Per Scholas Lab

Name: Pelumi Johnson
Date: January 15, 2026
Institution: Per Scholas
Lab Title: Configuring Detective Controls for Object Access Activity

Objective

The objective of this lab was to configure and test detective controls by enabling and validating windows object access auditing. The lab focused on confirming that object deletion activity is properly recorded, identifying the correct audit records in Event Viewer, and verifying that user actions can be traced through Security log events.

Tools & Environment Used

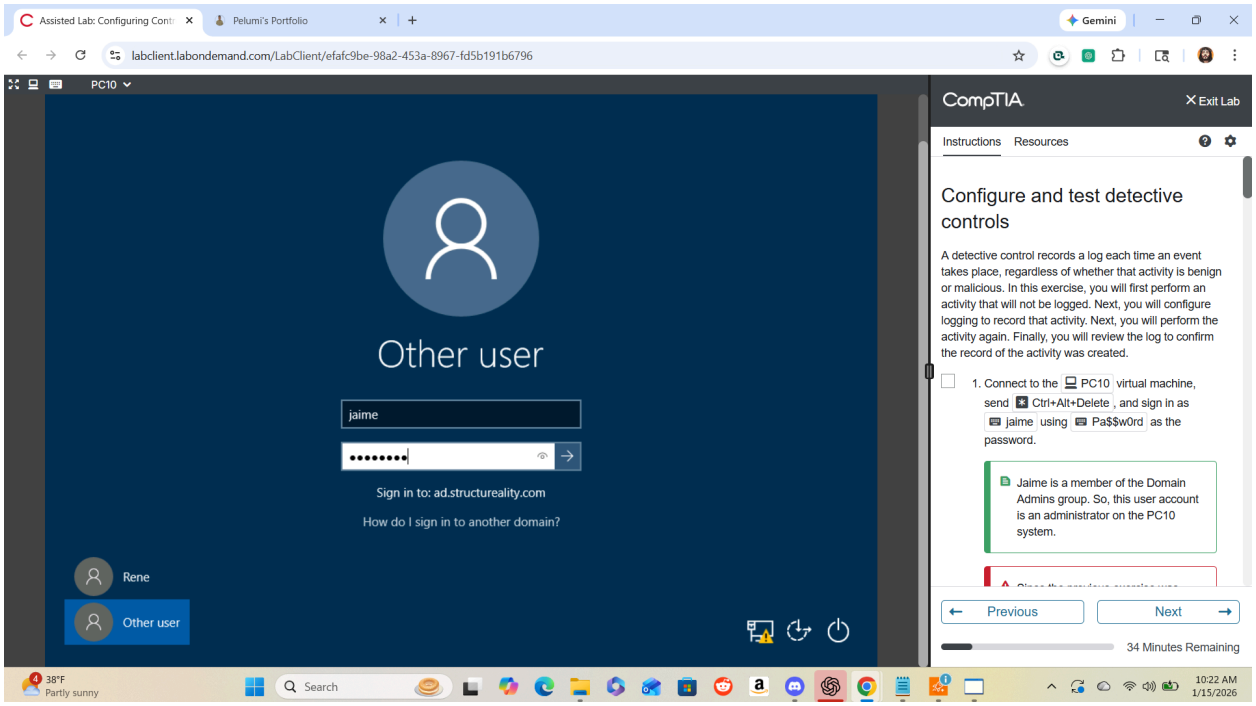
- uCertify Virtual Lab
- Windows Client Machine (PC10)
- Local Security Policy
- Advanced Security Settings (NTFS Auditing)
- File Explorer
- Event Viewer (Windows Logs → Security)
- Domain User Accounts (Administrator)

Lab Overview

Detective controls do not prevent actions; they record events so activity can be reviewed and investigated. This lab demonstrated how to confirm when auditing is not occurring, enable object access auditing at the system level, configure auditing on a specific folder, and then validate that a deletion produces the correct Security Event Log records.

