Module 6 – Lab 6: Monitoring Evidence and Compliance Reasoning

Estimated Time: 30–45 minutes

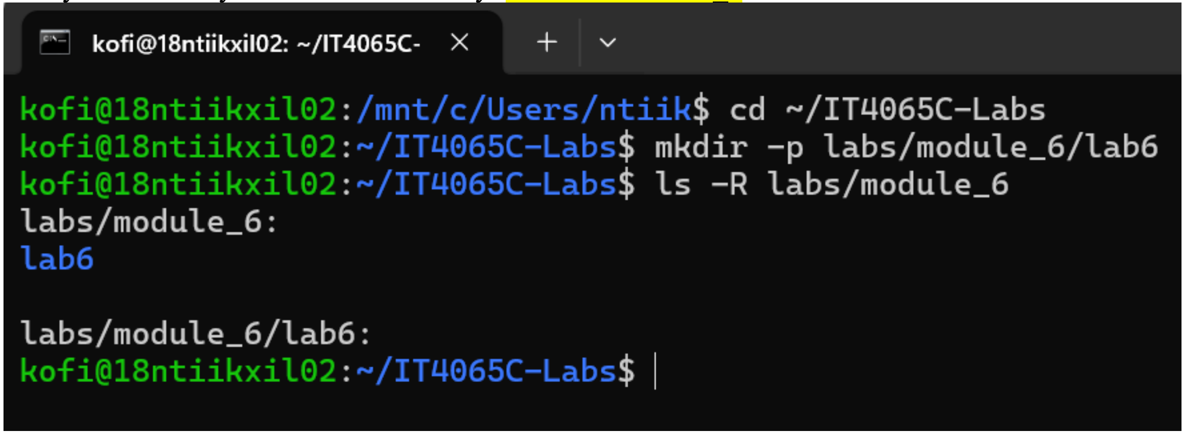
Purpose

In this lab, you move from *building* systems to *auditing* them. You will take on the role of a Data Administrator reviewing a 32-hour window of access logs. Your goal is to separate routine business activity from suspicious behavior and prepare a brief report for your Governance Committee.

Step 1: Generate the Audit Evidence

Before you can analyze the data, you must run the audit script to generate your report.

1. Navigate to the lab directory**:** cd ~/IT4065C-Labs
2. Create the Lab 6 directory (one time only): mkdir -p labs/module_6/lab6
3. Verify the directory was created correctly: ls -R labs/module_6

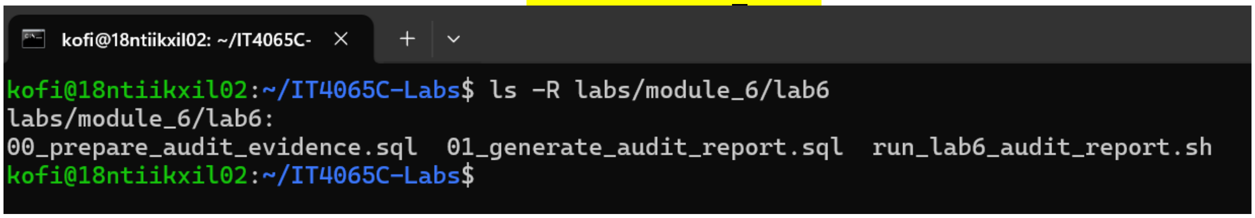


```
kofi@18ntiikxil02:/mnt/c/Users/ntiik$ cd ~/IT4065C-Labs
kofi@18ntiikxil02:~/IT4065C-Labs$ mkdir -p labs/module_6/lab6
kofi@18ntiikxil02:~/IT4065C-Labs$ ls -R labs/module_6
labs/module_6:
lab6

labs/module_6/lab6:
kofi@18ntiikxil02:~/IT4065C-Labs$
```

4. Download **Lab6_Source.zip** from Canvas.
5. Unzip the archive.
6. Navigate to the Lab 6 directory: cd ~/IT4065C-Labs/labs/module_6/lab6
7. Copy the following files into the lab6 directory:
   - *run_lab6_audit_report.sh*
   - *00_prepare_audit_evidence.sql*
   - *01_generate_audit_report.sql*

