

- NSHUTI Kevin
 - 26770
 - Assignment 2
 - Group F
-

Q1. Investigating Compromised System Directories (2 pts)

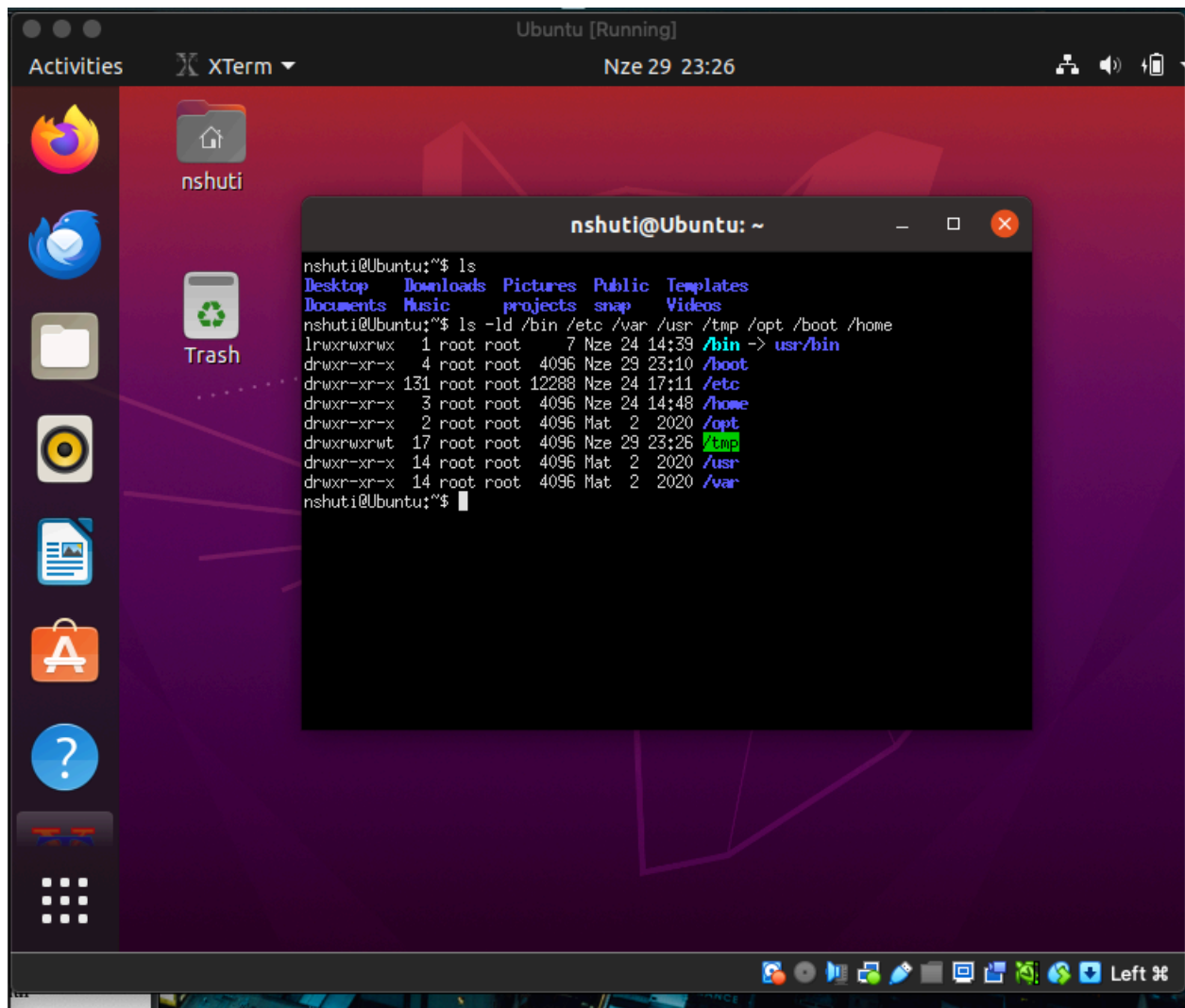
Task: Identify which directories may contain system configs, essential binaries, and logs that attackers could target.

Answer:

- `/bin` → essential binaries
- `/etc` → system configs
- `/var` → logs (evidence of intrusion)
- `/usr` → installed applications/libraries
- `/tmp` → temporary attacker payloads
- `/opt` → third-party apps (hidden malware possible)
- `/boot` → bootloader/kernel (persistence risk)
- `/home` → user files/dotfiles (backdoors in `.bashrc`, `authorized_keys`)

Commands Run:

```
ls -ld /bin /etc /var /usr /tmp /opt /boot /home
ls -l /var/log | head
find /bin /usr/bin -perm /6000 -type f -ls | head
```



```
Ubuntu [Running]
Activities XTerm Nze 29 23:33
nshuti@Ubuntu: ~

total 1108
drwxr-xr-x 3 root root 4096 Mar 2 2020 acpi
-rw-r--r-- 1 root root 3028 Mar 2 2020 adduser.conf
drwxr-xr-x 3 root root 4096 Mar 2 2020 alsa
drwxr-xr-x 2 root root 4096 Mar 24 16:17 alternatives
-rw-r--r-- 1 root root 401 Nya 16 2019 anacrontab
-rw-r--r-- 1 root root 433 Ukw 2 2017 apg.conf
drwxr-xr-x 5 root root 4096 Mar 2 2020 apm
drwxr-xr-x 3 root root 4096 Mar 24 15:27 apparmor
drwxr-xr-x 8 root root 4096 Mar 24 16:29 apparmor.d
ls: write error: Broken pipe
nshuti@Ubuntu:~$ ls -l /var/log | head -n 10
total 4528
-rw-r--r-- 1 root root 38288 Mar 24 17:11 alternatives.log
drwxr-xr-x 2 root root 4096 Mar 29 23:09 apt
-rw-r----- 1 syslog adm 33642 Mar 29 23:30 auth.log
-rw-r----- 1 root root 51214 Mar 29 23:22 boot.log
-rw-r--r-- 1 root root 105058 Mar 2 2020 bootstrap.log
-rw-rw---- 1 root utmp 0 Mar 2 2020 btmp
drwxr-xr-x 2 root root 4096 Mar 24 15:15 cups
drwxr-xr-x 2 root root 4096 Mar 28 2020 dist-upgrade
-rw-r--r-- 1 root adm 46643 Mar 29 23:22 dmesg
nshuti@Ubuntu:~$ ls -l /usr/bin | head -n 5
total 174368
-rwxr-xr-x 1 root root 59736 Mar 5 2019 [
-rwxr-xr-x 1 root root 31248 Mar 6 2024 aa-enabled
-rwxr-xr-x 1 root root 35344 Mar 6 2024 aa-exec
-rwxr-xr-x 1 root root 22912 Mar 14 2021 aconnect
ls: write error: Broken pipe
nshuti@Ubuntu:~$ ls -l /tmp | head -n 10
total 40
-rw----- 1 nshuti nshuti 0 Mar 29 23:23 config-err-DyiMvt
drwx----- 3 root root 4096 Mar 29 23:23 snap-private-tmp
drwx----- 2 nshuti nshuti 4096 Mar 29 23:23 ssh-3HIJthidTolp
drwx----- 3 root root 4096 Mar 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-colornd.service-cx20vi
drwx----- 3 root root 4096 Mar 29 23:23 systemd-private-d5b564fef08f40d69b203c734a8c8523-fwupd.service-i5Dacf
drwx----- 3 root root 4096 Mar 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-ModemManager.service-51I
i
drwx----- 3 root root 4096 Mar 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-switcheroo-control.servi
-FxBr7h
```

```
Ubuntu [Running]
Activities XTerm Nze 29 23:36
nshuti@Ubuntu: ~

-rwxr-xr-x 1 root root 31248 Mar 6 2024 aa-enabled
-rwxr-xr-x 1 root root 35344 Mar 6 2024 aa-exec
-rwxr-xr-x 1 root root 22912 Mar 14 2021 aconnect
ls: write error: Broken pipe
nshuti@Ubuntu:~$ ls -l /tmp | head -n 10
total 40
-rw----- 1 nshuti nshuti 0 Nze 29 23:23 config-err-DyiMvt
drwx----- 3 root root 4096 Nze 29 23:23 snap-private-tmp
drwx----- 2 nshuti nshuti 4096 Nze 29 23:23 ssh-3HIJthidTolp
drwx----- 3 root root 4096 Nze 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-colornd.service-cx20vi
drwx----- 3 root root 4096 Nze 29 23:23 systemd-private-d5b564fef08f40d69b203c734a8c8523-fwupd.service-i5Dacf
drwx----- 3 root root 4096 Nze 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-ModemManager.service-5I
i
drwx----- 3 root root 4096 Nze 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-switcheroo-control.serv
-FxBr7h
drwx----- 3 root root 4096 Nze 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-systemd-logind.service-
owj
drwx----- 3 root root 4096 Nze 29 23:22 systemd-private-d5b564fef08f40d69b203c734a8c8523-systemd-resolved.servic
tFJUe
nshuti@Ubuntu:~$ find /bin /usr/bin /sbin /usr/sbin -perm /6000 -type f -ls 2>/dev/null | head -n 20
655741 40 -rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount
664660 32 -rwsr-xr-x 1 root root 31032 Gas 21 2022 /usr/bin/pkexec
666661 88 -rwsr-xr-x 1 root root 88464 Gas 6 2024 /usr/bin/gpasswd
666010 164 -rwsr-xr-x 1 root root 166056 Mar 4 2023 /usr/bin/sudo
666680 68 -rwsr-xr-x 1 root root 68208 Gas 6 2024 /usr/bin/passwd
665585 44 -rwsr-sr-x 1 root root crontab 43720 Gas 13 2020 /usr/bin/crontab
666569 84 -rwsr-sr-x 1 root root shadow 84512 Gas 6 2024 /usr/bin/chage
666641 32 -rwsr-sr-x 1 root root shadow 31312 Gas 6 2024 /usr/bin/expiry
665377 56 -rwsr-xr-x 1 root root root 55528 Mar 9 2024 /usr/bin/mount
666637 52 -rwsr-xr-x 1 root root root 53040 Gas 6 2024 /usr/bin/chsh
664411 344 -rwsr-sr-x 1 root root ssh 350504 Mar 11 14:16 /usr/bin/ssh-agent
665475 68 -rwsr-xr-x 1 root root root 67816 Mar 9 2024 /usr/bin/su
666606 84 -rwsr-xr-x 1 root root root 85064 Gas 6 2024 /usr/bin/chfn
665802 40 -rwsr-xr-x 1 root root root 39144 Mar 9 2024 /usr/bin/umount
665502 16 -rwsr-sr-x 1 root root tty 14488 Mar 30 2020 /usr/bin/bsd-write
666630 44 -rwsr-xr-x 1 root root root 44784 Gas 6 2024 /usr/bin/newgrp
666312 44 -rwsr-sr-x 1 root root shadow 43168 Mar 10 2024 /usr/sbin/pam_extrausers_chkpwd
666459 44 -rwsr-sr-x 1 root root shadow 43160 Mar 10 2024 /usr/sbin/unix_chkpwd
662225 388 -rwsr-xr-x 1 root root dip 395144 Nya 23 2020 /usr/sbin/pppd
nshuti@Ubuntu:~$
```

Q2. Directory Structure Creation (2 pts)

Task: Create a project structure with minimal commands.