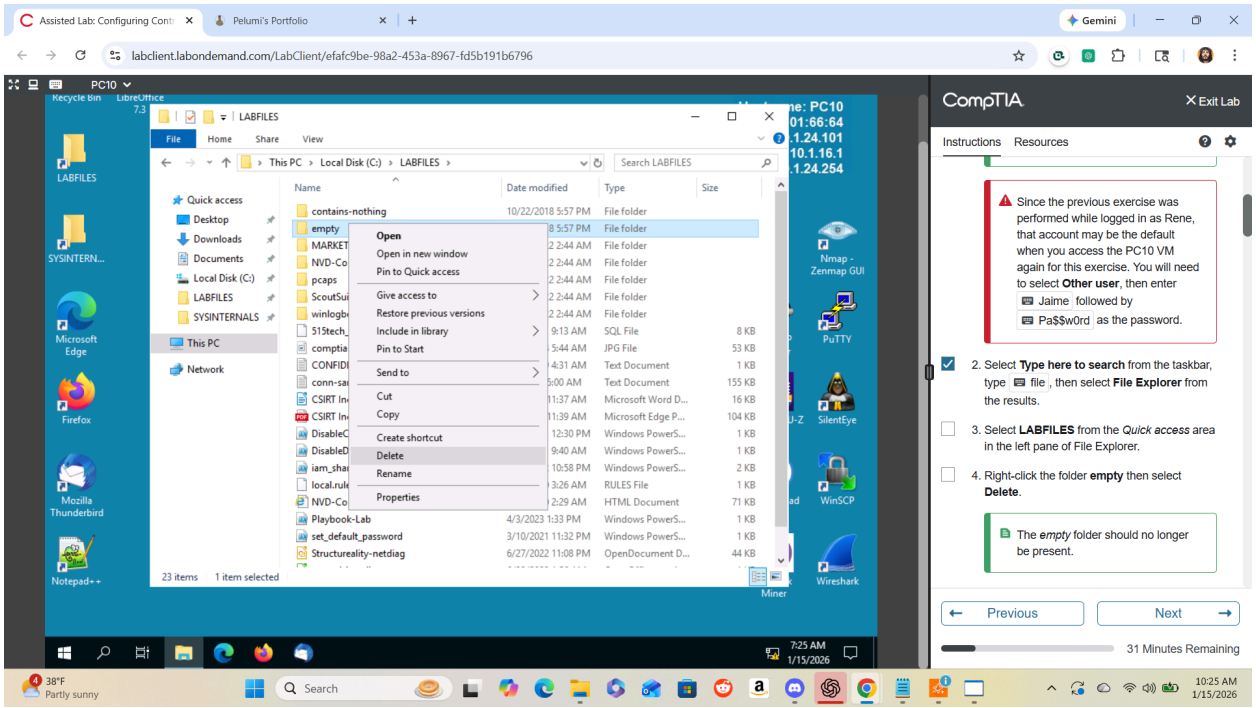
Step 1: Logging in as Administrator

The PC10 client machine was accessed and the session was signed in using the administrator account Jaime. Administrative privileges were required to configure audit policy and auditing settings on protected objects.



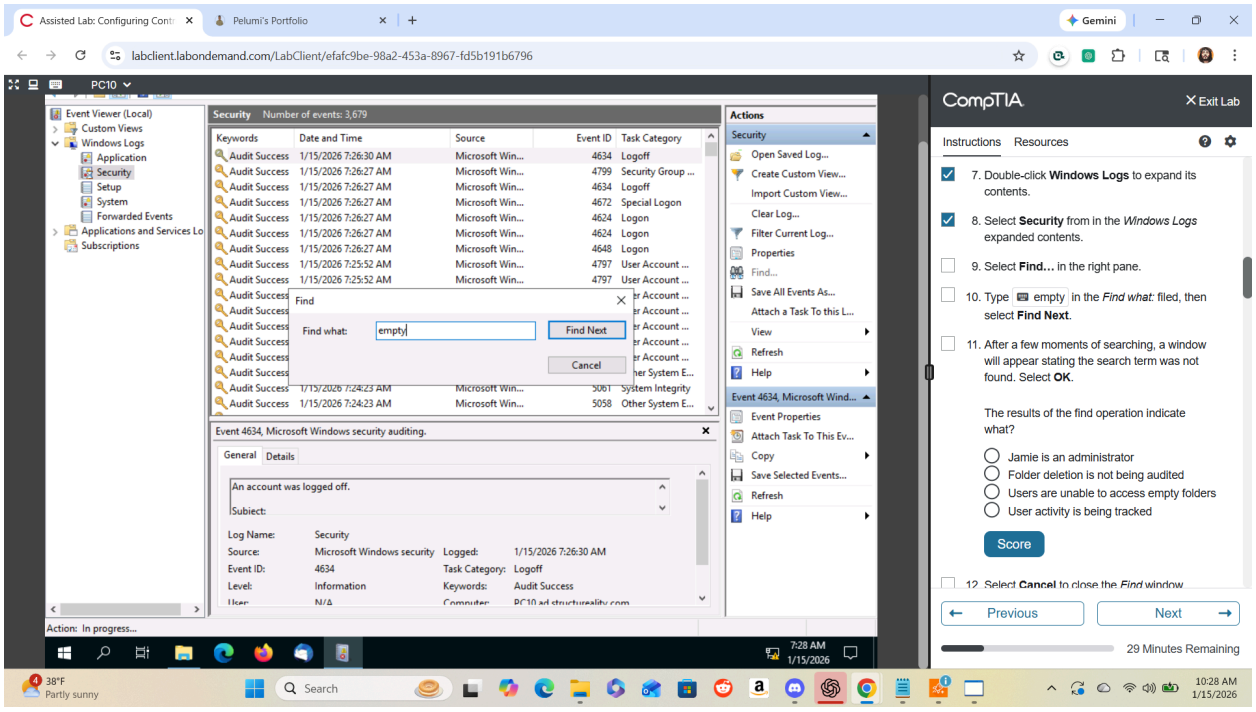
Step 2: Performing Activity Before Auditing (Baseline Test)

