Hack The Box

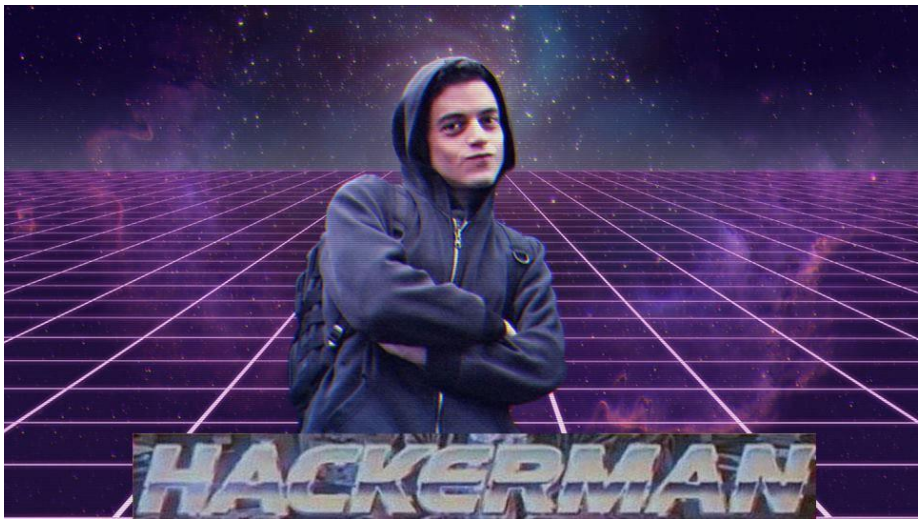
Stego Challenge

Hackerman

Easy – Retired Chall

SirenCeol

After extract the given zipped file, I only got 1 file named “hackerman.jpg” and the person in picture is called Elliot from Mr. Robot series but that is unrelevant to solve with this chall,



because of the given description of the chall I know this chall involved steghide, but to extract the string inside the photo I need to know the password that’s why I choose stegcracker to crack the password with bruteforce method

```
root@opacite:~/Tools/Forensic# stegcracker ~/Downloads/hackerman.jpg ~/wordlists
/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file '/root/Downloads/hackerman.jpg' with wordlist '/root/wordlists/ro
ckyou.txt'..
Successfully cracked file with password: almost
Tried 11924 passwords
Your file has been written to: /root/Downloads/hackerman.jpg.out
almost
```

Using stegcracker + rockyou.txt wordlist I got the password of the steghide it is “almost” and the output of stegcracker is on “/root/Downloads/hackerman.jpg.out” and if I open it, it has base64 string

```
root@opacite:~/Downloads# cat hackerman.jpg.out
SFRCezN2MWxfYzBycH0=
root@opacite:~/Downloads# echo "SFRCezN2MWxfYzBycH0=" | base64 -d
HTB{3v1l_c0rp}root@opacite:~/Downloads#
```

So after I decode the string I got the flag.

HTB{3v1l_c0rp}