BIZIMANA Olivier (27582)

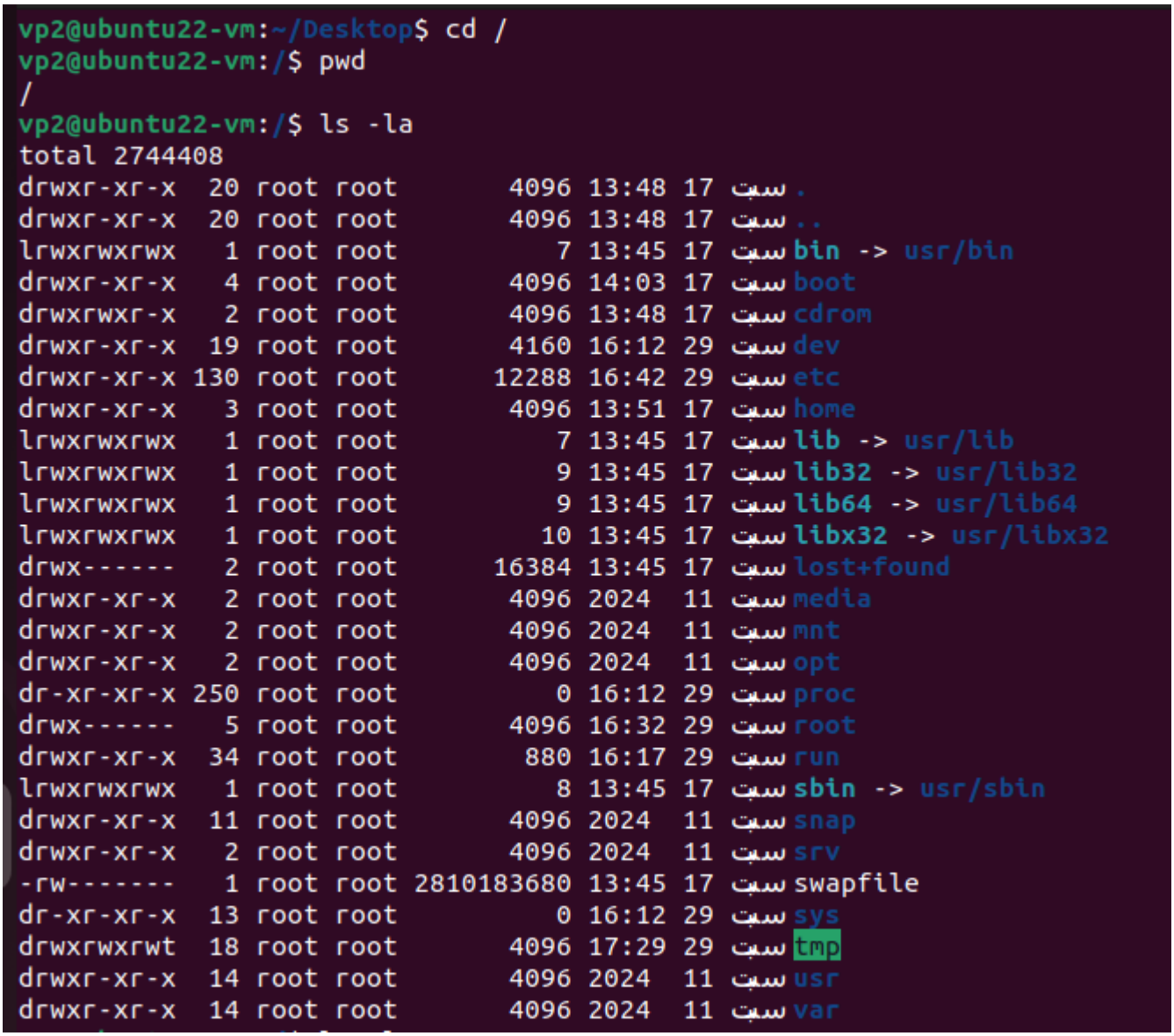
On 30 September 2025

Introduction to Linux

Assignment 2

1. Navigate to the root directory and Identify directories.

- **/bin:** Essential binaries; attackers replace for malicious execution.
- **/etc:** Config files; attackers modify for privilege escalation.
- **/var:** Variable data like logs; attackers erase evidence.
- **/usr:** Secondary binaries (/usr/bin); similar to /bin, attackers target for non-essential tools.
- **/tmp:** Temporary files; attackers use for staging malware, as it's writable.
- **/opt:** Add-on software; attackers hide custom tools here.
- **/boot:** Boot files (kernel); attackers modify for rootkits.
- **/home:** User homes; attackers target for user-level persistence (e.g., .ssh keys).



