What's Your Name

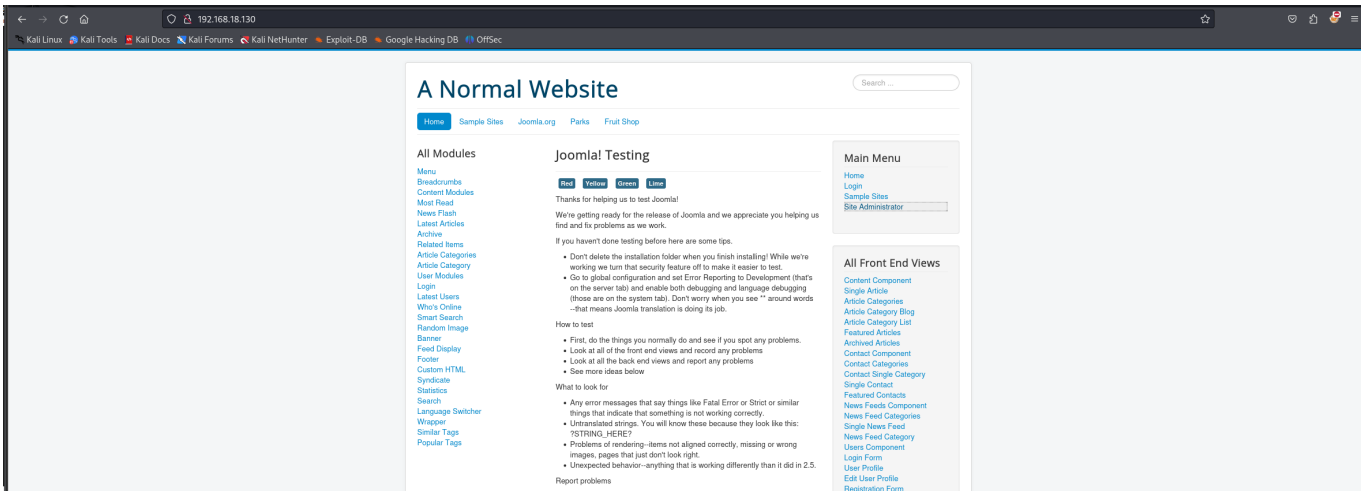
https://tryhackme.com/jr/hacksocweeklyctf

We start with our nmap scan and find 2 open ports and 3 closed ports.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-02 11:46 EDT
Nmap scan report for 192.168.18.130
Host is up (0.00071s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE       VERSION
22/tcp   open   ssh           OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 4e:04:09:96:50:62:d8:57:8b:5f:3a:a8:1a:f2:46:f0 (ECDSA)
|_  256 94:fe:8a:df:3f:be:84:2d:6c:d6:7d:11:fd:43:00:7f (ED25519)
80/tcp   open   http          nginx 1.18.0 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management  - Version 3.4.6
|_http-title: Home
|_http-server-header: nginx/1.18.0 (Ubuntu)
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
4444/tcp closed krb524
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 15.91 seconds
```

We notice an outdated Joomla version (3.4.6) which may be vulnerable to various critical vulnerabilities. Looking at the website it appears to be quite bare with lots of pages not added to the domain.

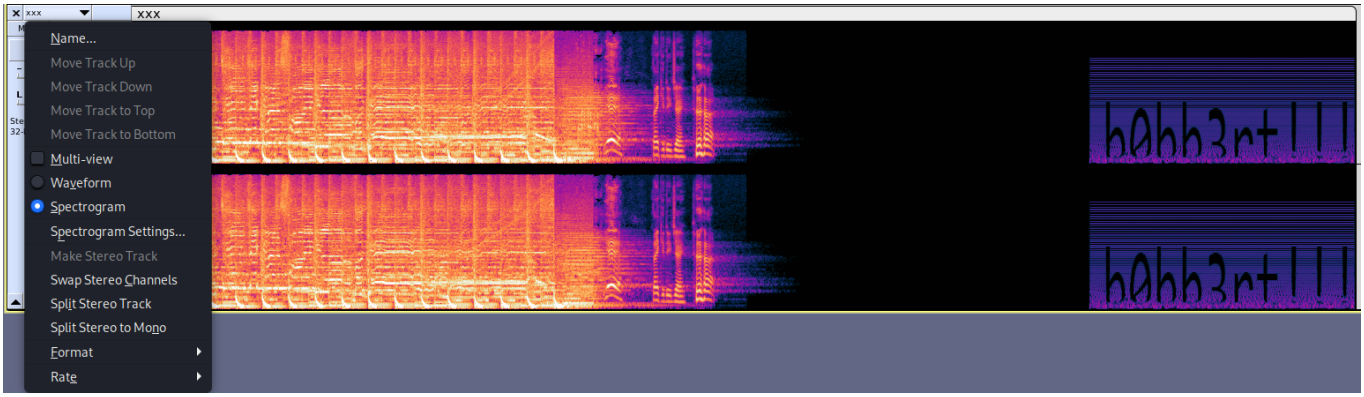


Using the right kind of directory guessing wordlist, the user is intended to find "zoo.html" which contains a bare-bones HTML page. The page is titled "Bobbert's Private Zone" and contains two lines, the first saying "Buy a book to remember my password in" and then a second line that says "This is my favourite song" with nothing appearing to be following.

