ENPM685 Final Project Report

Dheepshika Raghunathan

# Objective

The objective of this report is to detail the procedure that I used to find the 6 flags in the ENPM685 Pictures, Inc. Systems. ENPM685 Pictures, Inc. has 2 systems, one is a Linux server and the other is the Windows desktop of the CEO. The CEO is Bob Dobbs and has Administrator access to the desktop.

# Contents

[1. Objective 2](#_Toc514114177)

[2. Contents 2](#_Toc514114178)

[3. Procedure to find Flag 1 3](#_Toc514114179)

[4. Procedure to find Flag 2 7](#_Toc514114180)

[5. Procedure to find Flag 3 11](#_Toc514114181)

[6. Procedure to find Flag 4 14](#_Toc514114182)

[7. Procedure to find Flag 5 18](#_Toc514114183)

[8. Procedure to find Flag 6 19](#_Toc514114184)

[9. Flags 21](#_Toc514114185)

[9.1. Flag 1 21](#_Toc514114186)

[9.2. Flag 2 21](#_Toc514114187)

[9.3. Flag 3 22](#_Toc514114188)

[9.4. Flag 4 22](#_Toc514114189)

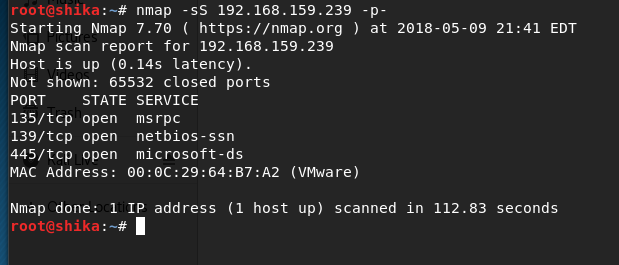
[9.5. Flag 5 22](#_Toc514114190)

[9.6. Flag 6 23](#_Toc514114191)

[10. Relevant Files 23](#_Toc514114192)

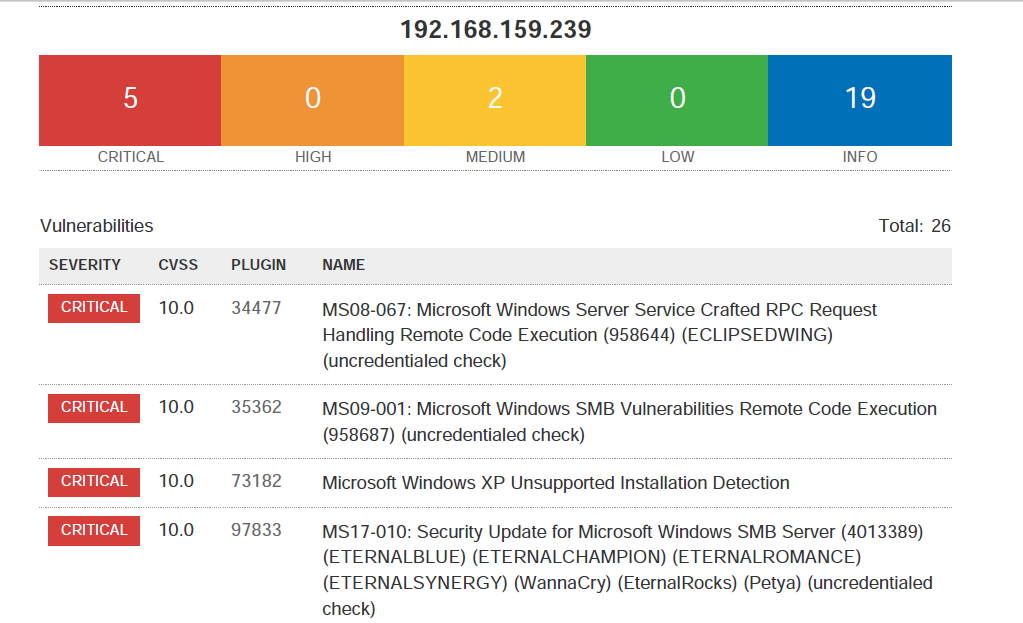
# Procedure to find Flag 1

I found Flag 1 in the Windows CEO desktop. To get into the system, I first had to find all the open ports in the CEO system. To do this I ran an Nmap scan as below.

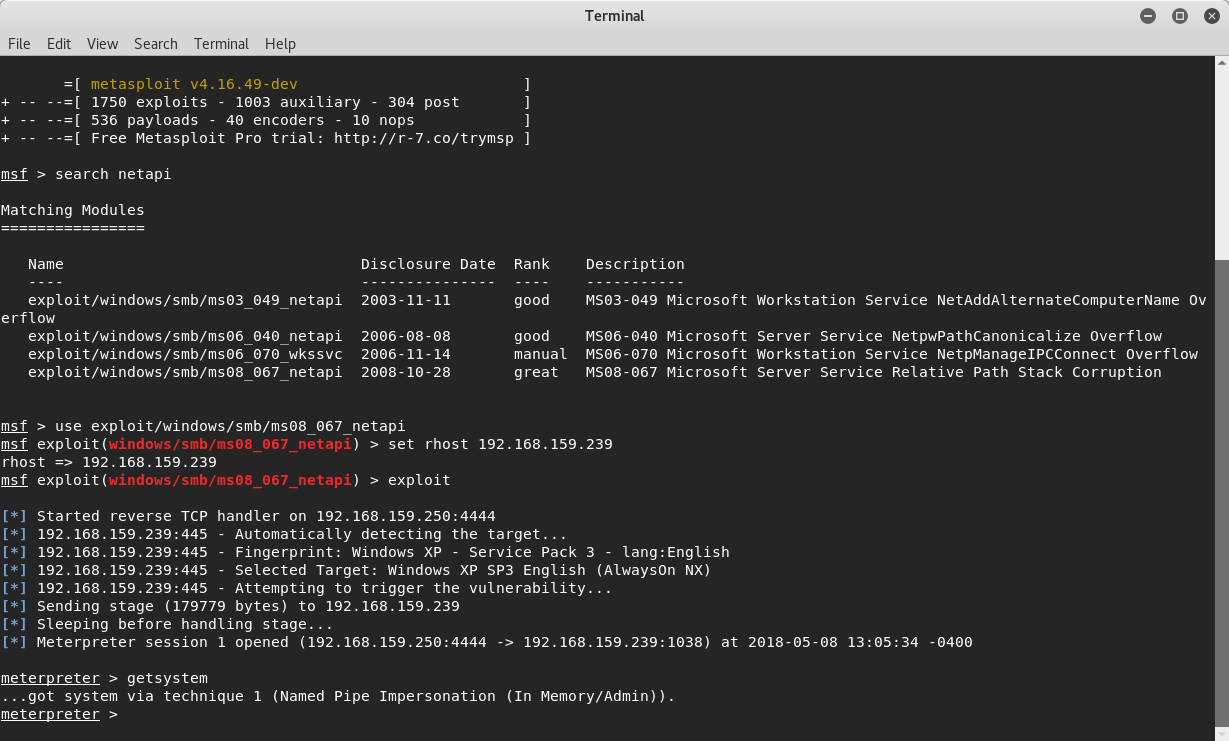


This scan indicates that only ports 135, 139 and 445 are open. To find further vulnerabilities, I ran a NESSUS scan on the CEO desktop system.

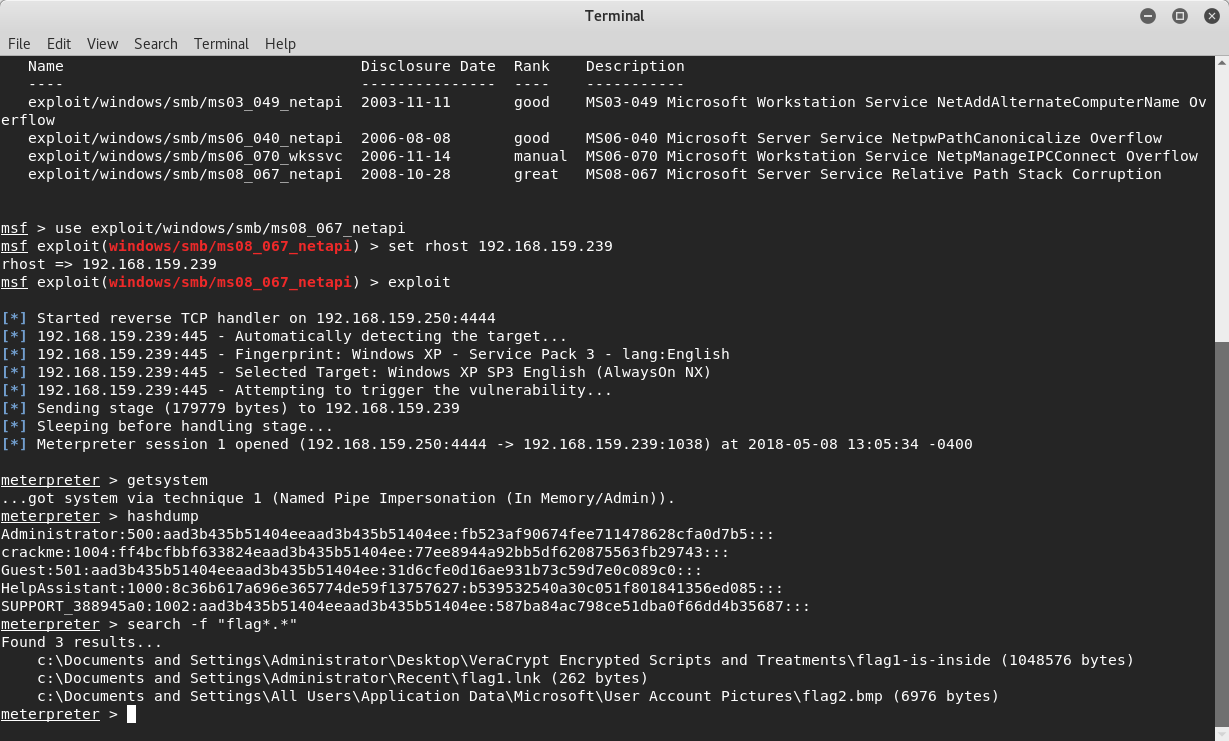
The scan found the below vulnerabilities in the CEO desktop.



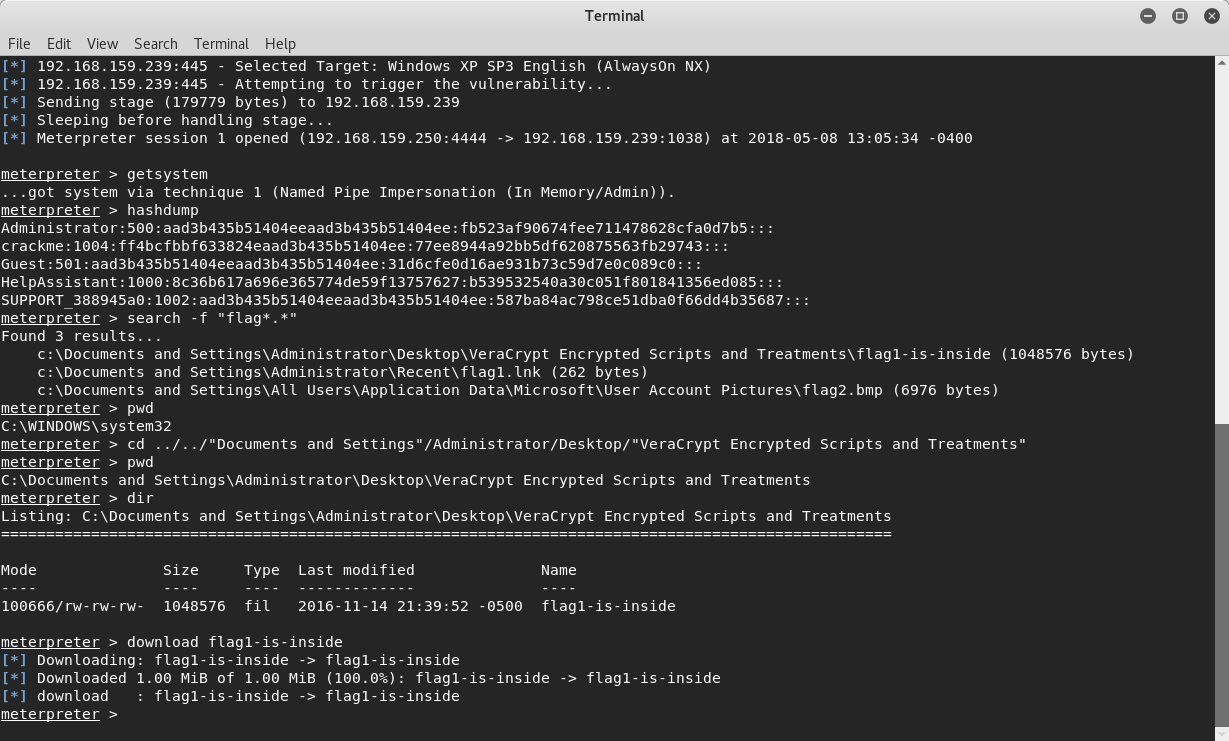
To exploit these vulnerabilities, I used Metasploit. After a few trials I found that MS08-067 was exploitable. I exploited the same as below and was able to get a shell in the CEO desktop machine.



