NAMES: NIYOMUFASHA Olive

ID:26033

Assignment2

1. Directories likely to contain modified configs, malicious binaries and logs:

   -/var: (/var/log/auth.log).An attacker might replace delete logs to hide an intrusion,evidence:Missing entries or unusual access.

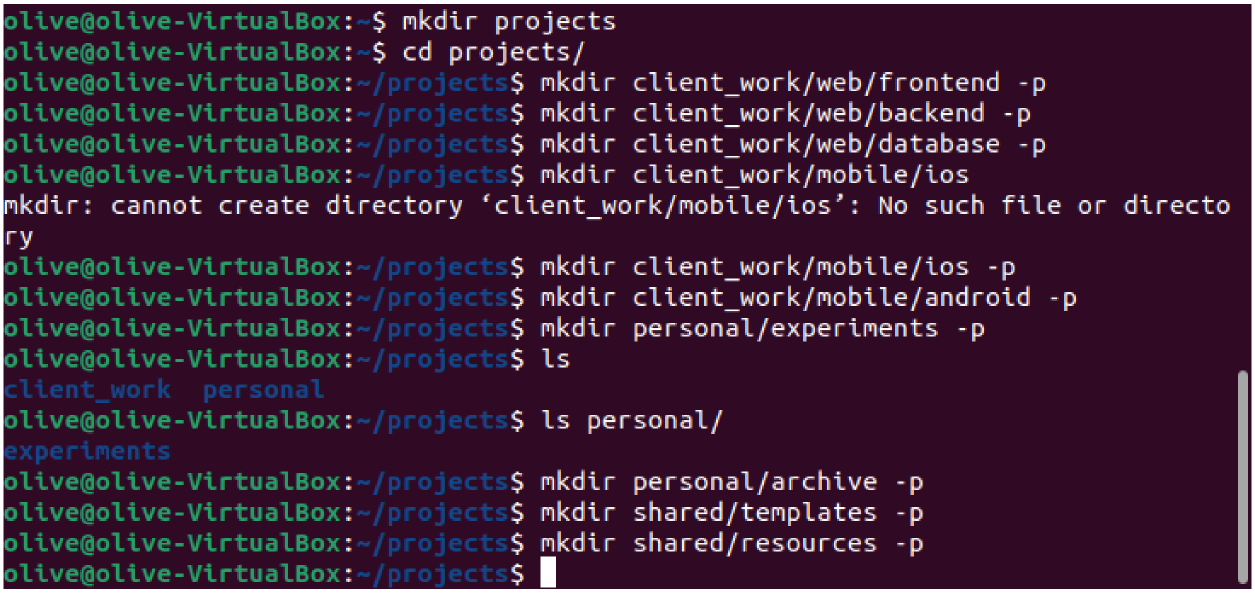
   -/etc: System configuration files(/etc/passwd,/etc/shadow).an attacker might modify for persistence
   -/bin:Essential binaries (ls,cp),An attacker might replace them with trojans for backdoors ,evidence:unexpected file sizes or hashes.

   And the reasoning For All

   -/var:variable data like logs:attackers erase evidence.
   -/etc: Config files :attackers modify for privilege escalation.
   -/bin: Essential binaries;attackers replace for malicious execution.
   -/usr: Secondary binaries similar to /bin,attackers target for non-essential tools
   -/temp:temprary files: attackers use for staging malware,as its writable
   -/boot: boot files(kernal): attackers modify for rootkits
   -/home: User homes:attackers target for user-level persistence(eg.,.sshkeys)

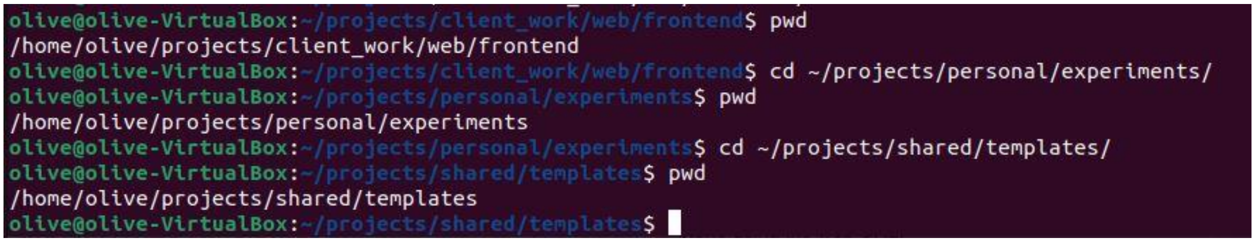
2.Mkdir –p: creates parent directories as needed and does not throw errors if directories already exist

{}: those braces expansion creates multiple directory paths from a single command.



