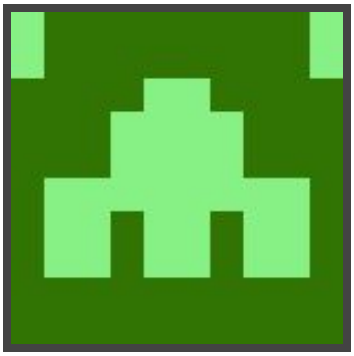
Hack The Box

PEN-TESTING LABS



Beep

16th October 2017 / Document No D17.100.22

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Medium

Classification: Official

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

SYNOPSIS

Beep has a very large list of running services, which can make it a bit challenging to find the correct entry method. This machine can be overwhelming for some as there are many potential attack vectors. Luckily, there are several methods available for gaining access.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

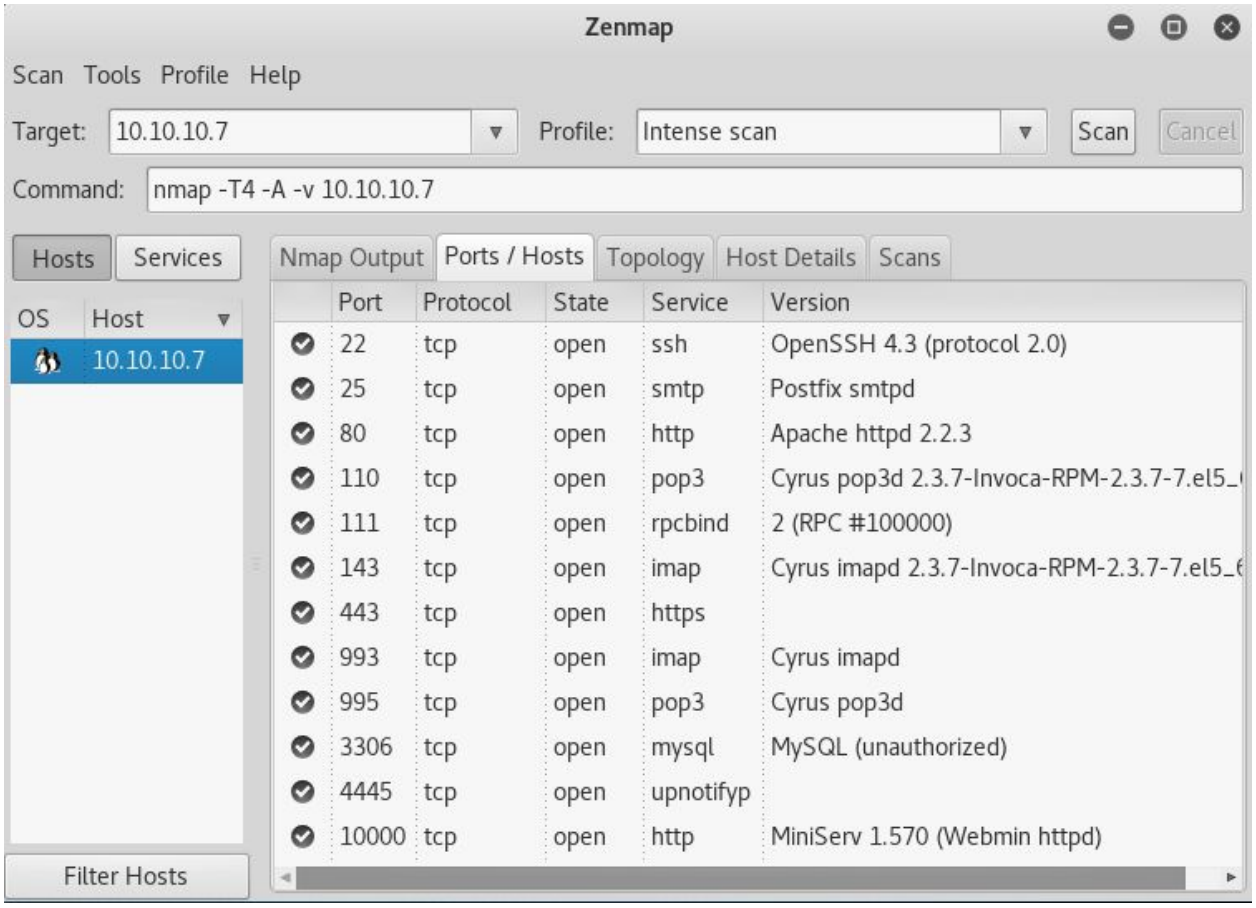
Skills Learned

- Web-based fuzzing
- Identifying known exploits
- Exploiting local file inclusion vulnerabilities

