REG.NO.:

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2024-2025

SLOT: B2 + TB2

Programme Name & Branch : **B. Tech Computer Science and Engineering**
Course Code and Course Name : **BCSE317L Information Security**
Faculty Name(s) : **Common to ALL batches**
Class Number(s) : **Common to ALL batches**
Date of Examination : **17 March 2025**
Exam Duration : **90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes
  CO4: Differentiate the needs and application of security in Operating System and Firewalls.
  CO5: Analyse various method of securing databases

Q. No	Question	M	CO	BL
1.	a) List a few functions managed by an operating system. Map these functions to various layers of the operating system that follows the layered design. Justify how such a layering enhances security of the OS (Identify at least two functions for each layer) [5 Marks] b) How do modern operating systems ensure the integrity and authenticity of software components loaded during the boot process? [5 Marks] Answer a) Key Operating System Functions: • Security Functions: Basic access control, privilege management. • Synchronization, Allocation: Resource management, process coordination. • Scheduling, Sharing, Memory Management: Core OS functionalities. • File Systems, Device Allocation: File and device management. • Utility Functions: Higher-level OS utilities. • Compilers, Database Managers: System software. • User Processes: User-level applications. • Subprocesses of User Processes: Threads or child processes. **Mapping Functions to Layers:** Hardware: Physical components of the computer system. Security Functions: Basic access control, privilege management, hardware-level security features. Synchronization, Allocation:	10	CO4	4

Resource allocation (CPU, memory, devices), process synchronization mechanisms (semaphores, mutexes).

Scheduling, Sharing, Memory Management:

Process scheduling algorithms, memory allocation and management (paging, segmentation), resource sharing.

File Systems, Device Allocation:

File system operations (read, write, create, delete), device driver management, I/O handling.

Utility Functions:

System utilities (e.g., command-line interpreters, system monitoring tools).

Compilers, Database Managers:

System software that provides development tools and data management capabilities.

User Processes:

User-level applications (e.g., web browsers, word processors).

Subprocesses of User Processes:

Threads or child processes created by user applications.

Security Enhancements

- Hardware layer isolation.
- Security functions layer privilege separation.
- Lower layer-controlled access.
- Layered abstraction reducing complexity.

b)

Modern operating systems employ several key mechanisms to ensure the integrity and authenticity of software components loaded during the boot process. Here's a breakdown of the primary techniques:

Secure Boot (UEFI Secure Boot):

This UEFI (Unified Extensible Firmware Interface) feature ensures that only digitally signed bootloaders and operating system components are loaded.
The firmware contains a database of trusted certificates (public keys).
Each boot component is signed by a trusted authority. The firmware verifies the signature against its database.
If the signature is invalid, the boot process is halted, preventing the loading of potentially malicious software.

Measured Boot:

Measured boot extends secure boot by creating a chain of trust.
It measures (hashes) each boot component as it's loaded and stores these measurements in a Trusted Platform Module (TPM).
The TPM is a hardware component that provides secure storage for cryptographic keys and measurements.
This creates a tamper-proof record of the boot process, allowing later verification of the system's state.

	Trusted Platform Module (TPM): The TPM is a dedicated hardware chip that provides cryptographic functions and secure storage. It's used to store cryptographic keys, certificates, and measurements of the boot process. The TPM can also be used to generate and store encryption keys, which can be used to protect sensitive data. **Code Signing:** Operating system components, device drivers, and other software are digitally signed by their developers or vendors. This ensures that the software hasn't been tampered with and that it comes from a trusted source. The operating system verifies the digital signatures before loading the software.			
2.	You're in charge of network security for a small online business. You have a security appliance that can control access to your company's network, but it hasn't been properly configured yet. This means: • Employees can browse websites; however, your company's security policy doesn't permit employees using internet. • Employees can connect to their work computers from anywhere, but these connections aren't necessarily secure. • Anyone could potentially access your company's MySQL database over the network • There are no restrictions on file transfers, so anyone could upload or download files from your systems • There's no way to track who is accessing your network or what they are doing. You start receiving reports of suspicious activity on the network. Given this lack of security measures, what kinds of suspicious activity might you be seeing? How would you go about configuring the security appliance to address these risks and protect your company's valuable data and resources? Configuring a Firewall (like UFW shown below) for addressing the Risks Suspicious Activity You Might Be Seeing: Unauthorized Access to the MySQL Database: Attempts to connect to the MySQL database from unknown IP addresses. Brute-force login attempts against the MySQL server. Unusual database queries or data modifications. Uncontrolled File Transfers: Large, unexpected file uploads or downloads. Access to sensitive files by unauthorized users. Malware being uploaded to the system.	10	CO4	4

Insecure Remote Connections:
Brute-force attacks against SSH or other remote access services.
Unauthorized remote access to employee workstations.
Data exfiltration through unencrypted remote connections.