Commands:

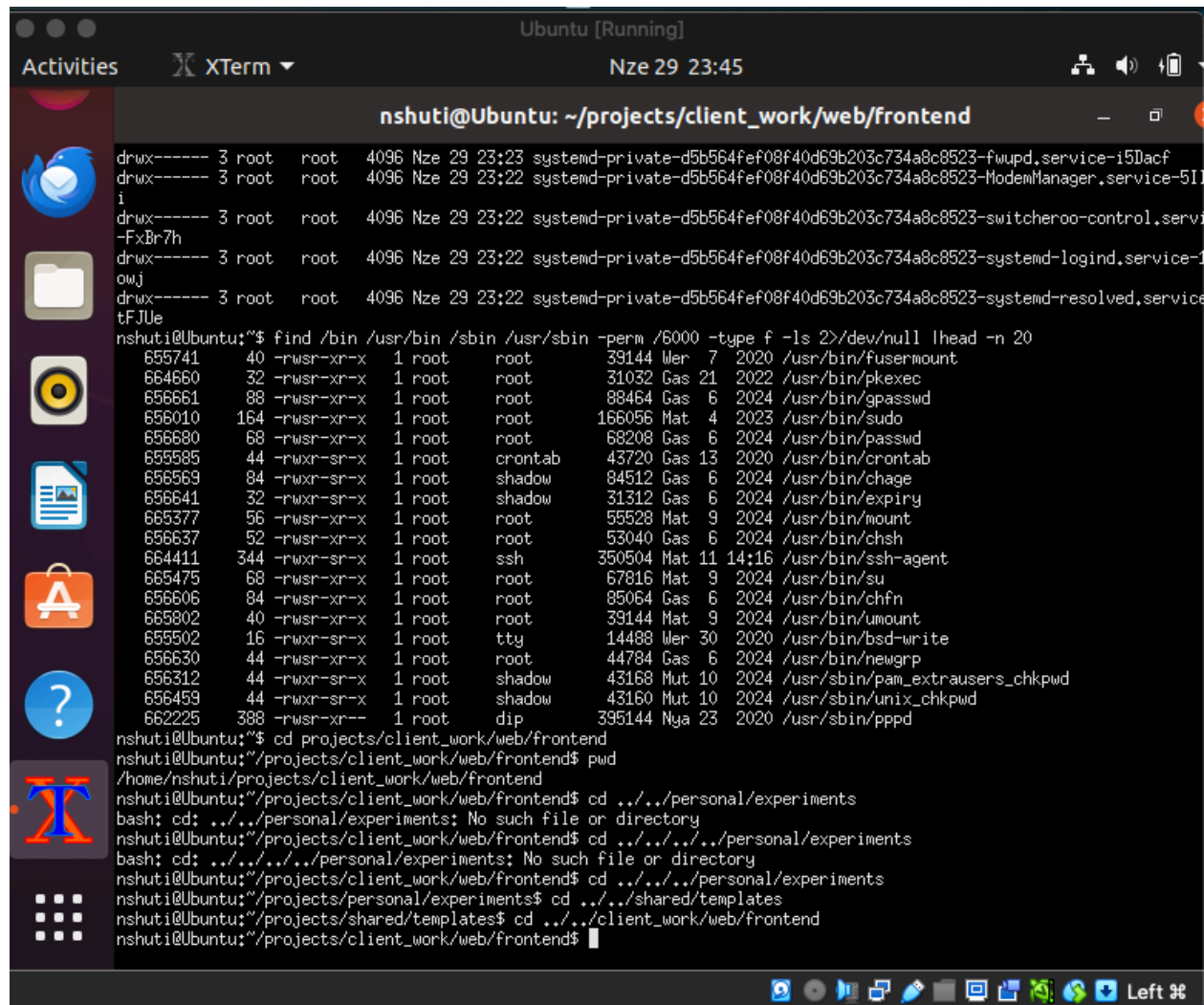
```
mkdir -p
~/ia2_work/projects/{client1/{src,tests,docs},client2/{src,tests,docs}
,personal/{notes,experiments}}
tree -L 3 ~/ia2_work/projects
```

Q3. Relative Path Navigation (1 pt)

Task: Navigate using ≤ 3 `cd` commands.

Commands:

```
pwd # starting location
cd ../../../../personal/experiments
pwd
cd ../../shared/templates
pwd
cd ../../client_work/web/frontend
pwd
```



The screenshot shows a terminal window titled "Ubuntu [Running]" with the user "nshuti" at the prompt "nshuti@Ubuntu: ~/projects/client_work/web/frontend". The terminal displays the output of several commands:

```
nshuti@Ubuntu:~$ find /bin /usr/bin /sbin /usr/sbin -perm /6000 -type f -ls 2>/dev/null | head -n 20
655741 40 -rwsr-xr-x 1 root root 39144 Mar 7 2020 /usr/bin/fusermount
664660 32 -rwsr-xr-x 1 root root 31032 Gas 21 2022 /usr/bin/pkexec
656661 88 -rwsr-xr-x 1 root root 88464 Gas 6 2024 /usr/bin/gpasswd
656010 164 -rwsr-xr-x 1 root root 166056 Mar 4 2023 /usr/bin/sudo
656680 68 -rwsr-xr-x 1 root root 68208 Gas 6 2024 /usr/bin/passwd
655585 44 -rwxr-sr-x 1 root crontab 43720 Gas 13 2020 /usr/bin/crontab
656569 84 -rwxr-sr-x 1 root shadow 84512 Gas 6 2024 /usr/bin/chage
656641 32 -rwxr-sr-x 1 root shadow 31312 Gas 6 2024 /usr/bin/expiry
665377 56 -rwsr-xr-x 1 root root 55528 Mar 9 2024 /usr/bin/mount
656637 52 -rwsr-xr-x 1 root root 53040 Gas 6 2024 /usr/bin/chsh
664411 344 -rwxr-sr-x 1 root ssh 350504 Mar 11 14:16 /usr/bin/ssh-agent
665475 68 -rwsr-xr-x 1 root root 67816 Mar 9 2024 /usr/bin/su
656606 84 -rwsr-xr-x 1 root root 85064 Gas 6 2024 /usr/bin/chfn
665802 40 -rwsr-xr-x 1 root root 39144 Mar 9 2024 /usr/bin/umount
655502 16 -rwxr-sr-x 1 root tty 14488 Mar 30 2020 /usr/bin/bsd-write
656630 44 -rwsr-xr-x 1 root root 44784 Gas 6 2024 /usr/bin/newgrp
656312 44 -rwxr-sr-x 1 root shadow 43168 Mar 10 2024 /usr/sbin/pam_extrausers_chkpwd
656459 44 -rwxr-sr-x 1 root shadow 43160 Mar 10 2024 /usr/sbin/unix_chkpwd
662225 388 -rwsr-xr-x 1 root dip 395144 May 23 2020 /usr/sbin/pppd

nshuti@Ubuntu:~$ cd projects/client_work/web/frontend
nshuti@Ubuntu:~/projects/client_work/web/frontend$ pwd
/home/nshuti/projects/client_work/web/frontend
nshuti@Ubuntu:~/projects/client_work/web/frontend$ cd ../../personal/experiments
bash: cd: ../../personal/experiments: No such file or directory
nshuti@Ubuntu:~/projects/client_work/web/frontend$ cd ../../../../personal/experiments
bash: cd: ../../../../personal/experiments: No such file or directory
nshuti@Ubuntu:~/projects/client_work/web/frontend$ cd ../../../../personal/experiments
nshuti@Ubuntu:~/projects/personal/experiments$ cd ../../shared/templates
nshuti@Ubuntu:~/projects/shared/templates$ cd ../../client_work/web/frontend
nshuti@Ubuntu:~/projects/client_work/web/frontend$
```

Q4. Web Project Structure (2 pts)

Task: Create HTML, CSS, JS, and backup files.

