Walkthrough – Coffee Addicts

Contents

[Host Discovery 2](#_Toc146544041)

# Host Discovery



# Nmap



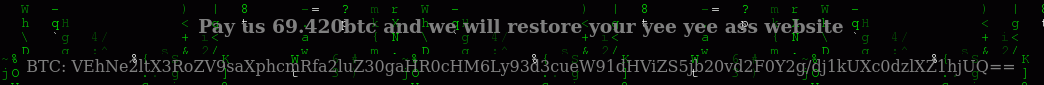
# HTTPie

Before looking at the website, I used this tool to view the message received when I try to visit the website.



There is a message saying I need to add “coffeeaddicts.thm” to my hosts file.

After doing so, I visited the site. There was a message stating the site has been hacked and that a ransom needed to be paid.

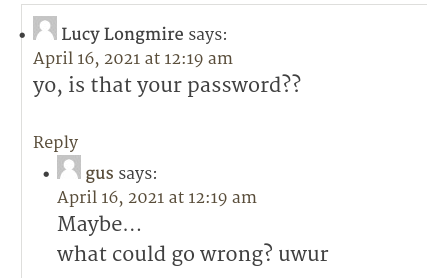


I realised it was base64 so I decoded it. There was a video url. It was a rick roll…

# Nikto

A word press framework has been found.

# Viewing Website

After look at the website for quite some time I realised that there are posts ‘/?p=X’, where x is a number. I looked through at didn’t find much. I then went back and found that ‘/?p=9’ contains two comments.

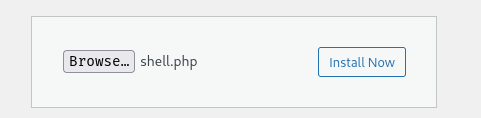
Then under the image a caption was set.



I tried this combination as credentials and it worked. Credentials – gus:gusineedyouback

The url I login to was /wordpress/wp-login.php.

# Exploitation

Now that I am inside the dashboard, I can try to upload a reverse shell. I first navigated to the plugins section and uploaded my php shell.

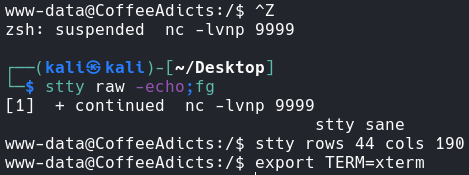
Then after uploading it, I spent time trying to find out where it was hidden. However I couldn’t find the resting place for this file. I then downloaded the “Thumbnail slider” extension for wordpress and then I found it.

<http://coffeeaddicts.thm/wordpress/wp-content/uploads/2023/10/shell.php>

The step was to download the file online, then install the plugin, then navigate to media, then view my php file.

# Escalation

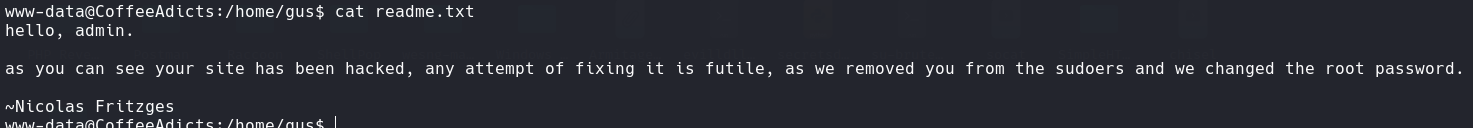
## Upgrade the shell



Now I have a full terminal.

# Flag 1



In Gus’s home directory I found flag 1. 

Now I found another User called ‘BadByte, which is the hacking group which hacked the site.

I found that they have allowed read access to the others group. This allowed me to view the id\_rsa for the ssh key. I can now attempt to crack the password.

# SSH2John



# John



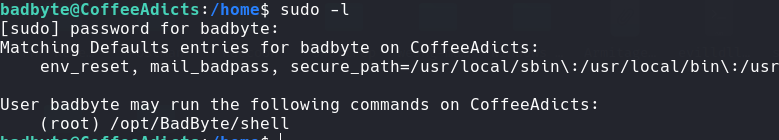
However I cannot ssh into the account.

I found a shell file written in C++.

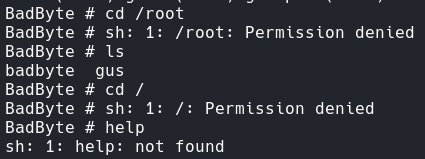
Running it just changes the output of the terminal. I now spent a couple of more minutes trying to figure it out, however I finally retried the ssh.

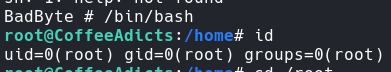
Unexpectedly, the password for the SSH account is the same as the password cracked previously.

The files discovered prior are actually an escalation for the hacking group.



Since I can now run the shell binary discovered earlier, AS ROOT, I will have a root shell.

I am now root! However, I do not have any commands to use, since I continuously get errors.

To me this looks like a restricted shell. I will need to break out of this if I want to get into the root directory.

Now I have emerged from the restrictions I can enter the root directory.

# Flag 2

