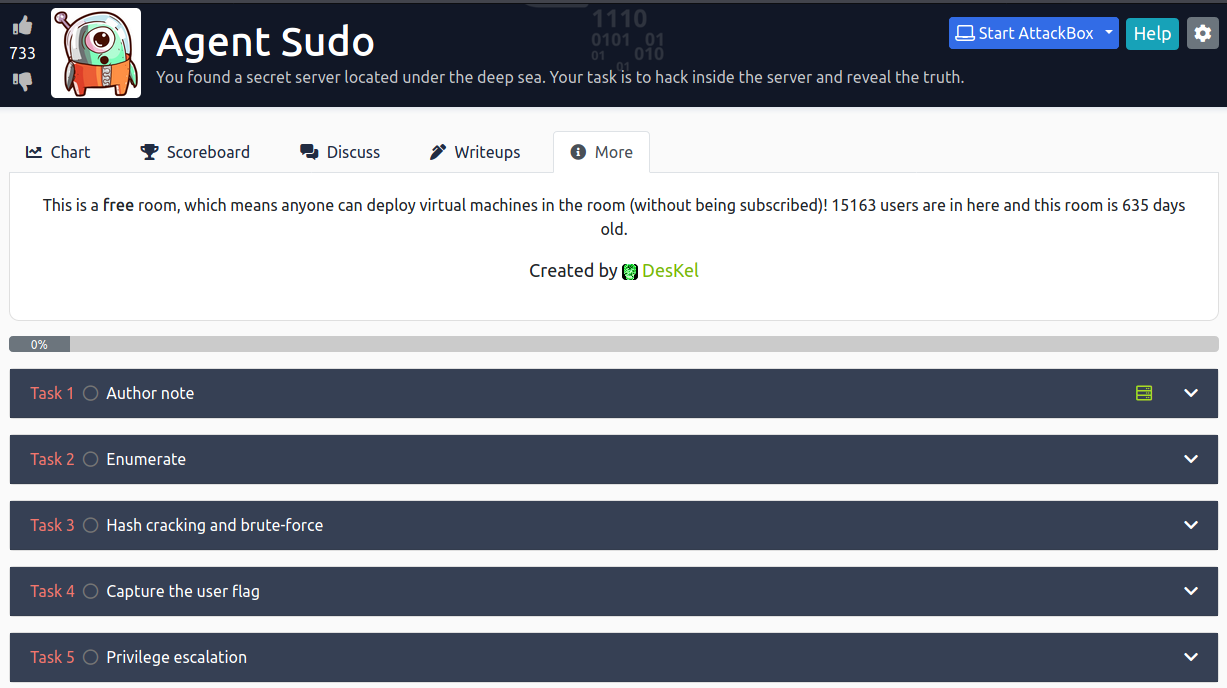
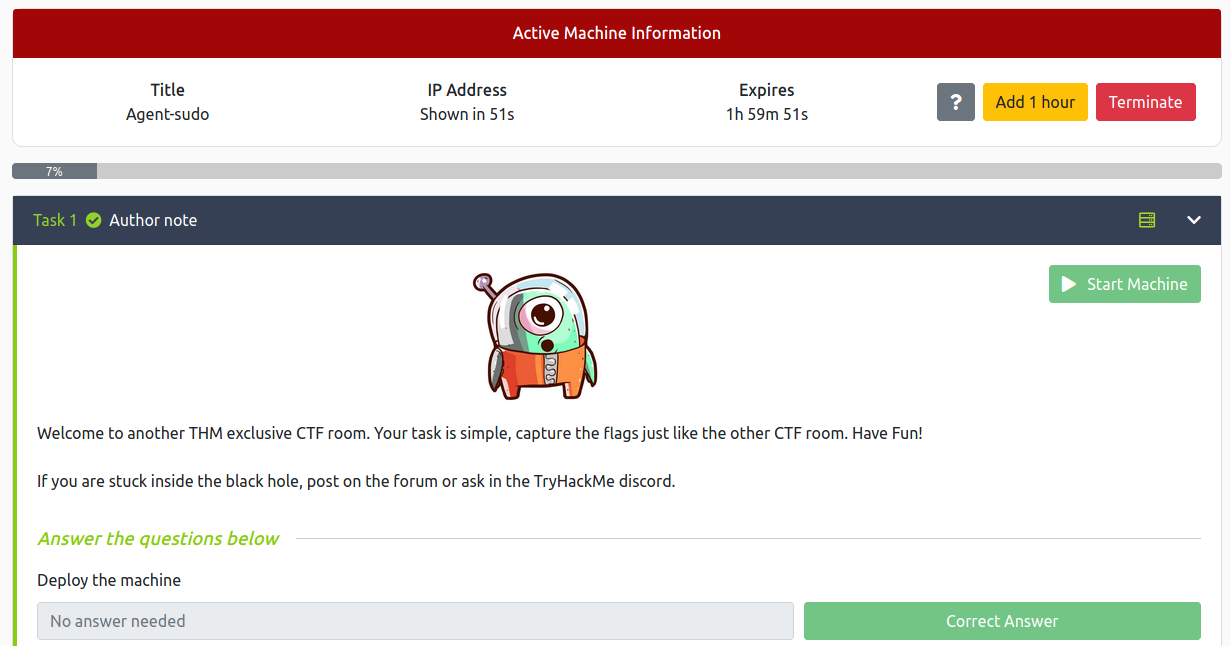
**Agent Sudo write-up**

