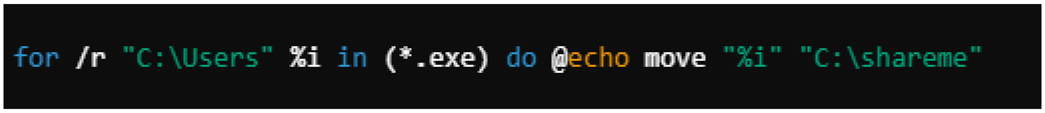
Colby Heilner
Professor Torres
10/6/24
IT 120
Lab 7

Part A: I sent a link to the Windows 10 VM (student/hacker)

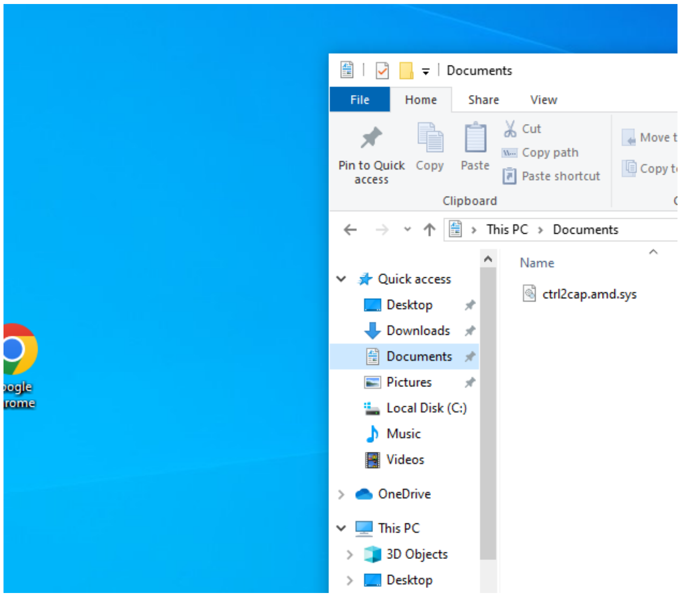
Secure your data in Windows (use the Admin command prompt)

- Centralize your data and share it on the network
  - Locate all files on your Windows that are exe, pdf, and xls, and put them in a shared folder called "shareme".
    Okay after a bit of looking i landed on this command to move the file to my SHAREME folder

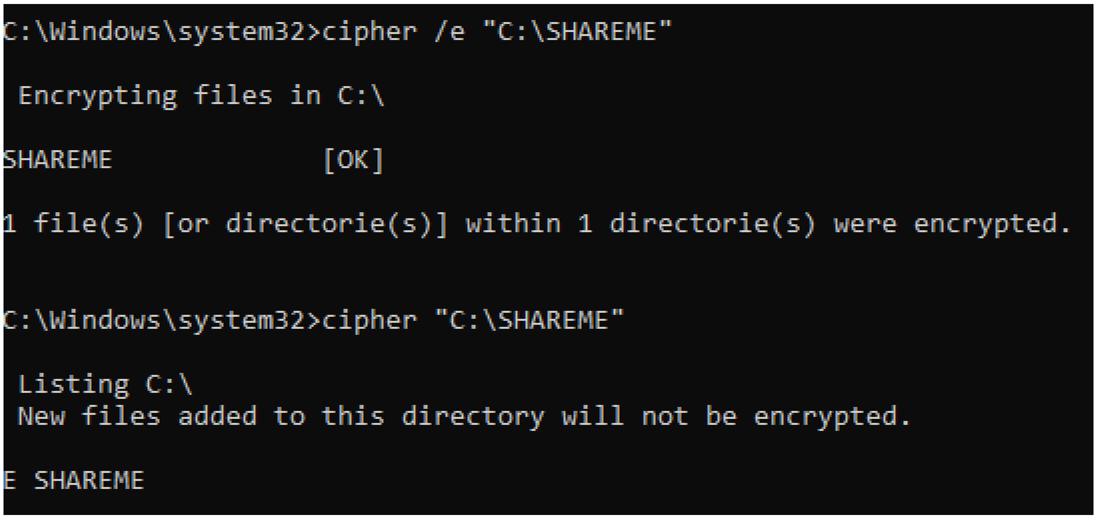


```
for /r "C:\Users" %i in (*.exe) do @echo move "%i" "C:\shareme"
```

