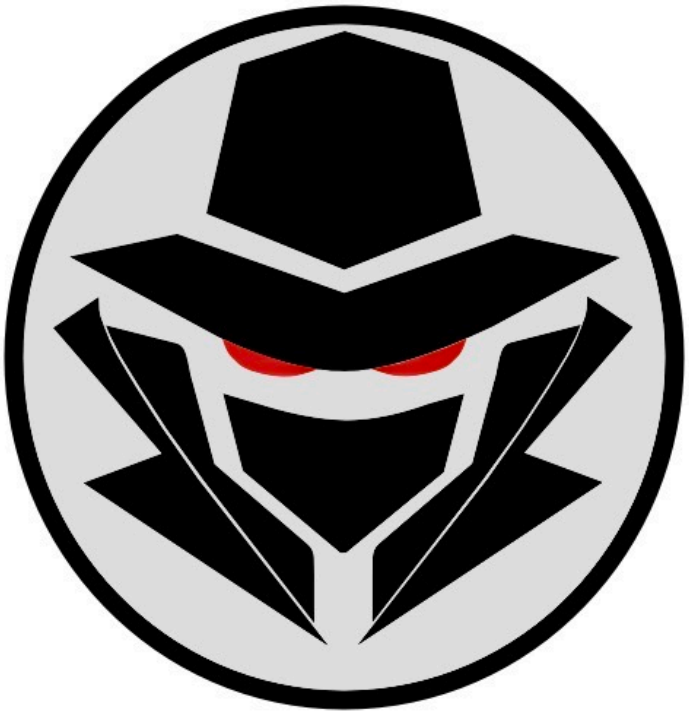
ROT

I might be hidden deep, You need to find me ASAP.

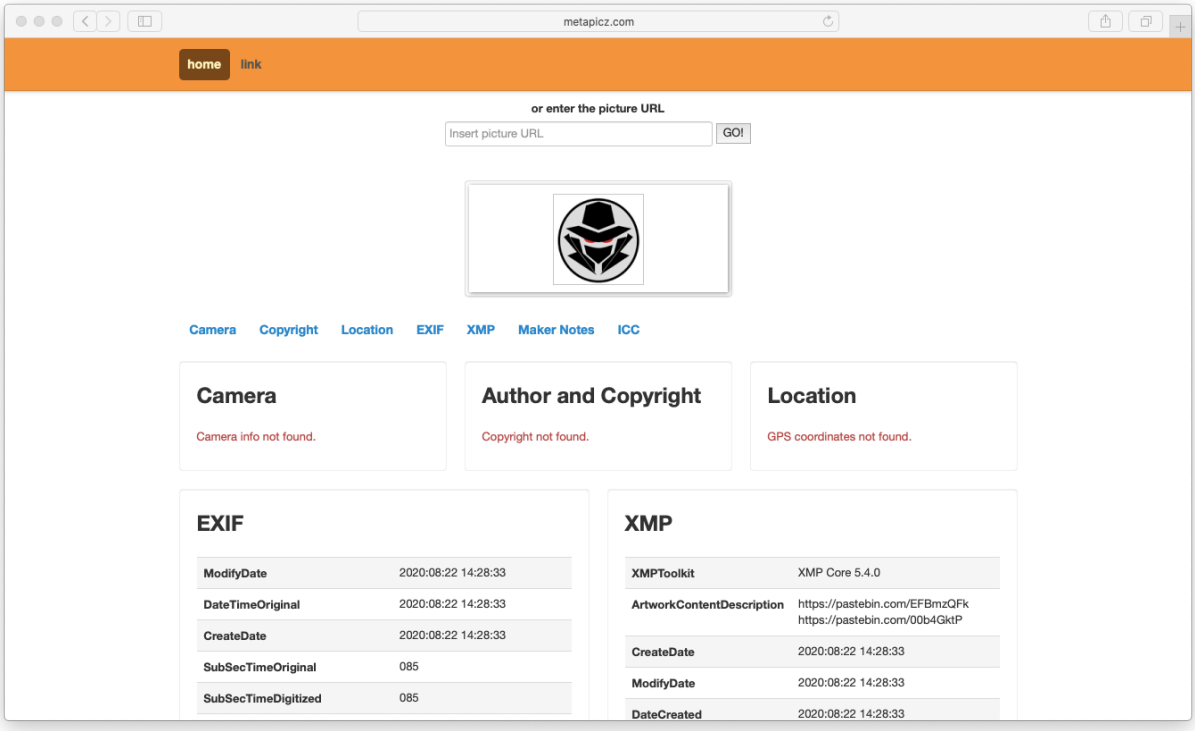
Flag:- HTB{M0naC0h@sBeeNPwn3d}
Category:- EASY, OSINT

