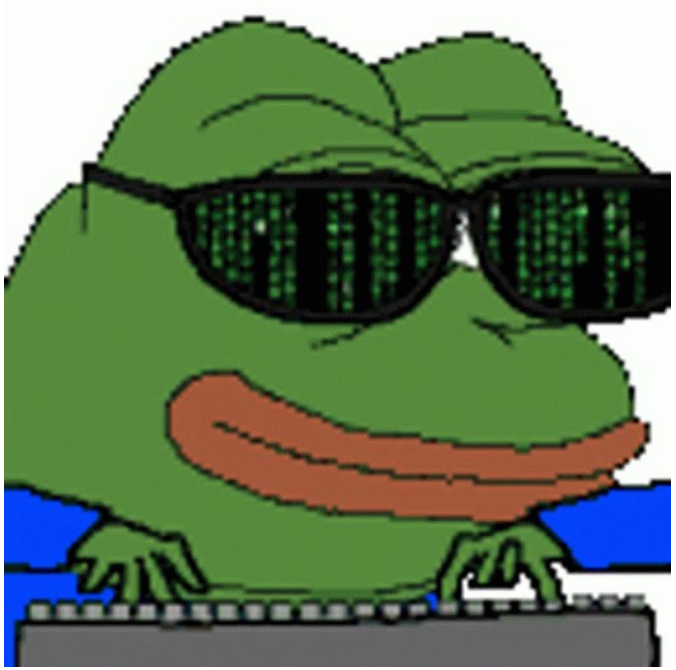
Linux Operations Basics: Part 5 Filesystems and Permissions

