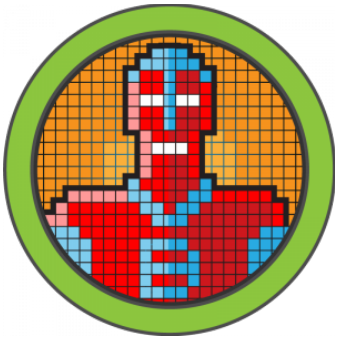
Hack The Box
PEN-TESTING LABS



Blocky

5th October 2017 / Document No D17.100.07

Prepared By: Alexander Reid (Arrexel)
Machine Author: Arrexel
Difficulty: Easy
Classification: Official

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

SYNOPSIS

Blocky is fairly simple overall, and was based on a real-world machine. It demonstrates the risks of bad password practices as well as exposing internal files on a public facing system. On top of this, it exposes a massive potential attack vector: Minecraft. Tens of thousands of servers exist that are publicly accessible, with the vast majority being set up and configured by young and inexperienced system administrators.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

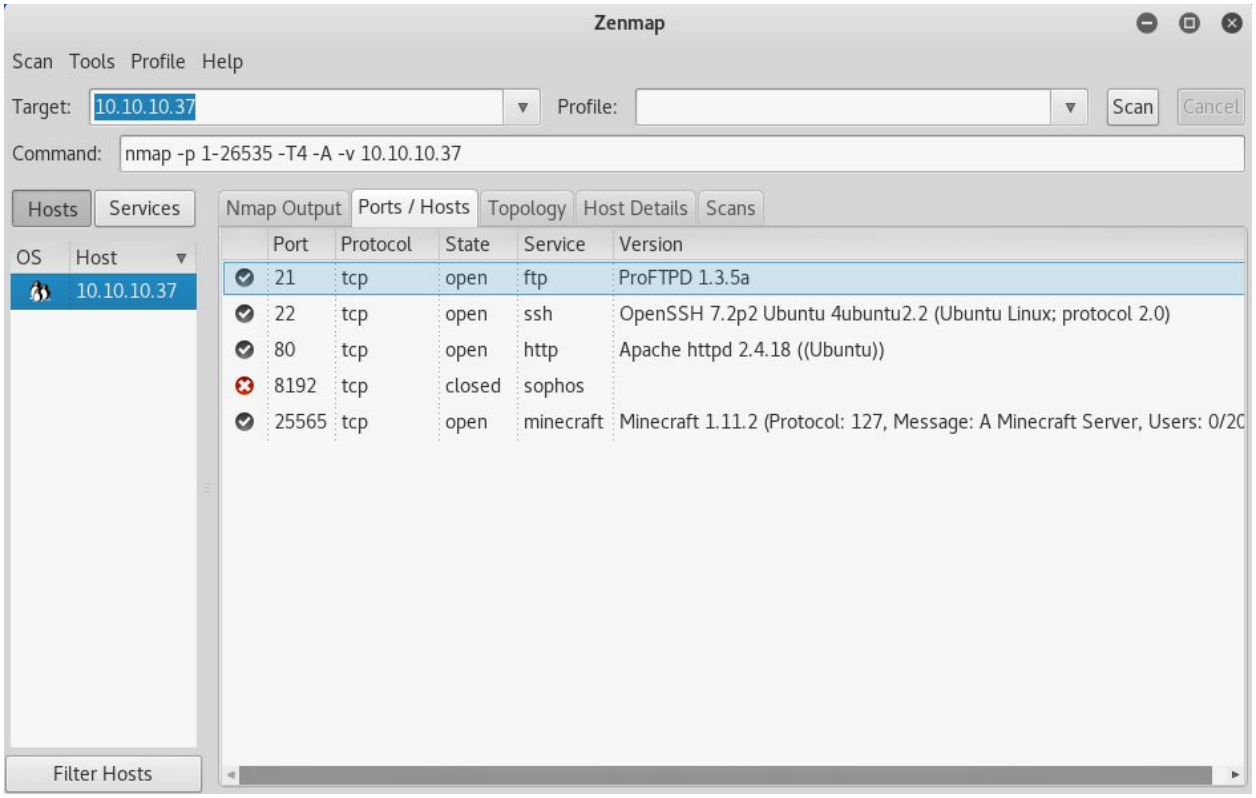
Skills Learned

- Exploiting bad password practices
- Decompiling JAR files
- Basic local Linux enumeration

