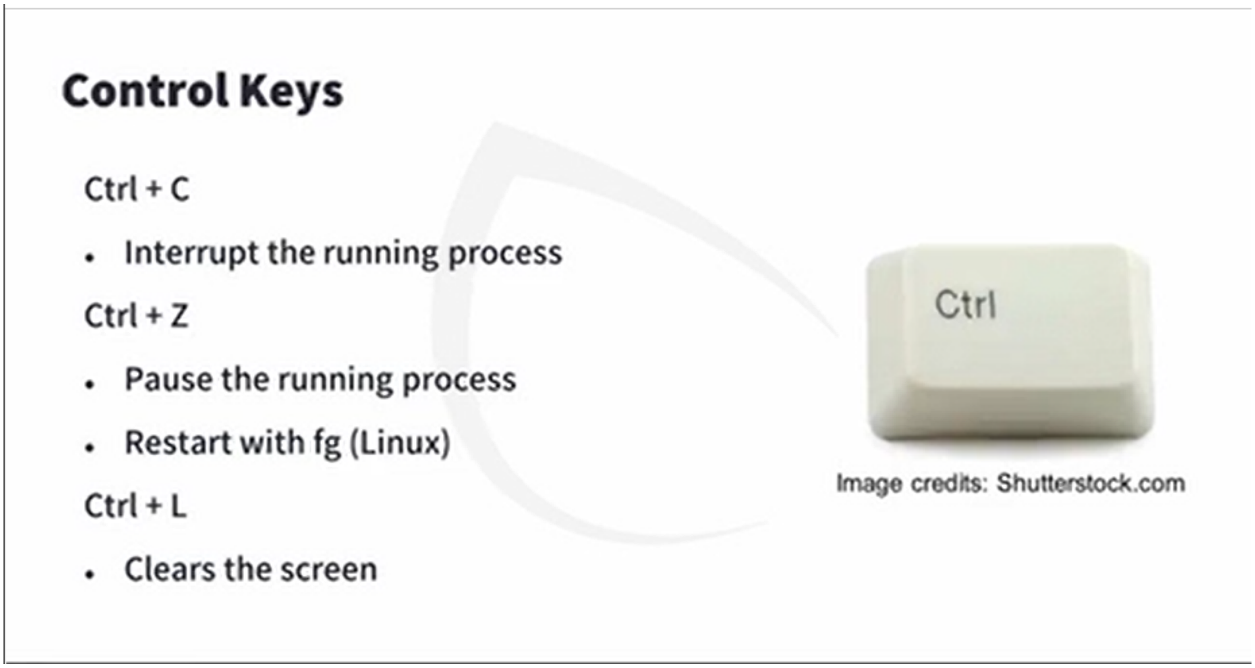
Command Line Basics



Control Keys

Ctrl + C

- Interrupt the running process

Ctrl + Z

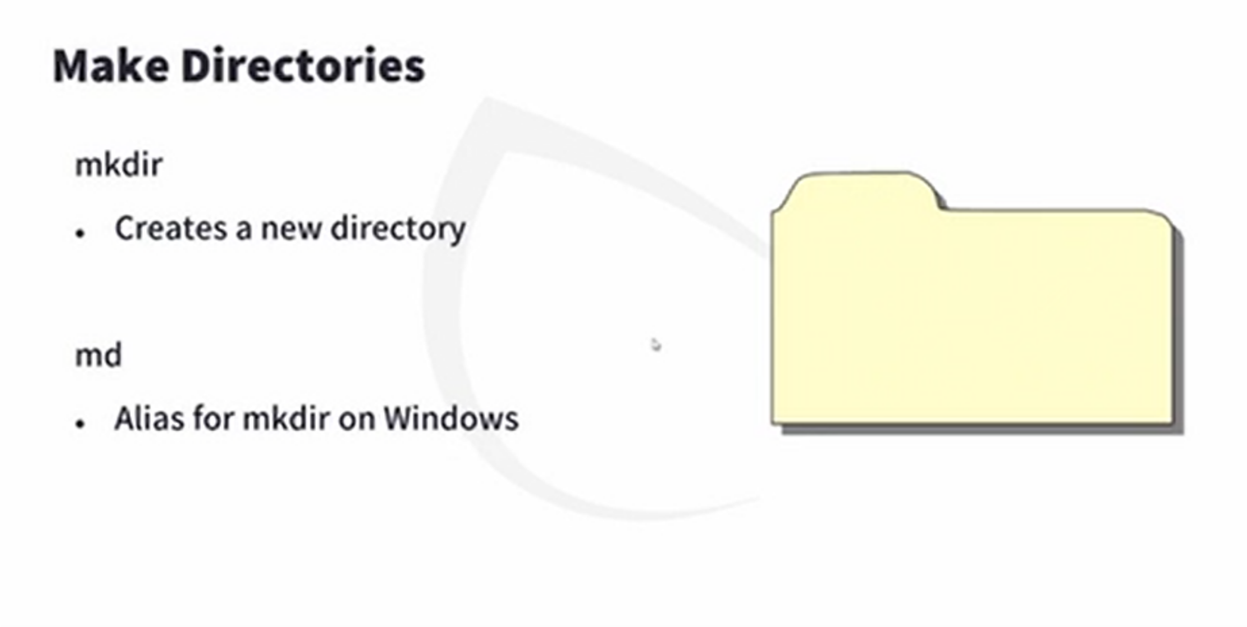
- Pause the running process
- Restart with fg (Linux)

Ctrl + L

- Clears the screen

Image credits: Shutterstock.com

- To go back two dir—- cd..\..
- For Changing drives in windows—- cd /d D:\
- For graphical representation of files within a drive—- tree /f || and for one by one display— tree |more (for both linux and windows.
-