Class:
Linux OS Operations

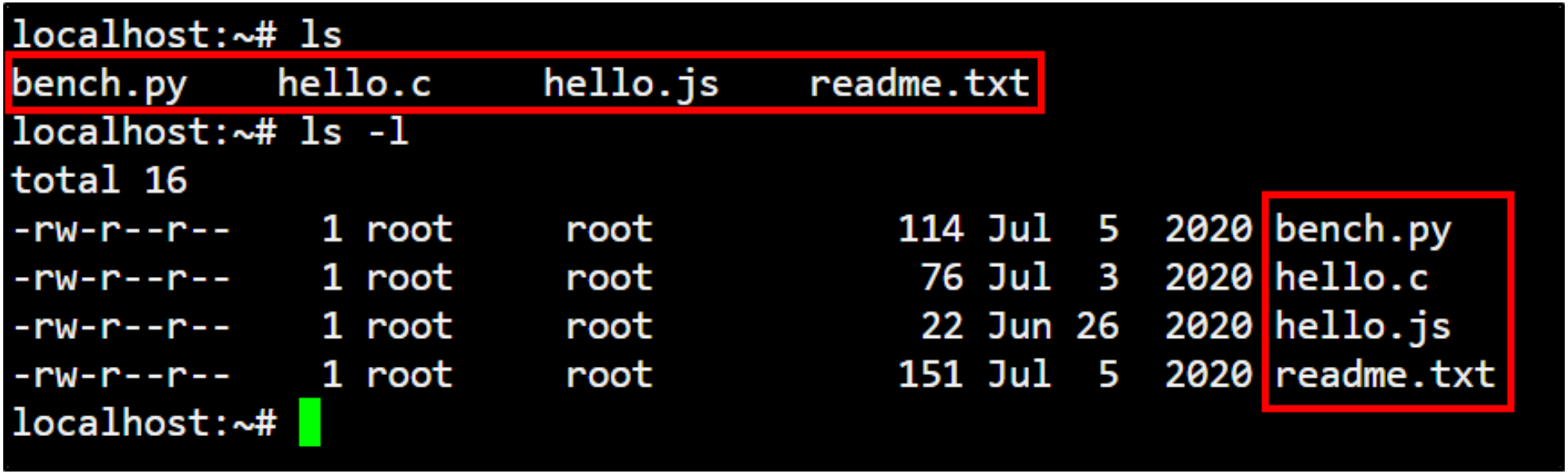
Workshop Number:
AS-LIN-05

Document Version:
1.2

Special Requirements:
None

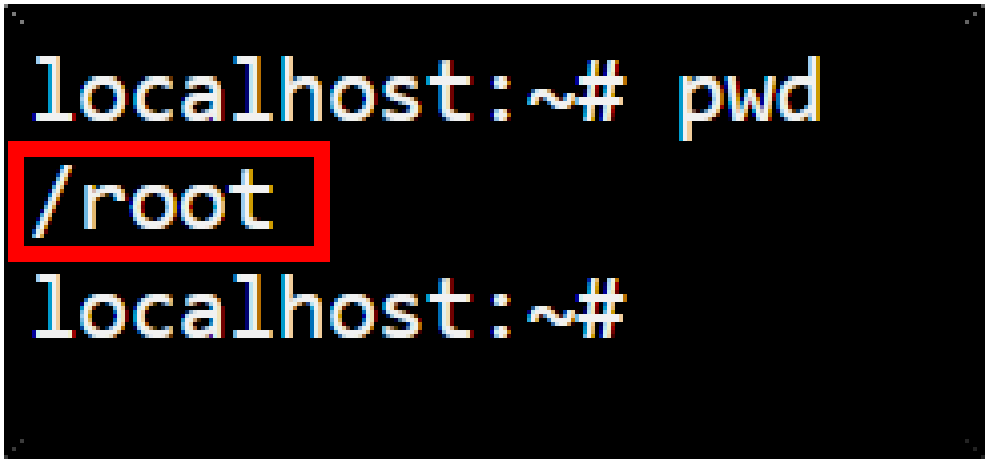


LS command: list directory contents



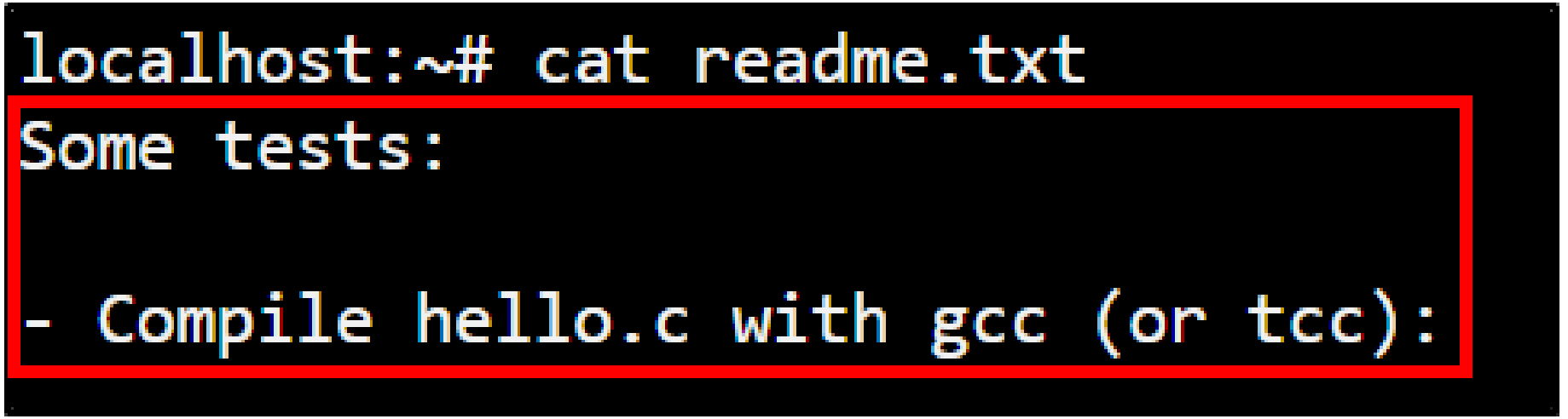
The LS command lists out the current directory's contents. It's often used with the -l switch to output in list form, or with the -a switch to output hidden files as well