This is write-up for Agent Sudo in TryHackMe which we will need to hack into server and elevate our privilege to rock this room!

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



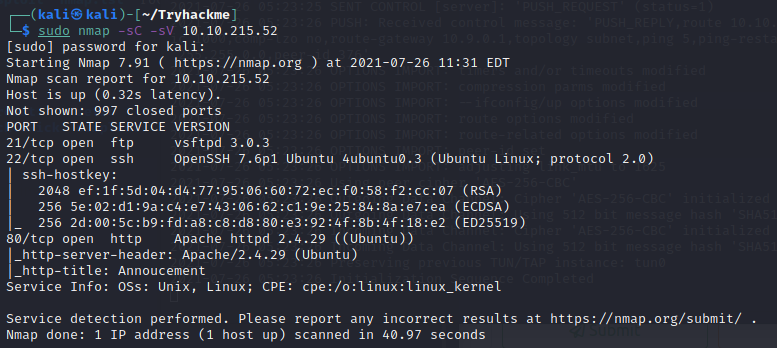
In first task it’s an Author note and we can deploy machine in this task





**How many open ports?**

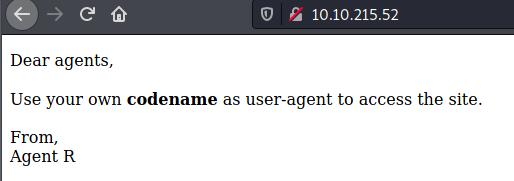
Always reconnaissance and use nmap to scan ports and we found that 3 ports are opened





**How you redirect yourself to a secret page?**

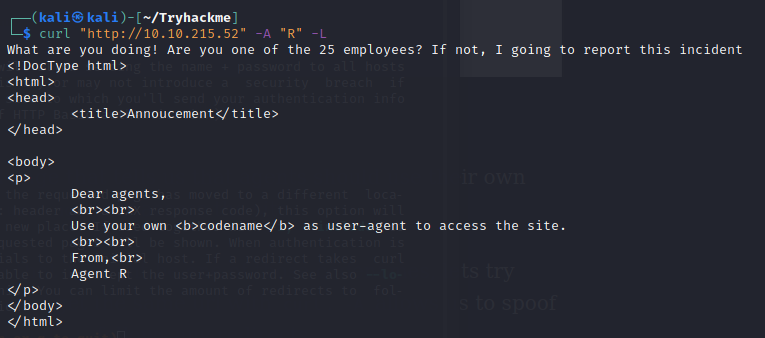
Access website that this machine is running we will see that Agent R left some message for us to use codename which I think it’s 1 alphabet character as user-agent



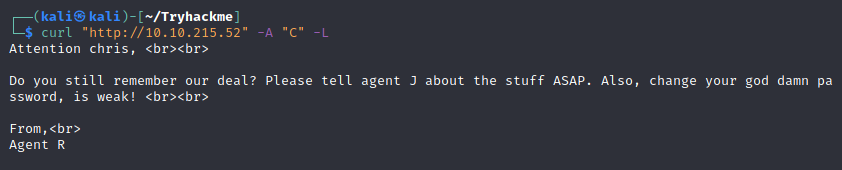


**What is the agent name?**

I’ll use curl to return response and change user-agent with tag -A and use -L to follow redirect to any site that it’ll lead us to our content and it’s obviously not Agent R

