

Scenario

In this lab, I will learn about several types of security controls, including preventive, detective, directive, and corrective.

As a security team member of Structureality Inc, I'm working to improve my organization's security stance. This lab focuses on configuring, using or testing the security controls to ensure we understand the nature of the various types of controls. These exercises will facilitate my recommendations on the remediations to resolve security weaknesses. First, I will work with a preventive control, then a detective control. Next, I will work with a directive control and finally, a corrective control.

will be working from a virtual machine named PC10, hosting Windows Server 2019, which serves as a client in this lab environment.

Objectives

This activity is designed to test our understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

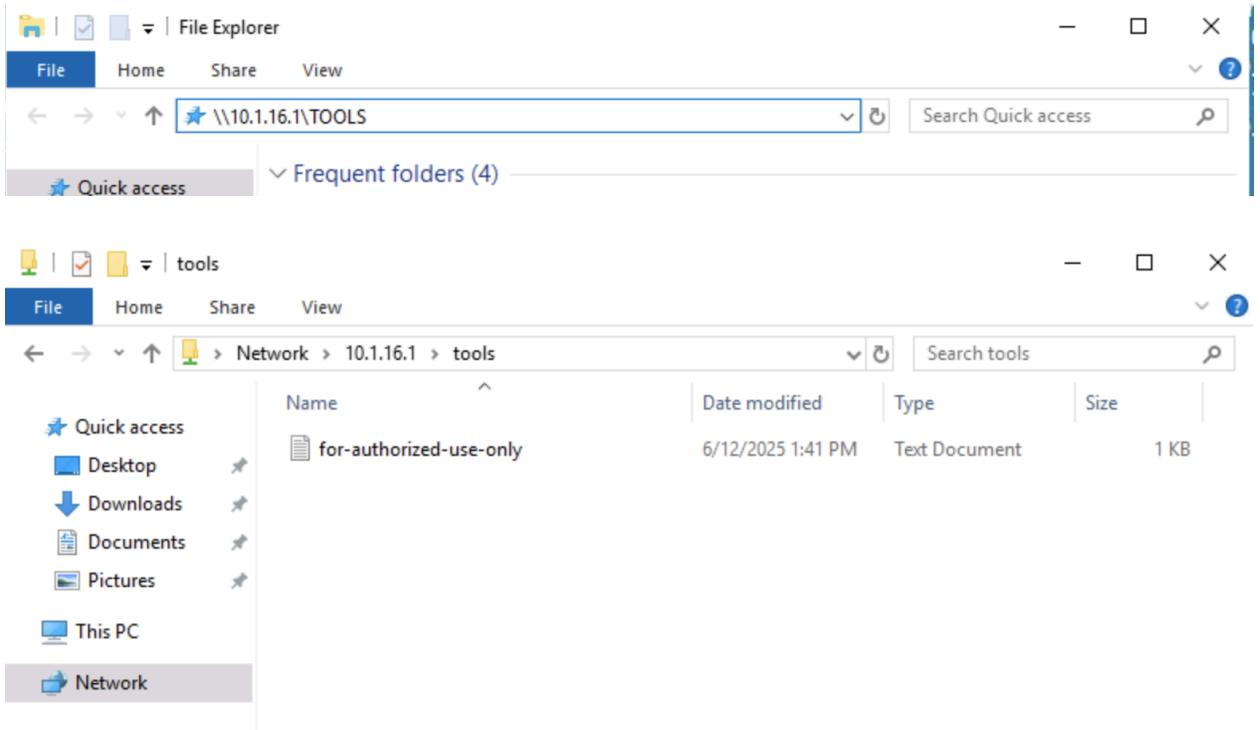
- 1.1 Compare and contrast various types of security controls.

Configure and test preventive controls

A preventive control attempts to stop an unwanted activity from taking place. In this exercise, I will first perform an undesirable activity. Next, I will implement a preventive control to block that activity. And finally, I will attempt the unwanted activity again to test the preventive control.

A TOOLS folder has been configured on the DC10 server. This folder is designed to hold utilities and data files that must only be accessible to domain and local administrators only. Users without an administrative rule should be prevented from viewing the share.

1. Now we will Verify whether the share has been configured with appropriate permissions by trying to access it using a non-administrative account.
2. select **Other user**. In the User name box, type **Sam**. In the Password box, type **Pa\$\$w0rd**, and press **Enter**.
3. From the taskbar, select **File Explorer** and look for the file by typing **\\\10.1.16.1\TOOLS** and hit enter.



Sam is not an administrator and should not have access. I need to implement a prevention control so that Sam and other non-administrators cannot access this share.

4. Now, Select the DC10 VM, sign in as Structureality\Administrator using Pa\$\$w0rd as the password.
5. In **Server Manager**, select **File and Storage Services**, and then select **Shares**. Right-click the **TOOLS** share, then select **Properties**. Select the **Permissions** tab, and then click **Customize permissions**.

Server Manager

File and Storage Services > Shares

Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders

SHARES
All shares | 3 total

Share	Local Path
DC10 (3)	
NETLOGON	C:\Windows\SYSVOL\sysvol\ad.str...
SYSVOL	C:\Windows\SYSVOL\sysvol
TOOLS	C:\TOOLS

VOLUME
TOOLS on DC10

(C:)	
Capacity: 39.4 GB	
33.2% Used	13.1 GB Used Space
	26.3 GB Free Space

[Go to Volumes Overview >](#)

QUOTA
TOOLS on DC10

To use quotas, File Server Resource Manager must be installed.

To install File Server Resource Manager, start the Add Roles and Features Wizard.

TOOLS Properties

TOOLS

Show All

General

Permissions



Settings



General

Server Name: DC10

Share name: TOOLS

Share description: Shared TOOLS Folder

Folder path: C:\TOOLS

Protocol: SMB

Availability type: Not Clustered

TOOLS Properties

- □ ×

TOOLS

Show All

General

+

Permissions

-

Settings

+

Permissions

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

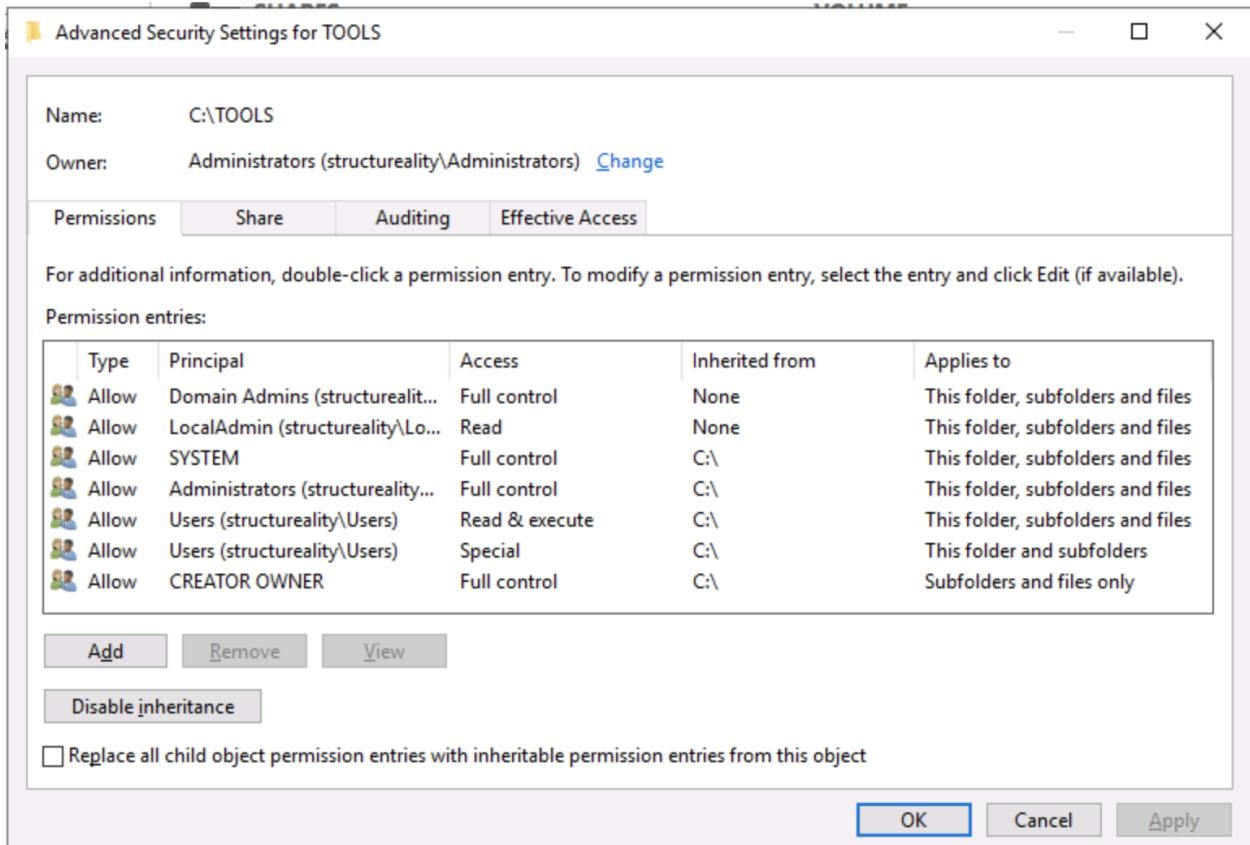
Share permissions: Everyone Full Control

Folder permissions:

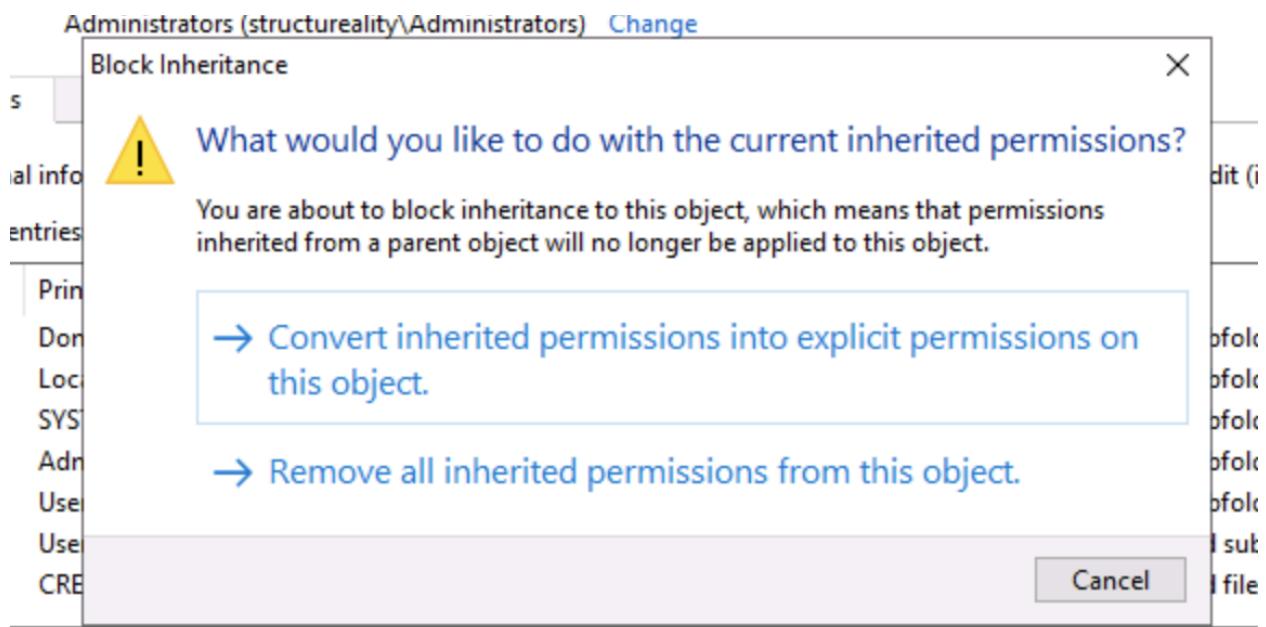
Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders an...
Allow	BUILTIN\Users	Special	This folder an...
Allow	BUILTIN\Users	Read & execu...	This folder, su...
Allow	BUILTIN\Administrators	Full Control	This folder, su...
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, su...
Allow	structureality\LocalAdmin	Read	This folder, su...
Allow	structureality\Domain Admins	Full Control	This folder, su...

< >

Customize permissions...



6. Which account or group object on the access control list should NOT have been assigned permissions on the share? **Users**
7. Observe that the Domain Admins and LocalAdmin security groups have been granted permissions on the folder. However, observe that the Domain Users group has inherited read permissions from the share's parent folder. This is the misconfiguration that allows Sam to view the share.
8. Select the **Disable inheritance** button. In the Block inheritance dialog, select **Convert inherited permissions...**



9. From the Permission entries panel, select the first **Users (structureality\Users)** object, and then click the Remove button.

The screenshot shows the 'Permission entries:' panel. It lists several security principals and their access rights. The row for 'Users (structureality\Users)' is selected, highlighted with a blue background. Below the table are buttons for 'Add', 'Remove', and 'Edit'. An 'Enable inheritance' link is also visible.

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (structurealit...	Full control	None	This folder, subfolders and files
Allow	LocalAdmin (structureality\Lo...	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (structureality...	Full control	None	This folder, subfolders and files
Allow	Users (structureality\Users)	Read & execute	None	This folder, subfolders and files
Allow	Users (structureality\Users)	Special	None	This folder and subfolders
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

10. Remove the remaining **Users (structureality\Users)** object.

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (structurealit...)	Full control	None	This folder, subfolders and files
Allow	LocalAdmin (structureality\Lo...)	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (structureality...)	Full control	None	This folder, subfolders and files
Allow	Users (structureality\Users)	Read & execute	None	This folder, subfolders and files
Allow	Users (structureality\Users)	Special	None	This folder and subfolders
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

Add Remove Edit

Enable inheritance

TOOLS Properties

Advanced Security Settings for TOOLS

Name: C:\TOOLS

Owner: Administrators (structureality\Administrators) Change

Permissions Share Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (structurealit...)	Full control	None	This folder, subfolders and files
Allow	LocalAdmin (structureality\Lo...)	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (structureality...)	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

Add Remove Edit

Enable inheritance

Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

11. Select **Remove** to remove the *Everyone* group from the object's ACL entirely.

The screenshot shows the Windows File Explorer context menu for a folder named 'TOOLS'. The 'Security' option is highlighted. Below the menu, two dialog boxes are displayed side-by-side.

Advanced Security Settings for TOOLS

Name: C:\TOOLS
Owner: Administrators (structureality\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.
Network location for this share: \\DC10.ad.structureality.com\TOOLS
Permission entries:

Type	Principal	Access
Allow	Everyone	Full Control

Properties

Owner: Administrators (structureality\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.
Network location for this share: \\DC10.ad.structureality.com\TOOLS
Permission entries:
No groups or users have permission to access this object. However, the owner of this object can assign permissions.

The default privilege over objects in Windows is *no access*. Thus, without an explicitly defined *allow*, users will have a default or implicit *deny*.

It is important not to implement an explicit *deny* at this juncture as it may have unintended consequences. For example, administrators are users, so they are automatically members of the Domain Users and Everyone groups. Setting *deny* for one of these groups would also deny access to the administrators who need access. In the majority of cases, explicit deny permissions will not be required.

