Names: ISHIMWE Patrick **Date 29th Sept 2025**

ID: 25595

Lecture: KAYITARE Elie

Introduction to Linux Assignment#2.

1. 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.

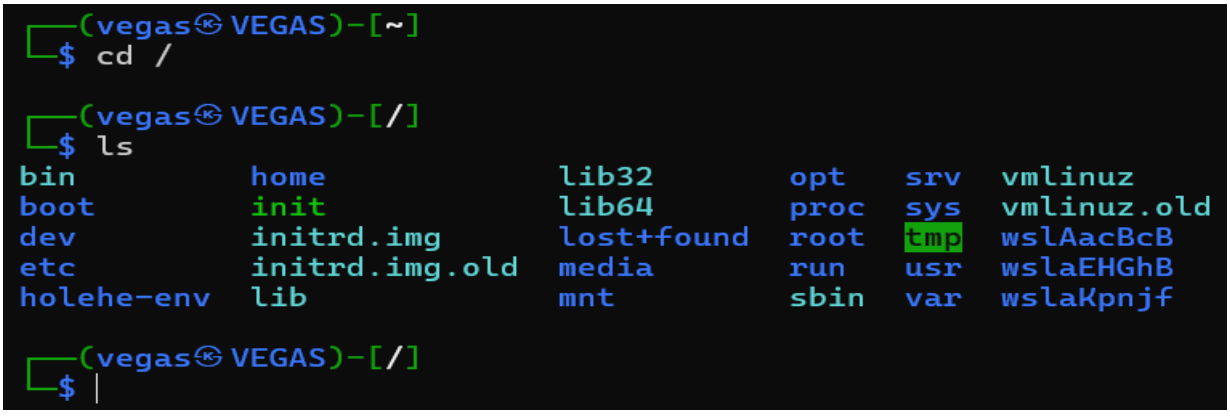
- /usr: Secondary binaries (/usr/bin); similar to /bin, attackers target for non-essential tools.

- /tmp: Temporary files; attackers use for staging malware, as it's writable.

- /opt: Add-on software; attackers hide custom tools here.

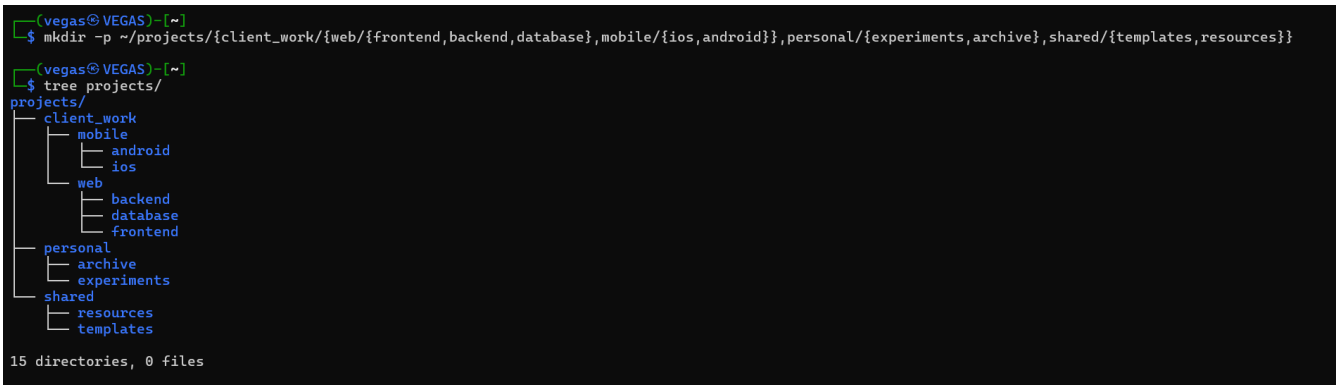
- /boot: Boot files (kernel); attackers modify for rootkits.

- /home: User homes; attackers target for user-level persistence (e.g., .ssh keys).