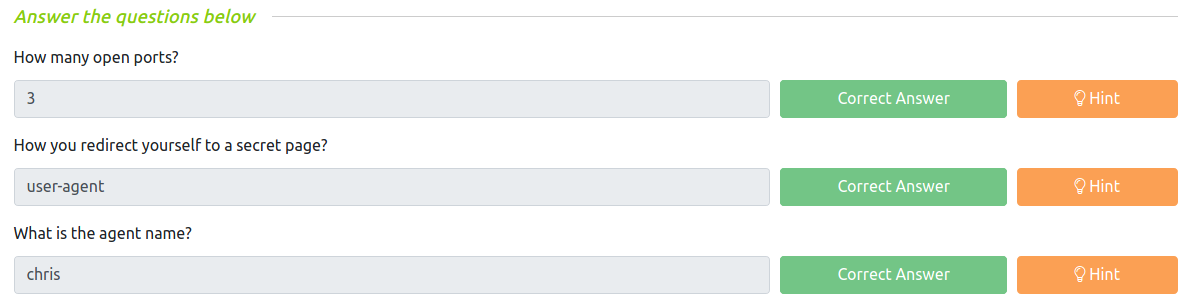


Change until we got that Agent C is valid, His name is Chris and he also has a weak password





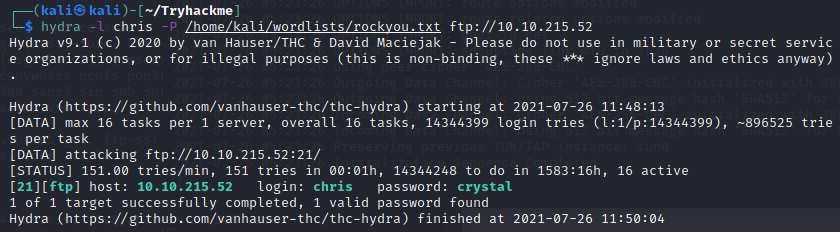
Answer - Enumerate





**FTP password**

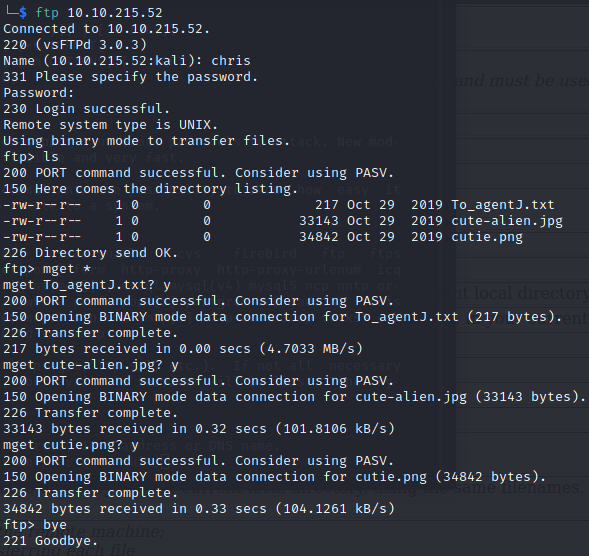
We know that we have ftp server is running but we can’t connect with anonymous user so we need to use hydra to bruteforce ftp password of chris user



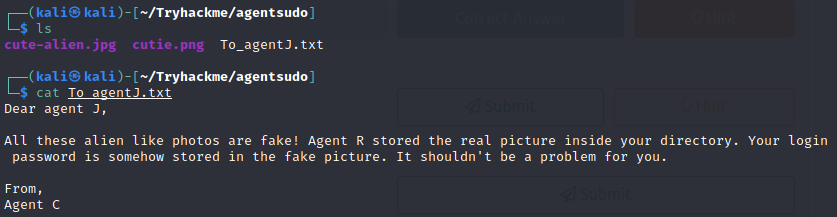


**Zip file password**

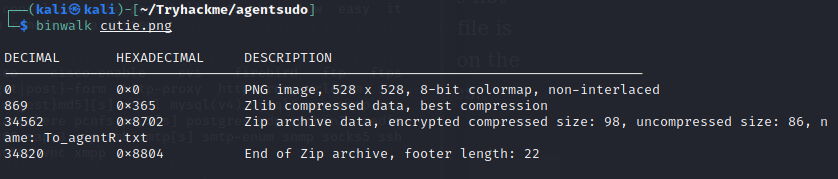
Using that password to connect to FTP server and download everything that we found