12. Select **OK** to close the dialogs.

Name: C:\TOOLS

Owner: Administrators (structureality\Administrators) [Change](#)

[Permissions](#) [Share](#) [Auditing](#) [Effective Access](#)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (structurealit...)	Full control	None	This folder, subfolders and files
Allow	LocalAdmin (structureality\Lo...)	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (structureality...)	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only

Name: C:\TOOLS

Owner: Administrators (structureality\Administrators) [Change](#)

[Permissions](#) [Share](#) [Auditing](#) [Effective Access](#)

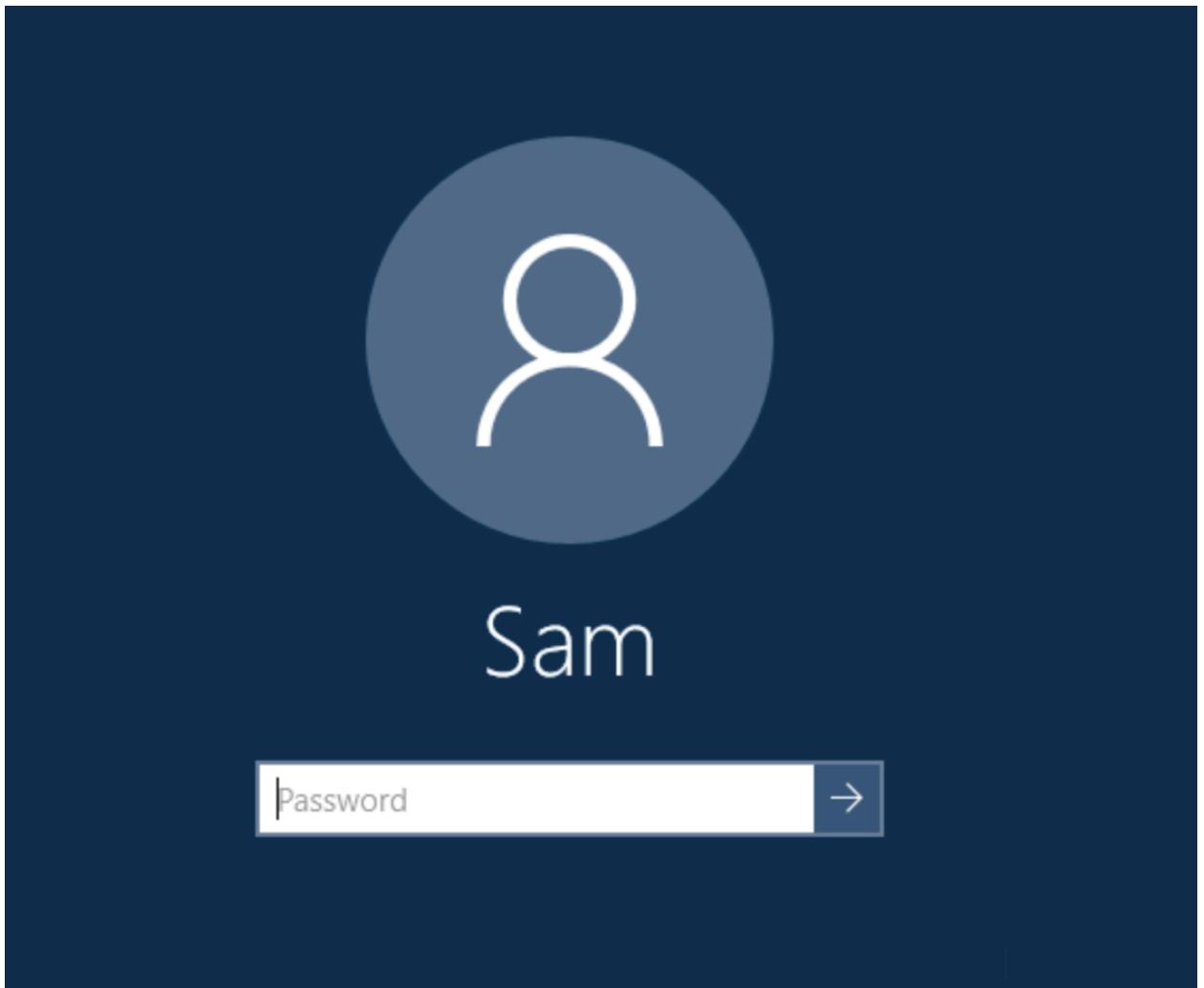
To modify share permissions, select the entry and click Edit.

Network location for this share: \\DC10.ad.structureality.com\TOOLS

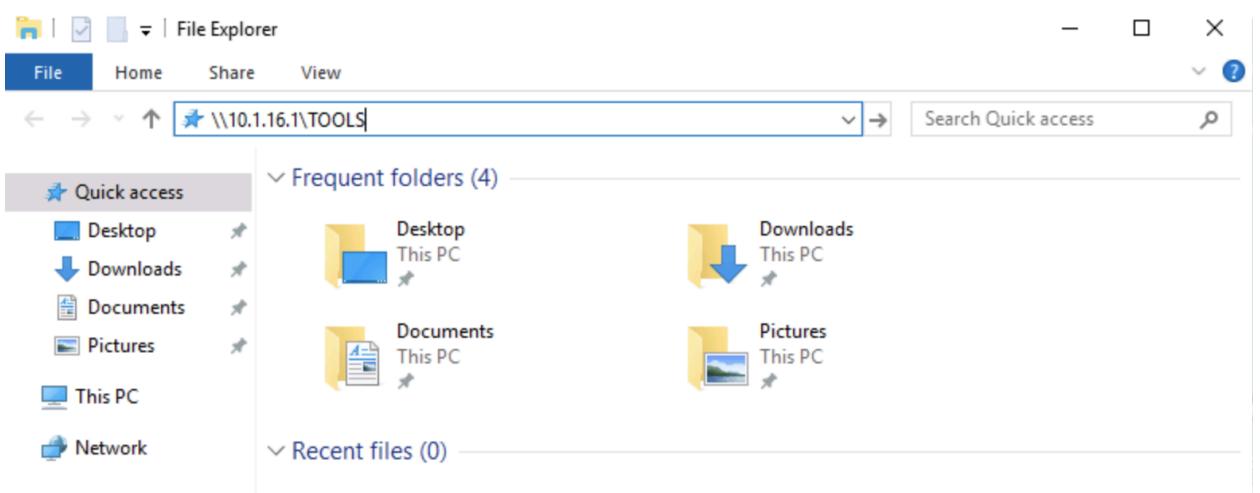
Permission entries:

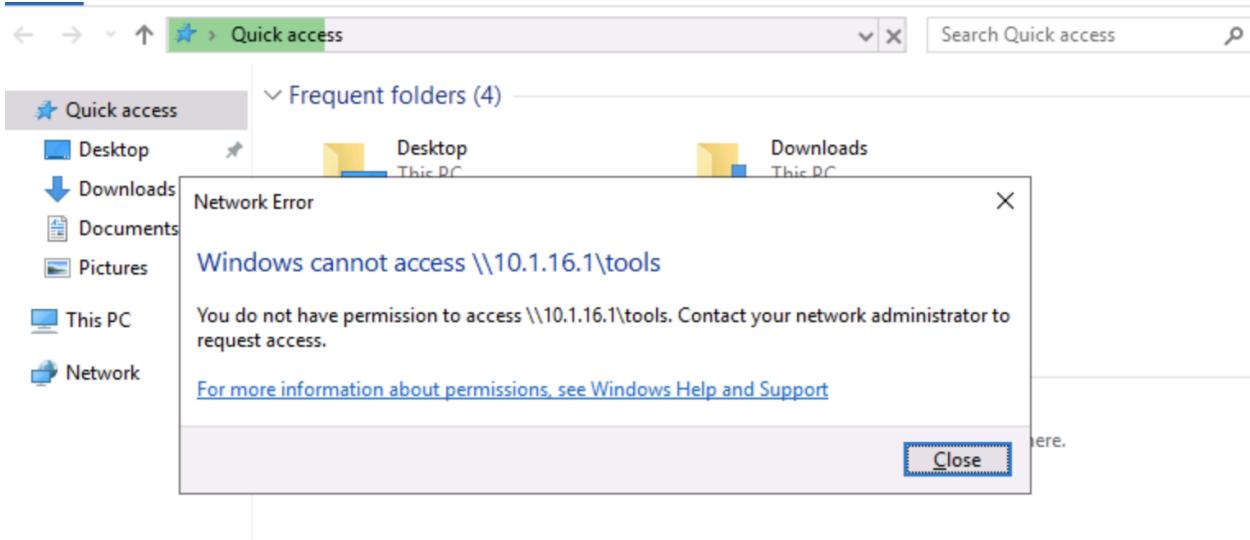
No groups or users have permission to access this object. However, the owner of this object can assign permissions.

13. Switch back to the PC10 VM, sign in as Sam using Pa\$\$w0rd as the password.



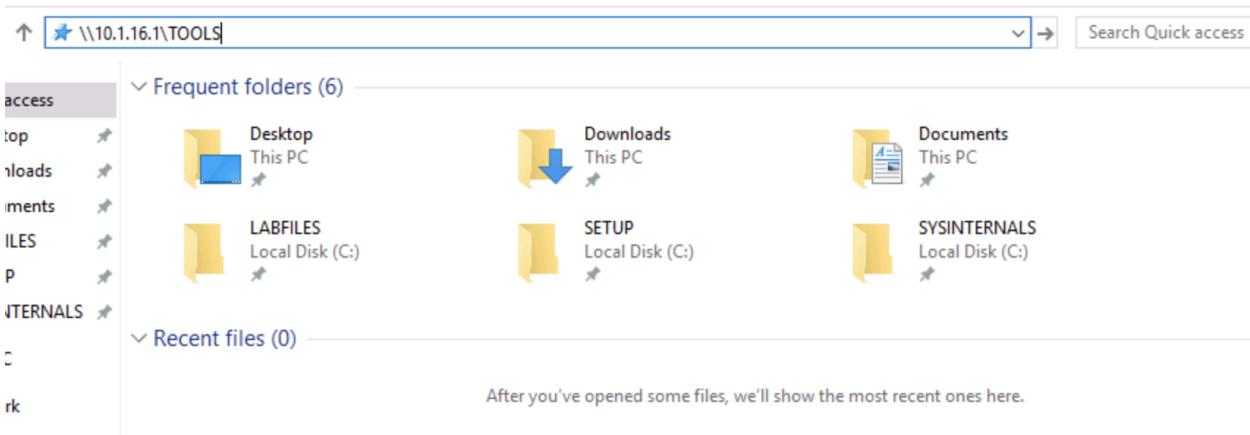
14. Open File Explorer and browse to \\10.1.16.1\TOOLS.

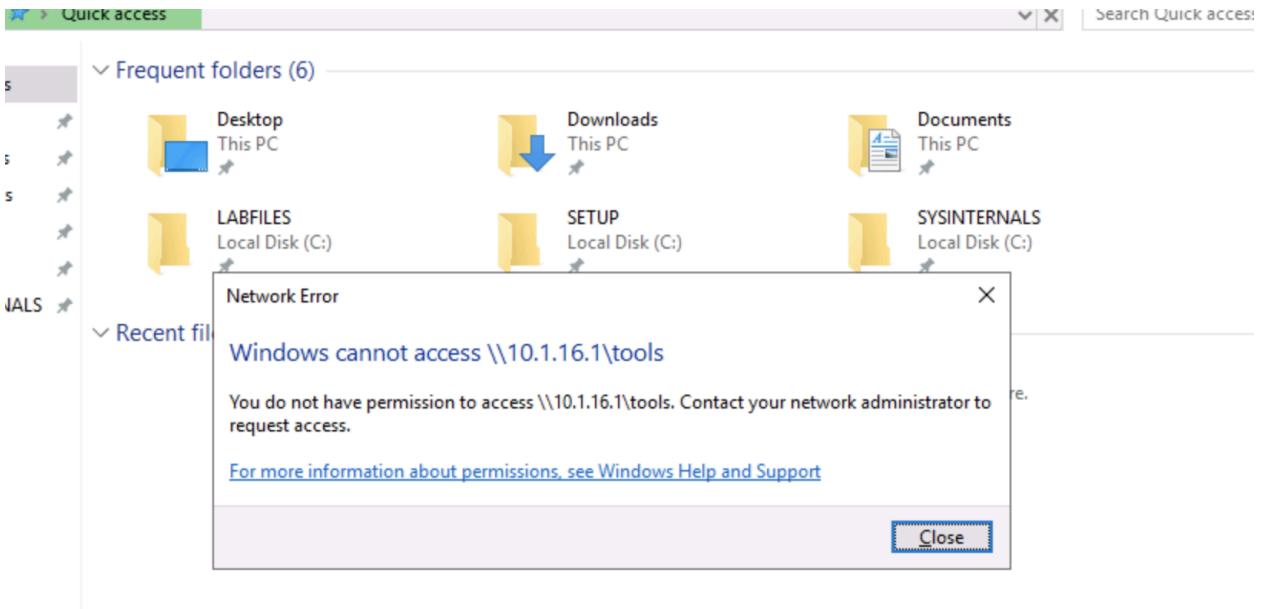




we should see a *Network Error* message indicating that we cannot access this resource.

15. Now, sign in as **Jaime** using **Pa\$\$w0rd** as the password. Try to Open File Explorer and browse to **\\\10.1.16.1\TOOLS**.





The share should be accessible to Jaime's account because it is a member of the LocalAdmin security group. This group has local administrator privileges over computers joined to the domain, but does not have full Domain Admins privileges.

File access controls are classed as preventive in terms of functionality. What category of security control are file permissions? **Technical**

I have successfully implemented a preventive control to block nonadministrative users from accessing resources only for administrators. However, in a real-world situation, we should compare any concerning issue to company security policy and configuration baselines. If we have discovered a variant or violation, it must be reported to the security team. This report may include recommendations for remediation.

Configure and test detective controls

A detective control records a log each time an event occurs, regardless of whether that activity is benign or malicious. In this exercise, we will first perform an activity that will not be logged. Next, we will configure logging to record that activity, and then we will perform the activity again. Finally, we will review the log to confirm the record of the activity was created.

16. sign in as **Jaime** using **Pa\$\$w0rd** as the password. **Jaime** is a member of the **LocalAdmin** group. So, this user account is an administrator on the PC10 system.
17. Open File Explorer, and from the Quick access pane, select **LABFILES**. Right-click the folder **empty** then select **Delete**.