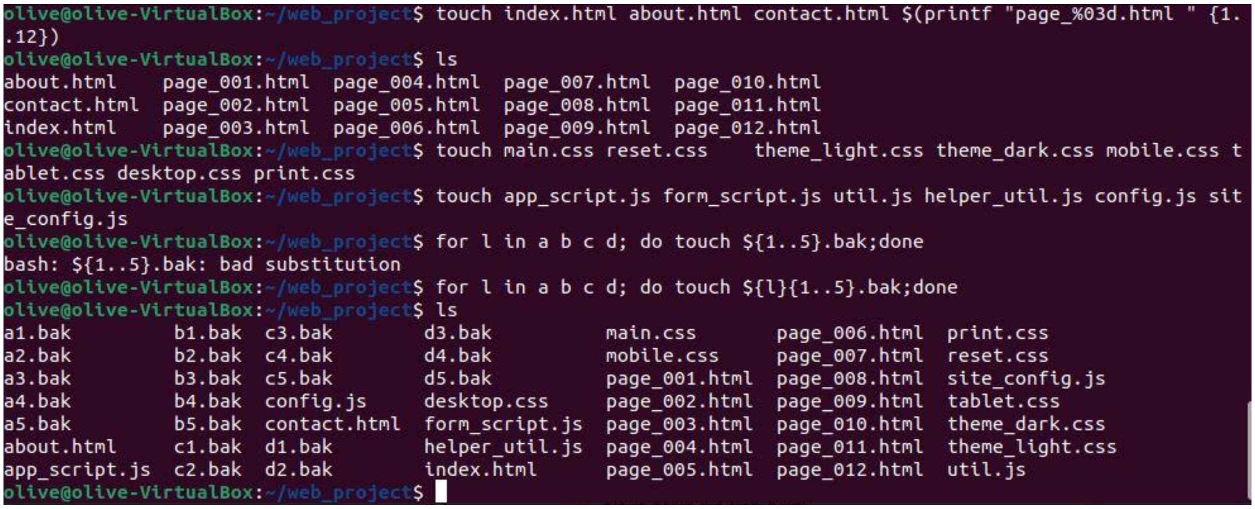
```
olive@olive-VirtualBox:~$ mkdir projects
olive@olive-VirtualBox:~$ cd projects/
olive@olive-VirtualBox:~/projects$ mkdir client_work/web/frontend -p
olive@olive-VirtualBox:~/projects$ mkdir client_work/web/backend -p
olive@olive-VirtualBox:~/projects$ mkdir client_work/web/database -p
olive@olive-VirtualBox:~/projects$ mkdir client_work/mobile/ios
mkdir: cannot create directory ‘client_work/mobile/ios’: No such file or directo
ry
olive@olive-VirtualBox:~/projects$ mkdir client_work/mobile/ios -p
olive@olive-VirtualBox:~/projects$ mkdir client_work/mobile/android -p
olive@olive-VirtualBox:~/projects$ mkdir personal/experiments -p
olive@olive-VirtualBox:~/projects$ ls
client_work  personal
olive@olive-VirtualBox:~/projects$ ls personal/
experiments
olive@olive-VirtualBox:~/projects$ mkdir personal/archive -p
olive@olive-VirtualBox:~/projects$ mkdir shared/templates -p
olive@olive-VirtualBox:~/projects$ mkdir shared/resources -p
olive@olive-VirtualBox:~/projects$ 
```

3. creating the project directories: this done without using absolute



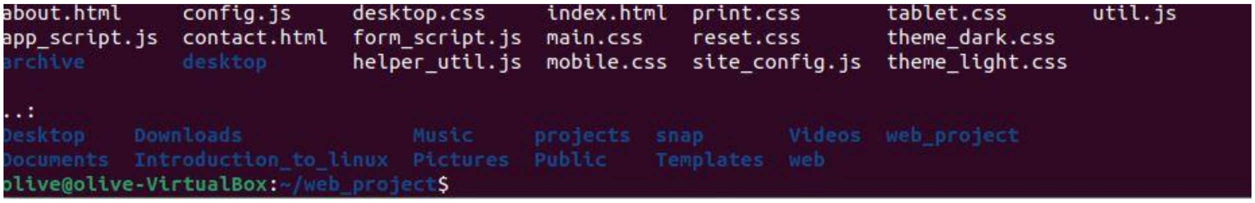
```
olive@olive-VirtualBox:~/projects/client_work/web/frontend$ pwd
/home/olive/projects/client_work/web/frontend
olive@olive-VirtualBox:~/projects/client_work/web/frontend$ cd ~/projects/personal/experiments/
olive@olive-VirtualBox:~/projects/personal/experiments$ pwd
/home/olive/projects/personal/experiments
olive@olive-VirtualBox:~/projects/personal/experiments$ cd ~/projects/shared/templates/
olive@olive-VirtualBox:~/projects/shared/templates$ pwd
/home/olive/projects/shared/templates
olive@olive-VirtualBox:~/projects/shared/templates$ 
```

4. creating files and CSS:and to list them all.



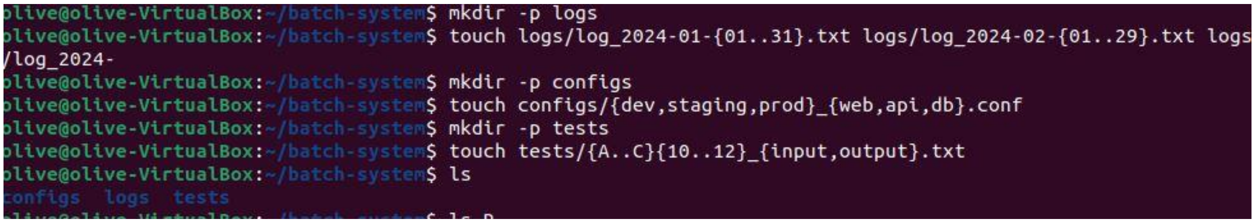
```
olive@olive-VirtualBox:~/web_project$ touch index.html about.html contact.html $(printf "page_%03d.html " {1.
.12})
olive@olive-VirtualBox:~/web_project$ ls
about.html    page_001.html  page_004.html  page_007.html  page_010.html
contact.html  page_002.html  page_005.html  page_008.html  page_011.html
index.html    page_003.html  page_006.html  page_009.html  page_012.html
olive@olive-VirtualBox:~/web_project$ touch main.css reset.css    theme_light.css theme_dark.css mobile.css t
ablet.css desktop.css print.css
olive@olive-VirtualBox:~/web_project$ touch app_script.js form_script.js util.js helper_util.js config.js sit
e_config.js
olive@olive-VirtualBox:~/web_project$ for l in a b c d; do touch ${1..5}.bak;done
bash: ${1..5}.bak: bad substitution
olive@olive-VirtualBox:~/web_project$ for l in a b c d; do touch ${l}{1..5}.bak;done
olive@olive-VirtualBox:~/web_project$ ls
a1.bak        b1.bak  c3.bak        d3.bak         main.css       page_006.html  print.css
a2.bak        b2.bak  c4.bak        d4.bak         mobile.css     page_007.html  reset.css
a3.bak        b3.bak  c5.bak        d5.bak         page_001.html  page_008.html  site_config.js
a4.bak        b4.bak  config.js     desktop.css    page_002.html  page_009.html  tablet.css
a5.bak        b5.bak  contact.html  form_script.js page_003.html  page_010.html  theme_dark.css
about.html    c1.bak  d1.bak        helper_util.js page_004.html  page_011.html  theme_light.css
app_script.js c2.bak  d2.bak        index.html     page_005.html  page_012.html  util.js
olive@olive-VirtualBox:~/web_project$ 
```