PWD command:
print working directory



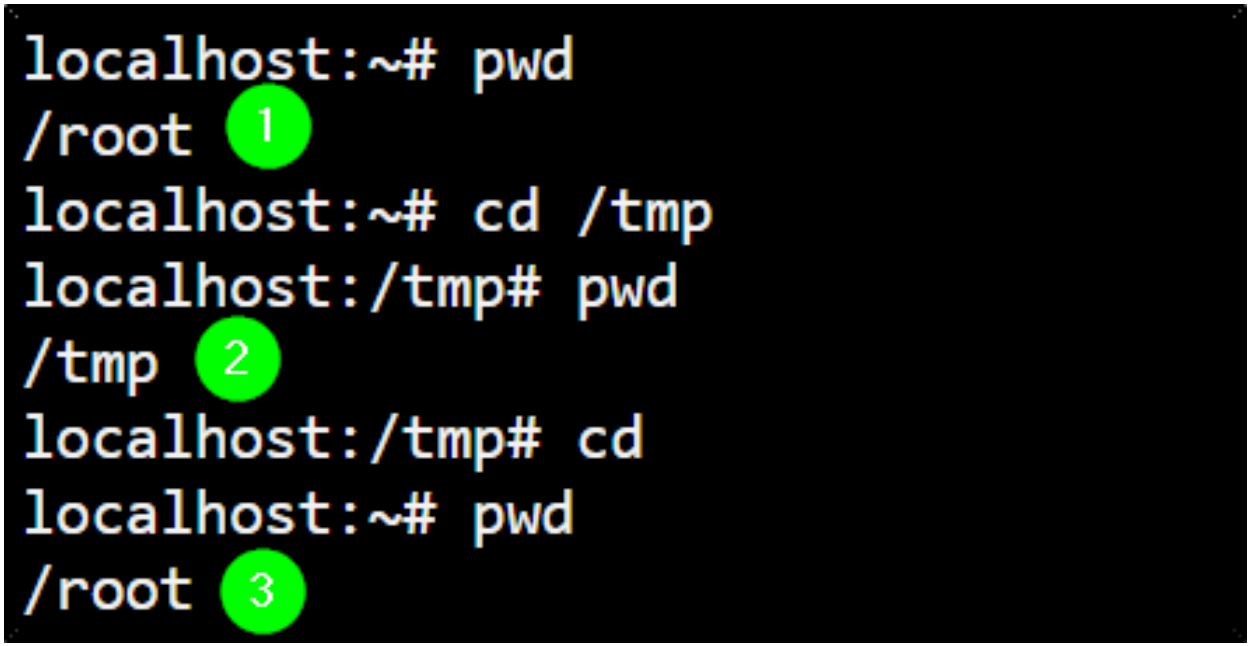
The PWD command outputs our current (working) directory. When we see a slash in front of a name in Linux, we know that's a directory name

CAT command:
read file contents



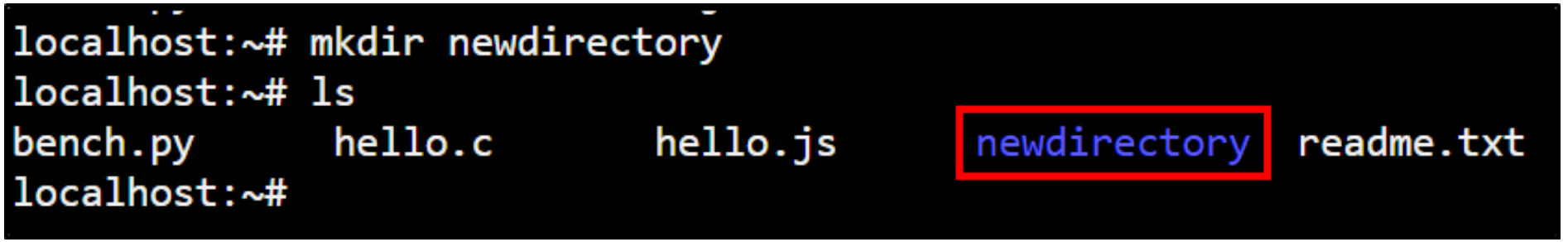
The CAT command is used to read file contents

CD command:
change working directory



The CD command is used to change our current (working) directory. If we use CD by itself, it will send us to our home directory

MKDIR command: create a new directory



The MKDIR command is used to create new directories. We usually can't create directories outside of our home directory or the /tmp directory

WGET command: download a file

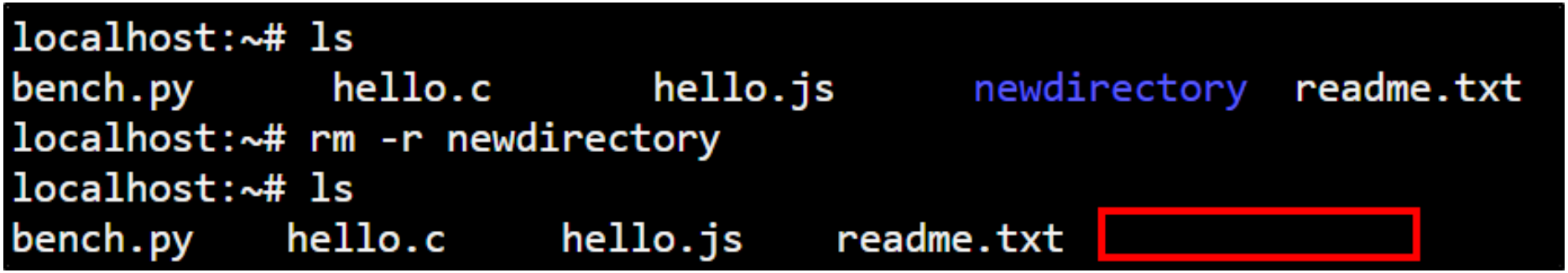
```
theshyhat-picoctf@webshell:~/obedientcat$ wget https://mercury.picoctf.net/static/217686fc11d733b80be62dcfc
fca6c75/flag
--2024-07-31 18:07:10--  https://mercury.picoctf.net/static/217686fc11d733b80be62dcfcfca6c75/flag
Resolving mercury.picoctf.net (mercury.picoctf.net)... 18.189.209.142
Connecting to mercury.picoctf.net (mercury.picoctf.net)|18.189.209.142|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 34 [application/octet-stream]
Saving to: 'flag'

flag                        100%[=======================================>]      34  --.-KB/s    in 0s

2024-07-31 18:07:10 (13.6 MB/s) - 'flag' saved [34/34]
```