2. Create the Exact Structure

mkdir -p ~/projects/{client_work/{web/{frontend,backend,database},mobile/{ios,android}},personal/{experiments,archive},shared/{templates,resources}}

```
vp2@ubuntu22-vm:~/Desktop$ cd ~
vp2@ubuntu22-vm:~$ mkdir -p projects/{client_work/{web/{frontend,backend,database},mobile/{ios,android}},personal/{experiments,archive},shared/{templates,resources}}
vp2@ubuntu22-vm:~$ ls -R projects
projects:
client_work  personal  shared

projects/client_work:
mobile  web

projects/client_work/mobile:
android  ios

projects/client_work/mobile/android:

projects/client_work/mobile/ios:

projects/client_work/web:
backend  database  frontend

projects/client_work/web/backend:

projects/client_work/web/database:

projects/client_work/web/frontend:

projects/personal:
archive  experiments

projects/personal/archive:

projects/personal/experiments:

projects/shared:
resources  templates
```

3. Navigate Without Absolute Paths

First, cd ../../../personal/experiments and then pwd

Second, cd ../../shared/templates and then pwd

Third, cd ../../client_work/web/frontend and then pwd

```
vp2@ubuntu22-vm:~/Desktop$ mkdir -p projects/{client_work/web/frontend,personal/experiments,shared/templates}
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client-work/web/frontend
bash: cd: /home/vp2/projects/client-work/web/frontend: No such file or directory
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ cd ../../../personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ pwd
/home/vp2/projects/personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ cd ../../shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ pwd
/home/vp2/projects/shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ cd ../../client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$
```

4. Create Realistic Web Project Structure

First, mkdir web_project

Second, touch web_project/{index,about,contact}.html web_project/page_{001..012}.html

Third, touch web_project/{main,util,config,app,helper,setup}_script.js

, touch web_project/{a,b,c,d}{1..5}.{bak,tmp,old,save}

Seventh, ls web_project/

```
vp2@ubuntu22-vm:~/Desktop$ cd ~
vp2@ubuntu22-vm:~$ mkdir web_project
vp2@ubuntu22-vm:~$ cd web_project
vp2@ubuntu22-vm:~/web_project$ touch{index,about,contact}.html                  page_{001..012}.html
touchindex.html: command not found
vp2@ubuntu22-vm:~/web_project$ touch {index,about,contact}.html                  page_{001..012}.html
vp2@ubuntu22-vm:~/web_project$ mkdir css && touch css/{main,reset,theme_{light,dark},mobile,table,desktop,print}.css
vp2@ubuntu22-vm:~/web_project$ mkdir js && touch js/{app_script,main_util,api_config,legacy_script,data_util,env_config}.js
vp2@ubuntu22-vm:~/web_project$ mkdir backups
vp2@ubuntu22-vm:~/web_project$ touch backups/{a{1..5}.bak,{1..5}.tmp,c{1..5}.old,d{1..5}.gz}
vp2@ubuntu22-vm:~/web_project$ ls -R
.:
about.html    index.html     page_003.html  page_007.html  page_011.html
backups       js             page_004.html  page_008.html  page_012.html
contact.html  page_001.html  page_005.html  page_009.html
css           page_002.html  page_006.html  page_010.html

./backups:
1.tmp  3.tmp  5.tmp   a2.bak  a4.bak  c1.old  c3.old  c5.old  d2.gz  d4.gz
2.tmp  4.tmp  a1.bak  a3.bak  a5.bak  c2.old  c4.old  d1.gz   d3.gz  d5.gz

./css:
desktop.css  mobile.css  reset.css  theme_dark.css
main.css     print.css   table.css  theme_light.css

./js:
api_config.js  data_util.js   legacy_script.js
app_script.js  env_config.js  main_util.js
vp2@ubuntu22-vm:~/web_project$
```

