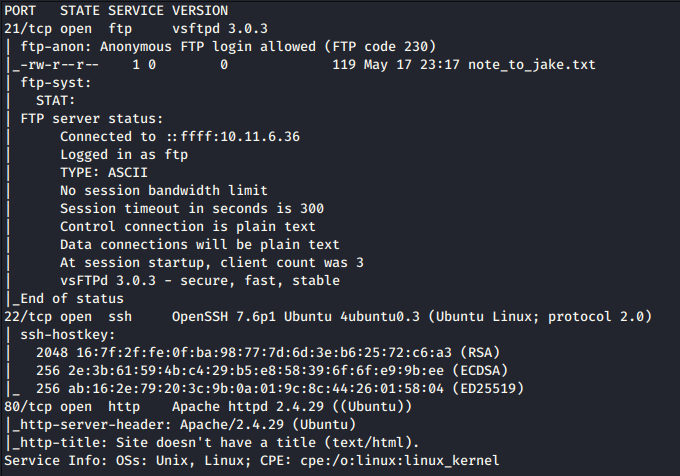
TryHackMe

Brooklyn Nine Nine

<https://tryhackme.com/room/brooklynninenine>

Walkthrough

1. NMAP SCAN



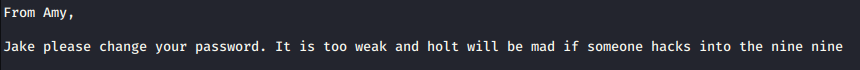
There are 3 ports open:

1. Port 21 – hosting FTP
2. Port 22 – hosting SSH
3. Port 80 – hosting HTTP

What can we do?

To start off, we can try to investigate the ftp server, as anonymous logins are allowed.

You know the drill: “ftp <IP>”

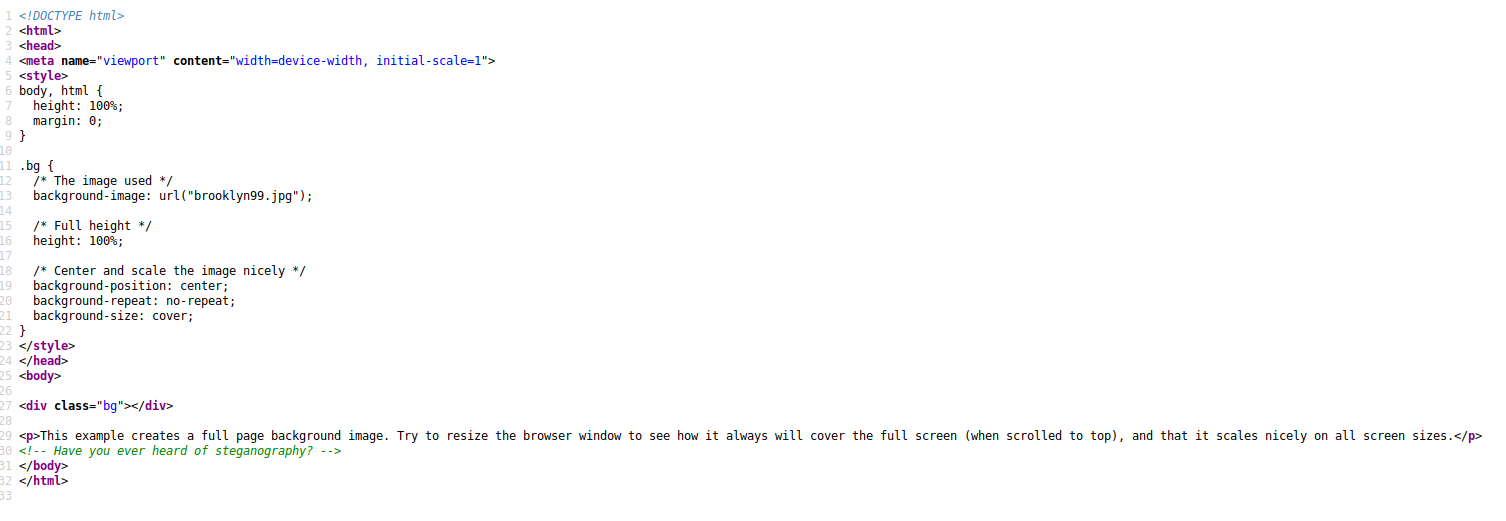
Inside the FTP server, we find a text file, note\_to\_jake.txt. We download it and print its contents:

From this, we can deduce that Jake has a shitty password, thus it can maybe be brute forced but not any more info other than that; let’s move on with our reconnaissance and such.