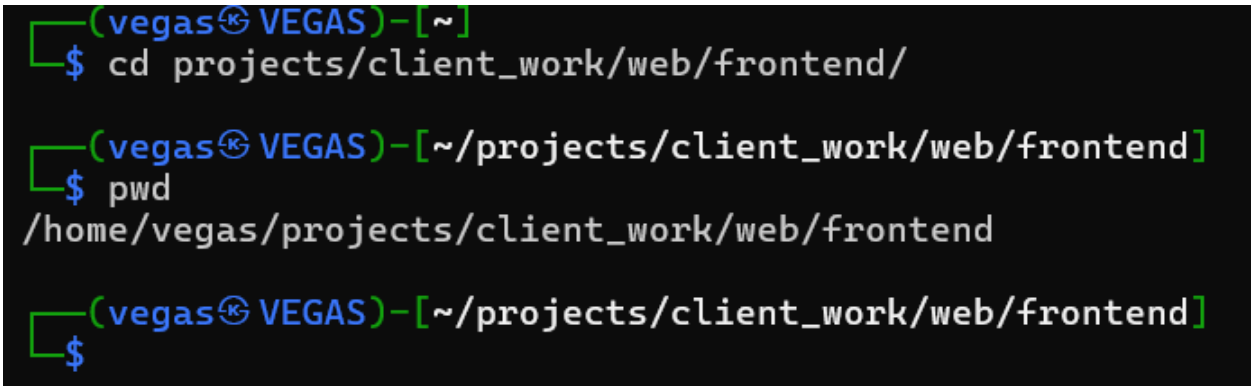


2. Create the Exact Structure

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

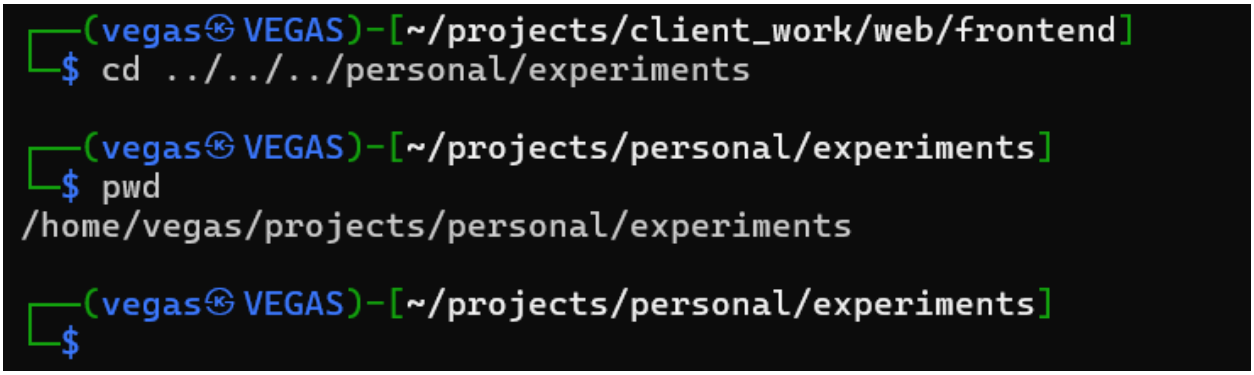


3. Navigate Without Absolute Paths



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

pwd



2. cd ../../shared/templates

pwd

```
┌──(vegas㉿VEGAS)-[~/projects/personal/experiments]
└─$ cd ../../shared/templates

┌──(vegas㉿VEGAS)-[~/projects/shared/templates]
└─$ pwd
/home/vegas/projects/shared/templates

┌──(vegas㉿VEGAS)-[~/projects/shared/templates]
└─$
```

3. cd ../../client_work/web/frontend

pwd

```
┌──(vegas㉿VEGAS)-[~/projects/shared/templates]
└─$ cd ../../client_work/web/frontend

┌──(vegas㉿VEGAS)-[~/projects/client_work/web/frontend]
└─$ pwd
/home/vegas/projects/client_work/web/frontend

┌──(vegas㉿VEGAS)-[~/projects/client_work/web/frontend]
└─$
```

4. Create Realistic Web Project Structure

mkdir web_project

```
┌──(vegas㉿VEGAS)-[~]
└─$ mkdir web_project

┌──(vegas㉿VEGAS)-[~]
```

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

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

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

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

```
┌──(vegas㉿VEGAS)-[~]
└─$ touch web_project/{index,about,contact}.html web_project/page_{001..012}.html

┌──(vegas㉿VEGAS)-[~]
└─$ ls projects/
client_work  personal  shared

┌──(vegas㉿VEGAS)-[~]
└─$ ls web_project/
about.html    index.html     page_002.html  page_004.html  page_006.html  page_008.html  page_010.html  page_012.html
contact.html  page_001.html  page_003.html  page_005.html  page_007.html  page_009.html  page_011.html

┌──(vegas㉿VEGAS)-[~]
└─$ touch web_project/{main,reset,theme_light,theme_dark,mobile,tablet,desktop,print}.css

┌──(vegas㉿VEGAS)-[~]
└─$ touch web_project/{main,util,config,app,helper,setup}_script.js

┌──(vegas㉿VEGAS)-[~]
└─$ touch web_project/{a,b,c,d}{1..5}.{bak,tmp,old,save}

┌──(vegas㉿VEGAS)-[~]
└─$
```

ls web_project/

```
┌──(vegas㉿VEGAS)-[~]
└─$ ls web_project/
a1.bak   a3.save  about.html     b3.bak   b5.save  c3.bak   c5.save          d2.save  d5.bak           page_001.html  page_011.html
a1.old   a3.tmp   app_script.js  b3.old   b5.tmp   c3.old   c5.tmp           d2.tmp   d5.old           page_002.html  page_012.html
a1.save  a4.bak   b1.bak         b3.save  c1.bak   c3.save  config_script.js  d3.bak   d5.save          page_003.html  print.css
a1.tmp   a4.old   b1.old         b3.tmp   c1.old   c3.tmp   contact.html      d3.old   d5.tmp           page_004.html  reset.css
a2.bak   a4.save  b1.save        b4.bak   c1.save  c4.bak   d1.bak           d3.save  desktop.css      page_005.html  setup_script.js
a2.old   a4.tmp   b1.tmp         b4.old   c1.tmp   c4.old   d1.old           d3.tmp   helper_script.js page_006.html  tablet.css
a2.save  a5.bak   b2.bak         b4.save  c2.bak   c4.save  d1.save          d4.bak   index.html       page_007.html  theme_dark.css
a2.tmp   a5.old   b2.old         b4.tmp   c2.old   c4.tmp   d1.tmp           d4.old   main.css         page_008.html  theme_light.css
a3.bak   a5.save  b2.save        b5.bak   c2.save  c5.bak   d2.bak           d4.save  main_script.js   page_009.html  util_script.js
a3.old   a5.tmp   b2.tmp         b5.old   c2.tmp   c5.old   d2.old           d4.tmp   mobile.css       page_010.html

┌──(vegas㉿VEGAS)-[~]
└─$
```