5. Use Wildcards for Cluttered Directory

First, mkdir archive desktop

Second, mv page_???.html archive /

Third, ls archive /

Fourth, and some find css/

```
vp2@ubuntu22-vm:~/web_project$ mkdir archive desktop
vp2@ubuntu22-vm:~/web_project$ mv page_???.html archive/
vp2@ubuntu22-vm:~/web_project$ ls archive/
page_001.html  page_004.html  page_007.html  page_010.html
page_002.html  page_005.html  page_008.html  page_011.html
page_003.html  page_006.html  page_009.html  page_012.html
vp2@ubuntu22-vm:~/web_project$ find css/ -name "*.css" ! -name "*mobile*" ! -name "*tablet*" -exec cp {} desktop/ \;
vp2@ubuntu22-vm:~/web_project$ ls desktop/
desktop.css  print.css  table.css       theme_light.css
main.css     reset.css  theme_dark.css
vp2@ubuntu22-vm:~/web_project$ mv css/table.css css/table.css
mv: 'css/table.css' and 'css/table.css' are the same file
vp2@ubuntu22-vm:~/web_project$ mv css/table.css css/tablet.css
vp2@ubuntu22-vm:~/web_project$ ls desktop/
desktop.css  print.css  table.css       theme_light.css
main.css     reset.css  theme_dark.css
vp2@ubuntu22-vm:~/web_project$ ls css/*.css
css/desktop.css  css/mobile.css  css/reset.css   css/theme_dark.css
css/main.css     css/print.css   css/tablet.css  css/theme_light.css
vp2@ubuntu22-vm:~/web_project$ rm desktop/*.css
vp2@ubuntu22-vm:~/web_project$ find css/ -name "*.css" ! -name "*mobile*" ! -name "*tablet*" -exec cp {} desktop/ \;
vp2@ubuntu22-vm:~/web_project$ ls desktop/
desktop.css  main.css  print.css  reset.css  theme_dark.css  theme_light.css
vp2@ubuntu22-vm:~/web_project$
```

6. Brace Expansion for File Naming

touch log_2024-{01..03}-{01..31}.txt

touch {web,api,db}_{dev,stg,prod}.conf touch {A,B,C}{10,11,12}_{input,output}.txt

ls

```
vp2@ubuntu22-vm:~/Desktop$ cd /
vp2@ubuntu22-vm:/$ pwd
/
vp2@ubuntu22-vm:/$ ls -la
total 2744408
drwxr-xr-x  20 root root       4096 13:48 17 سبت .
drwxr-xr-x  20 root root       4096 13:48 17 سبت ..
lrwxrwxrwx   1 root root          7 13:45 17 سبت bin -> usr/bin
drwxr-xr-x   4 root root       4096 14:03 17 سبت boot
drwxrwxr-x   2 root root       4096 13:48 17 سبت cdrom
drwxr-xr-x  19 root root       4160 16:12 29 سبت dev
drwxr-xr-x 130 root root      12288 16:42 29 سبت etc
drwxr-xr-x   3 root root       4096 13:51 17 سبت home
lrwxrwxrwx   1 root root          7 13:45 17 سبت lib -> usr/lib
lrwxrwxrwx   1 root root          9 13:45 17 سبت lib32 -> usr/lib32
lrwxrwxrwx   1 root root          9 13:45 17 سبت lib64 -> usr/lib64
lrwxrwxrwx   1 root root         10 13:45 17 سبت libx32 -> usr/libx32
drwx------   2 root root      16384 13:45 17 سبت lost+found
drwxr-xr-x   2 root root       4096 2024  11 سبت media
drwxr-xr-x   2 root root       4096 2024  11 سبت mnt
drwxr-xr-x   2 root root       4096 2024  11 سبت opt
dr-xr-xr-x 250 root root          0 16:12 29 سبت proc
drwx------   5 root root       4096 16:32 29 سبت root
drwxr-xr-x  34 root root        880 16:17 29 سبت run
lrwxrwxrwx   1 root root          8 13:45 17 سبت sbin -> usr/sbin
drwxr-xr-x  11 root root       4096 2024  11 سبت snap
drwxr-xr-x   2 root root       4096 2024  11 سبت srv
-rw-------   1 root root 2810183680 13:45 17 سبت swapfile
dr-xr-xr-x  13 root root          0 16:12 29 سبت sys
drwxrwxrwt  18 root root       4096 17:29 29 سبت tmp
drwxr-xr-x  14 root root       4096 2024  11 سبت usr
drwxr-xr-x  14 root root       4096 2024  11 سبت var
```