I then searched this system for files with the word “flag” in their name. The search resulted in 3 results of which one was Flag 1.

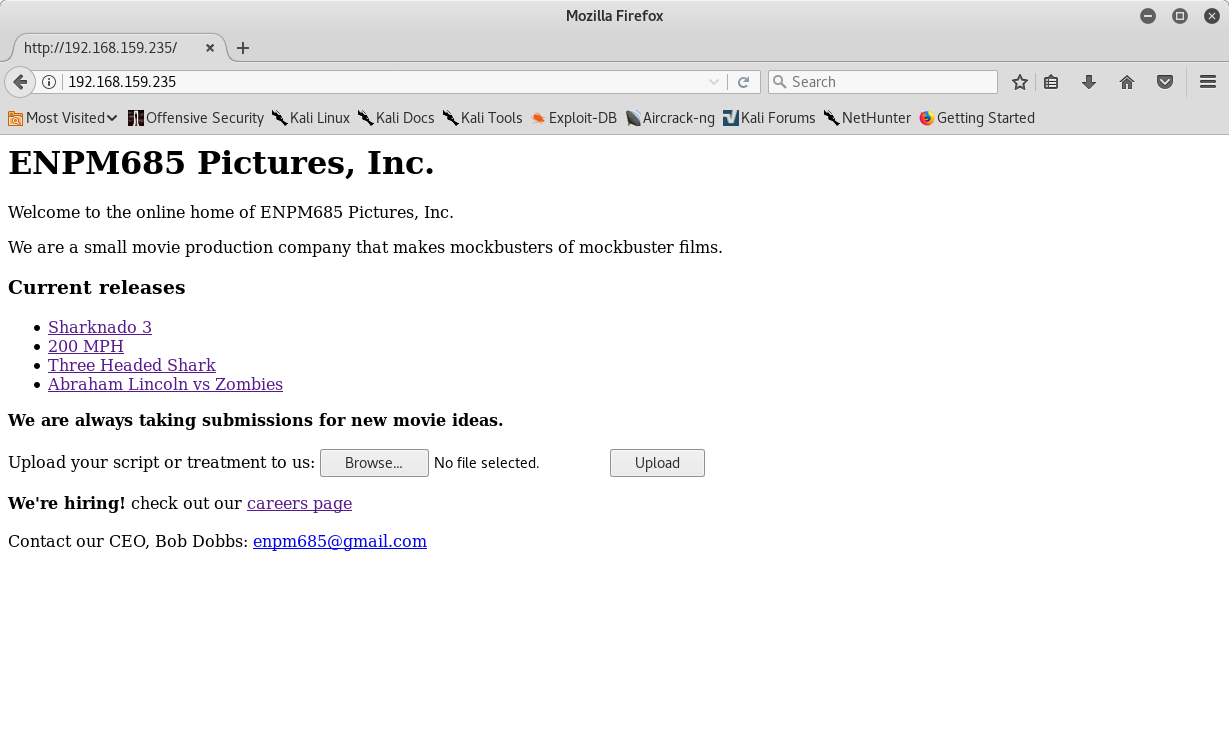


This indicates that Flag1 is inside a VeraCrypt Encrypted folder. I then proceeded to download the folder along with its contents.

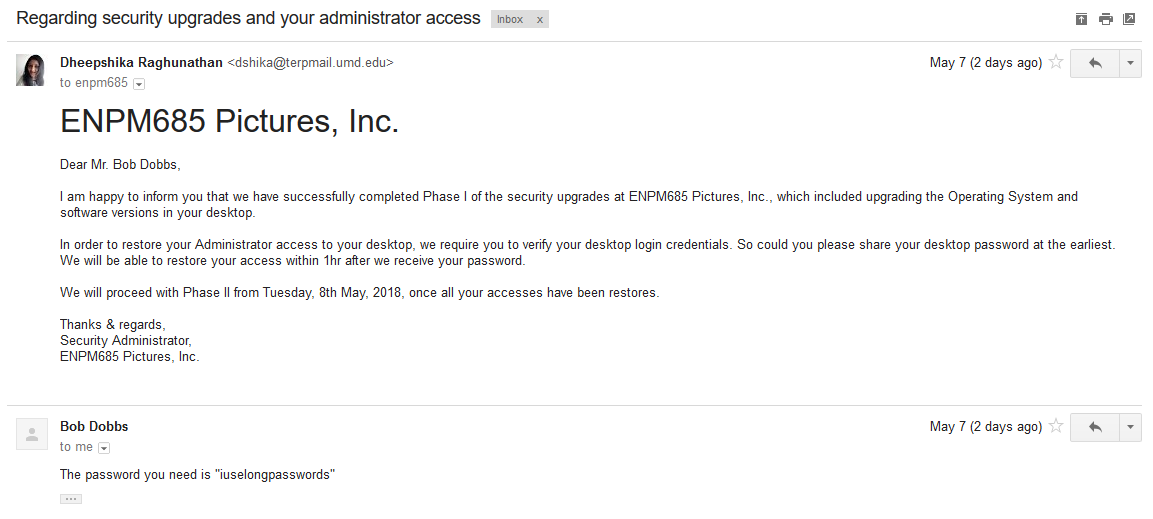


A password is required to open this folder.

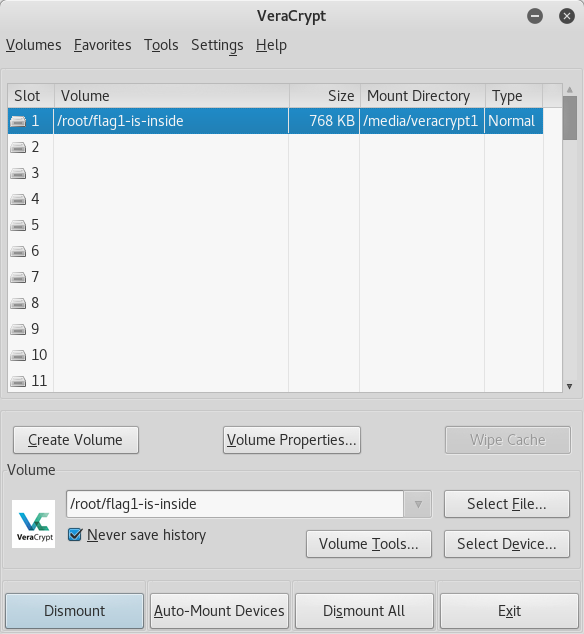
When I ran the Linux machine, I found a web page being hosted which contained the email ID of the CEO.

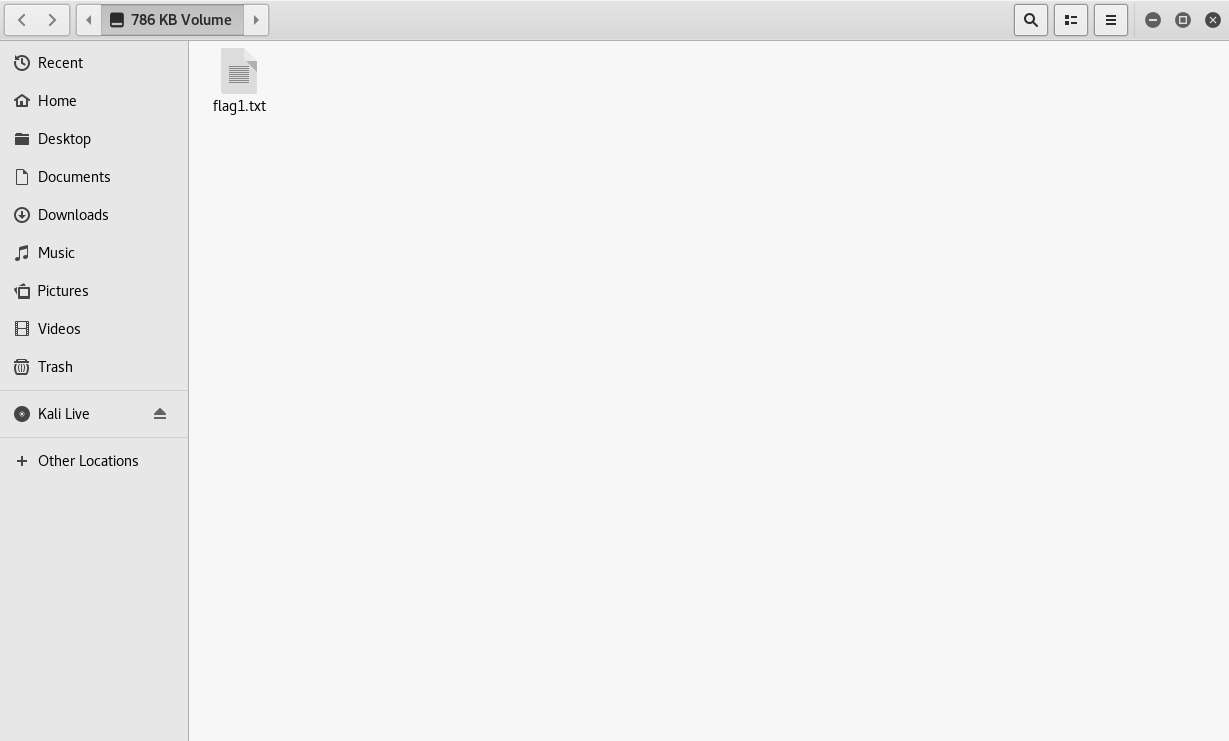


I then sent a phishing email to the CEO as below. To this the CEO replied with the required password.



Using this password, I opened the folder and found a file with the flag inside.

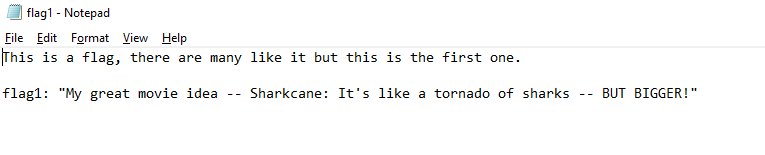




I found flag1 inside the below file named flag1.