5. Use Wildcards for Cluttered Directory

mv *_[0-9][0-9][0-9].html archive/

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir archive

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mv *_[0-9][0-9][0-9].html archive/
```

cp !(mobile|tablet).css desktop/

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir desktop

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ cp !(mobile|tablet).css desktop/
```

ls ???.*

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ ls ???.*
ls: cannot access '???.*': No such file or directory
```

ls [b-df-hj-np-tv-xzB-DF-HJ-NP-TV-XZ]*.*

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ ls [b-df-hj-np-tv-xzB-DF-HJ-NP-TV-XZ]*.*
b1.bak   b2.save  b4.bak   b5.save  c2.bak   c3.save  c5.bak           d1.bak   d2.save  d4.bak   d5.save          mobile.css      theme_light.css
b1.old   b2.tmp   b4.old   b5.tmp   c2.old   c3.tmp   c5.old           d1.old   d2.tmp   d4.old   d5.tmp           print.css
b1.save  b3.bak   b4.save  c1.bak   c2.save  c4.bak   c5.save          d1.save  d3.bak   d4.save  desktop.css      reset.css
b1.tmp   b3.old   b4.tmp   c1.old   c2.tmp   c4.old   c5.tmp           d1.tmp   d3.old   d4.tmp   helper_script.js  setup_script.js
b2.bak   b3.save  b5.bak   c1.save  c3.bak   c4.save  config_script.js d2.bak   d3.save  d5.bak   main.css         tablet.css
b2.old   b3.tmp   b5.old   c1.tmp   c3.old   c4.tmp   contact.html     d2.old   d3.tmp   d5.old   main_script.js   theme_dark.css
```

ls *.??

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ ls *.??
app_script.js  config_script.js  helper_script.js  main_script.js  setup_script.js  util_script.js
```

6. Brace Expansion for File Naming

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

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

touch {A,B,C}{10,11,12}_{input,output}.txt

ls

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch log_2024-{01..03}-{01..31}.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch {web,api,db}_{dev,stg,prod}.conf

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch {A,B,C}{10,11,12}_{input,output}.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ ls
A10_input.txt   api_prod.conf   b5.save         config_script.js  index.html          log_2024-01-28.txt  log_2024-02-25.txt  log_2024-03-22.txt
A10_output.txt  api_stg.conf    b5.tmp          contact.html      log_2024-01-01.txt  log_2024-01-29.txt  log_2024-02-26.txt  log_2024-03-23.txt
A11_input.txt   app_script.js   C10_input.txt   d1.bak            log_2024-01-02.txt  log_2024-01-30.txt  log_2024-02-27.txt  log_2024-03-24.txt
A11_output.txt  archive         C10_output.txt  d1.old            log_2024-01-03.txt  log_2024-01-31.txt  log_2024-02-28.txt  log_2024-03-25.txt
A12_input.txt   B10_input.txt   C11_input.txt   d1.save           log_2024-01-04.txt  log_2024-02-01.txt  log_2024-02-29.txt  log_2024-03-26.txt
A12_output.txt  B10_output.txt  C11_output.txt  d1.tmp            log_2024-01-05.txt  log_2024-02-02.txt  log_2024-02-30.txt  log_2024-03-27.txt
a1.bak          B11_input.txt   C12_input.txt   d2.bak            log_2024-01-06.txt  log_2024-02-03.txt  log_2024-02-31.txt  log_2024-03-28.txt
a1.old          B11_output.txt  C12_output.txt  d2.old            log_2024-01-07.txt  log_2024-02-04.txt  log_2024-03-01.txt  log_2024-03-29.txt
a1.save         B12_input.txt   c1.bak          d2.save           log_2024-01-08.txt  log_2024-02-05.txt  log_2024-03-02.txt  log_2024-03-30.txt
a1.tmp          B12_output.txt  c1.old          d2.tmp            log_2024-01-09.txt  log_2024-02-06.txt  log_2024-03-03.txt  log_2024-03-31.txt
a2.bak          b1.bak          c1.save         d3.bak            log_2024-01-10.txt  log_2024-02-07.txt  log_2024-03-04.txt  main.css
a2.old          b1.old          c1.tmp          d3.old            log_2024-01-11.txt  log_2024-02-08.txt  log_2024-03-05.txt  main_script.js
a2.save         b1.save         c2.bak          d3.save           log_2024-01-12.txt  log_2024-02-09.txt  log_2024-03-06.txt  mobile.css
a2.tmp          b1.tmp          c2.old          d3.tmp            log_2024-01-13.txt  log_2024-02-10.txt  log_2024-03-07.txt  print.css
a3.bak          b2.bak          c2.save         d4.bak            log_2024-01-14.txt  log_2024-02-11.txt  log_2024-03-08.txt  reset.css
a3.old          b2.old          c2.tmp          d4.old            log_2024-01-15.txt  log_2024-02-12.txt  log_2024-03-09.txt  setup_script.js
a3.save         b2.save         c3.bak          d4.save           log_2024-01-16.txt  log_2024-02-13.txt  log_2024-03-10.txt  tablet.css
a3.tmp          b2.tmp          c3.old          d4.tmp            log_2024-01-17.txt  log_2024-02-14.txt  log_2024-03-11.txt  theme_dark.css
a4.bak          b3.bak          c3.save         d5.bak            log_2024-01-18.txt  log_2024-02-15.txt  log_2024-03-12.txt  theme_light.css
a4.old          b3.old          c3.tmp          d5.old            log_2024-01-19.txt  log_2024-02-16.txt  log_2024-03-13.txt  util_script.js
a4.save         b3.save         c4.bak          d5.save           log_2024-01-20.txt  log_2024-02-17.txt  log_2024-03-14.txt  web_dev.conf
a4.tmp          b3.tmp          c4.old          d5.tmp            log_2024-01-21.txt  log_2024-02-18.txt  log_2024-03-15.txt  web_prod.conf
a5.bak          b4.bak          c4.save         db_dev.conf       log_2024-01-22.txt  log_2024-02-19.txt  log_2024-03-16.txt  web_stg.conf
a5.old          b4.old          c4.tmp          db_prod.conf      log_2024-01-23.txt  log_2024-02-20.txt  log_2024-03-17.txt
a5.save         b4.save         c5.bak          db_stg.conf       log_2024-01-24.txt  log_2024-02-21.txt  log_2024-03-18.txt
a5.tmp          b4.tmp          c5.old          desktop           log_2024-01-25.txt  log_2024-02-22.txt  log_2024-03-19.txt
about.html      b5.bak          c5.save         desktop.css       log_2024-01-26.txt  log_2024-02-23.txt  log_2024-03-20.txt
api_dev.conf    b5.old          c5.tmp          helper_script.js  log_2024-01-27.txt  log_2024-02-24.txt  log_2024-03-21.txt

┌──(vegas㉿VEGAS)-[~/web_project]
```