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

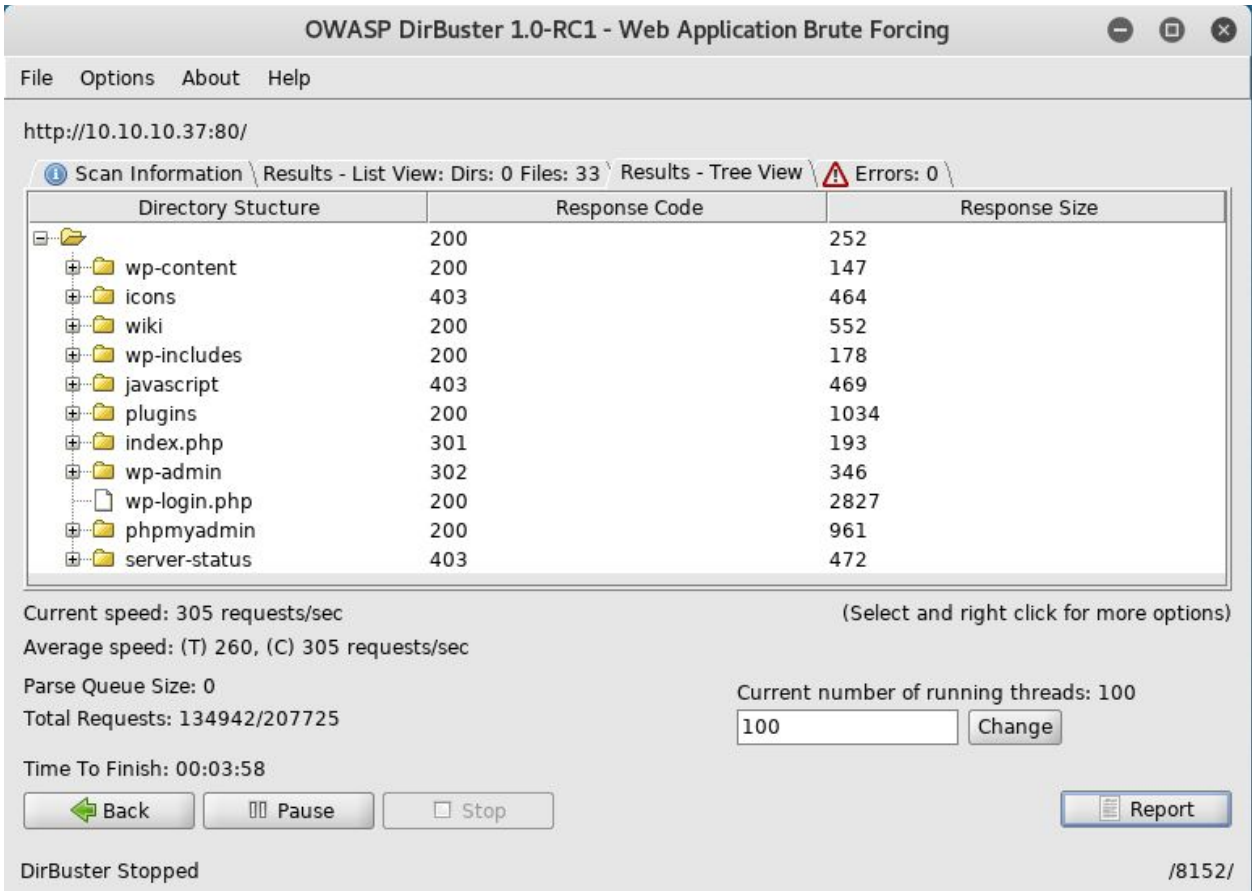
Enumeration

Nmap



There are quite a few open services. ProFTPD, OpenSSH, Apache, Minecraft and an unresponsive service on 8192 (which just happens to be the standard Minecraft Votifier port).

