

NAME: ISHIMWE Amos

ID: 26247

Assignment 2 – Individual

Course Code: COSC 8312

Adventist University of Central Africa

Answers

Question 1:

Directories investigation:

- /bin → Contains essential binaries (e.g., ls, cp, mv) that attackers could replace with malicious versions.
- /etc → Contains system configuration files (passwd, shadow, hosts). Attackers may modify these to gain persistence.
- /var → Contains logs (/var/log). Evidence of intrusion is likely found here.
- /usr → Contains user applications and libraries. Malicious replacements may occur.
- /tmp → Temporary storage, often abused by attackers for malware scripts.
- /opt → Third-party software; attackers could backdoor applications here.
- /boot → Kernel and bootloader; tampering here allows persistent rootkits.
- /home → User files. Attackers might store tools or exfiltrated data here.

Question 2:

To create the structure with minimal commands:

mkdir -p

projects/{client_work/{web/{frontend,backend,database},mobile/{ios,adroid}},personal/{experiments,archive},shared/{templates,resources}}

```
(amos@kali)~[~/Desktop]
$ cd Introduction_to_linux

(amos@kali)~[~/Desktop/Introduction_to_linux]
$ mkdir -p projects/{client_work/{web/{frontend,backend,database},mobile/{ios,adroid}},personal/{experiments,archive},shared/{templates,resources}}

(amos@kali)~[~/Desktop/Introduction_to_linux]
$
```

Question 3:

Navigate between directories with limited cd:

```
(amos@kali)~[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ cd ../../../../personal/experiments

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/personal/experiments]
$ pwd
/home/amos/Desktop/Introduction_to_linux/projects/personal/experiments

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/personal/experiments]
$ cd ../../shared/templates

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/shared/templates]
$ pwd
/home/amos/Desktop/Introduction_to_linux/projects/shared/templates

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/shared/templates]
$ cd ../../client_work/web/frontend

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ pwd
/home/amos/Desktop/Introduction_to_linux/projects/client_work/web/frontend

(amos@kali)~[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$
```

cd ../../../../personal/experiments

```
cd ../../shared/templates
cd ../../client_work/web/frontend
```

Question 4:

Efficient creation of project structure:

```
(amos@kali) - [~/Desktop/Introduction_to_linux/project
s/client_work/web/frontend]
$ touch {index,about,contact}.html page_{001..012}.html

(amos@kali) - [~/Desktop/Introduction_to_linux/project
s/client_work/web/frontend]
$ ls -l *.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 about.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 contact.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 index.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_001.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_002.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_003.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_004.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_005.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_006.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_007.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_008.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_009.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_010.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_011.html
-rw-rw-r-- 1 amos amos 0 Oct 1 04:19 page_012.html

(amos@kali) - [~/Desktop/Introduction_to_linux/project
s/client_work/web/frontend]
$
```

HTML files

```
touch {index,about,contact}.html page_{001..012}.html
```

CSS files

```
touch {main,reset,theme_light,theme_dark,mobile,tablet,desktop,print}.css
```

```

(amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ touch {main,reset,theme_light,theme_dark,mobile,table,desktop,print}.css

(amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls
about.html      page_003.html  page_011.html
contact.html    page_004.html  page_012.html
desktop.css     page_005.html  print.css
index.html      page_006.html  reset.css
main.css        page_007.html  table.css
mobile.css      page_008.html  theme_dark.css
page_001.html   page_009.html  theme_light.css
page_002.html   page_010.html

(amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$

```

JS files

touch {script1,script2,util1,util2,config1,config2}.js

```

(amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ touch {script1,script2,util1,util2,config1,config2}.js

(amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls -l *.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 config1.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 config2.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 script1.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 script2.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 util1.js
-rw-rw-r-- 1 amos amos 0 Oct  1 05:44 util2.js