Commands:

```
mkdir -p web_project/{html,css,js,backups}
touch web_project/html/{index,about,contact}.html
for i in $(seq -w 1 12); do touch web_project/html/page_${i}.html;
done
touch
web_project/css/{main,reset,theme_light,theme_dark,mobile,tablet,desktop,print}.css
touch
web_project/js/{app_script,init_script,helpers_util,dom_util,app_config,env_config}.js
for l in a b c d; do for n in {1..5}; do touch
web_project/backups/${l}${n}.{bak,tmp,old}; done; done
```

```
Ubuntu [Running]
Activities XTerm Nze 30 00:24
nshuti@Ubuntu: ~/website

touch: cannot touch 'backups/b1.tmp': No such file or directory
touch: cannot touch 'backups/b2.old': No such file or directory
touch: cannot touch 'backups/b3.bak': No such file or directory
touch: cannot touch 'backups/b4.tmp': No such file or directory
touch: cannot touch 'backups/b5.old': No such file or directory
touch: cannot touch 'backups/c1.tmp': No such file or directory
touch: cannot touch 'backups/c2.old': No such file or directory
touch: cannot touch 'backups/c3.bak': No such file or directory
touch: cannot touch 'backups/c4.tmp': No such file or directory
touch: cannot touch 'backups/c5.old': No such file or directory
touch: cannot touch 'backups/d1.tmp': No such file or directory
touch: cannot touch 'backups/d2.old': No such file or directory
touch: cannot touch 'backups/d3.bak': No such file or directory
touch: cannot touch 'backups/d4.tmp': No such file or directory
touch: cannot touch 'backups/d5.old': No such file or directory
nshuti@Ubuntu:~/website$ cd
nshuti@Ubuntu:~$ for letter in a b c d; do for n in $(seq 1 5); do ext=$(( (n % 3) + 1 )); case $ext in 1) extension=
;; 2)extension=tmp ;; 3)extension=old ;; esac; touch "backups/${letter}${n}.${extension}"; done; done
touch: cannot touch 'backups/a1.tmp': No such file or directory
touch: cannot touch 'backups/a2.old': No such file or directory
touch: cannot touch 'backups/a3.bak': No such file or directory
touch: cannot touch 'backups/a4.tmp': No such file or directory
touch: cannot touch 'backups/a5.old': No such file or directory
touch: cannot touch 'backups/b1.tmp': No such file or directory
touch: cannot touch 'backups/b2.old': No such file or directory
touch: cannot touch 'backups/b3.bak': No such file or directory
touch: cannot touch 'backups/b4.tmp': No such file or directory
touch: cannot touch 'backups/b5.old': No such file or directory
touch: cannot touch 'backups/c1.tmp': No such file or directory
touch: cannot touch 'backups/c2.old': No such file or directory
touch: cannot touch 'backups/c3.bak': No such file or directory
touch: cannot touch 'backups/c4.tmp': No such file or directory
touch: cannot touch 'backups/c5.old': No such file or directory
touch: cannot touch 'backups/d1.tmp': No such file or directory
touch: cannot touch 'backups/d2.old': No such file or directory
touch: cannot touch 'backups/d3.bak': No such file or directory
touch: cannot touch 'backups/d4.tmp': No such file or directory
touch: cannot touch 'backups/d5.old': No such file or directory
nshuti@Ubuntu:~$ cd website
nshuti@Ubuntu:~/website$
```

Q5. Wildcard Operations (2 pts)

Examples of patterns used:

- Move numeric: `mv html/page_*.html archive/`
- Copy excluding: `cp css/!(mobile.css|tablet.css) css_desktop/`
- Exactly 3 chars before dot: `find . -regex '.*[/^/]\{3\}\.[/^/]\+$'`
- Consonant start: `find . -regex '.*[b-df-hj-np-tv-z].*'`

- 2-char extension: `find . -regex '.*\.[[:alnum:]]{2}$'`

```

nshuti@Ubuntu: ~/website
total 0
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_01.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_02.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_03.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_04.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_05.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_06.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_07.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_08.html
-rw-rw-r-- 1 nshuti nshuti 0 Nze 29 23:54 page_09.html
nshuti@Ubuntu:~/website$ mkdir -p css_desktop
nshuti@Ubuntu:~/website$ shopt -s extglob
nshuti@Ubuntu:~/website$ cp css/(mobile,css|tablet.css) css_desktop/
nshuti@Ubuntu:~/website$ ls -l css_desktop
total 0
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 desktop.css
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 main.css
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 print.css
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 resret.css
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 theme_dark.css
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 00:30 theme_light.css
nshuti@Ubuntu:~/website$ ls -l | sed -n 's/^((...)\).*$/\0/p'
nshuti@Ubuntu:~/website$ find . -maxdepth 2 -type f -regex '.*[/\[\]\{3\}\.[/\]\+\$]' -print
nshuti@Ubuntu:~/website$ find . -type f -regextype posix-extended -regex './[b-df-hj-np-tv-zB-DF-HJ-NP-TV-Z].*' -print
./css/resret.css
./css/print.css
./css/theme_light.css
./css/tablet.css
./css/mobile.css
./css/theme_dark.css

```

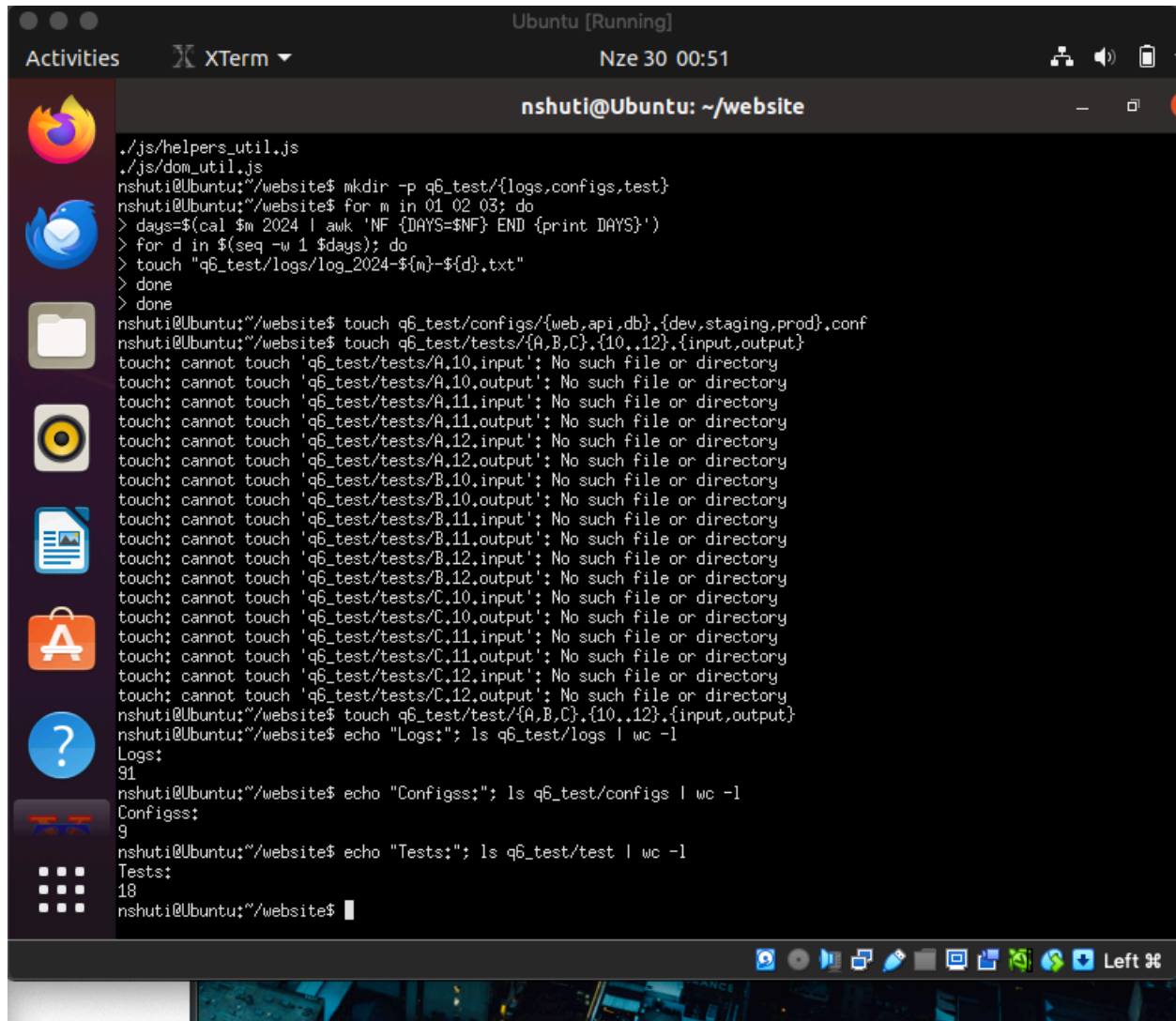
Q6. Brace Expansion (1 pt)

Commands:

```

for m in 01 02 03; do d=$(cal $m 2024 | awk 'NF {DAYS=$NF} END {print DAYS}'); for i in $(seq -w 1 $d); do touch logs/log_2024-$m-$i.txt; done; done
touch configs/{web,api,db}.{dev,staging,prod}.conf
touch tests/{A,B,C}.{10..12}.{input,output}

```

```
./js/helpers_util.js
./js/dom_util.js
nshuti@Ubuntu:~/website$ mkdir -p q6_test/{logs,configs,test}
nshuti@Ubuntu:~/website$ for m in 01 02 03; do
> days=$(cal $m 2024 | awk 'NF {DAYS=$NF} END {print DAYS}')
> for d in $(seq -w 1 $days); do
> touch "q6_test/logs/log_2024-${m}-${d}.txt"
> done
> done
nshuti@Ubuntu:~/website$ touch q6_test/configs/{web,api,db}.{dev,staging,prod}.conf
nshuti@Ubuntu:~/website$ touch q6_test/tests/{A,B,C}.{10..12}.{input,output}
touch: cannot touch 'q6_test/tests/A.10.input': No such file or directory
touch: cannot touch 'q6_test/tests/A.10.output': No such file or directory
touch: cannot touch 'q6_test/tests/A.11.input': No such file or directory
touch: cannot touch 'q6_test/tests/A.11.output': No such file or directory
touch: cannot touch 'q6_test/tests/A.12.input': No such file or directory
touch: cannot touch 'q6_test/tests/A.12.output': No such file or directory
touch: cannot touch 'q6_test/tests/B.10.input': No such file or directory
touch: cannot touch 'q6_test/tests/B.10.output': No such file or directory
touch: cannot touch 'q6_test/tests/B.11.input': No such file or directory
touch: cannot touch 'q6_test/tests/B.11.output': No such file or directory
touch: cannot touch 'q6_test/tests/B.12.input': No such file or directory
touch: cannot touch 'q6_test/tests/B.12.output': No such file or directory
touch: cannot touch 'q6_test/tests/C.10.input': No such file or directory
touch: cannot touch 'q6_test/tests/C.10.output': No such file or directory
touch: cannot touch 'q6_test/tests/C.11.input': No such file or directory
touch: cannot touch 'q6_test/tests/C.11.output': No such file or directory
touch: cannot touch 'q6_test/tests/C.12.input': No such file or directory
touch: cannot touch 'q6_test/tests/C.12.output': No such file or directory
nshuti@Ubuntu:~/website$ touch q6_test/test/{A,B,C}.{10..12}.{input,output}
nshuti@Ubuntu:~/website$ echo "Logs:"; ls q6_test/logs | wc -l
Logs:
91
nshuti@Ubuntu:~/website$ echo "Configss:"; ls q6_test/configs | wc -l
Configss:
9
nshuti@Ubuntu:~/website$ echo "Tests:"; ls q6_test/test | wc -l
Tests:
18
nshuti@Ubuntu:~/website$
```