LABFILES

Home Share View

This PC > Local Disk (C:) > LABFILES >

Search LABFILES

	Name	Date modified	Type	Size
k access	contains-nothing	10/22/2018 7:57 PM	File folder	
ktop	empty	10/22/2018 7:57 PM	File folder	
vnloads	MARKETING	AM	File folder	
:uments	NVD-Control	AM	File folder	
IFILES	pcaps	AM	File folder	
UP	ScoutSuite	AM	File folder	
INTERNALS	winlogbeat	AM	File folder	
PC	515tech_stor	3 AM	SQL File	8 KB
ork	comptia-log	4 AM	JPG File	53 KB
	CONFIDENTI	AM	Text Document	1 KB
	conn-sample	AM	Text Document	155 KB
	CSIRT Incident	PM	Microsoft Word D...	16 KB
	CSIRT Incident	PM	Microsoft Edge P...	104 KB
	DisableContr	10 AM	Windows PowerS...	1 KB
	DisableDisk	10 AM	Windows PowerS...	1 KB
	iam_shares	18 AM	Windows PowerS...	2 KB
	laptop-full	1 AM	Wireshark capture...	321 KB
	laptop-select	7 AM	Wireshark capture...	306 KB
	local.rules	3/10/2020 5:26 AM	RULES File	1 KB
	NVD-Control-RA-5-VULNERABILITY SCA...	1/21/2020 4:29 AM	Microsoft Edge H...	71 KB
	set_default_password	3/11/2021 1:32 AM	Windows PowerS...	1 KB
	Structureality-netdiag	6/28/2022 1:08 AM	OpenDocument D...	44 KB
	trusted-installs	6/29/2022 3:56 AM	OpenOffice.org 1....	1 KB

LABFILES

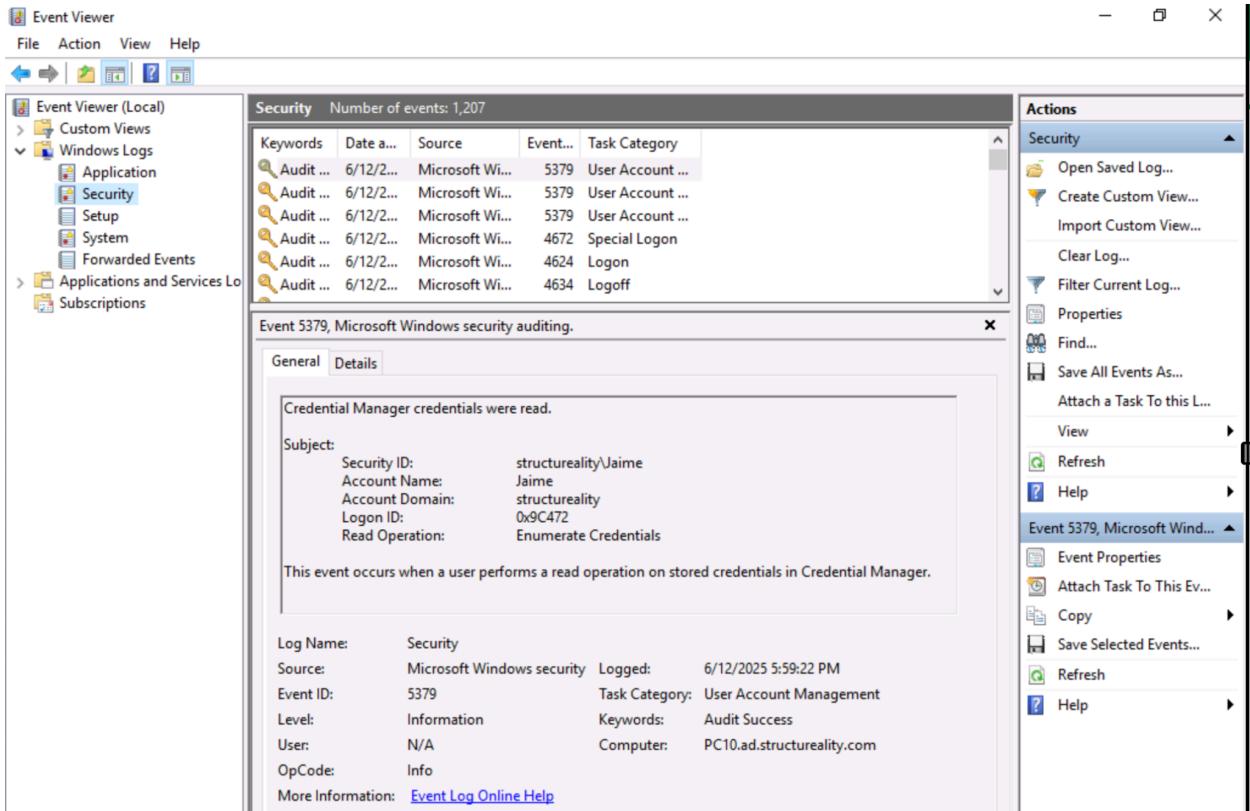
Home Share View

This PC > Local Disk (C:) > LABFILES >

	Name	Date modified	Type	Size
:k access	contains-nothing	10/22/2018 7:57 PM	File folder	
sktop	MARKETING	6/5/2023 1:48 AM	File folder	
wnloads	NVD-Control-RA-5-VULNERABILITY SCA...	6/5/2023 1:48 AM	File folder	
lcuments	pcaps	6/5/2023 1:48 AM	File folder	
BFILES	ScoutSuite	6/5/2023 1:48 AM	File folder	
TUP	winlogbeat	6/5/2023 1:48 AM	File folder	
SINTERNAL	515tech_store.sql	3/11/2021 11:13 AM	SQL File	8 KB
PC	comptia-logo	8/22/2018 7:44 AM	JPG File	53 KB
work	CONFIDENTIAL	3/28/2019 6:31 AM	Text Document	1 KB
	conn-sample	3/9/2020 7:00 AM	Text Document	155 KB
	CSIRT Incident Handling Form	2/1/2020 1:37 PM	Microsoft Word D...	16 KB
	CSIRT Incident Handling Form	2/1/2020 1:39 PM	Microsoft Edge P...	104 KB
	DisableController	3/22/2021 2:30 PM	Windows PowerS...	1 KB
	DisableDisk	3/22/2021 11:40 AM	Windows PowerS...	1 KB
	iam_shares	6/28/2022 12:58 AM	Windows PowerS...	2 KB
	laptop-full	2/21/2023 3:44 AM	Wireshark capture...	321 KB
	laptop-selected	2/21/2023 3:47 AM	Wireshark capture...	306 KB
	local.rules	3/10/2020 5:26 AM	RULES File	1 KB
	NVD-Control-RA-5-VULNERABILITY SCA...	1/21/2020 4:29 AM	Microsoft Edge H...	71 KB
	set_default_password	3/11/2021 1:32 AM	Windows PowerS...	1 KB
	Structureality-netdiag	6/28/2022 1:08 AM	OpenDocument D...	44 KB
	trusted-installs	6/29/2022 3:56 AM	OpenOffice.org 1....	1 KB

The *empty* folder should no longer be present.

18. Right-click **Start** and select **Event Viewer**. Maximize the Event Viewer window. Double-click **Windows Logs** to expand its contents. Select **Security** from in the *Windows Logs* expanded contents.



19. Select **Find...** in the right pane. Type **empty** in the *Find what:* field, then select **Find Next**. Type **empty** in the *Find what:* field, then select **Find Next**. After a few moments of searching, a window will appear stating the search term was not found. Select **OK**.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (selected), Application, Security, Setup, System, Forwarded Events, Applications and Services Log, and Subscriptions. The right pane shows the Security log with 1,207 events. A search dialog is open, showing results for 'Audit ...' and 'empty'. The details pane shows event 5379, which is a Microsoft Windows security auditing event. The event details include:

Log Name:	Source:	Event ID:	Task Category:
Security	Microsoft Windows security	5379	User Account Management
			Keywords: Audit Success
			Level: Information
			User: N/A
			Computer: PC10.ad.structureality.com
			OpCode: Info

The Actions pane on the right lists various options like Open Saved Log..., Create Custom View..., Import Custom View..., and Filter Current Log....

379, Microsoft Windows security auditing.

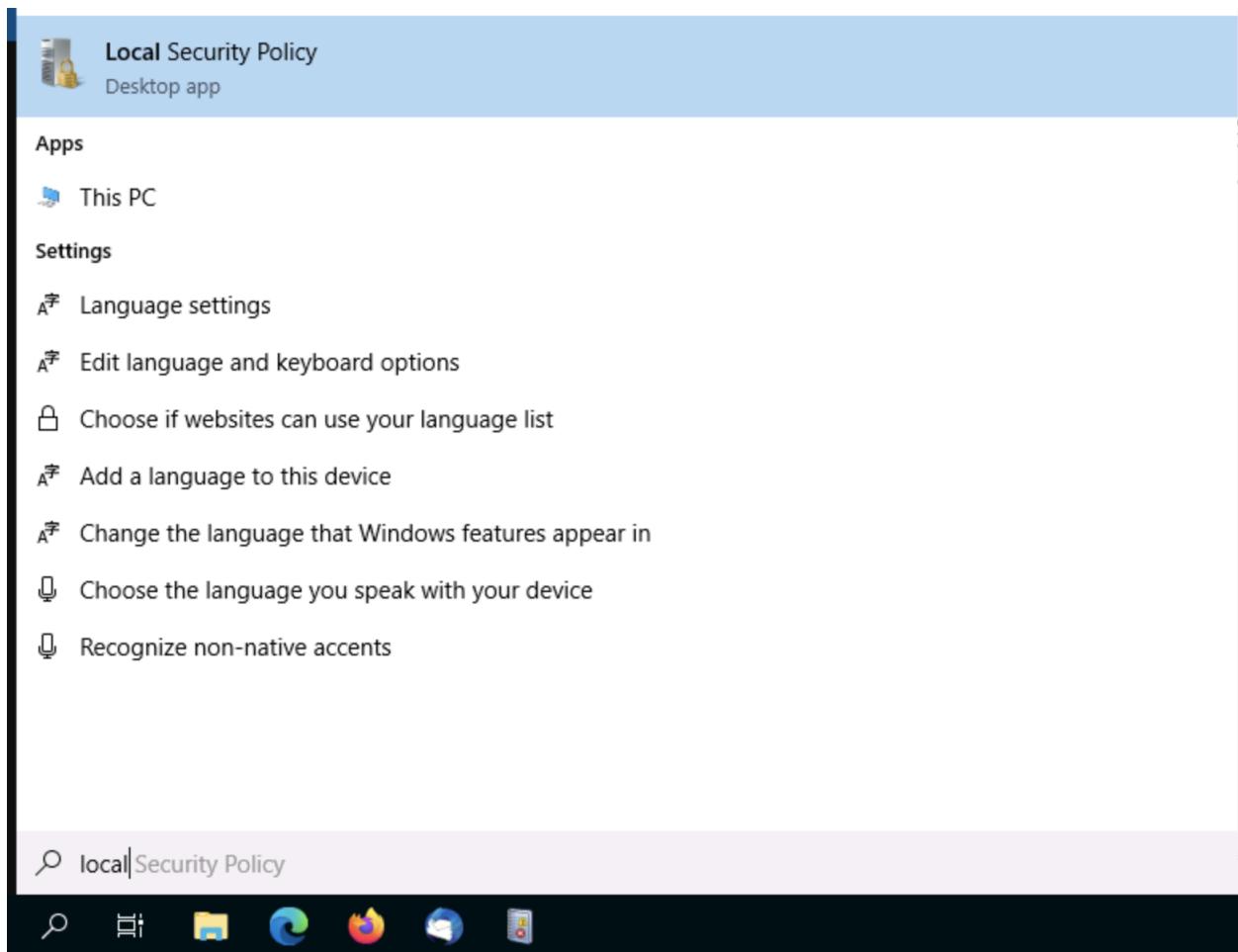
A modal dialog box titled 'Event Viewer' is displayed, containing an information icon and the message: 'Searching from the selected event to the end of the list, there is no event that contains the specified string. To search all events, select the first event in the list and run the search again.' There is an 'OK' button at the bottom right of the dialog.

The main Event Viewer window shows the Security log with one entry:

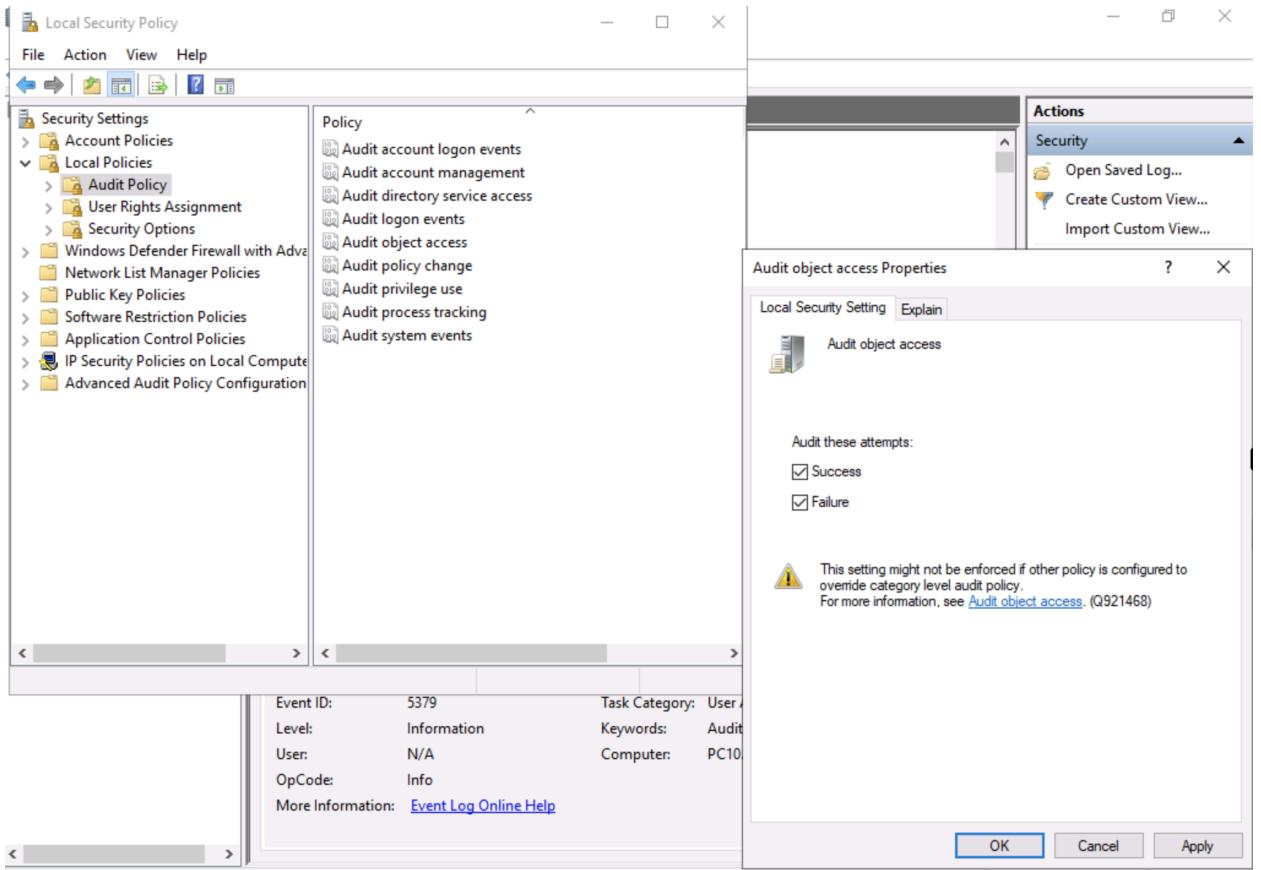
Name:	Source:	Event ID:	Task Category:
Security	Microsoft Windows security	379	User Account Management

The results of the find operation indicate what? **Folder deletion is not being audited**

20. Select **Cancel** to close the *Find* window. Select **Type here to search** from the taskbar, type **local**, then select **Local Security Policy** from the results.



