ENUMERATION :

NMAP SCAN :

sudo nmap -sV -sV -A -sS -T4 10.10.232.91



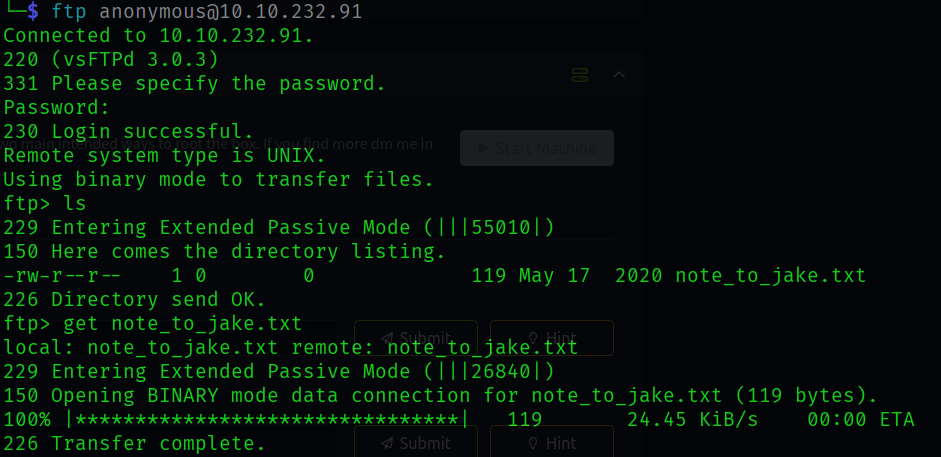
Meanwhile lets do directory enumeration using gobuster but no useful result :

gobuster dir -u http://10.10.232.91 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

A screenshot of a computer program

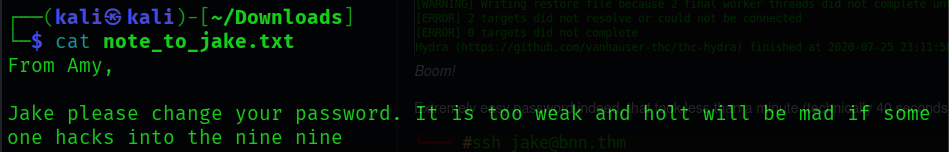
AI-generated content may be incorrect.

ftp Anonymous login is possible let login in using ftp :



Found a text file , lets download it to our computer .

Let cat the file :



From the message we found a name Jake which may be a user .

Lets use hydra to bruteforce the password

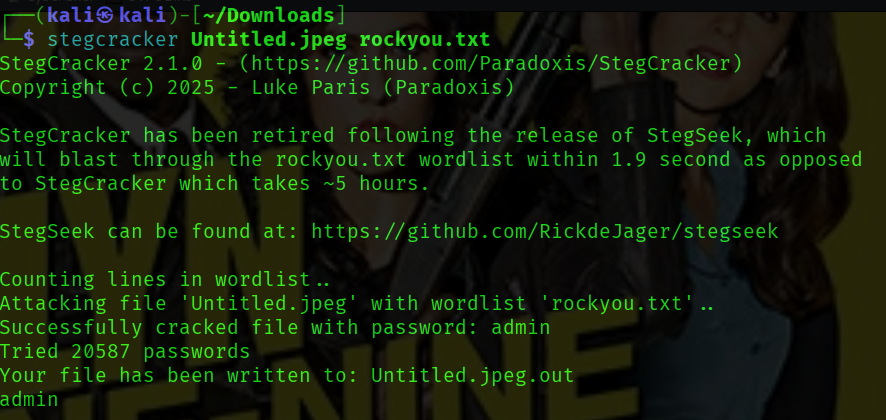
On inspecting the website we found a comment :

A screen shot of a computer

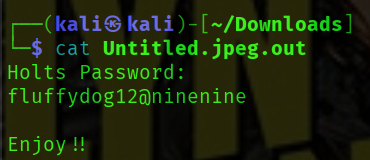
AI-generated content may be incorrect.

So we downloaded the image and did stegnography :

We used stegcracker to crack it



And while reading the out file got this message :

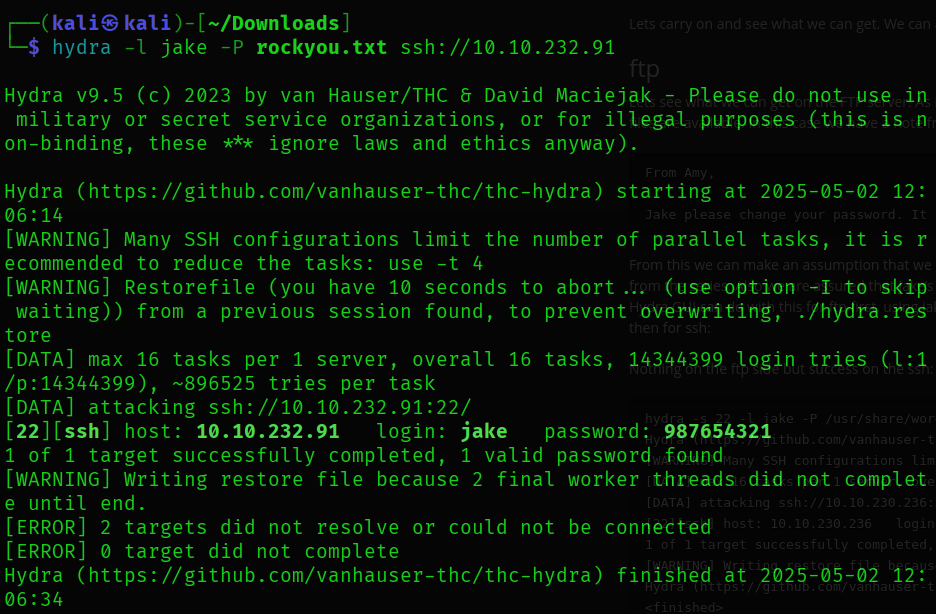


Lets save this for later .

Now lets focus on Jake lets use hydra to bruteforce the password.

Command -

hydra -l Jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.232.91

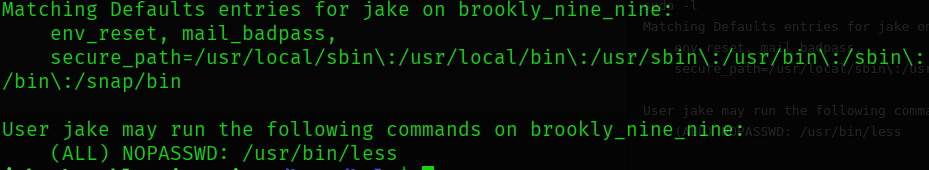


In user holt found the user.txt file



For the privilege escalation

Let see what the usr holt can do

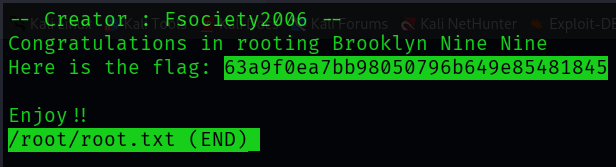


So without password usr jake can use /usr/bin/less .

Lets see

Lets use the command /usr/bin/less /root/root.txt





And here we found the root.txt flag …