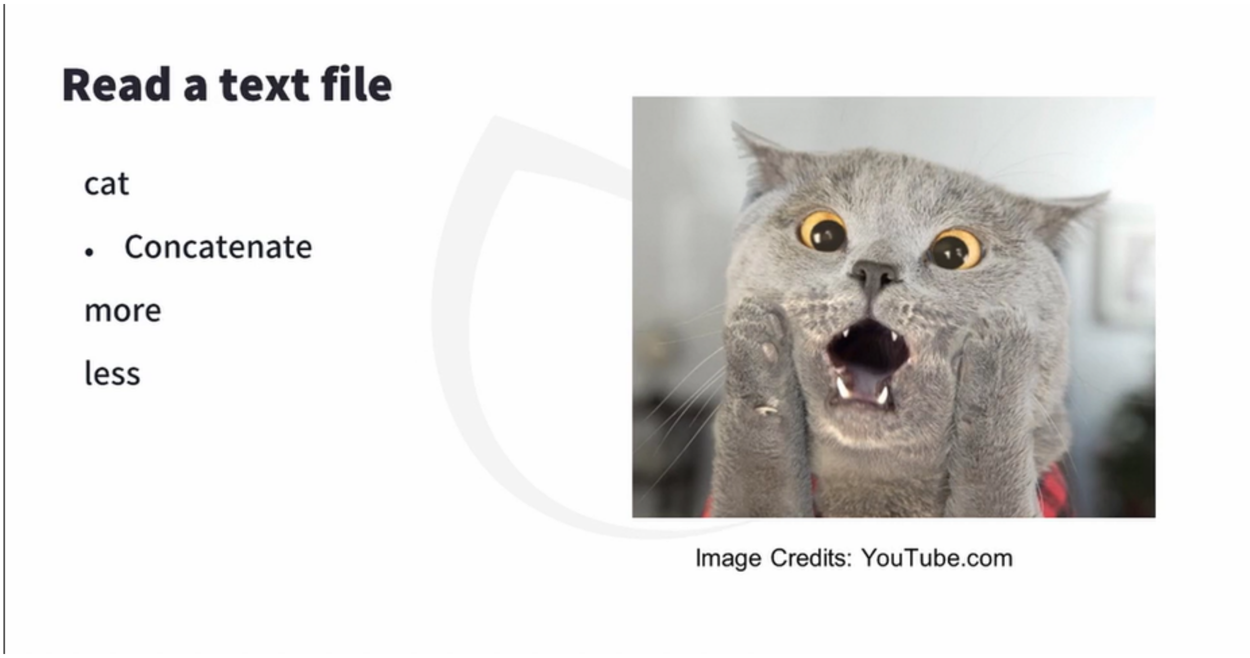
Make Directories

mkdir

- Creates a new directory

md

- Alias for mkdir on Windows



Read a text file

cat

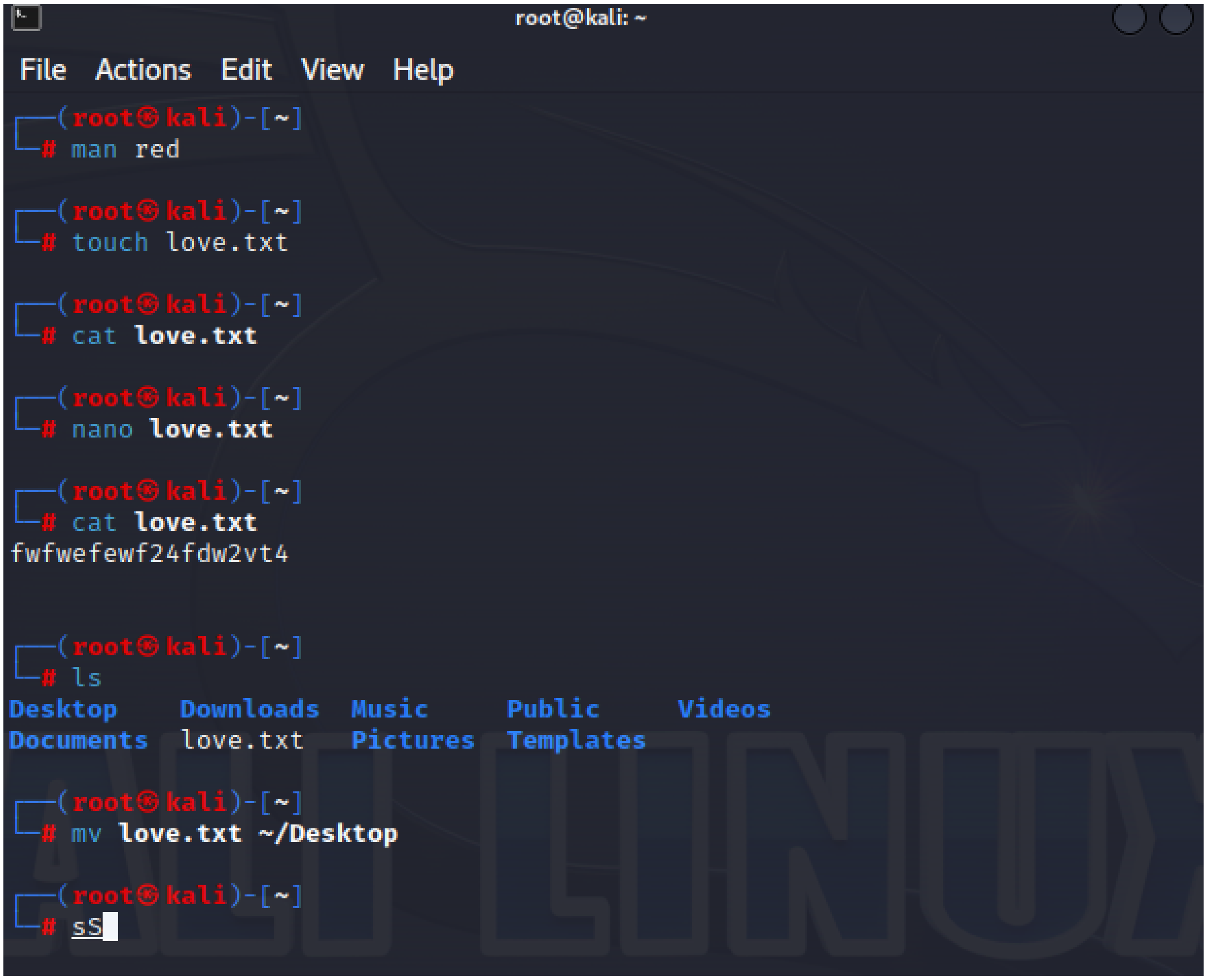
- Concatenate

more

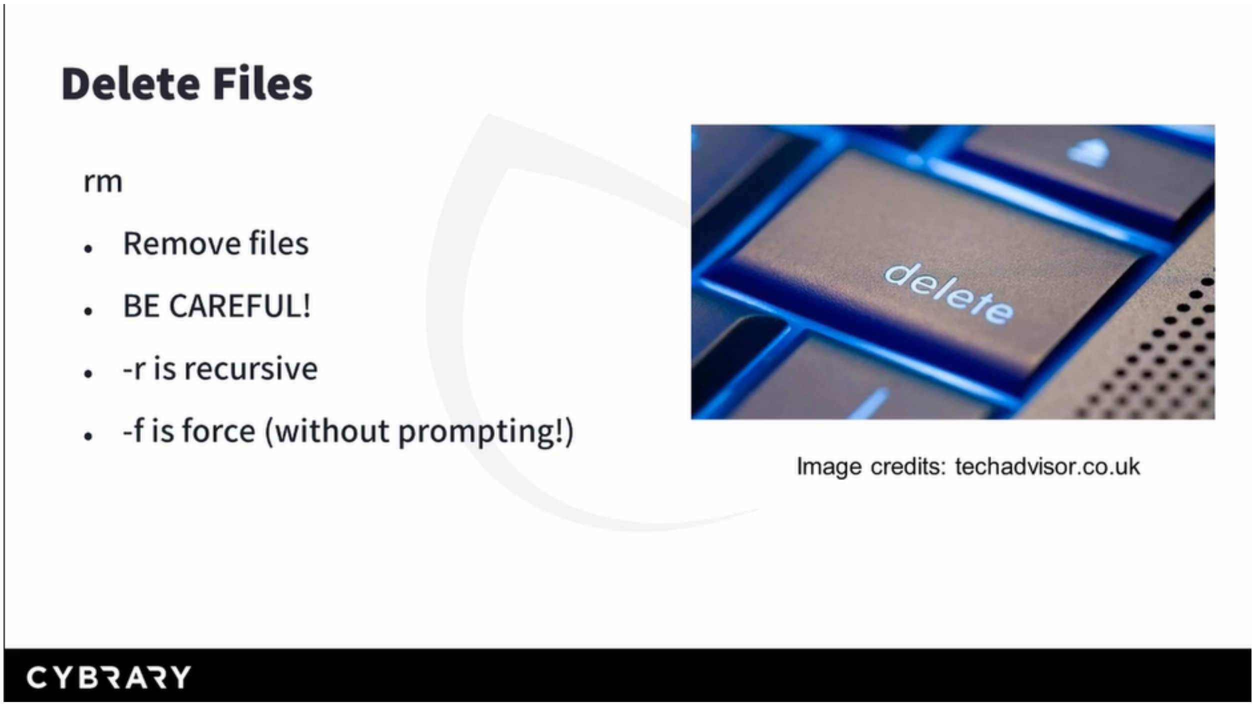
less

Image Credits: YouTube.com

For making files and moving



```
┌──(root㉿kali)-[~]
└─# man red

┌──(root㉿kali)-[~]
└─# touch love.txt

┌──(root㉿kali)-[~]
└─# cat love.txt

┌──(root㉿kali)-[~]
└─# nano love.txt

┌──(root㉿kali)-[~]
└─# cat love.txt
fwfwefewf24fdw2vt4


┌──(root㉿kali)-[~]
└─# ls
Desktop    Downloads  Music     Public     Videos
Documents  love.txt   Pictures  Templates

┌──(root㉿kali)-[~]
└─# mv love.txt ~/Desktop

┌──(root㉿kali)-[~]
└─# sS
```

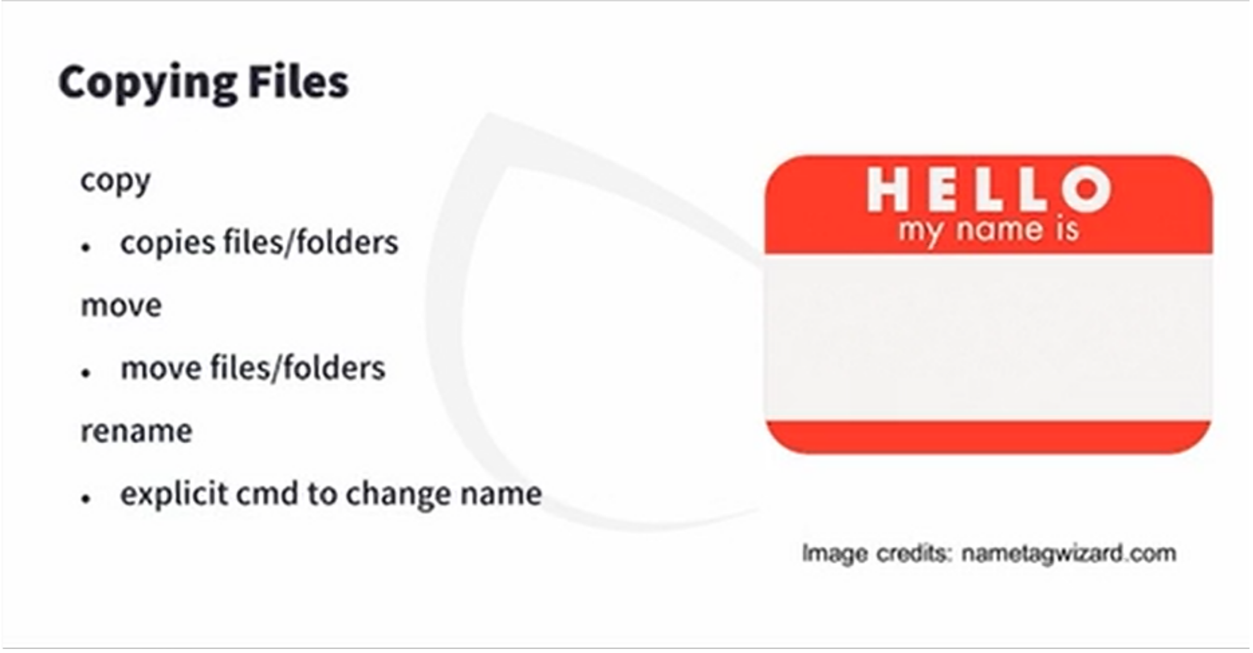


Delete Files

rm

- Remove files
- BE CAREFUL!
- -r is recursive
- -f is force (without prompting!)