Q7. Linux vs Windows Line Endings (1 pt)

Commands:

```
cat > linux.txt <<EOF
line one
line two
line three
EOF
awk '{print $0"\r"}' linux.txt > windows.txt
diff linux.txt windows.txt
cmp -l linux.txt windows.txt
```

Explanation:

- `diff` → shows differences in lines.
- `cmp` → shows CR (`0x0d`) mismatch.
- `comm` → compares sorted content, ignoring line endings.

```
nshuti@Ubuntu: ~/projects/q7/q7
nshuti@Ubuntu:~/projects/q7/q7$ cat > linux_conf.txt <<'EOF'
> line one
> line two
> line three
> EOF
nshuti@Ubuntu:~/projects/q7/q7$ awk '{printf "%s\r\n", $0}' linux_conf.txt > windows_conf.txt
nshuti@Ubuntu:~/projects/q7/q7$ xxd -g 1 linux_conf.txt | head
00000000: 6c 69 6e 65 20 6f 6e 65 0a 6c 69 6e 65 20 74 77  line one,line tw
00000010: 6f 0a 6c 69 6e 65 20 74 68 72 65 65 0a          o,line three.
nshuti@Ubuntu:~/projects/q7/q7$ xxd -g 1 windows_conf.txt | head
00000000: 6c 69 6e 65 20 6f 6e 65 0d 0a 6c 69 6e 65 20 74  line one..line t
0 0d 0a 6c 69 6e 65 20 74 68 72 65 65 0d 0a  wo..line three..
nshuti@Ubuntu:~/projects/q7/q7$ diff -u linux_conf.txt windows_conf.txt || true
--- linux_conf.txt      2025-09-30 23:04:16.719649471 +0200
+++ windows_conf.txt    2025-09-30 23:04:33.315166246 +0200
@@ -1,3 +1,3 @@
-line one
-line two
-line three
+line one
+line two
+line three
nshuti@Ubuntu:~/projects/q7/q7$ cmp -l linux_conf.txt windows_conf.txt | head
cmp: EOF on linux_conf.txt after byte 29
 9 12 15
10 154 12
11 151 154
12 156 151
13 145 156
14 40 145
15 164 40
16 167 164
17 157 167
18 12 157
nshuti@Ubuntu:~/projects/q7/q7$ sort linux_conf.txt > linux_sorted.txt
nshuti@Ubuntu:~/projects/q7/q7$ sort windows_conf.txt > windows_sorted.txt
nshuti@Ubuntu:~/projects/q7/q7$ comm linux_sorted.txt windows_sorted.txt || true
line one
    line one
line three
    line three
line two
    line two
nshuti@Ubuntu:~/projects/q7/q7$ command -v dos2unix >>/dev/null && dos2unix windo
ws_conf.txt linux2.txt || true
nshuti@Ubuntu:~/projects/q7/q7$
```

Q8. File Search with **find** (3 pts)

Examples:

- Larger than average: **find . -size +\${avg}c**

- Modified last 72 but not 24h: `find . -mtime -3 -mtime +1`
- Empty or hidden-only dirs: `find . -empty`
- World writable: `find . -perm -o=w`
- Other owners: `find . ! -user $(whoami) ! -user root`

- Backup/temp names: `find . -regex '.*\\.\\(bak\\|tmp\\|old\\)\\$'`

```

nshuti@Ubuntu: ~/projects/q9
2025-09-30 23:16:41 INFO: Normal line 149
nshuti@Ubuntu:~/projects/q9$ grep -n "ERROR" biglog.log | tail -n1 | cut -d: -f1
| while read lineno; do
> start=$((lineno-5)); if [ $start -lt 1 ]; then start=1; fi
> sed -n "${start},${(lineno+5)}p" biglog.log
> done
2025-09-30 23:16:41 INFO: Normal line 217
2025-09-30 23:16:41 INFO: Normal line 218
2025-09-30 23:16:41 INFO: Normal line 219
2025-09-30 23:16:41 INFO: Normal line 220
2025-09-30 23:16:41 INFO: Normal line 221
2025-09-30 23:16:41 ERROR: Something bad happened at line 222
2025-09-30 23:16:41 INFO: Normal line 223
2025-09-30 23:16:41 INFO: Normal line 224
2025-09-30 23:16:41 INFO: Normal line 225
2025-09-30 23:16:41 INFO: Normal line 226
2025-09-30 23:16:41 INFO: Normal line 227
nshuti@Ubuntu:~/projects/q9$ time cat biglog.log > /dev/null

real    0m0.004s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ time sed -n '1,250p' biglog.log > /dev/null

real    0m0.002s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ time awk '{print}' biglog.log > /dev/null

real    0m0.004s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ nl -ba biglog.log | grep "ERROR" > error_lines_with_numbers.txt
nshuti@Ubuntu:~/projects/q9$ nl -ba biglog.log | grep "ERROR" > error_lines_with_numbers.txt
cat error_lines_with_numbers.txtnshuti@Ubuntu:~/projects/q9$ cat error_lines_wit
h_numbers.txt
   37 2025-09-30 23:16:40 ERROR: Something bad happened at line 37
   74 2025-09-30 23:16:40 ERROR: Something bad happened at line 74
  111 2025-09-30 23:16:41 ERROR: Something bad happened at line 111
  148 2025-09-30 23:16:41 ERROR: Something bad happened at line 148
  185 2025-09-30 23:16:41 ERROR: Something bad happened at line 185
  222 2025-09-30 23:16:41 ERROR: Something bad happened at line 222
nshuti@Ubuntu:~/projects/q9$ wc -l biglog.log
250 biglog.log
nshuti@Ubuntu:~/projects/q9$

```

Q9. Log File Analysis (2 pts)

Commands:

```

for i in {1..250}; do echo "INFO line $i"; done > big.log
sed -n '101,150p' big.log
grep -n "ERROR" big.log | tail -1
nl big.log | grep ERROR

```

```

nshuti@Ubuntu: ~/projects/q9
2025-09-30 23:16:41 INFO: Normal line 149
nshuti@Ubuntu:~/projects/q9$ grep -n "ERROR" biglog.log | tail -n1 | cut -d: -f1
1 while read lineno; do
> start=$((lineno-5)); if [ $start -lt 1 ]; then start=1; fi
> sed -n "${start},${((lineno+5))}p" biglog.log
> done
2025-09-30 23:16:41 INFO: Normal line 217
2025-09-30 23:16:41 INFO: Normal line 218
2025-09-30 23:16:41 INFO: Normal line 219
2025-09-30 23:16:41 INFO: Normal line 220
2025-09-30 23:16:41 INFO: Normal line 221
2025-09-30 23:16:41 ERROR: Something bad happened at line 222
2025-09-30 23:16:41 INFO: Normal line 223
2025-09-30 23:16:41 INFO: Normal line 224
2025-09-30 23:16:41 INFO: Normal line 225
2025-09-30 23:16:41 INFO: Normal line 226
2025-09-30 23:16:41 INFO: Normal line 227
nshuti@Ubuntu:~/projects/q9$ time cat biglog.log > /dev/null

real    0m0.004s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ time sed -n '1,250p' biglog.log > /dev/null

real    0m0.002s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ time awk '{print}' biglog.log > /dev/null

real    0m0.004s
user    0m0.002s
sys     0m0.000s
nshuti@Ubuntu:~/projects/q9$ nl -ba biglog.log | grep "ERROR" > error_lines_with
_numbers.txt
nshuti@Ubuntu:~/projects/q9$ nl -ba biglog.log | grep "ERROR" > error_lines_with
_numbers.txt
cat error_lines_with_numbers.txtnshuti@Ubuntu:~/projects/q9$ cat error_lines_wit
h_numbers.txt
  37  2025-09-30 23:16:40 ERROR: Something bad happened at line 37
  74  2025-09-30 23:16:40 ERROR: Something bad happened at line 74
 111  2025-09-30 23:16:41 ERROR: Something bad happened at line 111
 148  2025-09-30 23:16:41 ERROR: Something bad happened at line 148
 185  2025-09-30 23:16:41 ERROR: Something bad happened at line 185
 222  2025-09-30 23:16:41 ERROR: Something bad happened at line 222
nshuti@Ubuntu:~/projects/q9$ wc -l biglog.log
250 biglog.log
nshuti@Ubuntu:~/projects/q9$

```

Q10. File Maintenance Automation (1 pt)

Examples:

- Change perms except executables:
`find . -type f ! -executable -exec chmod 644 {} \;`
- Disk space older 30d:
`find . -mtime +30 -print0 | du --files0-from=- -ch`
- Backup configs:
`find . -name '*.conf' -exec cp {} {}.backup \;`
- Remove stale tmp:
`find . -name '*.tmp' -atime +30 -delete`

```
Ubuntu [Running]
Activities XTerm Nze 30 23:23
nshuti@Ubuntu: ~/projects/q10
nshuti@Ubuntu:~/projects/q9$ cd ..
nshuti@Ubuntu:~/projects$ mkdir -p q10 && cd q10
nshuti@Ubuntu:~/projects/q10$ touch f1.txt f2.sh script_exec && chmod +x script_exec
nshuti@Ubuntu:~/projects/q10$ find . -maxdepth 1 -type f -ls
533235 0 -rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:20 ./f2.sh
533236 0 -rwxrwxr-x 1 nshuti nshuti 0 Nze 30 23:20 ./script_exec
533234 0 -rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:20 ./f1.txt
nshuti@Ubuntu:~/projects/q10$ find . -type f ! -executable -print -exec echo "chmod 644" {} \;
./f2.sh
chmod 644 ./f2.sh
./f1.txt
chmod 644 ./f1.txt
nshuti@Ubuntu:~/projects/q10$ find . -type f ! -executable -exec chmod 644 {} \;
nshuti@Ubuntu:~/projects/q10$ find . -type f -ls
533235 0 -rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:20 ./f2.sh
533236 0 -rwxrwxr-x 1 nshuti nshuti 0 Nze 30 23:20 ./script_exec
533234 0 -rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:20 ./f1.txt
nshuti@Ubuntu:~/projects/q10$ find . -type f -mtime +30 -print
nshuti@Ubuntu:~/projects/q10$ find . -type f -mtime +30 -print0 | du --files0-from=- -ch | tail -n1
0 total
nshuti@Ubuntu:~/projects/q10$ mkdir -p confs && touch confs/a.conf confs/b.conf
nshuti@Ubuntu:~/projects/q10$ find confs -name '*.conf' -print -exec echo cp {} {} backup \;
confs/a.conf
cp confs/a.conf confs/a.conf.backup
confs/b.conf
cp confs/b.conf confs/b.conf.backup
nshuti@Ubuntu:~/projects/q10$ find confs -name '*.conf' -exec cp {} {} backup \;
nshuti@Ubuntu:~/projects/q10$ ls -l confs
total 0
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:21 a.conf
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:22 a.conf.backup
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:21 b.conf
-rw-rw-r-- 1 nshuti nshuti 0 Nze 30 23:22 b.conf.backup
nshuti@Ubuntu:~/projects/q10$ find . -type f \( -name '*.tmp' -o -name '*~' \) -atime +30 -print
nshuti@Ubuntu:~/projects/q10$ mkdir -p trash_preview
nshuti@Ubuntu:~/projects/q10$ find . -type f \( -name '*.tmp' -o -name '*~' \) -atime +30 -exec mv -t trash_preview {} +
nshuti@Ubuntu:~/projects/q10$ ls -l trash_preview
total 0
nshuti@Ubuntu:~/projects/q10$
```

Q11. Compression Analysis (2 pts)

- Text compresses best with `xz/bzip2`.

- Already compressed (jpg/mp4) → no gain.
- Recommendation: **tar+gzip** for balance.

The screenshot shows an Ubuntu terminal window titled "nshuti@Ubuntu: ~/projects/q11". The terminal displays a series of commands and their outputs, comparing the performance and size of different compression methods. The commands include timing and disk usage (du) for various file formats.

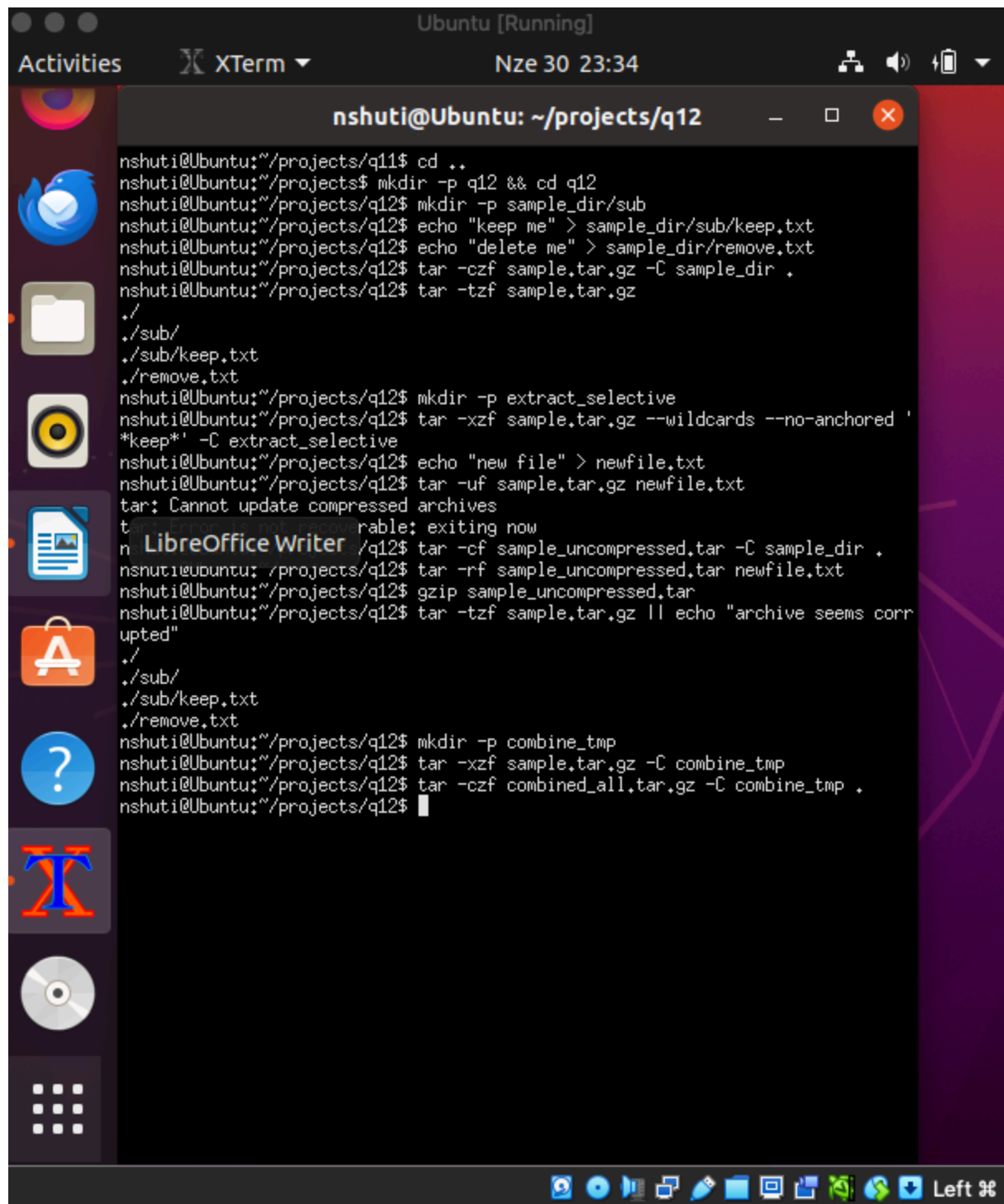
```

real    0m0,115s
user    0m0,088s
sys     0m0,005s
nshuti@Ubuntu:~/projects/q11$ du -b text_tarbz2.tar.bz2
380873 text_tarbz2.tar.bz2
nshuti@Ubuntu:~/projects/q11$
nshuti@Ubuntu:~/projects/q11$ time tar -cjf compressed_tarbz2.tar.bz2 compressed_files
real    0m0,349s
user    0m0,319s
sys     0m0,012s
nshuti@Ubuntu:~/projects/q11$ du -b compressed_tarbz2.tar.bz2
1508061 compressed_tarbz2.tar.bz2
nshuti@Ubuntu:~/projects/q11$ time tar -cJf text_tarxz.tar.xz text_files
real    0m0,253s
user    0m0,201s
sys     0m0,012s
nshuti@Ubuntu:~/projects/q11$ du -b text_tarxz.tar.xz
385096 text_tarxz.tar.xz
nshuti@Ubuntu:~/projects/q11$ time tar -cJf compressed_tarxz.tar.xz compressed_files
real    0m0,527s
user    0m0,448s
sys     0m0,060s
nshuti@Ubuntu:~/projects/q11$ du -b compressed_tarxz.tar.xz
1509968 compressed_tarxz.tar.xz
nshuti@Ubuntu:~/projects/q11$ time zip -r text_zip.zip text_files >/dev/null
real    0m0,042s
user    0m0,025s
sys     0m0,000s
nshuti@Ubuntu:~/projects/q11$ du -b text_zip.zip
398687 text_zip.zip
nshuti@Ubuntu:~/projects/q11$
nshuti@Ubuntu:~/projects/q11$ time zip -r compressed_zip.zip compressed_files >/dev/null
real    0m0,073s
user    0m0,028s
sys     0m0,028s
nshuti@Ubuntu:~/projects/q11$ du -b compressed_zip.zip
1503201 compressed_zip.zip
nshuti@Ubuntu:~/projects/q11$
  
```

The terminal window includes a sidebar with application icons (Activities, XTerm, and various system utilities) and a top bar showing the system status (Nze 30 23:30). The bottom of the window features a dock with additional application icons and a "Left" button.