7. Line Endings Comparison

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

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

diff linux.txt windows.txt

cmp linux.txt windows.txt

comm linux.txt windows.txt

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ printf "This is a test\nLine2\nLine3\n" > linux.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ printf "This is a test\r\nLine2\r\nLine3\r\n" > windows.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ diff linux.txt windows.txt
1,3c1,3
< This is a test
< Line2
< Line3
---
> This is a test
> Line2
> Line3

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ cmp linux.txt windows.txt
linux.txt windows.txt differ: byte 15, line 1

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ comm linux.txt windows.txt
This is a test
comm: file 1 is not in sorted order
Line2
Line3
        This is a test
comm: file 2 is not in sorted order
        Line2
        Line3
comm: input is not in sorted order
```

8. Security Audit with Find

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir -p test_env/{dir1,dir2,dir3,dir4,dir5}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch test_env/dir1/file{1..5}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch -m -d "2 days ago" test_env/dir1/file{1,2}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch -m -d "50 days ago" test_env/dir1/file

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

touch test_env/dir2/largefile

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch test_env/dir2/largefile

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ dd if=/dev/zero of=test_env/dir2/largefile bs=1k count=10
10+0 records in
10+0 records out
10240 bytes (10 kB, 10 KiB) copied, 0.0077372 s, 1.3 MB/s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

touch test_env/dir4/.hidden

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch test_env/dir4/.hidden

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

sudo chown nobody test_env/dir1/file4

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sudo chown nobody test_env/dir1/file4
[sudo] password for vegas:

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

sudo chmod 666 test_env/dir5/worldwritable

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sudo chmod 666 test_env/dir5/worldwritable
chmod: cannot access 'test_env/dir5/worldwritable': No such file or directory

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch test_env/dir5/worldwritable

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sudo chmod 666 test_env/dir5/worldwritable

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -type f -size +$(find test_env -type f -printf "%s\n" | awk '{sum+=$0; n++} END {print int(sum/n)}')c
test_env/dir2/largefile

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

find test_env -mtime -3 -mtime +1

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -mtime -3 -mtime +1
test_env/dir1/file1
test_env/dir1/file2

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -type d -empty -o \( -type d -name ".*" -not -empty \)
test_env/dir3

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

find test_env -perm /o=w

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -perm /o=w
test_env/dir5/worldwritable

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -user ! $(whoami) -a -VEGAS ! root
find: invalid user name or UID argument to -user: ‘!’

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find test_env -name "*~" -o -name "*.bak" -o -name "*.tmp"

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

9. Analyze Large Log

seq 1 300 > large_log.txt

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ seq 1 300 > large_log.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sed -n '126,175p' large_log.txt
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175

┌──(vegas㉿VEGAS)-[~/web_project]
```

grep -n -m1 -B5 "error" large_log.txt | tail -n 6

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ grep -n -m1 -B5 "error" large_log.txt | tail -n 6