Image credits: techadvisor.co.uk



Copying Files

copy

- copies files/folders

move

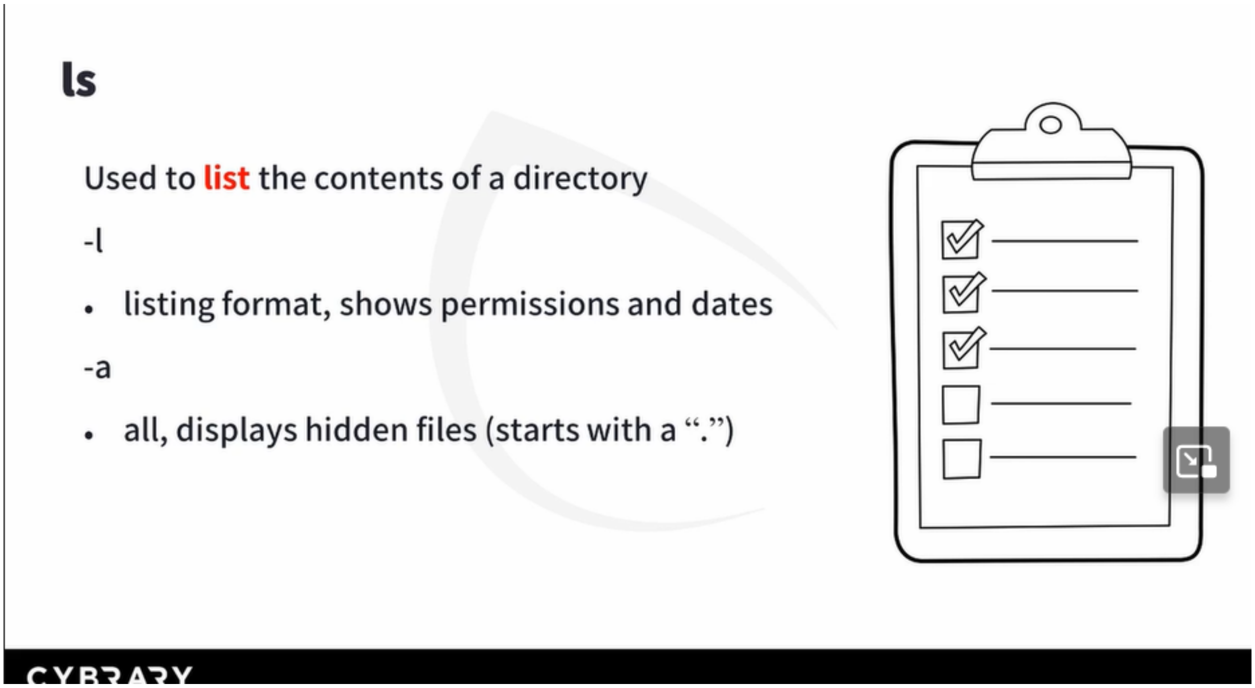
- move files/folders

rename

- explicit cmd to change name

Image credits: nametagwizard.com

For Linux



ls

Used to **list** the contents of a directory

-l

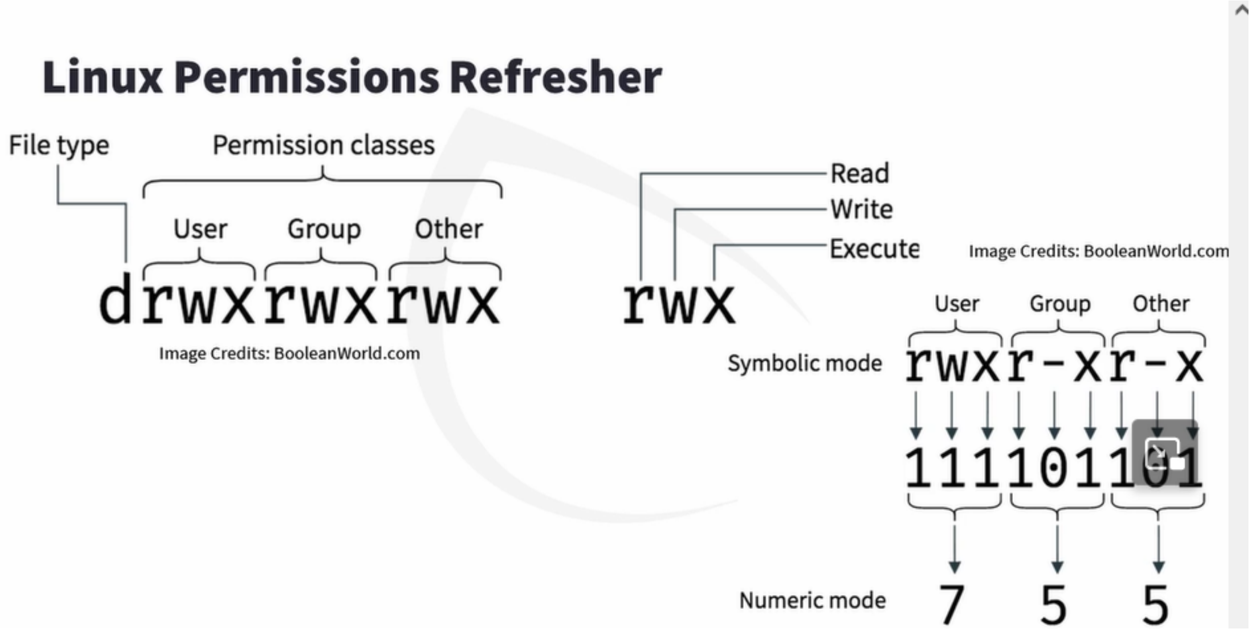
- listing format, shows permissions and dates

-a

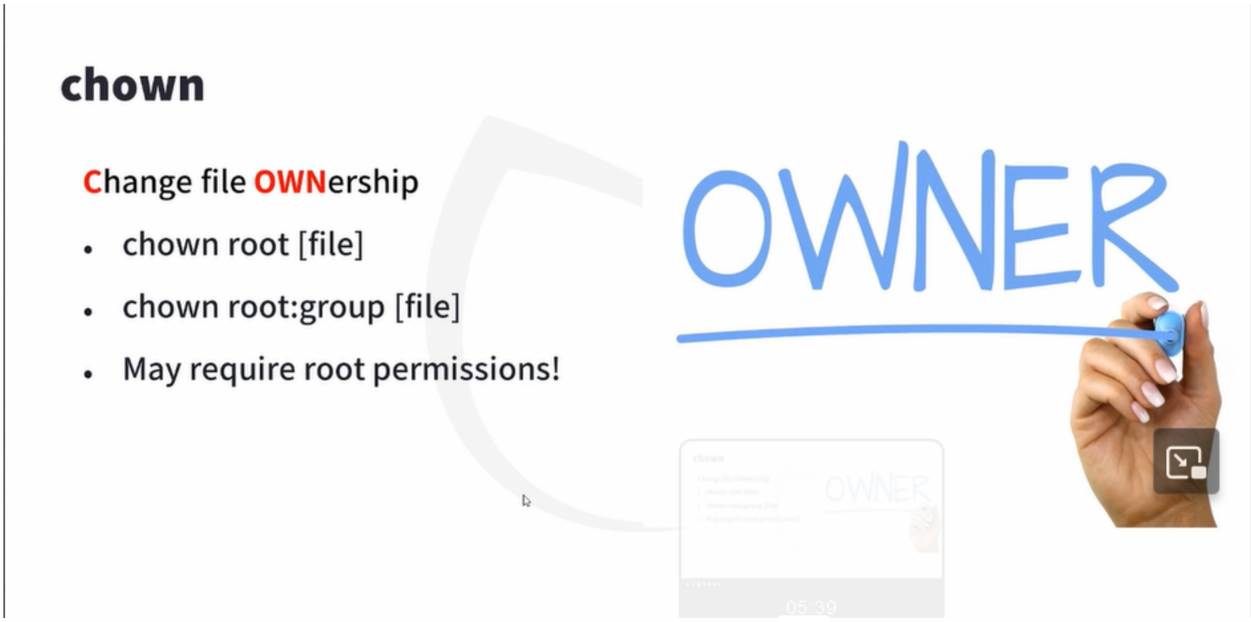
- all, displays hidden files (starts with a ".")

CYBRARY

Permissions



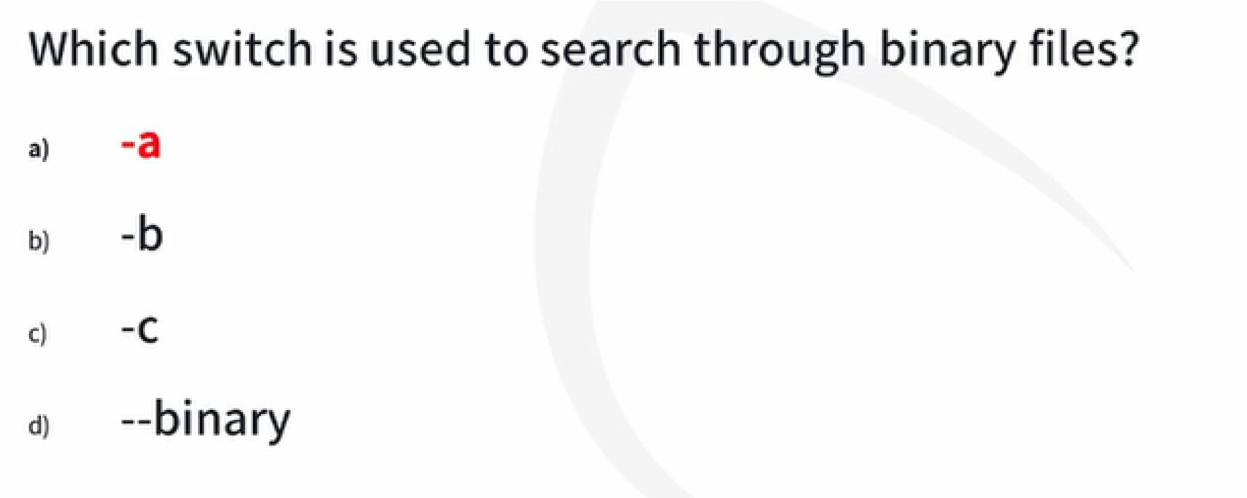
Linux Permissions Refresher



chown

Change file OWNership

- chown root [file]
- chown root:group [file]
- May require root permissions!



Which switch is used to search through binary files?

a) -a

b) -b

c) -c

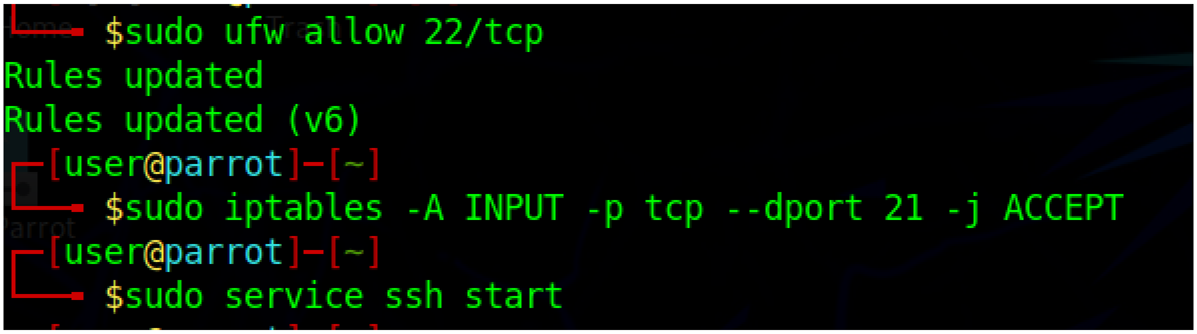
d) --binary

for sorting files

cat “filename” | sort | uniq -c (uniq - for dispalying non duplicate string and -c is for the count of those duplicate strings).

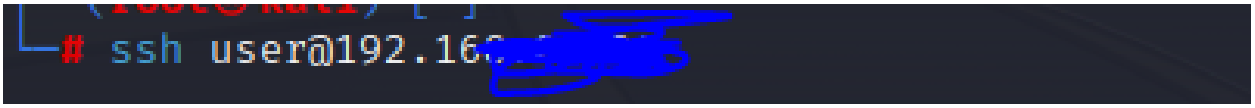
For Connecting to a remote server through ssh

step 1

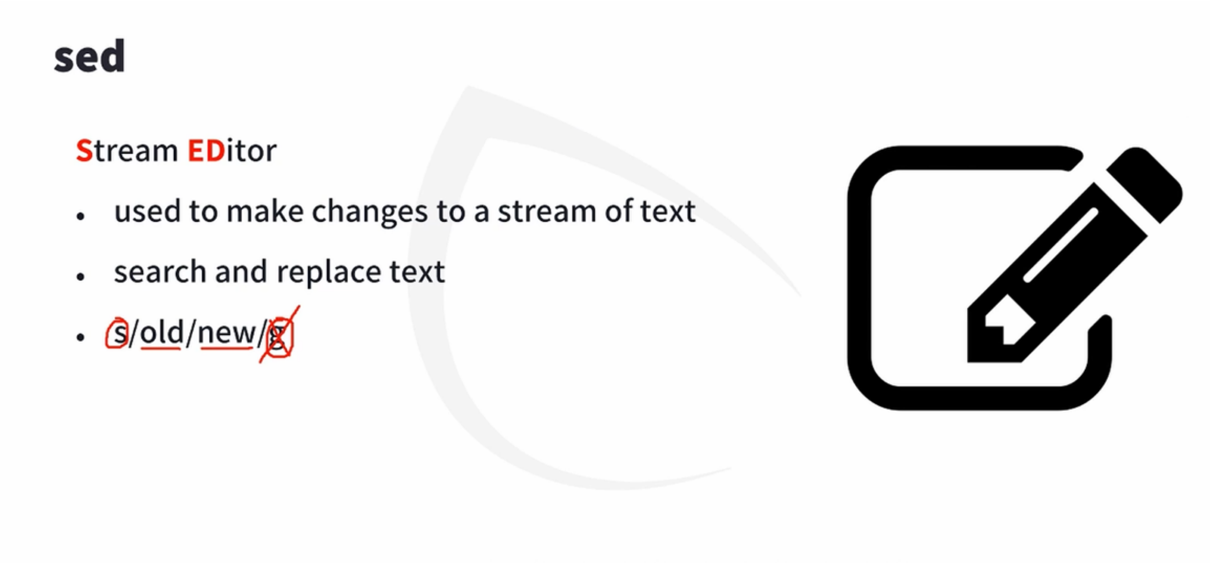


```
└──╼ $sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
┌─[user@parrot]─[~]
└──╼ $sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
┌─[user@parrot]─[~]
└──╼ $sudo service ssh start
```

