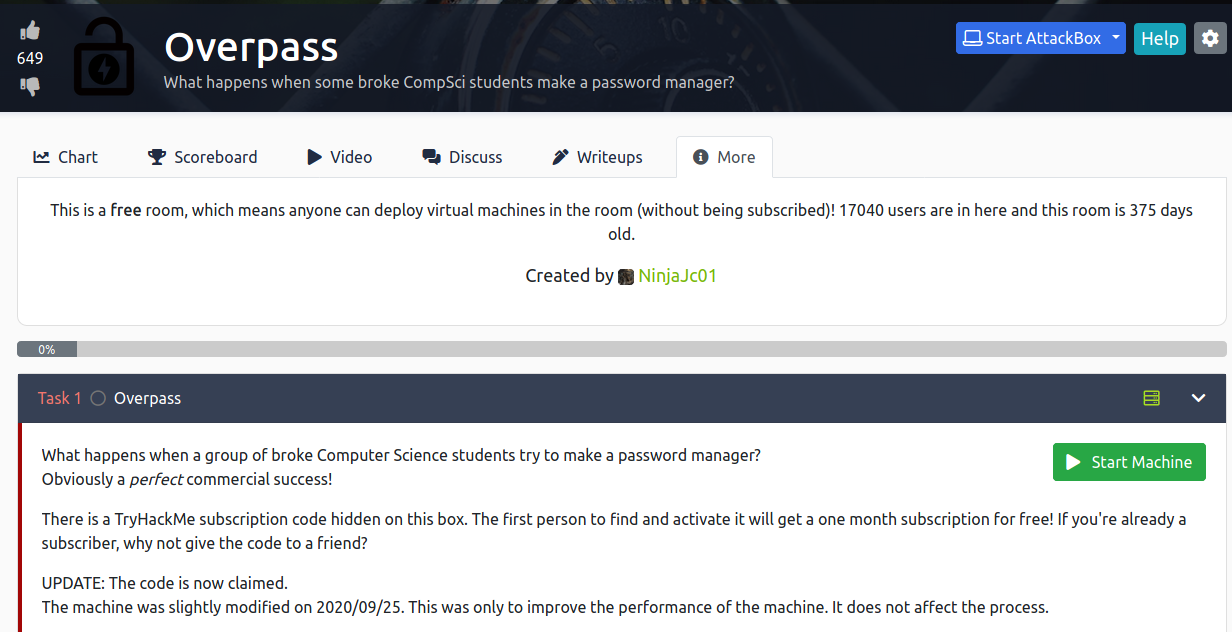
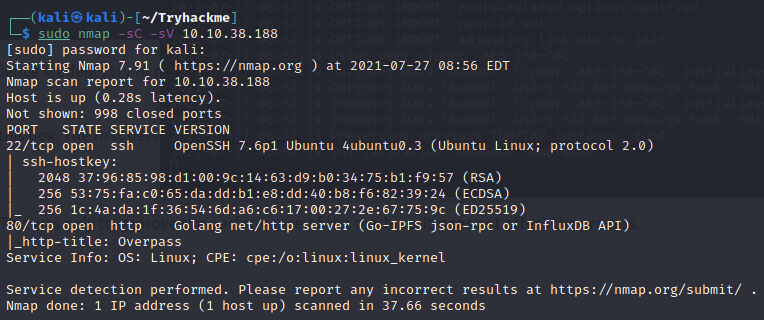
**Overpass write-up**

This is write-up for Overpass in TryHackMe which is a first CTF of this series which we have to break in the webserver, gain access to target machine, privilege escalation and rock this box

