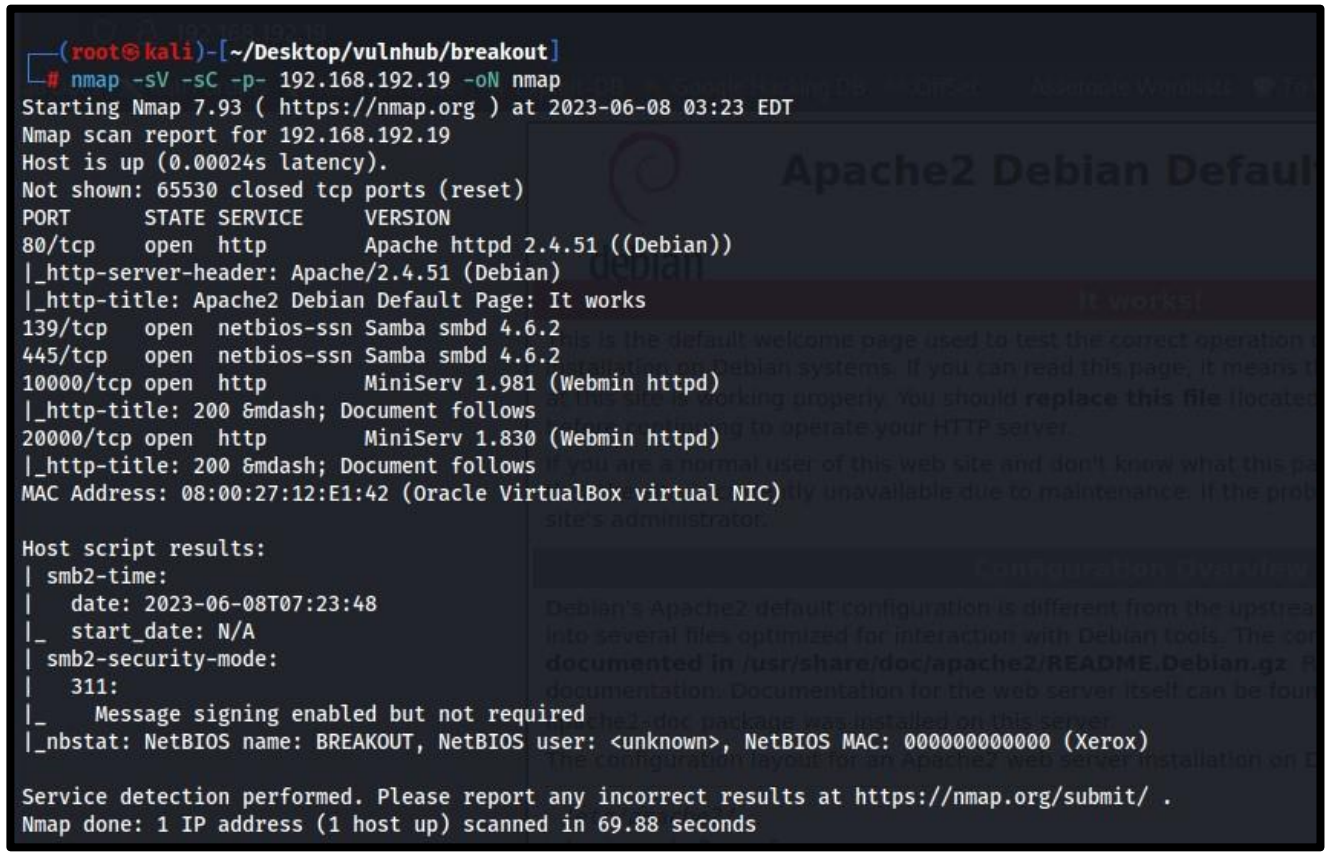
BREAKOUT

This is a box from vulnhub that is rated easy by the author. The box teaches you how to perform reconnaissance and how to identify and decrypt cipher.

The box wasn't hard for the first step getting user flag, but it was very easy for a person to end up in a rabbit hole.