7. Line Endings Comparison

printf "This is a test\nLine2\nLine3\n" > linux.txt

printf "This is a test\r\nLine2\r\nLine3\r\n" > windows.txt

diff linux.txt windows.txt cmp linux.txt windows.txt

comm linux.txt windows.txt

```
Need to get 384 kB of archives.
After this operation, 1,367 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 dos2unix amd64 7.4.2-2 [384 kB]
Fetched 384 kB in 6s (67.8 kB/s)
Selecting previously unselected package dos2unix.
(Reading database ... 208514 files and directories currently installed.)
Preparing to unpack .../dos2unix_7.4.2-2_amd64.deb ...
Unpacking dos2unix (7.4.2-2) ...
Setting up dos2unix (7.4.2-2) ...
Processing triggers for man-db (2.10.2-1) ...
vp2@ubuntu22-vm:~/Desktop$ echo -e "Line 1\nLine 2\nLine 3" > linux_file.txt
vp2@ubuntu22-vm:~/Desktop$ cp linux_file.txt windows_file.txt && unix2dos windows_file.txt
unix2dos: converting file windows_file.txt to DOS format...
vp2@ubuntu22-vm:~/Desktop$ diff linux_file.txt windows_file.txt
1,3c1,3
< Line 1
< Line 2
< Line 3
---
> Line 1
> Line 2
> Line 3
vp2@ubuntu22-vm:~/Desktop$ cmp linux-file.txt windows-file.txt
cmp: linux-file.txt: No such file or directory
vp2@ubuntu22-vm:~/Desktop$ cmp linux-file.txt windows_file.txt
cmp: linux-file.txt: No such file or directory
vp2@ubuntu22-vm:~/Desktop$ cmp linux_file.txt windows_file.txt
linux_file.txt windows_file.txt differ: byte 7, line 1
vp2@ubuntu22-vm:~/Desktop$ comm linux_file.txt windows_file.txt
Line 1
        Line 1
Line 2
        Line 2
Line 3
        Line 3
vp2@ubuntu22-vm:~/Desktop$
```

8. Security Audit with Find

mkdir -p test_env/{dir1,dir2,dir3,dir4,dir5}

touch test_env/dir1/file{1..5}

touch -m -d "2 days ago" test_env/dir1/file{1,2}

touch -m -d "50 days ago" test_env/dir1/file3

touch test_env/dir2/largefile

dd if=/dev/zero of=test_env/dir2/largefile bs=1k count=10

touch test_env/dir4/.hidden

sudo chown nobody test_env/dir1/file4

sudo chmod 666 test_env/dir5/worldwritable

find test_env -type f -size +$(find test_env type f -printf "%s\n" | awk '{sum+=$0; n++} END {print int(sum/n)}')c

```
vp2@ubuntu22-vm:~/Desktop$ mkdir find_test && cd find_test
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 10M large_file fallocate -l 50K average_file fallocate -l 1K small_file
fallocate: unexpected number of arguments
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 10M large_file
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 50K average_file
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 1K small_file
vp2@ubuntu22-vm:~/Desktop/find_test$ touch -d "3 days ago" old_file_3days_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ touch -d "1 day ago" old_file_1day_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ touch new_file_today
vp2@ubuntu22-vm:~/Desktop/find_test$ touch risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ chmod 666 risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ sudo chown root:root root_owned_file
[sudo] password for vp2:
chown: cannot access 'root_owned_file': No such file or directory
vp2@ubuntu22-vm:~/Desktop/find_test$ touch root_owned_file
vp2@ubuntu22-vm:~/Desktop/find_test$ sudo chown root:root root_owned_file
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir empty_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir hidden_only_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ touch hidden_only_dir/.hidden_file
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir normal_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ touch temp_report.tmp
vp2@ubuntu22-vm:~/Desktop/find_test$ touch config_old.bak
vp2@ubuntu22-vm:~/Desktop/find_test$ touch script~
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -mtime -3 -a -mtime +0
./old_file_1day_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f perm /0002
find: paths must precede expression: `perm'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -perm /0002
./risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \(-name "*.tmp" -o -name "*.bak" -o -name "*~"\)
find: paths must precede expression: `(-name'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \( -name "*.tmp" -o -name "*.bak" -o -name "*~"\)
find: invalid expression; I was expecting to find a ')' somewhere but did not see one.
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \( -name "*.tmp" -o -name "*.bak" -o -name "*~" \)
./config_old.bak
./temp_report.tmp
./script~
```