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

time cat large_log.txt > /dev/null

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ time cat large_log.txt > /dev/null

real    0m0.039s
user    0m0.008s
sys     0m0.029s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

time less large_log.txt > /dev/null

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ time less large_log.txt > /dev/null

real    0m0.060s
user    0m0.023s
sys     0m0.030s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

time tail large_log.txt > /dev/null

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ time tail large_log.txt > /dev/null

real    0m0.004s
user    0m0.003s
sys     0m0.001s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

grep -n "error" large_log.txt

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ grep -n "error" large_log.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

10. Automate with Find -exec

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sudo find . -type f -not -perm /a=x -exec chmod 644 {} \;

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ sudo find . -type f -perm /a=x -exec chmod 755 {} \;

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

2. Disk space old files:

find . -mtime +30 -exec du -c {} + | tail -1

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find . -mtime +30 -exec du -c {} + | tail -1
0       total

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

3. Backup conf:

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find . -name "*.conf" -exec cp {} {}.backup \;

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

4. Remove temp:

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ find . -name "*tmp" -atime +7 -print 'preview' then -exec rm {} \;
find: paths must precede expression: `preview'

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

time tar czf compressed/text.tar.gz compressed/text

du -h compressed/text.*

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir -p compressed/{text,media}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ seq 1 10000 > compressed/text/big_text.txt

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ dd if=/dev/urandom of=compressed/media/image.jpg bs=1M count=5
5+0 records in
5+0 records out
5242880 bytes (5.2 MB, 5.0 MiB) copied, 0.134246 s, 39.1 MB/s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ time tar czf compressed/text.tar.gz compressed/text

real    0m0.073s
user    0m0.014s
sys     0m0.056s

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ du -h compressed/text.*
24K     compressed/text.tar.gz

┌──(vegas㉿VEGAS)-[~/web_project]
└─$
```

12. Inherited Archives

mkdir -p test_archive && touch test_archive/{file1.txt,file2.conf}

tar -czf archive.tar.gz test_archive/

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir -p test_archive && touch test_archive/{file1.txt,file2.conf}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ tar -czf archive.tar.gz test_archive/
```

zip -r archive.zip . -i test_zip/

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ zip -r archive.zip . -i test_zip/
        zip warning: zip file empty
```

Examine: tar -tf archive.tar.gz

zip -l archive.zip

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

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ mkdir -p test_archive && touch test_archive/{file1.txt,file2.conf}

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ tar -czf archive.tar.gz test_archive/

┌──(vegas㉿VEGAS)-[~/web_project]
└─$ tar -tf archive.tar.gz
test_archive/
test_archive/file2.conf
test_archive/file1.txt
```

Update: tar -uf archive.tar newfile

zip -u archive.zip newfile

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ touch file1.html file2.css
zip -r archive.zip .
```

Corrupted: tar -tf corrupted.tar

tar -xf archive1.tar

unzip archive2.zip

tar -cf new.tar *

```
┌──(vegas㉿VEGAS)-[~/web_project]
└─$ tar -cf new.tar *
tar: new.tar: archive cannot contain itself; not dumped
```

13. Backup Rotation

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

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

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ mkdir -p test_data && touch test_data/file1.txt

┌──(vegas㉿VEGAS)-[~/projects]
└─$ tar -cpf backups/daily/inc_$(date +%Y-%m-%d).tar --listed-incremental=backups/snapshot.file test_data/
```

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

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ tar -cpf backups/weekly/full_$(date +%Y-%W).tar --listed-incremental=snapshot.file data

┌──(vegas㉿VEGAS)-[~/projects]
└─$
```

ls backups

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ ls backups/
daily  monthly  snapshot.file  weekly  weekly_snapshot.file

┌──(vegas㉿VEGAS)-[~/projects]
└─$
```

whoami && id

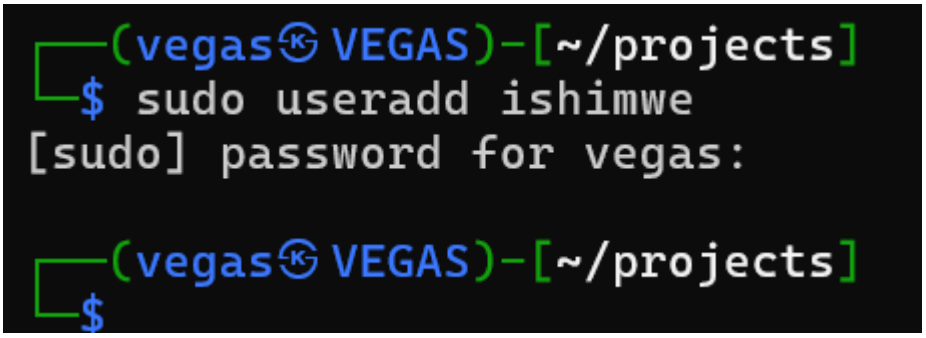
```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ whoami && id
vegas
uid=1000(vegas) gid=1000(vegas) groups=1000(vegas),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(users)
```