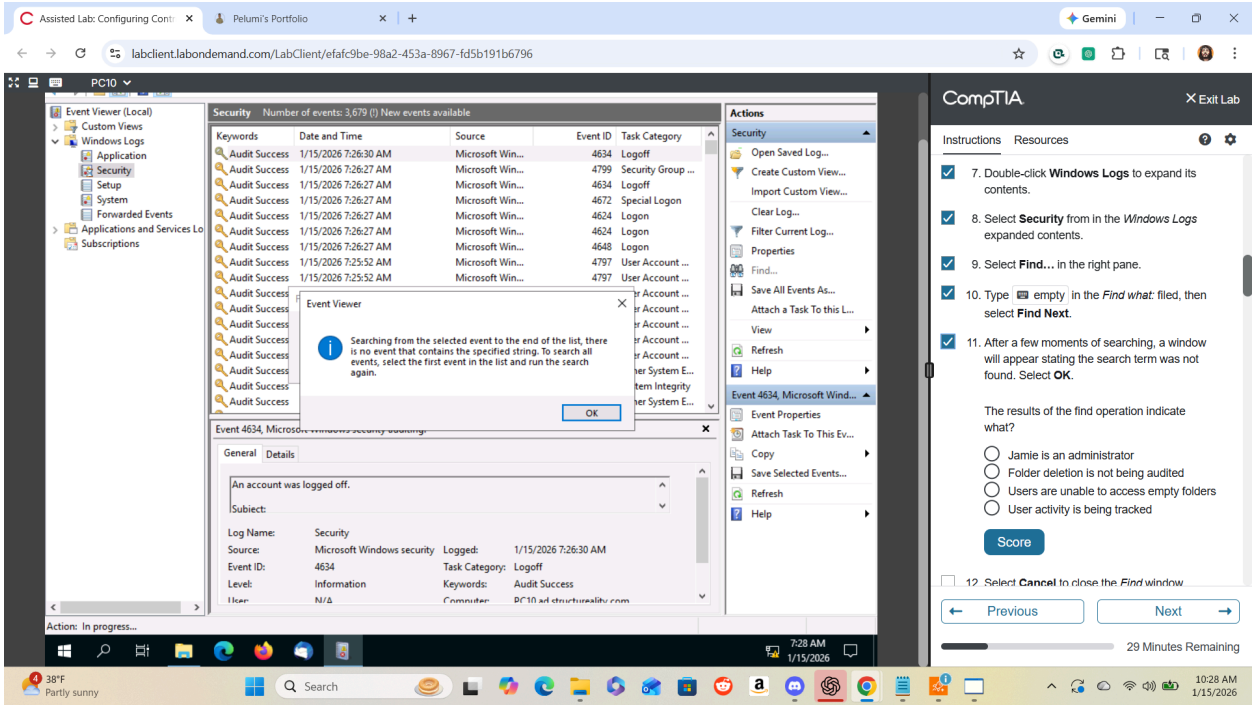
Before configuring auditing, a test was performed by deleting the folder named **empty** inside: **C:\LABFILES**



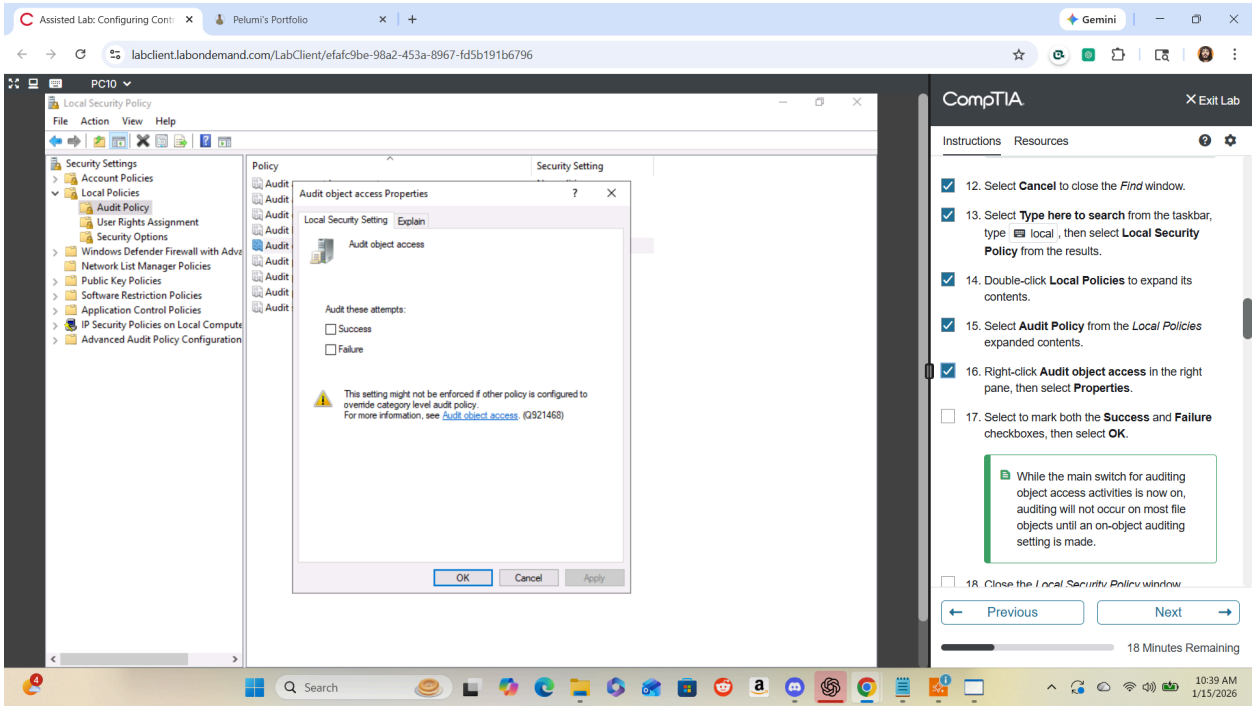
Event Viewer was opened (Windows Logs → Security) and the Find function was used to search for the term: empty

A message appeared stating the search term was not found. This indicated that folder deletion activity was not being audited at this stage.





Step 3: Enabling Object Access Auditing (System Policy)
Local Security Policy was opened and the following path was used:
Local Policies → Audit Policy