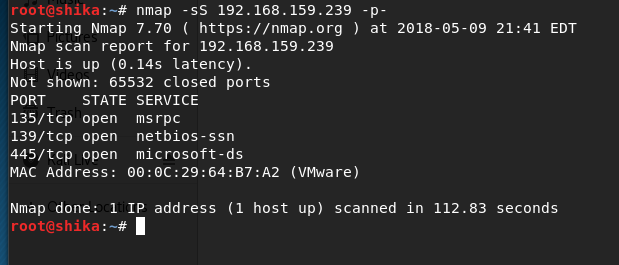


The below are the contents of flag 1,

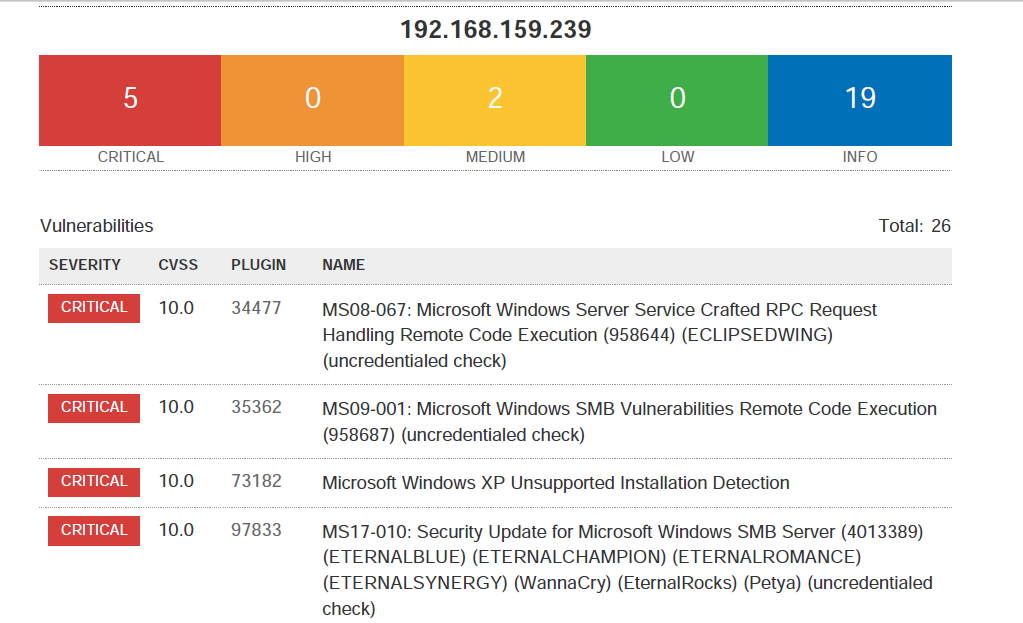


# Procedure to find Flag 2

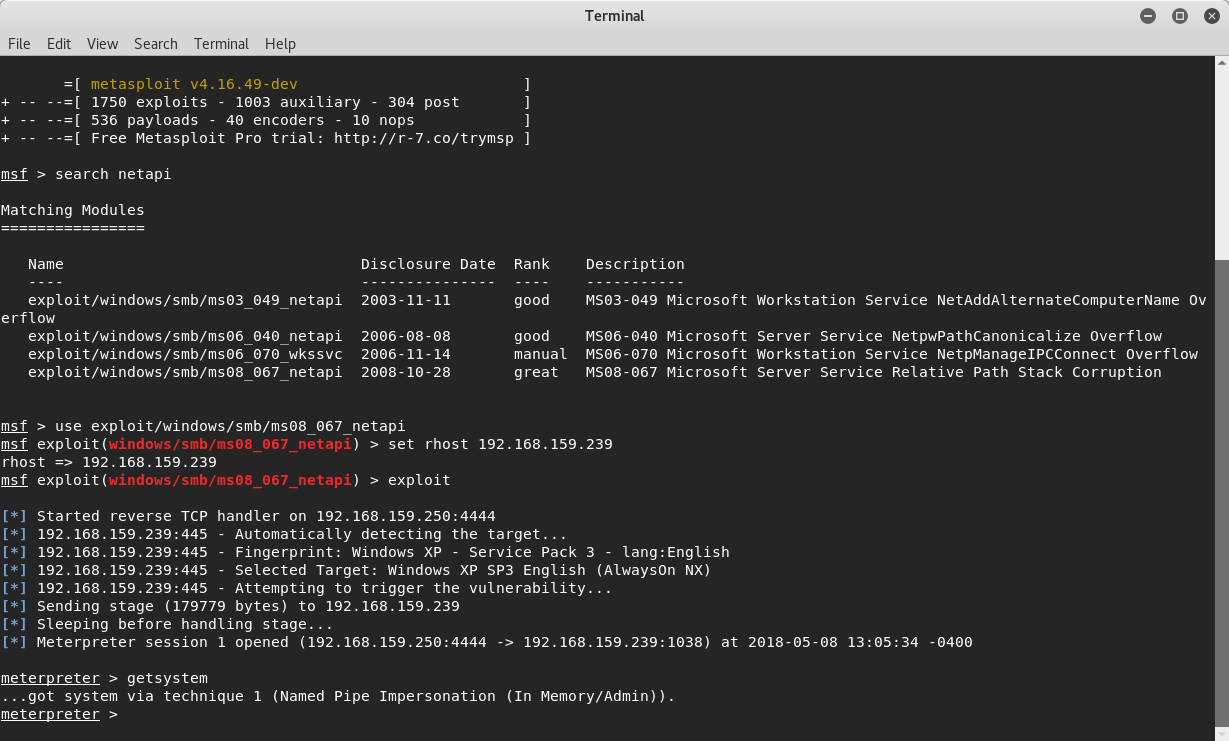
I searched for open ports in the CEO desktop machine and found that the below ports were open.



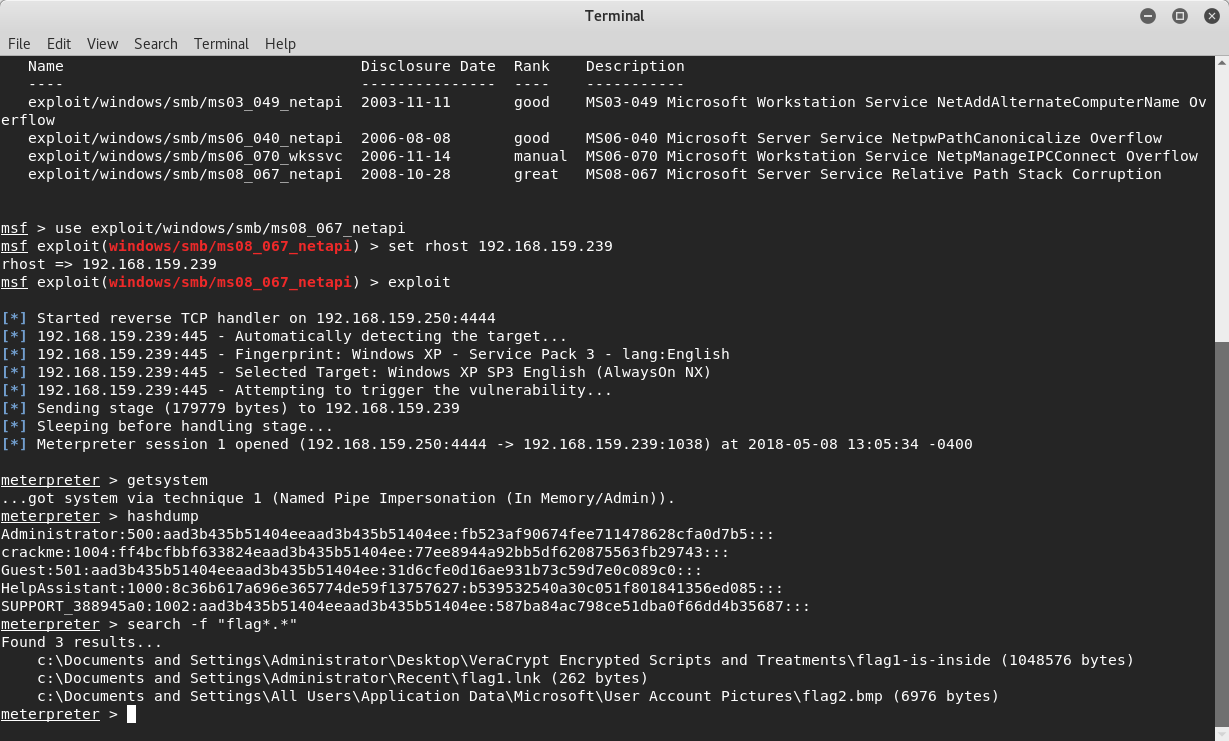
I used the same NESSUS scan as above to find the vulnerabilities in the CEO desktop. The scan resulted in the below vulnerabilities.



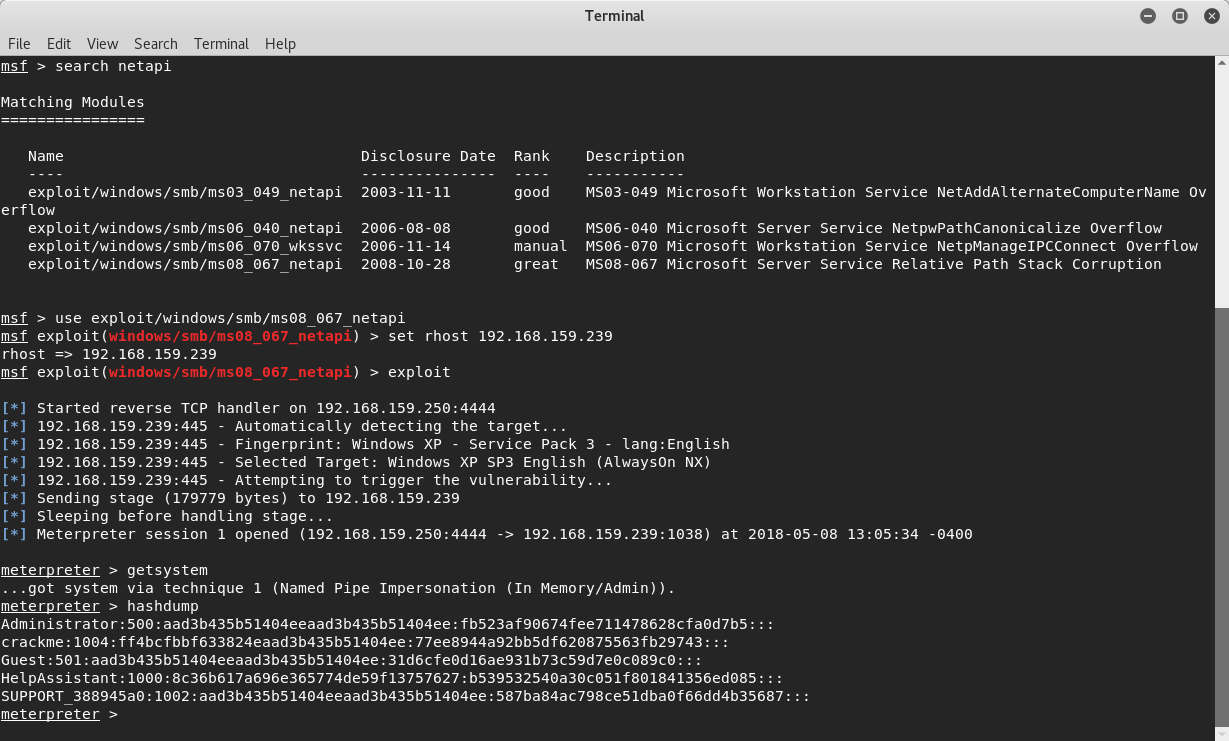
I then used the MS08-067vulnerability to exploit the CEO desktop system using Metasploit and was able to spawn a shell.



I then searched for files with the name “flag” in them. This resulted in 2 results with flag2.