find test_env -mtime -3 -mtime +1

find test_env -type d -empty -o \(-type d -name ".*" -not -empty \)

find test_env -perm /o=w

find test_env -user ! $(whoami) -a -user ! root

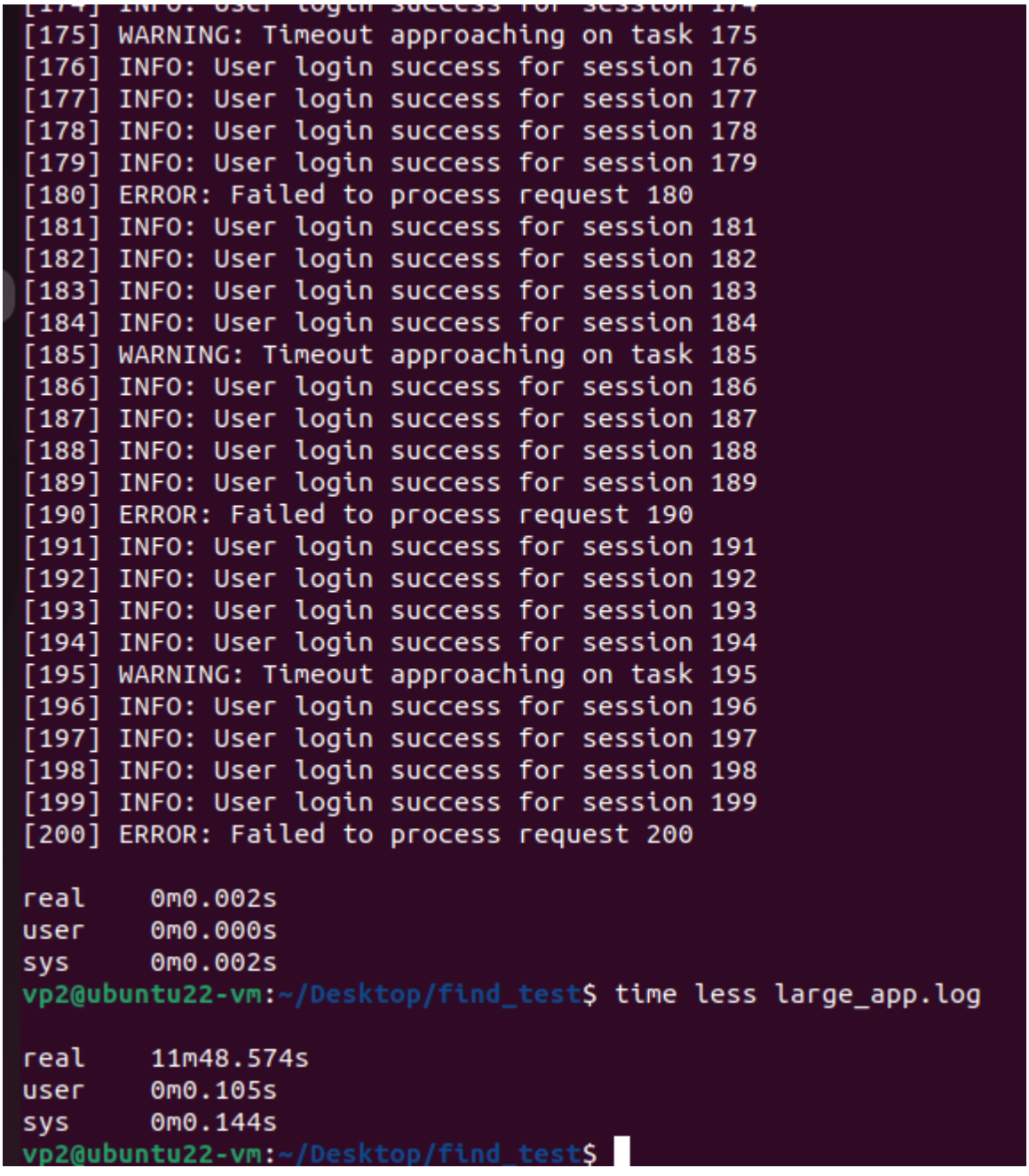
find test_env -name "*~" -o -name "*.bak" o -name "*.tmp"

```
./script~
vp2@ubuntu22-vm:~/Desktop/find_test$ find . type ! -user $USER ! -user root
find: ‘type’: No such file or directory
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type ! -user $USER ! -user root
find: Unknown argument to -type: !
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f ! -user $USER ! -user root
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type d \( -empty -o -name "hidden_only_dir" \)
./empty_dir
./hidden_only_dir
./normal_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ du -sk * | awk '{total += $1; count++} END {print total/count}'
736.286
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000K
find: invalid -size type `K'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000k
./large_file
vp2@ubuntu22-vm:~/Desktop/find_test$
```