   Do not rename these files.
8. Confirm the files are in the correct location: *ls -R labs/module_6/lab6*



```
kofi@18ntiikxil02:~/IT4065C-Labs$ ls -R labs/module_6/lab6
labs/module_6/lab6:
00_prepare_audit_evidence.sql  01_generate_audit_report.sql  run_lab6_audit_report.sh
kofi@18ntiikxil02:~/IT4065C-Labs$
```

9. To avoid repeated password prompts, run**:** export PGPASSWORD='Pa$$w0rd123!'
10. Execute the master script from root **(**~/IT4065C-Labs**):**
    bash labs/module_6/lab6/run_lab6_audit_report.sh

Note: The output will appear directly in your terminal. You will need to scroll up to see all sections (Section 0 through Section 8).

Note on Generative AI (The “Security Consultant” Model)

In this lab, your goal is to think like an auditor, not just a technician. You are permitted to use Generative AI tools (such as Copilot, Gemini, ChatGPT, or Claude) as a Security Consultant to help you interpret the audit evidence.

How to Use Generative AI Effectively

If you are reviewing the evidence, especially the Candidate Incidents in Section 7, and are unsure why a particular activity may represent a risk, you may describe the scenario to a Generative AI tool to gain an additional perspective.

Example Prompt:

“In a data audit log, I see a user with the ‘Analyst’ role attempting a ‘Role Switch’ to ‘Admin’ multiple times and being denied each time. From a data governance perspective, what risks does this behavior introduce, and what would be an appropriate next administrative action?”

Use AI responses as *input for your thinking,* not as final answers.

Important Constraints

- **Verification:** You are responsible for the accuracy of your analysis. If an AI tool suggests a risk or concern, you must confirm that the supporting evidence actually appears in your terminal output.
- **Authenticity:** You must write your final audit summary (Step 4) in your own words. Do not copy and paste AI-generated text directly into your submission.
- **Human Judgment:** Generative AI does not know our organization’s specific governance rules or company policies. Final decisions, interpretations, and conclusions are your responsibility.
- If you used GenAI, include a brief note or screenshot of the prompt you used and explain one thing the AI pointed out that you hadn't initially noticed.

Step 2: Investigation (The "Hunt")

Scroll through your terminal output. Your "Admin Brain" should be looking for three types of events:

1. **The "Normal":** Routine SELECT queries during business hours.
2. **The "Aggressive":** Repeated failures followed by attempts to change identity (Role Switching).
3. **The "Out-of-Bounds":** Successful access that happened at an unusual time.

Focus your attention on:

- **Section 2 & 3:** Who is analyst_02 and why are they so interested in raw_pii?
- **Section 4:** What was steward_01 doing in the middle of the night?
- **Section 7:** Review the incident_flag column—these are your primary talking points.

Step 3: Governance Reasoning

Based on the evidence in **Section 7**, answer the following questions in your final document:

1. **Principle of Least Privilege:** Does the activity of analyst_02 suggest they have too much access, or is the system successfully "stopping" them? Justify your answer.
2. **The "Steward" Dilemma:** steward_01 successfully exported masked data at 4:32 AM. In a real-world company, would you flag this as a violation or "acceptable usage"? What additional information would you need to decide?
3. **Accountability:** Look at the client_ip and app_name columns. How do these technical details help you hold a specific person accountable compared to just seeing a username?

Step 4: Prepare the Audit Summary

Format your response as a professional memo to your supervisor. Use the structure provided in Section 8 of your terminal output.

Section	**What to include**
Observed Activity	A brief summary of the 32-hour window (how many events, how many denials).
High-Risk Findings	Specifically address the analyst_02 and steward_01 incidents.
Compliance Impact	Does this activity represent a "Control Failure" (the system broke) or "Attempted Violation" (the system worked)?
Recommended Action	Suggest one follow-up (e.g., "Reset analyst_02's password" or "Interview the Data Steward").

Submission Instructions

Submit a single **PDF or Word** document.

- **Include:** Your written responses to Steps 3 and 4.
- **Include:** A screenshot of **Section 7 (Candidate Incidents)** from your terminal to prove you ran the script successfully.
- **Naming Format:** FirstName_Lab6.pdf

A great auditor doesn't just find errors; they find patterns. Don't just list the denied attempts, explain the *intent* you see behind those attempts.