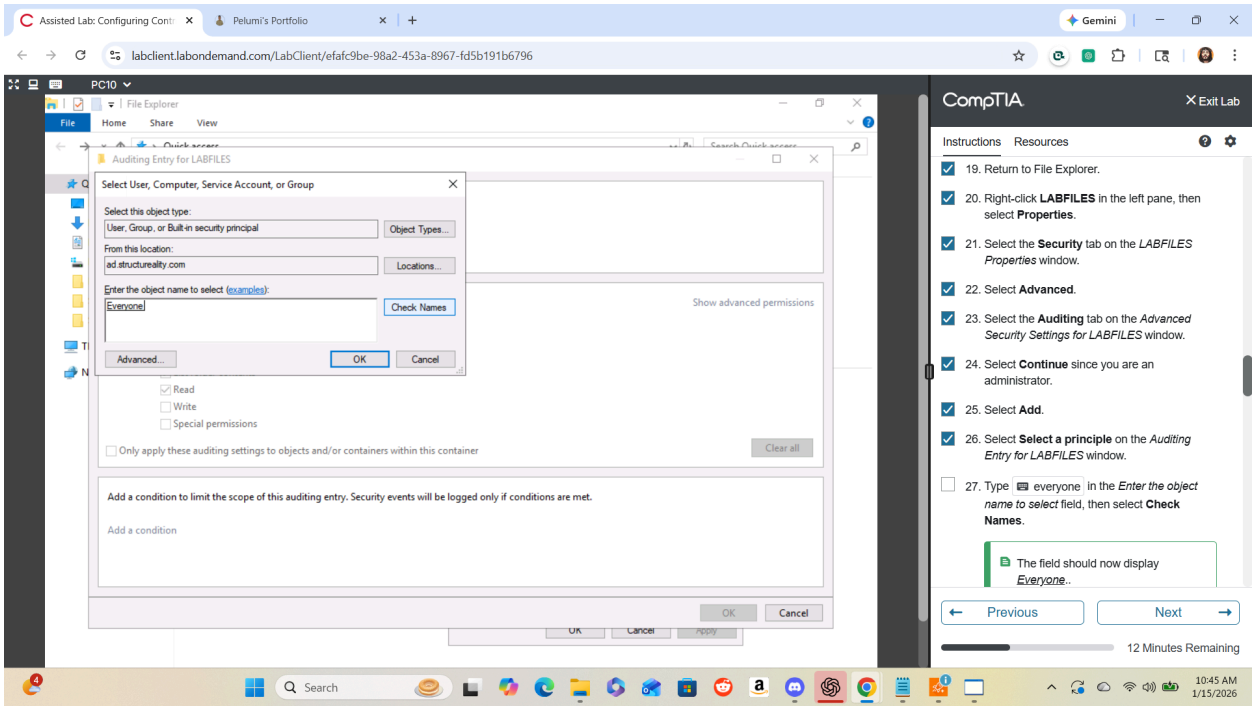


The policy Audit object access was opened, and both checkboxes were enabled:

- **Success**
- **Failure**

This turned on the system-level auditing switch for object access activity.

Step 4: Configuring Auditing on the LABFILES Folder (Object-Level Auditing)
File Explorer was used to locate:
C:\LABFILES

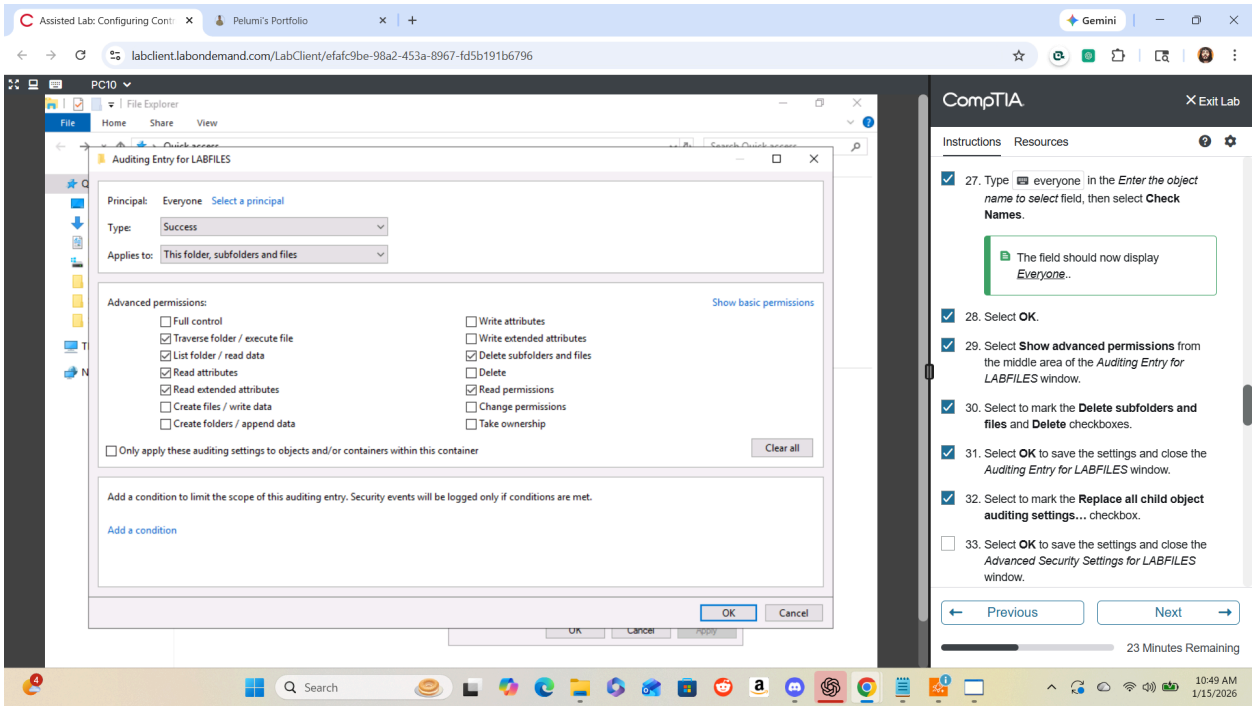


The following path was used to configure auditing:
LABFILES → Properties → Security → Advanced → Auditing → Add