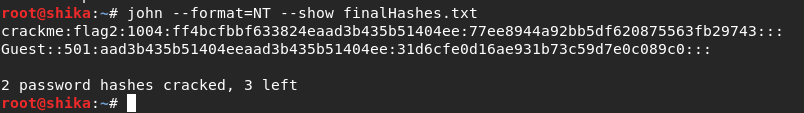


Here we find that one of the files is an image but is in the User Account Pictures folder. This means that flag2 might be associated with a user. So I then proceeded to do a hashdump of all the users in this system.

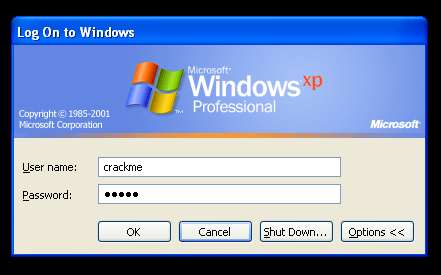


I then used John the Ripper to crack the passwords of these users.

This showed that the flag 2 was the password for the user crackme.



To log in as this user, I used Ctrl + Alt + Del on the CEO desktop. Here I entered crackme and flag2 as the credentials.



It asked me to change the password for crackme.

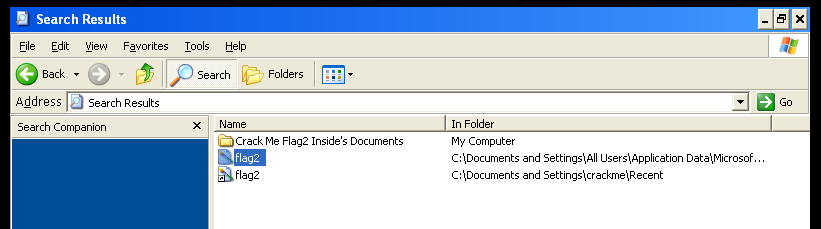


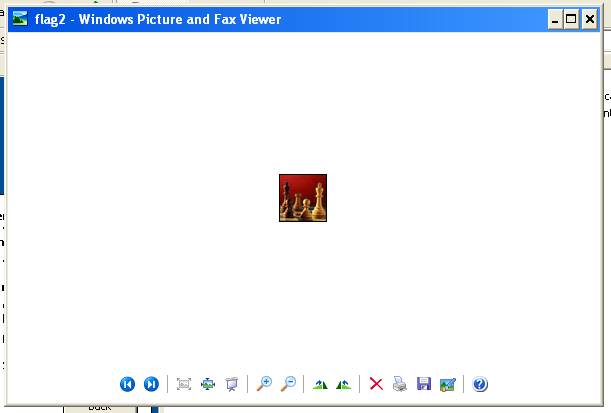
After changing the password, I was able to log in.



The desktop was displayed.

I then searched for the flag and found that it was the same image that I had found earlier in the search using metapreter.

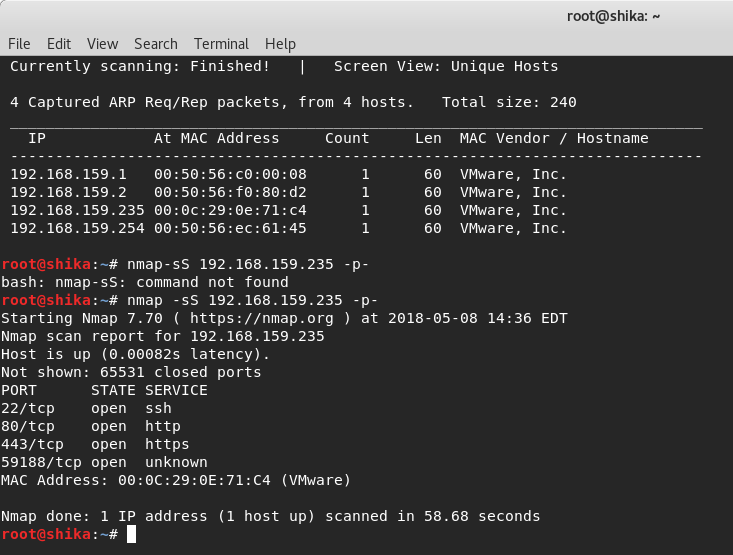




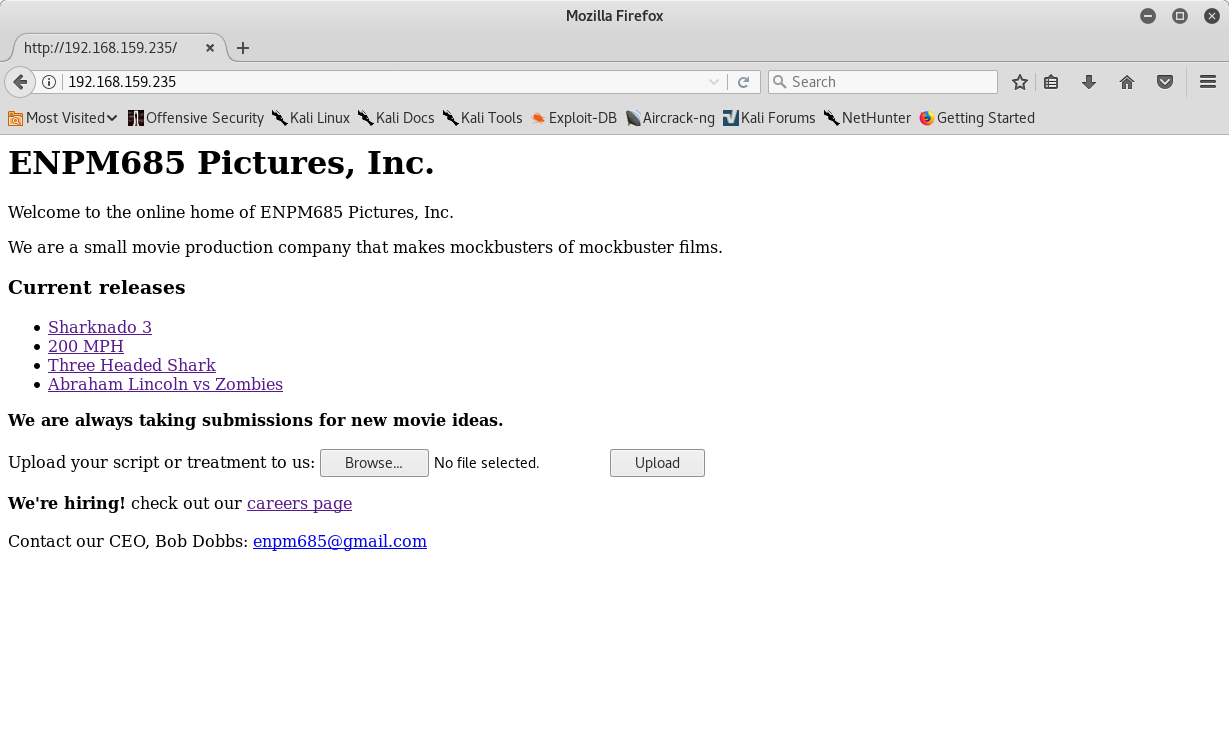
This would imply that user crackme whose password was flag2 and image was the above is Flag 2.

# Procedure to find Flag 3

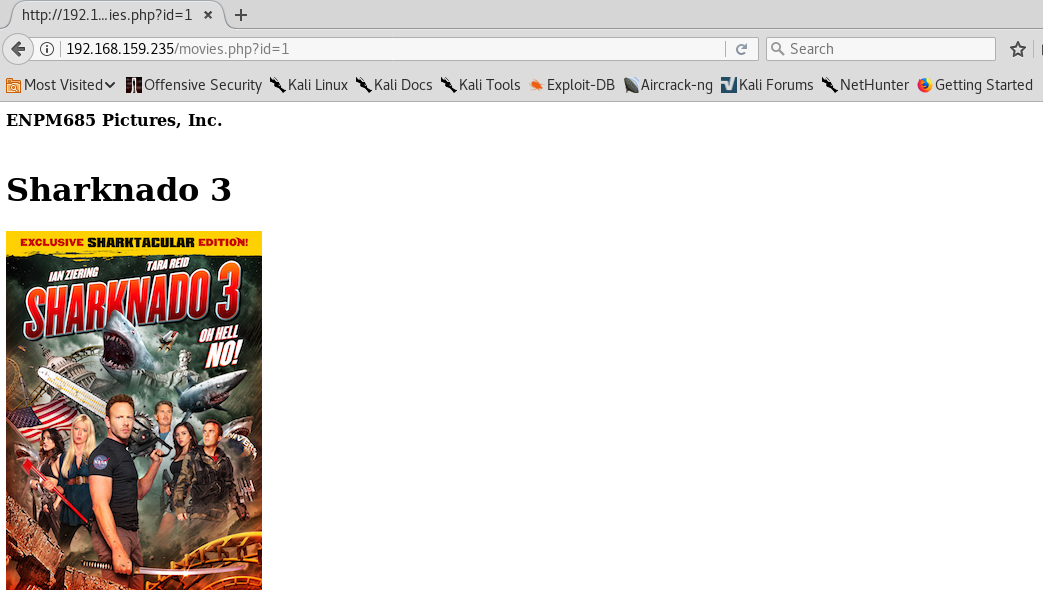
I first started with running an Nmap scan on the Linux system.



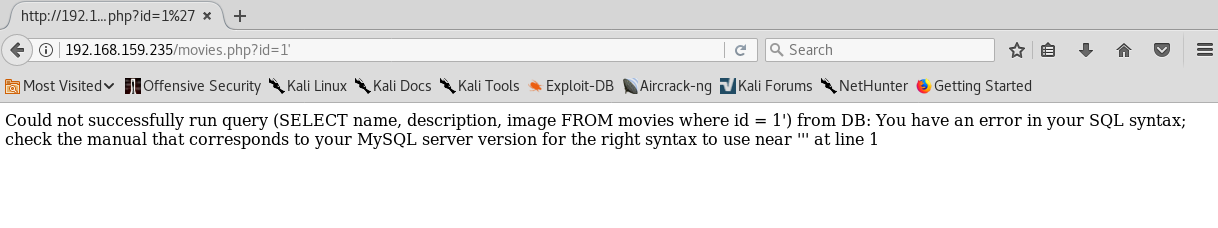
I found that ports 80 and 443 were open. This might indicate that a web application is running in the Linux machine. I then tried to access this web application using the Linux machine’s IP address in a browser. I found that the ENPM685 Pictures, Inc. website was running here.



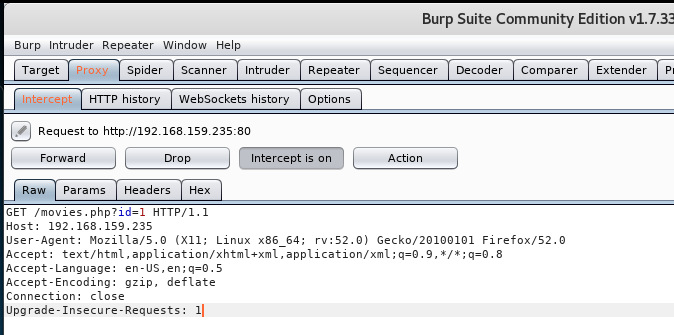
When I clicked on the current releases link, I found requests being sent with the **id** parameter.