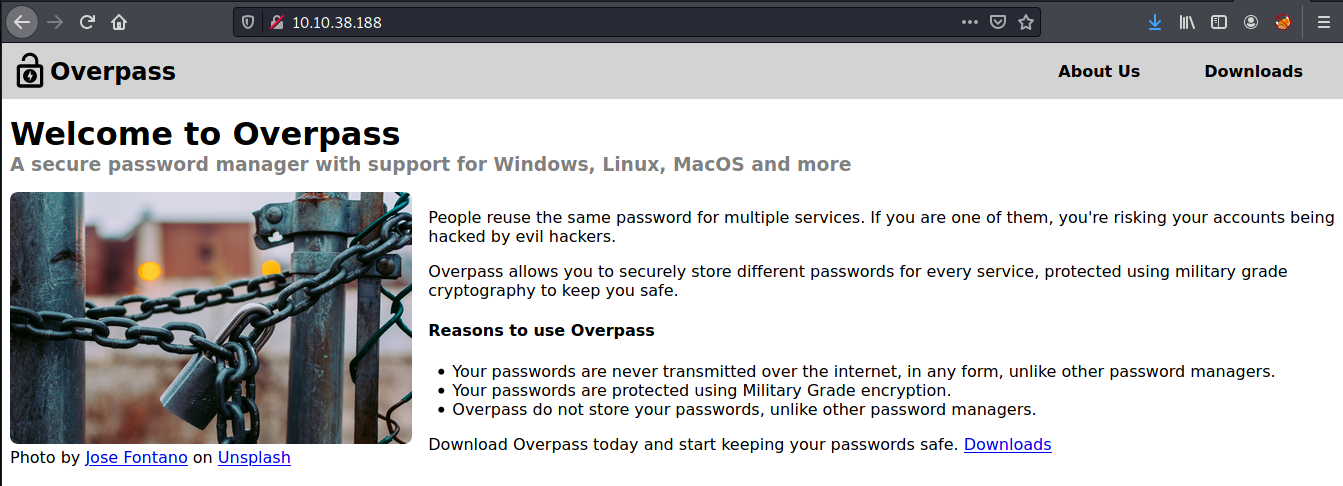
Site: <https://tryhackme.com/room/overpass>



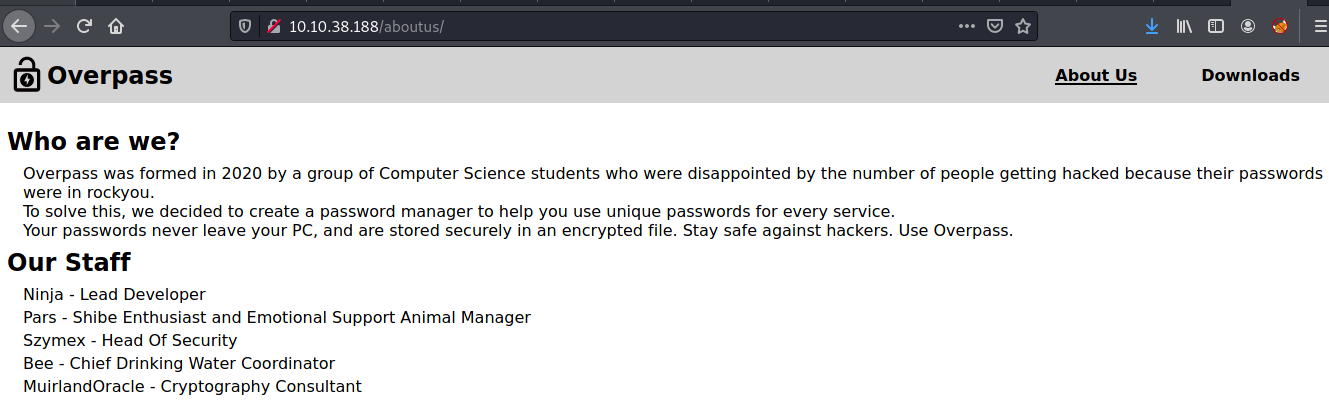
Starting with nmap and we see that ssh and webserver are running