step 2



```
└─# ssh user@192.16[redacted]
```

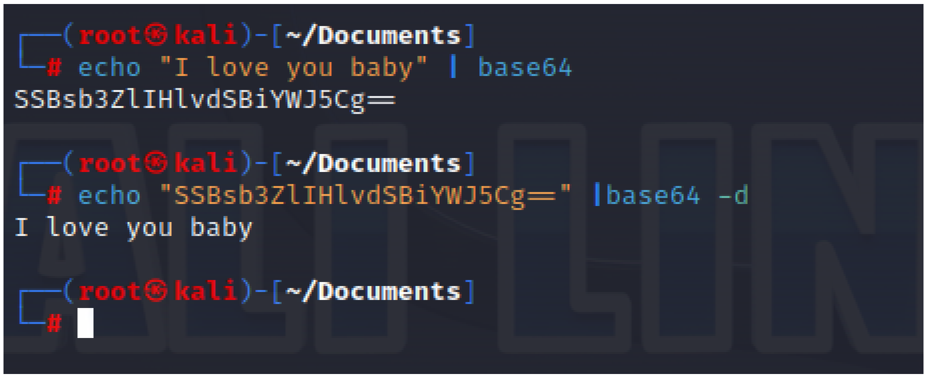


sed

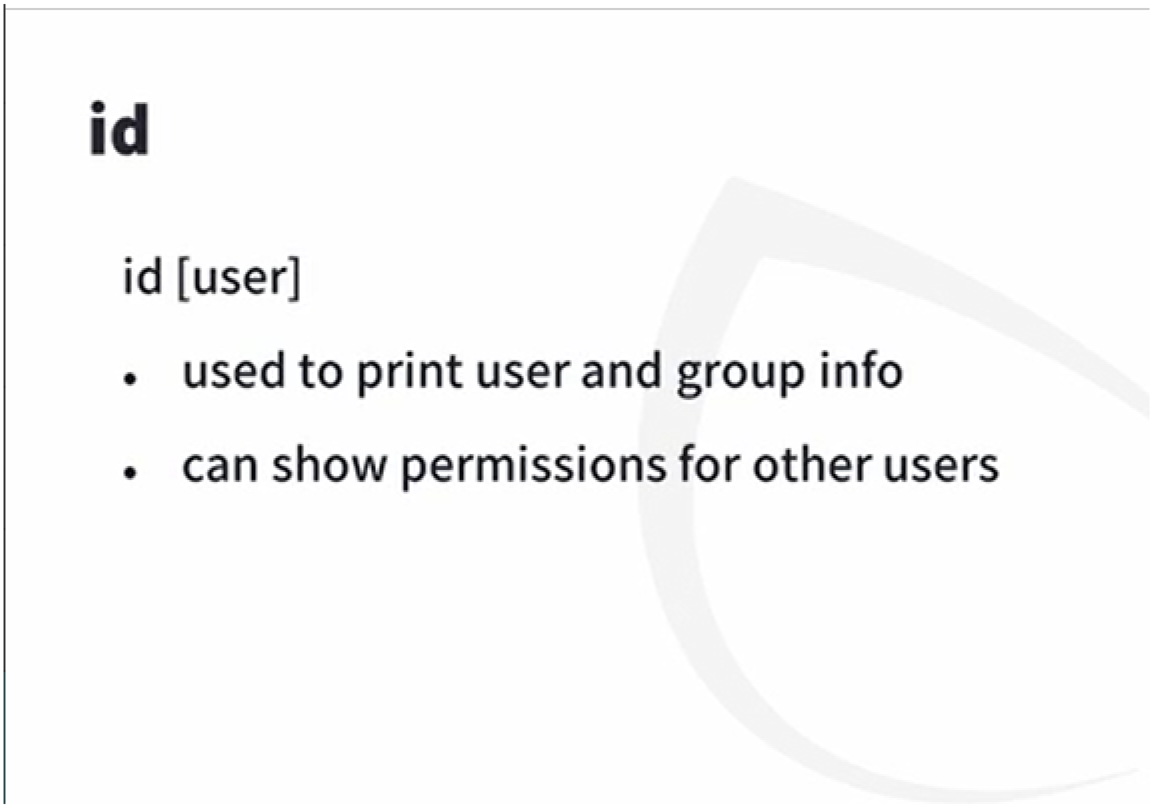
Stream EDitor

- used to make changes to a stream of text
- search and replace text
- s/old/new/~~g~~

for hashing



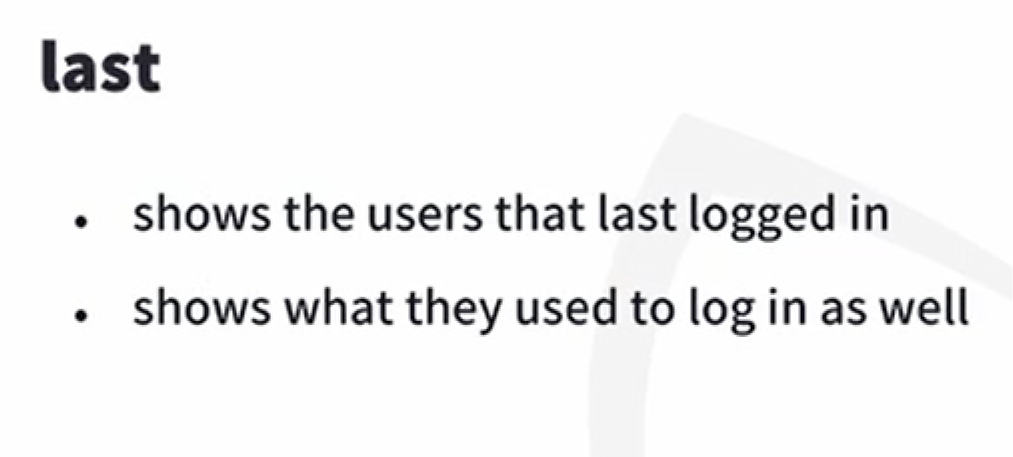
```
┌──(root㉿kali)-[~/Documents]
└─# echo "I love you baby" | base64
SSBsb3ZlIHlvdSBiYWJ5Cg==

┌──(root㉿kali)-[~/Documents]
└─# echo "SSBsb3ZlIHlvdSBiYWJ5Cg==" |base64 -d
I love you baby

┌──(root㉿kali)-[~/Documents]
└─# 
```



id

id [user]

- used to print user and group info
- can show permissions for other users



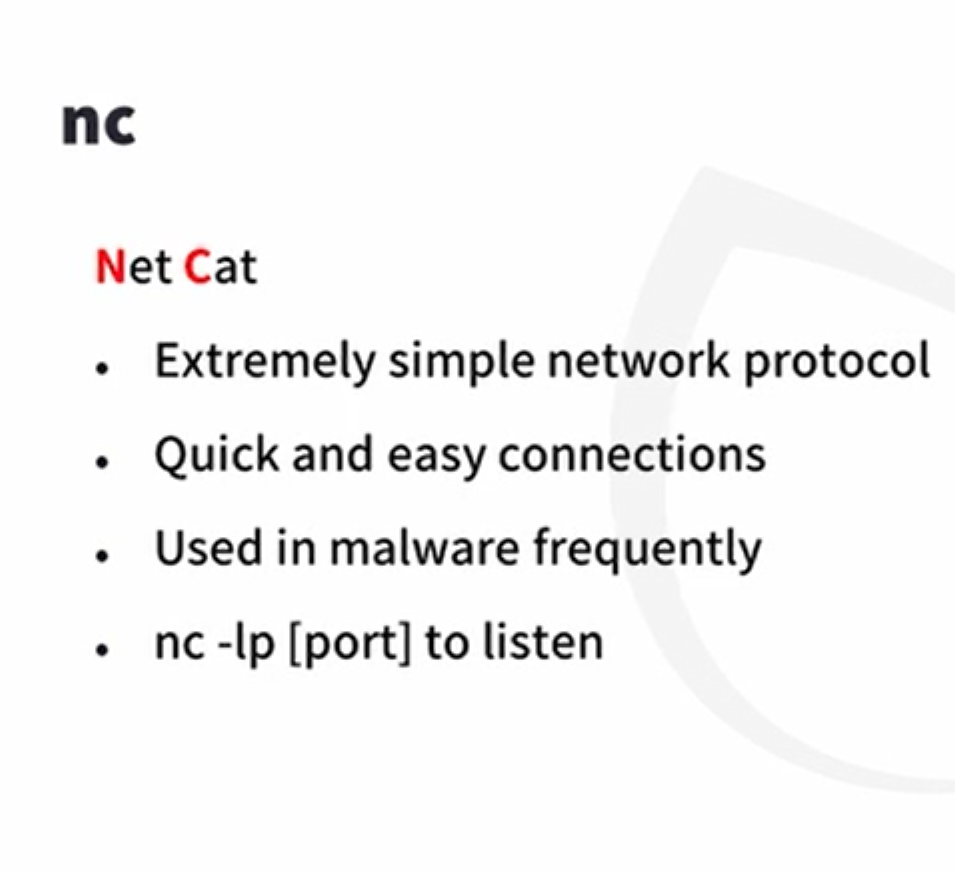
last

- shows the users that last logged in
- shows what they used to log in as well

ps- For showing the running process under a user

ps aux- for showing all the processes in the system

telnet- For remotely connecting to a system(should not be used today as it has no encription)