5.here all command are being listed



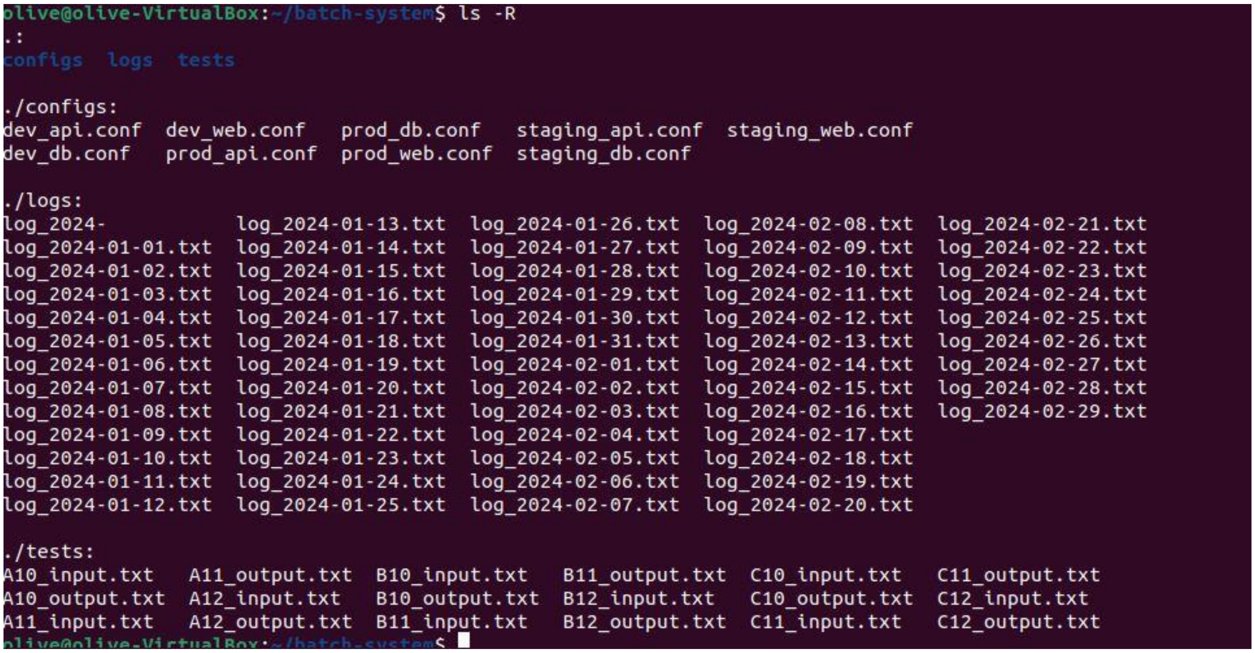
```
about.html     config.js     desktop.css     index.html  print.css       tablet.css       util.js
app_script.js  contact.html  form_script.js  main.css    reset.css       theme_dark.css
archive        desktop       helper_util.js  mobile.css  site_config.js  theme_light.css

..:
Desktop    Downloads            Music     projects  snap       Videos  web_project
Documents  Introduction_to_linux  Pictures  Public    Templates  web
olive@olive-VirtualBox:~/web_project$
```

6. For Log File



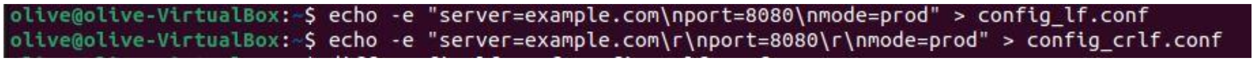
```
olive@olive-VirtualBox:~/batch-system$ mkdir -p logs
olive@olive-VirtualBox:~/batch-system$ touch logs/log_2024-01-{01..31}.txt logs/log_2024-02-{01..29}.txt logs
/log_2024-
olive@olive-VirtualBox:~/batch-system$ mkdir -p configs
olive@olive-VirtualBox:~/batch-system$ touch configs/{dev,staging,prod}_{web,api,db}.conf
olive@olive-VirtualBox:~/batch-system$ mkdir -p tests
olive@olive-VirtualBox:~/batch-system$ touch tests/{A..C}{10..12}_{input,output}.txt
olive@olive-VirtualBox:~/batch-system$ ls
configs  logs  tests
olive@olive-VirtualBox:~/batch-system$ ls -R
```

