```
┌──(kali㉿kali)-[~/Desktop/Project/Project_4]
└─$ python3 Project4.py

 [*] Parsing the auth.log file to extract command usage details.

[#] Timestamp: Jun 30 03:35:51, User: root, Command: /usr/bin/mkdir
[#] Timestamp: Jun 30 03:36:26, User: root, Command: /usr/bin/netstat -tapn
[#] Timestamp: Jun 30 03:36:39, User: root, Command: /usr/bin/netstat -tapn
[#] Timestamp: Jun 30 04:29:57, User: root, Command: /bin/bash
[#] Timestamp: Jun 30 04:30:04, User: root, Command: /usr/sbin/tc
[#] Timestamp: Jun 30 04:30:43, User: root, Command: /usr/sbin/adduser rogue_user
[#] Timestamp: Jun 30 04:31:56, User: root, Command: /usr/bin/netstat -tapn
[#] Timestamp: Jun 30 04:33:24, User: root, Command: /bin/bash
[#] Timestamp: Jun 30 04:34:02, User: root, Command: /usr/sbin/userdel -r rogue_user
[#] Timestamp: Jun 30 04:34:34, User: root, Command: /usr/bin/kill -9 102600
[#] Timestamp: Jun 30 04:34:56, User: root, Command: /usr/sbin/userdel -r rogue_user

 [*] List of New Users

[#] New user added:
[#] Timestamp: Jun 30 04:30:43, New User: rogue_user
[#] Details:
  Jun 30 04:30:43 server useradd[102576]: new user: name=rogue_user, UID=1005, GID=1004, home=/home/rogue_user, shell=/
bin/bash, from=/dev/pts/2


 [*] List of Deleted Users

[#] Timestamp: Jun 30 04:34:56, Deleted User: rogue_user
[#] Details:
 Jun 30 04:34:56 server userdel[102783]: delete user 'rogue_user'


 [*] List of Password Changes

[#] Timestamp: Jun 30 04:30:53, Password Changed for User: rogue_user
[#] Details:
 Jun 30 04:30:53 server passwd[102587]: pam_unix(passwd:chauthtok): password changed for rogue_user

[#] Timestamp: Jun 30 04:33:03, Password Changed for User: rogue_user
[#] Details:
 Jun 30 04:33:03 server passwd[102634]: pam_unix(passwd:chauthtok): password changed for rogue_user


 [*] List of Attempted su Usage

[#] Timestamp: Jun 30 04:31:30, User: tc, Command: session opened for user rogue_user(uid=1005) by tc(uid=1000)
[#] Details:
Jun 30 04:31:30 server su: pam_unix(su:session): session opened for user rogue_user(uid=1005) by tc(uid=1000)


[#] Timestamp: Jun 30 04:32:10, User: tc, Command: session opened for user tc(uid=1000) by tc(uid=1005)
[#] Details:
Jun 30 04:32:10 server su: pam_unix(su:session): session opened for user tc(uid=1000) by tc(uid=1005)


[#] Timestamp: Jun 30 04:32:21, User: tc, Command: session opened for user rogue_user(uid=1005) by tc(uid=1000)
[#] Details:
Jun 30 04:32:21 server su: pam_unix(su:session): session opened for user rogue_user(uid=1005) by tc(uid=1000)


[#] Timestamp: Jun 30 04:33:11, User: tc, Command: session opened for user tc(uid=1000) by tc(uid=1005)
[#] Details:
Jun 30 04:33:11 server su: pam_unix(su:session): session opened for user tc(uid=1000) by tc(uid=1005)
```

```
 [*] List of Attempted SUDO Commands

[!] ALERT! Failed sudo attempt:
 Timestamp: Jun 30 03:35:51, User: root, Command: /usr/bin/mkdir
Details:
 Jun 30 03:35:51 server sudo:       tc : 3 incorrect password attempts ; TTY=pts/1 ; PWD=/home/tc ; USER=root ; COMMAND
=/usr/bin/mkdir


[!] ALERT! Failed sudo attempt:
 Timestamp: Jun 30 03:36:26, User: root, Command: /usr/bin/netstat -tapn
Details:
 Jun 30 03:36:26 server sudo:       tc : 3 incorrect password attempts ; TTY=pts/1 ; PWD=/home/tc ; USER=root ; COMMAND
=/usr/bin/netstat -tapn


[#] Timestamp: Jun 30 03:36:39, User: root, Command: /usr/bin/netstat -tapn
Details:
 Jun 30 03:36:39 server sudo:       tc : TTY=pts/1 ; PWD=/home/tc ; USER=root ; COMMAND=/usr/bin/netstat -tapn


[#] Timestamp: Jun 30 04:29:57, User: root, Command: /bin/bash
Details:
 Jun 30 04:29:57 server sudo:       tc : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/bin/bash


[#] Timestamp: Jun 30 04:30:04, User: root, Command: /usr/sbin/tc
Details:
 Jun 30 04:30:04 server sudo:     root : TTY=pts/2 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/tc


[#] Timestamp: Jun 30 04:30:43, User: root, Command: /usr/sbin/adduser rogue_user
Details:
 Jun 30 04:30:43 server sudo:       tc : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/usr/sbin/adduser rogue_user


[#] Timestamp: Jun 30 04:31:56, User: root, Command: /usr/bin/netstat -tapn
Details:
 Jun 30 04:31:56 server sudo: rogue_user : user NOT in sudoers ; TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/usr/bin/n
etstat -tapn


[#] Timestamp: Jun 30 04:33:24, User: root, Command: /bin/bash
Details:
 Jun 30 04:33:24 server sudo:       tc : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/bin/bash


[#] Timestamp: Jun 30 04:34:02, User: root, Command: /usr/sbin/userdel -r rogue_user
Details:
 Jun 30 04:34:02 server sudo:       tc : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/usr/sbin/userdel -r rogue_user


[#] Timestamp: Jun 30 04:34:34, User: root, Command: /usr/bin/kill -9 102600
Details:
 Jun 30 04:34:34 server sudo:       tc : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/usr/bin/kill -9 102600


[#] Timestamp: Jun 30 04:34:56, User: root, Command: /usr/sbin/userdel -r rogue_user
Details:
 Jun 30 04:34:56 server sudo:       tc : TTY=pts/1 ; PWD=/home ; USER=root ; COMMAND=/usr/sbin/userdel -r rogue_user



 ********** END OF SCRIPT **********
```