Unnecessary Internet Browsing:
Employees visiting websites that are not work-related.
Potential exposure to malware or phishing attacks.
High network usage.

Port Scanning and Probing:
Automated tools scanning your network for open ports and vulnerabilities.
Attempts to exploit known vulnerabilities in your systems.

Increased network traffic:
Unusual spikes in network traffic.

Configuring UFW to Address These Risks:

Deny All Incoming and Outgoing Traffic (Default Policy):
Start by establishing a secure baseline by denying all incoming and outgoing connections by default.
sudo ufw default deny incoming
sudo ufw default deny outgoing

Allow Essential Services (Whitelist Approach):
Only allow the specific services that are required for business operations.
SSH (Secure Shell):
If remote access is needed, restrict it to specific IP addresses and use strong authentication (e.g., SSH keys).
sudo ufw allow from <trusted_IP_address> to any port 22 proto tcp

Web Server (HTTP/HTTPS):
If you have a public-facing web server, allow incoming connections on ports 80 (HTTP) and 443 (HTTPS).
sudo ufw allow 80,443/tcp

MySQL (Restrict to Local or Trusted IPs):
Only allow connections to the MySQL database from trusted IP addresses or the local machine.
sudo ufw allow from <trusted_IP_address> to any port 3306 proto tcp

If the database is only accessed locally : sudo ufw allow from 127.0.0.1 to any port 3306 proto tcp

Allow necessary outgoing connections:
Allow outgoing DNS request.
sudo ufw allow out 53/udp

	If the company needs to connect to specific external servers, allow the specific ports and ip addresses. Disable Unnecessary Services: Disable any services that are not required, such as FTP (File Transfer Protocol), Telnet, or other remote access protocols. Logging: Enable UFW logging to monitor network activity and detect suspicious behavior. sudo ufw logging high Review the logs regularly to identify potential security threats. sudo less /var/log/ufw.log Enable UFW: Once you have configured the rules, enable UFW. sudo ufw enable Rate Limiting (Optional): Use rate limiting to prevent brute-force attacks against SSH or other services. sudo ufw limit ssh			
3.	You're an IT specialist responsible for a company's computer network. You're reviewing network logs and notice that a computer with the IP address 10.02.0.5 is sending out a continuous stream of ICMP Echo requests to a server in your network. This seems unusual to you. Currently, you don't have any specific security measures in place to deal with this kind of activity. a) Does this activity raise any security concerns? What could be the potential consequences if this activity is left unchecked? [4 Marks] b) What kind of security measures could you implement to address this situation and better protect your network from such pings in the future [6 Marks] Answer a) Security Concerns and Potential Consequences: Yes, a continuous stream of ICMP Echo requests (pings) from a single host (10.0.2.0.5) to a server raises significant security concerns. **Potential Security Concerns:** Network Scanning/Reconnaissance: The host might be performing a ping sweep to discover active hosts on the network. Denial-of-Service (DoS) Attack: The continuous pings could be a part of a DoS attack, attempting to overwhelm the server with traffic. Resource Exhaustion: The server might be consuming excessive resources responding to the pings, potentially impacting its performance. Malicious Activity Indication: This can be an indication of a compromised machine, or a machine that is being used for malicious purposes.	10	CO4	3

Potential Consequences if Left Unchecked:

Network Discovery: An attacker could map your network topology and identify vulnerable systems.
Server Downtime: A DoS attack could render the server unavailable.
Network Congestion: Excessive ICMP traffic can contribute to network congestion.
Further Attacks: Reconnaissance activities often precede more serious attacks.

b) Security Measures with Snort: (students can use any IDPS)

Snort Rule for ICMP Flood Detection:
Create a Snort rule to detect and alert on excessive ICMP Echo requests from the suspicious IP address.
This rule would belong in the "Security Functions" layer of the provided image, as it is a core security function.