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

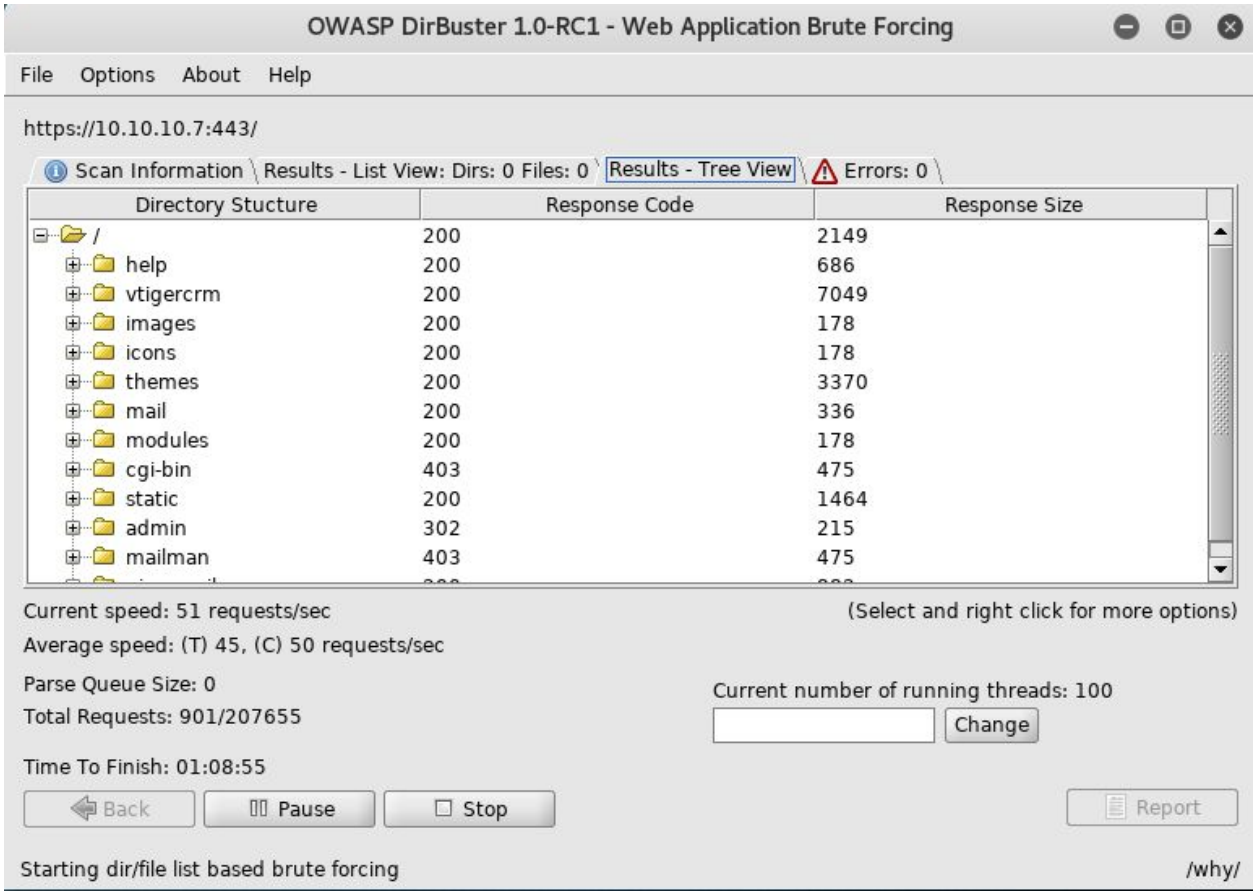
Enumeration

Nmap



Nmap finds quite a long list of services. For now, Apache, which is running on ports 80 and 443, will be the primary target.

Dirbuster



Dirbuster also finds a huge list of directories with several content management systems and open source applications. There are several vulnerabilities that can lead to shell amongst the results.

Exploitation

Exploit: https://www.exploit-db.com/exploits/37637/

Browsing to the main web directory reveals a copy of **Elastix**. Some searching finds a local file inclusion vulnerability for Elastix 5.3.0 and 5.4.0; **Exploit-DB 37637**.

The proof of concept is extremely simple. Browsing to **https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action** will expose the credentials for AMPortal.

The machine is vulnerable to password reuse, and it is possible to SSH in directly as the root user with the **AMPDBPASS** password. The flags can be obtained from **/home/fanis/user.txt** and **/root/root.txt**