HackTheBox – Blocky

I added blockys IP address – 10.10.10.37 to /etc/hosts as blocky.htb

I started with the usual fast nmap scan of the top 1000 ports followed by a fast scan of all ports.

```
root@kali:~/Desktop/HTB/Blocky# nmap blocky.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 20:52 BST
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.20s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
8192/tcp closed sophos

Nmap done: 1 IP address (1 host up) scanned in 10.18 seconds
root@kali:~/Desktop/HTB/Blocky# nmap blocky.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 20:53 BST
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.42% done; ETC: 20:55 (0:00:17 remaining)
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.017s latency).
Not shown: 65530 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
80/tcp    open   http
8192/tcp  closed sophos
25565/tcp open   minecraft

Nmap done: 1 IP address (1 host up) scanned in 132.45 seconds
root@kali:~/Desktop/HTB/Blocky#
```

A more thorough scan reveals that we have an FTP Server, an SSH Server, a web server, sophos antivirus (great...) and a Minecraft server, interesting...

 # Nmap 7.80 scan initiated Tue Apr 21 20:56:18 2020 as: nmap -A -p21,22,80,8192,25565 -oN nmap.txt blocky.htb
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.018s latency).

PORT   STATE SERVICE   VERSION
21/tcp   open   ftp   ProFTPD 1.3.5a
22/tcp   open   ssh   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)
| 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_ 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp   open   http   Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft – Under Construction!
8192/tcp closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Device type: general purpose|WAP|specialized|storage-misc|broadband router|printer
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (94%), Asus embedded (90%), Crestron 2-Series (89%),

HP embedded (89%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel cpe:/h:asus:rt-ac66u cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:3.4 cpe:/o:linux:linux_kernel:2.6.22
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 or 4.2 (94%), Linux 4.2 (94%), Linux 4.4 (94%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.12 (91%), Linux 3.2 - 4.9 (91%), Linux 3.8 - 3.11 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8192/tcp)
HOP RTT ADDRESS
1 19.51 ms 10.10.14.1
2 19.56 ms blocky.htb (10.10.10.37)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
 # Nmap done at Tue Apr 21 20:56:31 2020 -- 1 IP address (1 host up) scanned in 12.27 seconds

After checking if I could access FTP anonymously (which I couldn't) I moved on to the web server. I used dirb to bruteforce directories to see if there was anything of interest.

DIRB v2.22
By The Dark Raver

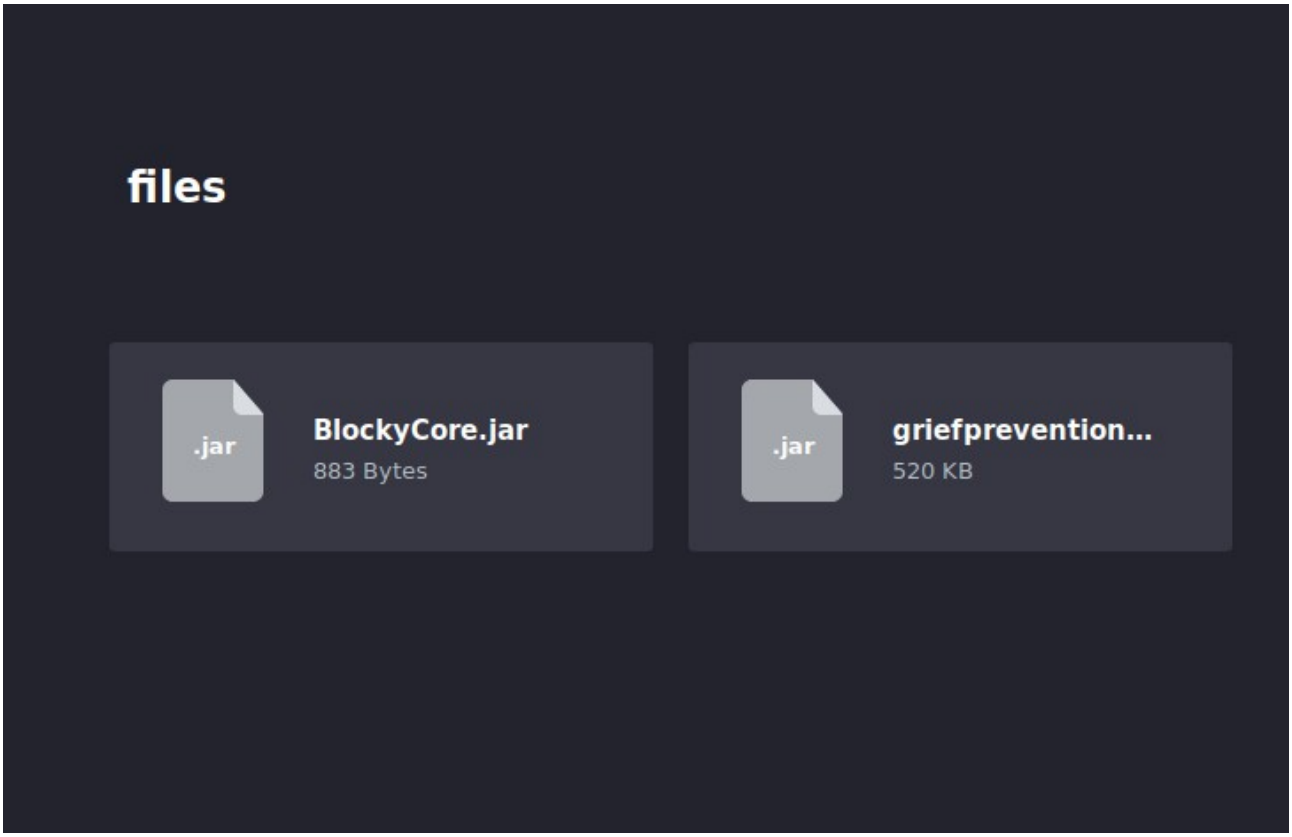
OUTPUT_FILE: dirb.txt
START_TIME: Sat Mar 21 14:31:54 2020
URL_BASE: http://blocky.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