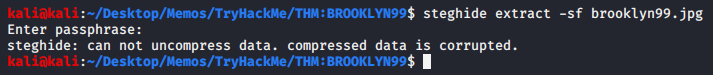
I tried going over to the HTTP service and was greeted by this:

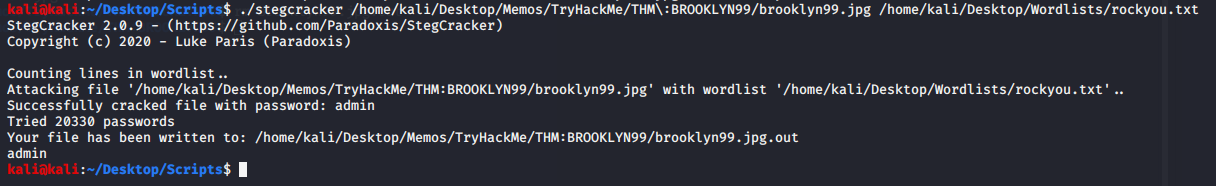


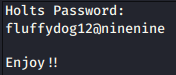
Nothing interesting here, maybe the source code will lead me somewhere?

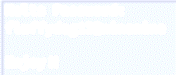


That green comment makes me feel like we have to do some investigation on the .jpg file we were presented with on the website so I downloaded it and ran steghide on it.

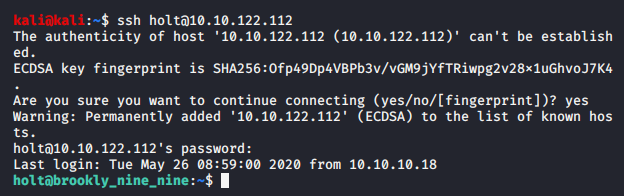
Trying to extract the data itself has proven to be a bit of a nuissance since the data is protected by a password.

In this case, we use stegcracker with the help of the rockyou.txt wordlist in order to crack the password protecting the data we need to extract from the picture itself.

We found the password and stegcracker already decompressed the hidden data.

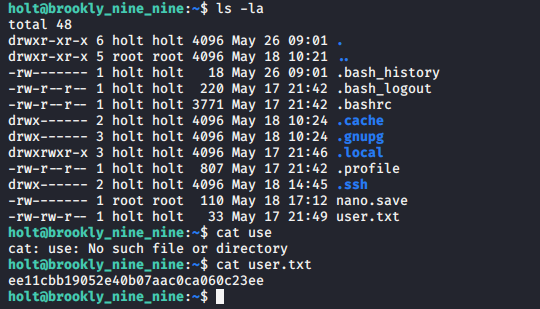
It appears as though the data itself is just a .txt file and it reads:

We found Holts’ credentials; Try to connect via ssh?



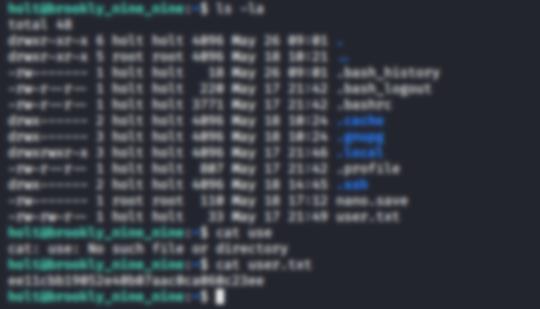
SUCCESS!

Have a look around the directory:

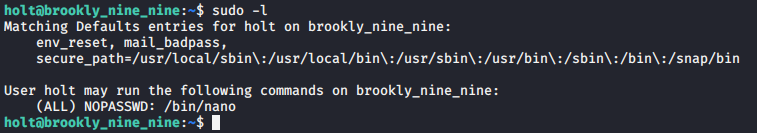


We got the user flag.

Now, onto our next task, the root flag…

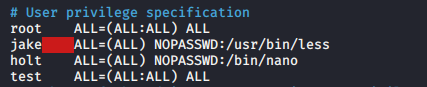


First thing that comes to mind is to check what the sudo -l command outputs:

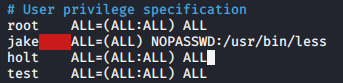


Interesting, we can use a text editor as root. What can we do with that…? \*Click\* Oh, that’s right, we can change the sudoers file so that we can run sudo on ALL commands as the user ‘holt’:

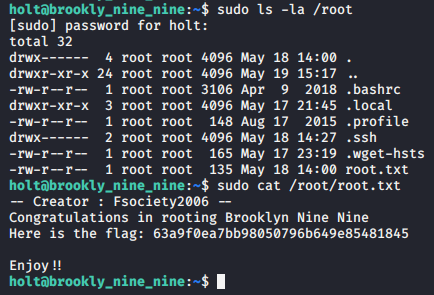
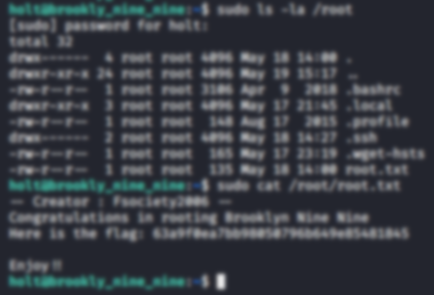




We change the permissions for holt to:



Save the file and now you can run sudo at will, ON ANYTHING!



END

😊