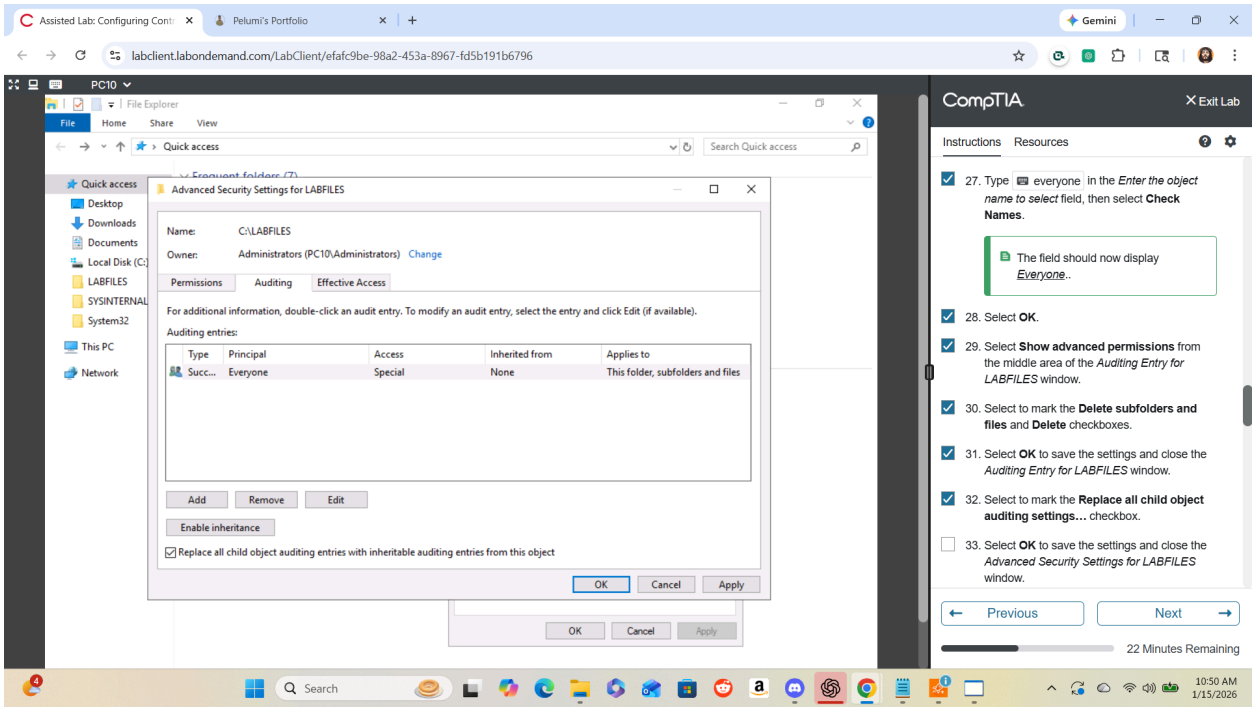
A new auditing entry was created with:
Principal: Everyone
Type: Success
Applies to: This folder, subfolders and files

Show advanced permissions was selected, and the auditing options were configured to include:

- **Delete**
- **Delete subfolders and files**

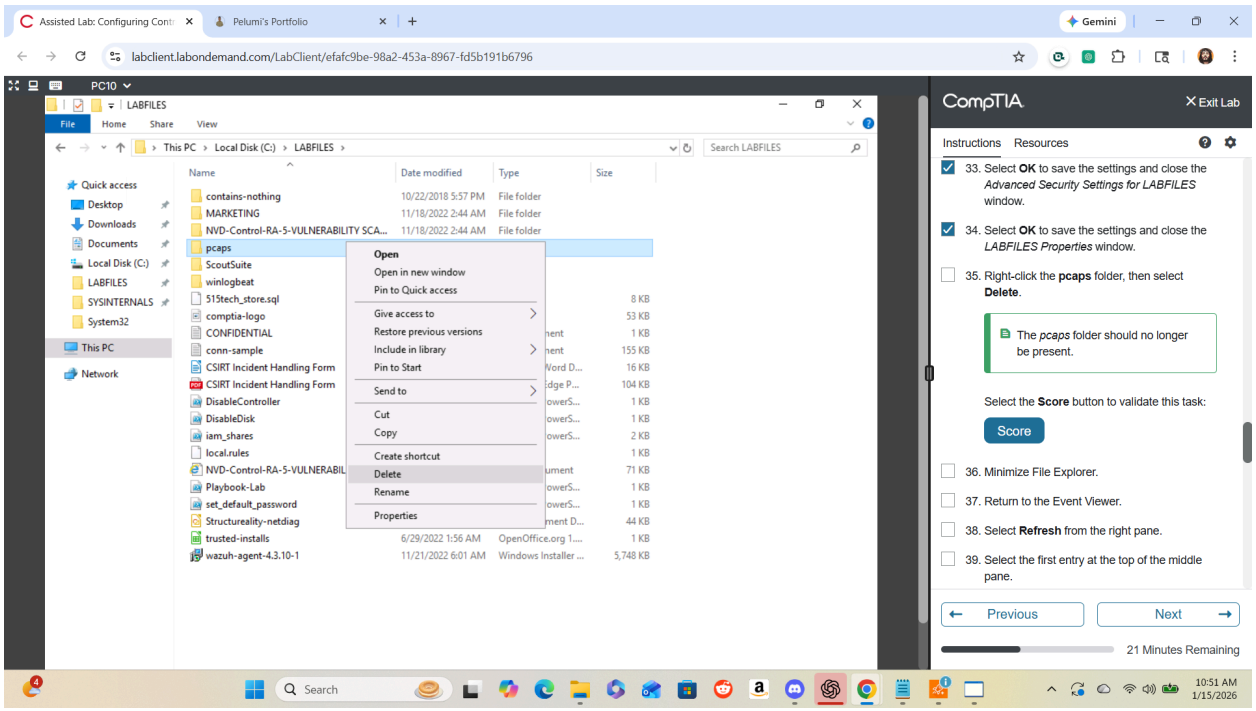


The Replace all child object auditing entries option was selected to ensure the settings applied to subfolders and files within **LABFILES.**