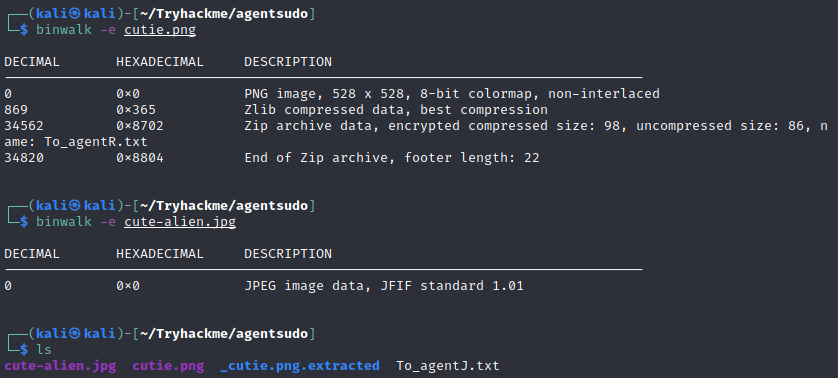
Read text file and Agent C told Agent J that 1 of this picture has password inside it (Steganography)



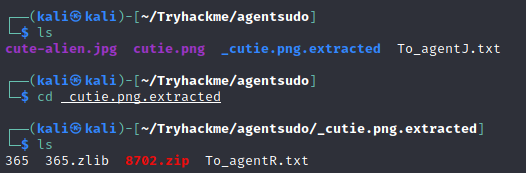
We can use binwalk for png image and we can see that this image have zip file within



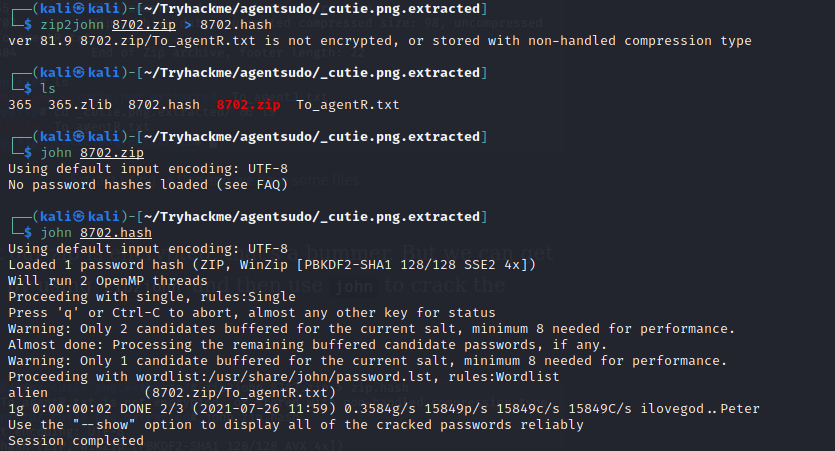
Using tag –e to extract and just for remind that we can’t use binwalk for jpg file



In directory that we extracted for png file, we have 1 encrypted zip file and blank text file



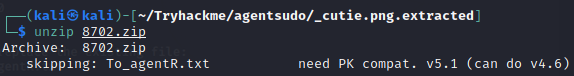
We can use John the ripper to crack password for this zip file



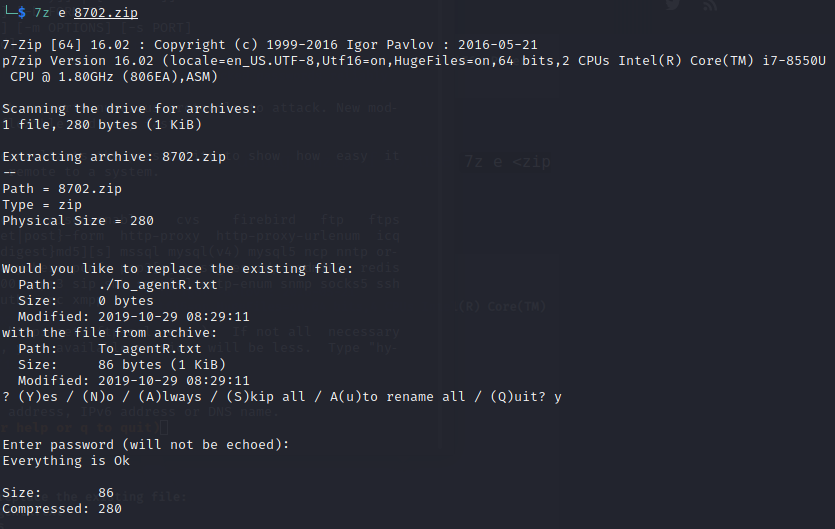


**steg password**

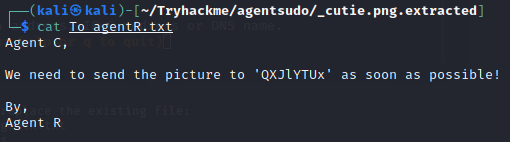
But after we got this zip file password we can’t use unzip