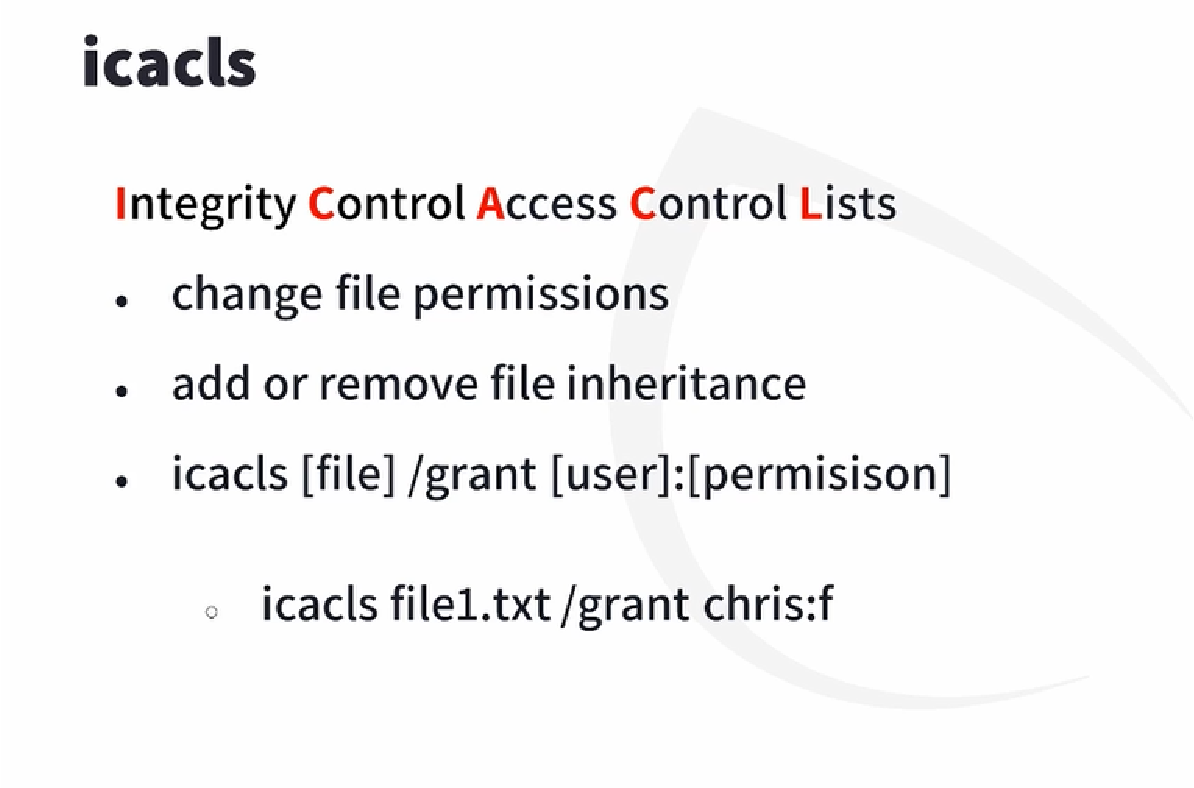


nc

Net Cat

- Extremely simple network protocol
- Quick and easy connections
- Used in malware frequently
- nc -lp [port] to listen

WINDOWS

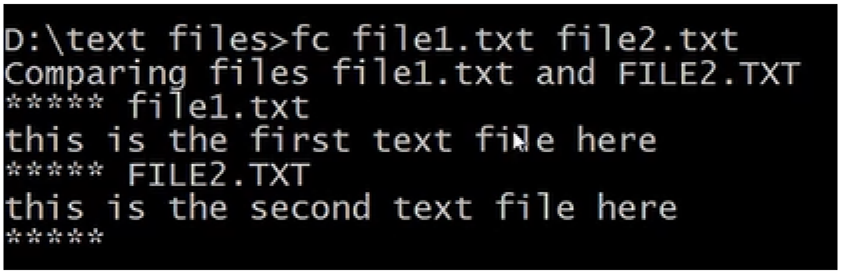


icacls

Integrity Control Access Control Lists

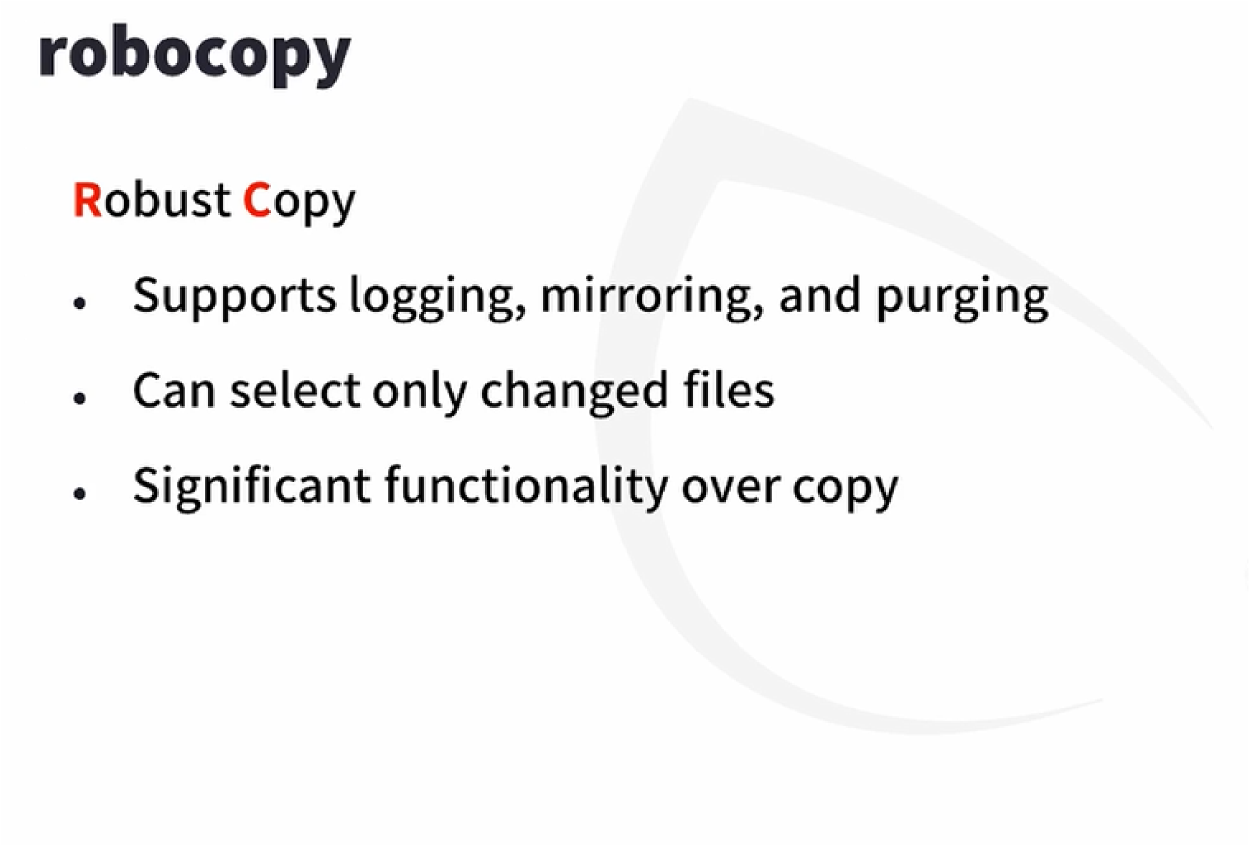
- change file permissions
- add or remove file inheritance
- icacls [file] /grant [user]:[permisison]
  - icacls file1.txt /grant chris:f

fc- File comaparison



```
D:\text files>fc file1.txt file2.txt
Comparing files file1.txt and FILE2.TXT
***** file1.txt
this is the first text file here
***** FILE2.TXT
this is the second text file here
*****
```

- xcopy- copis files and dir trees

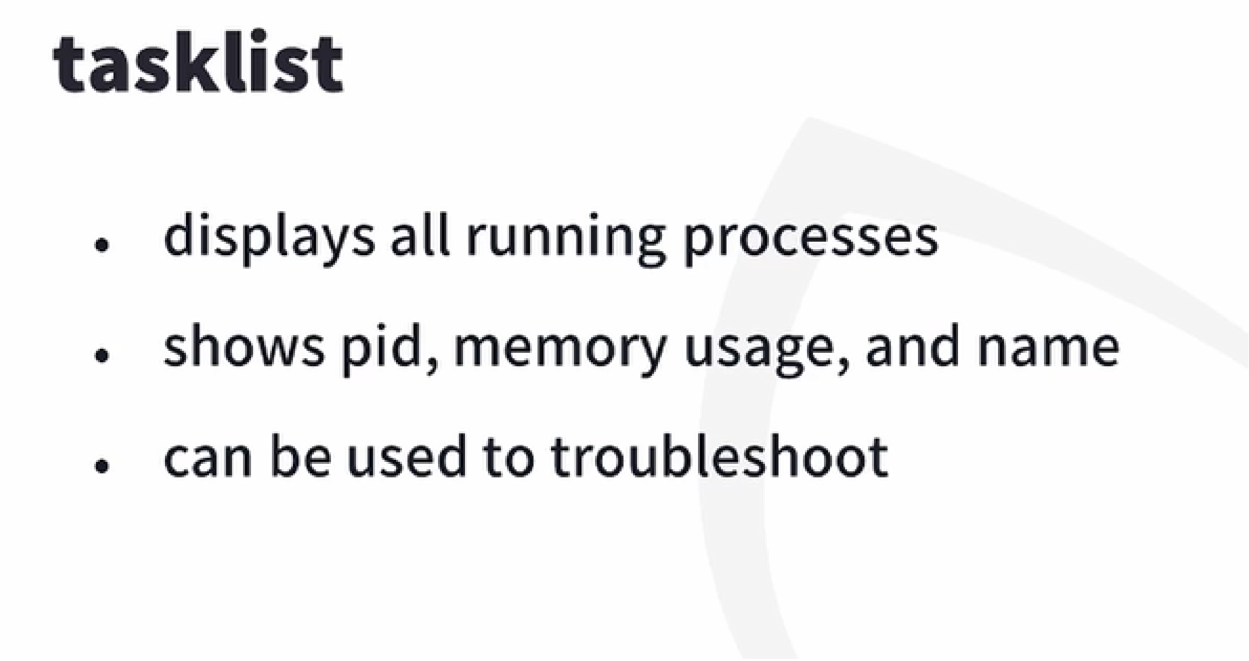


robocopy

Robust Copy

- Supports logging, mirroring, and purging
- Can select only changed files
- Significant functionality over copy