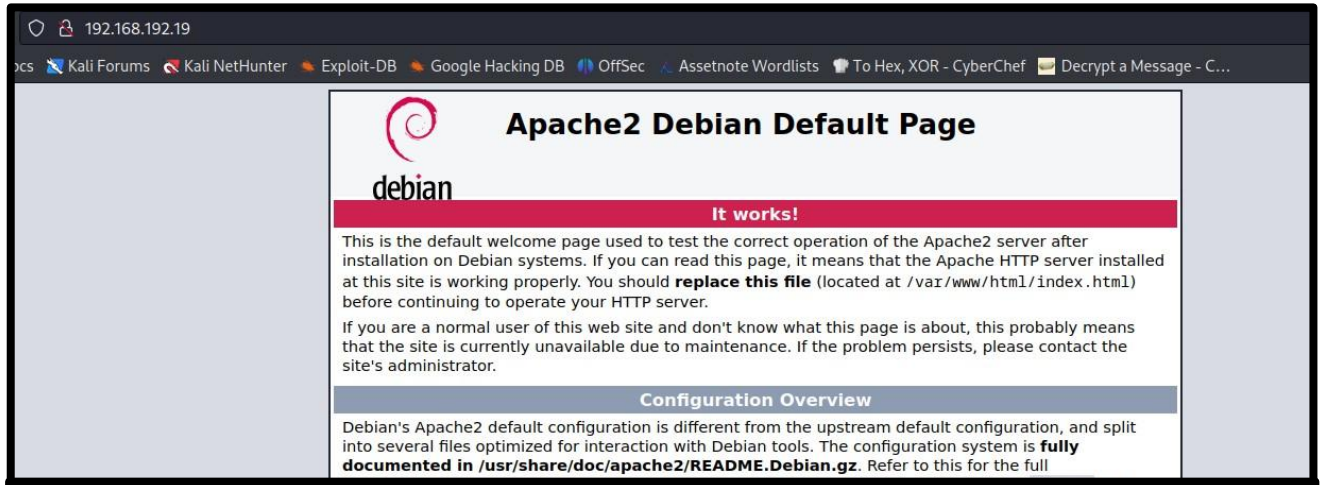
Author: Kharim Mchatta

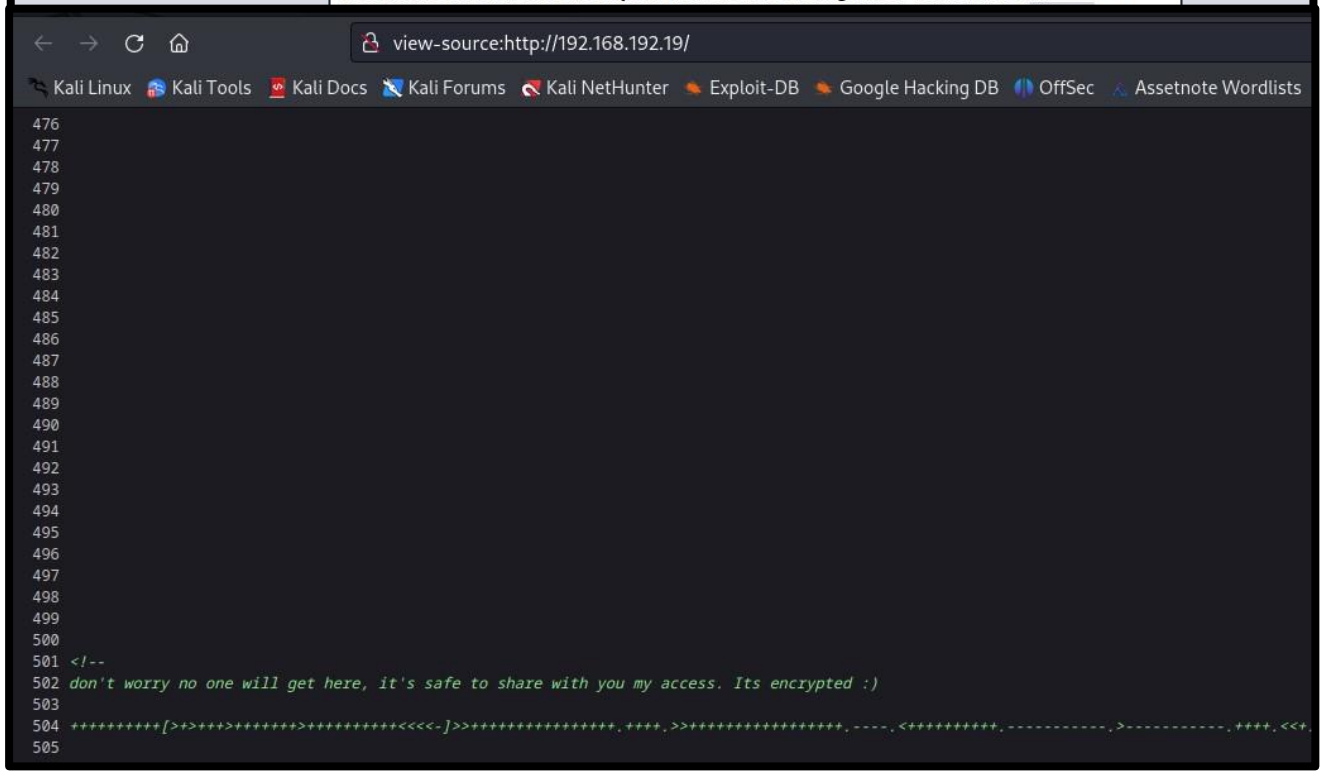
Date: 6/9/2023



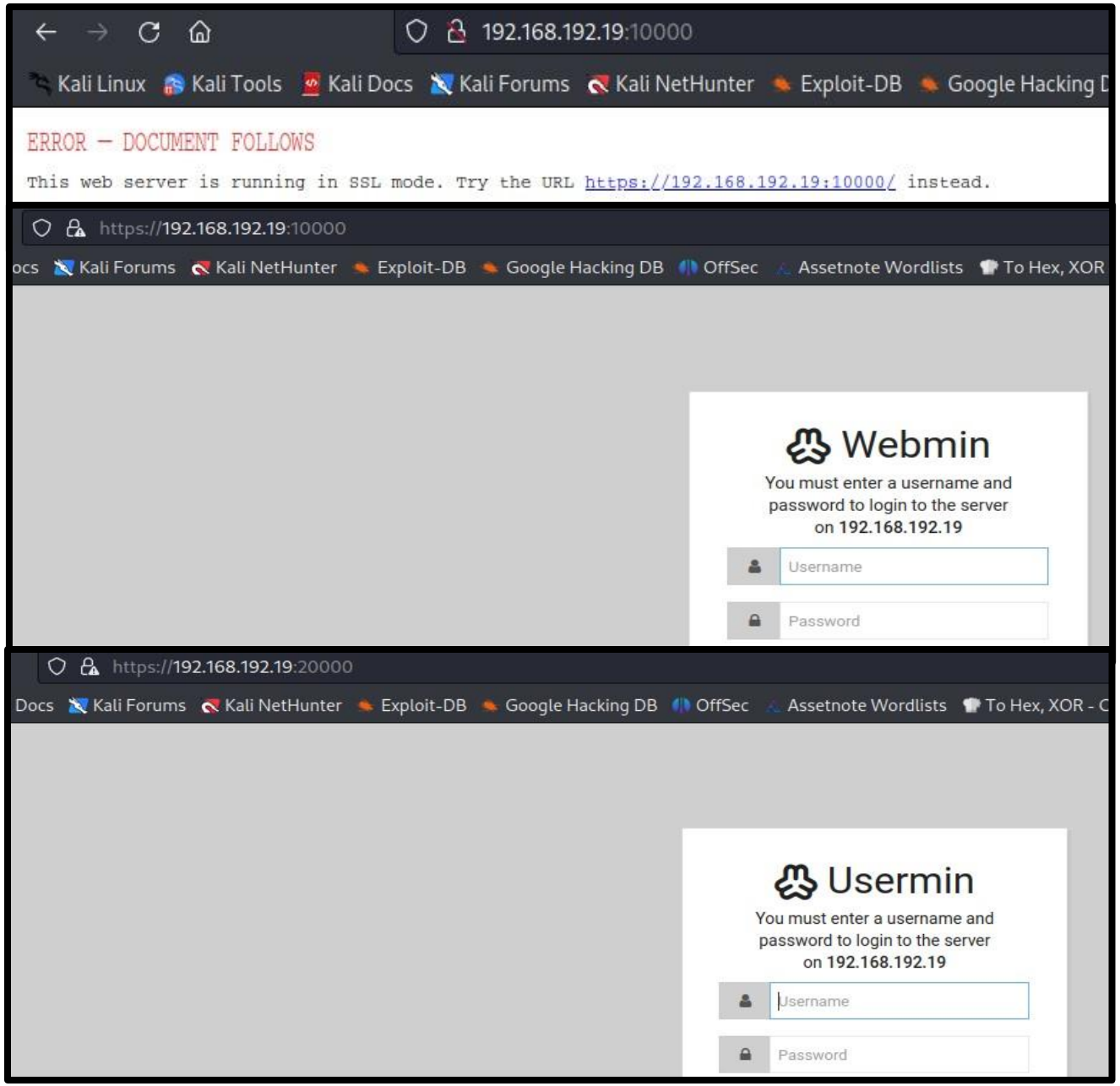
```
┌──(root㉿kali)-[~/Desktop/vulnhub/breakout]
└─# nmap -sV -sC -p- 192.168.192.19 -oN nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 03:23 EDT
Nmap scan report for 192.168.192.19
Host is up (0.00024s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
MAC Address: 08:00:27:12:E1:42 (Oracle VirtualBox virtual NIC)

Host script results:
| smb2-time:
|   date: 2023-06-08T07:23:48
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.88 seconds
```

I scanned the target ip 192.168.192.19 using nmap to see what ports are open and services are running on the target. From the results we can see that port 80 139, 445, 10000 and 20000 are open. Port 139 and 443 are associated with smb services which are usually associated with file shares.