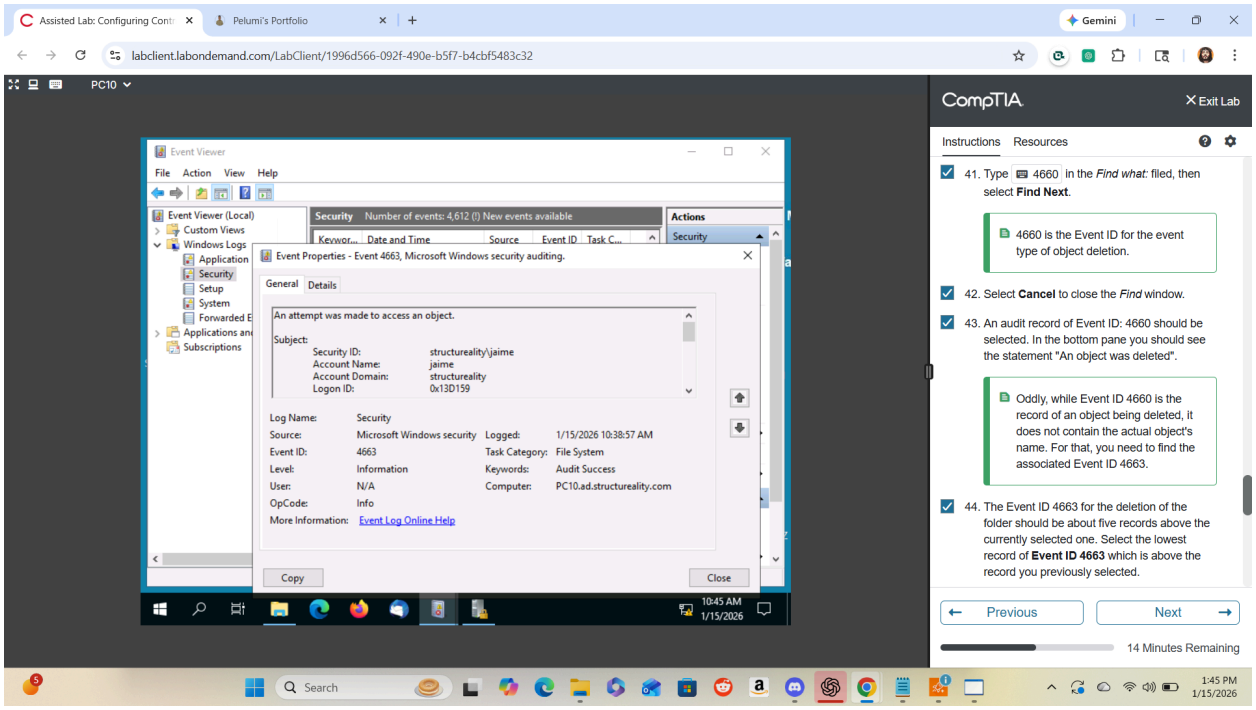
Step 5: Performing the Audited Deletion Activity
After auditing was configured, a deletion was performed within:
C:\LABFILES

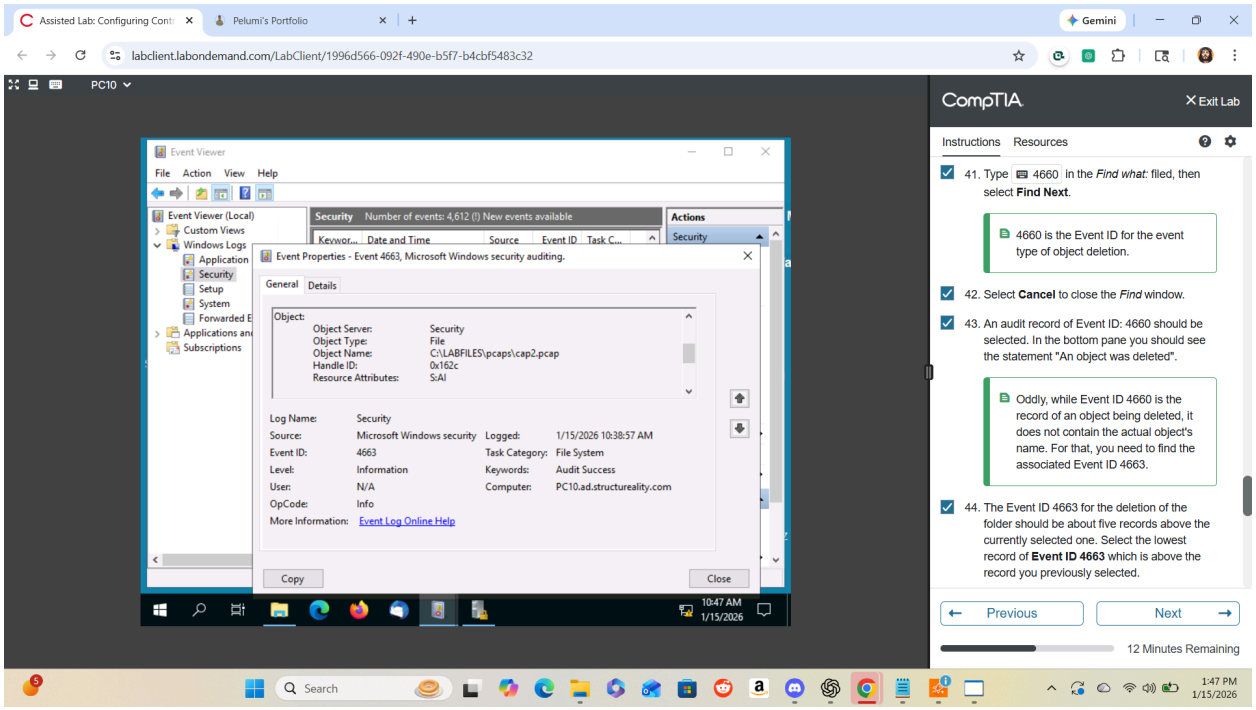
The folder **pcaps** was right-clicked and deleted to generate an auditable event.