```

Backup files (20 total, 5 for each prefix a-d)

touch {a,b,c,d}{1..5}.bak


```
amos@kali: ~/Desktop/Introduction_to_linux/projects/client_work/web/frontend
File Actions Edit View Help
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ touch {a,b,c,d}{1..5}.bak

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls -l *.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 a1.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 a2.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 a3.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 a4.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 a5.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 b1.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 b2.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 b3.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 b4.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 b5.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 c1.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 c2.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 c3.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 c4.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 c5.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 d1.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 d2.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 d3.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 d4.bak
-rw-rw-r-- 1 amos amos 0 Oct 1 05:48 d5.bak
```

Question 5:

Wildcard operations:

```
mv *[0-9].* ../../../../archive/
```

```
amos@kali: ~/Desktop/Introduction_to_linux/projects/client_work/web/frontend
File Actions Edit View Help
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ mv *[0-9].* ../../../../personal/archive

(amos@kali)-[~/Desktop/Introduction to linux/projects/client work/web/fro
```

```
cp !(mobile|tablet)*.css ../../../../../
```

```
File Actions Edit View Help

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ cp !(mobile|tablet)*.css ../../../../../../

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$
```

ls ???.*

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls ???.*
ls: cannot access '???.*': No such file or directory
```

ls [b-df-hj-np-tv-z]*

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls [b-df-hj-np-tv-z]*
contact.html  main.css    print.css   table.css   theme_light.css
desktop.css   mobile.css  reset.css   theme_dark.css

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$
```

ls *.*[??]

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls *.*[??]
ls: cannot access '*.*[??]': No such file or directory

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$
```

Question 6:

Logs for Q1 2024

```

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ touch log-2024-{01..03}-{01..31}.txt

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls -l *.txt
ls: cannot access 'l': No such file or directory
log-2024-01-01.txt  log-2024-02-01.txt  log-2024-03-01.txt
log-2024-01-02.txt  log-2024-02-02.txt  log-2024-03-02.txt
log-2024-01-03.txt  log-2024-02-03.txt  log-2024-03-03.txt
log-2024-01-04.txt  log-2024-02-04.txt  log-2024-03-04.txt
log-2024-01-05.txt  log-2024-02-05.txt  log-2024-03-05.txt
log-2024-01-06.txt  log-2024-02-06.txt  log-2024-03-06.txt
log-2024-01-07.txt  log-2024-02-07.txt  log-2024-03-07.txt
log-2024-01-08.txt  log-2024-02-08.txt  log-2024-03-08.txt
log-2024-01-09.txt  log-2024-02-09.txt  log-2024-03-09.txt
log-2024-01-10.txt  log-2024-02-10.txt  log-2024-03-10.txt
log-2024-01-11.txt  log-2024-02-11.txt  log-2024-03-11.txt
log-2024-01-12.txt  log-2024-02-12.txt  log-2024-03-12.txt
log-2024-01-13.txt  log-2024-02-13.txt  log-2024-03-13.txt
log-2024-01-14.txt  log-2024-02-14.txt  log-2024-03-14.txt
log-2024-01-15.txt  log-2024-02-15.txt  log-2024-03-15.txt

```

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

Config files for environments

```

(amos@kali)-[~]
$ cd Desktop Introduction_to_linux/projects/client_work/web/frontend
bash: cd: too many arguments

(amos@kali)-[~]
$ cd Desktop/Introduction_to_linux/projects/client_work/web/frontend

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ touch {web,api,db}_{dev,staging,prod}.conf

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ ls -l *.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 api_dev.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 api_prod.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 api_staging.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 db_dev.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 db_prod.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 db_staging.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 web_dev.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 web_prod.conf
-rw-rw-r-- 1 amos amos 0 Oct  1 06:36 web_staging.conf

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ █

```

touch {web,api,db}_{dev,staging,prod}.conf

Test files

```

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ touch {A..c}{10..12}_{input,output}.txt
bash: bad substitution: no closing `` in `10_input.txt

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ touch {A..C}{10..12}_{input,output}.txt

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ ls -l *.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A10_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A10_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A11_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A11_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A12_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 A12_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B10_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B10_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B11_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B11_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B12_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 B12_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 C10_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 C10_output.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 C11_input.txt
-rw-rw-r-- 1 amos amos 0 Oct  1 06:42 C11_output.txt

```

touch {A..C}{10..12}_{input,output}.txt

Question 7:

```

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ echo "config test" > linux.txt unix2dos linux.txt windows.txt

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$

```

```

echo "Config test" > linux_file.txt
unix2dos linux_file.txt windows_file.txt
diff linux_file.txt windows_file.txt
cmp linux_file.txt windows_file.txt
comm linux_file.txt windows_file.txt

```

Reason: Windows uses CRLF endings, Linux uses LF. Tools detect differences. Cross-platform compatibility issues arise.

Question 8:

Find usage:

```
(amos@kali)-[~/audit_test]
$ AVG=$(find . -type f -printf "%s\n" | awk '{s+=$1}END{if(NR>0)print s/NR}')
> find . -type f -size +"${AVG}c"
>
```

```
find . -size +$(du -b | awk '{sum+=$1} END {print sum/NR}')c
find . -mtime -3 ! -mtime -1
find . -type d -empty -o -type d -exec sh -c 'ls -A {} | grep -qv "^\.\" \;' -print
find . -perm -o=w
find . ! -user $USER ! -user root
find . -regex '.*(~|.bak|.tmp)$'
```

Question 9:

Create log file

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ seq 1 250 > biglog.txt

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$
```

seq 1 250 > logfile.log

Middle 50 lines

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ sed -n '100,150p' biglog.txt
100
101
102
103
104
105
106
107
108
109
```

sed -n '101,150p' logfile.log

Last occurrence of word

```

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ grep -n '200' biglog.txt | tail -1
200:200
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$

```

grep -n "error" logfile.log | tail -1

With context

```

(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ grep -A5 -B5 '200' biglog.txt | tail -11
195
196
197
198
199
200
201
202
203
204
205
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$

```

grep -n -A5 -B5 "error" logfile.log

Timing different tools

time cat logfile.log

```

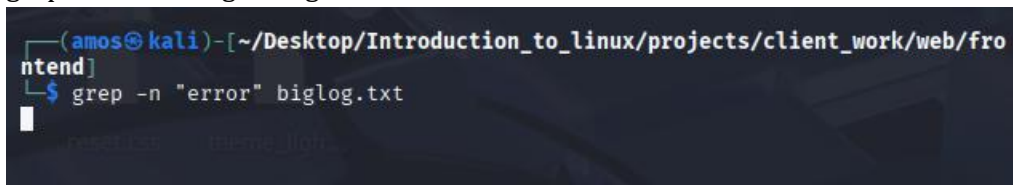
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ time cat biglog.txt
1
2
3
4
5
6
7
8
9
10
11
12
13
14

```

time less logfile.log

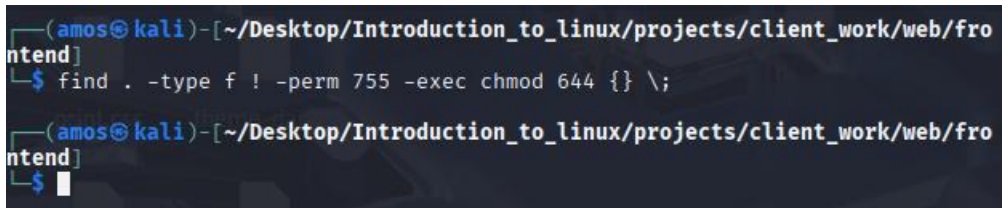


Errors only with line numbers
grep -n "error" logfile.log



Question 10:

`find . -type f ! -perm -111 -exec chmod 644 {} \;`



`find . -type f -perm -111 -exec chmod 755 {} \;`

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ find . -type f -perm -111 -exec chmod 755 {} \;
```

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$
```

find . -name "*.tmp" -atime +7 -print

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ find . -name "*.tmp" -atime +7 -print
```

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$
```

find . -name "*.tmp" -atime +7 -delete

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ find . -name "*.tmp" -atime +7 -delete
find: unknown predicate `-atime +7 -delete'
```