My computer looked gross before but now
All of it looks alot better

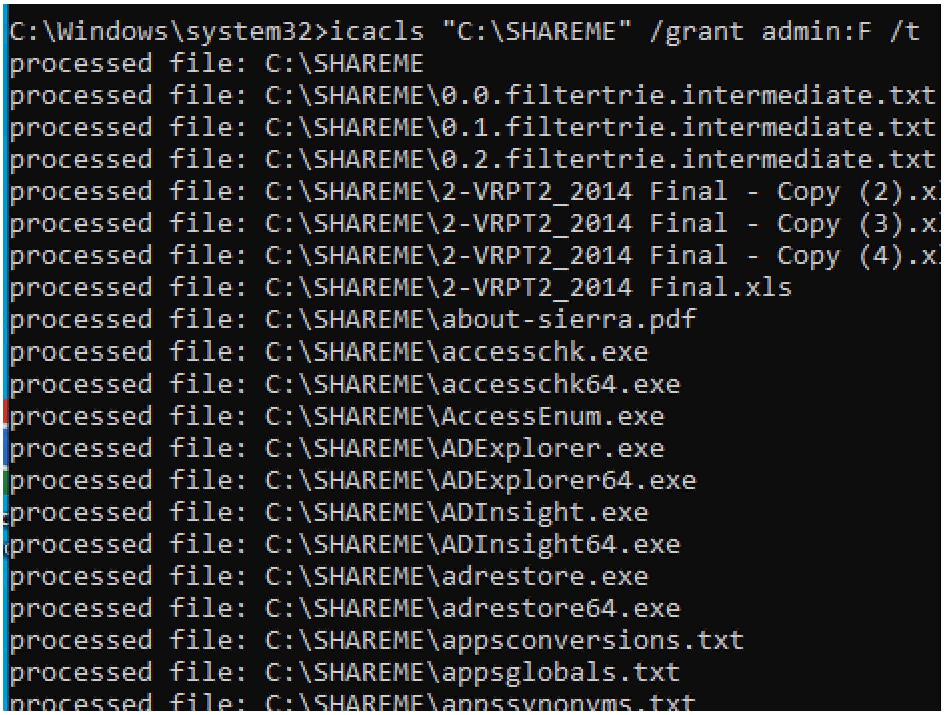


- Encrypt your shareme folder via the command prompt



```
C:\Windows\system32>cipher /e "C:\SHAREME"

 Encrypting files in C:\

SHAREME             [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.


C:\Windows\system32>cipher "C:\SHAREME"

 Listing C:\
 New files added to this directory will not be encrypted.

E SHAREME
```