The WGET command is used to download files. We usually can't download files outside of our home directories or the /tmp directory

RM command:
delete files or directories



The RM command is used to delete files or directories. Directories that aren't empty can't be deleted unless we use the -r switch.

NC command:
connect to remote server

```
nc jupiter.challenges.picoctf.org 4427
```

The NC (Netcat) command is used to connect to remote servers (other internet connected computers).

NC command:
connect to remote server

```
nc jupiter.challenges.picoctf.org 4427
```

To connect using netcat, we need to know the address of the server to connect to, and the port number.

NC command:
connect to remote server

```
nc jupiter.challenges.picoctf.org 4427
```

The NC command is similar to the SSH command, but NC is an older command.

GREP command:
delete files or directories

```
theshyhat-picoctf@webshell:~$ nc jupiter.challenges.picoctf.org 4427 | grep flag
Again, I really don't think this is a flag
Not a flag either
Not a flag either
Not a flag either
```

The GREP command is used to search for text inside of output or inside of files.

FIND command: searching for files

```
find . -name uber-secret.txt
./.secret/deeper_secrets/deepest_secrets/uber-secret.txt
```

The FIND command is used to search for files in the filesystem. One way to search is by the name of the file.

Command Piping:
passing output to another command

```
nc jupiter.challenges.picoctf.org 4427 | grep pico
```

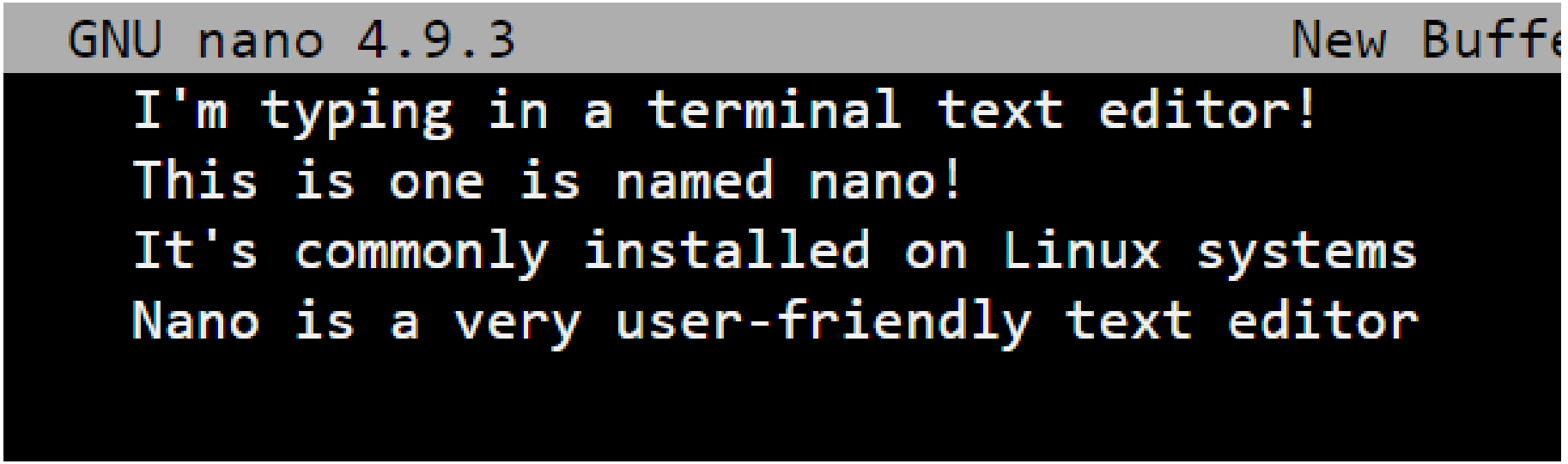
In Linux, command piping is the process of passing the output of one command into the input of a second command.