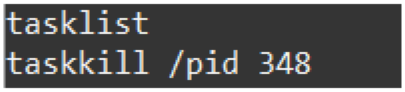
for History in Windows- doskey /history



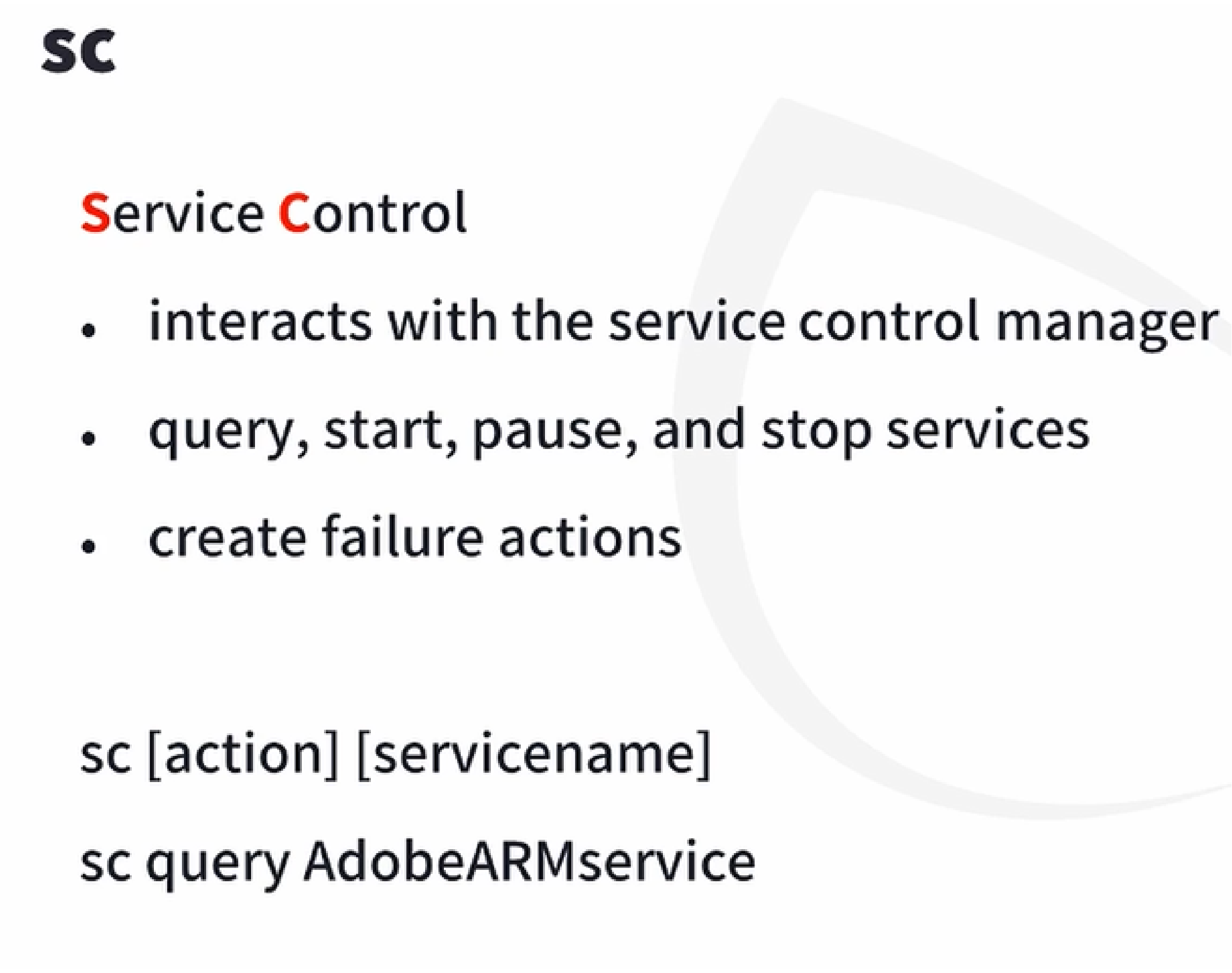
tasklist

- displays all running processes
- shows pid, memory usage, and name
- can be used to troubleshoot

for killing a process and showing trasklist



```
tasklist
taskkill /pid 348
```

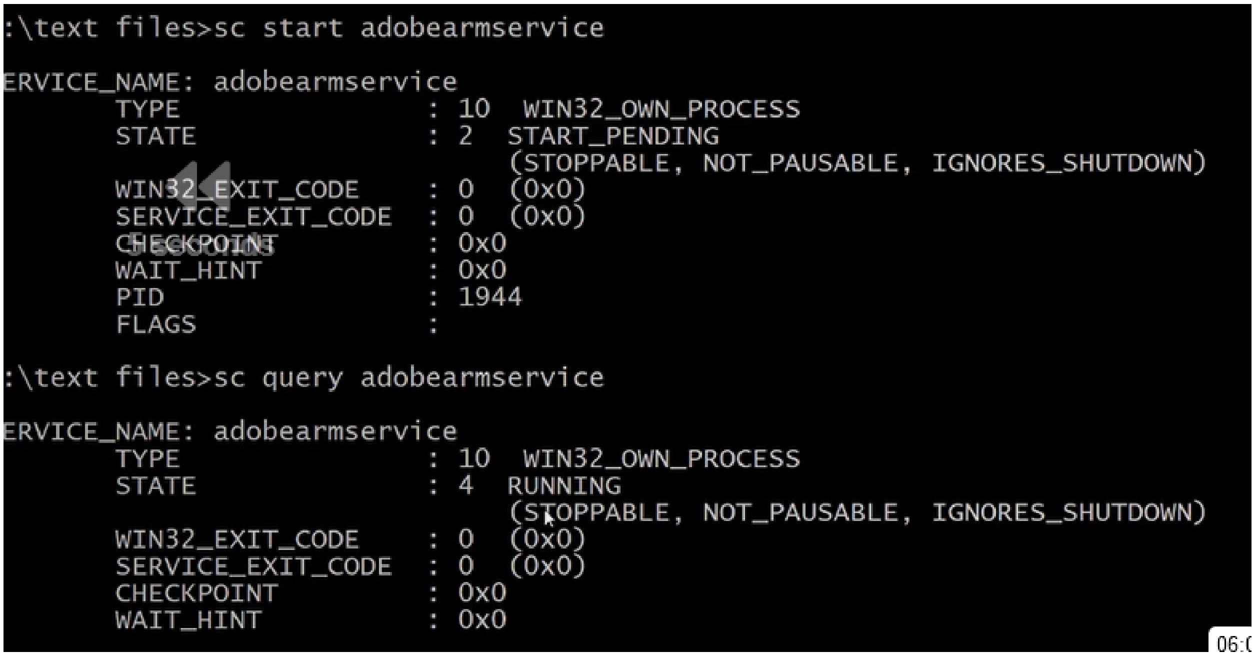


sc

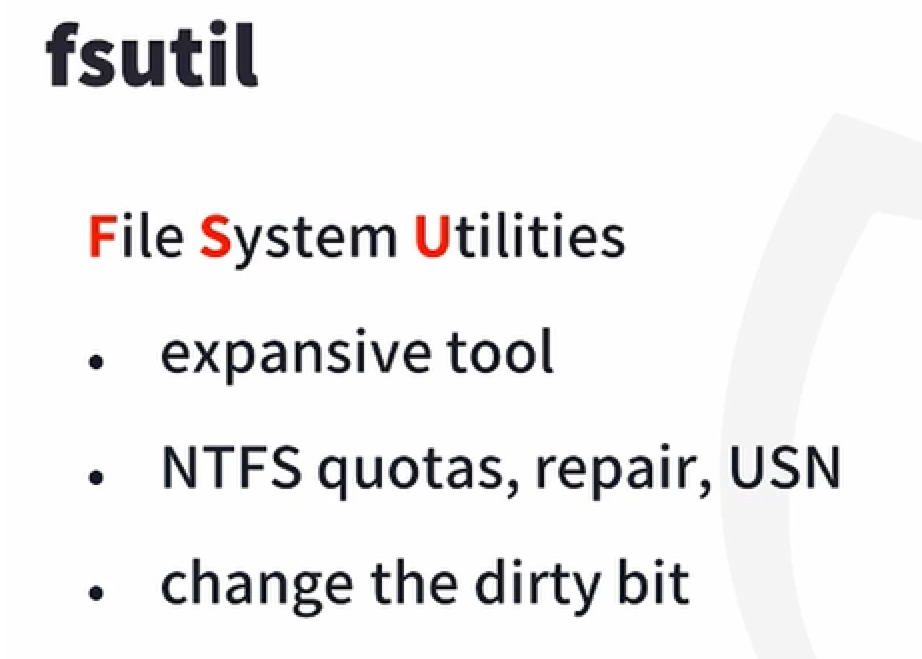
Service Control

- interacts with the service control manager
- query, start, pause, and stop services
- create failure actions

```
sc [action] [servicename]
sc query AdobeARMservice
```