Dirbuster



After a bit of trial and error, it is clear that fuzzing a Wordpress website presents a few challenges for recursive and PHP file fuzzing. Using the Dirbuster lowercase medium wordlist and only fuzzing for directories discovers a **plugins** directory, which is not to be confused with the official Wordpress **wp-content/plugins** directory. A quick peek inside reveals some jar files, which Minecraft uses to add additional features to a server.

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

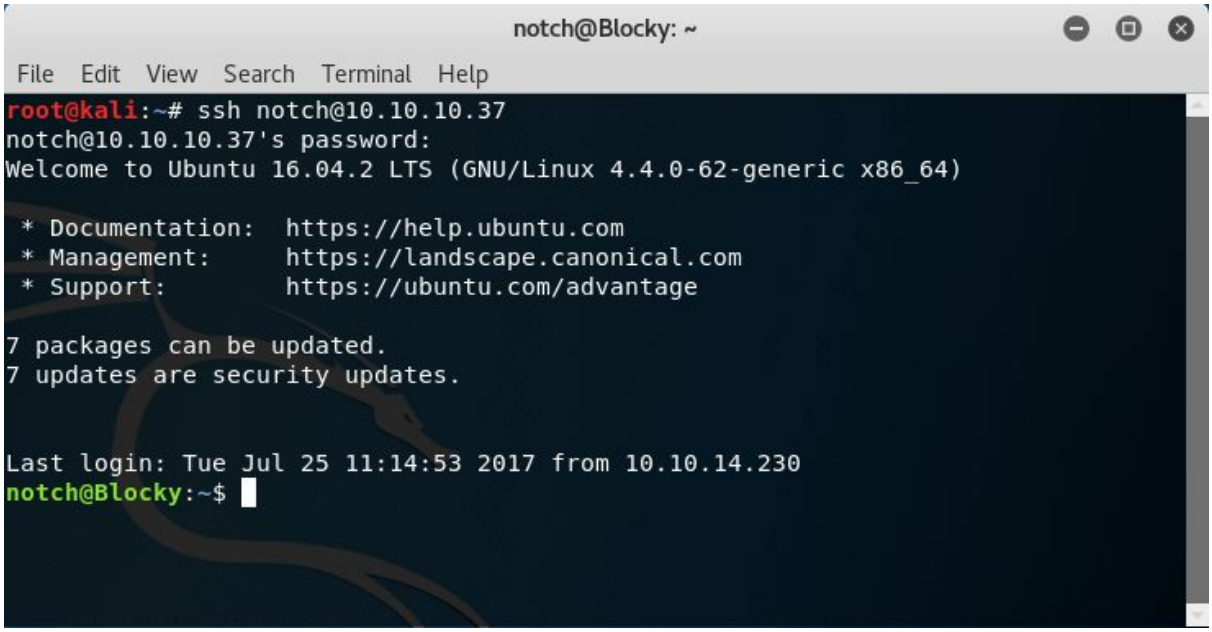
Exploitation

Looking at the jar files, griefprevention is an open source plugin that is freely available. BlockyCore, however, appears to be created by the server administrator, as its title relates directly to the server. Decompiling with JD-GUI exposes the credentials for the root MySQL user.

```
public class BlockyCore
{
  public String sqlHost = "localhost";
  public String sqlUser = "root";
  public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
```

While possible to login to PHPMyAdmin with these credentials, it is not the intended method for initial access. The PHPMyAdmin route is far more complex, and involves changing the Wordpress administrator password, creating a reverse PHP shell and escalating from the www-data user via the DCCP Double-Free technique (CVE-2017-6074).

The intended method for this machine is a simple username and password reuse. Attempting to connect via SSH to the **notch** user (username discovered in the Wordpress post) and supplying the MySQL root password gives immediate access.



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

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

After obtaining the user flag from **/home/notch/user.txt**, running LinEnum gives a very long list of data. Refer to **linenum_blocky.txt** to view the full report. At first glance, the method to obtain the root flag is quite obvious; notch is part of the sudoers group. Simply **sudo -i** for a full root shell, and grab the root flag from **/root/root.txt**