6b. For Testing and configuring



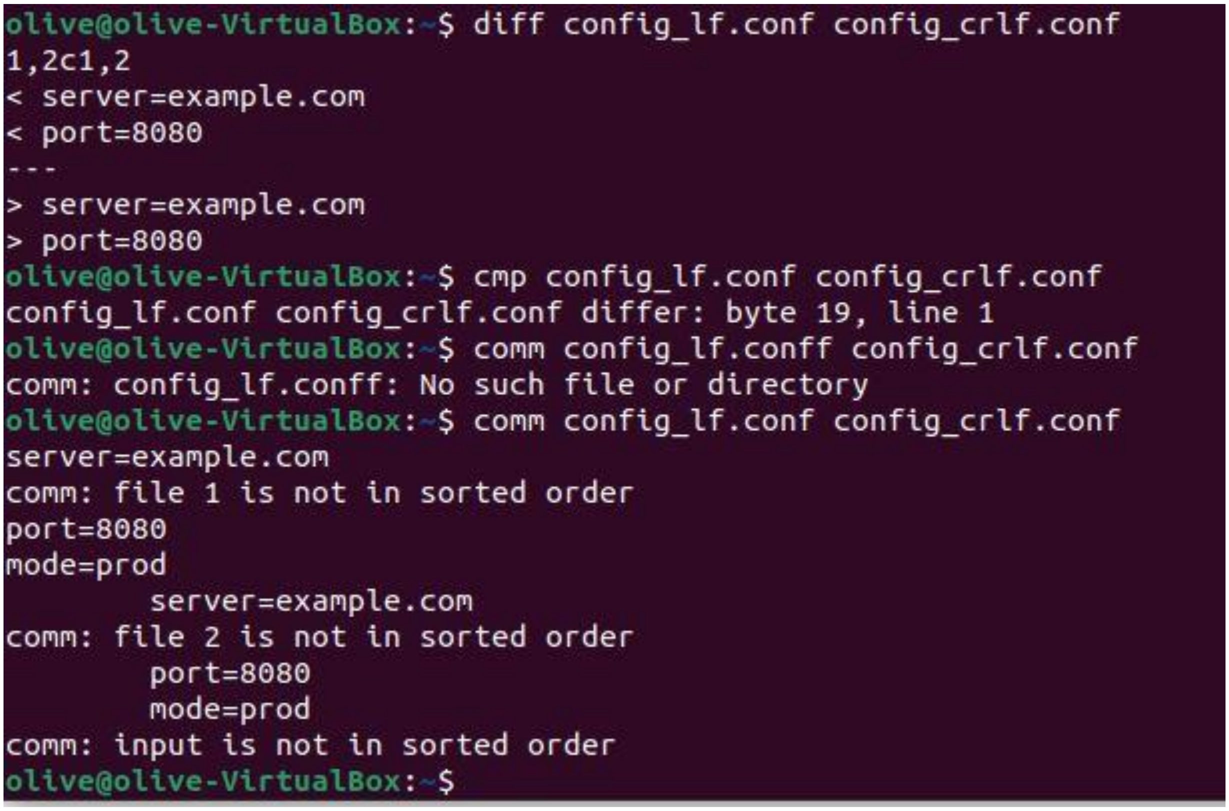
```
olive@olive-VirtualBox:~/batch-system$ ls -R
.:
configs  logs  tests

./configs:
dev_api.conf  dev_web.conf   prod_db.conf   staging_api.conf  staging_web.conf
dev_db.conf   prod_api.conf  prod_web.conf  staging_db.conf

./logs:
log_2024-           log_2024-01-13.txt  log_2024-01-26.txt  log_2024-02-08.txt  log_2024-02-21.txt
log_2024-01-01.txt  log_2024-01-14.txt  log_2024-01-27.txt  log_2024-02-09.txt  log_2024-02-22.txt
log_2024-01-02.txt  log_2024-01-15.txt  log_2024-01-28.txt  log_2024-02-10.txt  log_2024-02-23.txt
log_2024-01-03.txt  log_2024-01-16.txt  log_2024-01-29.txt  log_2024-02-11.txt  log_2024-02-24.txt
log_2024-01-04.txt  log_2024-01-17.txt  log_2024-01-30.txt  log_2024-02-12.txt  log_2024-02-25.txt
log_2024-01-05.txt  log_2024-01-18.txt  log_2024-01-31.txt  log_2024-02-13.txt  log_2024-02-26.txt
log_2024-01-06.txt  log_2024-01-19.txt  log_2024-02-01.txt  log_2024-02-14.txt  log_2024-02-27.txt
log_2024-01-07.txt  log_2024-01-20.txt  log_2024-02-02.txt  log_2024-02-15.txt  log_2024-02-28.txt
log_2024-01-08.txt  log_2024-01-21.txt  log_2024-02-03.txt  log_2024-02-16.txt  log_2024-02-29.txt
log_2024-01-09.txt  log_2024-01-22.txt  log_2024-02-04.txt  log_2024-02-17.txt
log_2024-01-10.txt  log_2024-01-23.txt  log_2024-02-05.txt  log_2024-02-18.txt
log_2024-01-11.txt  log_2024-01-24.txt  log_2024-02-06.txt  log_2024-02-19.txt
log_2024-01-12.txt  log_2024-01-25.txt  log_2024-02-07.txt  log_2024-02-20.txt

./tests:
A10_input.txt   A11_output.txt  B10_input.txt   B11_output.txt  C10_input.txt   C11_output.txt
A10_output.txt  A12_input.txt   B10_output.txt  B12_input.txt   C10_output.txt  C12_input.txt
A11_input.txt   A12_output.txt  B11_input.txt   B12_output.txt  C11_input.txt   C12_output.txt
olive@olive-VirtualBox:~/batch-system$
```

7. creating different files. The picture below shows how I created different files



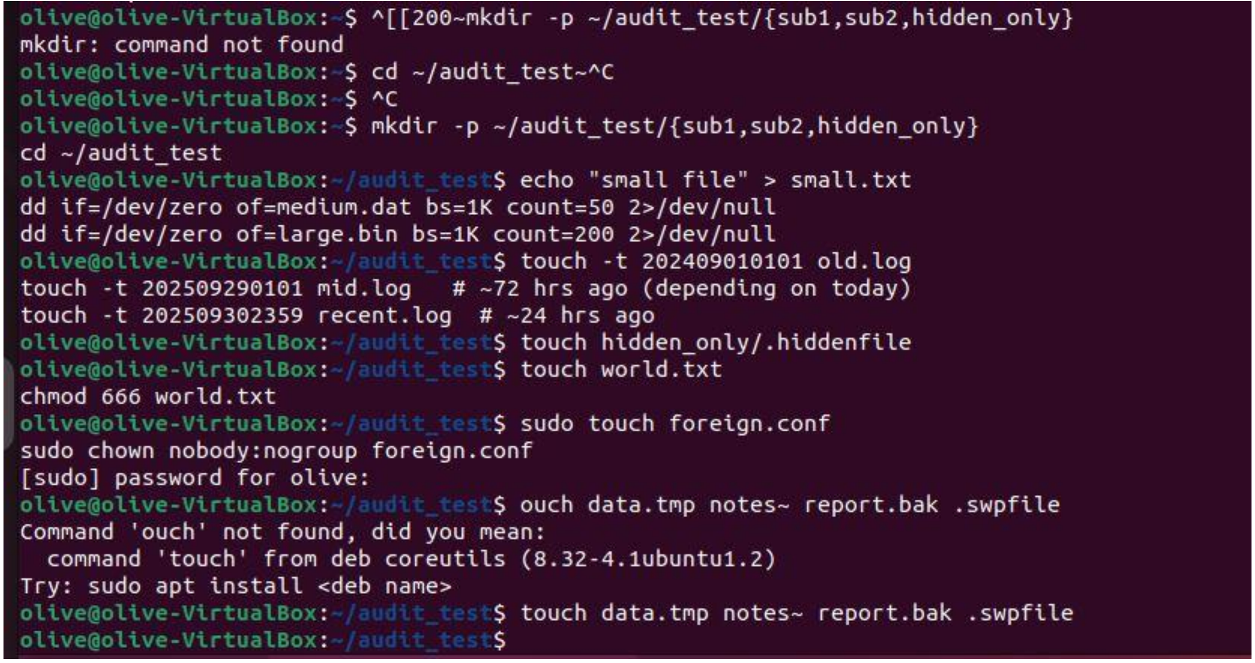
```
olive@olive-VirtualBox:~$ echo -e "server=example.com\nport=8080\nmode=prod" > config_lf.conf
olive@olive-VirtualBox:~$ echo -e "server=example.com\r\nport=8080\r\nmode=prod" > config_crlf.conf
```