Q12. Archive Handling (1 pt)

- List contents: `tar -tzf archive.tar.gz`
- Selective extract: `tar -xzf archive.tar.gz --wildcards '*keep*'`
- Update: `tar -rf archive.tar newfile`
- Corrupt handling: `tar -tzf archive.tar.gz || echo "bad archive"`
- Merge: extract all → `tar -czf new.tar.gz combined_dir/`

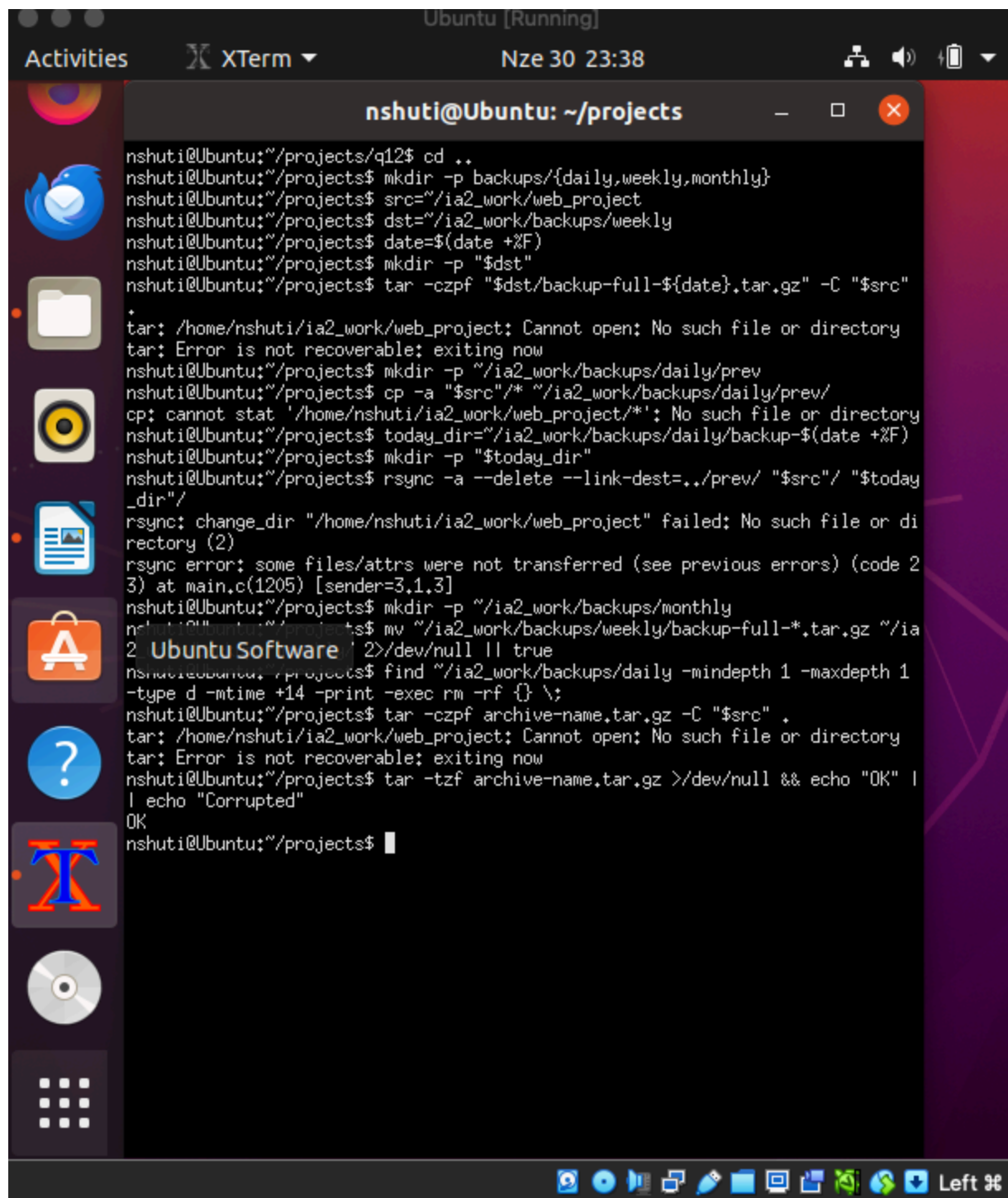


The screenshot shows an Ubuntu terminal window titled "Ubuntu [Running]" with the time "Nze 30 23:34". The terminal session is conducted by a user named "nshuti" in the directory "~/projects/q12". The commands and their outputs are as follows:

```
nshuti@Ubuntu:~/projects/q11$ cd ..
nshuti@Ubuntu:~/projects$ mkdir -p q12 && cd q12
nshuti@Ubuntu:~/projects/q12$ mkdir -p sample_dir/sub
nshuti@Ubuntu:~/projects/q12$ echo "keep me" > sample_dir/sub/keep.txt
nshuti@Ubuntu:~/projects/q12$ echo "delete me" > sample_dir/remove.txt
nshuti@Ubuntu:~/projects/q12$ tar -czf sample.tar.gz -C sample_dir .
nshuti@Ubuntu:~/projects/q12$ tar -tzf sample.tar.gz
./
./sub/
./sub/keep.txt
./remove.txt
nshuti@Ubuntu:~/projects/q12$ mkdir -p extract_selective
nshuti@Ubuntu:~/projects/q12$ tar -xzf sample.tar.gz --wildcards --no-anchored '*keep*' -C extract_selective
nshuti@Ubuntu:~/projects/q12$ echo "new file" > newfile.txt
nshuti@Ubuntu:~/projects/q12$ tar -uf sample.tar.gz newfile.txt
tar: Cannot update compressed archives
tar: Exiting with failure: exiting now
nshuti@Ubuntu:~/projects/q12$ tar -cf sample_uncompressed.tar -C sample_dir .
nshuti@Ubuntu:~/projects/q12$ tar -rf sample_uncompressed.tar newfile.txt
nshuti@Ubuntu:~/projects/q12$ gzip sample_uncompressed.tar
nshuti@Ubuntu:~/projects/q12$ tar -tzf sample.tar.gz || echo "archive seems corrupted"
./
./sub/
./sub/keep.txt
./remove.txt
nshuti@Ubuntu:~/projects/q12$ mkdir -p combine_tmp
nshuti@Ubuntu:~/projects/q12$ tar -xzf sample.tar.gz -C combine_tmp
nshuti@Ubuntu:~/projects/q12$ tar -czf combined_all.tar.gz -C combine_tmp .
nshuti@Ubuntu:~/projects/q12$
```

Q13. Backup Rotation (1 pt)

- Daily incremental → `rsync --link-dest`
- Weekly full → `tar -czf backup-full-YYYYMMDD.tar.gz`
- Monthly archive → move weekly → `monthly/`
- Cleanup → `find backups/daily -mtime +14 -exec rm -rf {} \;`



```
Ubuntu [Running]
Activities XTerm Nze 30 23:38
nshuti@Ubuntu: ~/projects

nshuti@Ubuntu:~/projects/q12$ cd ..
nshuti@Ubuntu:~/projects$ mkdir -p backups/{daily,weekly,monthly}
nshuti@Ubuntu:~/projects$ src="/ia2_work/web_project"
nshuti@Ubuntu:~/projects$ dst="/ia2_work/backups/weekly"
nshuti@Ubuntu:~/projects$ date=$(date +%F)
nshuti@Ubuntu:~/projects$ mkdir -p "$dst"
nshuti@Ubuntu:~/projects$ tar -czpf "$dst/backup-full-${date}.tar.gz" -C "$src"
tar: /home/nshuti/ia2_work/web_project: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
nshuti@Ubuntu:~/projects$ mkdir -p ~/ia2_work/backups/daily/prev
nshuti@Ubuntu:~/projects$ cp -a "$src"/* ~/ia2_work/backups/daily/prev/
cp: cannot stat '/home/nshuti/ia2_work/web_project/*': No such file or directory
nshuti@Ubuntu:~/projects$ today_dir="/ia2_work/backups/daily/backup-$(date +%F)"
nshuti@Ubuntu:~/projects$ mkdir -p "$today_dir"
nshuti@Ubuntu:~/projects$ rsync -a --delete --link-dest=../prev/ "$src"/ "$today_dir"/
rsync: change_dir "/home/nshuti/ia2_work/web_project" failed: No such file or directory (2)
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main,c(1205) [sender=3.1.3]
nshuti@Ubuntu:~/projects$ mkdir -p ~/ia2_work/backups/monthly
nshuti@Ubuntu:~/projects$ mv ~/ia2_work/backups/weekly/backup-full-*.tar.gz ~/ia2_work/backups/monthly/
nshuti@Ubuntu:~/projects$ find ~/ia2_work/backups/daily -mindepth 1 -maxdepth 1 -type d -mtime +14 -print -exec rm -rf {} \;
nshuti@Ubuntu:~/projects$ tar -czpf archive-name.tar.gz -C "$src" .
tar: /home/nshuti/ia2_work/web_project: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
nshuti@Ubuntu:~/projects$ tar -tzf archive-name.tar.gz >/dev/null && echo "OK" |
echo "Corrupted"
OK
nshuti@Ubuntu:~/projects$
```

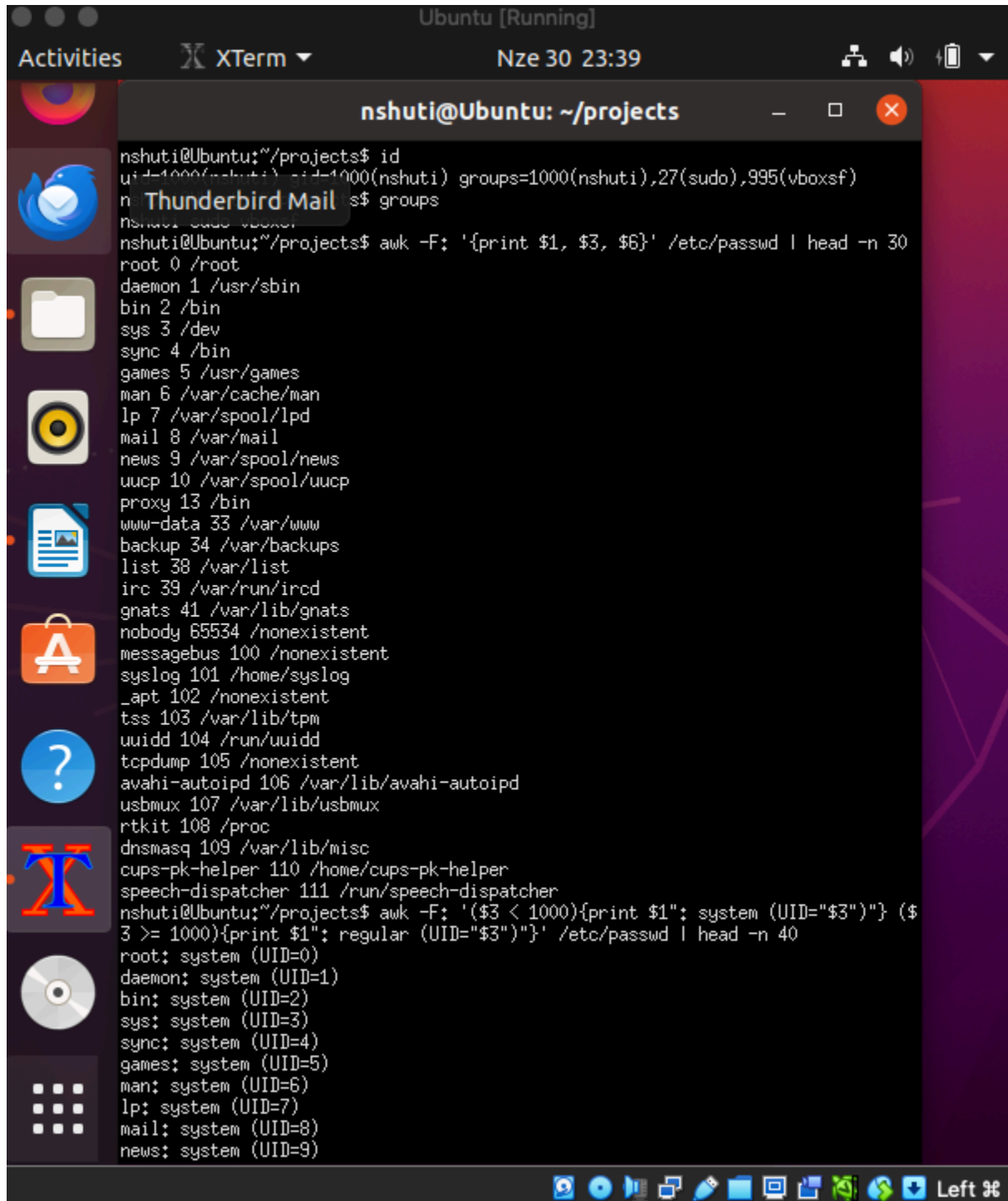
Q14. User & Groups Analysis (2 pts)