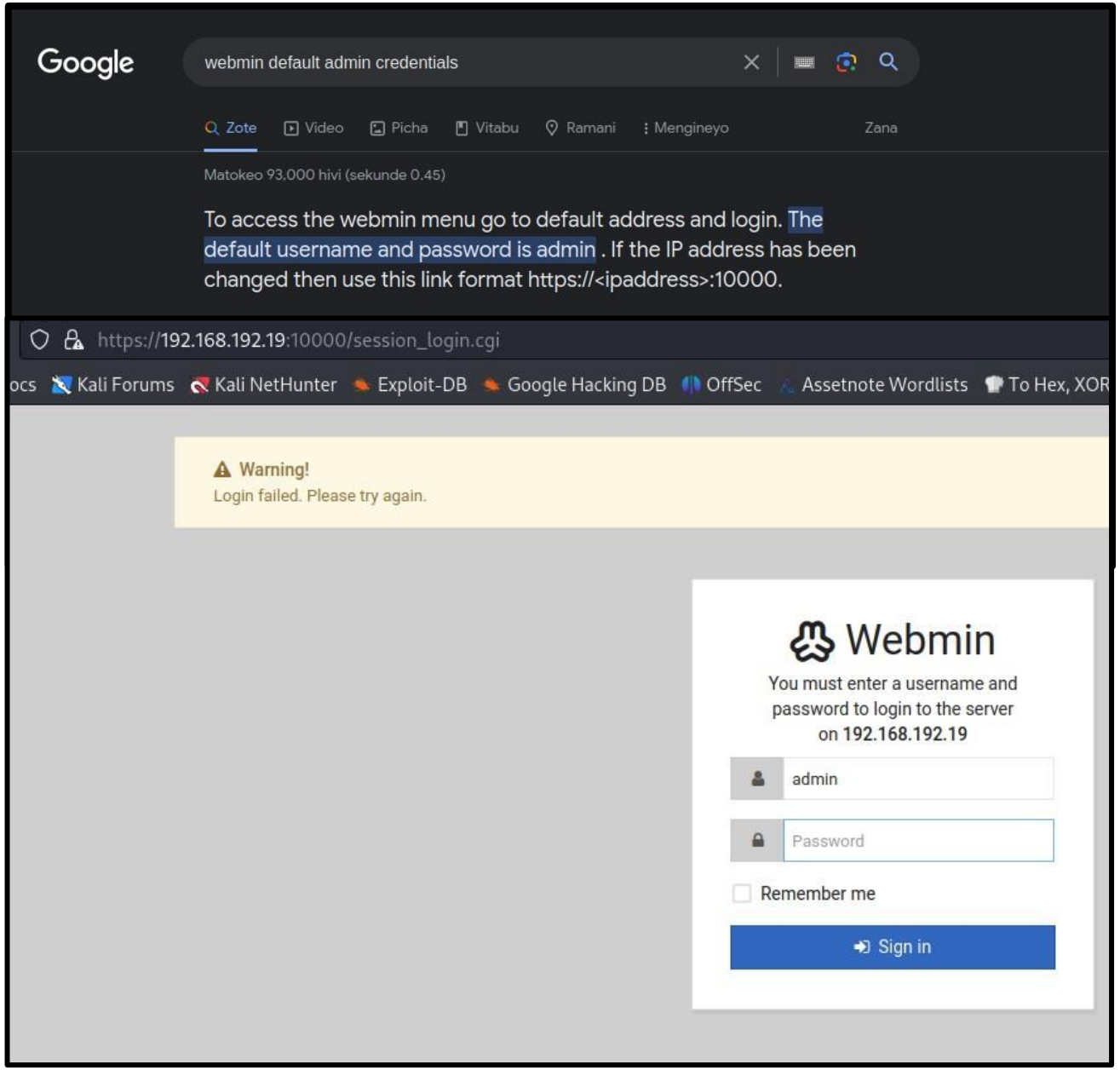




Navigating to http://192.168.162.19 a web application was, and it was a default web page of apache server. Next, I checked the page source and scrolling till the bottom of the page there was a cipher kept as a comment by the author of the box which stated **don't worry no one will get here, its safe to share with you my access, its encrypted.**