The difference between files created



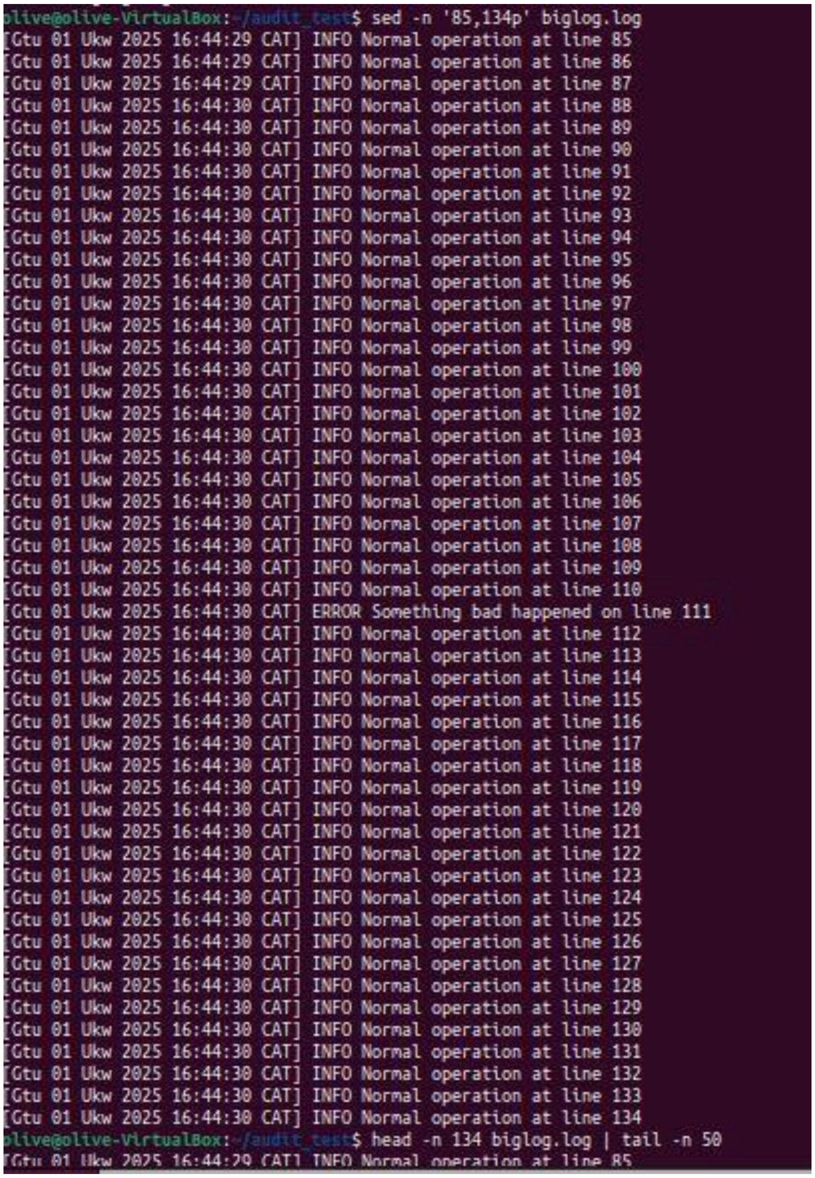
```
olive@olive-VirtualBox:~$ diff config_lf.conf config_crlf.conf
1,2c1,2
< server=example.com
< port=8080
---
> server=example.com
> port=8080
olive@olive-VirtualBox:~$ cmp config_lf.conf config_crlf.conf
config_lf.conf config_crlf.conf differ: byte 19, line 1
olive@olive-VirtualBox:~$ comm config_lf.conff config_crlf.conf
comm: config_lf.conff: No such file or directory
olive@olive-VirtualBox:~$ comm config_lf.conf config_crlf.conf
server=example.com
comm: file 1 is not in sorted order
port=8080
mode=prod
        server=example.com
comm: file 2 is not in sorted order
        port=8080
        mode=prod
comm: input is not in sorted order
olive@olive-VirtualBox:~$
```