Commands:

```
id
```

```
groups
```

```
awk -F: '{print $1,$3,$6}' /etc/passwd | head
```



The screenshot shows an Ubuntu terminal window titled "nshuti@Ubuntu: ~/projects". The terminal displays the following commands and their outputs:

```
nshuti@Ubuntu:~/projects$ id
uid=1000(nshuti) gid=1000(nshuti) groups=1000(nshuti),27(sudo),995(vboxsf)

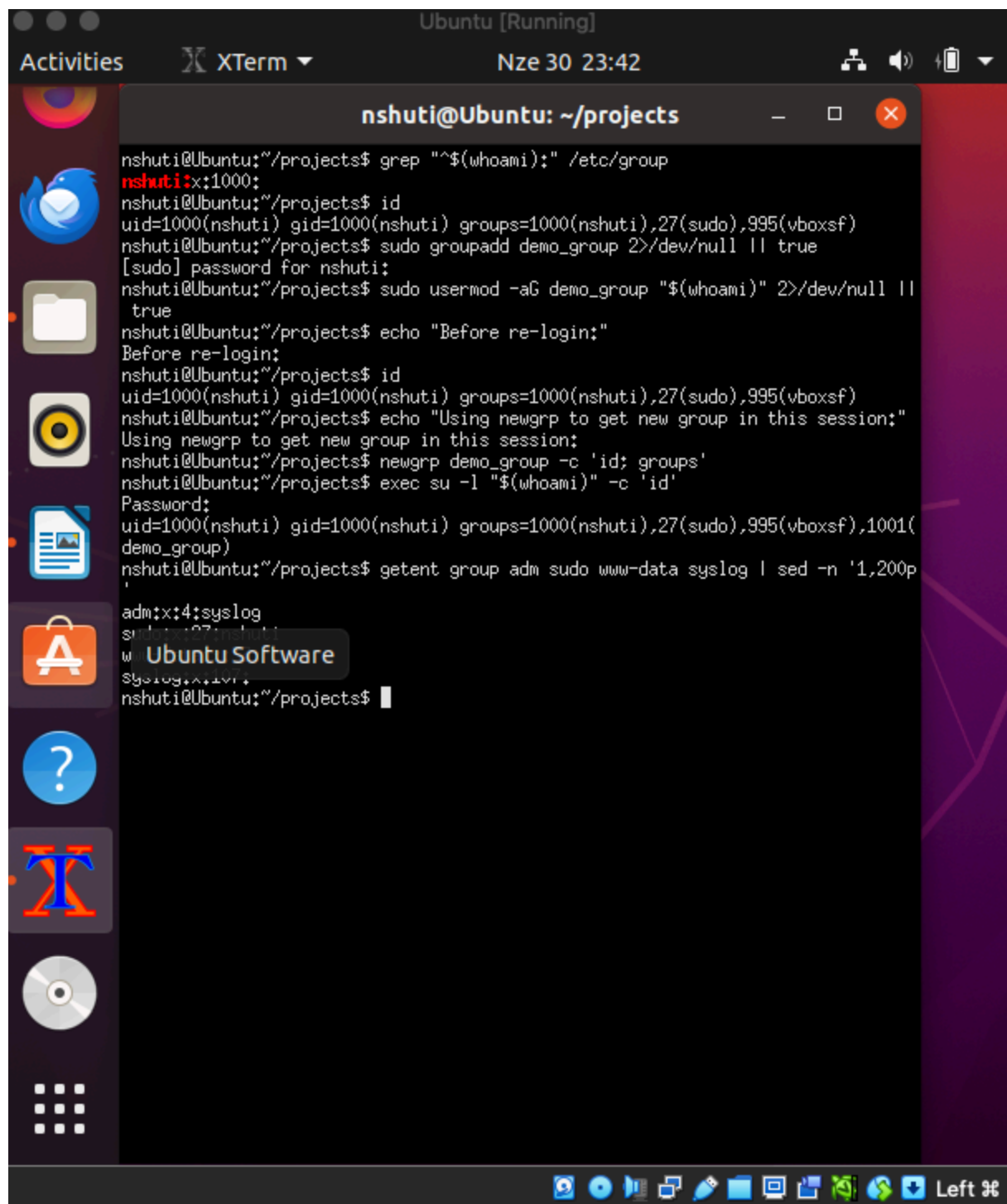
nshuti@Ubuntu:~/projects$ groups
nshuti : sudo vboxsf

nshuti@Ubuntu:~/projects$ awk -F: '{print $1, $3, $6}' /etc/passwd | head -n 30
root 0 /root
daemon 1 /usr/sbin
bin 2 /bin
sys 3 /dev
sync 4 /bin
games 5 /usr/games
man 6 /var/cache/man
lp 7 /var/spool/lpd
mail 8 /var/mail
news 9 /var/spool/news
uucp 10 /var/spool/uucp
proxy 13 /bin
www-data 33 /var/www
backup 34 /var/backups
list 38 /var/list
irc 39 /var/run/ircd
gnats 41 /var/lib/gnats
nobody 65534 /nonexistent
messagebus 100 /nonexistent
syslog 101 /home/syslog
_apt 102 /nonexistent
tss 103 /var/lib/tpm
uidd 104 /run/uidd
tcpdump 105 /nonexistent
avahi-autoipd 106 /var/lib/avahi-autoipd
usbmux 107 /var/lib/usbmux
rtkit 108 /proc
dnsmasq 109 /var/lib/misc
cups-pk-helper 110 /home/cups-pk-helper
speech-dispatcher 111 /run/speech-dispatcher

nshuti@Ubuntu:~/projects$ awk -F: '($3 < 1000){print $1": system (UID=\"$3\")"} ($3 >= 1000){print $1": regular (UID=\"$3\")"}' /etc/passwd | head -n 40
root: system (UID=0)
daemon: system (UID=1)
bin: system (UID=2)
sys: system (UID=3)
sync: system (UID=4)
games: system (UID=5)
man: system (UID=6)
lp: system (UID=7)
mail: system (UID=8)
news: system (UID=9)
```

Q15. Group Membership Propagation (1 pt)

- Add user to group: `sudo usermod -aG demo_group $USER`
- Effective only after re-login → or use `newgrp`.



