How To Pwn TryHackMe Hacking Streak System

Hello This is ***Edd13Mora*** and today I will show you how I was able to Pwn The Hacking streak system from ***TryhackMe***

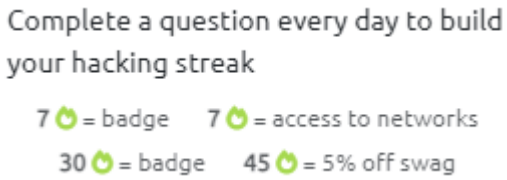
For people who have no idea about what is TryHackme :

It's a platform where you can Learn cyber security. Earn points by answering questions, and maintaining your hacking streak through short lessons.

It's one of the best places where beginners can start.

Explanation

So The Hacking Streak System is a system implemented in TryHackMe where players need to answer every day at least one question correctly and earn 1 point, players who will answer 7 points for 7 days straight will earn special badges and sometimes special gifts.



The Main Idea of this system, is to motivate players to visit the platform and play every day, but sometimes it's really hard to keep the motivation to solve something every 24h without forgetting 1 day.

Many people will like to achieve 200 days of solving or even 300 or more but this needs a lot of discipline which basically I don't have =)

Time To Bypass The Discipline

As you can see here, I have 0 points, which mean I still didn’t solved any challenge for today!

I will not sumbit the answer of the first day directly because I will try to do a trick the Get the points of everyday without answiring and without touching my machine =)

Bug

TryHackMe also allow us as members to create our Hacking CTF Boxes and share them with the community, You need to know somthing importand :

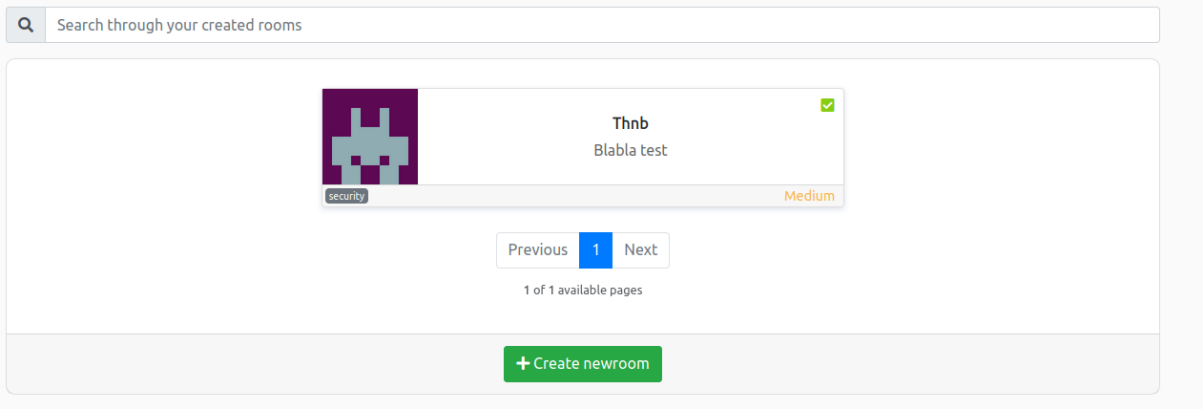
To make your room public for everyone, it needs to be evaluatrd by the THM Team in order to make sure it diserve to be published, But in the other hand you can create your box in private mode and share the link with your friends .

So the question that comes to my mind is, does the answers of private rooms get accounted when we solve them 😈 ?