8. Create a test environment with diverse file types, sizes, and ages



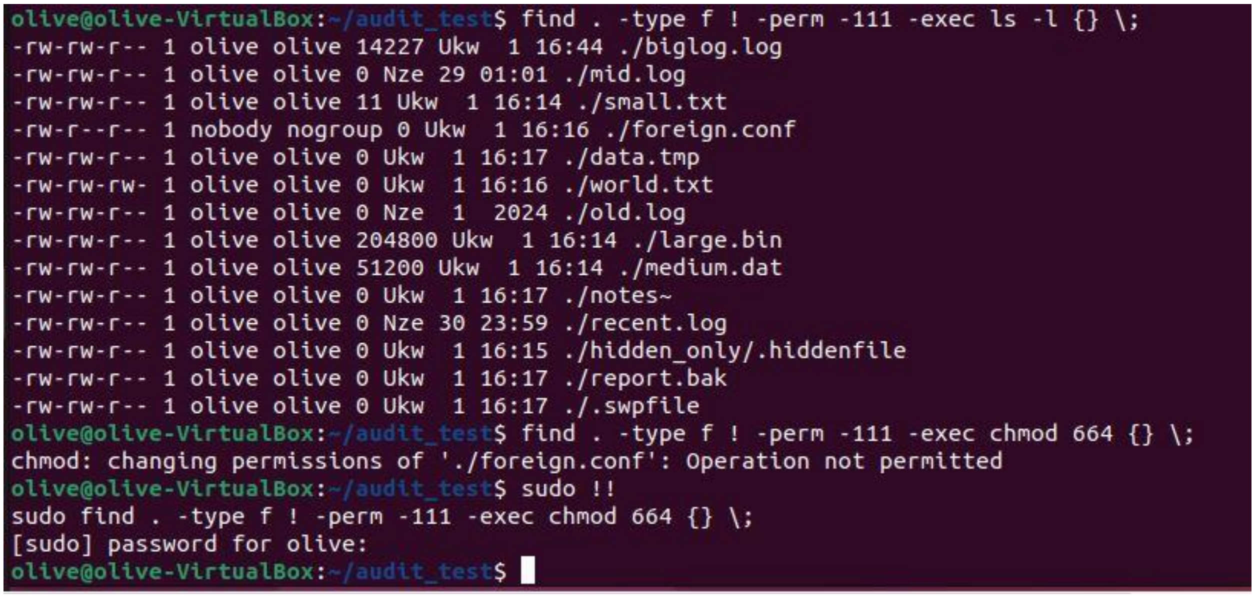
```
olive@olive-VirtualBox:~$ ^[[200~mkdir -p ~/audit_test/{sub1,sub2,hidden_only}
mkdir: command not found
olive@olive-VirtualBox:~$ cd ~/audit_test~^C
olive@olive-VirtualBox:~$ ^C
olive@olive-VirtualBox:~$ mkdir -p ~/audit_test/{sub1,sub2,hidden_only}
cd ~/audit_test
olive@olive-VirtualBox:~/audit_test$ echo "small file" > small.txt
dd if=/dev/zero of=medium.dat bs=1K count=50 2>/dev/null
dd if=/dev/zero of=large.bin bs=1K count=200 2>/dev/null
olive@olive-VirtualBox:~/audit_test$ touch -t 202409010101 old.log
touch -t 202509290101 mid.log   # ~72 hrs ago (depending on today)
touch -t 202509302359 recent.log  # ~24 hrs ago
olive@olive-VirtualBox:~/audit_test$ touch hidden_only/.hiddenfile
olive@olive-VirtualBox:~/audit_test$ touch world.txt
chmod 666 world.txt
olive@olive-VirtualBox:~/audit_test$ sudo touch foreign.conf
sudo chown nobody:nogroup foreign.conf
[sudo] password for olive:
olive@olive-VirtualBox:~/audit_test$ ouch data.tmp notes~ report.bak .swpfile
Command 'ouch' not found, did you mean:
  command 'touch' from deb coreutils (8.32-4.1ubuntu1.2)
Try: sudo apt install <deb name>
olive@olive-VirtualBox:~/audit_test$ touch data.tmp notes~ report.bak .swpfile
olive@olive-VirtualBox:~/audit_test$
```

9. Show how to: display the middle 50 lines of the file, find the last occurrence of a specific word and show 5 lines of context,



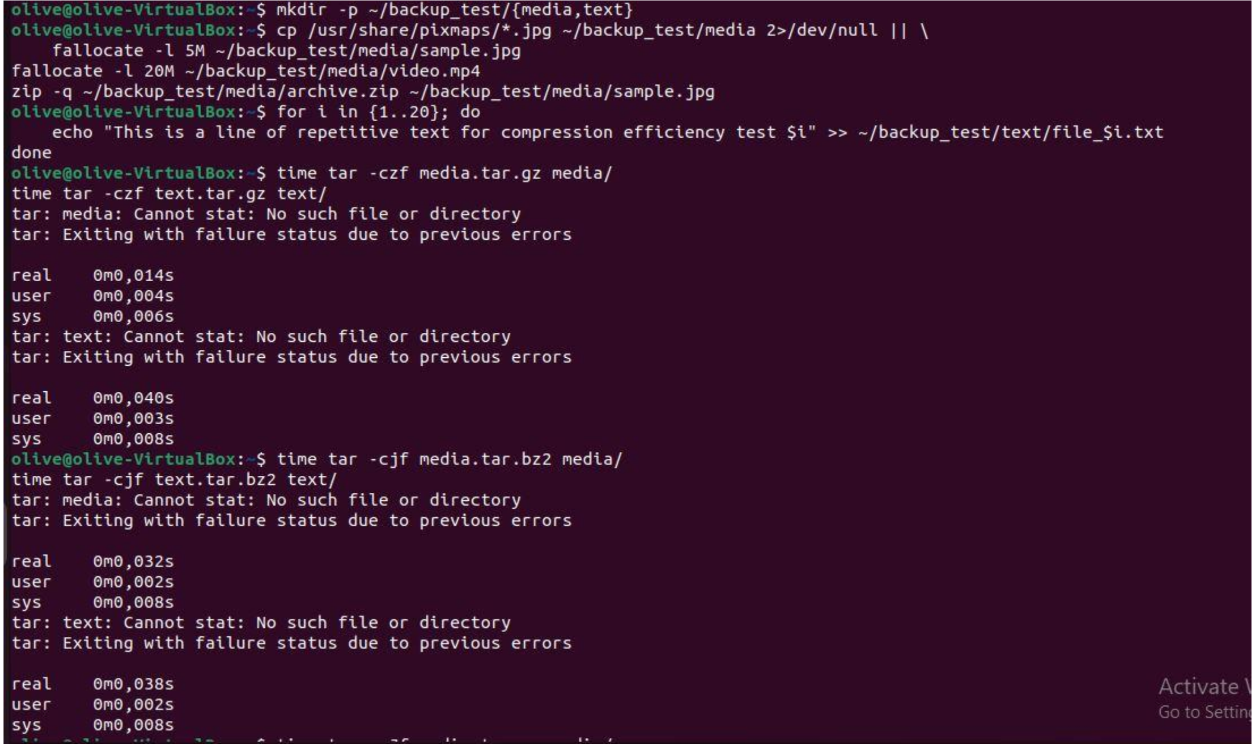
```
olive@olive-VirtualBox:~/audit_test$ sed -n '85,134p' biglog.log
[Gtu 01 Ukw 2025 16:44:29 CAT] INFO Normal operation at line 85
[Gtu 01 Ukw 2025 16:44:29 CAT] INFO Normal operation at line 86
[Gtu 01 Ukw 2025 16:44:29 CAT] INFO Normal operation at line 87
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 88
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 89
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 90
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 91
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 92
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 93
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 94
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 95
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 96
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 97
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 98
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 99
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 100
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 101
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 102
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 103
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 104
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 105
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 106
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 107
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 108
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 109
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 110
[Gtu 01 Ukw 2025 16:44:30 CAT] ERROR Something bad happened on line 111
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 112
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 113
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 114
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 115
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 116
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 117
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 118
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 119
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 120
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 121
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 122
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 123
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 124
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 125
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 126
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 127
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 128
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 129
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 130
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 131
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 132
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 133
[Gtu 01 Ukw 2025 16:44:30 CAT] INFO Normal operation at line 134
olive@olive-VirtualBox:~/audit_test$ head -n 134 biglog.log | tail -n 50
[Gtu 01 Ukw 2025 16:44:29 CAT] INFO Normal operation at line 85
```

