Names: ISHIMWE Belise Date 30th Sept 2025

ID: 27304

Lecturer: KAYITARE Elie

## Introduction to Linux Assignment#2.

ans1. Investigating a Compromised System.

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

-/etc: System configuration files (e.g., /etc/passwd, /etc/shadow). An attacker might modify for persistence (e.g., add users). Evidence: Altered timestamps or unauthorized changes.

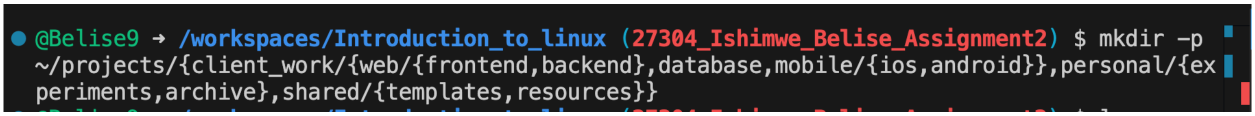
-/bin: Essential binaries (e.g., ls, cp). An attacker might replace them with trojans for backdoors. Evidence: Unexpected file sizes or hashes.

-/var: Log files (e.g., /var/log/auth.log). An attacker might delete logs to hide an intrusion. Evidence: Missing entries or unusual access.

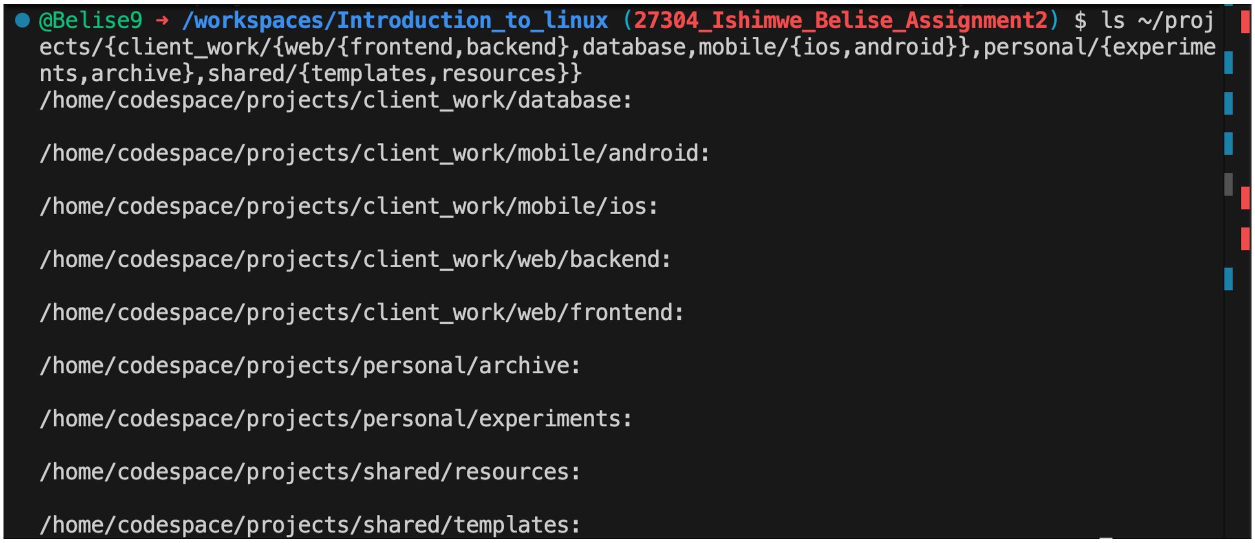
Reasoning for all:

- /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).

Ans2.

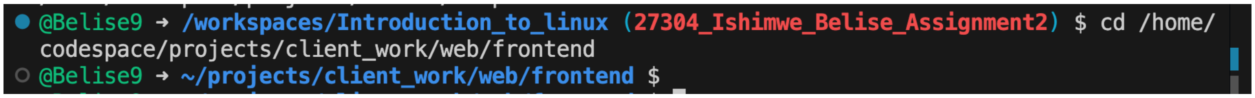


```
● @Belise9 → /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ mkdir -p
  ~/projects/{client_work/{web/{frontend,backend},database,mobile/{ios,android}},personal/{ex
  periments,archive},shared/{templates,resources}}
```