Command Piping:
passing output to another command

```
nc jupiter.challenges.picoctf.org 4427 | grep pico
```

This is a very useful feature, because it allows commands to be chained together to achieve a lot of flexible output.

Terminal Text Editors

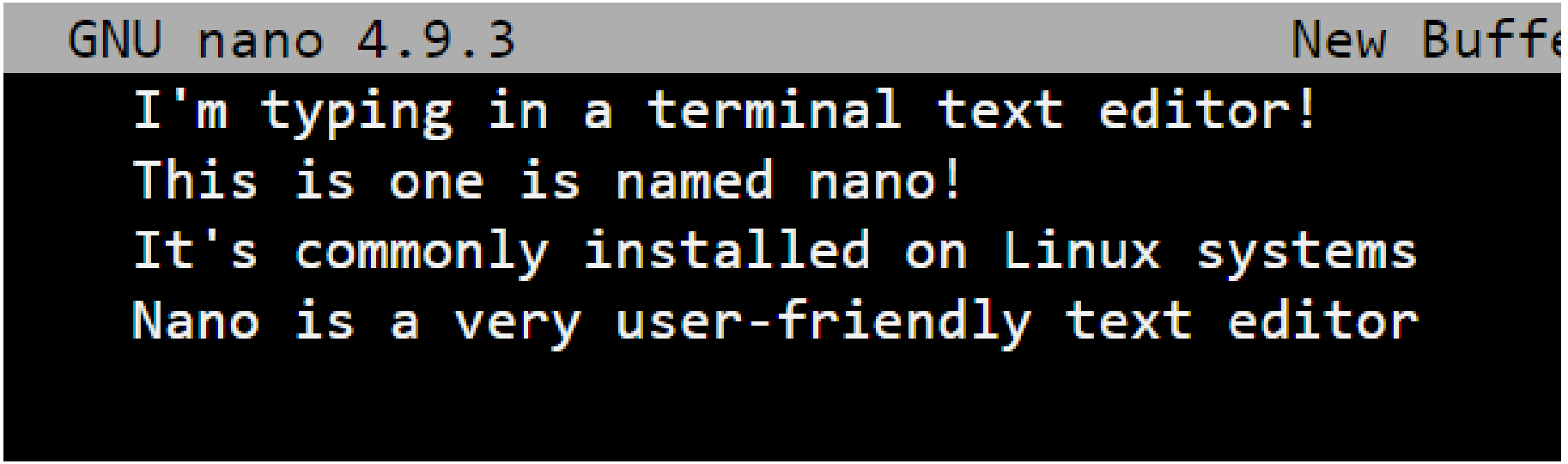


From time to time, we'll need to write new files or modify existing ones. To do so, we'll need to use Linux text editors.

Terminal Text Editors

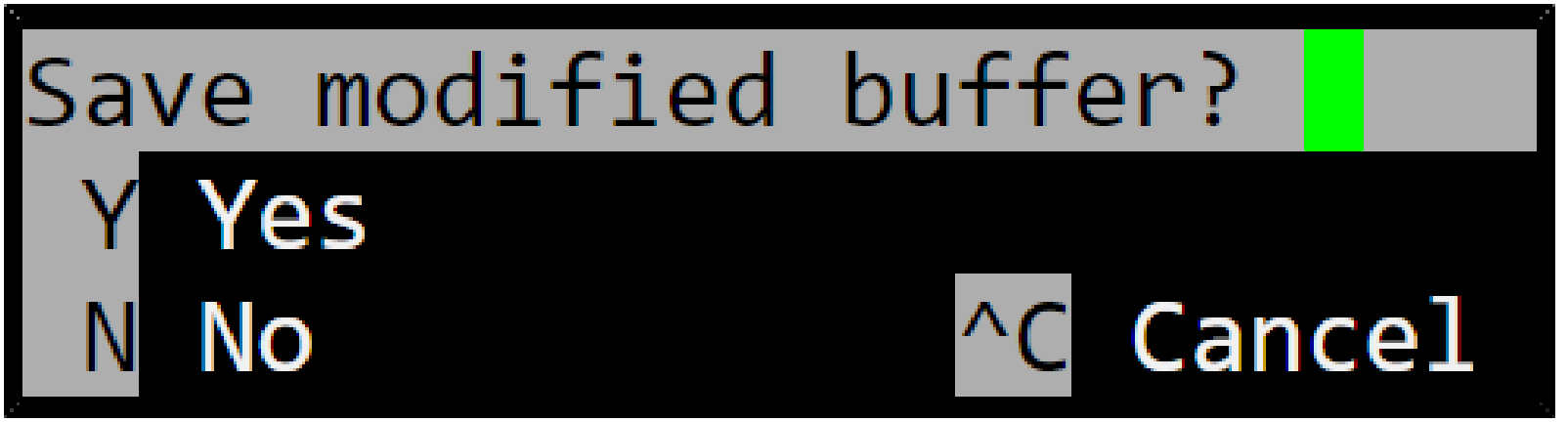
Two commonly installed text editors on Linux systems are Nano and Vim.