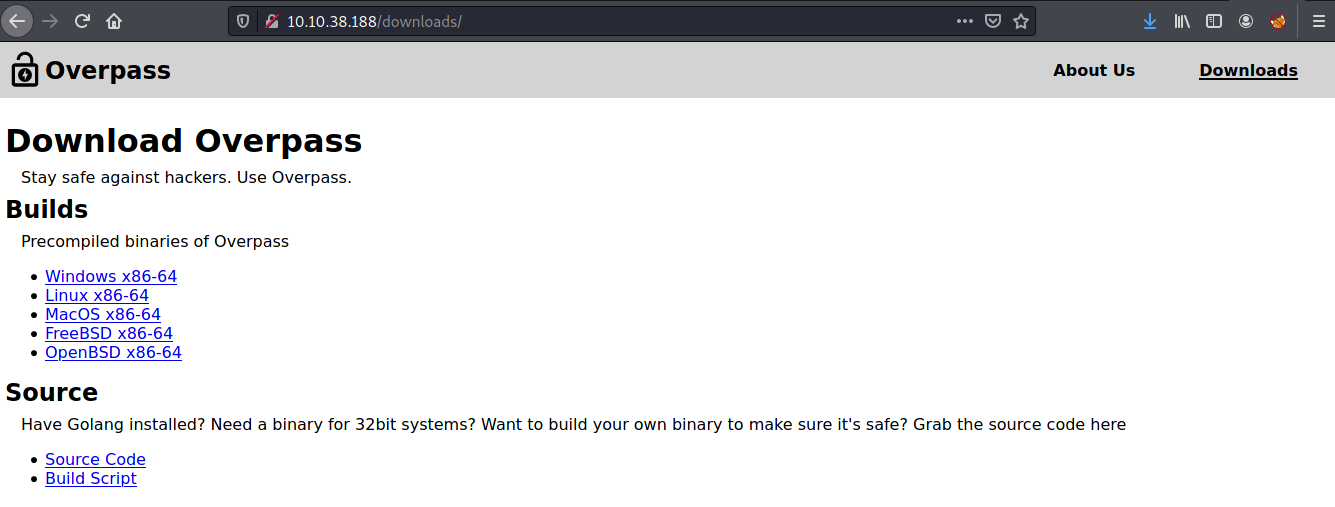
Access the website, we will see what they are doing, and do more recons



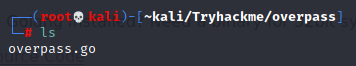
In About Us these all could be potentially username



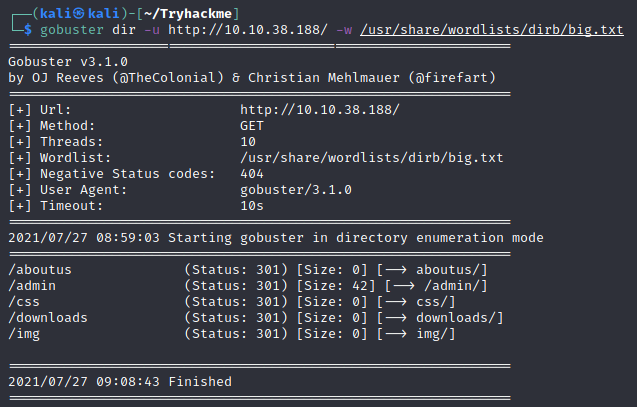
At Downloads page we can see that they are giving their clients their source code



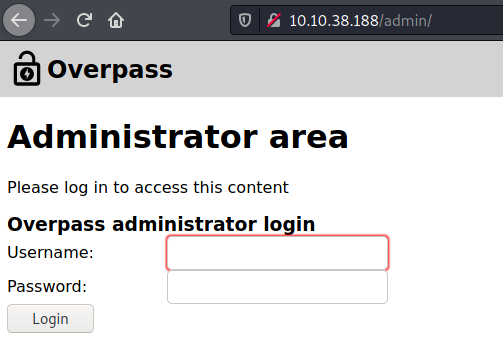
Download source code to understand what their application works