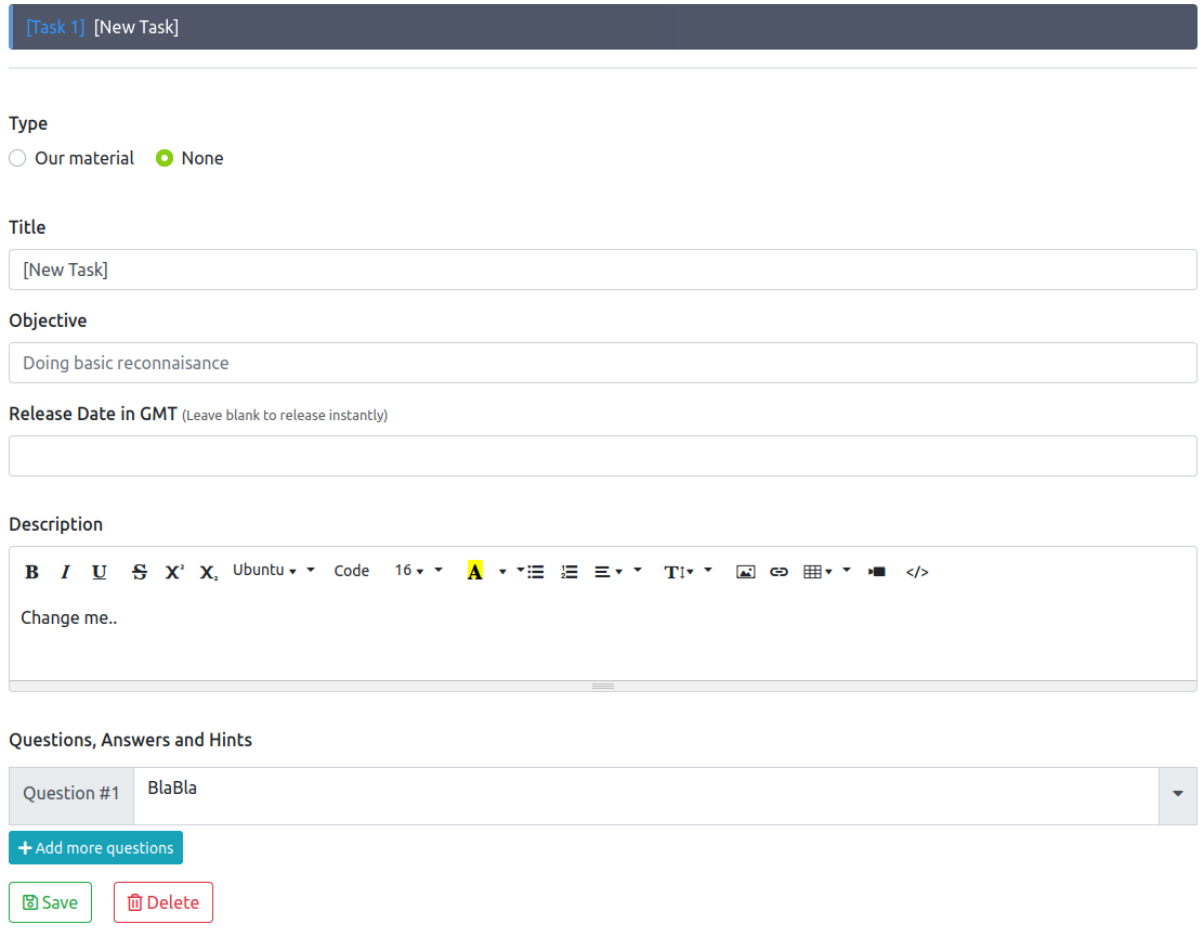
Well the answer is YES and this is the bug we gonna exploit to have our daily points

Exploitation

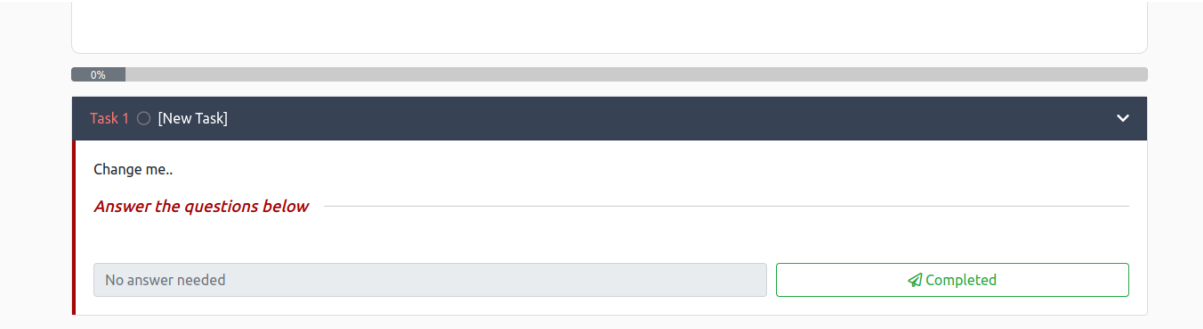
The Idea is to create a private room ‘**Blabla test**’ and everyday add a random question ‘**BlaBla**’ with a random answer ‘**Blabla**’ so you earn your point easly !