10 changing permission



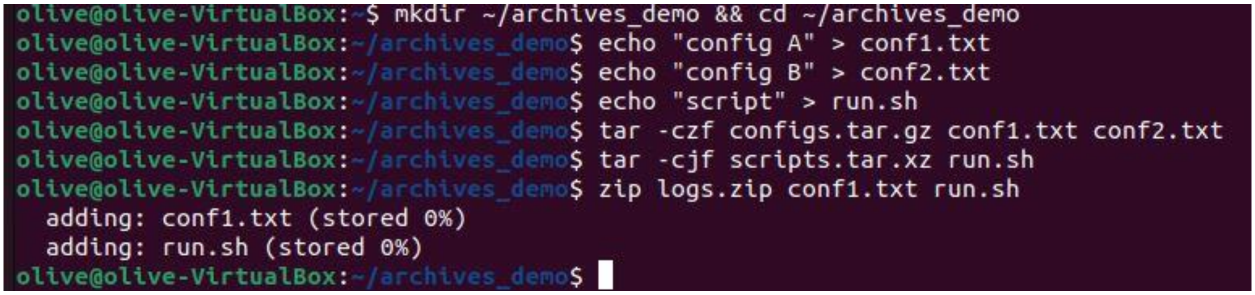
```
olive@olive-VirtualBox:~/audit_test$ find . -type f ! -perm -111 -exec ls -l {} \;
-rw-rw-r-- 1 olive olive 14227 Ukw  1 16:44 ./biglog.log
-rw-rw-r-- 1 olive olive 0 Nze 29 01:01 ./mid.log
-rw-rw-r-- 1 olive olive 11 Ukw  1 16:14 ./small.txt
-rw-r--r-- 1 nobody nogroup 0 Ukw  1 16:16 ./foreign.conf
-rw-rw-r-- 1 olive olive 0 Ukw  1 16:17 ./data.tmp
-rw-rw-rw- 1 olive olive 0 Ukw  1 16:16 ./world.txt
-rw-rw-r-- 1 olive olive 0 Nze  1  2024 ./old.log
-rw-rw-r-- 1 olive olive 204800 Ukw  1 16:14 ./large.bin
-rw-rw-r-- 1 olive olive 51200 Ukw  1 16:14 ./medium.dat
-rw-rw-r-- 1 olive olive 0 Ukw  1 16:17 ./notes~
-rw-rw-r-- 1 olive olive 0 Nze 30 23:59 ./recent.log
-rw-rw-r-- 1 olive olive 0 Ukw  1 16:15 ./hidden_only/.hiddenfile
-rw-rw-r-- 1 olive olive 0 Ukw  1 16:17 ./report.bak
-rw-rw-r-- 1 olive olive 0 Ukw  1 16:17 ./.swpfile
olive@olive-VirtualBox:~/audit_test$ find . -type f ! -perm -111 -exec chmod 664 {} \;
chmod: changing permissions of './foreign.conf': Operation not permitted
olive@olive-VirtualBox:~/audit_test$ sudo !!
sudo find . -type f ! -perm -111 -exec chmod 664 {} \;
[sudo] password for olive:
olive@olive-VirtualBox:~/audit_test$ 
```

11. Creating directories with different file types and sizes, then create archives



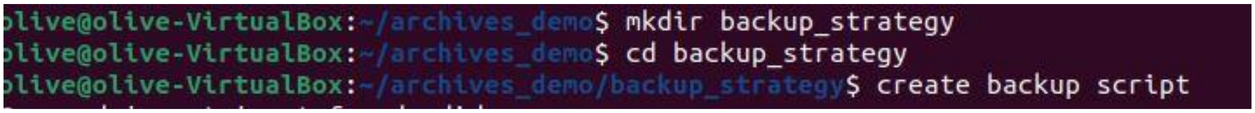
```
olive@olive-VirtualBox:~$ mkdir -p ~/backup_test/{media,text}
olive@olive-VirtualBox:~$ cp /usr/share/pixmaps/*.jpg ~/backup_test/media 2>/dev/null || \
    fallocate -l 5M ~/backup_test/media/sample.jpg
fallocate -l 20M ~/backup_test/media/video.mp4
zip -q ~/backup_test/media/archive.zip ~/backup_test/media/sample.jpg
olive@olive-VirtualBox:~$ for i in {1..20}; do
    echo "This is a line of repetitive text for compression efficiency test $i" >> ~/backup_test/text/file_$i.txt
done
olive@olive-VirtualBox:~$ time tar -czf media.tar.gz media/
time tar -czf text.tar.gz text/
tar: media: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

real    0m0,014s
user    0m0,004s
sys     0m0,006s
tar: text: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

real    0m0,040s
user    0m0,003s
sys     0m0,008s
olive@olive-VirtualBox:~$ time tar -cjf media.tar.bz2 media/
time tar -cjf text.tar.bz2 text/
tar: media: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

real    0m0,032s
user    0m0,002s
sys     0m0,008s
tar: text: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

real    0m0,038s
user    0m0,002s
sys     0m0,008s
```