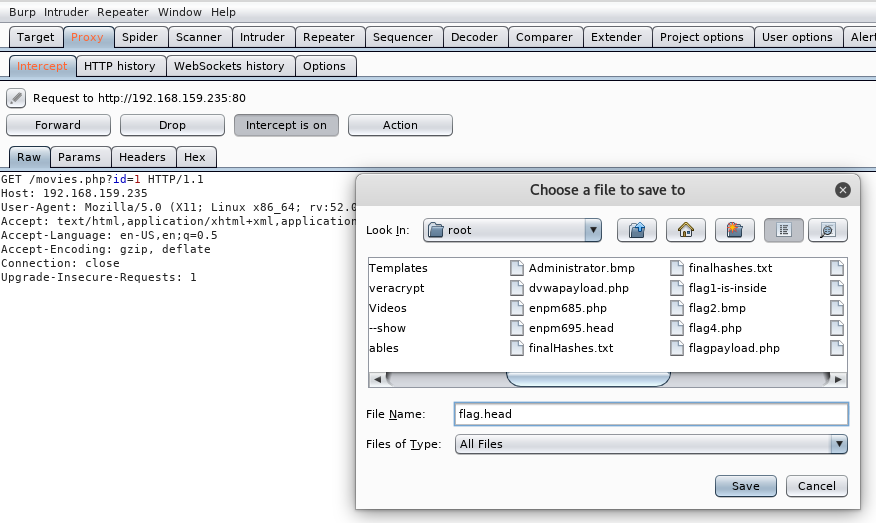
I then tried to put an apostrophe (**‘**) at the end of the request to check if it was possible to perform SQL injection on this request. There result was that the query that was being performed was displayed in the error message.



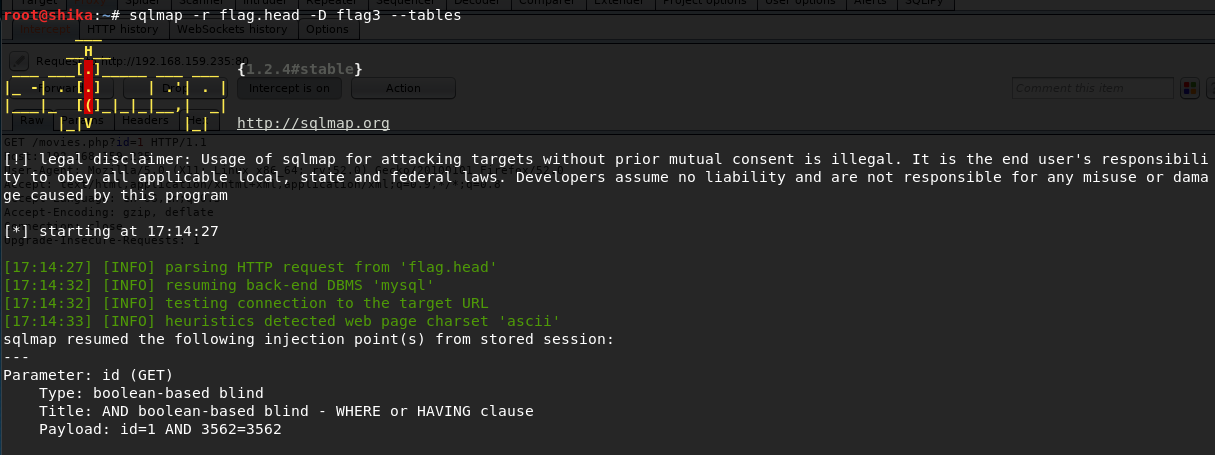
I then proceeded with grabbing the header details to perform SQL injection using SQLMap. I used Burpsuite to grab the header details.

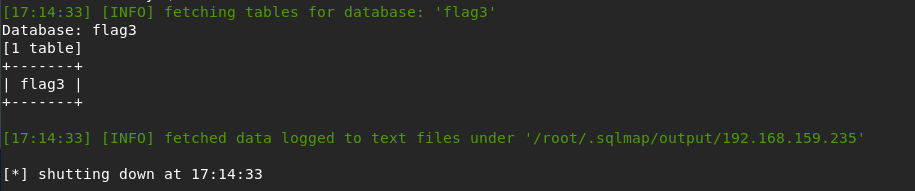


I saved the header details to a file.

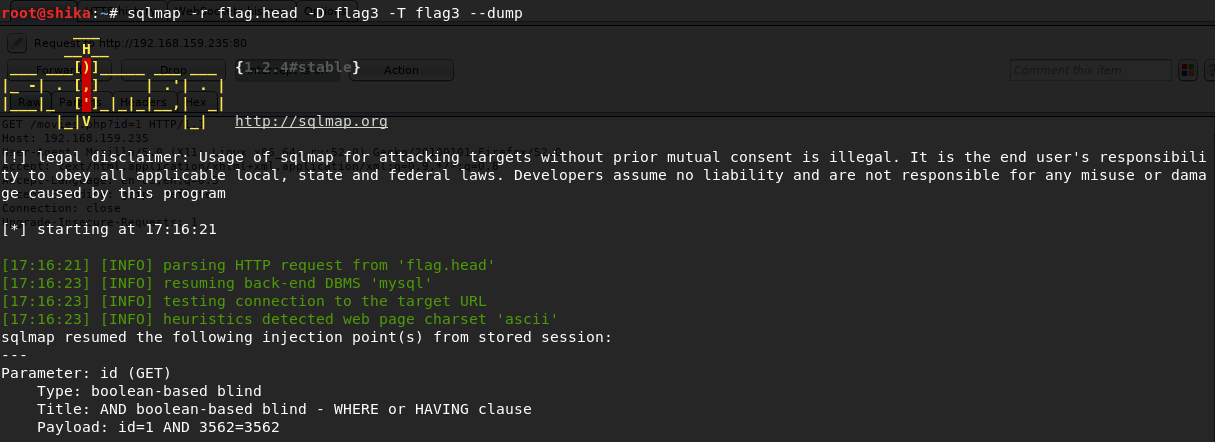


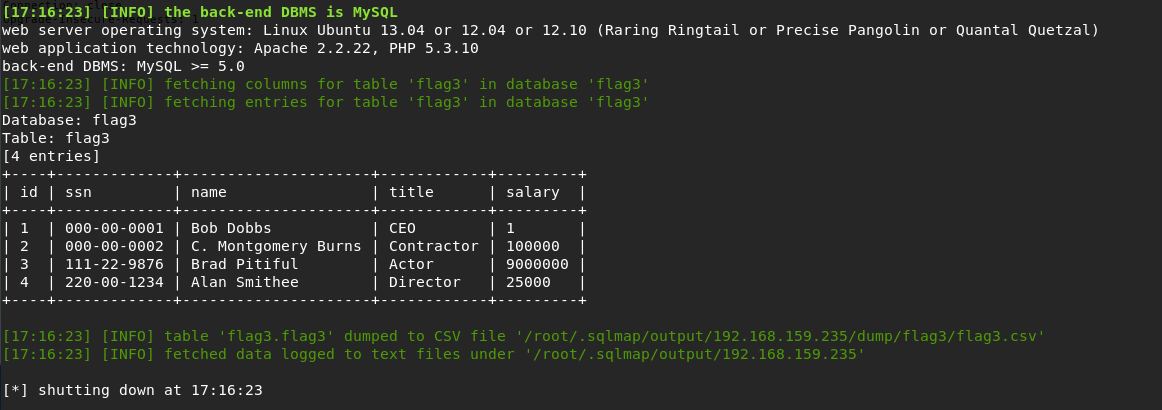
I then used this header file as input when performing the SQL injection attack.





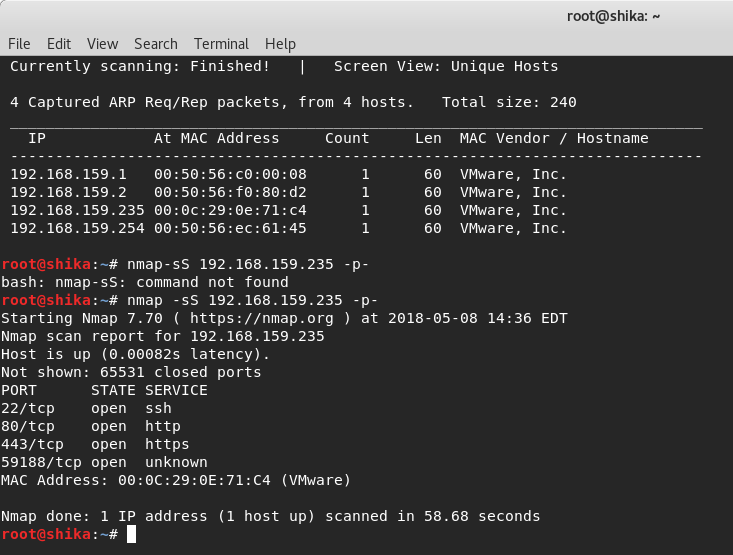
In this I found a table called flag3. I dumped the contents of the table flag3 to find the Flag 3.



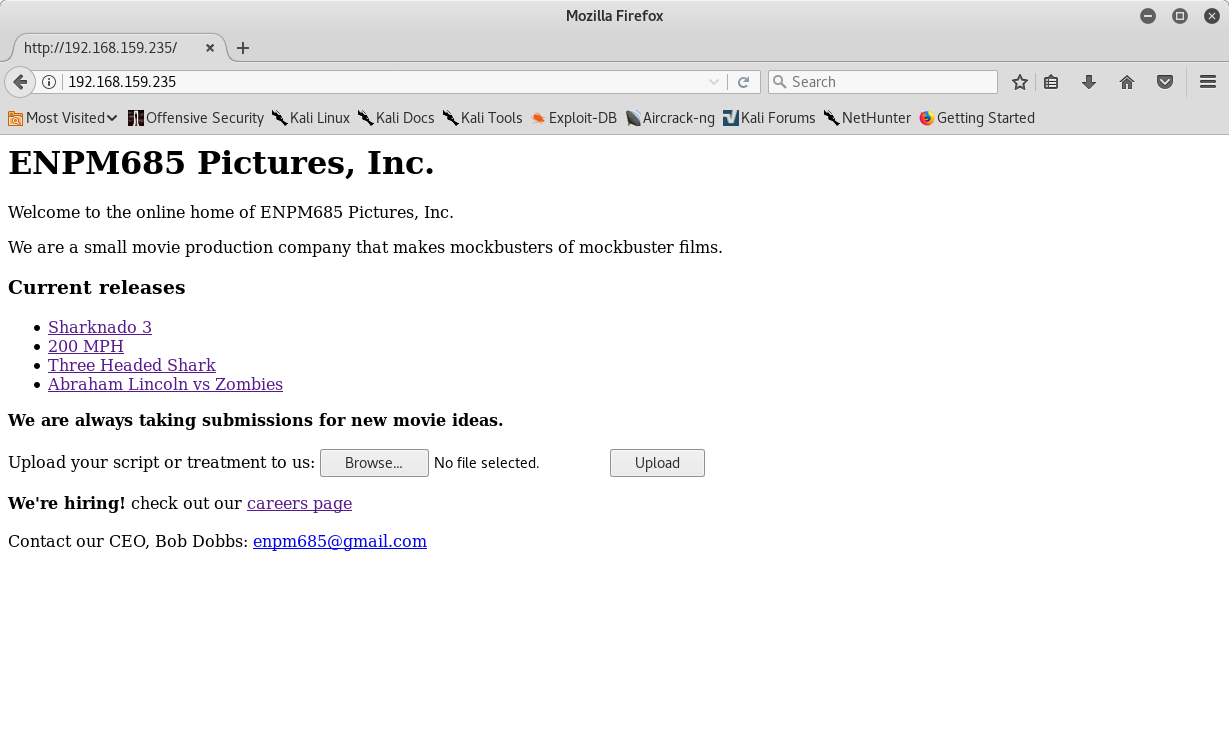


# Procedure to find Flag 4

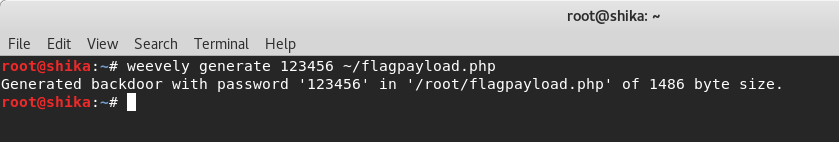
When I ran the Nmap scan on the Linux machine, I found that ports 80 and 443 were open.



