HW 3

● Graded

Student

Sivachandran P

Total Points

50 / 50 pts

Question 1

DAC and MAC

10 / 10 pts

✓ **+ 10 pts Correct**

+ 7.5 pts Mostly Correct

+ 5 pts Partially Correct

+ 2.5 pts Attempt

+ 0 pts Not Relevant/Plagiarism/Use of AI Tools

while the answer is correct. you need to stick to 2 main dis/advantages of DAC and MAC. It is not a correct way to pour out all the learnings you had in the course.

Question 2

SUID Programs

10 / 10 pts

✓ **+ 10 pts Correct**

+ 7.5 pts Mostly Correct

+ 5 pts Partially Correct

+ 2.5 pts Attempt

+ 0 pts Not Relevant/Plagiarism/Use of AI Tools

although the answer is correct, the question asked is for mentioning 2 dangers. please stick to what is asked.

Question 3

Program Isolation

10 / 10 pts

✓ **+ 10 pts Correct**

+ 7.5 pts Mostly Correct

+ 5 pts Partially Correct

+ 2.5 pts Attempt

+ 0 pts Not Relevant/Plagiarism/Use of AI Tools

Question 4

Chroot Jail

10 / 10 pts

✓ **+ 10 pts Correct**

+ 7.5 pts Mostly Correct

+ 5 pts Partially Correct

+ 2.5 pts Attempt

+ 0 pts Not Relevant/Plagiarism/Use of AI Tools

While the answer is correct, you can answer precisely

Question 5

TOCTOU

10 / 10 pts

✓ **+ 10 pts Correct**

+ 7.5 pts Mostly Correct

+ 5 pts Partially Correct

+ 2.5 pts Attempt

+ 0 pts Not Relevant/Plagiarism/Use of AI Tools

keep the answer short

Q1 DAC and MAC

10 Points

Please keep your answers for each part of the question within 2-3 sentences. Please use your own understanding to explain.

(a) Write two disadvantages of Discretionary Access Control (DAC)?

1) Poor data protection: It can't provide the necessary assurance to protect sensitive data

2) Security: Since users can grant and revoke permissions, which lead to data leaks. For the users who no longer have access bloated Access control lists (ACLs)

3) Lack of visibility: Its difficult to monitor those who have access rights and for which activity

Additional info: DAC access carol system used in cloud storage platforms (Google Drive, Microsoft OneDrive, Android and iOS smartphone apps). It allows users to mark the persons possible to access their files/folders, and the level of access they should have.
It is not recommended for protecting very confidential data and lack of centralized control.

(b) Explain two advantages of Mandatory Access Control (MAC)?

1) High level data protection (more secure system): Without any room for data leakage protecting most confidential data more proper

2) Centralized information: Makes entire system centralized one and under the control of single authority. It cannot be de-centralized by any user other than head of administrator after category is set.

3) Privacy: Only admin could perform changes in category (or list of users could access to any category)

Additional info: System allows or deny access to private information in any organization. Admins need to spend huge efforts at the time of planning information flow properly. It works on a hierarchy pattern and makes different from other systems.

Q2 SUID Programs

10 Points

Please keep your answers within 2-3 sentences. Please use your own understanding to explain.

(a) If the Suid permission bit of a binary in Unix is set to 1, and the binary is owned by the root, then what happens when the program executes?

While SUID (Saved/Set User ID) bit is set to 1 on a binary owned by "root", during execution of program it runs with "root"privileges (which allows to perform tasks that required root-level access, such as modifying system files or accessing protected resources), without bother the user whoever starts the program. In other words it enables program to run with the privileges the owner rather than privileges of the user executing it.

1) Effective User ID (euid) becomes root - "EUID" temporarily switched to Owner's ID while regular user (not super user) runs the binary.
2) Real User ID (raid) stays the same - remains their original ID
3) Program runs with elevated privileges - program runs with root privileges

(b) State 2 dangers of Suid programs?

1) Privilege escalation: Vulnerabilities exploited by regular user or attacker with root-level privileges (more vulnerable to exploitation)

2) Misconfigured permissions: Unintentional user access leads to sensitive actions leading to unauthorized operations

3) Backdoor creation: Allowing attackers bypass security mechanisms and gain root access repeatedly

4) Bypassing access controls: Since SUID programs allow users to execute certain operations as rot, helps control mechanisms access bypass, exposing critical system files or executing unauthorized commands

5) Temporary but dangerous root access: Eventhough root access via SUID program is temporary, program execution can last potentially damaging effects on the system

Q3 Program Isolation

10 Points

Please keep your answers within 2-3 sentences. Please use your own understanding to explain.