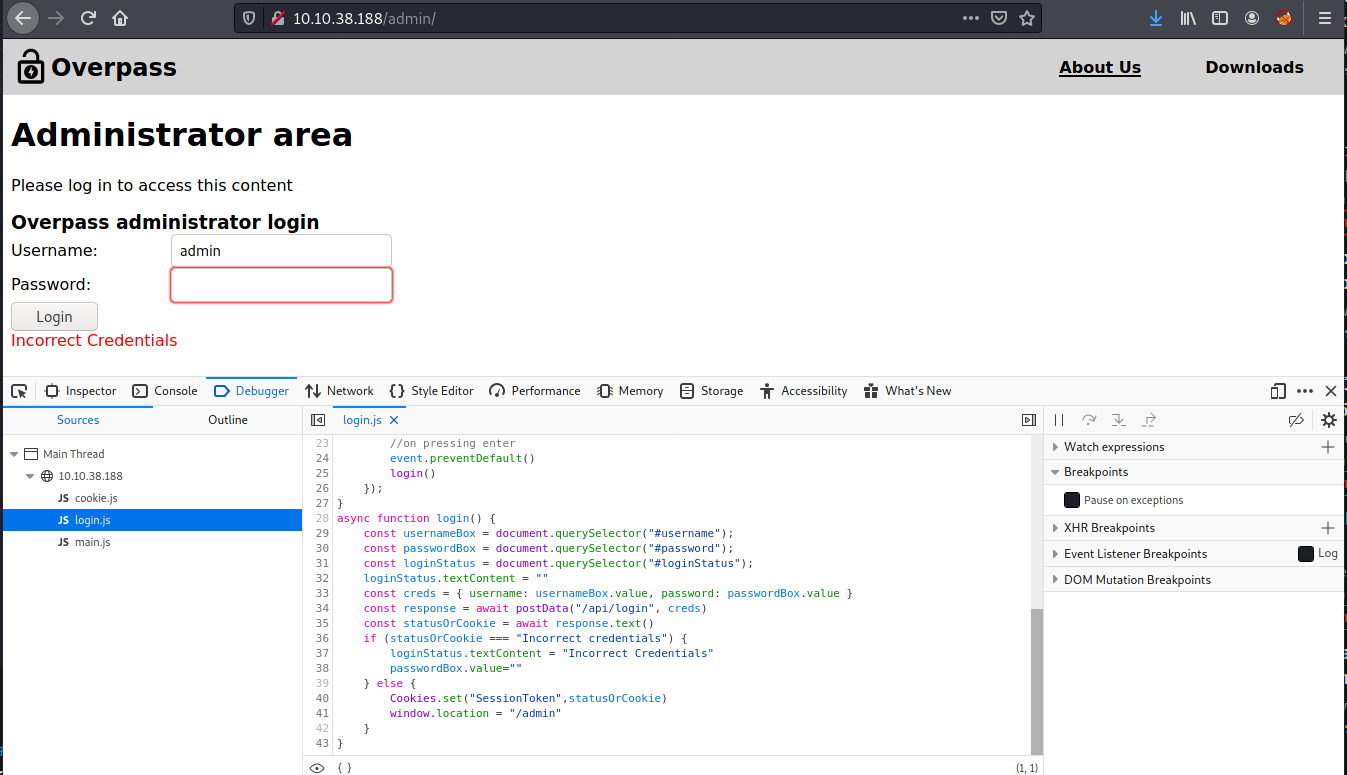
Now it’s time for gobuster to shine and we can see that /admin is very stand out