-

9. Analyze Large Log

seq 1 300 > large_log.txt



sed -n '126,175p' large_log.txt

grep -n -m1 -B5 "error" large_log.txt | tail n 6
time cat large_log.txt > /dev/null

-

time less large_log.txt > /dev/null

time tail large_log.txt > /dev/null

grep -n "error" large_log.txt

10. Automate with Find -exec

```
empty_dir       normal_dir       script~
vp2@ubuntu22-vm:~/Desktop/find_test$ for i in {001..200}; do if (($((10#$i)) % 10 == 0)); then echo "[$i] ERROR: Failed to process reque
st $i"; elif (($((10#$i)) % 5 == 0)); then echo "[$i] WARNING: Timeout approaching on task $i"; else echo "[$i] INFO: User login success
 for session $i"; fi ; done > large_app.log
vp2@ubuntu22-vm:~/Desktop/find_test$ ls -l large_app.log
-rw-rw-r-- 1 vp2 vp2 9320 02:38 30 سبت large_app.log
vp2@ubuntu22-vm:~/Desktop/find_test$ head large_app.log
[001] INFO: User login success for session 001
[002] INFO: User login success for session 002
[003] INFO: User login success for session 003
[004] INFO: User login success for session 004
[005] WARNING: Timeout approaching on task 005
[006] INFO: User login success for session 006
[007] INFO: User login success for session 007
[008] INFO: User login success for session 008
[009] INFO: User login success for session 009
[010] ERROR: Failed to process request 010
vp2@ubuntu22-vm:~/Desktop/find_test$ head -n 125 large_app.log | tail -n 50
```

Permissions: sudo find . -type f -not -perm /a=x -
exec chmod 644 {} \;

sudo find . -type f -perm /a=x -exec chmod 755 {} \;

Disk space old files: find . -mtime +30 -exec du -c {} + | tail -1

Backup conf: find . -name "*.conf" -exec cp {} {}.backup \;

Remove temp: find . -name "*tmp" -atime +7 -print (preview) then -exec rm {} \;
time tar czf compressed/text.tar.gz compressed/text du -h compressed/text.*

11. Compression analysis

tar -czf text.tar.gz text_dir

tar -cjf text.tar.bz2 text_dir

tar -cJf text.tar.xz text_dir

-

```
./script~
vp2@ubuntu22-vm:~/Desktop/find_test$ find . type ! -user $USER ! -user root
find: ‘type’: No such file or directory
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type ! -user $USER ! -user root
find: Unknown argument to -type: !
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f ! -user $USER ! -user root
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type d \( -empty -o -name "hidden_only_dir" \)
./empty_dir
./hidden_only_dir
./normal_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ du -sk * | awk '{total += $1; count++} END {print total/count}'
736.286
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000K
find: invalid -size type `K'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000k
./large_file
vp2@ubuntu22-vm:~/Desktop/find_test$
```