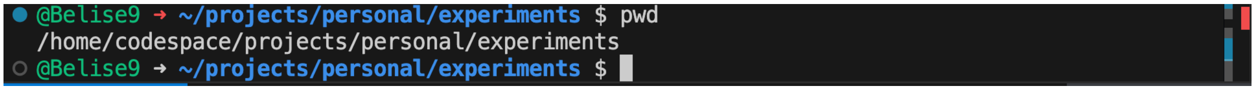


```
● @Belise9 → /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ ls ~/proj
  ects/{client_work/{web/{frontend,backend},database,mobile/{ios,android}},personal/{experime
  nts,archive},shared/{templates,resources}}
  /home/codespace/projects/client_work/database:

  /home/codespace/projects/client_work/mobile/android:

  /home/codespace/projects/client_work/mobile/ios:

  /home/codespace/projects/client_work/web/backend:

  /home/codespace/projects/client_work/web/frontend:

  /home/codespace/projects/personal/archive:

  /home/codespace/projects/personal/experiments:

  /home/codespace/projects/shared/resources:

  /home/codespace/projects/shared/templates:
```

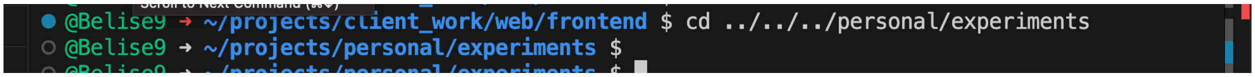
Ans3



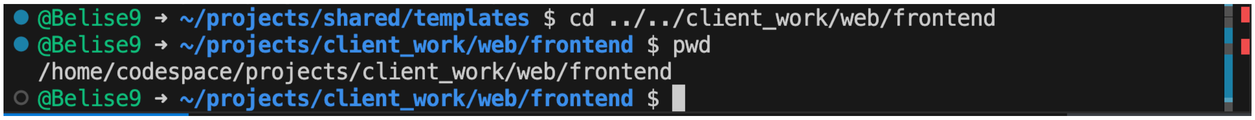
```
● @Belise9 → /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ cd /home/
  codespace/projects/client_work/web/frontend
○ @Belise9 → ~/projects/client_work/web/frontend $
```



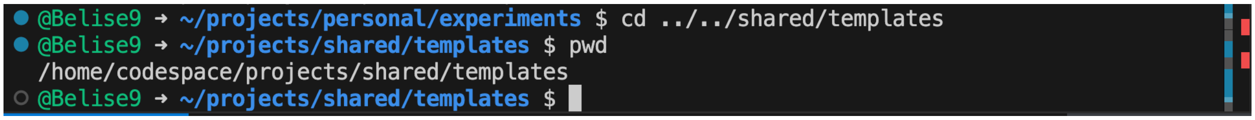
```
● @Belise9 → ~/projects/personal/experiments $ pwd
  /home/codespace/projects/personal/experiments
○ @Belise9 → ~/projects/personal/experiments $
```



```
● @Belise9 → ~/projects/client_work/web/frontend $ cd ../../../personal/experiments
○ @Belise9 → ~/projects/personal/experiments $
```



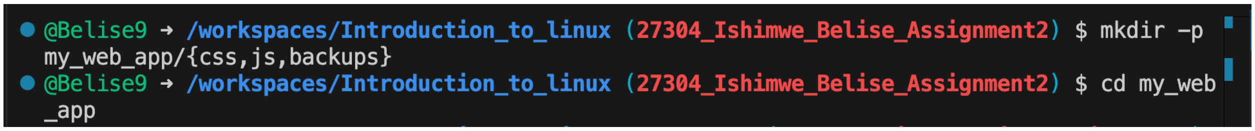
```
● @Belise9 → ~/projects/shared/templates $ cd ../../client_work/web/frontend
● @Belise9 → ~/projects/client_work/web/frontend $ pwd
  /home/codespace/projects/client_work/web/frontend
○ @Belise9 → ~/projects/client_work/web/frontend $ 
```



```
● @Belise9 → ~/projects/personal/experiments $ cd ../../shared/templates
● @Belise9 → ~/projects/shared/templates $ pwd
  /home/codespace/projects/shared/templates
○ @Belise9 → ~/projects/shared/templates $ 
```

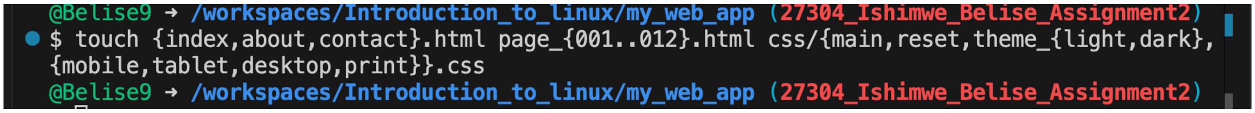
4.