Writeup:-

1. We have been given an image in the challenge.



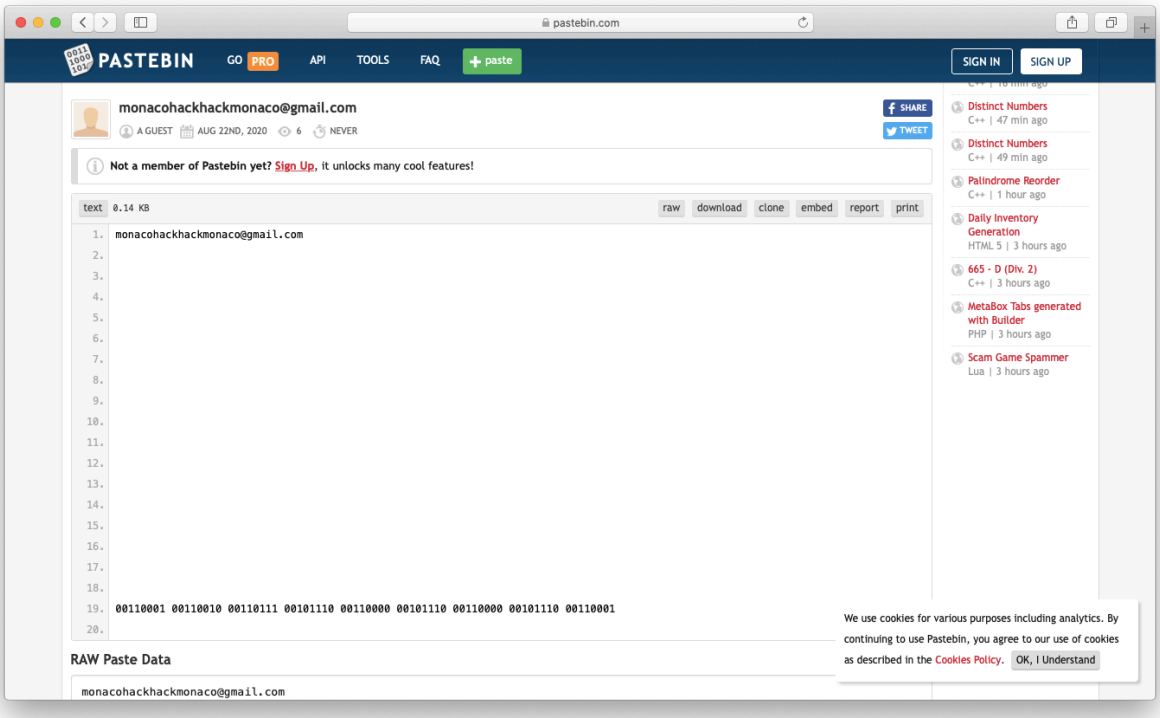
2. We analyze the image's metadata and found two pastebins link.