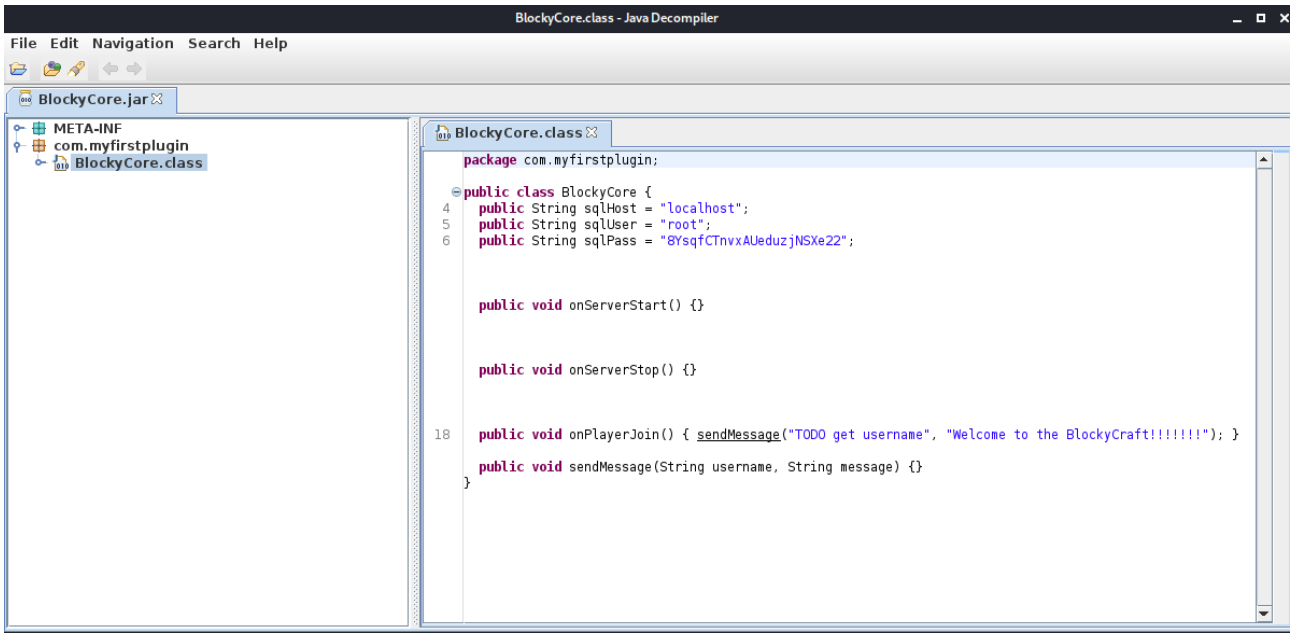
---- Scanning URL: http://blocky.htb/ ----
+ http://blocky.htb/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://blocky.htb/javascript/
==> DIRECTORY: http://blocky.htb/phpmyadmin/
==> DIRECTORY: http://blocky.htb/plugins/
+ http://blocky.htb/server-status (CODE:403|SIZE:298)
==> DIRECTORY: http://blocky.htb/wiki/
==> DIRECTORY: http://blocky.htb/wp-admin/
==> DIRECTORY: http://blocky.htb/wp-content/
==> DIRECTORY: http://blocky.htb/wp-includes/

+ http://blocky.htb/xmlrpc.php (CODE:405|SIZE:42)

There is a few promising results here, after looking through some of them I ended up at /plugins where I found the following 2 files.



I used a Java decompiler to look at the contents of both files where I found a username (root?!?!) and password for an SQL database.



I tried these credentials against SSH with no luck.

```
root@kali:~# ssh root@blocky.htb
root@blocky.htb's password:
Permission denied, please try again.
```

I decided to look around the website a little more and noticed a username on one of the posts – **Notch**

JULY 2, 2017 BY NOTCH

Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 🙂

Search …

RECENT POSTS

Welcome to BlockyCraft!

RECENT COMMENTS

ARCHIVES

July 2017

CATEGORIES

Uncategorized

META

Log in

Entries RSS

Comments RSS

WordPress.org

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

I successfully tried SSH again with the same password only this time against Notch.

```
root@kali:~# ssh notch@blocky.htb
notch@blocky.htb'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: Sun Dec 24 09:34:35 2017
notch@Blocky:~$
```

The simplest of enumeration lead me to the root account, sudo -l revealed that notch could run anything as root, and as I knew their password, so could I!