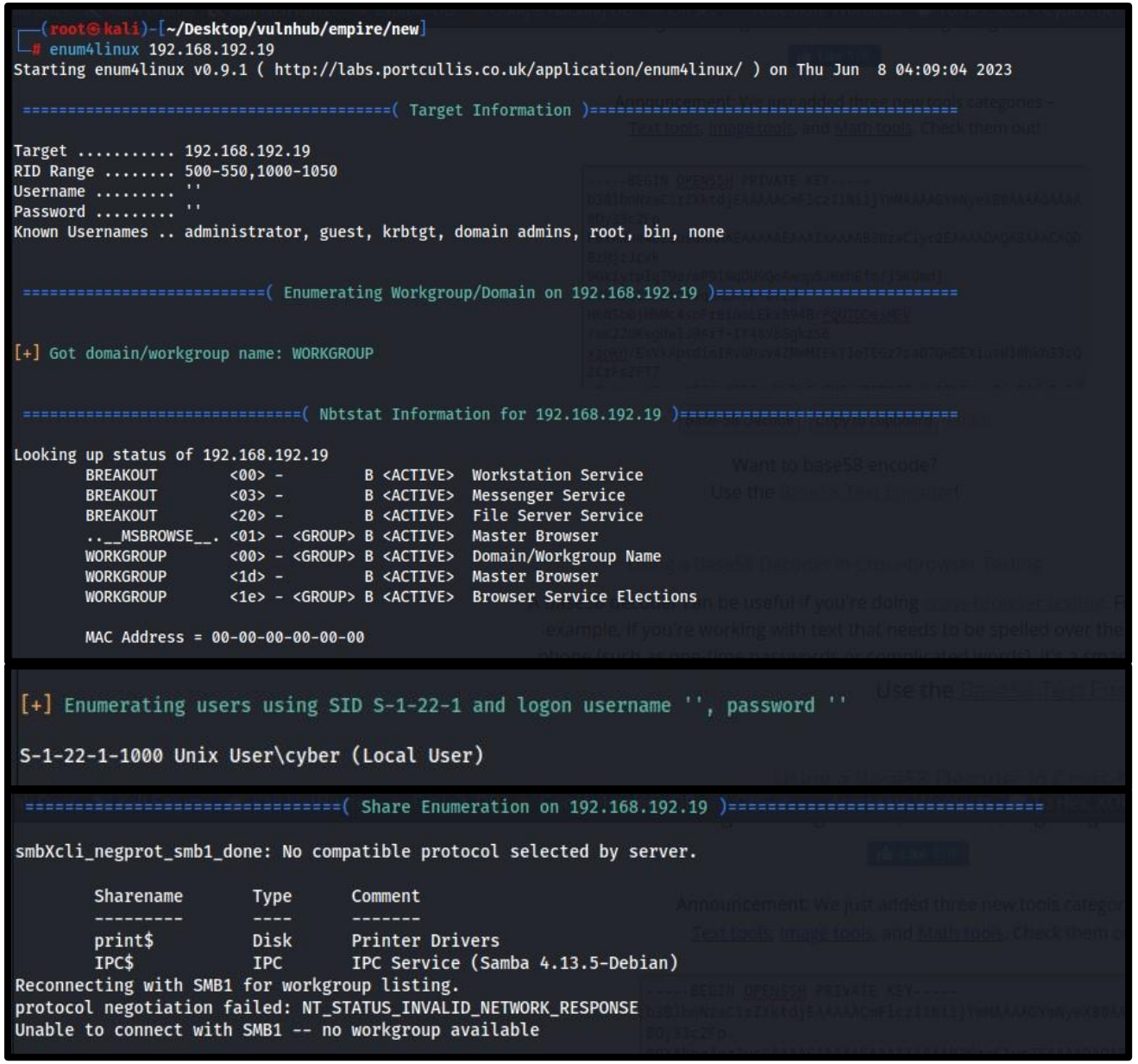


After reviewing the main web application, I had to go and check the other two web applications which nmap had reported and navigating through .10000 it gave me an error wanting me to access the page on https rather than http, clicking on the link I found it was a web application, I accessed the second web application which was .20000 and it was the similar web application like the first one.