zip -r text.zip text_dir

12. Inherited Archives

mkdir -p test_archive &&

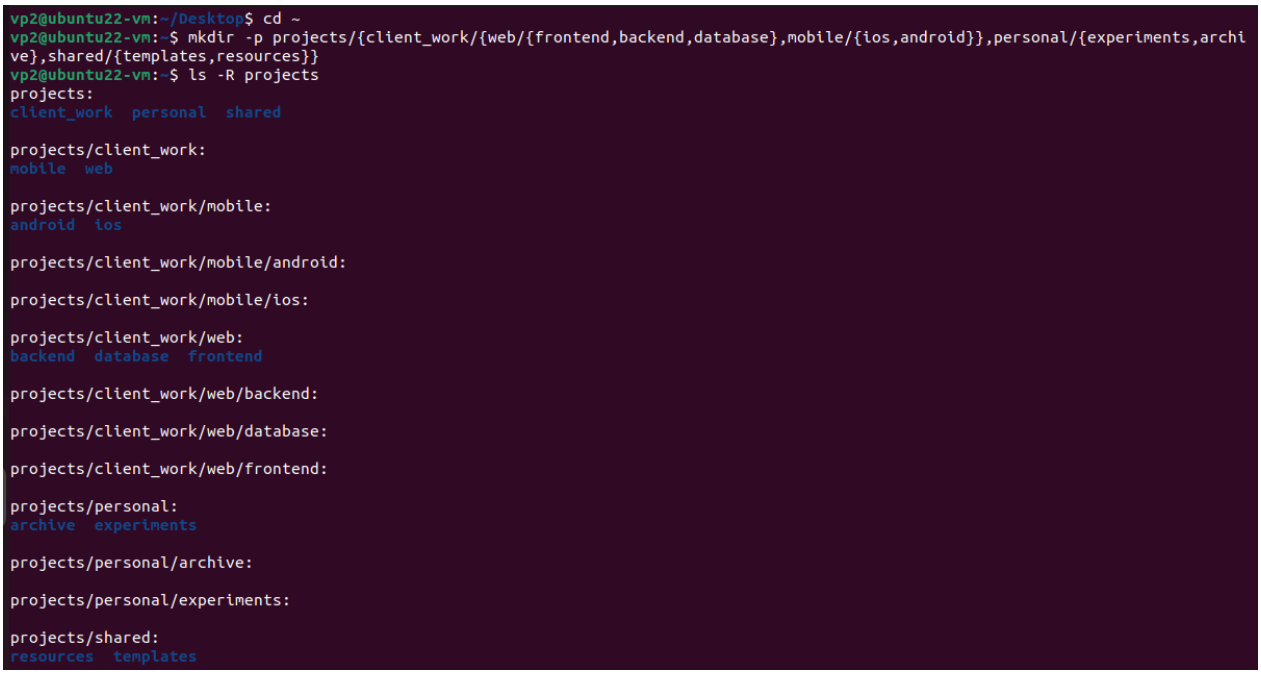
touch test_archive/{file1.txt,file2.conf}

tar -czf archive.tar.gz test_archive/

zip -r archive.zip . -i test_zip/

tar -tf archive.tar.gz

zip -l archive.zip



Extract pattern: tar -xf archive.tar.gz --wildcards "*conf"

Update: tar -uf archive.tar newfile zip -u archive.zip newfile

Corrupted: tar -tf corrupted.tar tar -xf archive1.tar unzip archive2.zip tar -cf new.tar *

13. Backup Rotation

mkdir -p test_data && touch test_data/file1.txt tar -cpf

backups/daily/inc_$(date +%Y-%m-%d).tar --listed-incremental=snapshot.file /data

tar -cpf backups/weekly/full_$(date +%Y-%W).tar --listed-incremental=snapshot.file /data

ls backups

whoami && id

cat /etc/passwd

```
vp2@ubuntu22-vm:~/Desktop$ mkdir -p projects/{client_work/web/frontend,personal/experiments,shared/templates}
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client-work/web/frontend
bash: cd: /home/vp2/projects/client-work/web/frontend: No such file or directory
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ cd ../../../personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ pwd
/home/vp2/projects/personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ cd ../../shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ pwd
/home/vp2/projects/shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ cd ../../client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$
```

sudo useradd ishimwe

Groups

groups ishimwe

14. User Access Issues

sudo find . -type f -perm /a=x -exec chmod 755 {} \;

Disk space old files: find . -mtime +30 -exec du -c {} + | tail -1

Backup conf: find . -name "*.conf" -exec cp {} {}.backup \;

