This is the ctf for agent sudo on tryhackme.

We first do an nmap scan and see
ftp
ssh
http

When visiting the website we get the following text:
Dear agents,

Use your own codename as user-agent to access the site.

From,
Agent R

user-agent is a term used in http header files.
Then I started burpsuite and tried to change the user-agent to R and got
What are you doing! Are you one of the 25 employees? If not, I going to report this incidentDear agents,

Use your own codename as user-agent to access the site.

From,
Agent R

So instead I tried to send it to intruder and assumed that the condenames were numbers of the alphabet.
In intruder I set to enumerate around user-agent: with sniper and did a simple wordlist with the alphabet in capital letters.
On the response from C I got.

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

From,
Agent R

Now I have the username chris!
So I then did password cracking with hydra with the username chris and got the password:crystal.
Now I could login and got 2 images and a .txt file with instructions that said something were hidden in the images.
So next I did nc -l 1234 < alien.jpg
on kali nc <target ip> 1234 > alien.jpg
nc -l 1234 > cute-alien.jpg
nc <target ip> 1234 > cute-alien.jpg

Now I googled on kali steganography and found stegcracker which I installed, when whan ran with stegcracker cute-alien.jpg said a new much faster program called stegseek exists which I then installed. Now I could quicly crack the image with stegseek cute-alien.jpg which gave a message.txt and the password Area51. The message included the name james and the password hackerrules.

The second image I could extract the contents with binwalk which put the contents in a folder. In this folder was a zip file which password could be cracked with john.
zip2john 8702.zip > johnformat.txt
john johnformat.txt --wordlist=/usr/share/wordlists/rockyou.txt
This gave the password alien.
When extracting the zip with 7z e 8702.zip and entering alien we got a new text file with QXJIYTUx which in base64 decoded is just Area51 again.

Now we try to do ssh james@<target ip> with password Area51 and get access. We can now get the user flag.
Now do sudo -l and we see (ALL, !root) /bin/bash which when we google the first result is from exploit db which points to CVE-2019-14287

From its description we can make a python file and paste the contents from the CVE. So in the target machine we do just that and when we run the file we get prompted a username where we write james and then we get root acces! Machine Rooted!