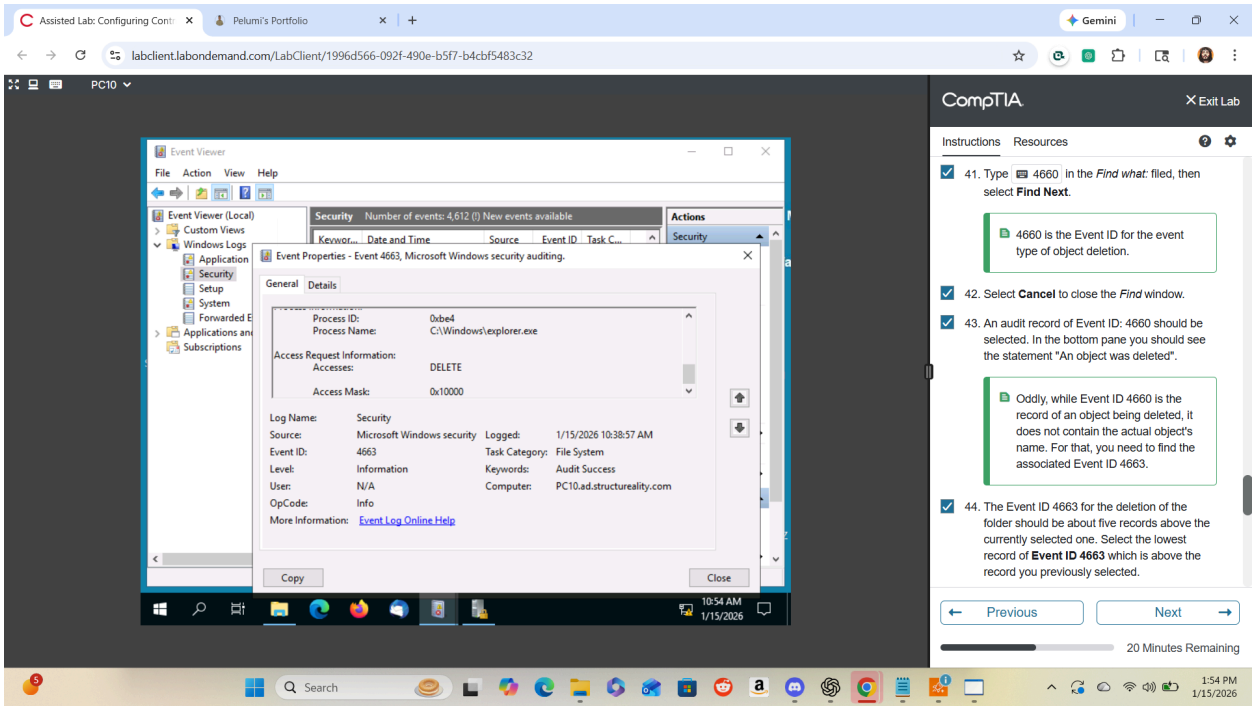


Step 6: Locating the Deletion Record (Event ID 4660)
Event Viewer (Windows Logs → Security) was refreshed, and the Find function was used to search for: **4660**

Event ID 4660 was located, confirming that an object deletion event was recorded.