21. Double-click **Local Policies** to expand its contents. Select **Audit Policy** from the *Local Policies* expanded contents. Right-click **Audit object access** in the right pane, then select **Properties**. Select to mark both the **Success** and **Failure** checkboxes, then select **OK**.

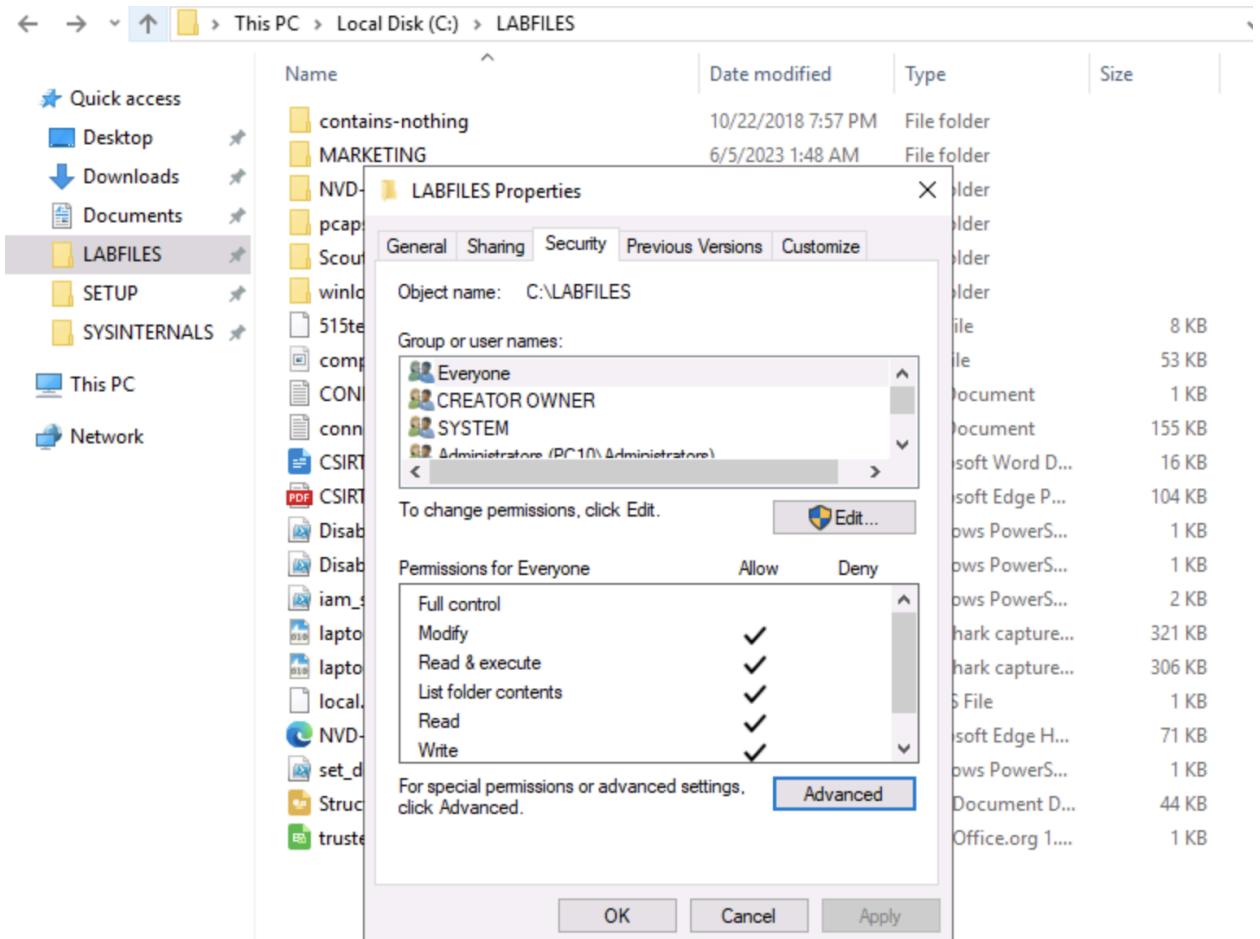


While the main switch for auditing object access activities is now on, auditing will not occur on most file objects until an on-object auditing setting is made.

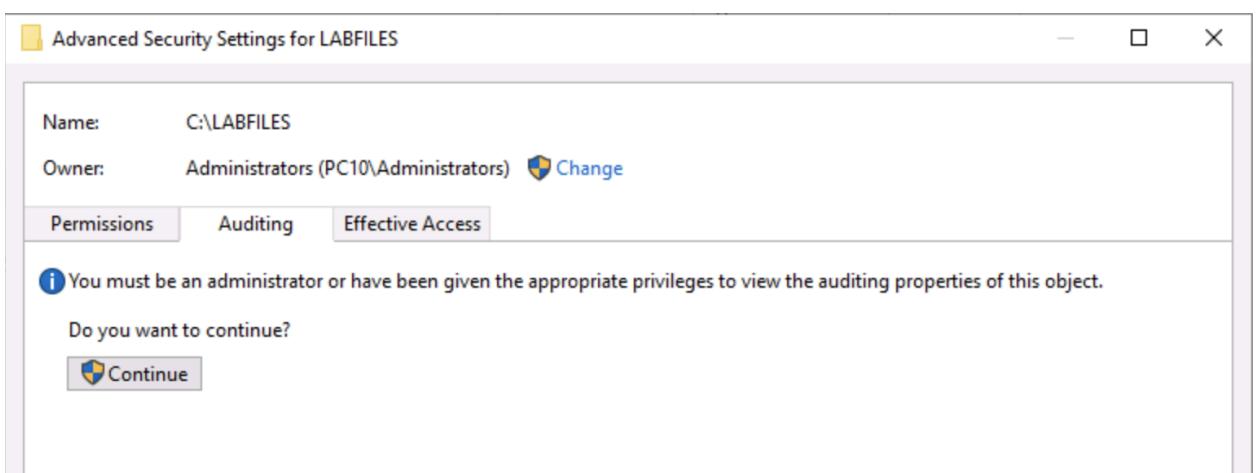
22. Close the *Local Security Policy* window.

The setting change should apply immediately. If the next steps do not result in a record of a folder deletion in the Security log accessed through the Event Viewer, restart PC10 and repeat from here, but we will then need to delete the **MKT** folder.

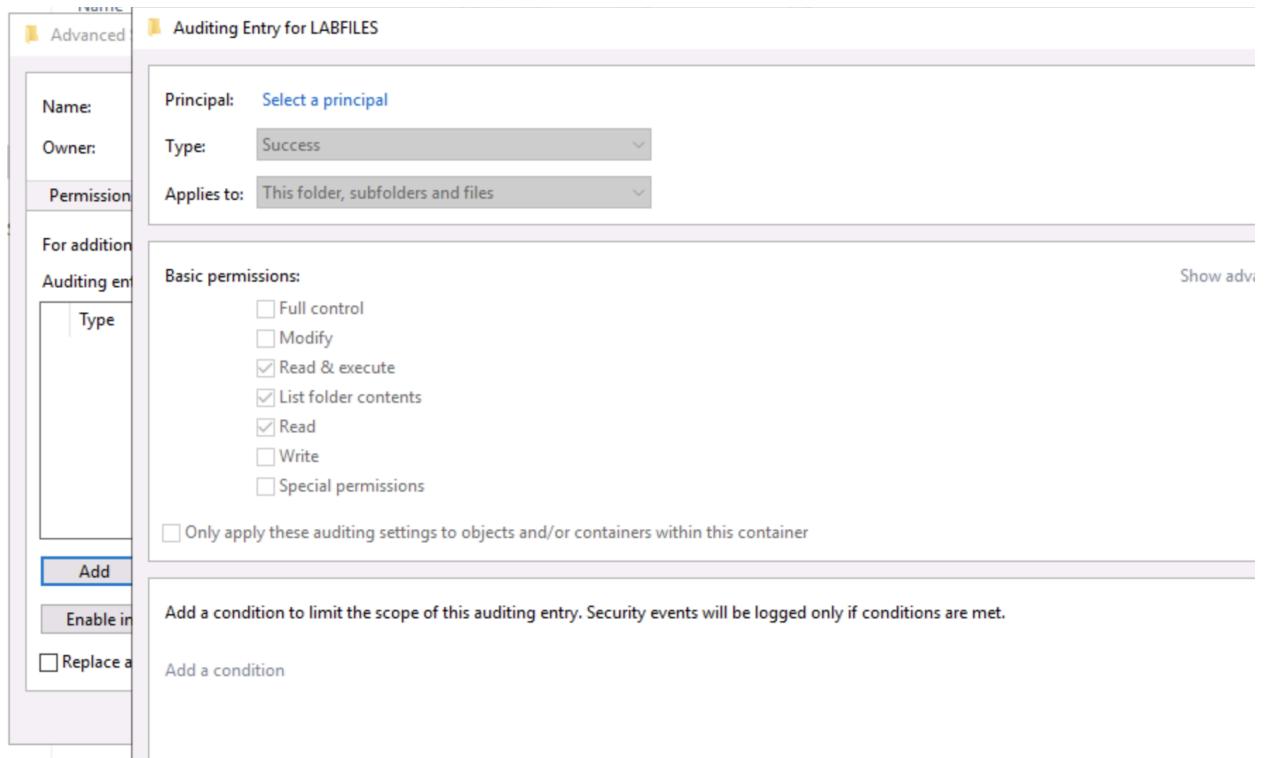
22. Return to File Explorer. Right-click **LABFILES** in the left pane, then select **Properties**. Select the **Security** tab on the *LABFILES Properties* window.

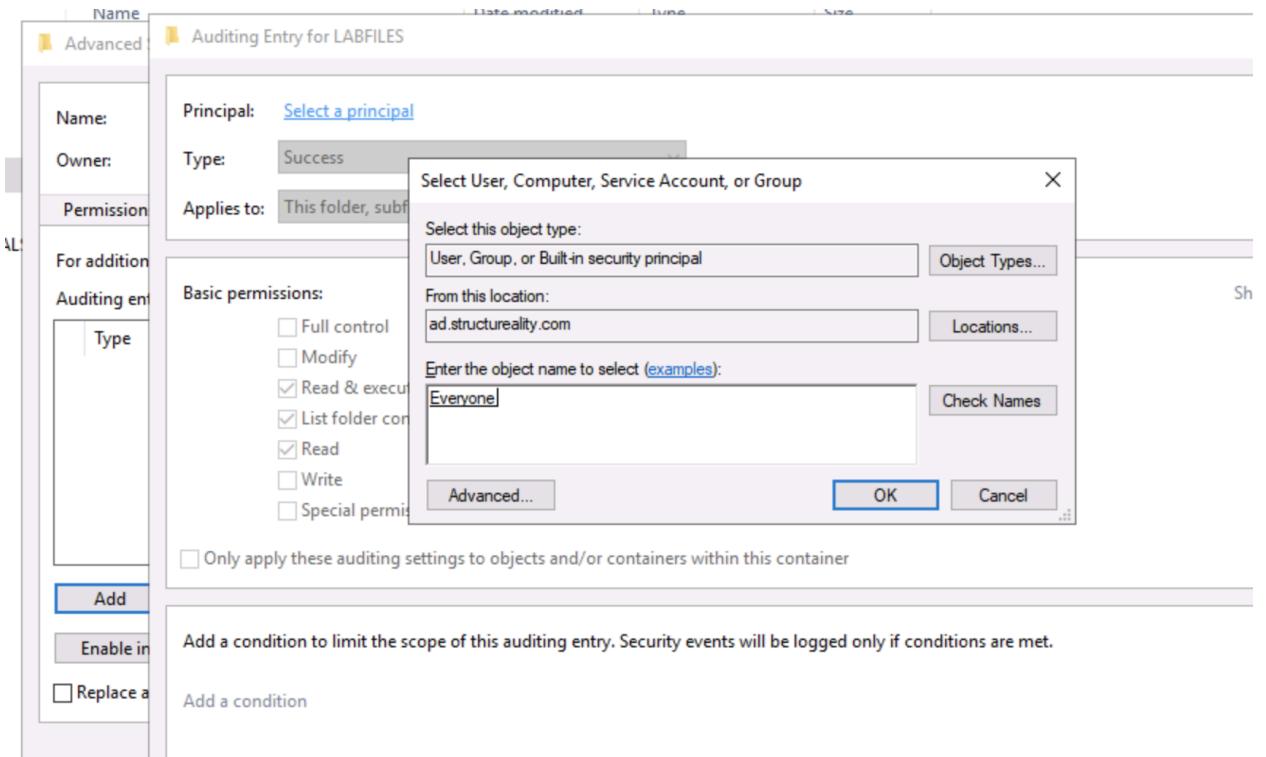


23. Select **Advanced**. Select the **Auditing** tab on the *Advanced Security Settings for LABFILES* window. Select **Continue** since we are an administrator.



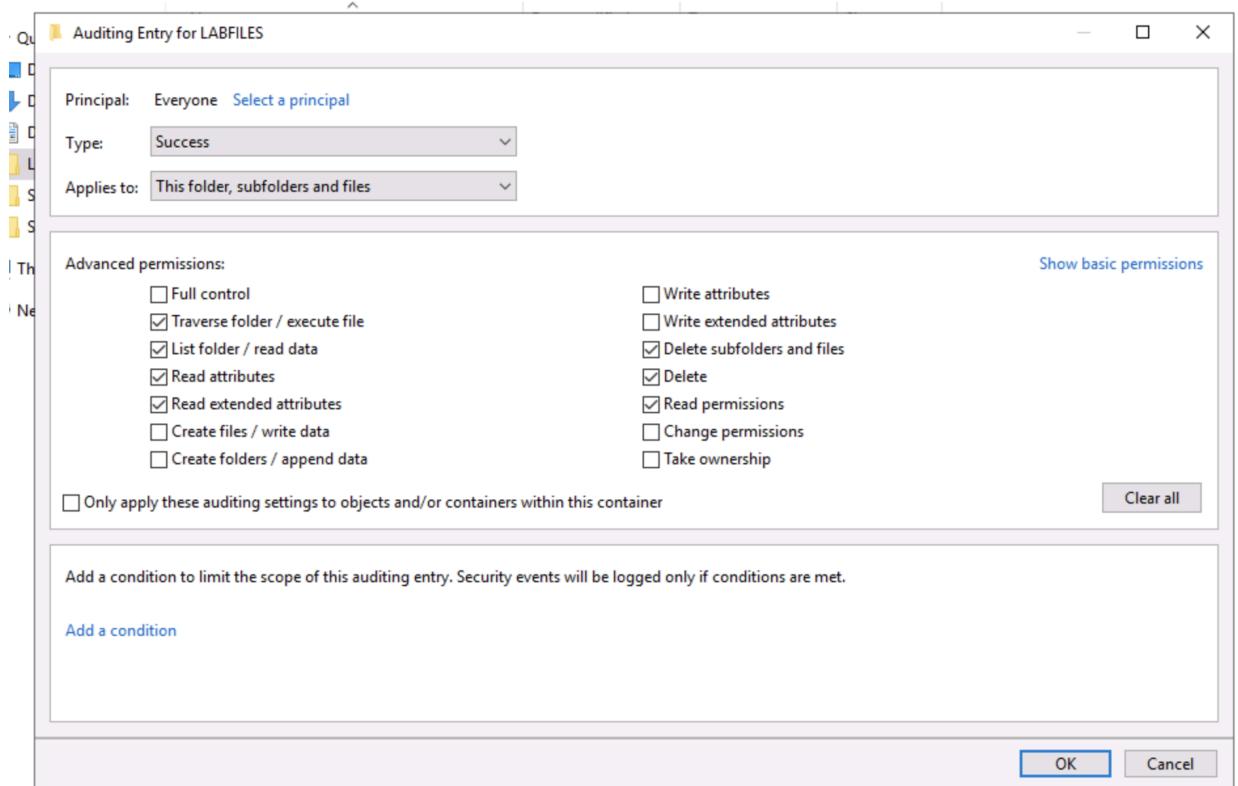
24. Select **Add**. Select **Select a principle** on the *Auditing Entry for LABFILES* window. Type **everyone** in the *Enter the object name to select* field, then select **Check Names**.





