Risk Management Report

Name: Ernest Nyabayo Osindo
Date: 28/01/2026

Section 1: Objective of the Lab

In this lab, the objective is to ensure compliance with internal audit policies for system security within **FinSecure**. Specifically, we are tasked with developing a Python script to perform three key compliance checks:

1. **File System Permissions on Sensitive Directories**
   Ensuring that sensitive directories (e.g., `/secure_data`) have the correct permissions, restricting access to only the owner.

2. **Active User Session Monitoring**
   Monitoring the number of active user sessions to ensure no unauthorized or suspicious sessions are active.

3. **Disk Space Utilization to Prevent Data Loss or Service Disruption**
   Checking disk space utilization to prevent system failures or data loss caused by full disks.

These requirements are essential for maintaining the integrity of **FinSecure's** systems. By automating these checks, we reduce the chances of unauthorized access and ensure the system's stability by preventing data loss or service disruption due to disk space issues.

Section 2: Explanation of Script Functions

Task/Function Name: `check_file_permissions`

- **What it does:** Checks the permissions of sensitive directories to ensure that only the owner has access (i.e., no access to the group or others).

- **How it works:** The function uses Python's `os` and `stat` modules to retrieve the permissions of the `/secure_data` directory and compares the access control bits to ensure that only the owner has permission to access the directory.

- **Why it is important:** This function is critical in ensuring that sensitive data stored in specific directories is not accessible by unauthorized users or groups, thereby preventing data breaches or unauthorized access.

Task/Function Name: `check_active_sessions`

- **What it does:** Monitors the number of active user sessions and flags if the number of sessions exceeds the compliance threshold (in this case, 5 sessions).

- **How it works:** The function uses the `subprocess` module to run the `who` command and captures the list of active sessions. It counts the number of active sessions and compares it to the threshold, reporting compliance or non-compliance accordingly.

- **Why it is important:** Monitoring active sessions ensures that no unauthorized users are logged into the system. Excessive or suspicious active sessions could indicate a potential security breach, so it's essential to track them.

Task/Function Name: `check_disk_space`

- **What it does:** Checks the disk space utilization for the root directory (`/`). If the disk usage exceeds 80%, it flags the system as non-compliant.

- **How it works:** The function uses Python's `shutil` module to get disk usage statistics and calculates the percentage of disk space used. If the usage exceeds the 80% threshold, the system is flagged as non-compliant.

- **Why it is important:** Monitoring disk space is critical to prevent data loss or service disruption. Full disks can cause system crashes or slow performance, so keeping disk usage within acceptable limits ensures that the system remains operational and secure.

Section 3: Application of Risk Identification Concepts

Context:

This lab scenario focuses on the assessment of system security compliance for **FinSecure** by automating the monitoring of key areas: file permissions, active user sessions, and disk space utilization. These aspects are directly related to **risk identification** as they highlight areas where potential vulnerabilities might exist.

Process:

The following processes were applied to address the compliance requirements:

1. **File permissions:** Ensured sensitive directories had appropriate access controls.
2. **Active sessions monitoring:** Checked the number of active sessions to ensure only authorized users are logged in.
3. **Disk space utilization:** Monitored disk usage to avoid service disruption or data loss due to full disks.

Outcome:

These steps helped mitigate risks by identifying and reporting non-compliance in these key areas. Ensuring proper file permissions, monitoring user sessions, and controlling disk space are effective ways to safeguard against unauthorized access and operational failures.

Section 4: Testing and Results

Testing the Script:

The script was tested by running it on a Linux system with various configurations. The expected output for each function is as follows:

1. **Test for File Permissions:**
    - **Expected output:**
        - If the directory `/secure_data` has correct permissions (only owner access), the output will be: `Permissions for '/secure_data' are compliant.`

        - If the permissions are incorrect, it will output: `Permissions for '/secure_data' are NOT compliant.`
        - If the directory is missing, the function will output: `Directory '/secure_data' does not exist.`

2. **Test for Active Sessions:**
    - **Expected output:**
        - If there are fewer than 5 active sessions, the function will output: `Active sessions compliance is met.`
        - If there are more than 5 active sessions, it will output: `Too many active sessions: Compliance NOT met.`
3. **Test for Disk Space:**
    - **Expected output:**
        - If disk space is less than 80% used, the output will be: `Disk space utilization is compliant.`
        - If disk space usage exceeds 80%, the output will be: `Disk space utilization is NOT compliant.`

Sample Output:

```
Starting System Audit Compliance Checker...


Checking file permissions compliance...

Permissions for '/secure_data' are compliant.


Checking active sessions compliance...

Active sessions: 3
```

```
Active sessions compliance is met.


Checking disk space compliance...
Disk usage: 75.12%
Disk space utilization is compliant.


Compliance check completed.
```

Section 5: Conclusion

In this lab, I developed a Python script to perform compliance checks for **FinSecure**. The script successfully monitors **file permissions**, **active user sessions**, and **disk space utilization**.

Challenges Encountered:

- **File Permission Checks:** Ensuring correct interpretation of file permissions required attention to detail. Using the `stat` module helped address this challenge effectively.
- **Active Sessions Monitoring:** Identifying the correct threshold for active sessions required testing on various configurations to ensure accuracy.
- **Disk Space Monitoring:** Calculating disk usage and setting an appropriate threshold was straightforward but required careful attention to system partition layouts.

This lab demonstrated the importance of **risk identification** and **proactive monitoring** in maintaining a secure system environment. By automating these compliance checks, **FinSecure** can continuously monitor its systems for potential risks and ensure compliance with internal audit policies.