# HackTheBox Sherlock

## Brutus

By Ernky

### What you’ll learn in this Box:

* Unix auth.log
* Wtmp logs

Downloading the Files

When downloading the files from the website, you’ll get a zip folder containing two files: auth.log and wtmp. There’s a key on the website: hacktheblue, which you’ll need to extract the files into your desktop.

Analyzing the log files.

In the auth.log file, you can track the brute-force attempts from these:

A close up of a newspaper

Description automatically generated

There are a lot of repeated activities which does the same authorization attempt. All of them results in “authentication failure” and “Invalid user admin”. Based on these log activities, we can tell that the attacker was trying to brute force different password combinations for authentication. The IP address the attacker used is 65.2.161.68.

Answer 1: 65.2.161.68

After a while of brute-forcing tho, the attacker eventually got authorized for one of the user accounts.

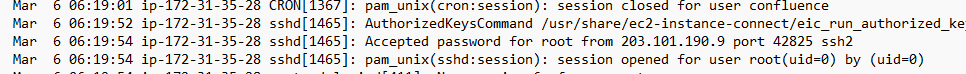
A close up of a computer screen

Description automatically generated

We can tell that it was the attacker who got access by the IP address shown there, which matches the attacker’s IP address. And the account they got access into is the ‘root’ account. You can tell its root from “Accepted password for **root** from 65.2.161.68”

Answer 2: root

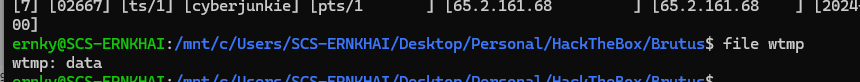
Now don’t get confused with the first accepted password event from the beginning of the log file.



Because this is a legit IP that’s accessing an account.

Ok so now we gotta find the timestamp of the instance where the attacker got authorized. If you look at the auth.log timestamps, you’ll find that its missing the year. And for this Box, the answer wants it in YYYY-MM-DD HH:MM:SS format!!

To find the year, we gotta look at the other file given by the Box, wtmp. This is a data file, probably the metadata of the logs.



And to open this, first you gotta open WSL on the file directory where the files are downloaded in. Then, the command “utmpdump <filename>” basically dumps the raw data out for you to see. Its gonna look like this:

A screenshot of a computer program

Description automatically generated

Now, to find out what time did the attacker log into the server, you need to look at the IP address of the user in each event log. You’ll find that the first activity with the attacker’s IP address is found in 2024-03-06 06:37:45. This means that the attacker has just logged into the server.

And if you compare that time with the auth.log file, you can see that the attacker created a new session of user root during that time. Tho the time is off by 1 second, which is kinda misleading.

A screen shot of a computer code

Description automatically generated

Answer 3: 2024-03-06 06:37:45

Now we gotta find out the session number that was assigned to the attacker’s SSH session. The question said to refer to the session from question 2, which was specifically the session in which the attacker created a new account on. So, this refers to the second SSH session made by the attacker, not the first. The first SSH session was just the brute-forcing attempts, then only after that they created a new account. The SSH session number can be found here:

A screen shot of a computer code

Description automatically generated

As you can see, after opening session 37, the attacker creates a new account for cyberjunkie.

Answer 4: 37

After the attacker got access to the server, they added a new user called ‘cyberjunkie’. The first instance of this is here:

A close-up of a text

Description automatically generated

And the attacker gave this new account higher privileges here:

A screenshot of a computer code

Description automatically generated

By grouping cyberjunkie to sudo, the account will have the same privileges as an admin.

Answer 5: cyberjunkie

What is a MITRE ATT&CK sub-technique? Googling mitre attack will show you the website that lists all the techniques used by attackers and its relevant sub-technique ID. The Box wants us to find the sub-technique ID used for persistence by creating a new account.

A screenshot of a computer

Description automatically generated

So just navigate to Persistence -> Create Account -> Local Account to find the ID.

Answer 6: T1136.001

Now we gotta find out what time did the attacker’s first SSH session end. The phrasing is a bit confusing because you might mistaken the first SSH session as literally the first SSH session to end. But actually, you are supposed to find the SSH session used by cyberjunkie. Which is here:

A screenshot of a computer screen

Description automatically generated

Answer 7: 2024-03-06 06:37:24

We’re reaching the end of the Box now!

Lastly, they want us to find the command used by the attacker to download a script. By looking at auth.log, scroll to the bottom and you’ll find an activity which has a command that sources from github. This already looks a lot like downloading something from the internet.

A screenshot of a computer

Description automatically generated

This is the line where the attacker runs the script using sudo function.