Example Snort rule:
alert icmp 10.0.2.0/24 any -> <server_IP_address> any (msg:"ICMP Flood Detected from 10.0.2.0.5"; threshold: type both, track by_src, count 10, seconds 5; sid:1000002; rev:1;)

This rule triggers an alert if 10 or more ICMP packets are sent from any IP address within the 10.0.2.0/24 subnet to the specified server IP address within 5 seconds. This rule can be tuned, and the IP address can be changed to just the 10.0.2.0.5 address.

Snort rules for Rejecting the icmp packets

reject icmp 10.0.2.0.5 any -> any any (msg:"Reject ICMP from 10.0.2.0.5"; sid:1000004; rev:1;)

reject: This action discards the packet and sends an ICMP "destination unreachable" message back to the sender. This informs the sender that the packet was blocked.

In this case, using reject provides feedback to the sender (10.0.2.0.5) that their ICMP traffic is being blocked. This can be useful for troubleshooting or for notifying the sender that their activity is not permitted.

Snort rules for Logging the packets

log icmp 10.0.2.0.5 any -> any any (msg:"Log ICMP from 10.0.2.0.5"; sid:1000005; rev:1;)

Explanation:
log: This action tells Snort to log the packet's information. It doesn't drop or reject the packet; it simply records it.

	icmp: This specifies that the rule applies to ICMP traffic. 10.0.2.0.5: This is the source IP address that will be logged. any any -> any any: This indicates that the rule applies to any source port, any destination IP address, and any destination port. (msg:"Log ICMP from 10.0.2.0.5"; sid:1000005; rev:1;): msg: This provides a descriptive message for the log entry. sid: This is the Snort rule ID (unique identifier). rev: This is the rule revision number.			
4.	As a database administrator you are asked to maintain the following data for a company Employee_id, Employee_name, Employee_address, Project_Id, Project_name, Department_id and Department Name Consider the following rules • An employee can work on many projects • Every employee can work for only one department. List all the strategies and associated implementation details (SQL Queries as required) for managing the data such that your implementation satisfies the following database security parameters. • Physical Integrity • Logical Integrity • Element Integrity • User Authentication • Reliability Ans • Physical Integrity – Provide strategies on Database Backup and Back up Policy, protection against power outages, hardware failures. • Logical Integrity – Provide the 3NF schema for the database and establish primary, foreign keys . Provide SQL queries • Element Integrity – Provide SQL queries for Not null, check, default and unique constraints on the elements. • User Authentication – Provide SQL queries for User account creation and granting privileges to users. • Reliability – Provide insights on the database support for replication, 2 phase updates and locking protocols.	10	CO5	3
5.	A form receives user input in a textbox and supplies the value directly to a SQL query on the server-side script as shown below. (userinput in the SQL query is the value received from the textbox) $sql = "SELECT username, salary FROM employee WHERE username = '". $userinput . "'"; • Elaborate on how a hacker can exploit this weakness to get more control over your database. (6 Marks)	10	CO5	4

- List a few strategies to prevent such an attack. (4 Marks)

Answer

a) Provide the following Malicious SQL queries that can be executed. Explain their purpose with sample output from these queries. (More queries as taught in the class can be given by students)

```
1' and 1=1#
1' and 1=1 union select database(),user()#
1' and 1=1 union select null,table_name from information_Schema.tables#
1' and 1=1 union select user,password from users#
```

b)

Here are the key strategies to prevent SQL injection attacks:

Parameterized Queries (Prepared Statements):

- This is the most effective defense.
- Parameterized queries treat user input as data, not as executable code.
- The SQL query is defined with placeholders, and the user input is passed as separate parameters.
- This ensures that the database interprets the input as literal values, preventing malicious code from being executed. (sample code can be given)

```
$sql = "SELECT username, salary FROM employee WHERE username = ? ";
$stmt = $conn->prepare($sql);
$stmt->bind_param("s",$enteredUsername);
$stmt->execute();
```

Input Validation and Sanitization:

- Validate user input to ensure it conforms to expected formats and lengths.
- Sanitize input by removing or escaping special characters that could be used for SQL injection.

	• This is not as effective as prepared statements, and should be used in conjunction with them. **Stored Procedures:** • Use stored procedures to encapsulate SQL logic on the database server. • Stored procedures can help prevent SQL injection by limiting the ability of user input to directly modify the SQL code. **Principle of Least Privilege:** • Grant the database user used by the web application only the necessary permissions. • Avoid using database accounts with administrative privileges. • This limits the damage a hacker can do if they manage to inject SQL code.			

****