Step1.



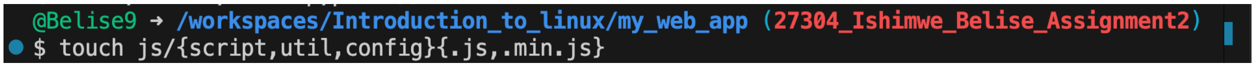
```
● @Belise9 → /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ mkdir -p
  my_web_app/{css,js,backups}
● @Belise9 → /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ cd my_web
  _app
```

Step2.



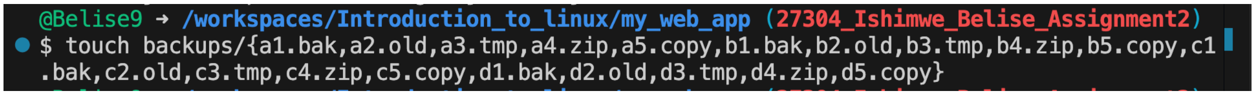
```
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch {index,about,contact}.html page_{001..012}.html css/{main,reset,theme_{light,dark},
  {mobile,tablet,desktop,print}}.css
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step3.



```
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch js/{script,util,config}{.js,.min.js}
```

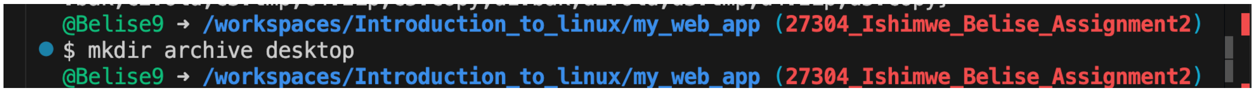
Step4.



```
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch backups/{a1.bak,a2.old,a3.tmp,a4.zip,a5.copy,b1.bak,b2.old,b3.tmp,b4.zip,b5.copy,c1
  .bak,c2.old,c3.tmp,c4.zip,c5.copy,d1.bak,d2.old,d3.tmp,d4.zip,d5.copy}
```

Ans5.

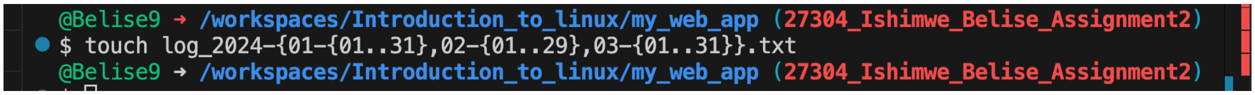
1. step



```
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ mkdir archive desktop
  @Belise9 → /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

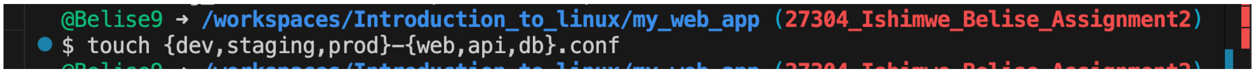
Ans6.

1.step



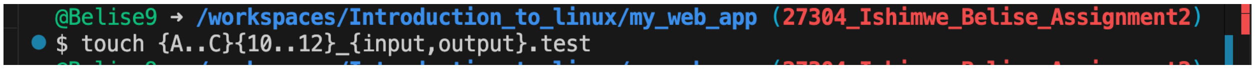
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch log_2024-{01-{01..31},02-{01..29},03-{01..31}}.txt
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step2.



```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch {dev,staging,prod}-{web,api,db}.conf
```