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$
```

Question 11:

tar -czf text.tar.gz textdir/

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ tar -czf text.tar.gz text_dir/
```

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$
```

echo "This is a text file for compression testing" > text_dir/file1.txt

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$ echo "This is a text file for compression testing" > text_dir/file1.txt
```

```
(amos@kali)-[~/Desktop/Introduction_to_linux/projects/client_work/web/fro
ntend]
$
```

tar -cjf text.tar.xz textdir/

zip -r text.zip textdir/

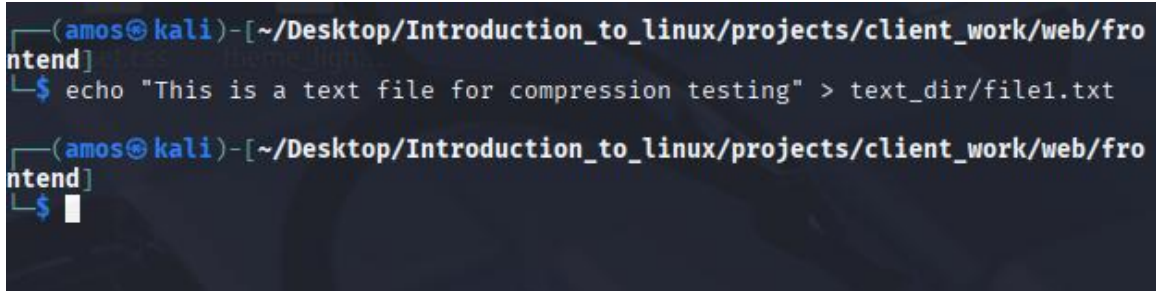
Analysis:

- Already compressed files (.jpg, .mp4, .zip) → little gain with extra compression. Use zip for speed.

- Text files compress best with xz/bzip2.
Recommendation: tar+xz for backups, zip for speed.

Question 12:

tar -tf archive.tar
echo "This is a text file for compression testing" > text_dir/file1.txt

A terminal window screenshot with a dark background. The prompt is (amos@kali) - [~/Desktop/Introduction_to_linux/projects/client_work/web/fro ntend]. The command echo "This is a text file for compression testing" > text_dir/file1.txt has been entered and executed, resulting in a new line prompt \$.

tar -rf archive.tar newfile.txt
zip -FF corrupted.zip --out repaired.zip
tar -cf merged.tar file1.tar.gz file2.zip

Question 13:

Daily incremental → tar --listed-incremental
Weekly full → tar -cf weekly_full.tar /data
Monthly archive → tar -cf monthly.tar /data

Verify integrity → tar -tvf
Naming → backup_YYYYMMDD_type.tar

Question 14:

id user1
id user2
cat /etc/passwd

System users: UID < 1000.
Security risk: regular users in system groups (wheel, adm, sudo).

Question 15:

id -nG
newgrp groupname

Check group access to /var/log, /var/www, /etc/sudoers
Principle of least privilege → assign only required groups.

Question 16:

sudo -i → root login shell

```
(amos@kali)~[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ sudo -i
[sudo] password for amos:
(root@kali)~[~]
#
```

sudo su → switch user via sudo

```
(amos@kali)~[~/Desktop/Introduction_to_linux/projects/client_work/web/frontend]
$ sudo su
(root@kali)~[~/home/.../projects/client_work/web/frontend]
#
```

su - → full login as target user

sudo -u username command → run as another user

Logs: /var/log/auth.log

Risk: NOPASSWD in sudoers → dangerous.

Bonus Question 17:

mkdir forensic/{regular,links,devices,perms,archives}

touch forensic/regular/file.txt

ln forensic/regular/file.txt forensic/links/hardlink

ln -s forensic/regular/file.txt forensic/links/symlink

chmod 1777 forensic/perms/sticky

chmod 4755 forensic/perms/setuid

Analysis: Investigators use ls -l, stat, file, strings, tar, md5sum to identify tampering.
Artifacts like unusual SUID, odd timestamps, unexpected symbolic links indicate compromise.