- Configure file/folder policies



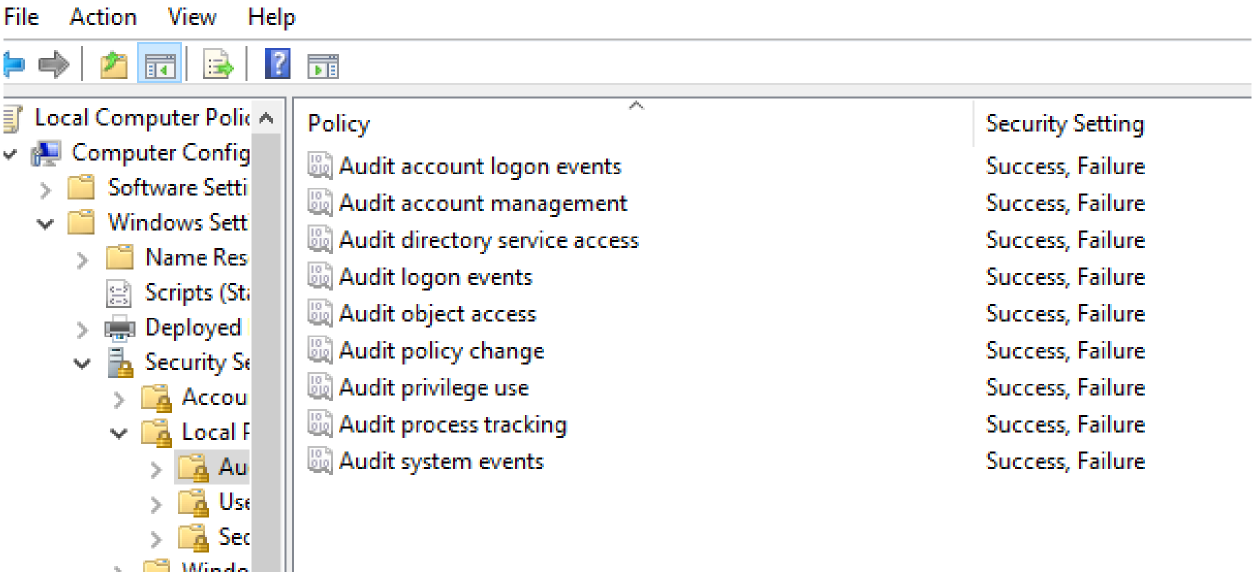
```
C:\Windows\system32>icacls "C:\SHAREME" /grant admin:F /t
processed file: C:\SHAREME
processed file: C:\SHAREME\0.0.filtertrie.intermediate.txt
processed file: C:\SHAREME\0.1.filtertrie.intermediate.txt
processed file: C:\SHAREME\0.2.filtertrie.intermediate.txt
processed file: C:\SHAREME\2-VRPT2_2014 Final - Copy (2).x
processed file: C:\SHAREME\2-VRPT2_2014 Final - Copy (3).x
processed file: C:\SHAREME\2-VRPT2_2014 Final - Copy (4).x
processed file: C:\SHAREME\2-VRPT2_2014 Final.xls
processed file: C:\SHAREME\about-sierra.pdf
processed file: C:\SHAREME\accesschk.exe
processed file: C:\SHAREME\accesschk64.exe
processed file: C:\SHAREME\AccessEnum.exe
processed file: C:\SHAREME\ADExplorer.exe
processed file: C:\SHAREME\ADExplorer64.exe
processed file: C:\SHAREME\ADInsight.exe
processed file: C:\SHAREME\ADInsight64.exe
processed file: C:\SHAREME\adrestore.exe
processed file: C:\SHAREME\adrestore64.exe
processed file: C:\SHAREME\appsconversions.txt
processed file: C:\SHAREME\appsglobals.txt
processed file: C:\SHAREME\appssynonyms.txt
```

○ Configure audit policies for your new folder, auditing access, edit, delete, and move policies