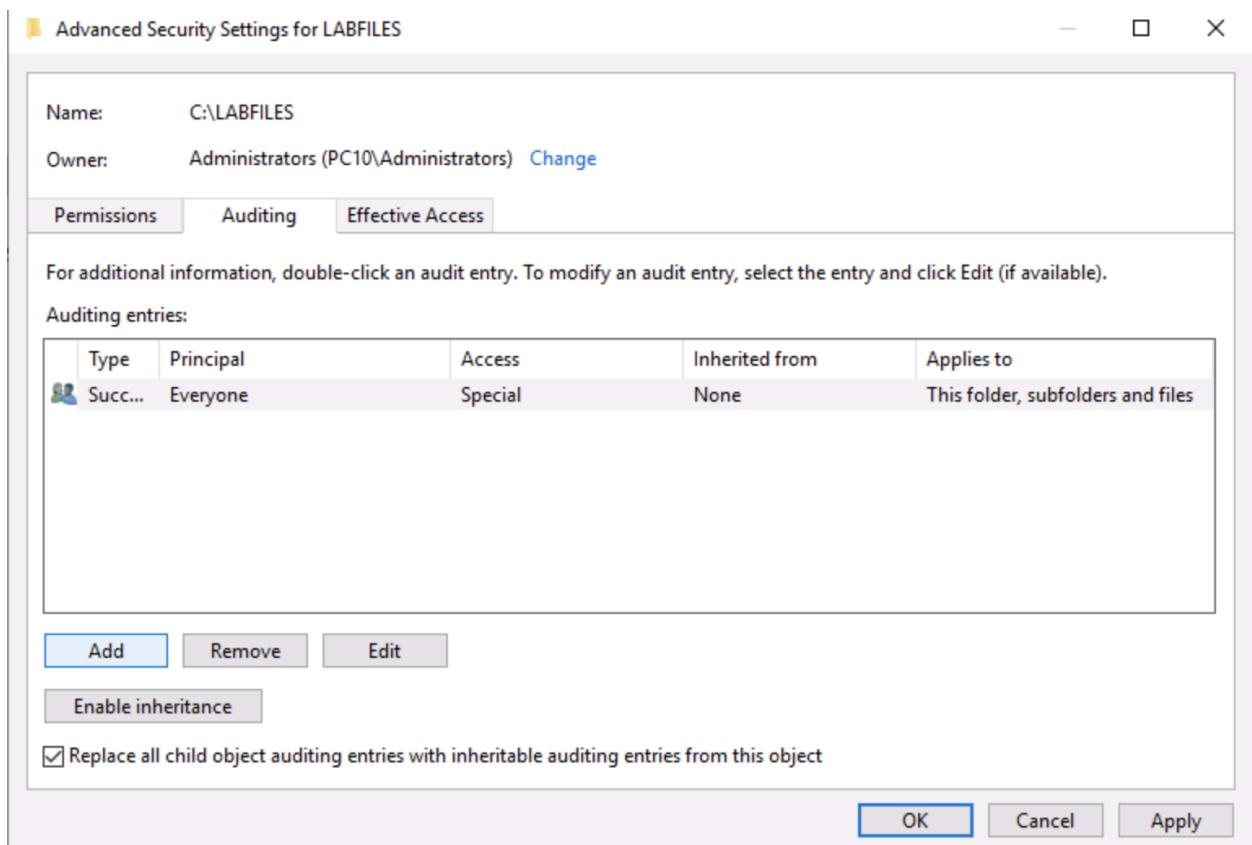
The field should now display Everyone..

25. Select **OK**. Select **Show advanced permissions** from the middle area of the *Auditing Entry for LABFILES* window. Select to mark the **Delete subfolders and files** and **Delete** checkboxes.

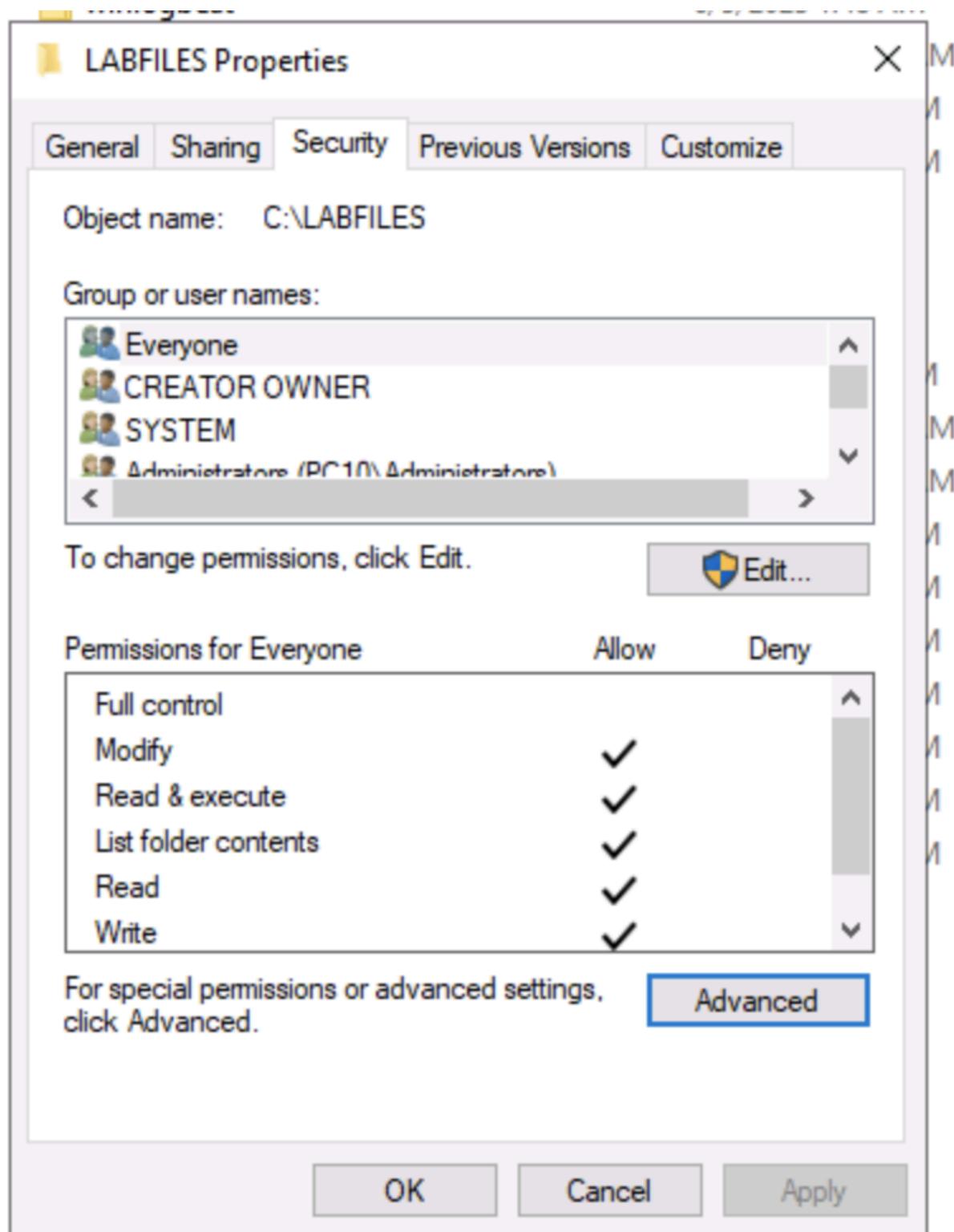


26. Select **OK** to save the settings and close the *Auditing Entry for LABFILES* window. Select **OK** to save the settings and close the *Advanced Security Settings*

for *LABFILES* window.



27. Select **OK** to save the settings and close the *LABFILES Properties* window.



28. Return to File Explorer. Right-click the **pcaps** folder, then select **Delete**.

This PC > Local Disk (C:) > LABFILES				
	Name	Date modified	Type	Size
Quick access	contains-nothing	10/22/2018 7:57 PM	File folder	
Desktop	MARKETING	6/5/2023 1:48 AM	File folder	
Downloads	NVD-Control-RA-5-VULNERABILITY SCA...	6/5/2023 1:48 AM	File folder	
Documents	pcaps	6/5/2023 1:48 AM	File folder	
LABFILES	<ul style="list-style-type: none">OpenOpen in new windowPin to Quick accessGive access toRestore previous versionsInclude in libraryPin to StartSend toCutCopyCreate shortcutDeleteRenameProperties	023 1:48 AM 023 1:48 AM 021 11:13 AM 018 7:44 AM 019 6:31 AM 020 7:00 AM 020 1:37 PM 020 1:39 PM 021 2:30 PM 021 11:40 AM 022 12:58 AM 023 3:44 AM 023 3:47 AM 020 5:26 AM 020 4:29 AM 021 1:32 AM 022 1:08 AM	File folder File folder SQL File JPG File Text Document Text Document Microsoft Word D... Microsoft Edge P... Windows PowerS... Windows PowerS... Windows PowerS... Wireshark capture... Wireshark capture... RULES File Microsoft Edge H... Windows PowerS... OpenDocument D... OpenOffice.org 1....	8 KB 53 KB 1 KB 155 KB 16 KB 104 KB 1 KB 1 KB 2 KB 321 KB 306 KB 1 KB 71 KB 1 KB 44 KB 1 KB
Scou				
winlo				
515te				
com				
CON				
conn				
CSIR				
PDF CSIR				
Disab				
Disab				
iam_				
laptop				
laptop				
local				
NVD				
set_d				
Struct				
trusted-installs				

This PC > Local Disk (C:) > LABFILES >				
	Name	Date modified	Type	Size
	contains-nothing	10/22/2018 7:57 PM	File folder	
	MARKETING	6/5/2023 1:48 AM	File folder	
	NVD-Control-RA-5-VULNERABILITY SCA...	6/5/2023 1:48 AM	File folder	
	ScoutSuite	6/5/2023 1:48 AM	File folder	
	winlogbeat	6/5/2023 1:48 AM	File folder	
	515tech_store.sql	3/11/2021 11:13 AM	SQL File	8 KB
	comptia-logo	8/22/2018 7:44 AM	JPG File	53 KB
	CONFIDENTIAL	3/28/2019 6:31 AM	Text Document	1 KB
	conn-sample	3/9/2020 7:00 AM	Text Document	155 KB
	CSIRT Incident Handling Form	2/1/2020 1:37 PM	Microsoft Word D...	16 KB
	CSIRT Incident Handling Form	2/1/2020 1:39 PM	Microsoft Edge P...	104 KB
	DisableController	3/22/2021 2:30 PM	Windows PowerS...	1 KB
	DisableDisk	3/22/2021 11:40 AM	Windows PowerS...	1 KB
	iam_shares	6/28/2022 12:58 AM	Windows PowerS...	2 KB
	laptop-full	2/21/2023 3:44 AM	Wireshark capture...	321 KB
	laptop-selected	2/21/2023 3:47 AM	Wireshark capture...	306 KB
	local.rules	3/10/2020 5:26 AM	RULES File	1 KB
	NVD-Control-RA-5-VULNERABILITY SCA...	1/21/2020 4:29 AM	Microsoft Edge H...	71 KB
	set_default_password	3/11/2021 1:32 AM	Windows PowerS...	1 KB
	Structureality-netdiag	6/28/2022 1:08 AM	OpenDocument D...	44 KB
	trusted-installs	6/29/2022 3:56 AM	OpenOffice.org 1....	1 KB

The *pcaps* folder should no longer be present.

29. Minimize File Explorer. Return to the Event Viewer. Select **Refresh** from the right pane.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Custom Views, Windows Logs (selected), Application, Security (selected), Setup, System, Forwarded Events, Applications and Services Log, and Subscriptions. The middle pane shows the Security log with 2,260 events available. A specific event, Event 4662, is selected. The right pane contains an 'Actions' menu with various options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., View, Refresh, Help, and a detailed view of the selected event.

30. Select the first entry at the top of the middle pane.

This screenshot is identical to the one above, showing the Event Viewer interface with the Security log selected. The first entry in the list is highlighted, indicating it has been selected as per the previous step's instruction.

This sets the search-from point for the Find function, which only searches from the currently selected entry to earlier entries (i.e., down).

31. Select **Find...** in the right pane. Type **4660** in the *Find what:* field, then select **Find Next**. Select **Cancel** to close the *Find* window.

The screenshot shows the Windows Event Viewer interface. The main pane displays a list of audit events from Microsoft Windows security auditing. One event is selected, showing its details. A 'Find' dialog box is overlaid on the bottom pane, containing a 'Find what:' input field with the value '4660', a 'Find Next' button, and a 'Cancel' button. The right pane contains a sidebar titled 'Actions' with various options like 'Open Saved Log...', 'Create Custom View...', and 'Event Properties'.

Keywords	Date a...	Source	Event...	Task Category
Audit ...	6/12/2...	Microsoft Wi...	4660	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4656	File System
Audit ...	6/12/2...	Microsoft Wi...	4658	File System
Audit ...	6/12/2...	Microsoft Wi...	4690	Handle Manip...

Event 4660, Microsoft Windows security auditing.

General Details

An object was deleted.

Subject: Security Logon ID: 0x1A2CDE

Object: Object Server: Security

Find

Find what: 4660

Find Next Cancel

Actions

- Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help
- Event 4660, Microsoft Wind...
- Event Properties

4660 is the Event ID for the event type of object deletion.

32. An audit record of Event ID: 4660 should be selected. In the bottom pane, we should see the statement "An object was deleted".

Security Number of events: 2,260 (!) New events available

Keywords	Date a...	Source	Event...	Task Category
Audit ...	6/12/2...	Microsoft Wi...	4660	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4656	File System
Audit ...	6/12/2...	Microsoft Wi...	4658	File System
Audit ...	6/12/2...	Microsoft Wi...	4690	Handle Manip...