Remove temp: find . -name "*tmp" -atime +7 -print (preview) then -exec rm {} \;


```
vp2@ubuntu22-vm:~/Desktop$ mkdir -p projects/{client_work/web/frontend,personal/experiments,shared/templates}
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client-work/web/frontend
bash: cd: /home/vp2/projects/client-work/web/frontend: No such file or directory
vp2@ubuntu22-vm:~/Desktop$ cd ~/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ cd ../../../personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ pwd
/home/vp2/projects/personal/experiments
vp2@ubuntu22-vm:~/projects/personal/experiments$ cd ../../shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ pwd
/home/vp2/projects/shared/templates
vp2@ubuntu22-vm:~/projects/shared/templates$ cd ../../client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$ pwd
/home/vp2/projects/client_work/web/frontend
vp2@ubuntu22-vm:~/projects/client_work/web/frontend$
```


15. Group Members Issues

id

getent group ishimwe

usermod -aG ishimwe ishimwe

sudo -u ishimwe id

su - ishimwe

Id

16. Sudo Audit sudo –l

```
./script~
vp2@ubuntu22-vm:~/Desktop/find_test$ find . type ! -user $USER ! -user root
find: ‘type’: No such file or directory
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type ! -user $USER ! -user root
find: Unknown argument to -type: !
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f ! -user $USER ! -user root
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type d \( -empty -o -name "hidden_only_dir" \)
./empty_dir
./hidden_only_dir
./normal_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ du -sk * | awk '{total += $1; count++} END {print total/count}'
736.286
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000K
find: invalid -size type `K'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -size +5000k
./large_file
vp2@ubuntu22-vm:~/Desktop/find_test$
```

sudo –i

sudo su –

su – vegas

last

17.Forensic Analysis

mkdir -p forensics/{reg,dir,sym,hard,dev} touch forensics/reg/file

ln forensics/reg/file

forensics/hard/hardlink ln -s

forensics/reg/file

forensics/sym/symlink sudo mknod

forensics/dev/block b 8 0 chmod +t

forensics/dir chmod u+s

forensics/reg/file chmod g+s

forensics/reg/file sudo chown vegas

forensics/reg/file ls –l forensics

stat forensics/reg/file

getfacl forensics/dir

```
vp2@ubuntu22-vm:~/Desktop$ mkdir find_test && cd find_test
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 10M large_file fallocate -l 50K average_file fallocate -l 1K small_file
fallocate: unexpected number of arguments
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 10M large_file
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 50K average_file
vp2@ubuntu22-vm:~/Desktop/find_test$ fallocate -l 1K small_file
vp2@ubuntu22-vm:~/Desktop/find_test$ touch -d "3 days ago" old_file_3days_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ touch -d "1 day ago" old_file_1day_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ touch new_file_today
vp2@ubuntu22-vm:~/Desktop/find_test$ touch risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ chmod 666 risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ sudo chown root:root root_owned_file
[sudo] password for vp2:
chown: cannot access 'root_owned_file': No such file or directory
vp2@ubuntu22-vm:~/Desktop/find_test$ touch root_owned_file
vp2@ubuntu22-vm:~/Desktop/find_test$ sudo chown root:root root_owned_file
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir empty_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir hidden_only_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ touch hidden_only_dir/.hidden_file
vp2@ubuntu22-vm:~/Desktop/find_test$ mkdir normal_dir
vp2@ubuntu22-vm:~/Desktop/find_test$ touch temp_report.tmp
vp2@ubuntu22-vm:~/Desktop/find_test$ touch config_old.bak
vp2@ubuntu22-vm:~/Desktop/find_test$ touch script~
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -mtime -3 -a -mtime +0
./old_file_1day_ago
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f perm /0002
find: paths must precede expression: `perm'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f -perm /0002
./risky_file_world_writable
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \(-name "*.tmp" -o -name "*.bak" -o -name "*~"\)
find: paths must precede expression: `(-name'
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \( -name "*.tmp" -o -name "*.bak" -o -name "*~"\)
find: invalid expression; I was expecting to find a ')' somewhere but did not see one.
vp2@ubuntu22-vm:~/Desktop/find_test$ find . -type f \( -name "*.tmp" -o -name "*.bak" -o -name "*~" \)
./config_old.bak
./temp_report.tmp
./script~
```