**TryHackMe: 0x41haz Room Write-Up [No Answer]**

A picture containing indoor, cup, white, close

Description automatically generated

0x41haz Room Image/Logo

**Room Description:** *“Simple Reversing Challenge”*

**Task 1: Find the password!**

*“In this challenge, you are asked to solve a simple reversing solution. Download and analyze the binary to discover the password.”*

*“There may be anti-reversing measures in place!”*

So to get started with 0x41haz we need to Download the Task Files. And we can do that by simply pressing on the Blue button on the right of Task 1.

Graphical user interface, text, application, chat or text message

Description automatically generated

0x41haz Download Task Files

So after downloading the Task File I decided to run a simple file command on the Task File. The ‘***file***’ command allows me to get more information about what type of file ‘***.0x41haz***’ is.

A screenshot of a computer

Description automatically generated with medium confidence

file 0x41haz.0x41haz

After running the file command it is clear that we are dealing with an ELF 64bit executable file type. Though there is a slight problem with the file “***MSB \*unknown arch 0x3e00\* (SYSV)***”. So, I decided to Google the problem. And on GitHub I was able to find a hint. “To bypass this, you need to patch the sixth byte (0x02) to 0x01.” Next thing to do will be to find a Hex Editor and patch the sixth byte from a 0x02 to a 0x01. For this I have decided to use a browser based Hex Editor instead of the one available in Kali Linux.

Graphical user interface

Description automatically generated with medium confidence

0x41haz on hexed.it

I decided to use [hexed.it](https://hexed.it/) for this part of the task.

A screenshot of a computer

Description automatically generated with medium confidence

0x41haz on hexed.it with the sixth byte changed from a 02 to a 01

After changing the sixth byte from a 02 to a 01 we get the following output as shown in the figure below when running the file command

A screenshot of a computer

Description automatically generated

file 0x41haz.0x41haz after the sixth byte change

For the next part I will be using **Radare2** or simply **r2** to inspect the file more. Below is a screenshot of how to get started with r2 on this file (r2 should be pre-installed on Kali Linux).

A screenshot of a computer

Description automatically generated with medium confidence

**r2** 0x41haz.0x41haz

After that I will type ‘**aaa**’ to analyze all referenced code.

Text

Description automatically generated

**aaa** on 0x41haz.0x41haz

Ok, once that is done we can do ‘**s main**’ to initialise a seek on the main. Once that is done we can try to open the file in pdf just to see what we get. Below it shows what we are able to see.

Text

Description automatically generated

pdf file view on 0x41haz.0x41haz

And with that he have our answer. Now we can test it by running 0x41haz.

Text

Description automatically generated

0x41haz.0x41haz Answer Verification

And to get the correct answer for TryHackMe, simply add THM{**answer**}. And you would complete this room.

Graphical user interface, text, application

Description automatically generated

0x41haz Room Completed

Thank you for reading my 0x41haz Room Write-Up and if you want to try the room yourself the link is below. I took a lot longer then expected to complete this room as it was more complicated then I expected it to be. I have also attached my LinkTree if you want to get in contact with me.

0x41haz Room Link: [https://tryhackme.com/room/](https://tryhackme.com/room/0x41haz)0x41haz

My LinkTree — <https://linktr.ee/StefanPBargan>