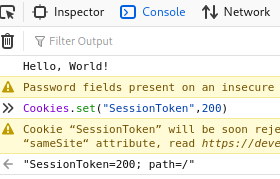
And it’s admin login page



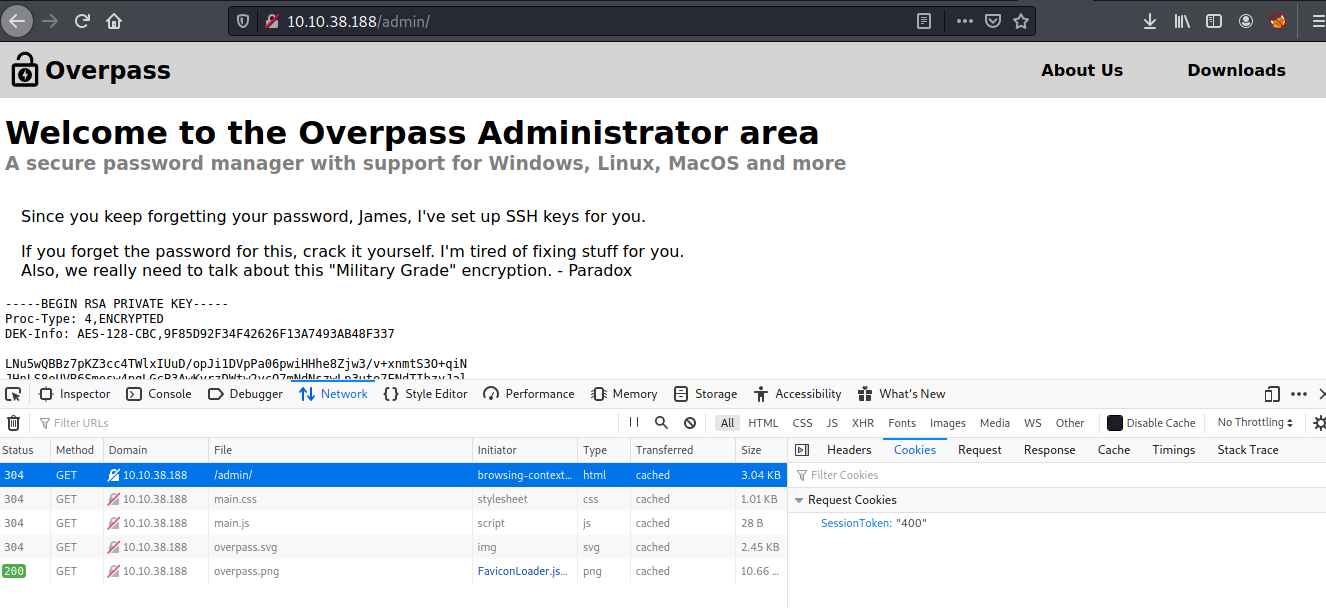
Using Dev tools to see what inside and we can see login.js which when login is success, user set session will be set and it could be lead to Broken authentication vulnerability



Set cookie to anything and after refresh this page, we should be able to bypass this authentication