cat /etc/passwd

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tcpdump:x:102:103::/nonexistent:/usr/sbin/nologin
sshd:x:103:65534::/run/sshd:/usr/sbin/nologin
vegas:x:1000:1000:,,,:/home/vegas:/bin/bash
_galera:x:104:65534::/nonexistent:/usr/sbin/nologin
mysql:x:105:106:MariaDB Server,,,:/nonexistent:/bin/false
snort:x:106:107:Snort IDS:/var/log/snort:/usr/sbin/nologin
_sentrypeer:x:107:108::/var/lib/sentrypeer:/usr/sbin/nologin
cntlm:x:108:65534::/var/run/cntlm:/bin/sh
stunnel4:x:992:992:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
sslh:x:110:109::/nonexistent:/usr/sbin/nologin
```

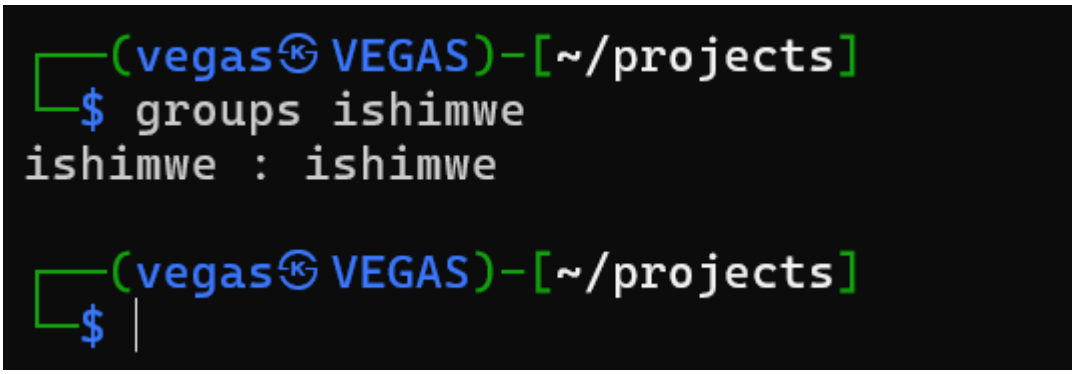
```
_rpc:x:109:65534::/run/rpcbind:/usr/sbin/nologin
sslh:x:110:109::/nonexistent:/usr/sbin/nologin
arpwatch:x:111:112:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
ntpsec:x:112:113::/nonexistent:/usr/sbin/nologin
Debian-exim:x:113:114::/var/spool/exim4:/usr/sbin/nologin
uuidd:x:114:115::/run/uuidd:/usr/sbin/nologin
redsocks:x:115:116::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:116:118::/var/lib/gophish:/usr/sbin/nologin
freerad:x:117:119::/etc/freeradius:/usr/sbin/nologin
iodine:x:118:65534::/run/iodine:/usr/sbin/nologin
gpsd:x:119:20:GPSD system user,,,:/run/gpsd:/bin/false
clamav:x:120:120::/var/lib/clamav:/bin/false
miredo:x:121:65534::/var/run/miredo:/usr/sbin/nologin
Debian-snmp:x:122:121::/var/lib/snmp:/bin/false
statd:x:123:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:124:122::/var/lib/redis:/usr/sbin/nologin
freerad-wpe:x:125:123::/etc/freeradius-wpe:/usr/sbin/nologin
postgres:x:126:124:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mosquitto:x:127:125::/var/lib/mosquitto:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
_gvm:x:128:129::/var/lib/openvas:/usr/sbin/nologin
avahi:x:129:130:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
inetsim:x:130:131::/var/lib/inetsim:/usr/sbin/nologin
usbmux:x:131:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
cups-pk-helper:x:132:132:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
_defectdojo:x:133:133::/var/log/defectdojo:/usr/sbin/nologin
geoclue:x:134:134::/var/lib/geoclue:/usr/sbin/nologin
_dvwa:x:135:135::/var/log/dvwa:/usr/sbin/nologin
dradis:x:136:136::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:137:137::/var/lib/beef-xss:/usr/sbin/nologin
_juice:x:138:138::/var/lib/juice-shop:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
_caldera:x:139:139::/var/lib/caldera:/usr/sbin/nologin
tss:x:140:140:TPM software stack,,,:/var/lib/tpm:/bin/false
rtkit:x:141:141:RealtimeKit,,,:/proc:/usr/sbin/nologin
avahi:x:129:130:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
inetsim:x:130:131::/var/lib/inetsim:/usr/sbin/nologin
usbmux:x:131:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
cups-pk-helper:x:132:132:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
_defectdojo:x:133:133::/var/log/defectdojo:/usr/sbin/nologin
geoclue:x:134:134::/var/lib/geoclue:/usr/sbin/nologin
_dvwa:x:135:135::/var/log/dvwa:/usr/sbin/nologin
dradis:x:136:136::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:137:137::/var/lib/beef-xss:/usr/sbin/nologin
_juice:x:138:138::/var/lib/juice-shop:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
_caldera:x:139:139::/var/lib/caldera:/usr/sbin/nologin
tss:x:140:140:TPM software stack,,,:/var/lib/tpm:/bin/false
rtkit:x:141:141:RealtimeKit,,,:/proc:/usr/sbin/nologin
strongswan:x:142:65534::/var/lib/strongswan:/usr/sbin/nologin
lightdm:x:143:143:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:144:144:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:145:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
saned:x:146:147::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:147:148:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
colord:x:148:149:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openconnect:x:149:151:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
xrdp:x:150:152::/run/xrdp:/usr/sbin/nologin
_bloodhound:x:151:153::/var/lib/bloodhound:/usr/sbin/nologin

