Risk Assessment part 2 Report

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

Section 1: Objective of the Lab

The objective of this lab is to develop a Python script to assess the compliance of **FinSecure's** system security, focusing on three key areas:

1. **File System Permissions** on sensitive directories
2. **Active User Session Monitoring**
3. **Disk Space Utilization** to prevent data loss or service disruption

These compliance requirements are critical for ensuring that sensitive data is properly protected, no unauthorized sessions are active, and system stability is maintained through effective disk space management. By automating these checks, FinSecure can proactively mitigate security risks and comply with internal audit policies, reducing the likelihood of data breaches, unauthorized access, or system outages.

Section 2: Explanation of Script Functions

Task/Function Name: `check_file_permissions`

- **What it does:** This function checks whether sensitive directories, such as `/secure_data`, have the appropriate file system permissions. It ensures that only the owner has access to these directories.
- **How it works:** The function uses Python's `os` and `stat` modules to retrieve the permissions of the specified directory and verifies that the group and others have no permissions (i.e., only the owner can access the directory).
- **Why it is important:** This check is essential to prevent unauthorized access to sensitive data. Ensuring that only the owner has access to critical directories mitigates the risk of data breaches and unauthorized file modifications.

Task/Function Name: `check_active_sessions`

- **What it does:** This function monitors the number of active user sessions on the system and checks for unauthorized or suspicious sessions.
- **How it works:** The function uses the `who` command, executed via Python's `subprocess` module, to list all active user sessions. It then counts the number of active sessions and flags the system as non-compliant if the number of sessions exceeds a certain threshold (e.g., more than 5 sessions).
- **Why it is important:** Monitoring active sessions ensures that only authorized users are logged into the system. If the number of sessions exceeds the threshold, it could indicate unauthorized access, signaling the need for further investigation.

Task/Function Name: `check_disk_space`

- **What it does:** This function checks the disk space utilization of the system, specifically the root directory (`/`), and flags the system if usage exceeds a predefined threshold (e.g., 80%).
- **How it works:** The function uses the `shutil` module to get disk usage statistics. It calculates the percentage of used disk space and flags the system as non-compliant if the usage exceeds the set threshold (80%).
- **Why it is important:** Proper disk space management is essential for preventing data loss and service disruptions. If disk space exceeds critical levels, the system may slow down, crash, or even lose data. This function ensures that disk space usage is within a manageable limit, helping avoid operational issues.

Section 3: Application of Risk Identification Concepts

Context:

The lab scenario involves identifying and mitigating risks associated with file permissions, user session monitoring, and disk space utilization. These risks directly impact the security, availability, and integrity of the system and sensitive data.

Process:

To address these risks:

1. The **file permissions** function ensures sensitive data is not exposed to unauthorized users, minimizing the risk of data breaches.

2. The **active session monitoring** function identifies unauthorized access attempts, enabling swift corrective actions if needed.

3. The **disk space utilization** function prevents system crashes or data loss by monitoring disk space, ensuring that critical thresholds are not breached.

Outcome:

By automating these compliance checks, the script helps **FinSecure** identify and mitigate potential security risks, ensuring compliance with internal audit policies and improving overall system stability. The checks also enhance the organization's proactive security posture, reducing the likelihood of significant disruptions due to security breaches or operational failures.

Section 4: Testing and Results

Testing the Script:

The script can be tested by running it on a Linux system configured with varying conditions for file permissions, active sessions, and disk space. Each function should produce the following results:

1. **File Permissions:**

Expected output: If the directory `/secure_data` is correctly configured with owner-only permissions, the script should output:

```
Permissions for '/secure_data' are compliant.
```

If permissions are incorrect, it should output:

```
Permissions for '/secure_data' are NOT compliant.
```

If the directory is missing, the script should output:

```
Directory '/secure_data' does not exist.
```

-
2. **Active Sessions:**

Expected output: If the number of active sessions is under the threshold (e.g., 5), the output should be:

```
Active sessions compliance is met.
```

If the number of sessions exceeds the threshold, it should output:

```
Too many active sessions: Compliance NOT met.
```

-
3. **Disk Space Utilization:**

Expected output: If disk space usage is below 80%, the script should output:

```
Disk space utilization is compliant.
```

If disk space exceeds 80%, it should output:

```
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 critical system security compliance checks for **FinSecure**. By implementing and testing functions for file permissions, active sessions, and disk space utilization, I gained valuable experience in identifying and mitigating potential security risks.

Challenges Encountered:

- **File Permissions:** Ensuring that the permissions logic correctly identifies the owner-only access required attention to detail but was successfully implemented with Python's `stat` module.

- **Active Sessions:** Setting the appropriate threshold for active sessions and ensuring accurate session counting required testing with different configurations.

- **Disk Space Monitoring:** Calculating disk space usage and ensuring compliance with thresholds was straightforward but required careful attention to system partition layouts.

This lab emphasized the importance of **proactive security checks** and **risk identification** in maintaining system security. The script ensures that **FinSecure** remains compliant with internal audit policies and helps mitigate potential risks related to file security, unauthorized access, and system stability.