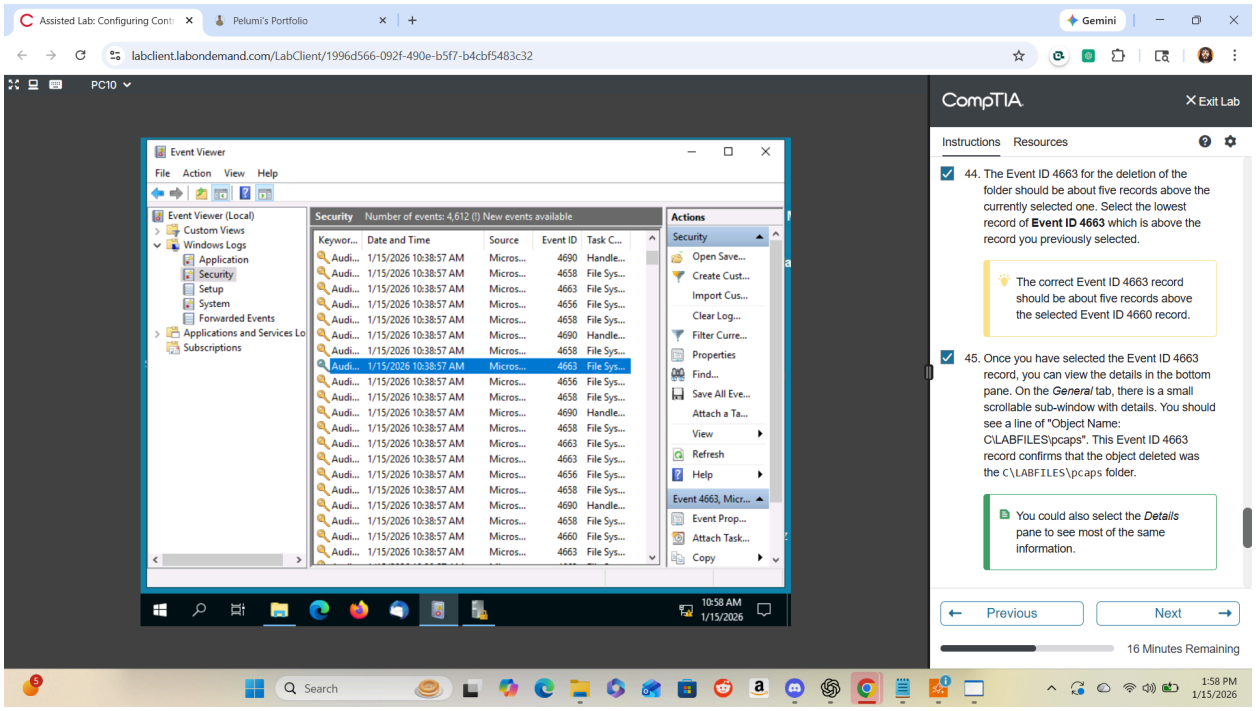

Assisted Lab: Configuring Contr
Pelumi's Portfolio
Gemini
labclient.labondemand.com/LabClient/1996d566-092f-490e-b5f7-b4cbf5483c32
PC10
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded E
Applications and
Subscriptions
Security Number of events: 4,612 (!) New events available
Keywor... Date and Time Source Event ID Task C...
Actions
Security
Event Properties - Event 4663, Microsoft Windows security auditing.
General Details
An attempt was made to access an object.
Subject:
Security ID: structureality\jaime
Account Name: jaime
Account Domain: structureality
Logon ID: 0x13D159
Log Name: Security
Source: Microsoft Windows security
Logged: 1/15/2026 10:38:57 AM
Event ID: 4663
Task Category: File System
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC10.ad.structureality.com
OpCode: Info
More Information: Event Log Online Help
Copy
Close
10:45 AM
1/15/2026
CompTIA
Exit Lab
Instructions
Resources
41. Type 4660 in the Find what: filed, then select Find Next.
4660 is the Event ID for the event type of object deletion.
42. Select Cancel to close the Find window.
43. An audit record of Event ID: 4660 should be selected. In the bottom pane you should see the statement "An object was deleted".
Oddly, while Event ID 4660 is the record of an object being deleted, it does not contain the actual object's name. For that, you need to find the associated Event ID 4663.
44. The Event ID 4663 for the deletion of the folder should be about five records above the currently selected one. Select the lowest record of Event ID 4663 which is above the record you previously selected.
Previous
Next
14 Minutes Remaining
Search
1:45 PM
1/15/2026


Assisted Lab: Configuring Contr
Pelumi's Portfolio
Gemini
labclient.labondemand.com/LabClient/1996d566-092f-490e-b5f7-b4cbf5483c32
PC10
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded E
Applications and
Subscriptions
Security Number of events: 4,612 (!) New events available
Keywor... Date and Time Source Event ID Task C...
Actions
Security
Event Properties - Event 4663, Microsoft Windows security auditing.
General Details
Object:
Object Server: Security
Object Type: File
Object Name: C:\LABFILES\pcaps\cap2.pcap
Handle ID: 0x162c
Resource Attributes: S:AI
Log Name: Security
Source: Microsoft Windows security
Logged: 1/15/2026 10:38:57 AM
Event ID: 4663
Task Category: File System
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC10.ad.structureality.com
OpCode: Info
More Information: Event Log Online Help
Copy
Close
10:47 AM
1/15/2026
CompTIA
Exit Lab
Instructions
Resources
41. Type 4660 in the Find what: filed, then select Find Next.
4660 is the Event ID for the event type of object deletion.
42. Select Cancel to close the Find window.
43. An audit record of Event ID: 4660 should be selected. In the bottom pane you should see the statement "An object was deleted".
Oddly, while Event ID 4660 is the record of an object being deleted, it does not contain the actual object's name. For that, you need to find the associated Event ID 4663.
44. The Event ID 4663 for the deletion of the folder should be about five records above the currently selected one. Select the lowest record of Event ID 4663 which is above the record you previously selected.
Previous
Next
12 Minutes Remaining
Search
1:47 PM
1/15/2026



Step 7: Correlating the Object Name (Event ID 4663)

Because Event ID 4660 does not display the object name, the associated Event ID 4663 record was located (about five records above the 4660 entry).



Event ID 4663 was opened and reviewed in the bottom pane. The record contained the deleted object path, confirming the deletion activity was successfully captured and attributable.

Step 8: Confirming the Purpose of a Detective Control. The lab knowledge check confirmed the purpose of a detective control is to: **Create a record of events and activities**

This aligns with the auditing outcome observed in Event Viewer.

Step 9: Validating Task Completion
The lab task validation confirmed the recorded activity and indicated successful completion after the deletion event was detected and verified through the log records.

Step 10: Signing Out
The session was signed out from PC10 to complete the lab.

Results:

- A baseline test confirmed folder deletion was not initially being audited
- Audit object access was enabled for Success and Failure in Local Security Policy
- Object-level auditing was configured on **C:\LABFILES** for deletions
- Deletion activity generated Security log records
- Event ID 4660 confirmed deletion occurred
- Event ID 4663 confirmed the object name/path and access details
- Detective control was implemented and validated

Conclusion:

This lab demonstrated a complete detective control workflow: validating the lack of auditing, enabling object access auditing, configuring auditing on a protected folder, and verifying that a folder deletion produced the correct Security Event Log records. By capturing and correlating Event IDs, user activity became traceable and verifiable supporting accountability and incident investigation requirements.