Nano Text Editor



Nano is the more straightforward and user-friendly of the two text editors.

Nano Text Editor



The most important command to know in the Nano text editor is the ` Ctrl + C `command, which lets us save the file and exit.

Base64 Command

The Base64 command encodes / decodes data according to the Base64 codec. It is often used to convert data for transmission across computer networks.

0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	I	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 Command

The characters used in Base 64 encoding are shown here. Note that all Base 64 encoded strings must consist of a number of characters that is divisible by 4.

0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	I	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64 Command

```
└─$ echo -n password | base64
cGFzc3dvcmQ=
```

In cases where an encoded string is not divisible by 4, the encoding process will “pad out” the string with equal symbols until the string is divisible by 4.

Base64 Command (decode)

1 – The command itself

2 – The decode switch

3 – The file to be operated upon

The Help Flag

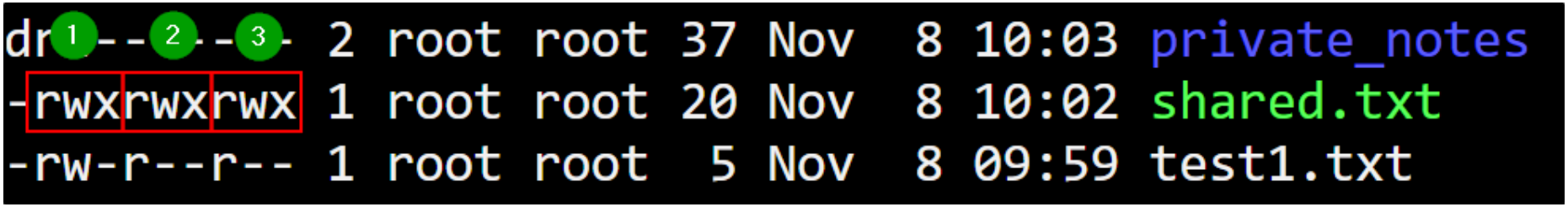
```
[root@localhost ~]# cat --help
Usage: cat [OPTION]... [FILE]...
Concatenate FILE(s) to standard output.

With no FILE, or when FILE is -, read standard input.

  -A, --show-all           equivalent to -vET
  -b, --number-nonblank    number nonempty output lines, overrides -n
```

The **--help** flag can be used as part of any command to return a relatively brief explanation as to how to use the command.

Linux File Permissions



Each file in the Linux filesystem has different (r)ead, (w)rite, and e(x)ecute permissions, depending on whether a user is (1), the file owner, (2), part of a certain group, or (3), any other user.

Noteworthy Linux File Directories

/etc where system files (user passwords) are stored

/var where log files and database files are stored

/root typically the folder with the most secure access

/tmp all files here are deleted on a regular basis

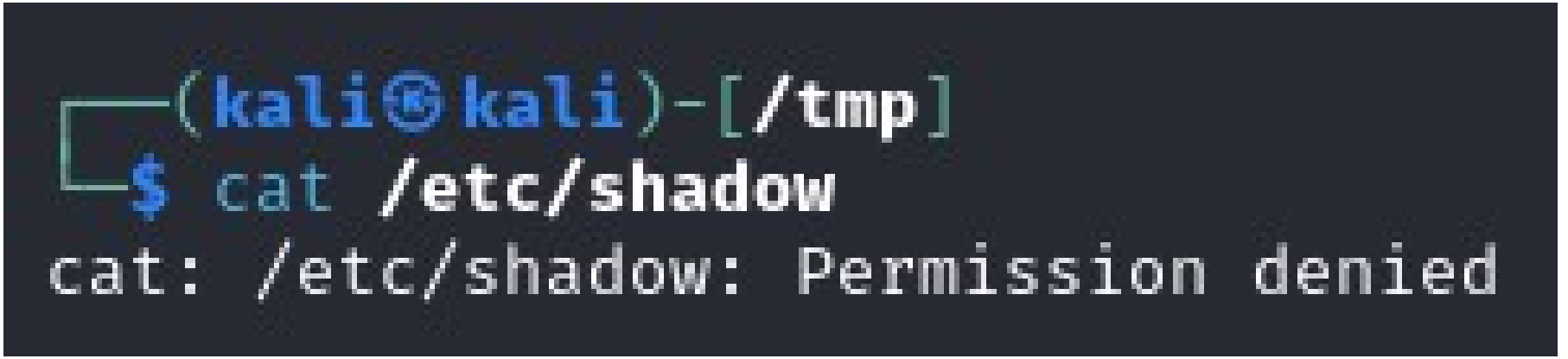
/home where individual user account files are stored