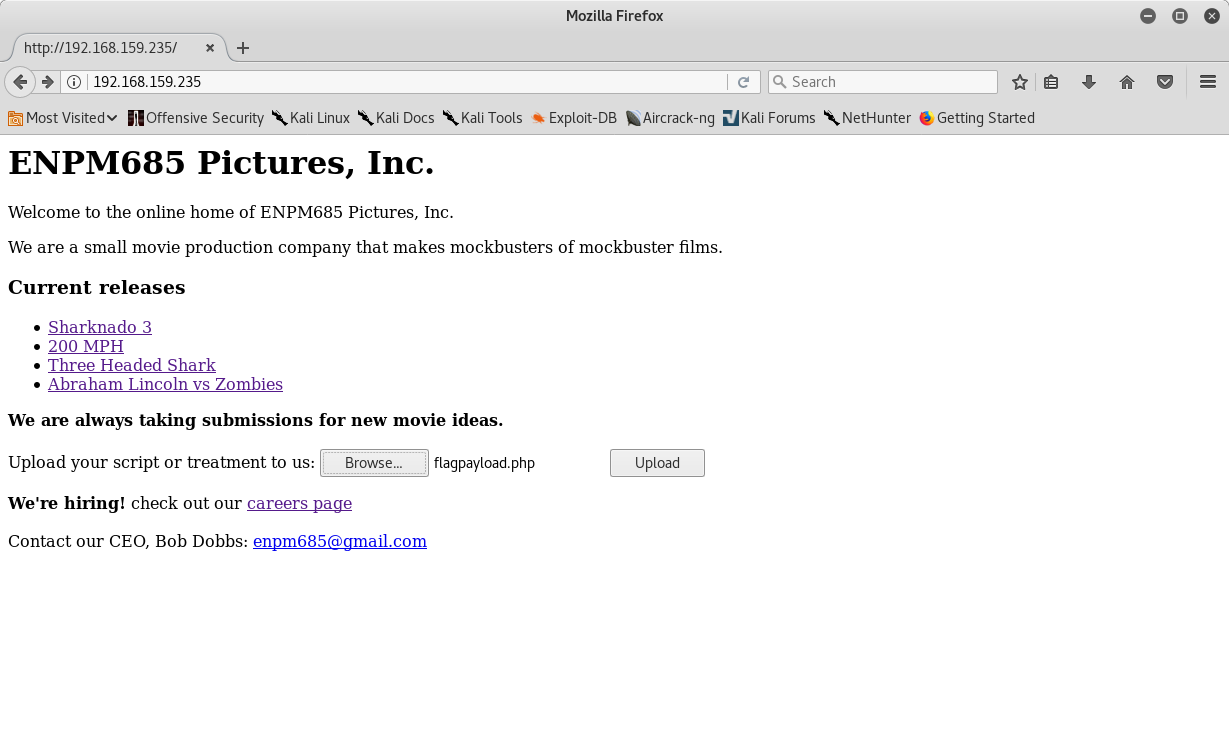
Since these ports are open, it is possible that a web application is running in this machine. So I tried to access this application using the Linux machine’s IP address in the browser. This showed that the website of ENPM685 Pictures, Inc. was running on this machine.



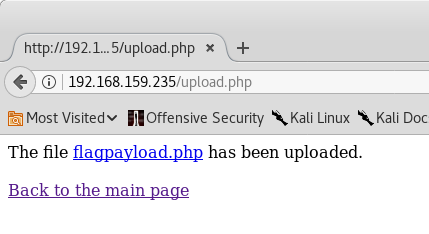
This page contains a file upload field that might have a file upload vulnerability. It might be possible to upload a backdoor through this field and gain access to the file system. So I created a Weevely backdoor.

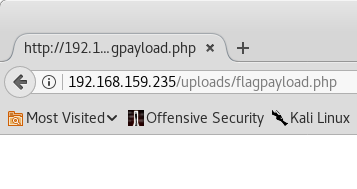


I then uploaded this payload in the above field.

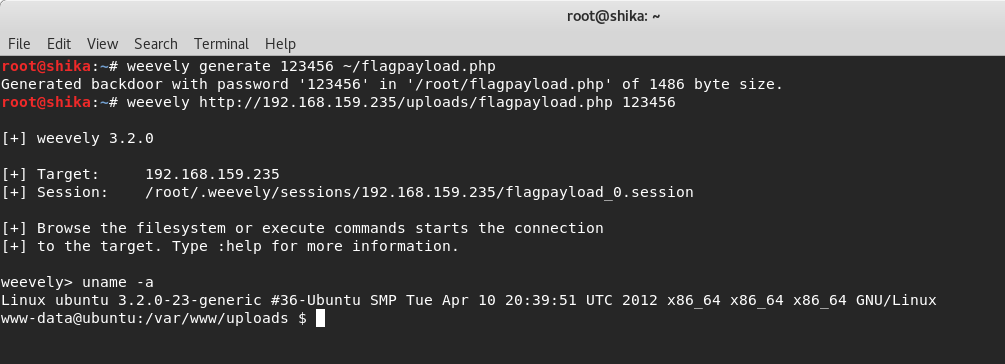


The file was uploaded successfully and was accessible through the link provided.

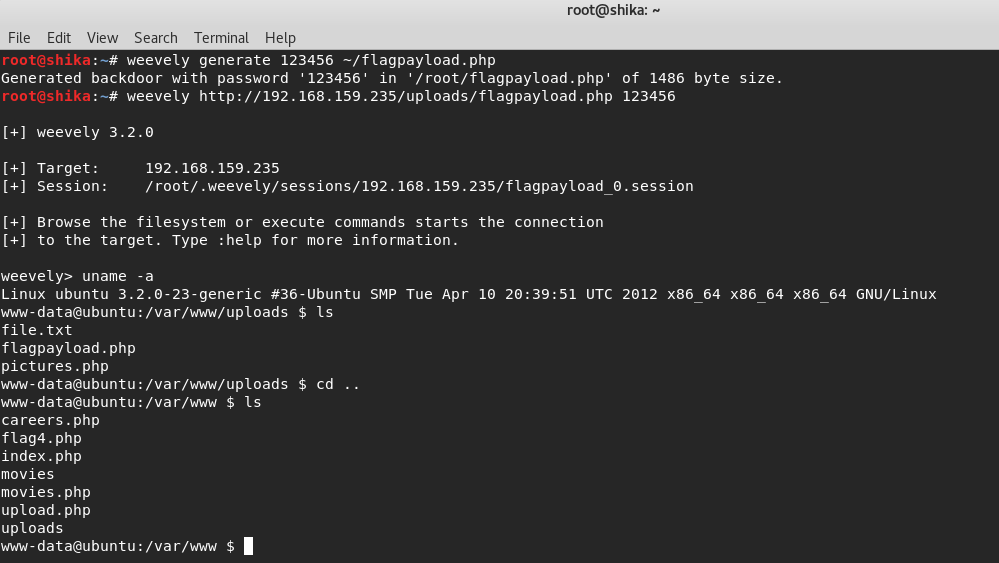




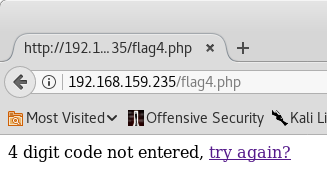
I then tried to access the backdoor file that I had uploaded in this location and get the shell.



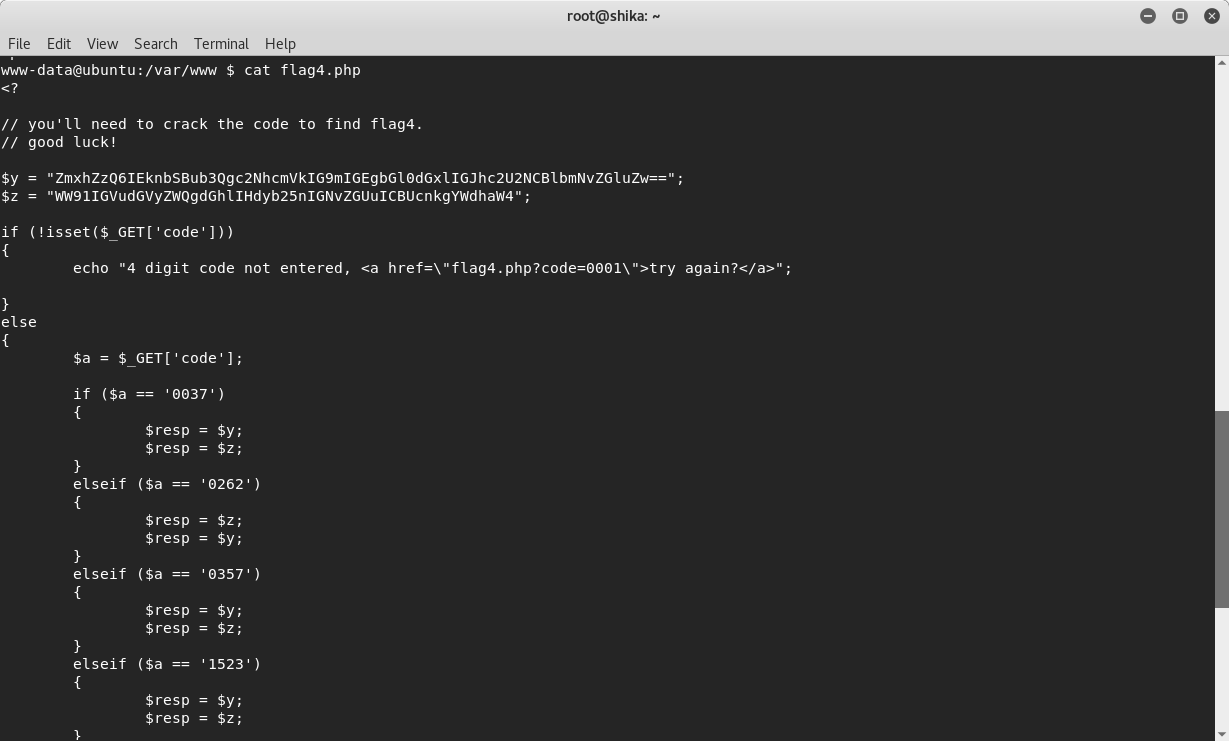
When I tried to list all the files in this directory, I found the flag4 file.



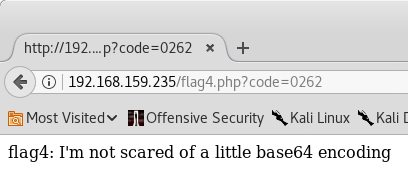
This was a PHP file, so I tried to access this file from the browser.



I found that this file requires a specific parameter (a 4 digit code) in the request to print the flag details. So I went back to analyze the contents of the file.



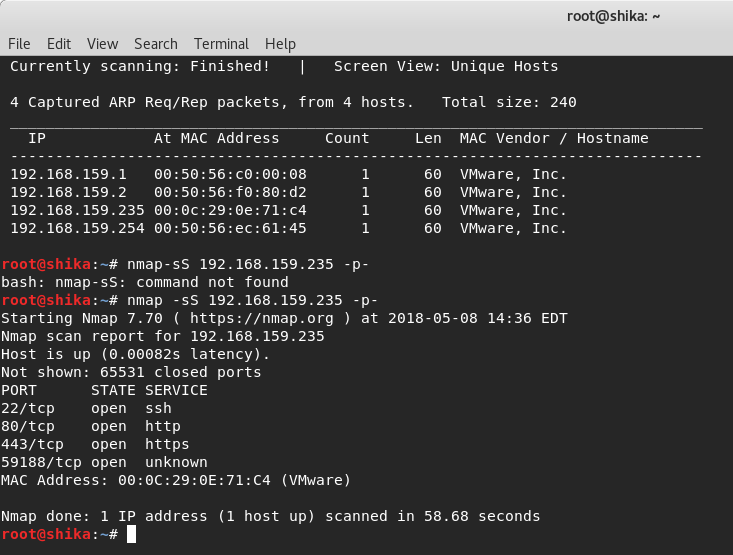
Here I found that only for code **0262** there was a change in the value of the variable. So I decided to try that as the input parameter.



