Writeup for Liikt#1337

Author: Faith Tiong

Heyya, this is Faith, still a n00b on CTF and this is my first time participating a CTF competition and I am grateful for the opportunity to do a writeup for Liikt#1337, thanks to everyone for the support as well <3

First of all, yes, this one is a really hard one for a newbie like me. And Liikt#1337 is under the Misc category of Intigriti’s first-ever 1337UP LIVE CTF 2022. Let’s dig into it, shall we?

We’ll first download Liikt.7z from the challenge site of Intigriti and extract all the files and find out that it’s a kali linux virtual machine. I go ahead and attempt to get the root access for the machine at first. The way of doing this is when then Kali machine is booting up, I press “e” on my keyboard and changed the ro to rw, and add on init=/bin/bash and deleted the “quiet splash” behind it too, and then it will prompt me to a CLI interface, I attempted to reset the root password by using the command “passwd root” there and restarted the whole machine.

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

After that, I attempted to login into the kali machine as root with the new password I reset earlier above. Then, I got into a nice GUI of Kali:

A picture containing text, monitor, electronics, display

Description automatically generated

And I fired up the kali terminal. Then type in “cat /etc/passwd”, then I got the first half part of the flag:

Text

Description automatically generated

This is amazing but we still have the 2nd half of the flag to find and the 2nd part is often more trickier. There’s also a user named liikt as shown in the picture above. I decided to browse around with the files and folders and found out the directory “/home/liikt”, and then found another interesting file “pwned.txt”.

Text

Description automatically generated

I go on and read the pwned.txt file and it did give out some interesting facts. I go onto the browser and typed in “blacknote.ctf.intigriti.io” and unfortunately it can’t be accessed on browser (see below):

Graphical user interface, text

Description automatically generated

It doesn’t seem to load, so we’ll try another method. I think that there may be some DBs laying around so I decided to check mysql status by “mysqladmin -u root -p status” and enter the password of the machine and it’s indeed running:

Text

Description automatically generated

Then, I go on and type in “mysql” in the terminal and luckily it didn’t asked me for any credentials so I proceed on to using some mysql commands like:

Text

Description automatically generated

1. show databases;

Here we got some interesting and sweet databases like “yeeter\_dump” as mentioned on “pwned.txt” before. Then I use the command: “use yeeter\_dump;” , “show tables;”, and then “SELECT \* from creds;”:

Graphical user interface, text

Description automatically generated

Here we found something for” liikt”:

A picture containing text

Description automatically generated

We got the “password” for user “liikt”, which is “best\_h3ckerman!69-“, now let’s see how can we use it. After a moment, I’ve thought of an idea of ssh. I quickly open another terminal window and type in “ssh [liikt@blacknote.ctf.intigriti.io](mailto:liikt@blacknote.ctf.intigriti.io)”, and use the password above and TA-DA, I successfully ssh-ed into it and found the 2nd half of the flag:

Text

Description automatically generated

So you’ll get 1337UP{5530491e6c0b5159ff82f00c4e57d0bb} as a complete flag if you combine them together!!

In conclusion, Liikt#1337 is very challenging and it took me around 3 hours or so to figure everything out, and for you, the one who’s reading this right now, always remember that you’re amazing, just the way you’re and you’ll definitely achive what you want in life, never give up on anything you like, Thanks!!