Event 4660, Microsoft Windows security auditing.

[General](#) [Details](#)**An object was deleted.****Subject:**

Security ID: structureality\Jaime
Account Name: Jaime
Account Domain: structureality
Logon ID: 0x1A2CDE

Object:

Object Server: Security
Handle ID: 0x618

Log Name: Security**Source:** Microsoft Windows security **Logged:** 6/12/2025 6:53:50 PM**Event ID:** 4660 **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](#)

 Event Properties - Event 4660, Microsoft Windows security auditing.

General Details

An object was deleted.

Subject:

Security ID:	structureality\Jaime
Account Name:	Jaime
Account Domain:	structureality
Logon ID:	0x3D3A9

Log Name: Security
Source: Microsoft Windows security
Event ID: 4660
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Clos**

Oddly, while Event ID 4660 is the record of an object being deleted, it does not contain the actual object's name. For that, we need to find the associated Event ID 4663.

33. The Event ID 4663 for the folder deletion should be about five records above the currently selected one. Select the lowest record of **Event ID 4663** above the currently selected Event ID 4660 record.

Security Number of events: 2,260 (!) New events available

Keywords	Date a...	Source	Event...	Task Category
Audit ...	6/12/2...	Microsoft Wi...	4660	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4656	File System
Audit ...	6/12/2...	Microsoft Wi...	4658	File System
Audit ...	6/12/2...	Microsoft Wi...	4690	Handle Manip...

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:	0x1A2CDE

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\LABFILES\pcaps\cap2.pcap

Log Name: Security
Source: Microsoft Windows security **Logged:** 6/12/2025 6:53:50 PM
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](#)

34. Once we have selected the Event ID 4663 record, we can view the details in the bottom pane. The *General* tab has a small scrollable sub-window with details. we should see a line of "Object Name: C\LABFILES\pcaps". This Event ID 4663 record confirms that the object deleted was the C\LABFILES\pcaps folder.

Security Number of events: 2,260 (!) New events available

Keywords	Date a...	Source	Event...	Task Category
Audit ...	6/12/2...	Microsoft Wi...	4660	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4663	File System
Audit ...	6/12/2...	Microsoft Wi...	4656	File System
Audit ...	6/12/2...	Microsoft Wi...	4658	File System
Audit ...	6/12/2...	Microsoft Wi...	4690	Handle Manip...

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:	0x1A2CDE

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\LABFILES\pcaps\cap2.pcap

Log Name: Security
Source: Microsoft Windows security **Logged:** 6/12/2025 6:53:50 PM
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](#)

Event Properties - Event 4663, Microsoft Windows security auditing.

General Details

Object Type: File
Object Name: C:\LABFILES\pcaps
Handle ID: 0x11cc
Resource Attributes: S:AI

Process Information:
Process ID: 0x179c

Log Name: Security
Source: Microsoft Windows security Logged: 7/15/2025 10:45:10 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

Event 4663, Microsoft Windows security auditing.

General Details

Friendly View XML View

- **EventData**

SubjectUserId	S-1-5-21-755481304-3118383057-1750507880-1106
SubjectUserName	Jaime
SubjectDomainName	structureality
SubjectLogonId	0x1a2cde
ObjectServer	Security
ObjectType	File
ObjectName	C:\LABFILES\pcaps\cap2.pcap
HandleId	0x618
AccessList	%%1537
AccessMask	0x10000
ProcessId	0x167c
ProcessName	C:\Windows\explorer.exe

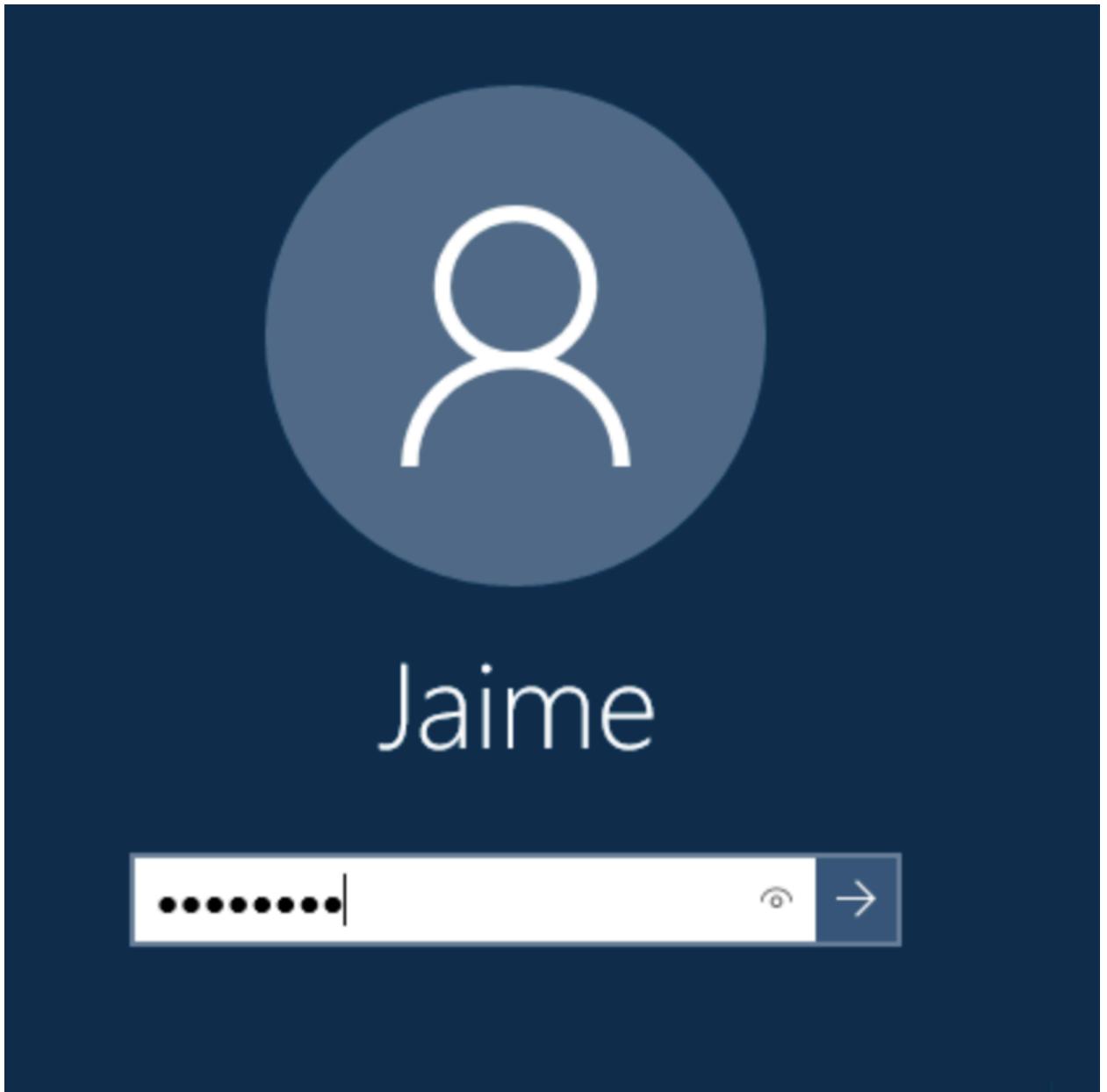
we could also select the *Details* pane to see most of the same information.

What is the purpose of a detective control? Create a record of events and activities

Configure and test directive controls

A directive control provides instruction to direct a user towards more compliant behavior. In this exercise, we will configure a directive control in the form of a login warning banner. Finally, we will test this directive control.

35. sign in as **Jaime** using **Pa\$\$w0rd** as the password.



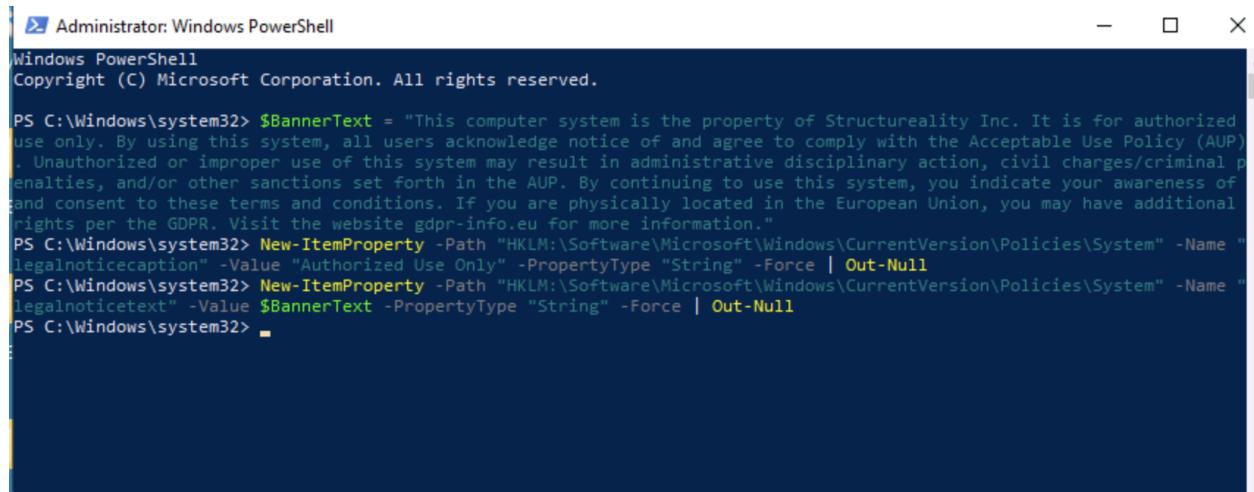
Jaime is a member of the LocalAdmin group. So, this user account is an administrator on the PC10 system.

36. Right-click **Start**, and select **Windows PowerShell (Admin)**. At the UAC prompt, select **Yes**. Enter the following code into the *Administrator: Windows PowerShell* console:

```
$BannerText = "This computer system is the property of Structureality Inc. It is for authorized use only. By using this system, all users acknowledge notice of and agree to comply with the Acceptable Use Policy (AUP). Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions set forth in the AUP. By continuing to use this system, we indicate our awareness of and consent to these terms and conditions. If we are physically located in the European Union, we may have additional rights per the GDPR. Visit the website gdpr-info.eu for more information." ENTER
```

```
New-ItemProperty -Path  
"HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"legalnoticecaption" -Value "Authorized Use Only" -PropertyType "String" -Force |  
Out-Null then hit ENTER
```

```
New-ItemProperty -Path  
"HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name  
"legalnoticetext" -Value $BannerText -PropertyType "String" -Force | Out-Null  
Then Hit ENTER
```



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The window displays the following command history:

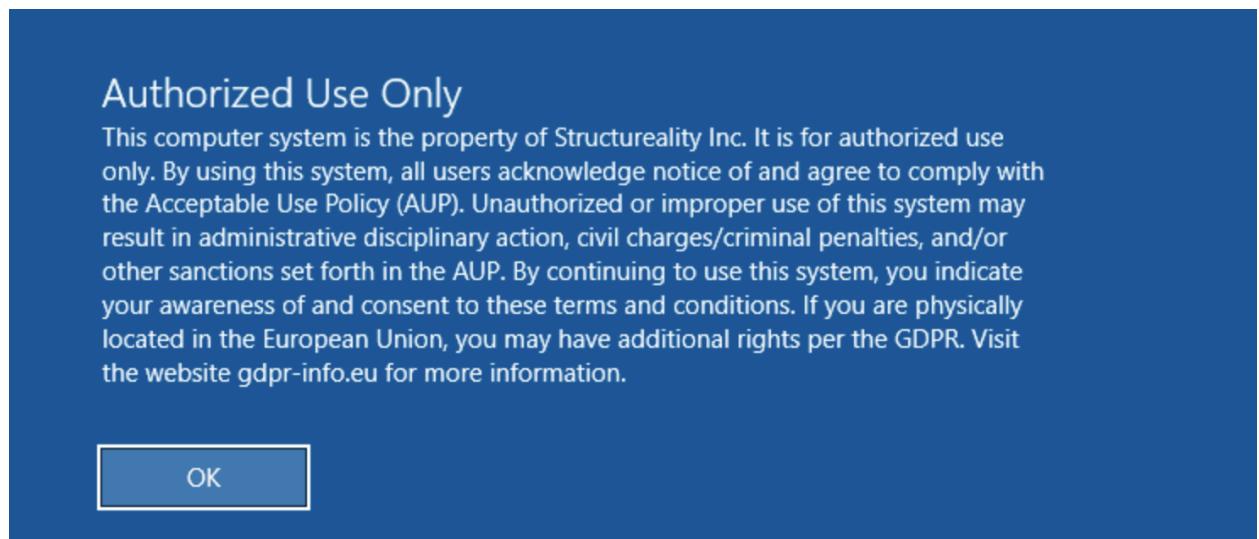
```
PS C:\Windows\system32> $BannerText = "This computer system is the property of Structureality Inc. It is for authorized use only. By using this system, all users acknowledge notice of and agree to comply with the Acceptable Use Policy (AUP). Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions set forth in the AUP. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions. If you are physically located in the European Union, you may have additional rights per the GDPR. Visit the website gdpr-info.eu for more information."  
PS C:\Windows\system32> New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticecaption" -Value "Authorized Use Only" -PropertyType "String" -Force | Out-Null  
PS C:\Windows\system32> New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "legalnoticetext" -Value $BannerText -PropertyType "String" -Force | Out-Null  
PS C:\Windows\system32>
```

The text of the warning banner in this exercise amalgamates several banners used by various commercial and educational facilities. Be sure to consult with

wer own legal counsel before setting a warning banner to ensure it complies with laws and regulations.

37. Sign out of PC10 by selecting the **Start** menu, then selecting **Jaime** (which will be a circle at the top of the menu), then select **Sign out**. If prompted that there are open programs, select **Sign out anyway**.

38. Connect to the **PC10** virtual machine, send **Ctrl+Alt+Delete**. we should be presented with the login warning banner that was just defined.



39. Read the warning banner, then select **OK**. sign-in process as **Jaime** using **Pa\$\$w0rd** as the password.

we have successfully implemented a directive control to inform personnel of the limitations and restrictions of a controlled system.