- Add a user and Access your shared folders and edit/delete some of its content

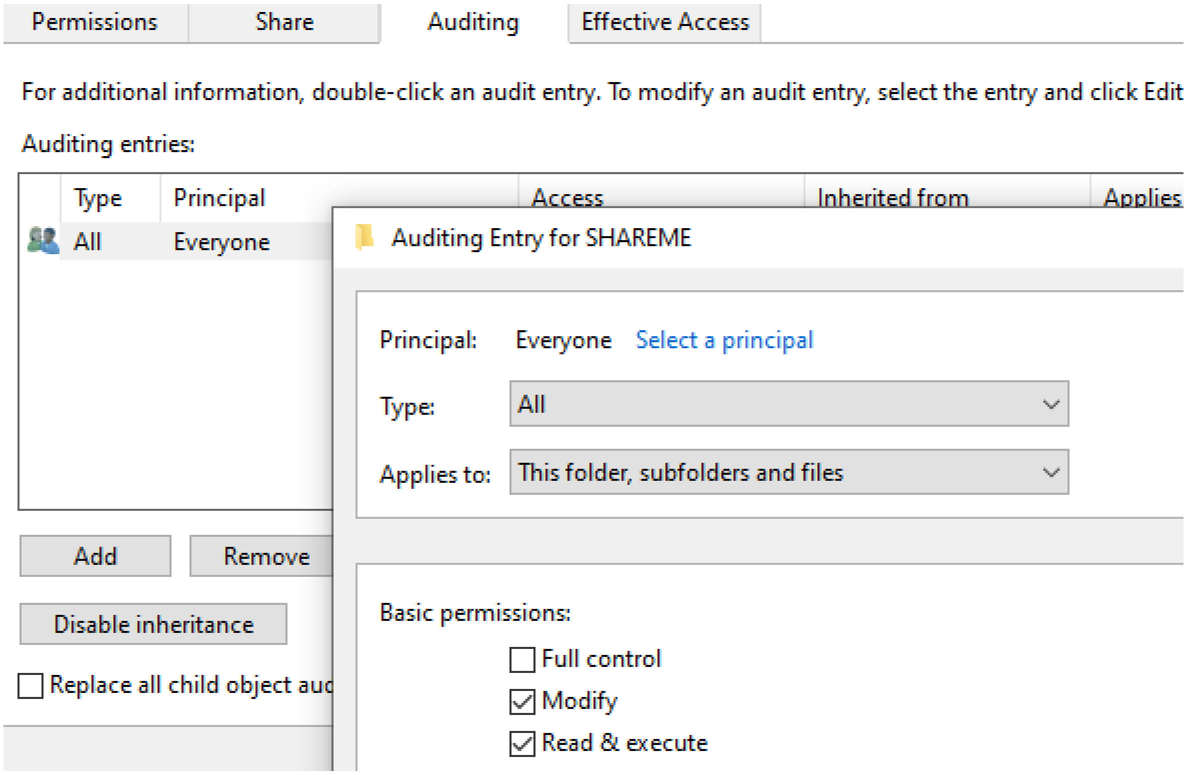
○ Locate the logs that show what you did in this folder

First come here toggle success and failure



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Then go to folder properties and enable what you want



For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit

Auditing entries:

Type	Principal	Access	Inherited from	Applies
All	Everyone			

□ Replace all child object auc

Auditing Entry for SHAREME

Principal: Everyone Select a principal

Type: All

Applies to: This folder, subfolders and files

Basic permissions:

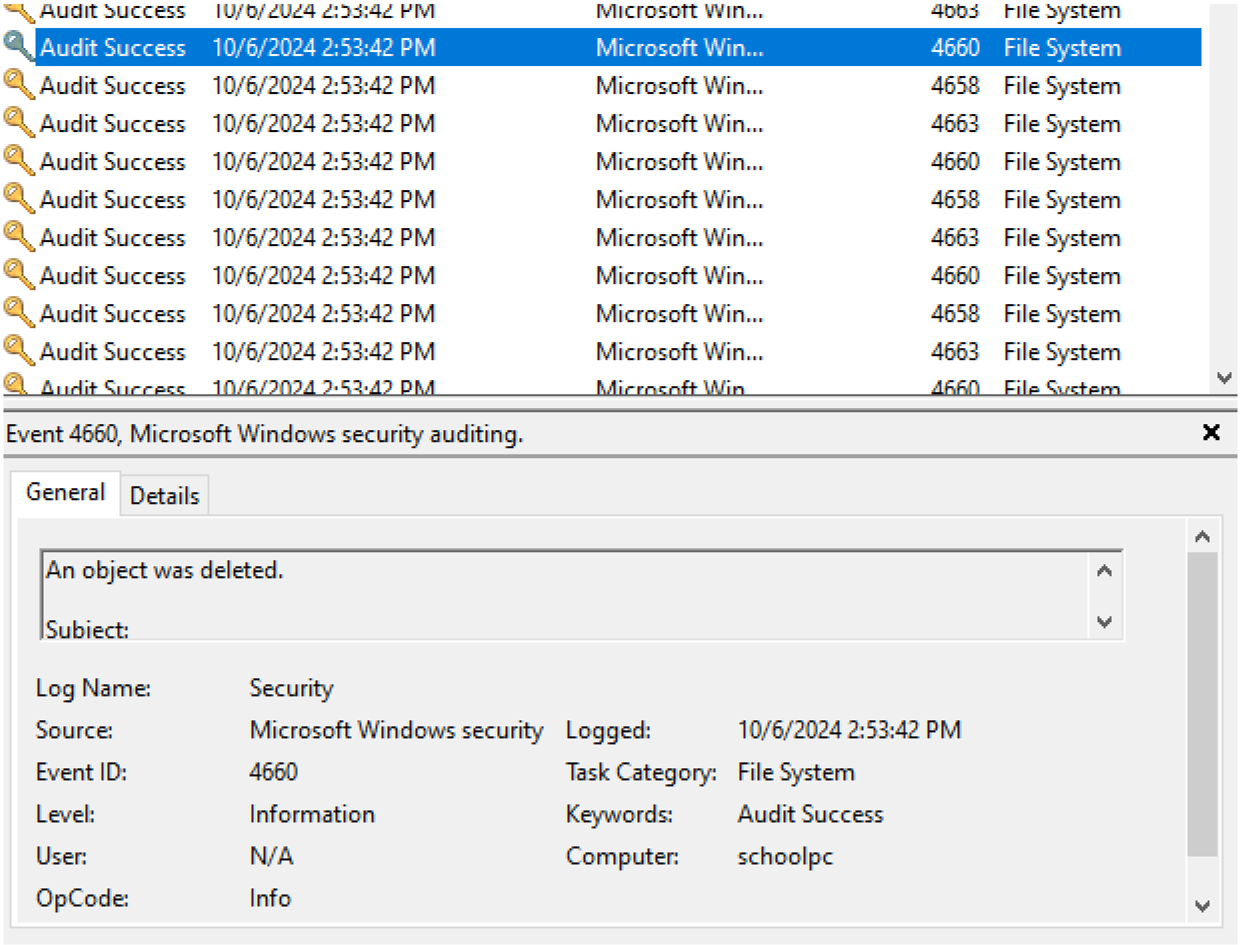
□ Full control

☑ Modify

☑ Read & execute

Here I have a audit for Everyone, success or failure And everyhting checked except full control.

Here is my audit log for deleting a file



Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4663	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4660	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4658	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4663	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4660	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4658	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4663	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4660	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4658	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4663	File System
Audit Success	10/6/2024 2:53:42 PM	Microsoft Win...	4660	File System

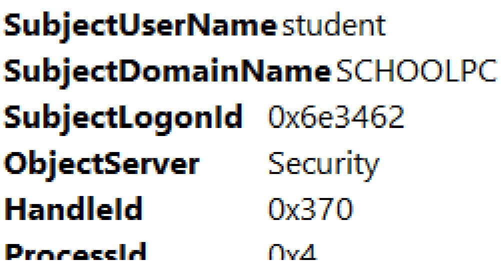
Event 4660, Microsoft Windows security auditing.

An object was deleted.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/6/2024 2:53:42 PM
Event ID:	4660	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	schoolpc
OpCode:	Info		

It would not show me users unless you went to details and friendly view



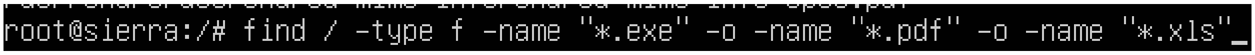
SubjectUserName	student
SubjectDomainName	SCHOOLPC
SubjectLogonId	0x6e3462
ObjectServer	Security
HandleId	0x370
ProcessId	0x4

Part B: I sent a link to the Ubuntu Server (student/hacker)

Secure your data in Linux (use the root)

- Centralize your data
- ○ Locate all files on your Linux that have the following extensions: exe, pdf, xls, and put them in a shared folder called "shareme".

To start I found all files with this command.