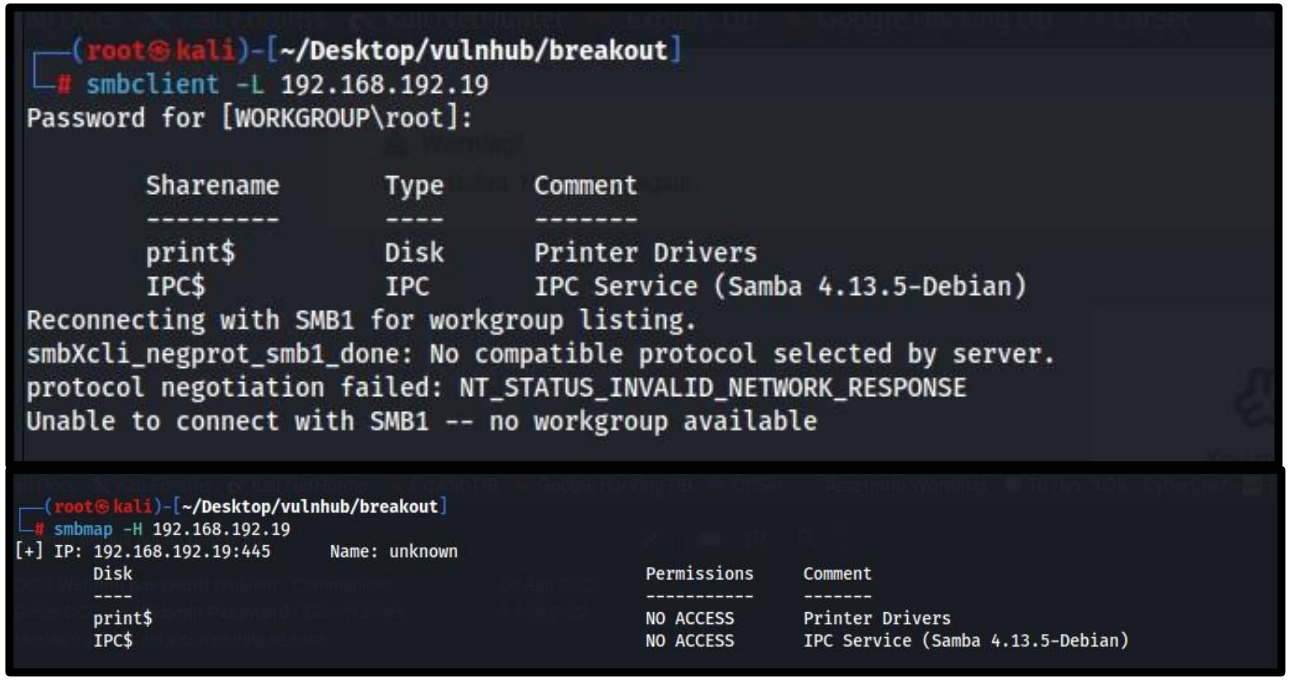
Next, I decided to try getting the default credentials on google and see if the admin had not removed them and testing the credentials out, they didn't work.

Author: Kharim Mchatta



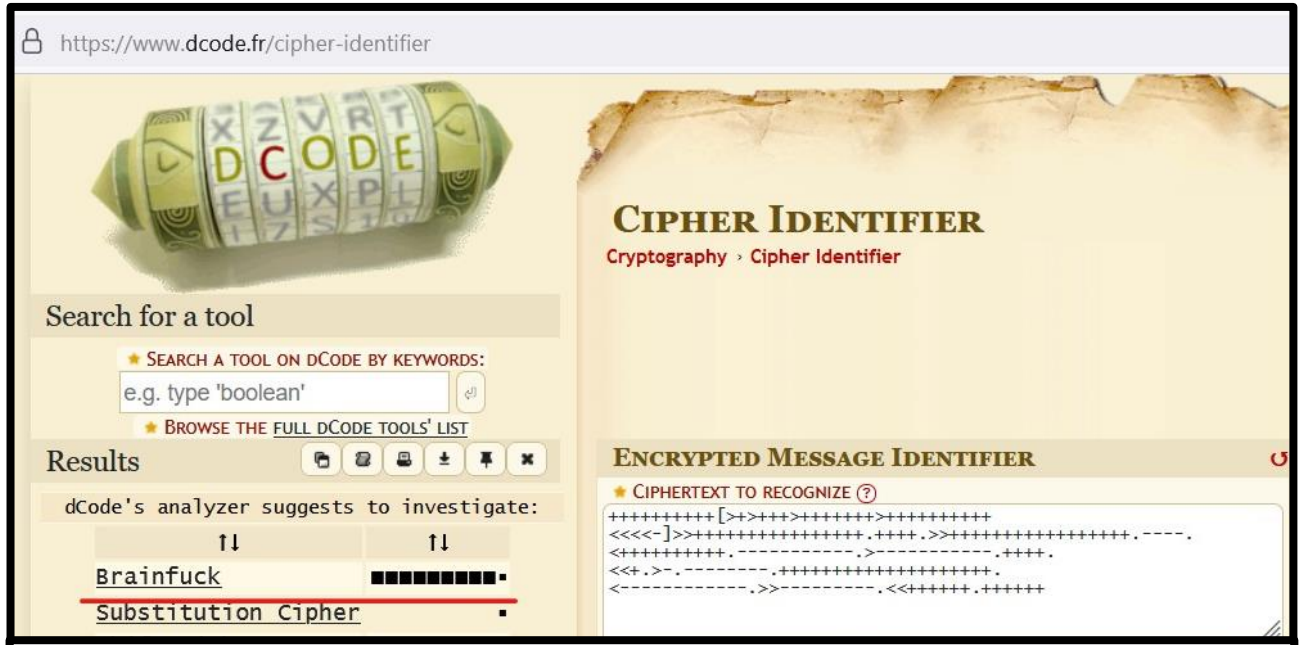
From our nmap result we had port 139 and 445 open which are associated with smb, I decided to utilize a tool called enum4linux to try and recon the service and from the result we managed to get a user called cyber, and there was no shared files on the machine.