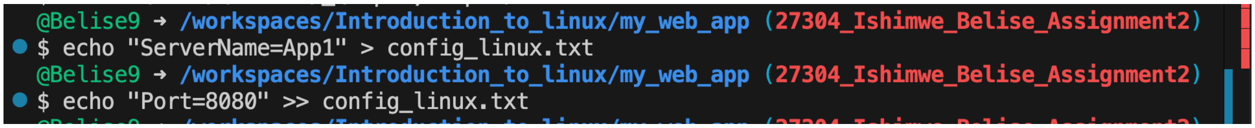
Step3.



```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ touch {A..C}{10..12}_{input,output}.test
```

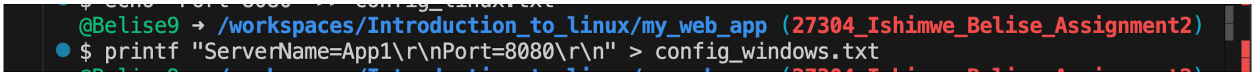
Ans7

Step1.



```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ echo "ServerName=App1" > config_linux.txt
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ echo "Port=8080" >> config_linux.txt
```

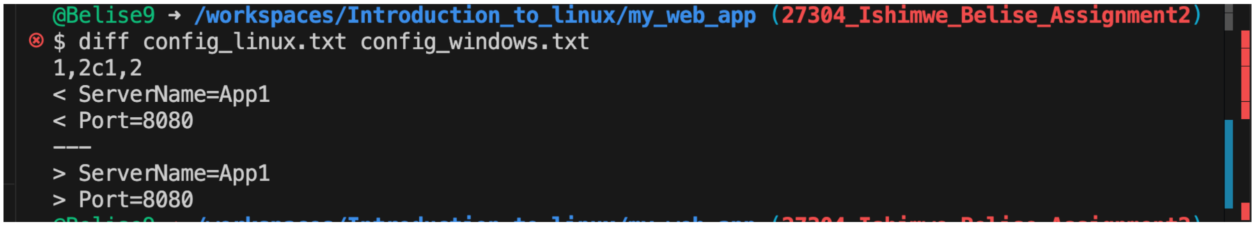
Step2.



```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
● $ printf "ServerName=App1\r\nPort=8080\r\n" > config_windows.txt
```

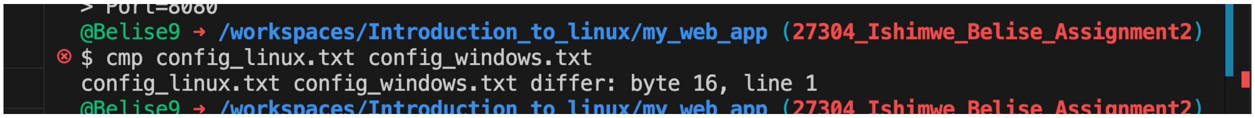
Comparing Files with Different Tools

Step1.