```
1 <!DOCTYPE html>
2 <html><head>
3 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
4     <meta charset="UTF-8">
5     <title>Bobbert's Private Zone</title>
6 </head>
7 <body>
8     <li>Buy a book to remember my passwords in.</li>
9     <li>This is my favourite song! <audio src="xxx.mp3"></audio></li>
10
11 </body></html>
12
```

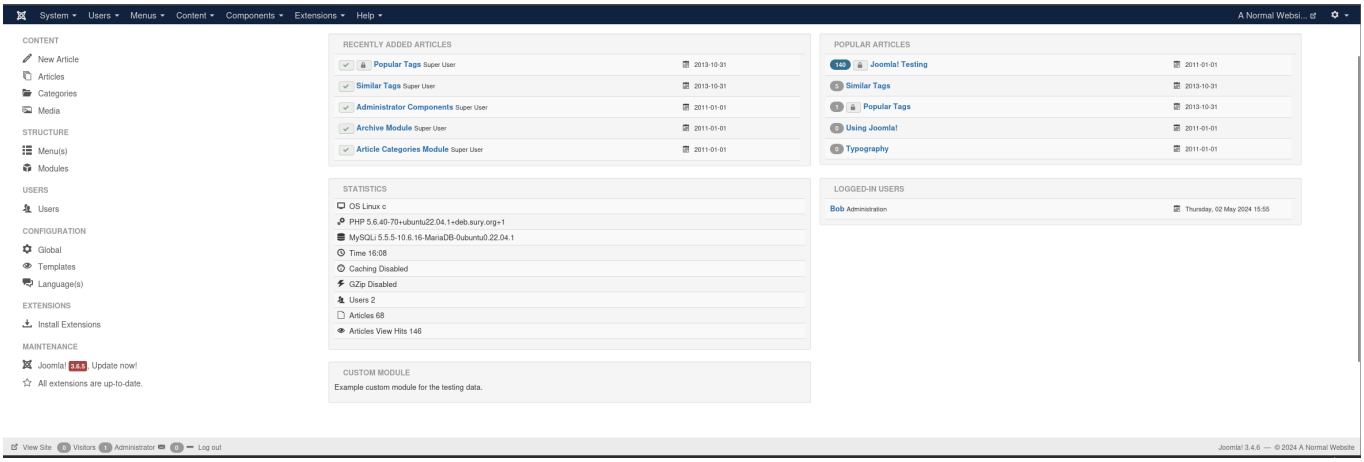
Viewing the source code we find the xxx.mp3 which when navigating to appears to play "DJ Got us Falling in Love" by Usher feat Pitbull. The audio clip contains a long silence at the end with a weird sound playing towards the end of it. This is hoped to hint the user that something is off and they should look into the audio file.

There are multiple forms of steganography that the user could check for in this audio file although this file has hidden something in the Spectogram. Using an app such as Audacity, we can import the file and view the spectogram, and find a piece of hidden text.



The text "b0bb3rt!!!" might indicate a login password.

Sure enough, heading over to the Administrator login we login with the credentials "bobbert:b0bb3rt!!!".



Through enumerating the administrator panel we find two notes which give us another set of credentials and further mentions to the outdated Joomla version.