Author: Kharim Mchatta



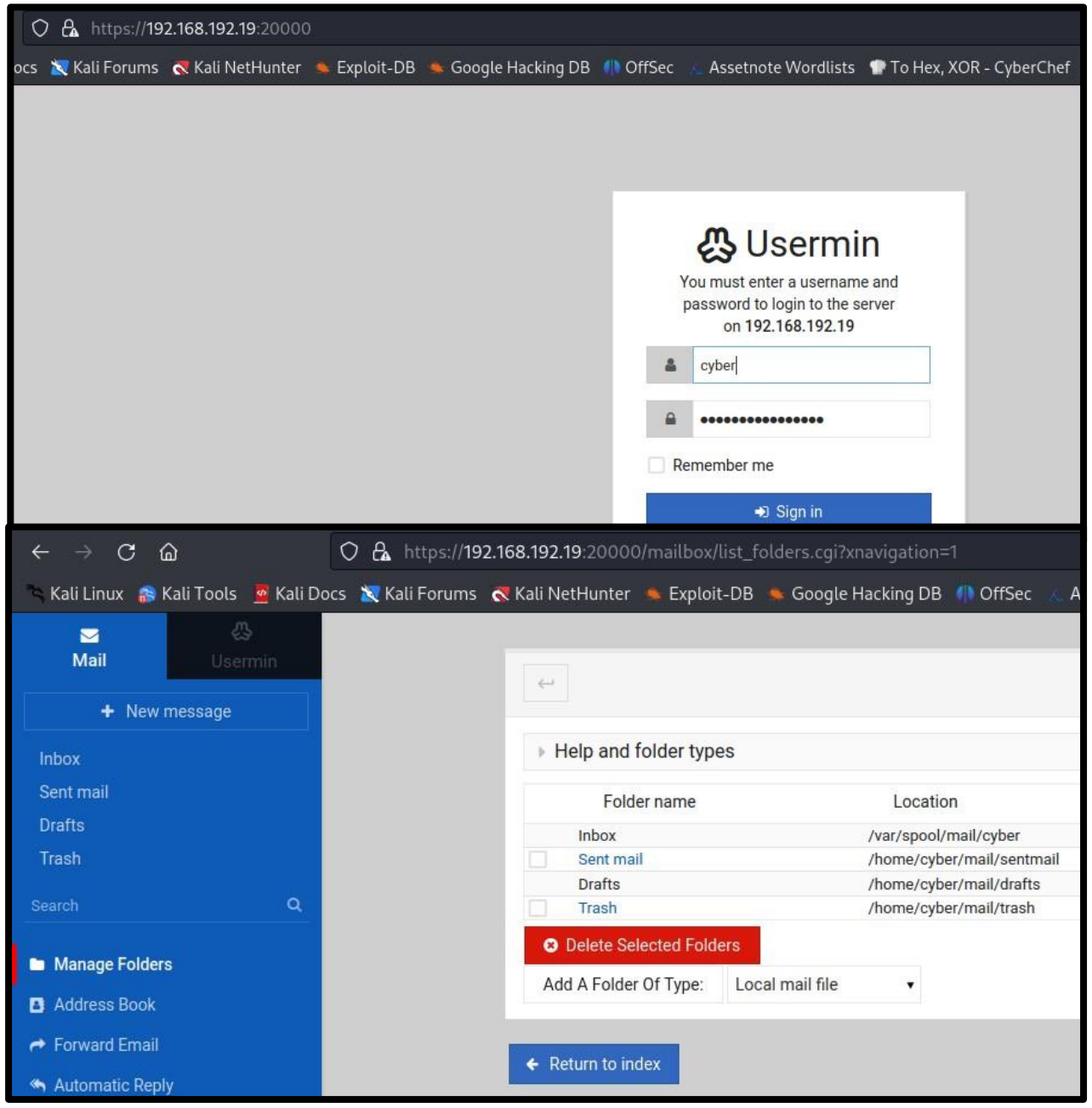
This is the rabbit hole which I was talking about initially where, my thought process was perhaps enum4linux was giving me false positive, so I had tried using other tools to enumerate for file shares, these tools were **smbclient** and **smbmap**.

I tried using the user anonymous perhaps I would get the share folders, but it didn't work, then I made use of the user cyber which we had obtained from enum4linux but also that was a head end.