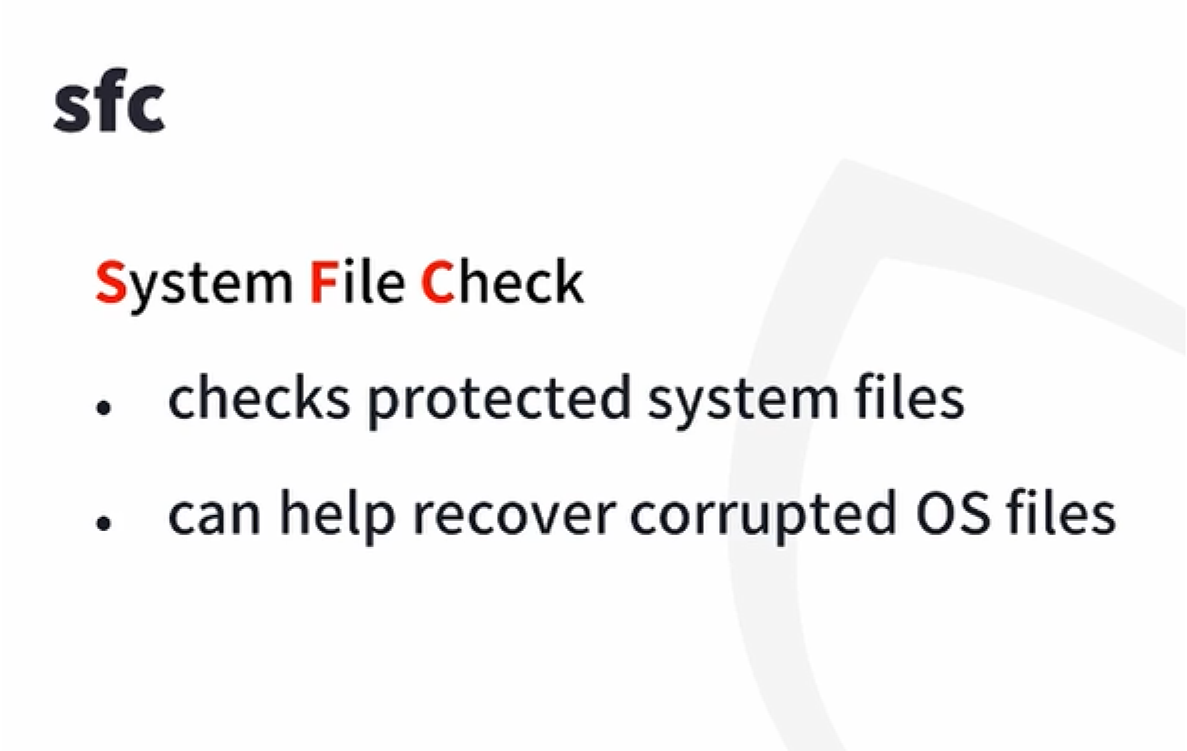
```
:\text files>sc start adobearmservice

ERVICE_NAME: adobearmservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 1944
        FLAGS              :

:\text files>sc query adobearmservice

ERVICE_NAME: adobearmservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```



fsutil

File **S**ystem **U**tilities

- expansive tool
- NTFS quotas, repair, USN
- change the dirty bit

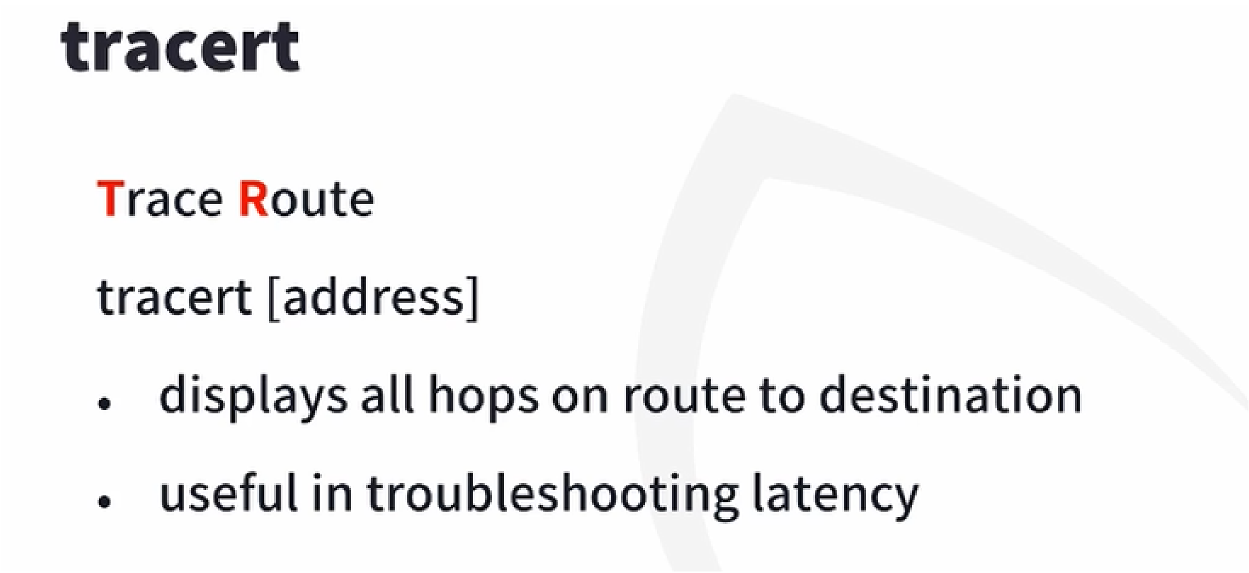


sfc

System **F**ile **C**heck

- checks protected system files
- can help recover corrupted OS files

FOr troubleshooting for network and for latency



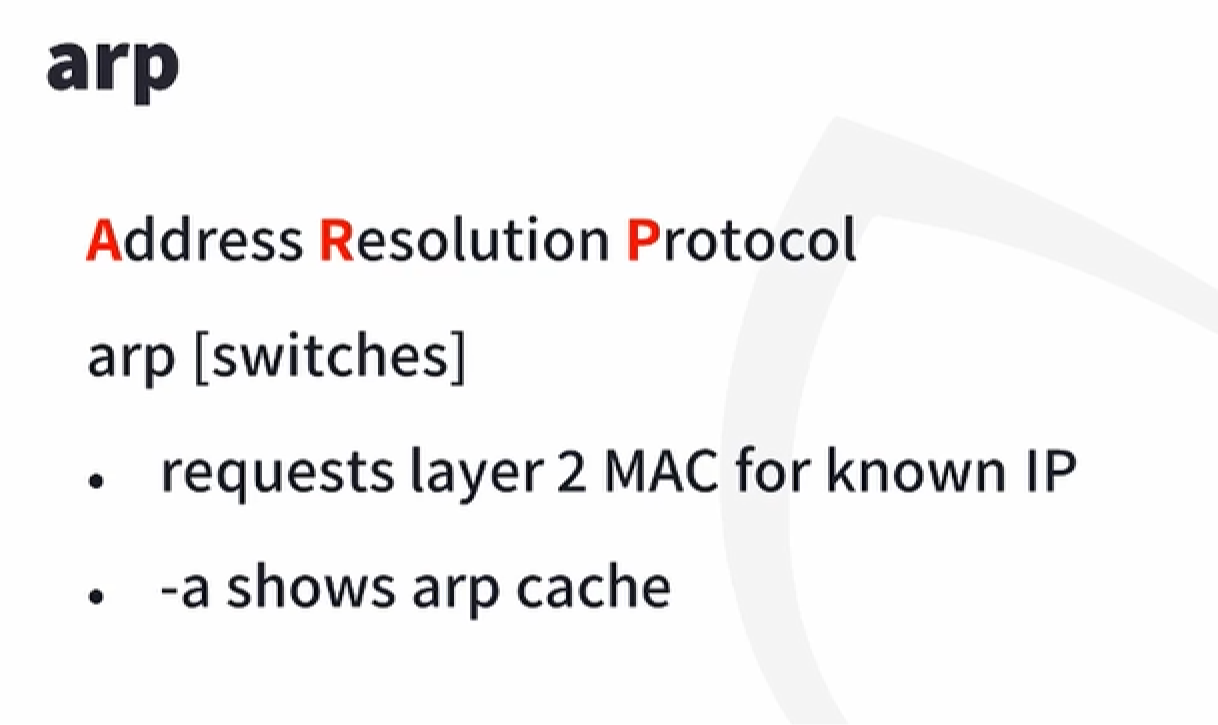
tracert

Trace **R**oute

tracert [address]

- displays all hops on route to destination
- useful in troubleshooting latency

DYNAMIC host configuration Protocol

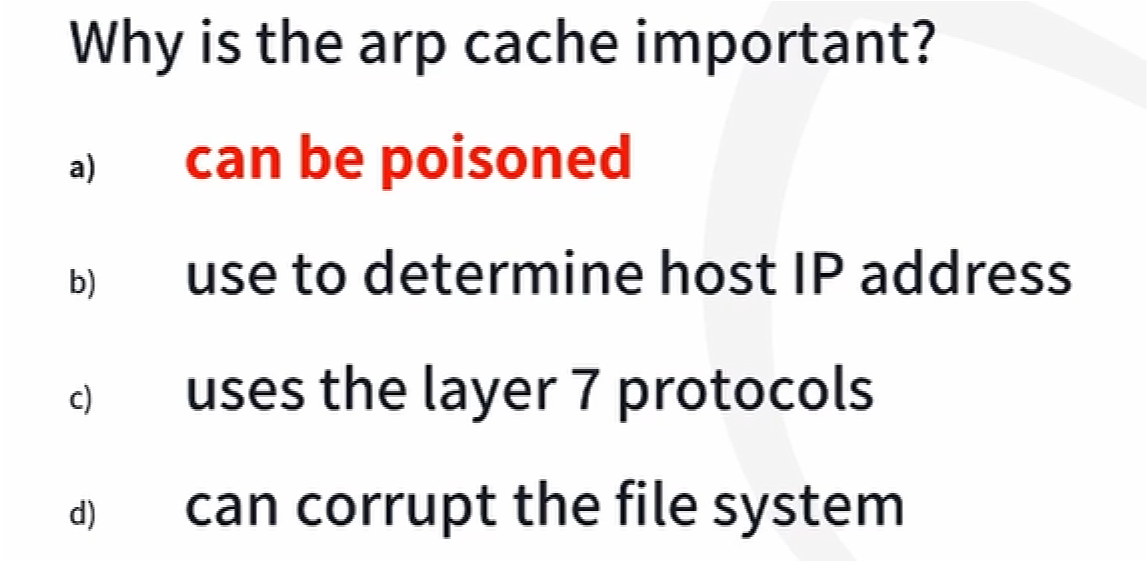


arp

Address Resolution Protocol

arp [switches]

- requests layer 2 MAC for known IP
- -a shows arp cache



Why is the arp cache important?

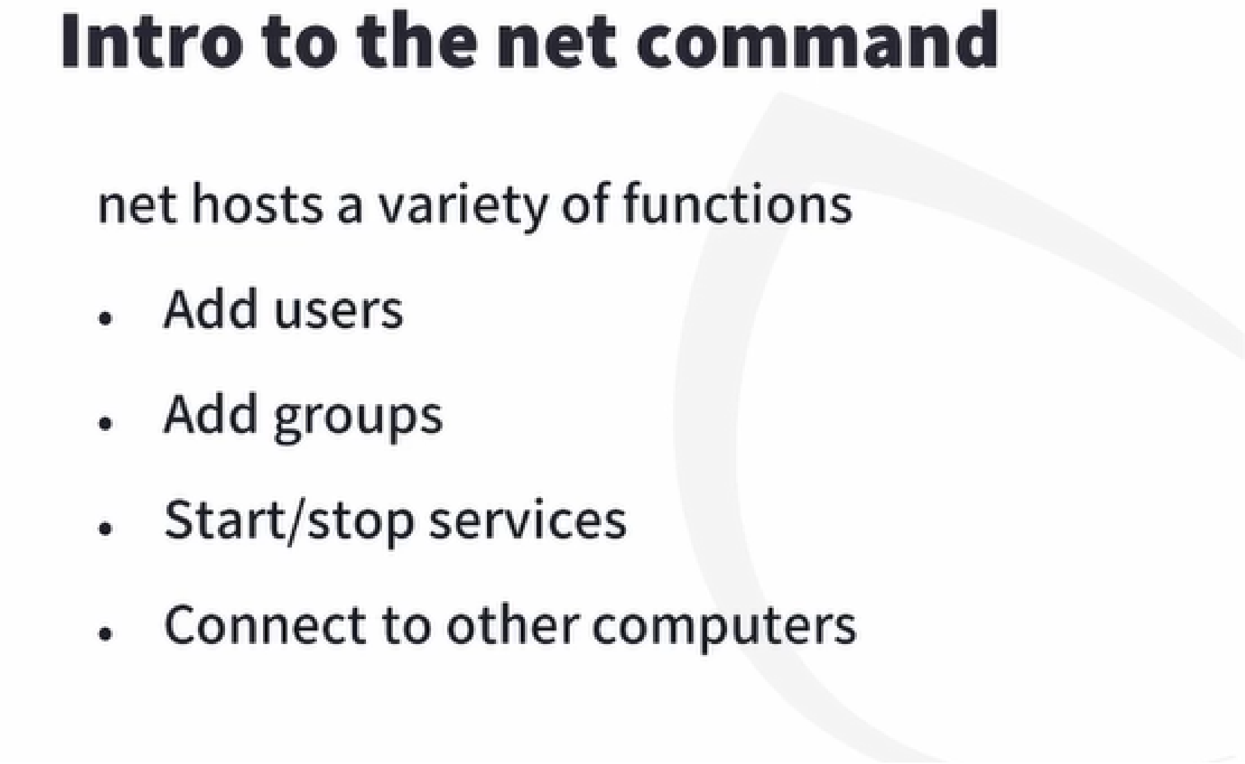
a) **can be poisoned**

b) use to determine host IP address

c) uses the layer 7 protocols

d) can corrupt the file system

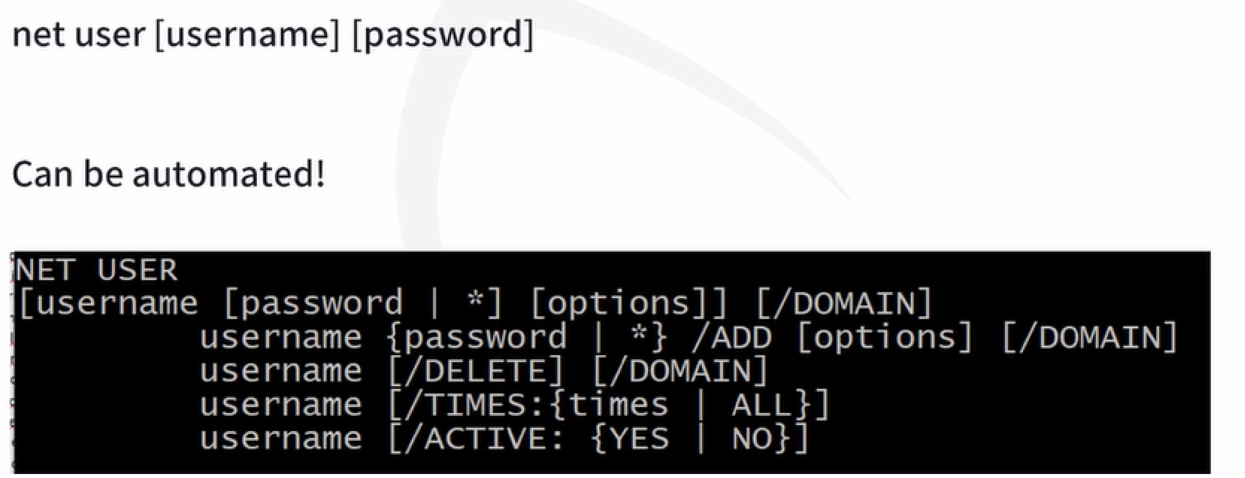
Net Command



Intro to the net command

net hosts a variety of functions

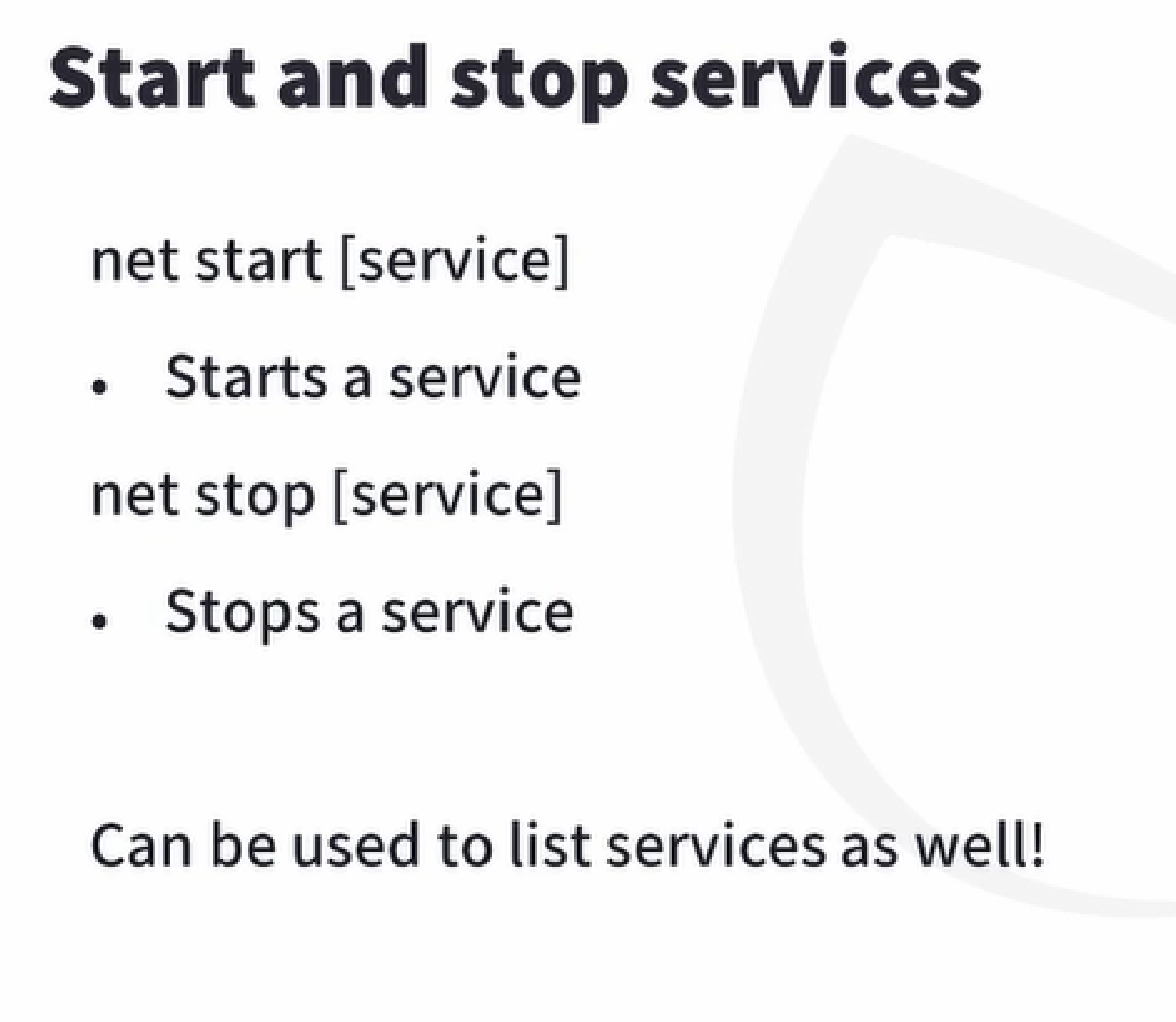
- Add users
- Add groups
- Start/stop services
- Connect to other computers



net user [username] [password]

Can be automated!