Notes for user Bob (ID #629)

1. **#2 REMINDER**

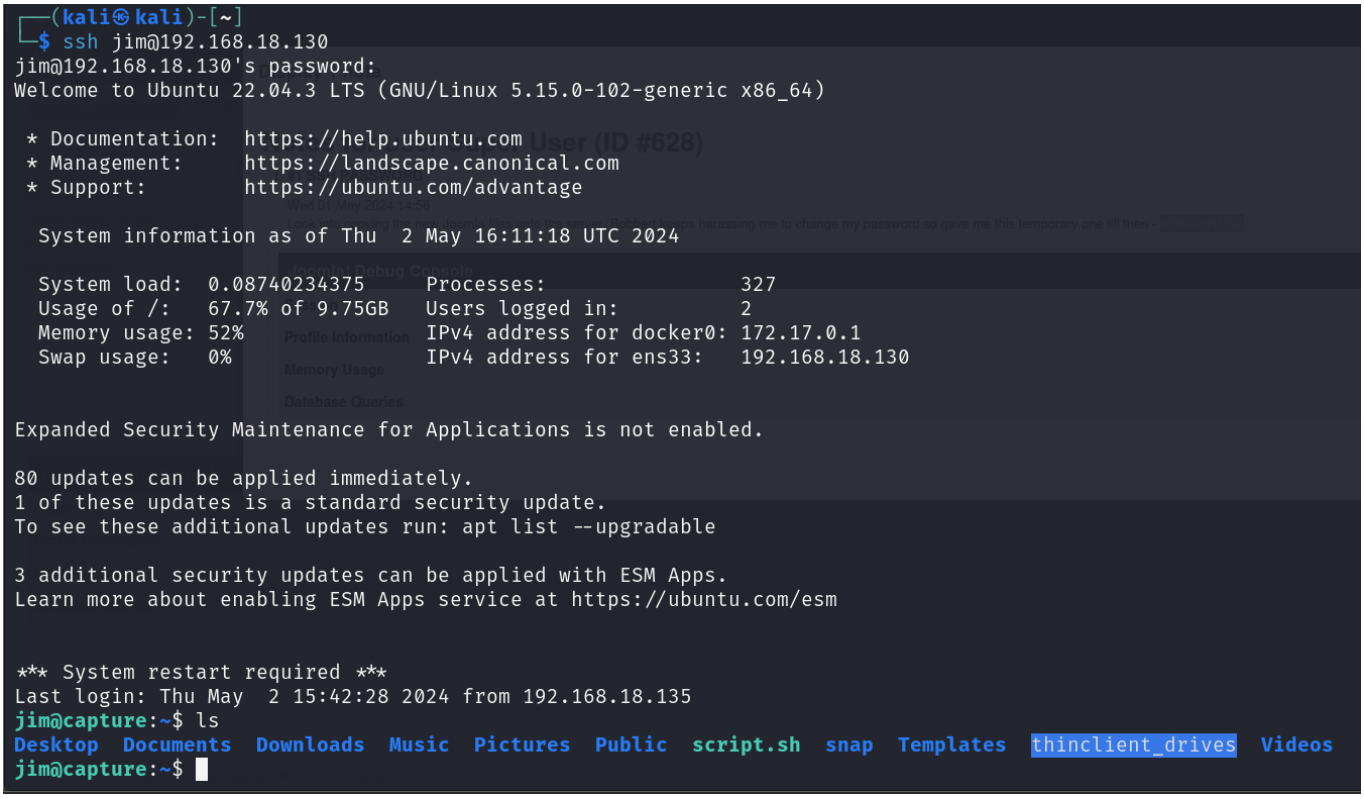
   Wed 01 May 2024 14:58
   Remind jim to update the website at some point.

Notes for user Super User (ID #628)

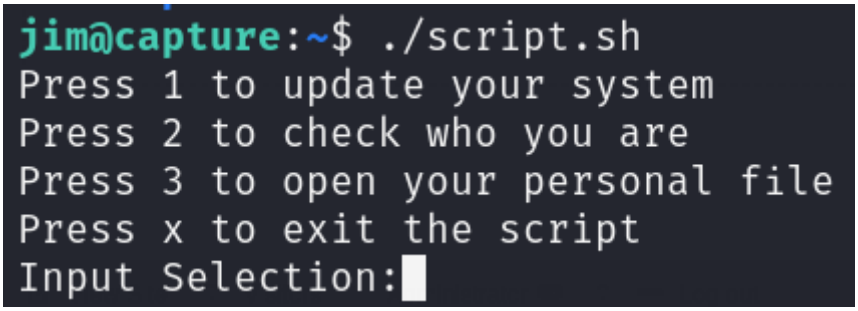
1. **#1 SSH PASSWORD**

   Wed 01 May 2024 14:56
   Look into copying the new Joomla files onto the server. Bobbert keeps harassing me to change my password so gave me this temporary one till then - bObbertRU!es

We take these credentials to SSH and get a successful login.

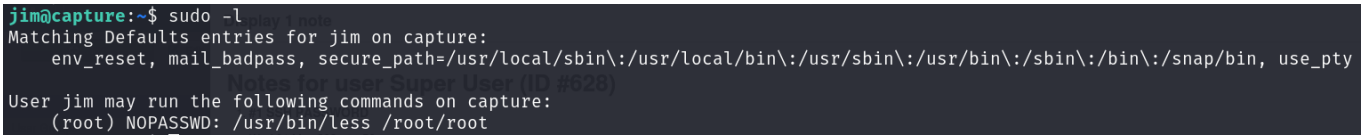


In our home directory we have "script.sh" which when we run, displays 3 options to us.