Question



And this is how the room looks like!



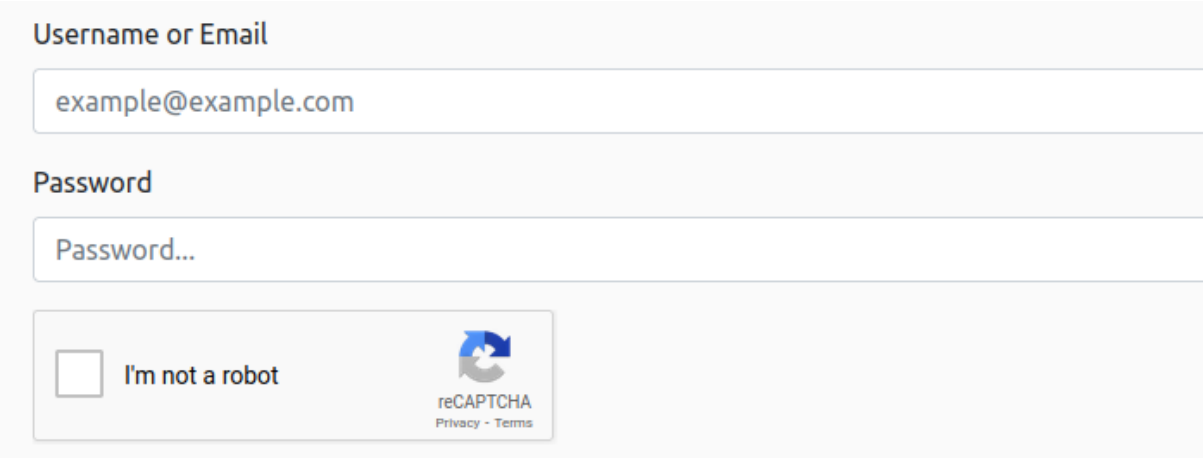
This will do the job for lazzy people but not me, since I will not be available everyday to create questions and answer them …

So whats the solution ? well Automation oufcourse 😎

Automation

Plan : So I needed to code a script that acces my private room, create a question answer it and then delete it, and this script will need to run every 24h to be able the earn the points.

Problemes : The mean probleme we will face during the developement of this script, is the login function, Its easy to developed automated authentification but not when whe have Google Captcha



So I spent 3 days searching about how Captchas works and how to bypass them!

Well I learned alot and I uderstood that thers multiple types of captcha, theres the normal ones with multiple valid bypasses, but the one we have in our case is a Google V2 Captcha and unfortunatly theres no way to bypasse it automatically!

It may sems the end of the road, but nah! as Hacker we always believe that nothing is impossible and theres always a way 🤠

So I asked some frinds for help to find the right was for this bypass, and then we found an article in meduim talking about captchas —> ***The Article***

After reading it I understood that the bypass is possible by ussing the API from ***2captcha*** website

We will need to integret the API in our script and then keep going in our exploit.

The sad thing is that the captcha will be solved by some people who works with 2captcha service, and they arent payed well 😟, Imagine solving 1000 captchas with all the complexity for 2$

Well thanks to thouse people who made none automated tasks automated 😀

So after another 3 days with lot of problem fixing and help from some friends I achived my Goal and Ive done the final script!

Check this 😎

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/7c4cbbbd-796d-4aee-9dbf-888b16ac9877/thm.mp4

As you can see the script is working fine and everythig is automated

So now we will need to make this script run one time every 24h, basicaly we can't make it in our main machine cause it can't be alive everyday so we can run in on a VPS.

But we have a problem, if we wanna use Linux VPS withou a browser interface the script won't work!

But from the beggining I had the solution for this issue and this is why I used Puppeter the code the script, since it support headles browsers 😀

So we can run it without interactive browser but only a terminal

Check this 😎

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/2d66e4f0-998c-4222-9fa6-8e0f134a04a0/headless.mp4

Voilla! and now we can put it in our VPS and set up a cron for it

This is the end of our adveture and finaly we tryed to hack TryHackMe 😇

Special thanks to [4K4A,Ilyase Dh, The Injector].

C***heck my other findings*** ***Github Medium Youtube Facebook***