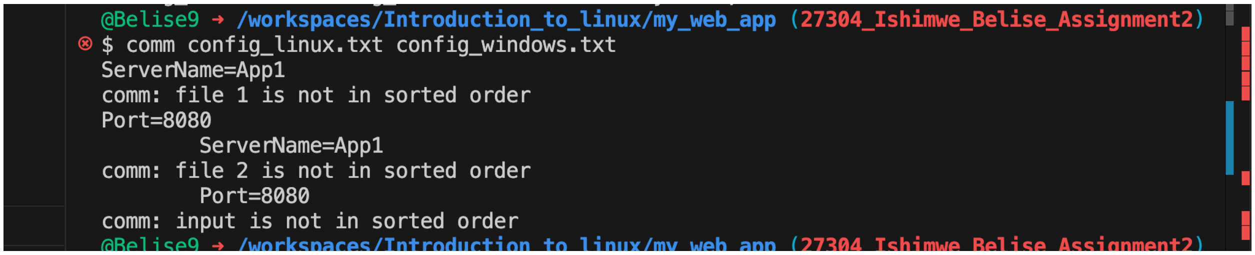
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
⊗ $ diff config_linux.txt config_windows.txt
1,2c1,2
< ServerName=App1
< Port=8080
---
> ServerName=App1
> Port=8080
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step2.



```
> Port=8080
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
⊗ $ cmp config_linux.txt config_windows.txt
config_linux.txt config_windows.txt differ: byte 16, line 1
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step3.



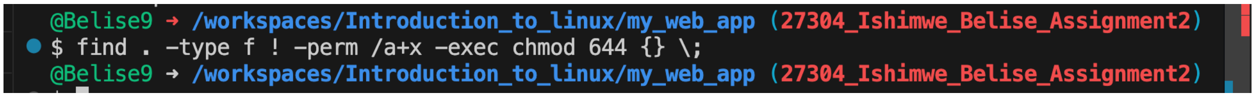
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
⊗ $ comm config_linux.txt config_windows.txt
ServerName=App1
comm: file 1 is not in sorted order
Port=8080
        ServerName=App1
comm: file 2 is not in sorted order
        Port=8080
comm: input is not in sorted order
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Ans8.

Ans9.

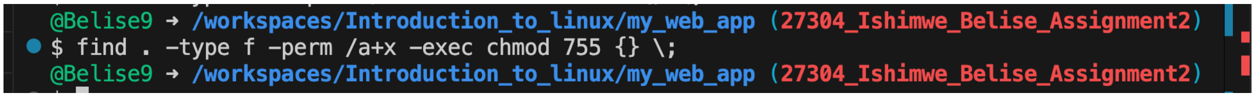
Ans10.

Step1



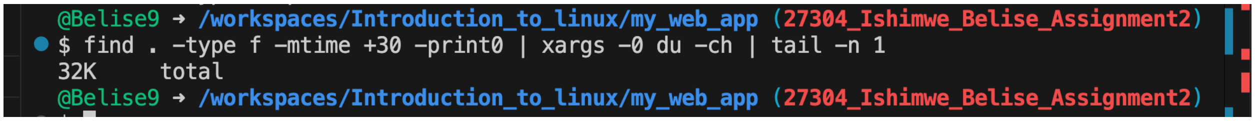
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f ! -perm /a+x -exec chmod 644 {} \;
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step2.



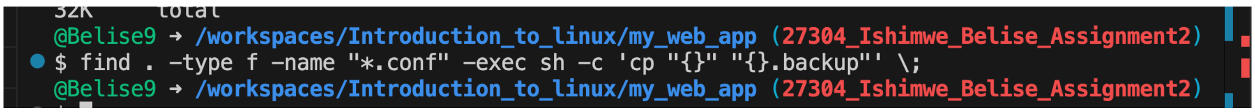
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f -perm /a+x -exec chmod 755 {} \;
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step3.



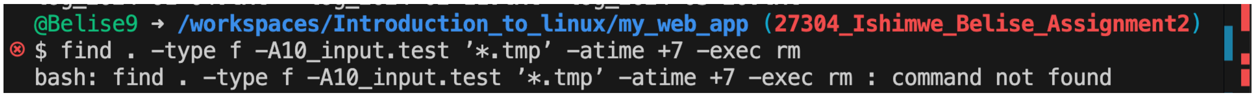
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f -mtime +30 -print0 | xargs -0 du -ch | tail -n 1
32K     total
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step4.



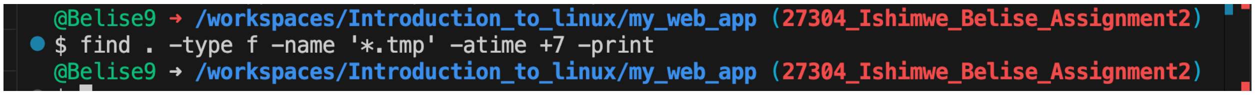
```
32K     total
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f -name "*.conf" -exec sh -c 'cp "{}" "{}.backup"' \;
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

Step5



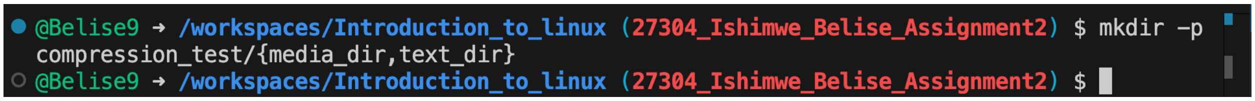
```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f -A10_input.test ’*.tmp’ -atime +7 -exec rm
bash: find . -type f -A10_input.test ’*.tmp’ -atime +7 -exec rm : command not found
```