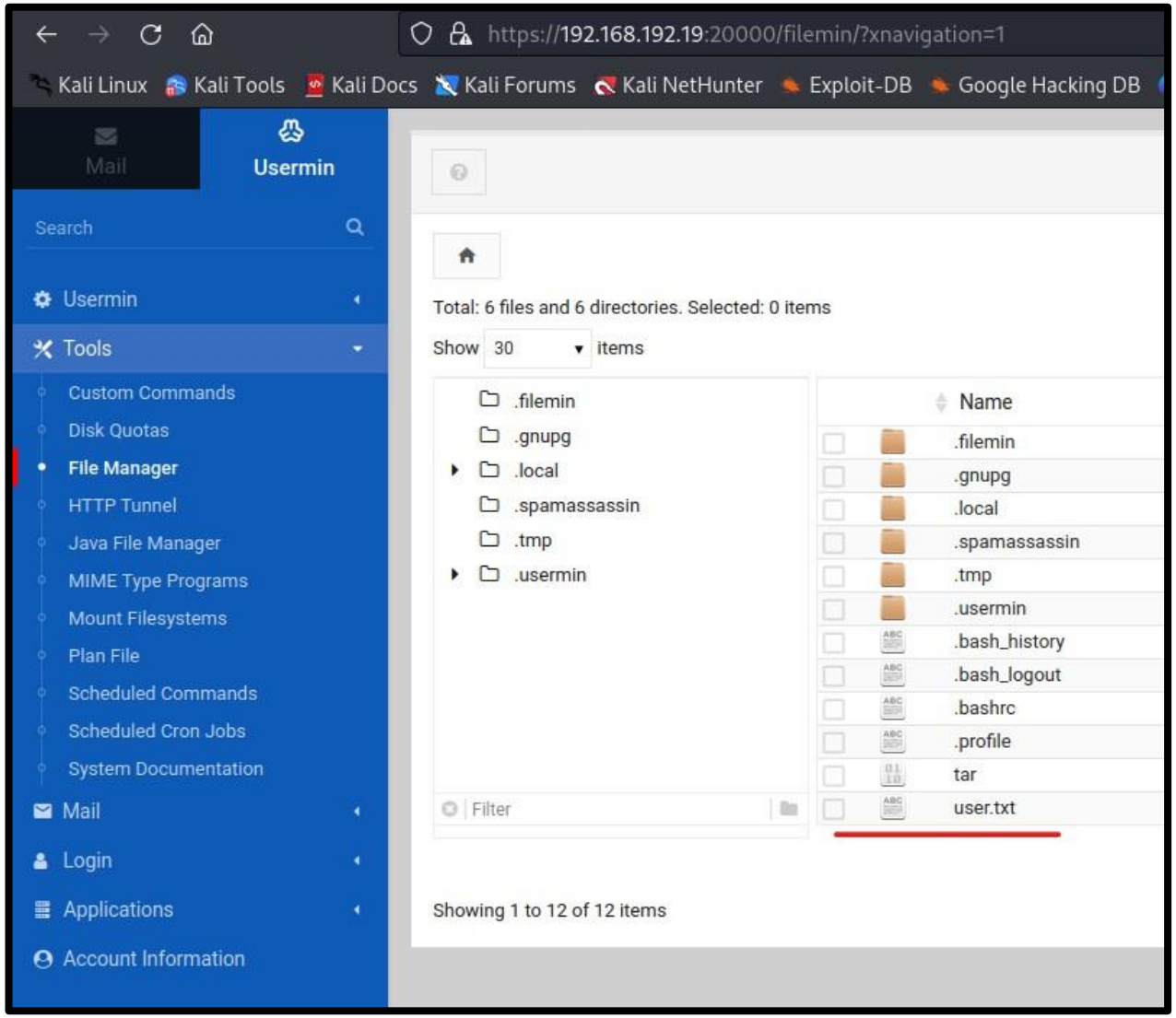
After trying everything with smb, I went back to the web application and googled online cipher identifier and select the first link and pasted the encrypted message on the text box and analyzed and it was identified as brainfuck cipher, then I went to the next page which was to decipher brainfuck cipher and pasted the cipher and managed to get a password.

You might be wondering how we know if this was the password, well remember from the main web application when we viewed the source page on the comment, the author gave us a hint by saying **don't worry no one will get here, its safe to share with you my access, its encrypted.**



Next, I used the credentials to login the web application, going through the mail tab there was nothing important there apart from seeing the server files paths as shown the image.

Author: Kharim Mchatta



Then I clicked on the usermin tab and started going through the tabs and when I got to file manager is when I saw the txt file.

If you look at the bottom left-hand side, you will see a terminal tab and when you click on it a terminal will appear and when you type in ls you will see the user.txt and you will be able to read the content using the command cat. The next thing from there is for you to establish a reverse shell connection to the server and once you have successfully done that you can privilege escalate to the root directory and be able to read the root flag.

Summary

---

1. Perform nmap
2. Open the web application
3. View source page to find comment
4. Retrieve the cipher
5. Identify type of cipher
6. Decode cipher
7. Use enum4linux to get user
8. Gain access to the **.20000** web page
9. Obtain the user flag

Author: Kharim Mchatta