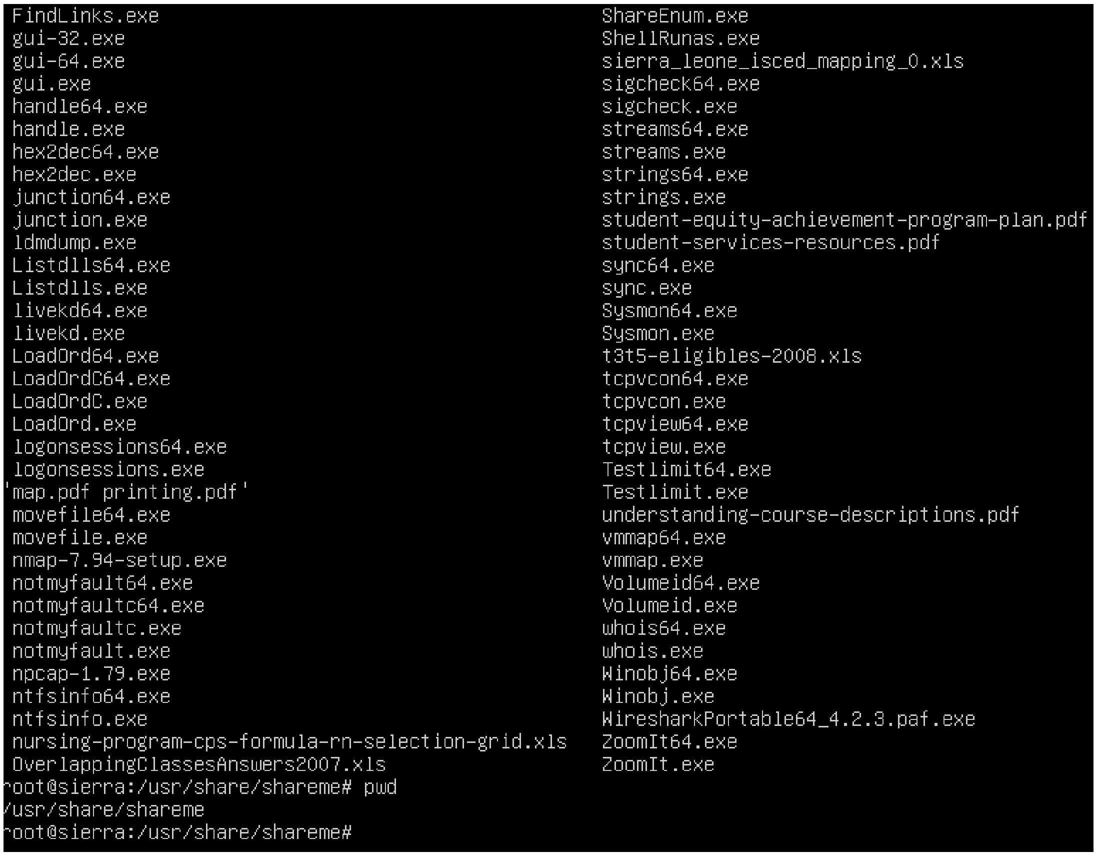


```
root@sierra:/# find / -type f -name "*.exe" -o -name "*.pdf" -o -name "*.xls"_
```

Then modified the command to also move these files i found into my shareme folder.

find / -type f \(-name "*.exe" -o -name "*.pdf" -o -name "*.xls" \) -exec mv {} ~/shareme/ \;