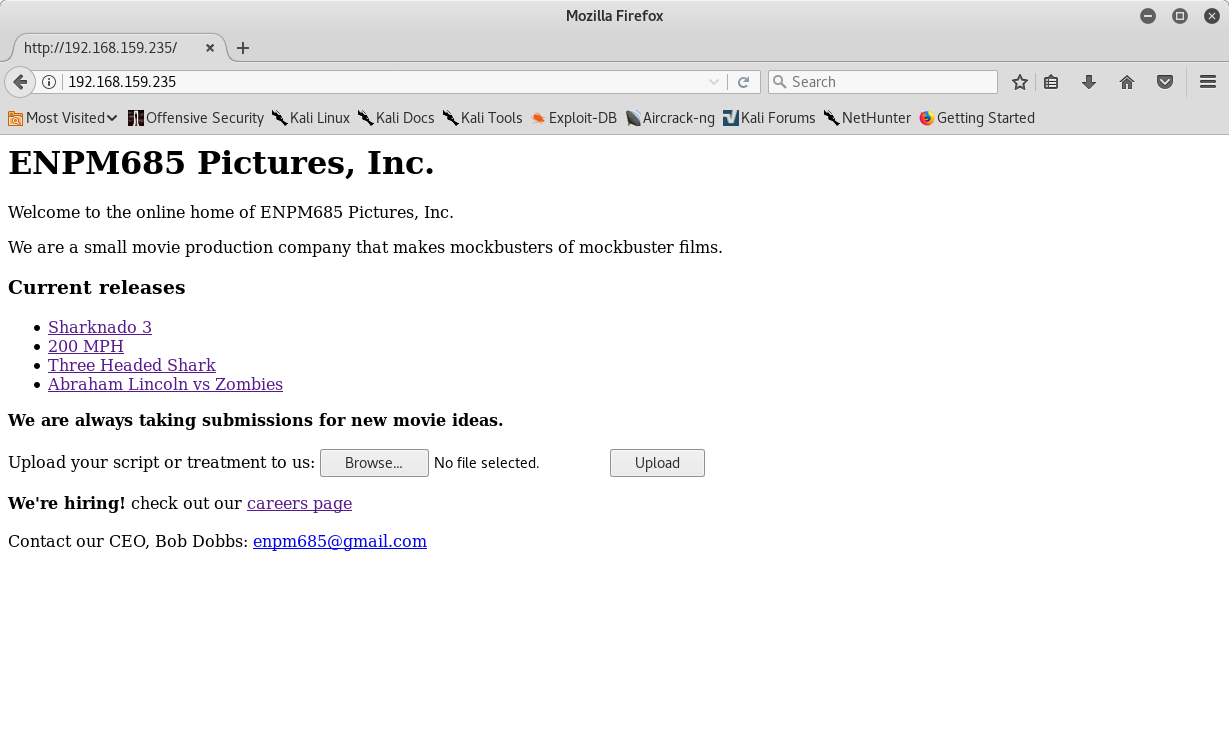
This revealed the Flag 4 contents as above.

# Procedure to find Flag 5

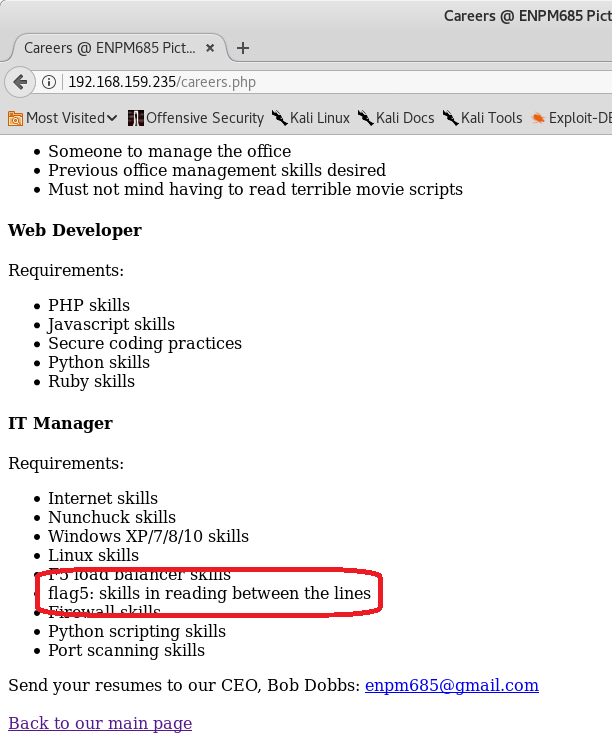
When I ran the Nmap scan on the Linux machine, I found that ports 80 and 443 were open.



Since these ports are open, it is possible that a web application is running in this machine. So I tried to access this application using the Linux machine’s IP address in the browser. This showed that the website of ENPM685 Pictures, Inc. was running on this machine.

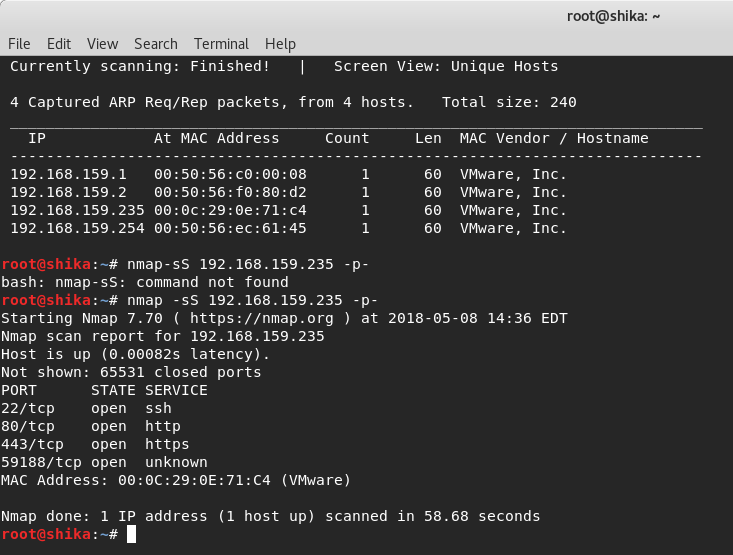


When I clicked on the careers page link, I found that Flag 5 was available in this page.

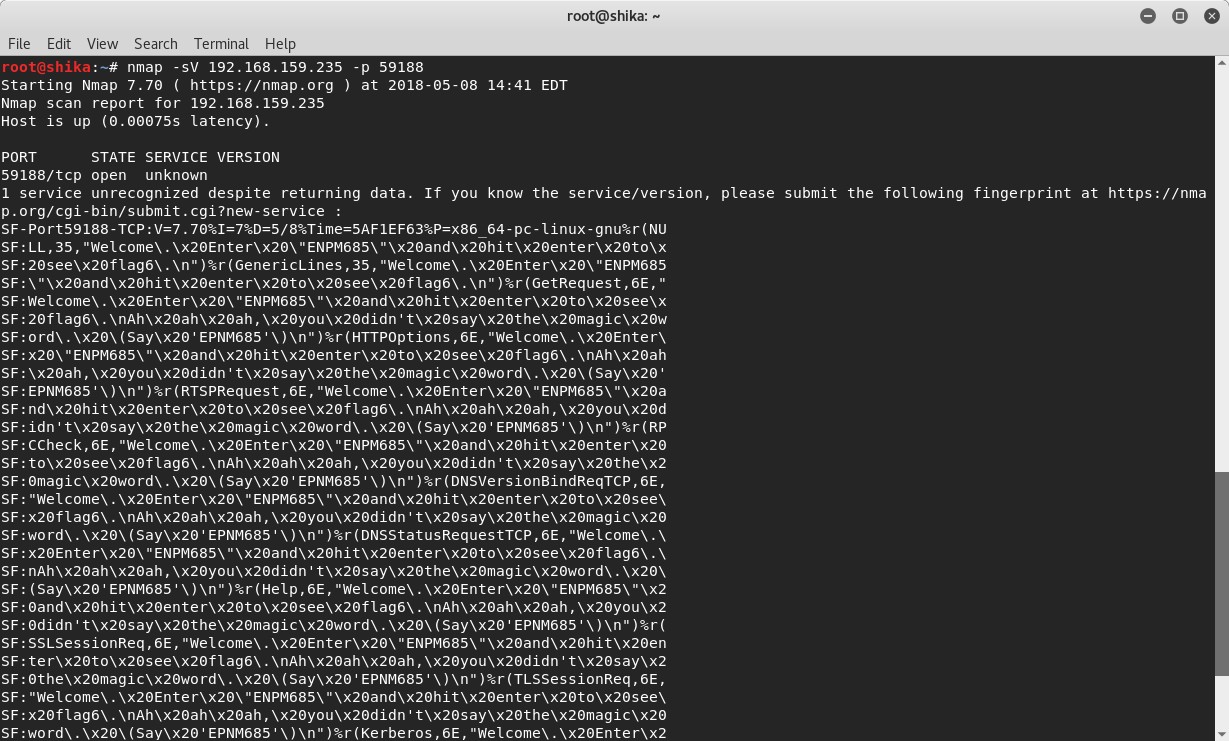


# Procedure to find Flag 6

I ran the Nmap scan for all the ports to find all the ports that were open in the Linux machine.

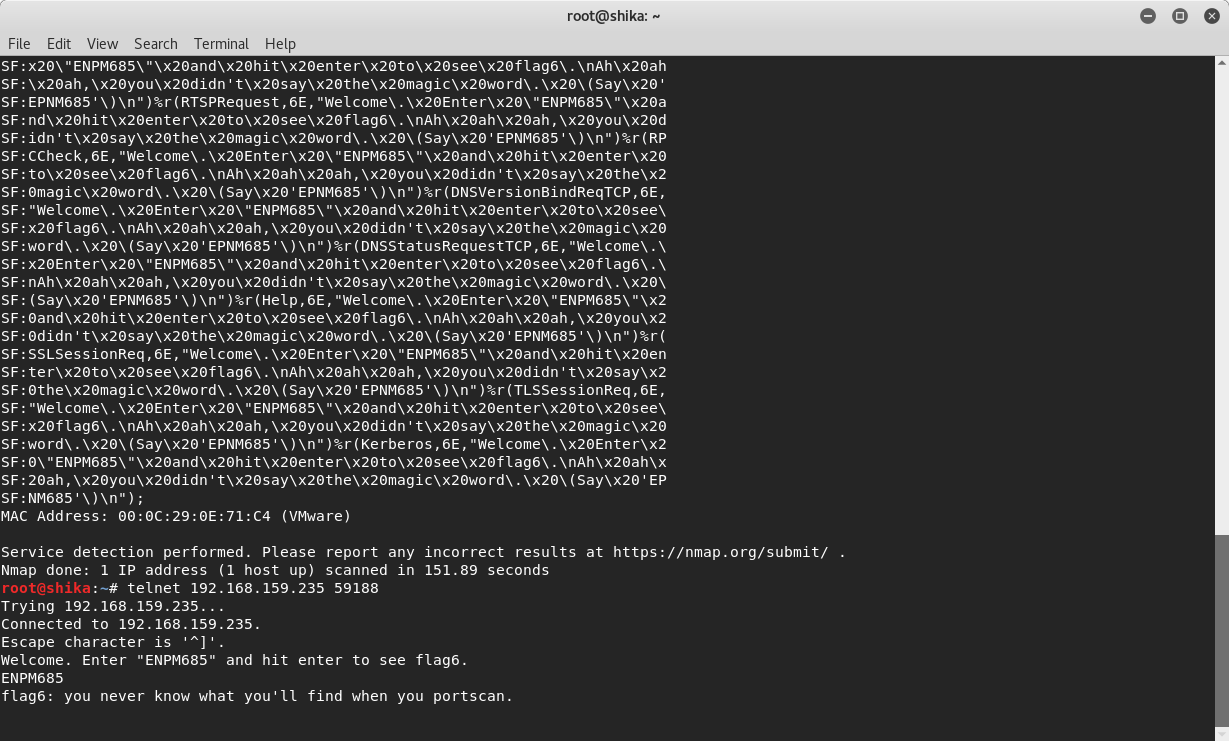


I found that the port **59188** was running an unknown service. I then tried to run a version scan of that port to find further details about the service running in this port.