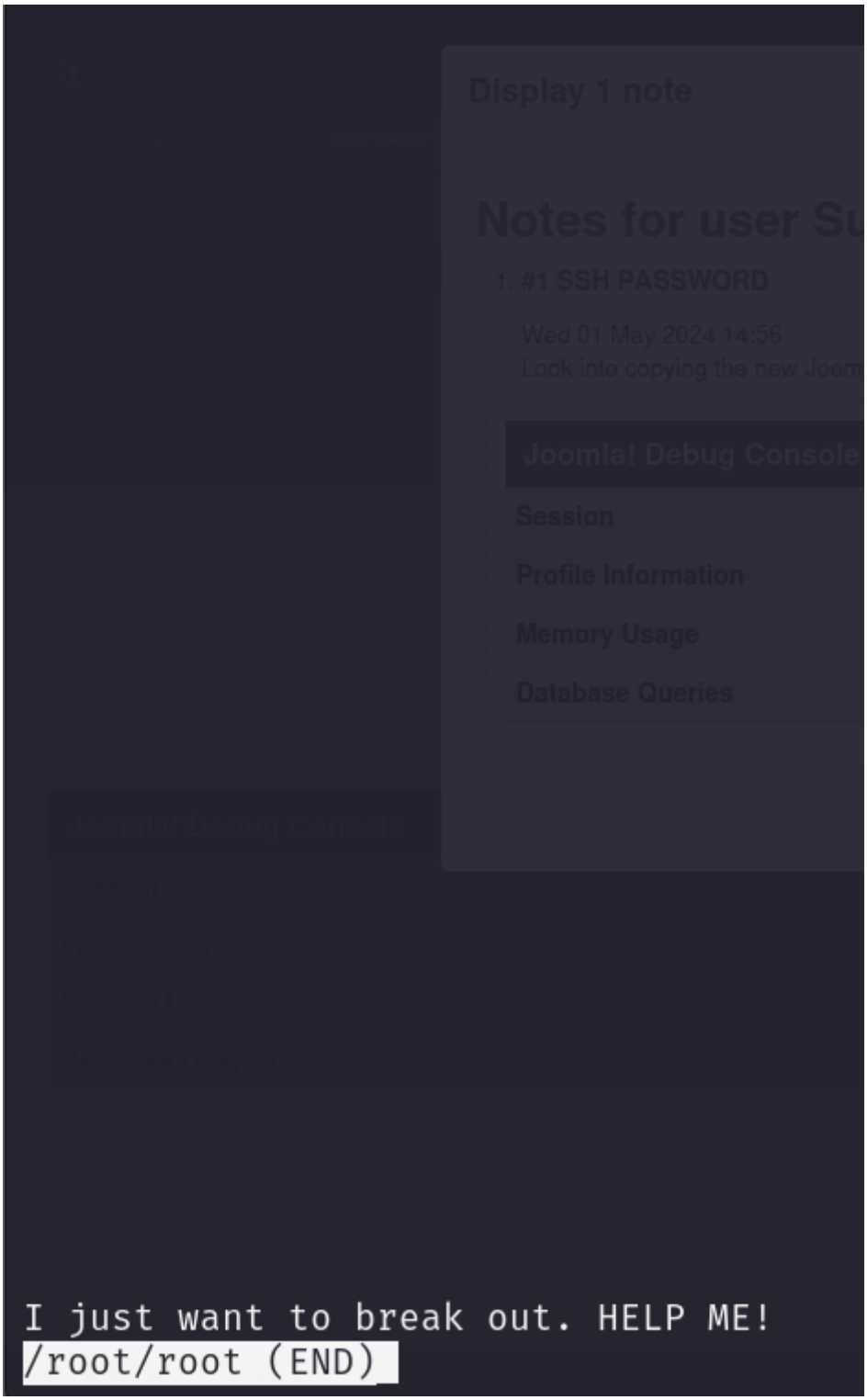


Pressing "3" and inputting our current user returns an error message that we don't have permissions to edit the file "jim" as root.

Checking our sudo privileges we can edit edit the root users "personal file" so as such, we run the script again.



Using "root", we enter an editor which contains the line "I just want to break out. HELP ME!" which is hoped to be a hint that the user is needed to break-out of their text editor.



Through the hacktricks article - https://book.hacktricks.xyz/linux-hardening/privilege-escalation (or GTFOBins) we can look for things related to privilege escalations through the `less` binary and find that we can just use !`shell command` so using `!/bin/bash` should give us root. Using

this payload we get root and find the flag in `/root/flag.txt`!