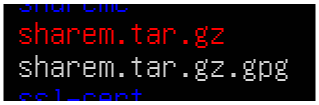
And they got moved,



```
 FindLinks.exe                                       ShareEnum.exe
 gui-32.exe                                          ShellRunas.exe
 gui-64.exe                                          sierra_leone_isced_mapping_0.xls
 gui.exe                                             sigcheck64.exe
 handle64.exe                                        sigcheck.exe
 handle.exe                                          streams64.exe
 hex2dec64.exe                                       streams.exe
 hex2dec.exe                                         strings64.exe
 junction64.exe                                      strings.exe
 junction.exe                                        student-equity-achievement-program-plan.pdf
 ldmdump.exe                                         student-services-resources.pdf
 Listdlls64.exe                                      sync64.exe
 Listdlls.exe                                        sync.exe
 livekd64.exe                                        Sysmon64.exe
 livekd.exe                                          Sysmon.exe
 LoadOrd64.exe                                       t3t5-eligibles-2008.xls
 LoadOrdC64.exe                                      tcpvcon64.exe
 LoadOrdC.exe                                        tcpvcon.exe
 LoadOrd.exe                                         tcpview64.exe
 logonsessions64.exe                                 tcpview.exe
 logonsessions.exe                                   Testlimit64.exe
'map.pdf printing.pdf'                               Testlimit.exe
 movefile64.exe                                      understanding-course-descriptions.pdf
 movefile.exe                                        vmmap64.exe
 nmap-7.94-setup.exe                                 vmmap.exe
 notmyfault64.exe                                    Volumeid64.exe
 notmyfaultc64.exe                                   Volumeid.exe
 notmyfaultc.exe                                     whois64.exe
 notmyfault.exe                                      whois.exe
 npcap-1.79.exe                                      Winobj64.exe
 ntfsinfo64.exe                                      Winobj.exe
 ntfsinfo.exe                                        WiresharkPortable64_4.2.3.paf.exe
 nursing-program-cps-formula-rn-selection-grid.xls   ZoomIt64.exe
 OverlappingClassesAnswers2007.xls                   ZoomIt.exe
root@sierra:/usr/share/shareme# pwd
/usr/share/shareme
root@sierra:/usr/share/shareme#
```

- Encrypt your shareme folder via the terminal using gpg or openssl
- Configure file/folder policies

I then compressed and added a passphrase for the file.



```
shareme
sharem.tar.gz
sharem.tar.gz.gpg
ssl-cert
```

I also made an admin account and ran these command to give it access and it only

sudo chown -R [user]:[group] ~/shareme

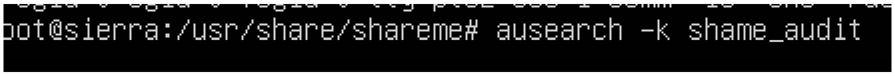
sudo chmod -R 700 ~/shareme

- ○ Configure audit policies for your new folder, auditing access, edit, delete, and move policies
- ○ utilize iwatch or auditd (these need to be downloaded) to configure auditing.
- Add a user and access your shared folders and edit/delete some of it's content
- ○ Locate the logs that show what you did in this folder

  After i enabled logs I used my admin user to try and mess with it

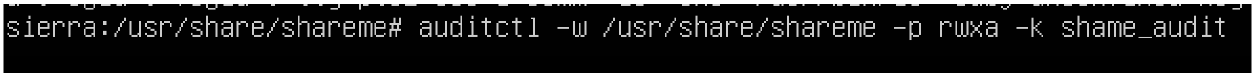
  Here you can see that I made a file useing nano in the shareme dir

  I viewed these logs by going to this

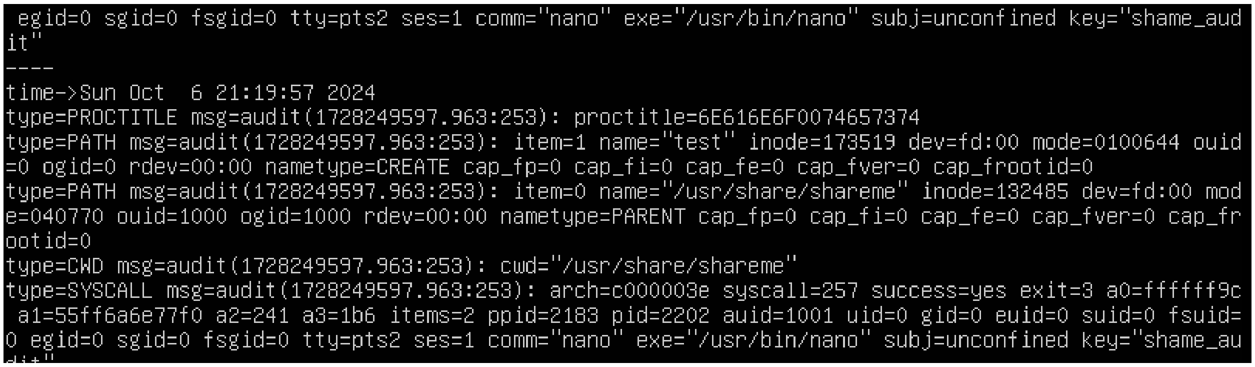


```
oot@sierra:/usr/share/shareme# ausearch -k shame_audit
```