12 Multiple archive



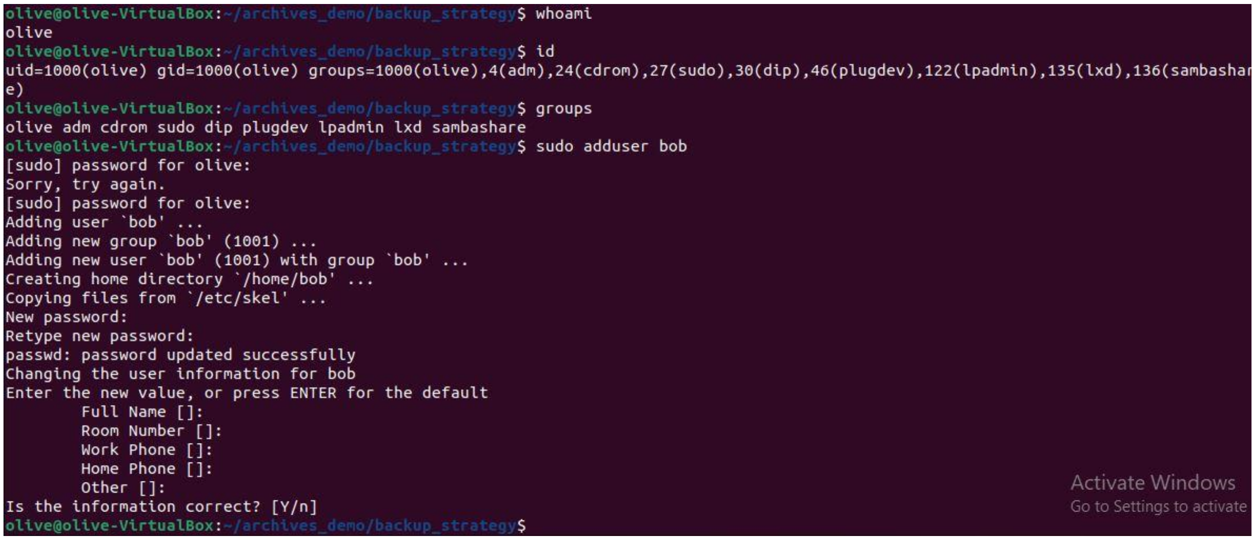
```
olive@olive-VirtualBox:~$ mkdir ~/archives_demo && cd ~/archives_demo
olive@olive-VirtualBox:~/archives_demo$ echo "config A" > conf1.txt
olive@olive-VirtualBox:~/archives_demo$ echo "config B" > conf2.txt
olive@olive-VirtualBox:~/archives_demo$ echo "script" > run.sh
olive@olive-VirtualBox:~/archives_demo$ tar -czf configs.tar.gz conf1.txt conf2.txt
olive@olive-VirtualBox:~/archives_demo$ tar -cjf scripts.tar.xz run.sh
olive@olive-VirtualBox:~/archives_demo$ zip logs.zip conf1.txt run.sh
  adding: conf1.txt (stored 0%)
  adding: run.sh (stored 0%)
olive@olive-VirtualBox:~/archives_demo$ 
```

13. Create archives that include metadata



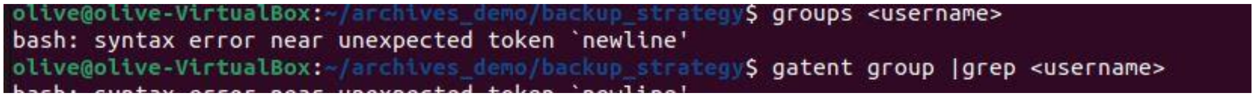
```
olive@olive-VirtualBox:~/archives_demo$ mkdir backup_strategy
olive@olive-VirtualBox:~/archives_demo$ cd backup_strategy
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ create backup script
```

14 Compare your user's groups with another user account's groups



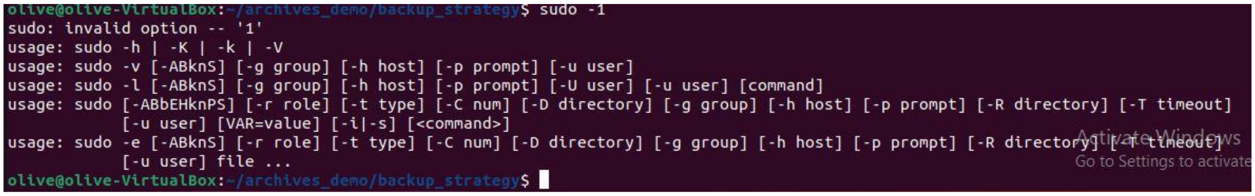
```
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ whoami
olive
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ id
uid=1000(olive) gid=1000(olive) groups=1000(olive),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),122(lpadmin),135(lxd),136(sambashar
e)
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ groups
olive adm cdrom sudo dip plugdev lpadmin lxd sambashare
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ sudo adduser bob
[sudo] password for olive:
Sorry, try again.
[sudo] password for olive:
Adding user `bob' ...
Adding new group `bob' (1001) ...
Adding new user `bob' (1001) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for bob
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
olive@olive-VirtualBox:~/archives_demo/backup_strategy$
```

15. analyse current user



```
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ groups <username>
bash: syntax error near unexpected token `newline'
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ gatent group |grep <username>
```

16 check current Group Membership



```
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ sudo -1
sudo: invalid option -- '1'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-ABbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
            [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-ABknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
            [-u user] file ...
olive@olive-VirtualBox:~/archives_demo/backup_strategy$ 
```