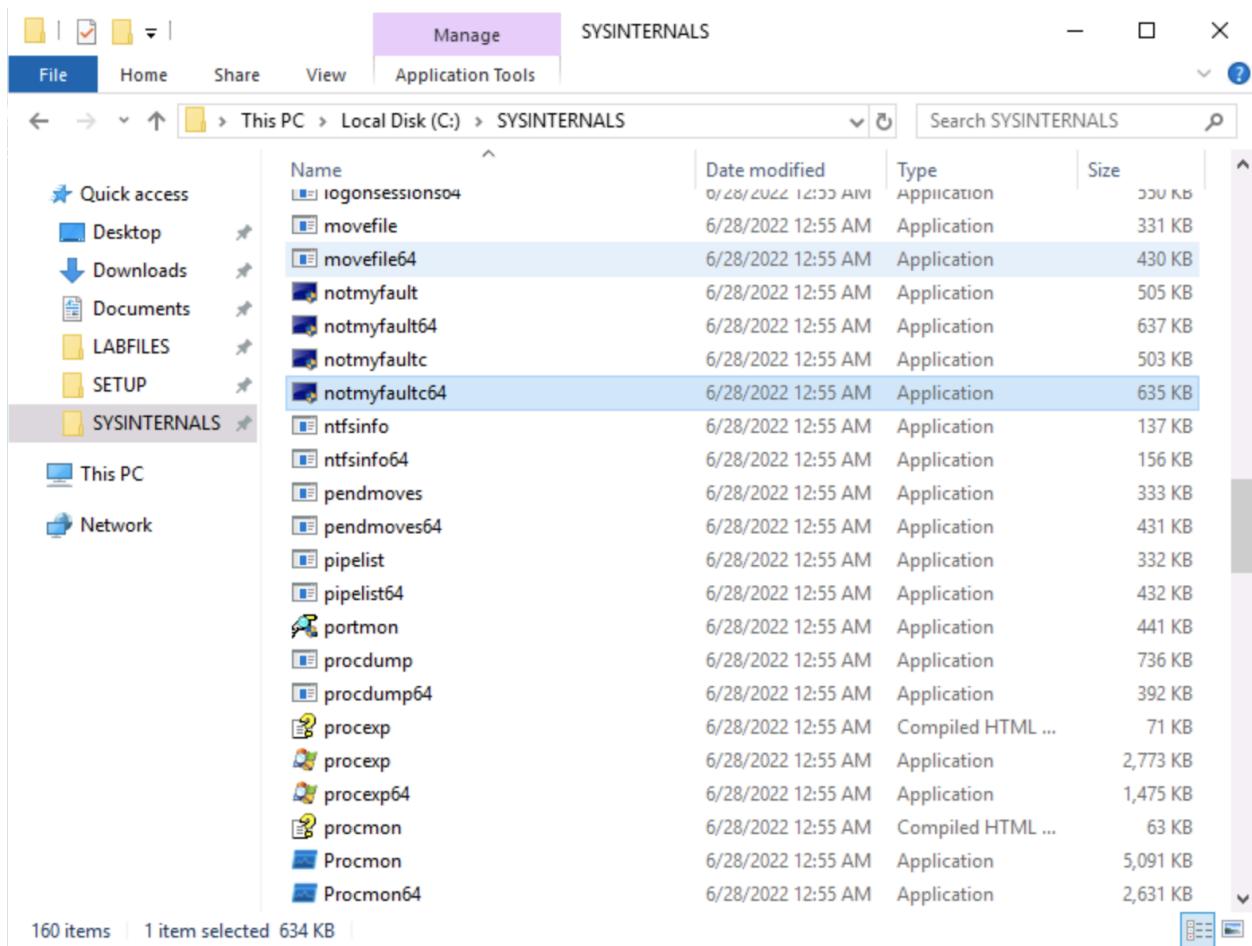
What is the goal of directive controls? Compliance

Configure and test corrective controls

A corrective control is intended to detect when something is in a less secure or less desirable state, then attempts to return to the more secure or more desirable state. In some cases, the corrective control can repair minor damage to restore a system to a more secure or desirable state.

In this exercise, we will first use a fault injection tool to trigger the existing correct control of Windows to trigger its native corrective control protection against misbehaving applications. Next, we will create and test a custom corrective control to protect the contents of a text file.

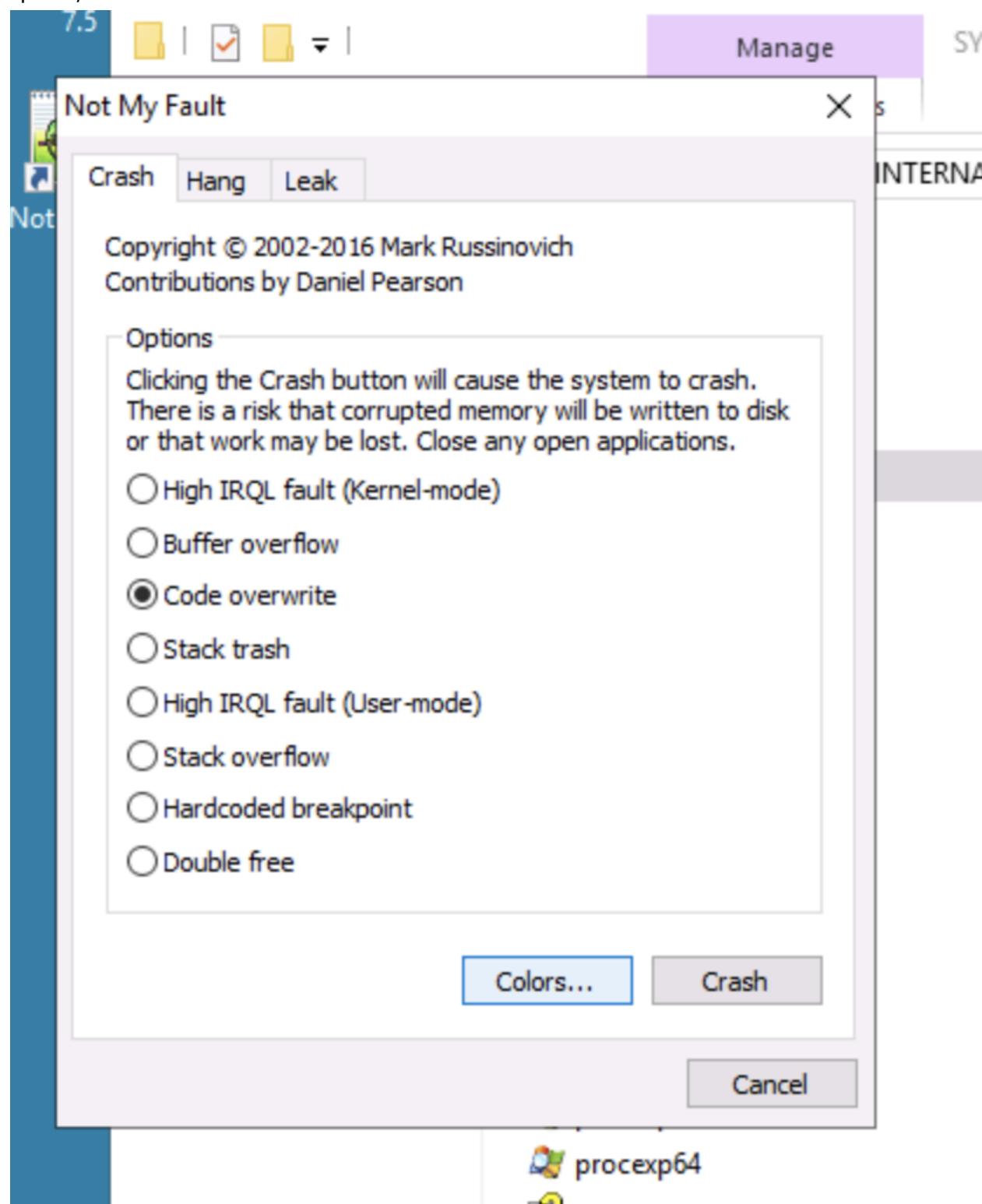
40. sign-in process as **Jaime** using **Pa\$\$w0rd** as the password. Open File Explorer, and from the Quick access pane, select **SYSINTERNALS**. Scroll to locate, then double-click **notmyfault64** to execute it.



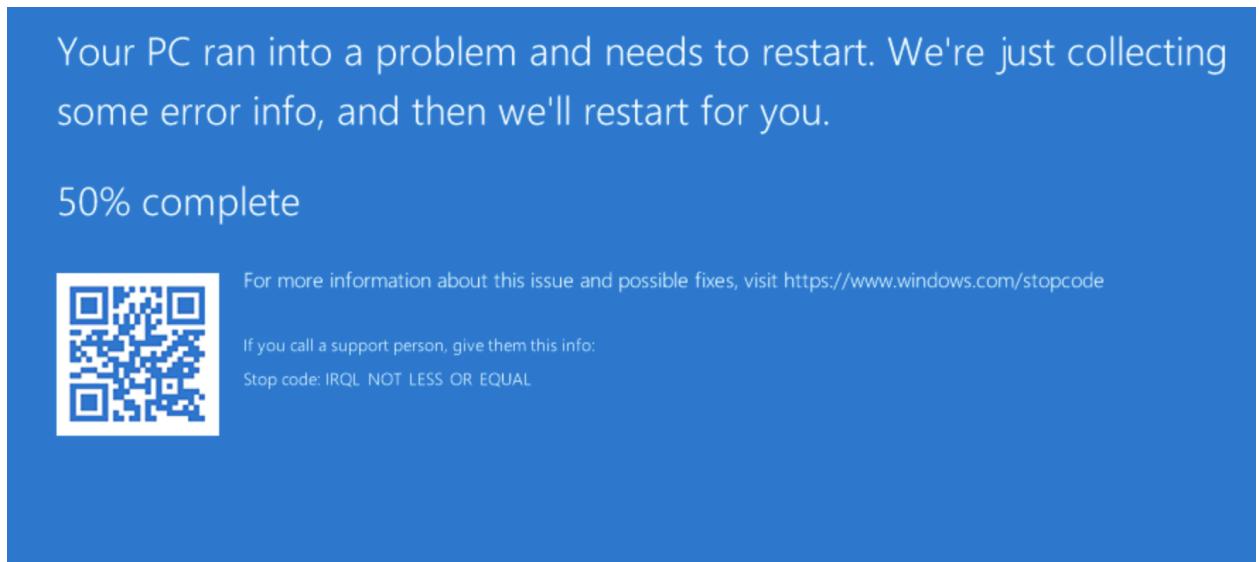
There is a CLI (command line interface) version of NotMyFault, which has a command in the file name: notmyfaultc64. If a Command Prompt window flashes open and disappears, we selected the CLI version, not the GUI version of NotMyFault64.

Windows Sysinternals is a website that offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment. We can experiment with the Sysinternals tools in this lab environment or go directly to sysinternals.com to learn more and download nearly 75 tools onto our system.

41. Select **Yes** on the User Account Control window. Select the **Code overwrite** option, then select **Crash**.



42. The PC10 system should immediately experience a stop error (often called the BSOD (Blue Screen of Death)). The system will perform a partial memory dump (for potential analysis - which will not be done in this lab) and then reboot.



we have verified that the Windows corrective control to protect the execution environment from misbehaving applications is active. While we might not prefer in-memory data to be lost, the stability of the Windows execution environment is protected by immediately ceasing all execution. we can be assured that the offending application will not be running once the system reboots. This native Windows protective feature is why we should save early and often when creating new content or media.

What are the dual purposes of corrective controls?

Return the system to a normal and generally secure condition

Address an unwanted or less secure state or event

43. Next, we will create our own corrective control to simulate the correction functions of the SigVerif utility.

44. Select **Type here to search** from the taskbar, type **powershell**, then select **Windows PowerShell** from the results. Enter "**This is important**" | **Set-Content notes.txt**.

In this exercise portion, we will create a corrective control to monitor the contents of a file. If the file contents change, the control will restore the file back to its preferred content.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\jaime> "This is important" | Set-Content notes.txt
PS C:\Users\jaime>
```

45. Enter type notes.txt.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\jaime> "This is important" | Set-Content notes.txt
PS C:\Users\jaime> type notes.txt
This is important
PS C:\Users\jaime>
```

46. Enter Get-FileHash ./notes.txt -Algorithm SHA256 | Select-Object -ExpandProperty Hash | Set-Content ./hash.txt.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\jaime> "This is important" | Set-Content notes.txt
PS C:\Users\jaime> type notes.txt
This is important
PS C:\Users\jaime> Get-FileHash ./notes.txt -Algorithm SHA256 | Select-Object -ExpandProperty Hash | Set-Content ./hash.txt
PS C:\Users\jaime> .
```

47. Enter type hash.txt. (This command displays the contents of the hash.txt file, which is the hash calculated from the notes.txt file.) Enter echo blah >> notes.txt. (This command injects new content into notes.txt, which changes the file.) Enter type notes.txt. (we should see different contents of the notes.txt file.) Enter if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt)) {Write-Host "The file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}. (This command calculates the hash of notes.txt and compares it to the

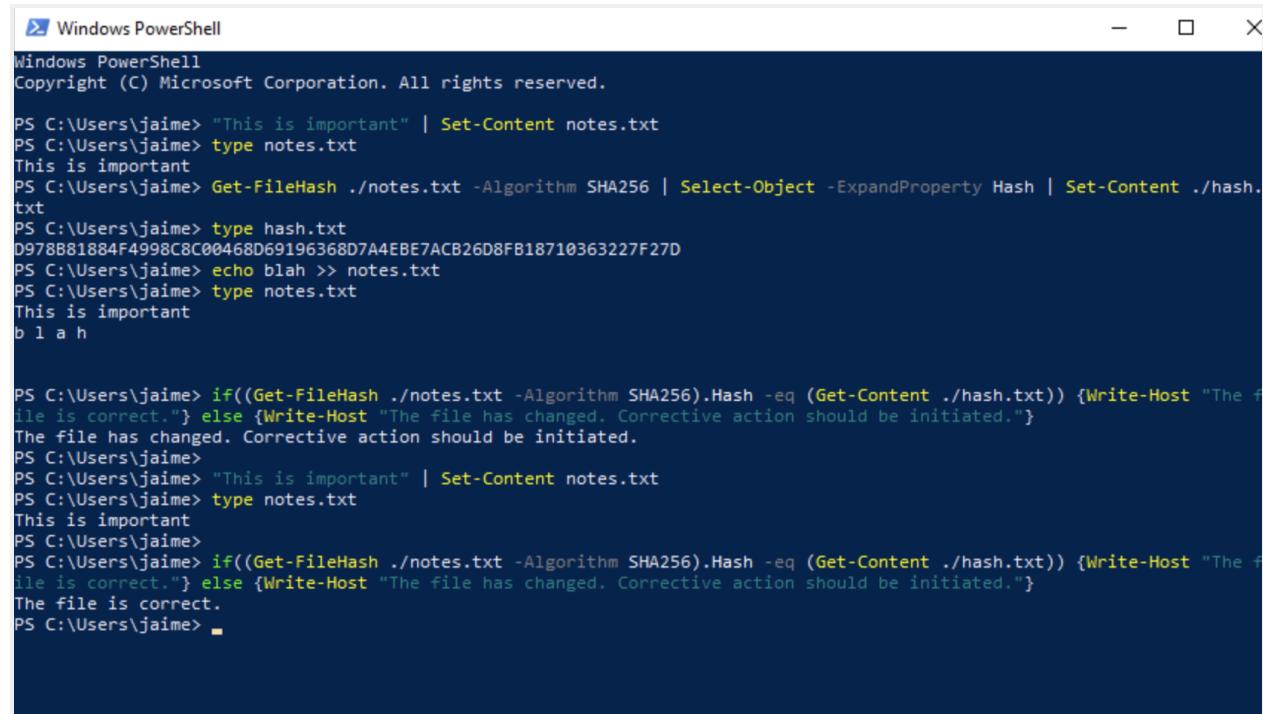
value stored in hash.txt. Since the file has changed, an error message is displayed.)