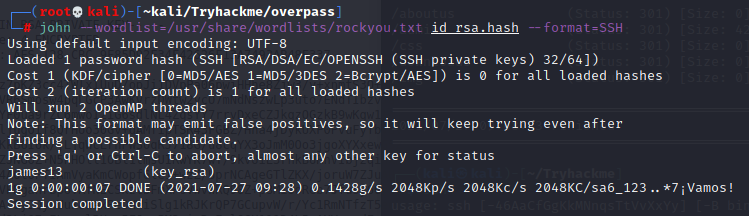


And we really made it here, we will get RSA private key of user james

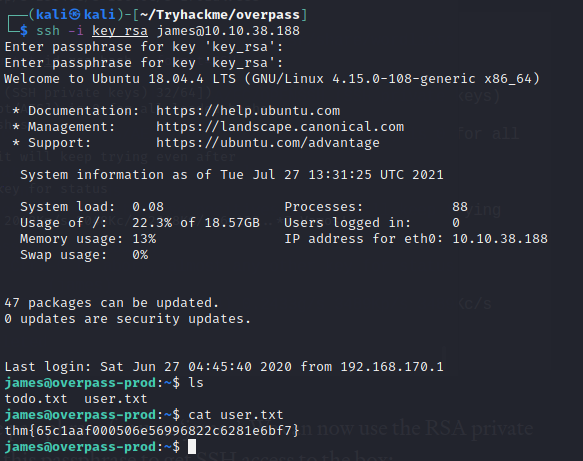


Crack password from this RSA key with ssh2john





After we got James’s SSH password

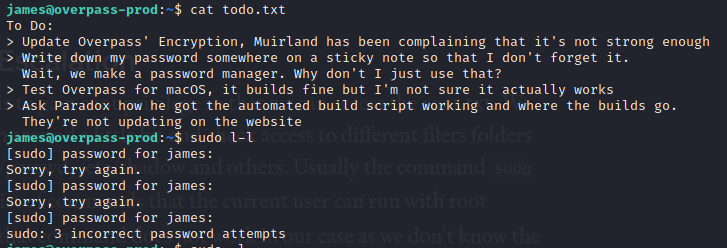


**Hack the machine and get the flag in user.txt**

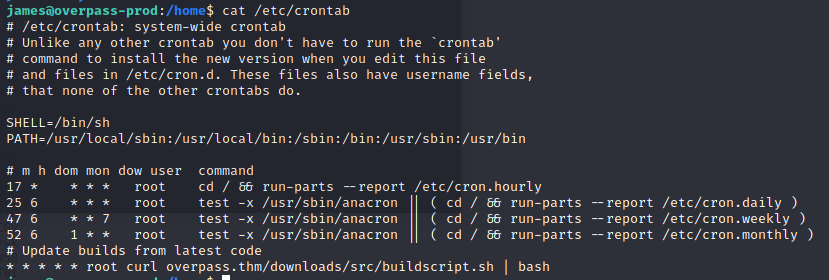


**Escalate your privileges and get the flag in root.txt**

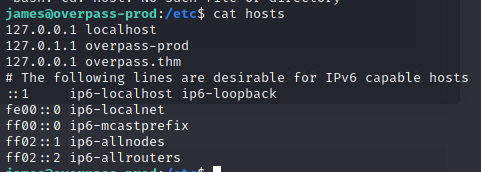
We can’t use sudo cause we don’t have James’s actual password but we got a hint that there is an automated script is running



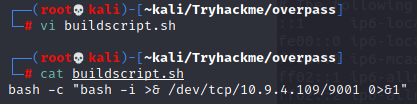
Cat crontab and we will see that buildscript.sh will be executed as a root every minute



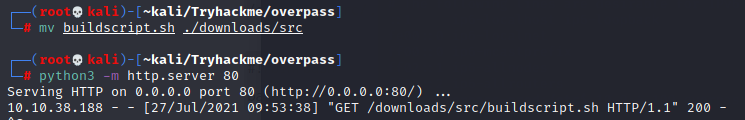
Let’s check out /etc/hosts we will see that overpass.thm is loopback address so we can edit to our ip and run a script from our machine



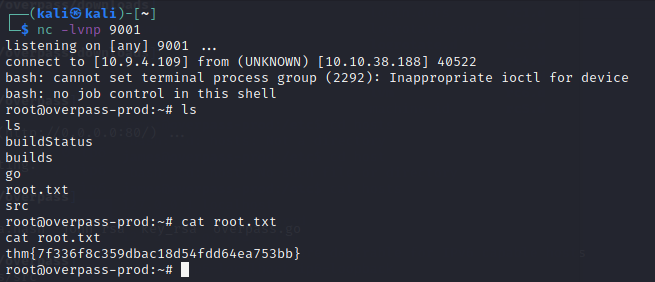
Write shell script for reverse shell and create directory based on how cronjobs is going to pull



Start simple http server and netcat listener and wait until our script will be pulled and executed



Now after got root shell, capture the root flag!





All flags