But we can use 7z to extract this and we will get a new text file



In this text file we will get base64 encoded password for other picture’s password



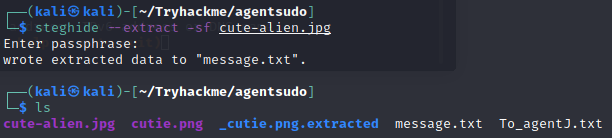
Decode it



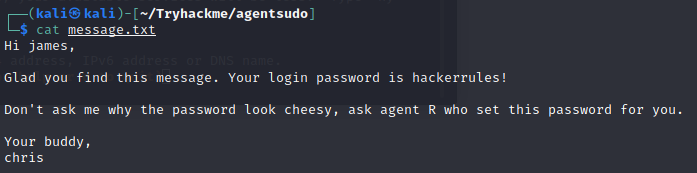


**Who is the other agent (in full name)?**

Extract jpeg file with steghide, we will get another text file



Now get both username and password of Agent J

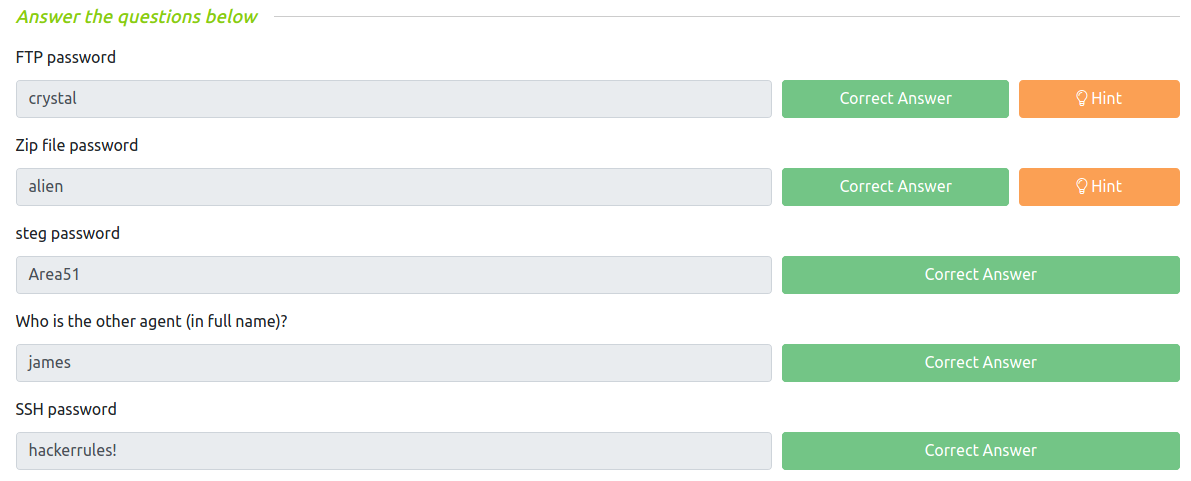




SSH password



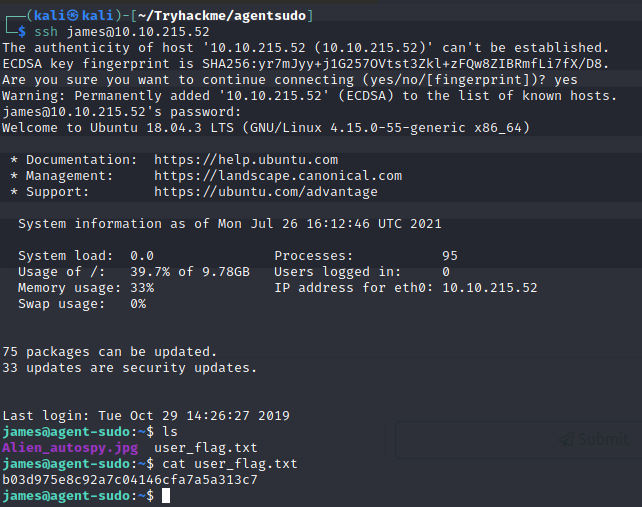
Answer – Hash cracking and brute-force





**What is the user flag?**

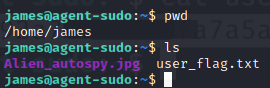
Connect to target machine using SSH and capture user flag