After running this



```
sierra:/usr/share/shareme# auditctl -w /usr/share/shareme -p rwxa -k shame_audit
```



```
 egid=0 sgid=0 fsgid=0 tty=pts2 ses=1 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shame_aud
it"
----
time->Sun Oct  6 21:19:57 2024
type=PROCTITLE msg=audit(1728249597.963:253): proctitle=6E616E6F0074657374
type=PATH msg=audit(1728249597.963:253): item=1 name="test" inode=173519 dev=fd:00 mode=0100644 ouid
=0 ogid=0 rdev=00:00 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1728249597.963:253): item=0 name="/usr/share/shareme" inode=132485 dev=fd:00 mod
e=040770 ouid=1000 ogid=1000 rdev=00:00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_fr
ootid=0
type=CWD msg=audit(1728249597.963:253): cwd="/usr/share/shareme"
type=SYSCALL msg=audit(1728249597.963:253): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c
 a1=55ff6a6e77f0 a2=241 a3=1b6 items=2 ppid=2183 pid=2202 auid=1001 uid=0 gid=0 euid=0 suid=0 fsuid=
0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=1 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shame_au
```

Part C:

Full Disk Encryption

- Discuss the process of full disk encryption in Windows using Bitlocker.
- ○ How do you fully encrypt your Windows with Bitlocker?
- ○ What is needed?
- ○ How do you un-encrypt your Windows system?
- ○ What type of encryption does Bitlocker use?

  Firstly you need Windows 10 Pro, Enterprise or Education versions.

Enable BitLocker:
Access through Control Panel > System and Security > BitLocker Drive Encryption.
Select Drive:
Choose the system drive (usually C:).
Start Encryption:
Click Turn on BitLocker and follow the prompts.

YOU NEDD A TMP. Or a trusted platform module. This is a little chip that is your ticket to making sure you do not lose your data and can prove to your other hardware components that they are who they say they are.

To unencrypt you can
Go to **Control Panel** > **System and Security** > **BitLocker Drive Encryption**.
Then
Click **Turn off BitLocker** next to the encrypted drive.

Bit locker uses AES

Typically uses 128-bit or 256-bit encryption keys for data protection.

- Discuss the process of full disk encryption in Linux using the Native Operating System (This is a feature that is shown during installation)
  - How do you fully encrypt your Ubuntu distribution?
  - What is needed?
  - How do you un-encrypt your Ubuntu distribution?
  - What type of encryption does Ubuntu utilize?

During the installation of ubuntu you can select to encrypt here is a formatted step by step

- When installing Ubuntu, select "Erase disk and install Ubuntu".
- Choose "Use LVM with the new Ubuntu installation" (Logical Volume Management).
- Check the option for "Encrypt the new Ubuntu installation for security".

Some requirements are

- Adequate disk space and memory.
- Backup Recovery Key:

- Remember the encryption passphrase; it's necessary to unlock the disk at boot.

To Un-encrypt

- **Boot into Recovery Mode**:
- If needed, access the recovery mode by holding **Shift** during boot.
- **Remove Encryption**:
- Use `cryptsetup` to unlock and copy data to a non-encrypted partition:

```
sudo cryptsetup luksOpen /dev/sdaX cryptroot

# Replace sdaX with your encrypted partition

sudo rsync -a /mnt/cryptroot/ /mnt/newdisk/

# Copy data to a new unencrypted partition
```

Types of encryption used

- **LUKS (Linux Unified Key Setup)**:
- Commonly used for encrypting disk partitions.
- **AES (Advanced Encryption Standard)**:
- Typically employs AES-256 encryption for securing data