┌──(vegas㉿VEGAS)-[~/projects]
└─$
```

sudo useradd ishimwe



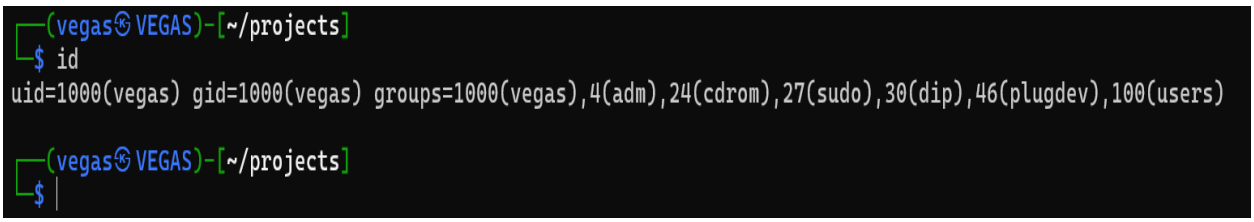
Groups

groups ishimwe



15. Group Membership Issues

id



getent group ishimwe

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ getent group ishimwe
ishimwe:x:1001:
```

usermod -aG ishimwe ishimwe

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ sudo usermod -aG ishimwe ishimwe

┌──(vegas㉿VEGAS)-[~/projects]
└─$
```

sudo -u ishimwe id

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ sudo -u ishimwe id
uid=1001(ishimwe) gid=1001(ishimwe) groups=1001(ishimwe),1000(vegas)
```

su - ishimwe

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ su - ishimwe
Password:
su: warning: cannot change directory to /home/ishimwe: No such file or directory
$
$ ls
backups  client_work  data  personal  shared  snapshot.file  test_data
$
```

Id

```
$ id
uid=1001(ishimwe) gid=1001(ishimwe) groups=1001(ishimwe),1000(vegas)
$
```

16. Sudo Audit

sudo –l

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ sudo -l
[sudo] password for vegas:
Matching Defaults entries for vegas on VEGAS:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User vegas may run the following commands on VEGAS:
    (ALL : ALL) ALL

┌──(vegas㉿VEGAS)-[~/projects]
└─$
```

sudo –i

sudo su –

su – vegas

last

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ sudo -i
┌──(root㉿VEGAS)-[~]
└─# sudo su -
┌──(root㉿VEGAS)-[~]
└─# su - vegas
┌──(vegas㉿VEGAS)-[~]
└─$ last
vegas    pts/3                        Mon Sep 29 22:04 - still logged in
root     pts/3                        Mon Sep 29 22:03 - still logged in
root     pts/1                        Mon Sep 29 22:03 - still logged in
vegas    pts/1                        Mon Sep 29 21:55 - still logged in
ishimwe  pts/1                        Mon Sep 29 21:41 - still logged in
root     pts/2                        Thu Aug 28 19:18 - 08:17 (3+12:59)
root     pts/1                        Sun Aug 17 20:46 - 14:30 (1+17:43)
root     pts/1                        Sun Aug 17 17:49 - 17:51  (00:01)
root     pts/1                        Sun Aug 17 12:57 - 12:58  (00:01)
root     pts/1                        Sun Aug 17 11:37 - 11:39  (00:02)
root     pts/1                        Sun Aug 17 11:21 - 11:30  (00:09)
dradis                                Wed Aug 13 14:20 - 14:20  (00:00)
root     pts/2                        Wed Aug 13 06:10 - 19:52  (13:41)
root     pts/1                        Tue Aug 12 15:30 - 21:58  (06:28)
dradis                                Thu Apr 24 18:25 - 18:25  (00:00)
vegas    :10                          Mon Jan 20 18:48 - 18:52  (00:03)
vegas    :10                          Mon Jan 20 10:32 - 10:32  (00:00)
vegas    :10                          Mon Jan 20 10:32 - 10:32  (00:00)
vegas    :10                          Mon Jan 20 10:29 - 10:31  (00:01)
dradis                                Mon Jan 20 09:30 - 09:30  (00:00)
dradis                                Mon Jan 20 09:30 - 09:30  (00:00)
dradis                                Mon Jan 20 09:30 - 09:30  (00:00)
postgres                              Fri Jan 17 20:36 - 20:36  (00:00)

