the password with a __password reset disk___________, as long as they created it before forgetting their password.

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

10. 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)

Multiple Choice

11. What is the purpose of the Windows Registry in the context of operating system security?
    A. Network traffic monitoring
    B. File encryption
    C. System configuration and settings storage
    D. User authentication

12. What is the purpose of the umask command in Unix-based operating systems like Linux?
    A. User authentication
    B. File encryption
    C. Defining default permissions for newly created files and directories
    D. Network traffic monitoring

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

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

15. 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)

16. 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.

17. 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.

18. 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.

19. 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.

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

Section B (Structured Questions) **[50 marks]**

Question 1

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]

c. 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 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

Figure 1 below illustrates a buffer overflow vulnerability.

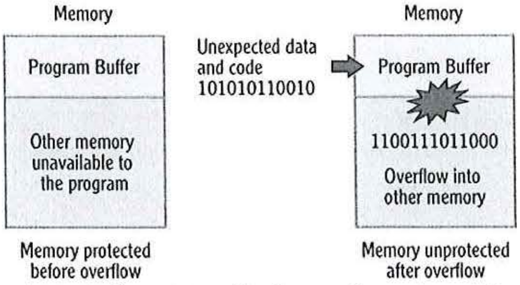

Memory
Program Buffer
Other memory unavailable to the program
Memory protected before overflow
Unexpected data and code 101010110010
Memory
Program Buffer
1100111011000
Overflow into other memory
Memory unprotected after overflow

Figure 1: Illustration of buffer overflow vulnerability.

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

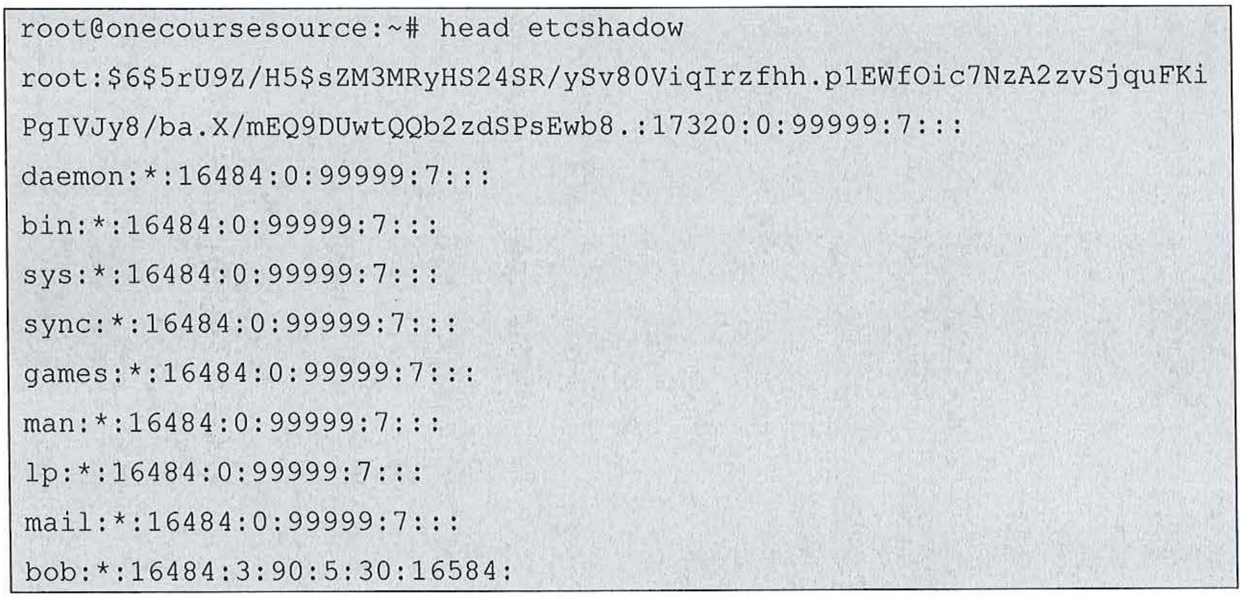
b. Give **three** ways by which buffer overflow attack can be mitigated. [6]

Question 4

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/ySv8OViqIrzfhh.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 5

Describe five way of securing audit logs in an operating system. [10]

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

Question 6

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 7

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

[10]

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