```
txt
PS C:\Users\jaime> type hash.txt
D978881884F4998C8C00468D69196368D7A4EBE7ACB26D8FB18710363227F27D
PS C:\Users\jaime> echo blah >> notes.txt
PS C:\Users\jaime> type notes.txt
This is important
b l a h

PS C:\Users\jaime> if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt)) {Write-Host "The file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}
The file has changed. Corrective action should be initiated.
PS C:\Users\jaime>
PS C:\Users\jaime> ■
```

48. Enter "This is important" | Set-Content notes.txt. (This command is the corrective action to reset the contents of notes.txt back to the desired content.) Enter

```
if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt))
{Write-Host "The file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}.(This command calculates the hash of notes.txt and compares it to the value stored in hash.txt. Since the file has been restored, a confirmation message is displayed. we have performed the corrective control manually. Now configure scripts to automate the process)
```



The screenshot shows a Windows PowerShell window titled "Windows PowerShell". The command history is as follows:

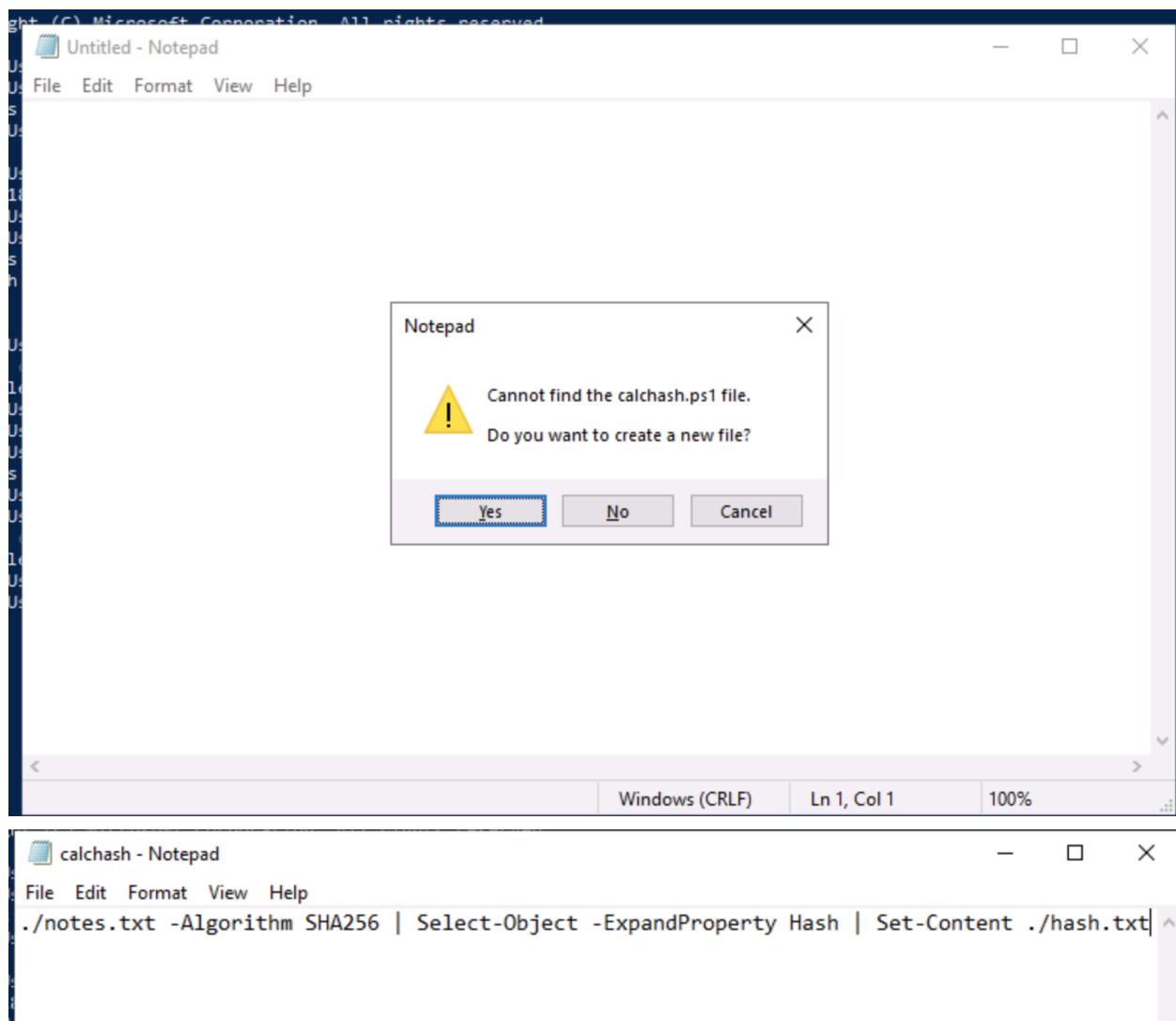
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

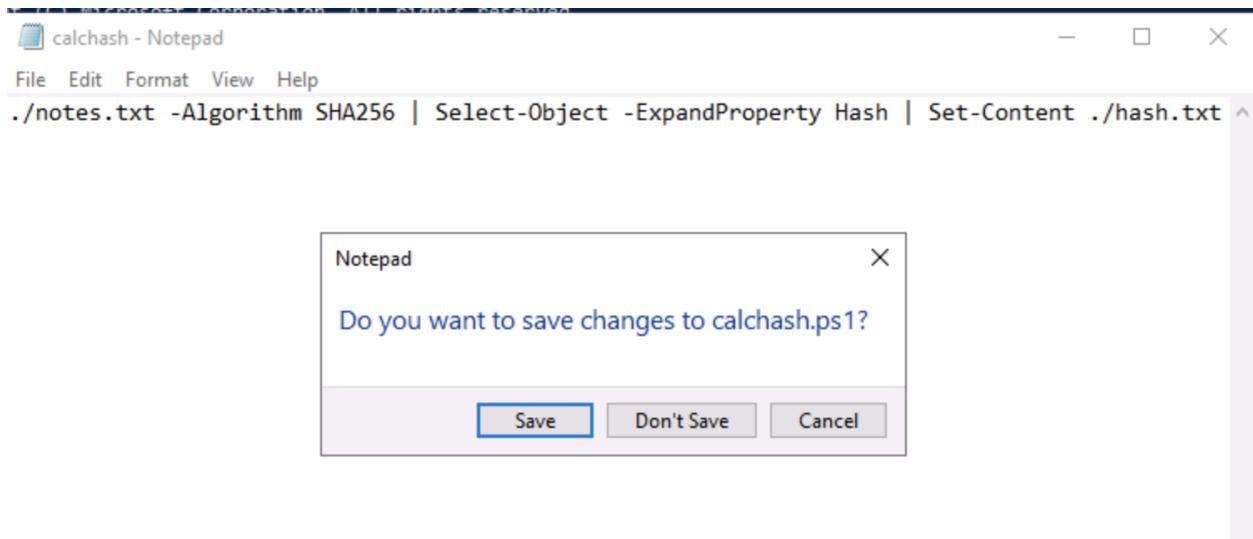
PS C:\Users\jaime> "This is important" | Set-Content notes.txt
PS C:\Users\jaime> type notes.txt
This is important
PS C:\Users\jaime> Get-FileHash ./notes.txt -Algorithm SHA256 | Select-Object -ExpandProperty Hash | Set-Content ./hash.txt
PS C:\Users\jaime> type hash.txt
D978881884F4998C8C00468D69196368D7A4EBE7ACB26D8FB18710363227F27D
PS C:\Users\jaime> echo blah >> notes.txt
PS C:\Users\jaime> type notes.txt
This is important
b l a h

PS C:\Users\jaime> if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt)) {Write-Host "The file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}
The file has changed. Corrective action should be initiated.
PS C:\Users\jaime>
PS C:\Users\jaime> "This is important" | Set-Content notes.txt
PS C:\Users\jaime> type notes.txt
This is important
PS C:\Users\jaime>
PS C:\Users\jaime> if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt)) {Write-Host "The file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}
The file is correct.
PS C:\Users\jaime> ■
```

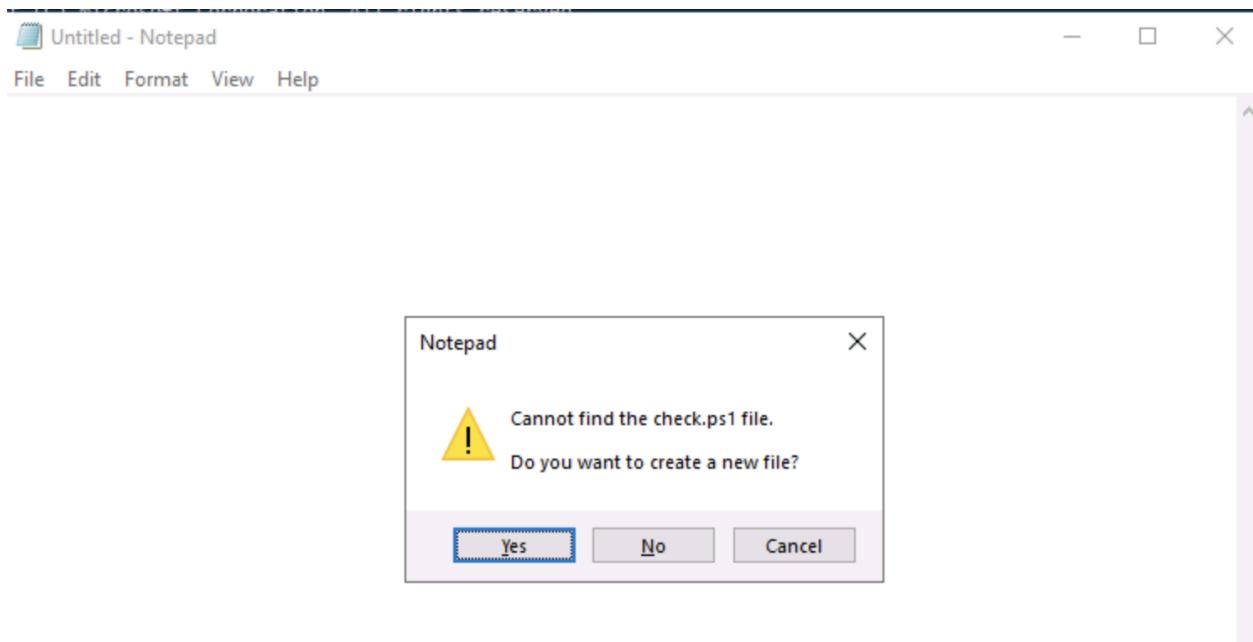
49. Enter notepad calchash.ps1. Select Yes on the Notepad window about creating a new file.Type the following into the new document: Get-FileHash ./notes.txt -Algorithm

SHA256 | Select-Object -ExpandProperty Hash | Set-Content ./hash.txt. Close Notepad, select **Save** when prompted.





50. Enter `./calhash.ps1`. (This command executes the PowerShell script of `calhash.ps1`, which generates a hash of the `notes.txt` file and saves it as `hash.txt`.. The "Set-Content" cmdlet performs a replacement rather than an append function when writing output into a file. The dot and slash (i.e., `./`) before the script name are essential for execution. Enter `type hash.txt`. (This command displays the contents of `hash.txt`) Enter `notepad check.ps1`.Select **Yes** on the *Notepad* window about creating a new file.



51. Select the empty area of the Notepad window, then select the `ctrl + v` below to paste the script into the VM.

```

if( (Get-FileHash ./notes.txt -Algorithm SHA256).Hash -ne (Get-Content
./hash.txt))

{

    "This is important" | Set-Content ./notes.txt

    Write-Host "The file has changed. Corrective action initiated."

}

else

{

    Write-Host "The file is correct. No corrective action needed."
}

```

Close **NotePad**, select **Save** when prompted.

52. Enter **./check.ps1**. (This command executes the PowerShell script of check.ps1, which calculates the hash of notes.txt and compares it to the value stored in hash.txt. If the file has not changed, a "No corrective action needed" message is displayed. If the file has changed, an "Corrective action initiated" message is displayed. The result should display the "The file is correct. No corrective action needed." message since we previously restored the notes.txt file manually.)

```

PS C:\Users\jaime>
PS C:\Users\jaime> if((Get-FileHash ./notes.txt -Algorithm SHA256).Hash -eq (Get-Content ./hash.txt)) {Write-Host "The
file is correct."} else {Write-Host "The file has changed. Corrective action should be initiated."}
The file is correct.
PS C:\Users\jaime> notepad calchash.ps1
PS C:\Users\jaime> ./calchash.ps1
PS C:\Users\jaime> type hash.txt
D978881884F4998C8C00468D69196368D7A4EBE7ACB26D8FB18710363227F27D
PS C:\Users\jaime> notepad check.ps1
PS C:\Users\jaime> ./check.ps1
The file is correct. No corrective action needed.
PS C:\Users\jaime>

```

53. Enter **type notes.txt**. we should see the correct contents of the notes.txt file. Enter **echo blah >> notes.txt**. This command injects new content into notes.txt, which changes the file. Enter **type notes.txt**. we should see the modified contents of the notes.txt file. Enter **./check.ps1**. This should display the "The file has changed. Corrective action initiated." message since the notes.txt file was modified. Enter **type**

notes.txt. we should see the corrected contents of the notes.txt file.

```
file is correct. } else {Write-Host The file has changed. Corrective action :  
The file is correct.  
PS C:\Users\jaime> notepad calchash.ps1  
PS C:\Users\jaime> ./calchash.ps1  
PS C:\Users\jaime> type hash.txt  
D978B81884F4998C8C00468D69196368D7A4EBE7ACB26D8FB18710363227F27D  
PS C:\Users\jaime> notepad check.ps1  
PS C:\Users\jaime> ./check.ps1  
The file is correct. No corrective action needed.  
PS C:\Users\jaime> type notes.txt  
This is important  
PS C:\Users\jaime> echo blah >> notes.txt  
PS C:\Users\jaime> type notes.txt  
This is important  
b l a h  
  
PS C:\Users\jaime> ./check.ps1  
The file has changed. Corrective action initiated.  
PS C:\Users\jaime> type notes.txt  
This is important  
PS C:\Users\jaime>
```

we have successfully implemented a simulation of a corrective control to repair the contents of a file should that file be modified.

This corrective action is similar to that performed by the Signature Verification (SigVerif) tool of Windows. SigVerif executes before each booting of Windows to ensure that the necessary files for a secure booting operation are present and meet a specific hash value. If any of those files are corrupted, they are removed and replaced with a valid file. The corrective actions we took manually can be automated to perform similarly. For example, we could schedule a boot task to run the check.ps1 script each time the system reboots. Also, we should run the calchash.ps1 script every time a valid change to notes.txt is performed. However, if we elect to change the contents of notes.txt, the correction action would need to be updated accordingly.

1. What is the primary purpose of preventive controls? Stop unwanted activity from succeeding
2. What is the primary purpose of detective controls? Record information about activities
3. What is the primary purpose of directive controls? Give instructions
4. What is the primary purpose of corrective controls? Restore a system back to preferred condition
5. What is the purpose of the dot and slash in front of the filenames in the PowerShell scripts and when executing PowerShell scripts? Reference the current working directory