wtmpdb begins Fri Jan 17 20:36:01 2025

┌──(vegas㉿VEGAS)-[~]
└─$
```

17. Bonus: Forensic Analysis

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

touch forensics/reg/file
ln forensics/reg/file forensics/hard/hardlink
ln -s forensics/reg/file forensics/sym/symlink

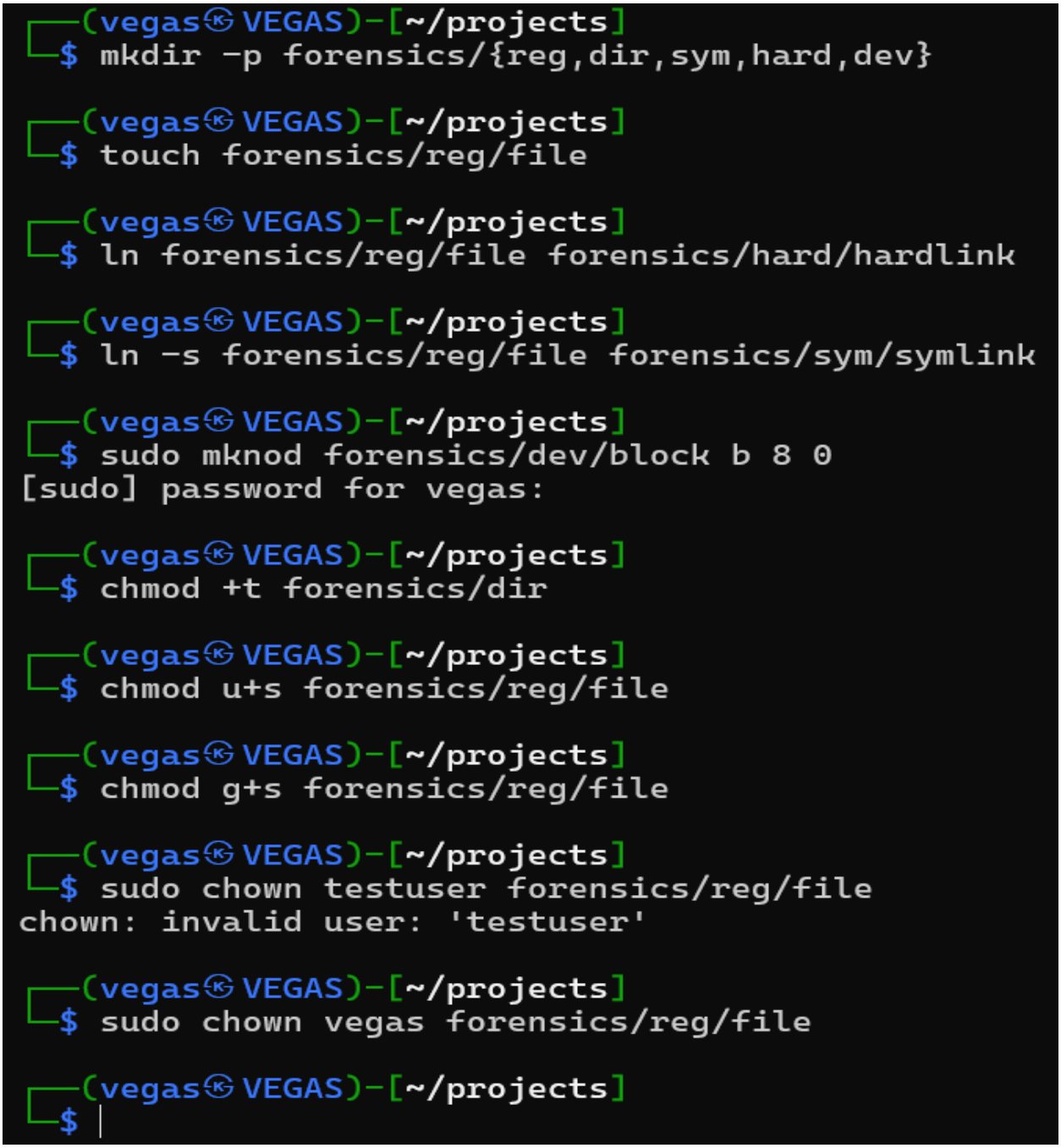
sudo mknod forensics/dev/block b 8 0

chmod +t forensics/dir

chmod u+s forensics/reg/file

chmod g+s forensics/reg/file

sudo chown vegas forensics/reg/file



ls –l forensics

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ ls -l forensics
total 20
drwxrwxr-x 2 vegas vegas 4096 Sep 29 22:16 dev
drwxrwxr-t 2 vegas vegas 4096 Sep 29 22:12 dir
drwxrwxr-x 2 vegas vegas 4096 Sep 29 22:14 hard
drwxrwxr-x 2 vegas vegas 4096 Sep 29 22:13 reg
drwxrwxr-x 2 vegas vegas 4096 Sep 29 22:15 sym
```

stat forensics/reg/file

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ stat forensics/reg/file
  File: forensics/reg/file
  Size: 0               Blocks: 0          IO Block: 4096   regular empty file
Device: 8,32    Inode: 989178      Links: 2
Access: (2664/-rw-rwSr--)  Uid: ( 1000/   vegas)   Gid: ( 1000/   vegas)
Access: 2025-09-29 22:13:59.252936797 +0200
Modify: 2025-09-29 22:13:59.252936797 +0200
Change: 2025-09-29 22:18:19.392847245 +0200
 Birth: 2025-09-29 22:13:59.252936797 +0200
```

getfacl forensics/dir

```
┌──(vegas㉿VEGAS)-[~/projects]
└─$ getfacl forensics/dir
# file: forensics/dir
# owner: vegas
# group: vegas
# flags: --t
user::rwx
group::rwx
other::r-x
```