(a) Why do we need to have provisions for program isolation?

Provisions for program isolation is mandatory to achieve protecting system security, to maintain system stability and helps to ensure efficient resource allocation. Otherwise leads to more vulnerable security threats, performance issues and software conflicts.

Several reasons for program isolation are:
Security (unauthorized access prevention & Security vulnerabilities containment), Stability and Fault tolerance (System crash prevention & Fault containment), Resource Management (efficient resource aollocation & control resource usage), Prevent interference (program independence & avoid conflicts), Privilege separation (least privilege principle & protection of sensitive process), Multi-tenancy, Sandboxing & Compliance and regulatory requirements

(b) Are programs running on distinct virtual machines always properly isolated?

There is a benefit of significant degree of isolation while running on distinct VM (Virtual Machines). But sometimes isolation got compromised, including hypervisor vulernabilities, misconfigurations, side-channel attacks and shared resources. therefore in virtualized environments, to enhance entire security, organizations should implement additional security measures (eg. N/W segmentation, security best practices, regular audits etc.)

Q4 Chroot Jail

10 Points

Please keep your answers within 2-3 sentences. Please use your own understanding to explain.

(a) What was the rationale behind the idea of chroot jail?

Chroot jail mechanism is a way to isolate applications and enhance system security by changing the apparent root directory for running process and its children.

This operation changes the apparent root directory for the current furling process and its children. In this environment cannot access the files outside the designed directory tree.
Use chroot system call to change the root directory to be at the base of this new tree and start process running in that chromed environment. It can't perform malicious read/write outside paths since it can't reference.

This kernel level virtualization is used instead of virtual machines (application layer virtualization) to create multiple isolated instances of the host OS.

(b) Why is it that chroot jail is not the best way to implement program confinement?

It is not considered the best way to implement since it has limitations and potential security risks, less effective compared to other confinement mechanisms.

1) Limited isolation - not true isolation - does not provide isolation from the rest of the system

2) Escape vulnerabilities - easily bypassed by gain access to the original root filesystem or sensitive ares of the system

3) Inadequate resources control - no resource limits (CPU, memory, I/O), process inside chroot jail can consume excessive resources

4) Insufficient security context - No mandatory access control (MAC) - difficult to implement fine-grained access controls

5) File system visibility - Unrestricted access to device files - security risks such as direct hardware access

6) Inconsistent behavior across systems - reliance on environment - certain libraries or binaries may not be available within the chroot, leading to unpredictable behavior

7) Administrative complexity - Management overhead, complexity in maintaining the jail

8) Not suitable for Multi-tenant environments - Limited use in cloud or multi-user scenarios - not sufficient to ensure security isolation.

Q5 TOCTOU

10 Points

Please keep your answers within 2-3 sentences. Please use your own understanding to explain.

(a) Explain what is a TOCTOU bug?

Time of Check to Time of Use (TOCTOU) is bug caused by changes in system between the checking condition (such as security credential) and use of result of this check at a later time.
It represents significant class of concurrency vulnerabilities that can compromise the security and reliability of software systems.

Check phase - Verifies condition
Use phase - Performs based on the result of check
Race condition - Issues arises between check and use system change operations

TOCTOU bugs leads to security vulnerabilities, Data integrity issues, Unpredictable behavior
Prevention strategies - Atomic operations, Locking mechanisms, Reduced check time, Avoiding checks

(b) Explain in the context of "system call interposition" how TOCTOU bug may compromise the goal of program confinement?

System Call Interposition - Security mechanism control and monitor the interactions between OS kernel and user-level apps.
Sandboxing - Limiting resources could access and action it can perform
Access Control - Policies to prevent unauthorized access to files, processes or n/w resources
Monitoring - Track of system calls or intrusion detection

TOCTOU compromise the goal of program confinement in few significant ways:
1) Timing vulnerabilities - Check status of resources and use after some delay, attacker can exploit this window
2) Inconsistent state - Another process alters the file permissions
3) Bypassing security policies - TOCTOU vulnerability can allow an application to evade these policies

Consequences for program confinement:
Security breach - access to files or resources that violate the confinement

model

Data corruption or leakage - Affecting the integrity and confidentiality of the data

Unlimited behavior - Actions that were not anticipated by the confinement policies.