Sudo – The Super Command

```
[root@localhost ~]# sudo --help
sudo - execute a command as another user
```

The **sudo** command can be added to any other command, and it allows the command to be executed in the context of the root user.

Sudo – The Super Command



Sudo needs to be used whenever we try to access or modify systems files or directories.

Sudo – The Super Command

```
└─$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bi
n\:/sbin\:/bin,
    use_pty

User kali may run the following commands on kali:
    (ALL : ALL) ALL
```

Generally, only system administrator accounts should be allowed to use **sudo** with all commands.

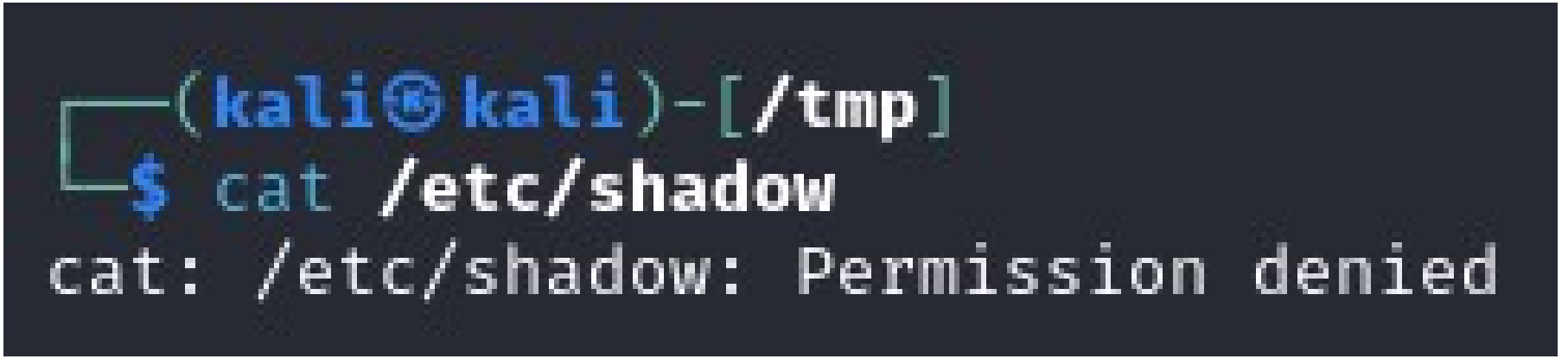
Sudo – The Super Command

```
└─$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bi
n\:/sbin\:/bin,
    use_pty

User kali may run the following commands on kali:
    (ALL : ALL) ALL
```