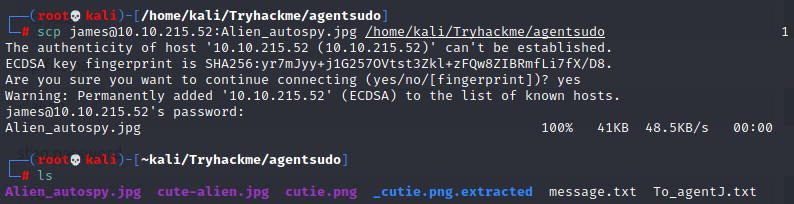


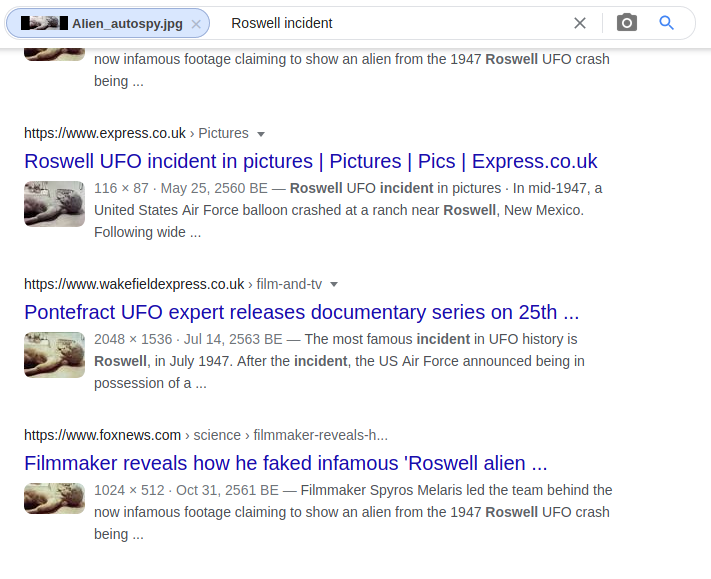
**What is the incident of the photo called?**

And we can see that this directory have an image beside flag and we need to find what incident of this image



Download this image via scp and use google image search to find what relevant to this image