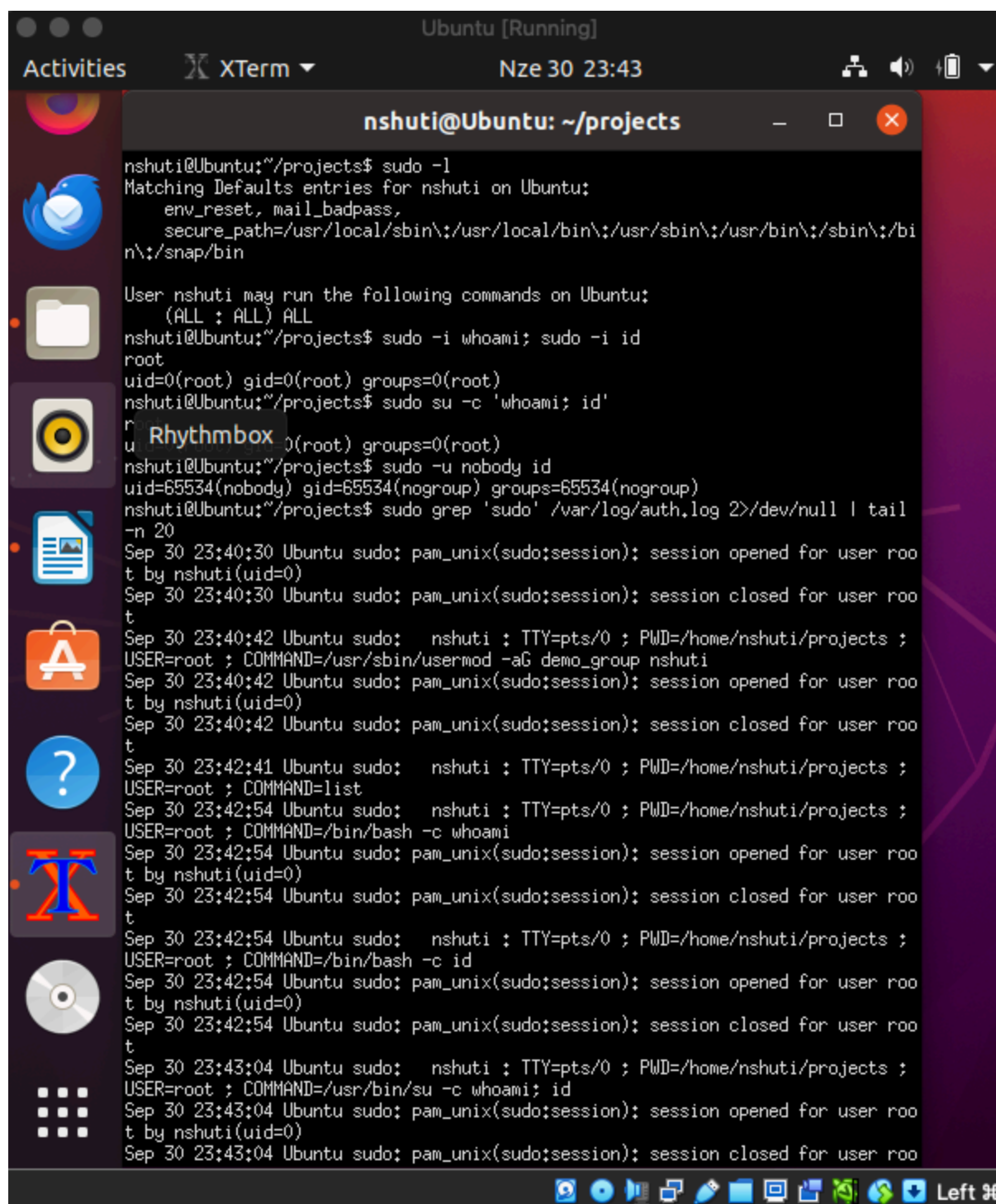
```
Ubuntu [Running]
Activities XTerm Nze 30 23:42
nshuti@Ubuntu: ~/projects

nshuti@Ubuntu:~/projects$ grep "^$(whoami):" /etc/group
nshuti:x:1000:
nshuti@Ubuntu:~/projects$ id
uid=1000(nshuti) gid=1000(nshuti) groups=1000(nshuti),27(sudo),995(vboxsf)
nshuti@Ubuntu:~/projects$ sudo groupadd demo_group 2>/dev/null || true
[sudo] password for nshuti:
nshuti@Ubuntu:~/projects$ sudo usermod -aG demo_group "$(whoami)" 2>/dev/null || true
nshuti@Ubuntu:~/projects$ echo "Before re-login:"
Before re-login:
nshuti@Ubuntu:~/projects$ id
uid=1000(nshuti) gid=1000(nshuti) groups=1000(nshuti),27(sudo),995(vboxsf)
nshuti@Ubuntu:~/projects$ echo "Using newgrp to get new group in this session:"
Using newgrp to get new group in this session:
nshuti@Ubuntu:~/projects$ newgrp demo_group -c 'id; groups'
nshuti@Ubuntu:~/projects$ exec su -l "$(whoami)" -c 'id'
Password:
uid=1000(nshuti) gid=1000(nshuti) groups=1000(nshuti),27(sudo),995(vboxsf),1001(demo_group)
nshuti@Ubuntu:~/projects$ getent group adm sudo www-data syslog | sed -n '1,200p'
adm:x:4:syslog
sudo:x:27:root
www-data:x:33:www-data
syslog:x:107:
nshuti@Ubuntu:~/projects$
```

Q16. Sudo Audit (1 pt)

- List privileges: `sudo -l`

- Compare: `sudo -i`, `sudo su`, `su -`
- Run as another user: `sudo -u nobody id`
- Audit logs: `grep sudo /var/log/auth.log`



Ubuntu [Running]

Activities XTerm Nze 30 23:43

nshuti@Ubuntu: ~/projects

```
nshuti@Ubuntu:~/projects$ sudo -l
Matching Defaults entries for nshuti on Ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nshuti may run the following commands on Ubuntu:
    (ALL : ALL) ALL
nshuti@Ubuntu:~/projects$ sudo -i whoami; sudo -i id
root
uid=0(root) gid=0(root) groups=0(root)
nshuti@Ubuntu:~/projects$ sudo su -c 'whoami; id'
root
uid=0(root) gid=0(root) groups=0(root)
nshuti@Ubuntu:~/projects$ sudo -u nobody id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
nshuti@Ubuntu:~/projects$ sudo grep 'sudo' /var/log/auth.log 2>/dev/null | tail
-n 20
Sep 30 23:40:30 Ubuntu sudo: pam_unix(sudo:session): session opened for user root
by nshuti(uid=0)
Sep 30 23:40:30 Ubuntu sudo: pam_unix(sudo:session): session closed for user root
Sep 30 23:40:42 Ubuntu sudo: nshuti : TTY=pts/0 ; PWD=/home/nshuti/projects ;
USER=root ; COMMAND=/usr/sbin/usermod -aG demo_group nshuti
Sep 30 23:40:42 Ubuntu sudo: pam_unix(sudo:session): session opened for user root
by nshuti(uid=0)
Sep 30 23:40:42 Ubuntu sudo: pam_unix(sudo:session): session closed for user root
Sep 30 23:42:41 Ubuntu sudo: nshuti : TTY=pts/0 ; PWD=/home/nshuti/projects ;
USER=root ; COMMAND=list
Sep 30 23:42:54 Ubuntu sudo: nshuti : TTY=pts/0 ; PWD=/home/nshuti/projects ;
USER=root ; COMMAND=/bin/bash -c whoami
Sep 30 23:42:54 Ubuntu sudo: pam_unix(sudo:session): session opened for user root
by nshuti(uid=0)
Sep 30 23:42:54 Ubuntu sudo: pam_unix(sudo:session): session closed for user root
Sep 30 23:42:54 Ubuntu sudo: nshuti : TTY=pts/0 ; PWD=/home/nshuti/projects ;
USER=root ; COMMAND=/bin/bash -c id
Sep 30 23:42:54 Ubuntu sudo: pam_unix(sudo:session): session opened for user root
by nshuti(uid=0)
Sep 30 23:42:54 Ubuntu sudo: pam_unix(sudo:session): session closed for user root
Sep 30 23:43:04 Ubuntu sudo: nshuti : TTY=pts/0 ; PWD=/home/nshuti/projects ;
USER=root ; COMMAND=/usr/bin/su -c whoami; id
Sep 30 23:43:04 Ubuntu sudo: pam_unix(sudo:session): session opened for user root
by nshuti(uid=0)
Sep 30 23:43:04 Ubuntu sudo: pam_unix(sudo:session): session closed for user root
```

Bonus Q17. Forensic Environment (2 pts)

- Create files: `touch regular.txt`
- Symlinks: `ln -s regular.txt sym.txt`
- Hard links: `ln regular.txt hard.txt`
- SUID/SGID: `chmod 4755 suid_file`
- Sticky dir: `chmod 1777 sticky_dir`
- Archives: `tar -czf file.tar.gz regular.txt`

```
Ubuntu [Running]
Activities XTerm Nze 30 23:48

nshuti@Ubuntu: ~/projects/forensic

-rwsr-xr-x 1 nshuti nshuti 0 Nze 30 23:45 setuid_exec
-rwxrwxrwt 1 nshuti nshuti 0 Nze 30 23:45 sticky_dir
lrwxrwxrwx 1 nshuti nshuti 11 Nze 30 23:44 symlink_to_regular.txt -> regular.
txt
nshuti@Ubuntu:~/projects/forensic$ getfacl owned_by_root.txt 2>/dev/null | sed -
n '1,200p'
# file: owned_by_root.txt
# owner: nshuti
# group: nshuti
user::rw-
user:nshuti:rwx
group::rw-
mask::rwx
other::r--

nshuti@Ubuntu:~/projects/forensic$ file symlink_to_regular.txt
symlink_to_regular.txt: symbolic link to regular.txt
nshuti@Ubuntu:~/projects/forensic$ ls -li
total 20
533407 drwxrwxr-x 2 nshuti nshuti 4096 Nze 30 23:46 archives
533400 drwxrwxr-x 2 nshuti nshuti 4096 Nze 30 23:44 dir1
533401 drwxrwxr-x 2 nshuti nshuti 4096 Nze 30 23:44 dir2
533399 -rw-rw-r-- 2 nshuti nshuti 13 Nze 30 23:44 hardlink_regular.txt
533406 -rw-rwxr--+ 1 nshuti nshuti 0 Nze 30 23:45 owned_by_root.txt
533399 -rw-rw-r-- 2 nshuti nshuti 13 Nze 30 23:44 regular.txt
533404 -rwxr-sr-x 1 nshuti nshuti 0 Nze 30 23:45 setgid_exec
533403 -rwsr-xr-x 1 nshuti nshuti 0 Nze 30 23:45 setuid_exec
533405 -rwxrwxrwt 1 nshuti nshuti 0 Nze 30 23:45 sticky_dir
533402 lrwxrwxrwx 1 nshuti nshuti 11 Nze 30 23:44 symlink_to_regular.txt -> r
egular.txt
nshuti@Ubuntu:~/projects/forensic$ find . -perm /6000 -type f -ls
533403 0 -rwsr-xr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setuid
_exec
XTerm 0 -rwxr-sr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setgid
nshuti@Ubuntu:~/projects/forensic$ find . -perm /6000 -type f -ls
533403 0 -rwsr-xr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setuid
_exec
533404 0 -rwxr-sr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setgid
_exec
nshuti@Ubuntu:~/projects/forensic$ find . -perm -2000 -type f -ls
533404 0 -rwxr-sr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setgid
_exec
nshuti@Ubuntu:~/projects/forensic$ find . -perm -4000 -type f -ls
533403 0 -rwsr-xr-x 1 nshuti nshuti 0 Nze 30 23:45 ./setuid
_exec
nshuti@Ubuntu:~/projects/forensic$
```

Reflection

- **What I Did:** Summarized Linux filesystem investigation, permissions, backups, and archives.
- **Why I Did It:** To simulate forensic investigation and system admin tasks.
- **What I Learned:** File manipulation, wildcard power, backup strategies, security audit basics.
- **Challenges:** VirtualBox Guest Additions setup, permissions issues.
- **Recommendations:** Automate repetitive tasks with scripts, always test dangerous commands with `-print` before executing.