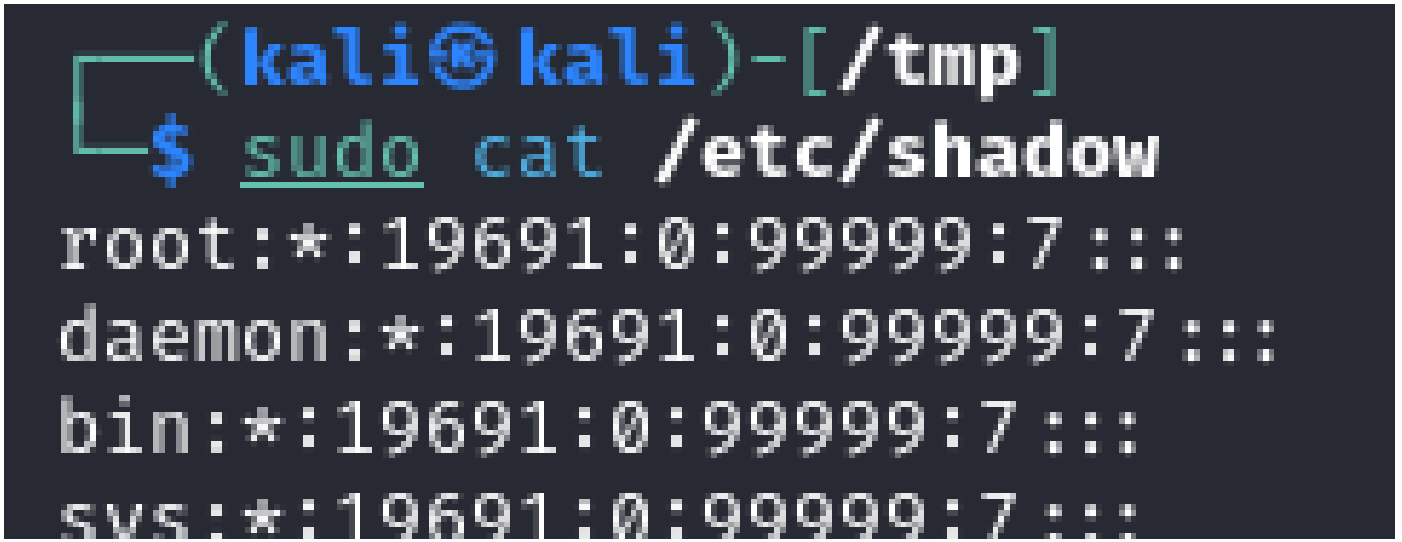
But some systems have users who are able to use **sudo** with a specific command for some reason or another.

Sudo – The Super Command



If you ever try to run a command as a regular user, and you see the permission denied message...

Sudo – The Super Command



You can usually retry that command with sudo to execute it successfully.

Sudo – The Super Command

```
┌──(kali㉿kali)-[/tmp]
└─$ rm -rf /
rm: it is dangerous to operate recursively on '/'
rm: use --no-preserve-root to override this failsafe
```

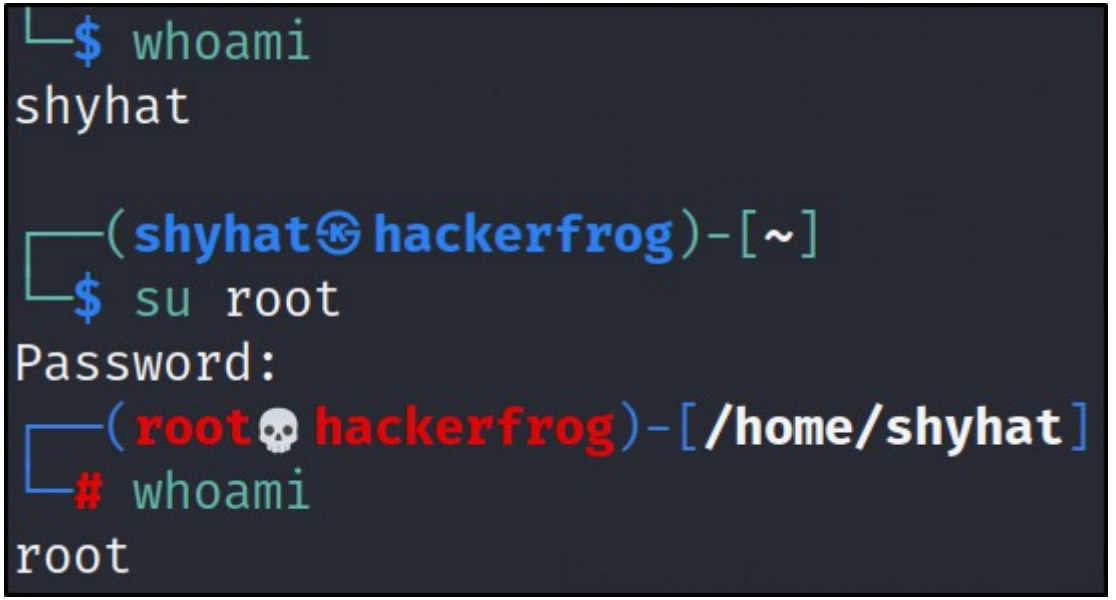
If we need to use sudo, we should always try to understand why we need to use it...

Sudo – The Super Command

```
┌──(kali㉿kali)-[/tmp]
└─$ rm -rf /
rm: it is dangerous to operate recursively on '/'
rm: use --no-preserve-root to override this failsafe
```

Since it means we're interacting with sensitive files or directories.

Su Command



The **su** (switch user) command is used to switch between active user accounts during a CLI session. When using the **su** command, the password of the user account being accessed must be supplied.