The version scan revealed unrecognisable data. I found some data in the version scan that says ‘flag6’ and ‘Say ENPM685’.

I then tried to telnet to this port. The connection was established and when I entered **ENPM685** and pressed enter, Flag 6 was revealed as below.

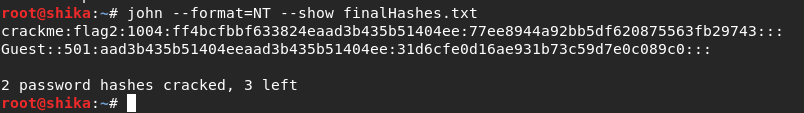


# Flags

## Flag 1

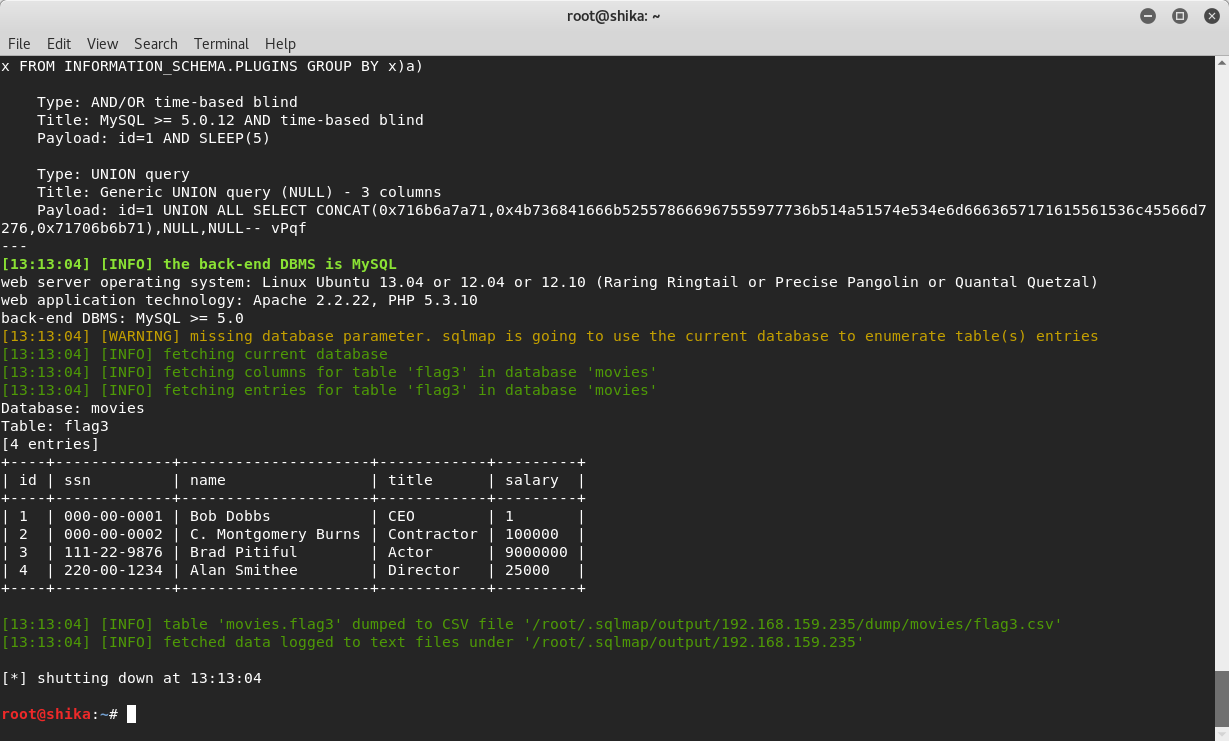


## Flag 2

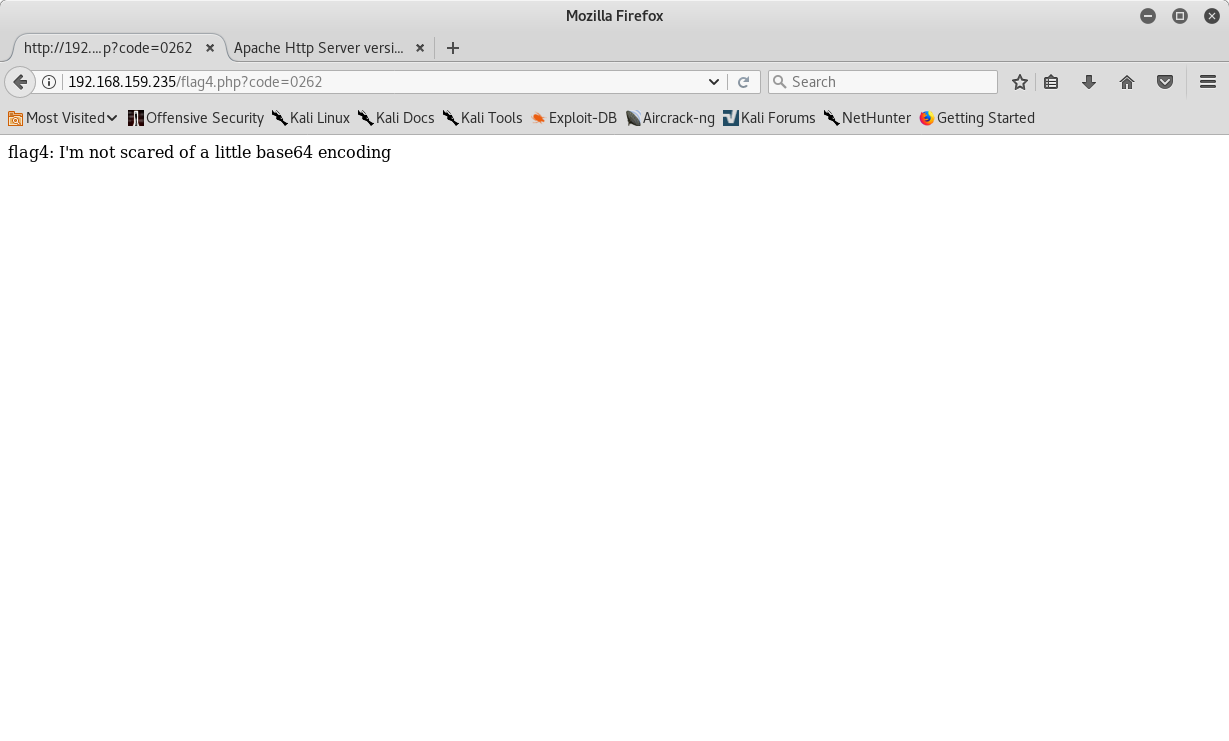


S:\ME Cybersecurity\Spring 2018\ENPM685 - Information Security Tools\Final Project\ENPM685 Project Files\flag2.bmp

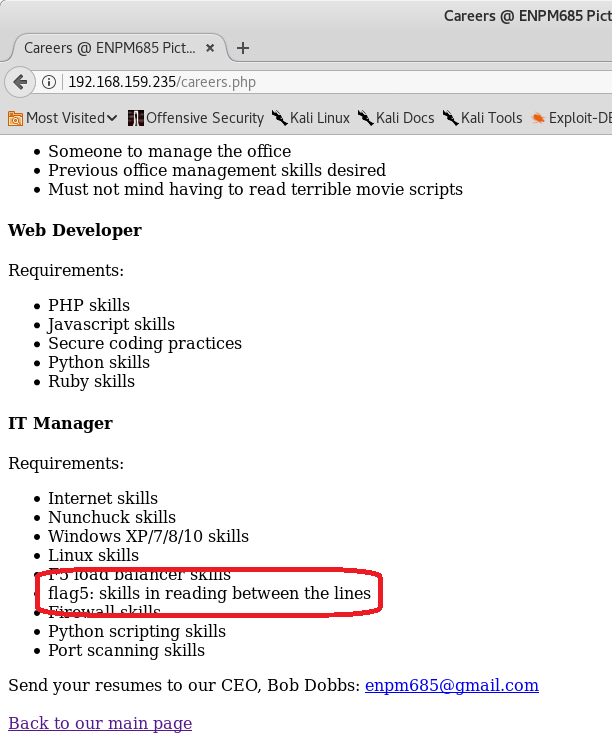
## Flag 3



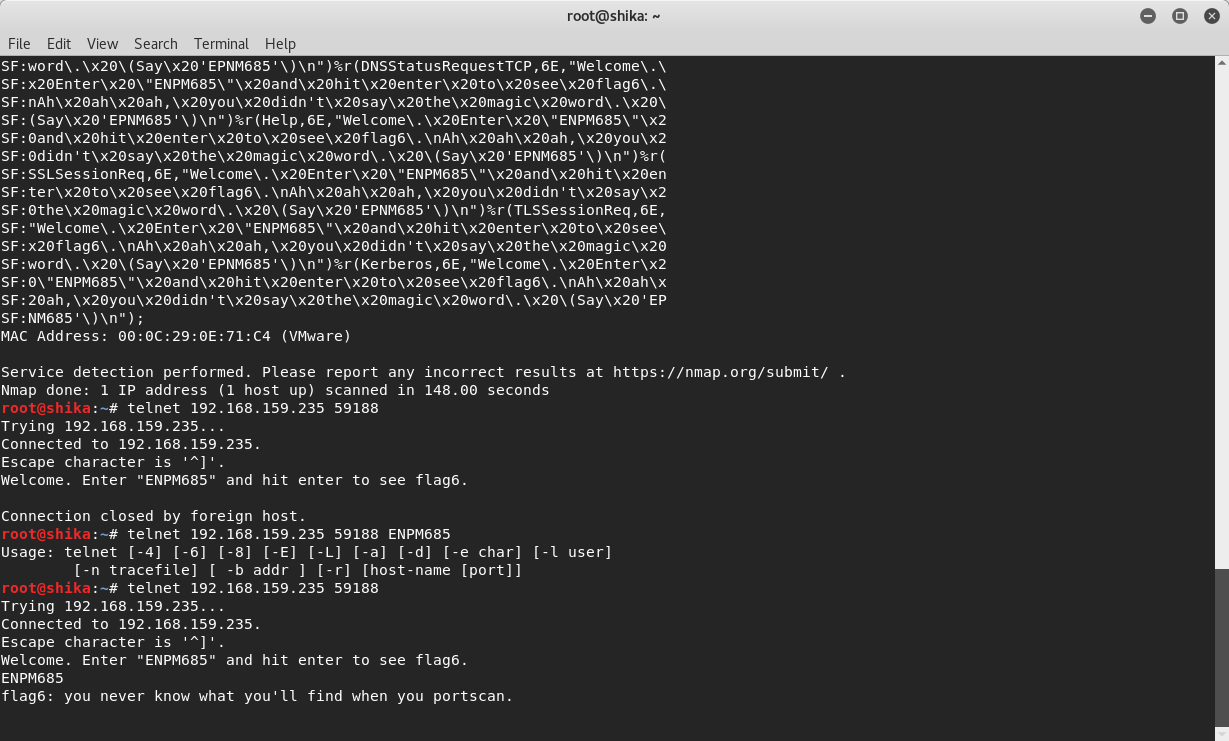
## Flag 4



## Flag 5



## Flag 6



# Relevant Files