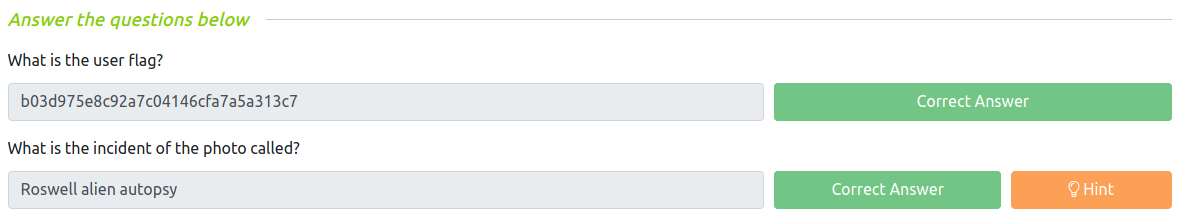


And Fox news has this answer





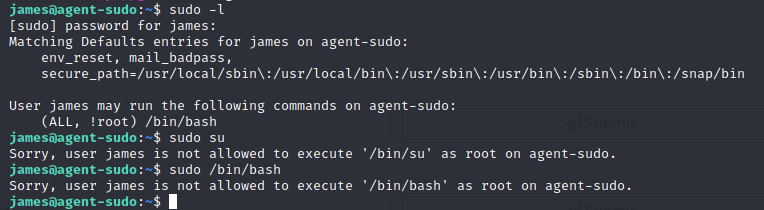
Answer – Capture the user flag



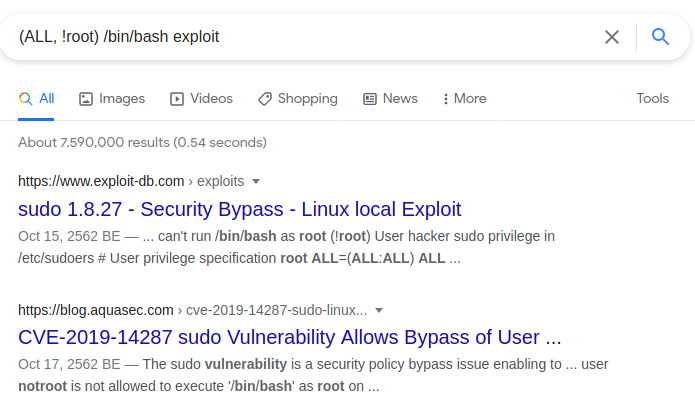


**CVE number for the escalation**

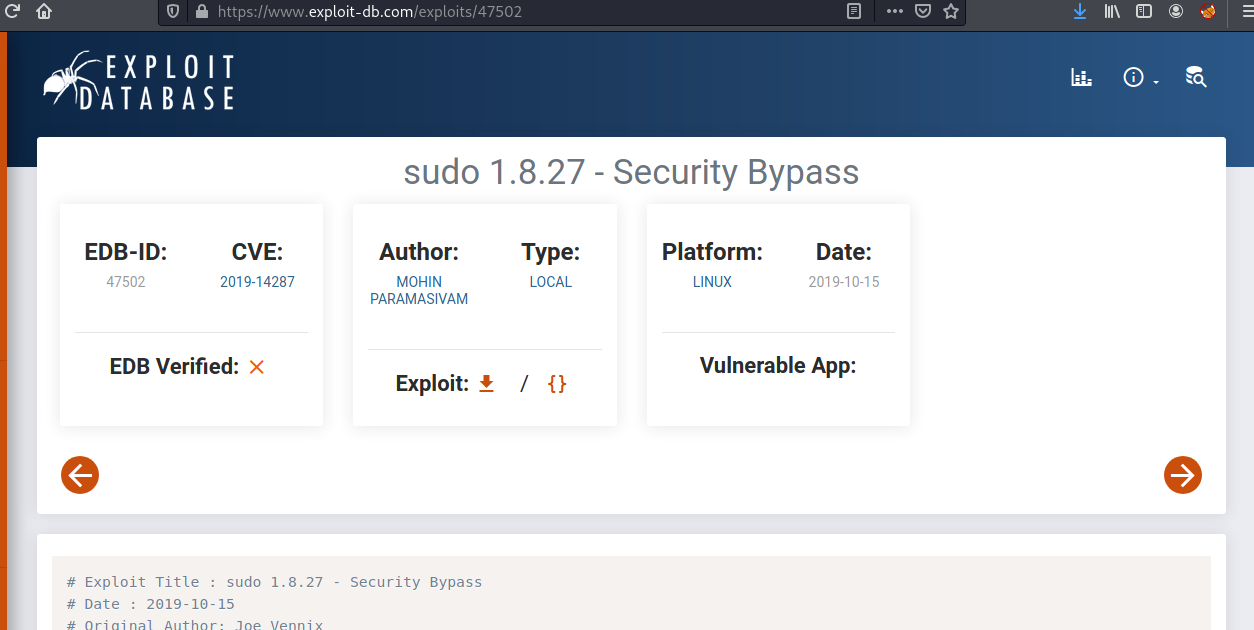
This task hint us that we need CVE to exploit, and we can’t use sudo here



Search in google and we found one in exploit-db



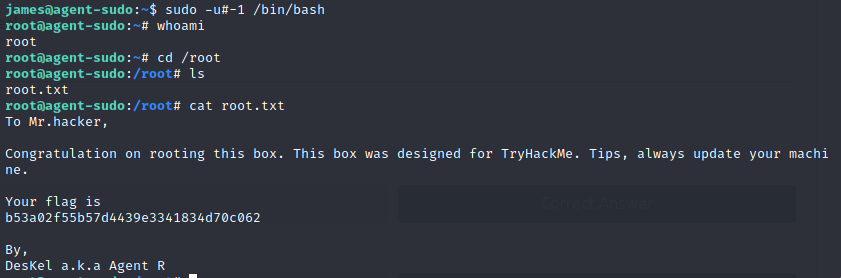
We got CVE number and how to exploit from here





**What is the root flag?**

Exploit it and capture our root flag!





**(Bonus) Who is Agent R?**



Answer – Privilege Escalation