```
NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]
```



Start and stop services

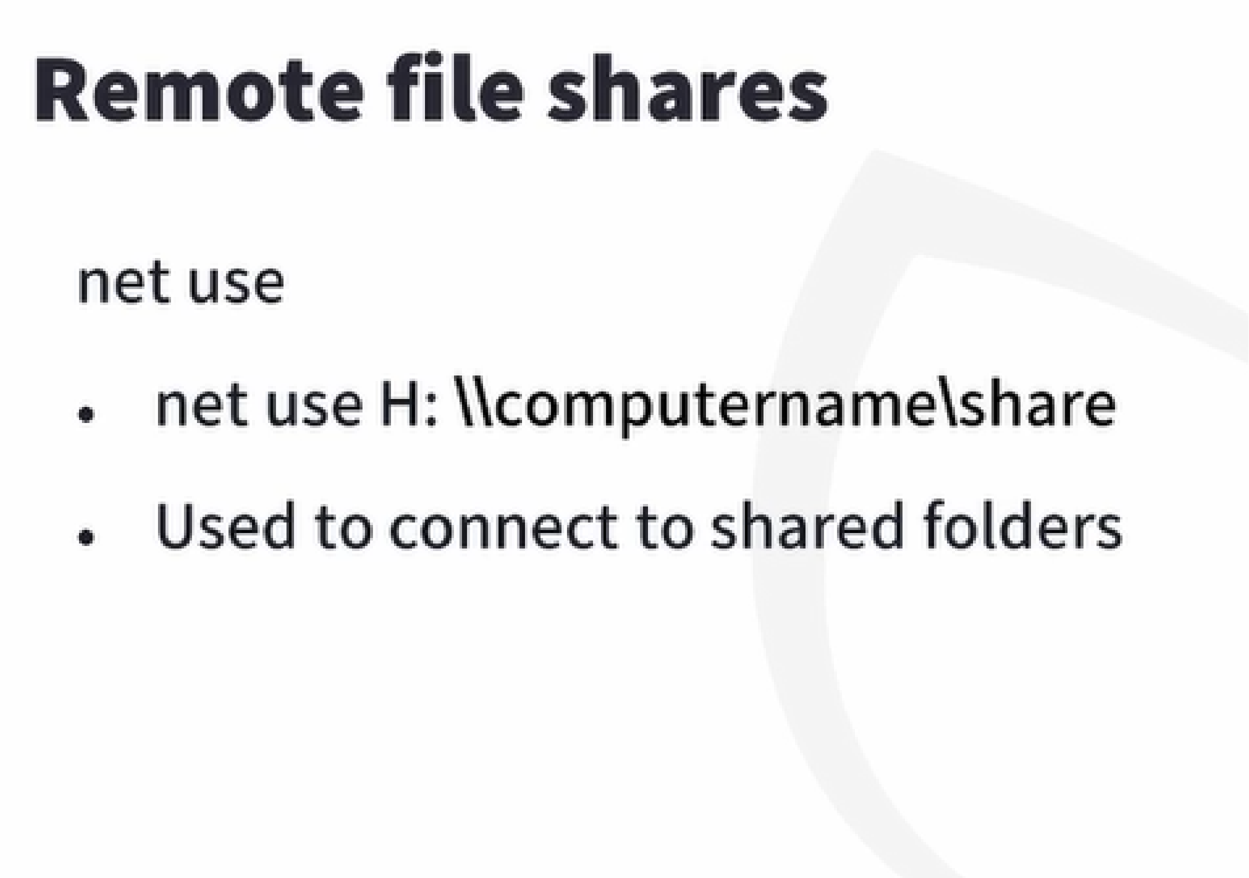
net start [service]

- Starts a service

net stop [service]

- Stops a service

Can be used to list services as well!



Remote file shares

net use

- net use H: \\computername\share
- Used to connect to shared folders

Advanced piping and ampersands in windows

Shell Scripting In Linux