Step6

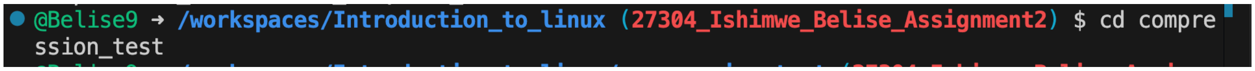


```
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
$ find . -type f -name '*.tmp' -atime +7 -print
@Belise9 ➜ /workspaces/Introduction_to_linux/my_web_app (27304_Ishimwe_Belise_Assignment2)
```

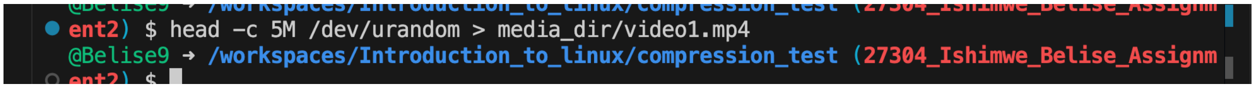
Ans11.



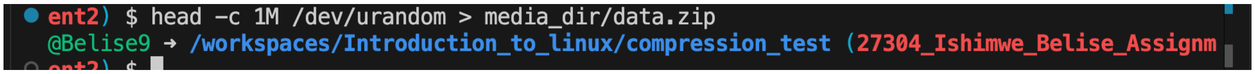
```
@Belise9 ➜ /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ mkdir -p
compression_test/{media_dir,text_dir}
@Belise9 ➜ /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $
```



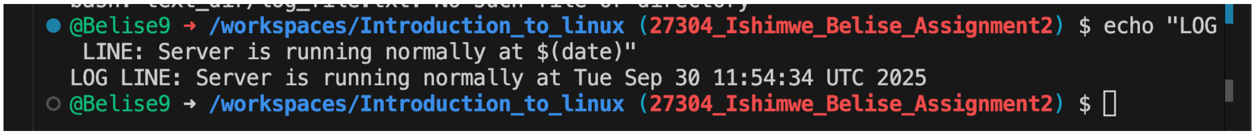
```
● @Belise9 ➜ /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ cd compre
  ssion_test
```



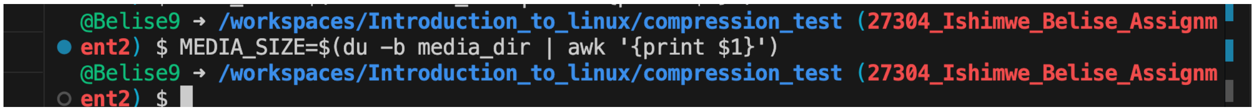
```
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
● ent2) $ head -c 5M /dev/urandom > media_dir/video1.mp4
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
○ ent2) $
```



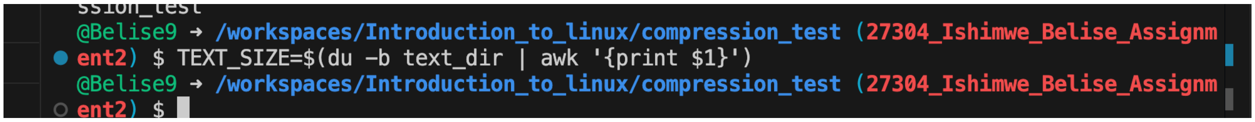
```
● ent2) $ head -c 1M /dev/urandom > media_dir/data.zip
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
○ ent2) $
```



```
  bash: text_dir/log_file.txt: No such file or directory
● @Belise9 ➜ /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $ echo "LOG
   LINE: Server is running normally at $(date)"
  LOG LINE: Server is running normally at Tue Sep 30 11:54:34 UTC 2025
○ @Belise9 ➜ /workspaces/Introduction_to_linux (27304_Ishimwe_Belise_Assignment2) $
```



```
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
● ent2) $ MEDIA_SIZE=$(du -b media_dir | awk '{print $1}')
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
○ ent2) $
```



```
  ssion_test
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
● ent2) $ TEXT_SIZE=$(du -b text_dir | awk '{print $1}')
  @Belise9 ➜ /workspaces/Introduction_to_linux/compression_test (27304_Ishimwe_Belise_Assignm
○ ent2) $
```

Ans12.