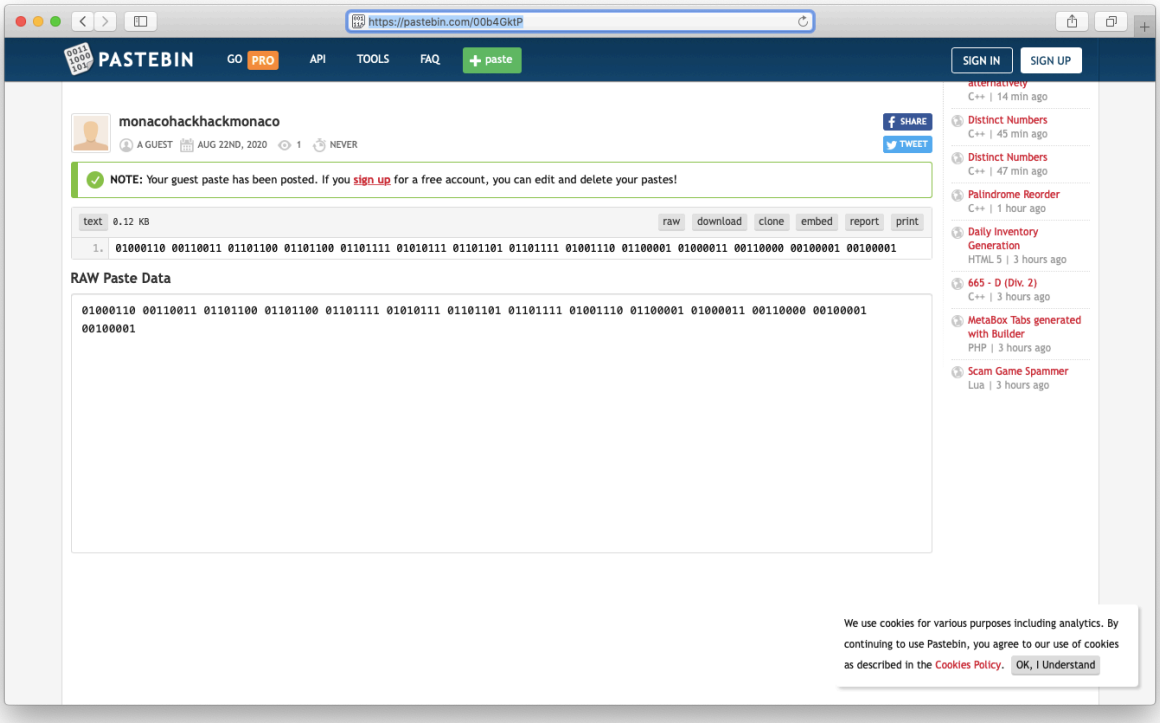
ROT

I might be hidden deep, You need to find me ASAP.

3. https://pastebin.com/EFBmzQFk



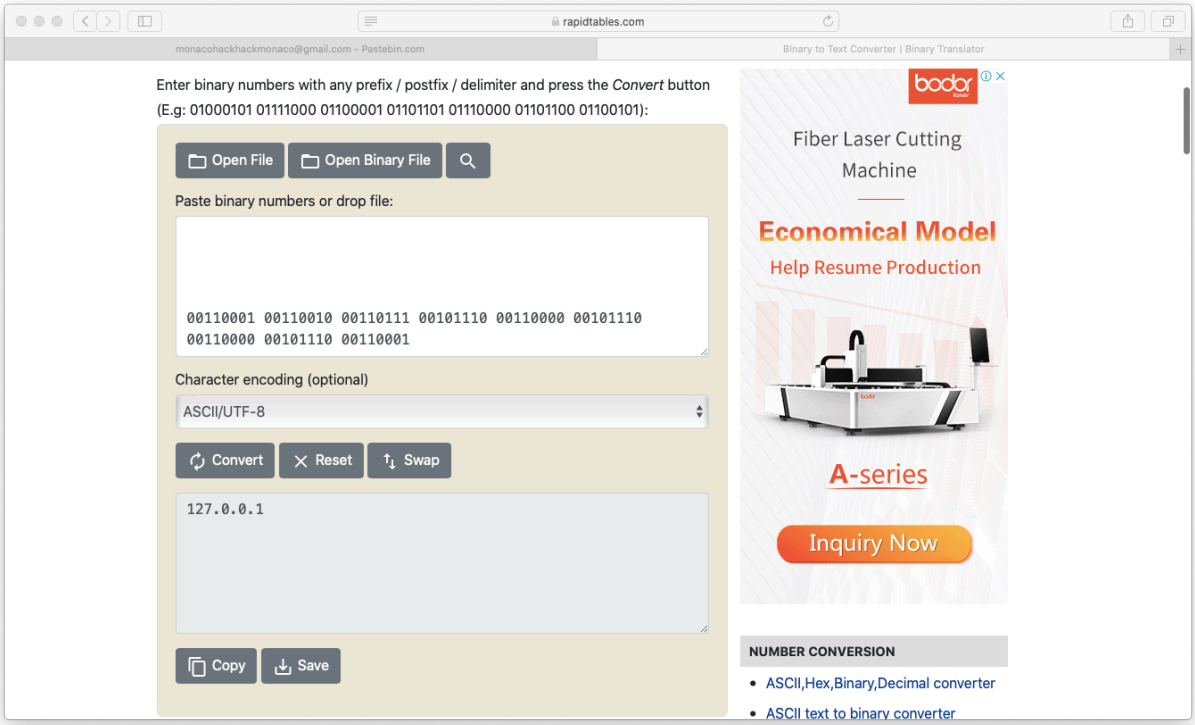
4. https://pastebin.com/00b4GktP

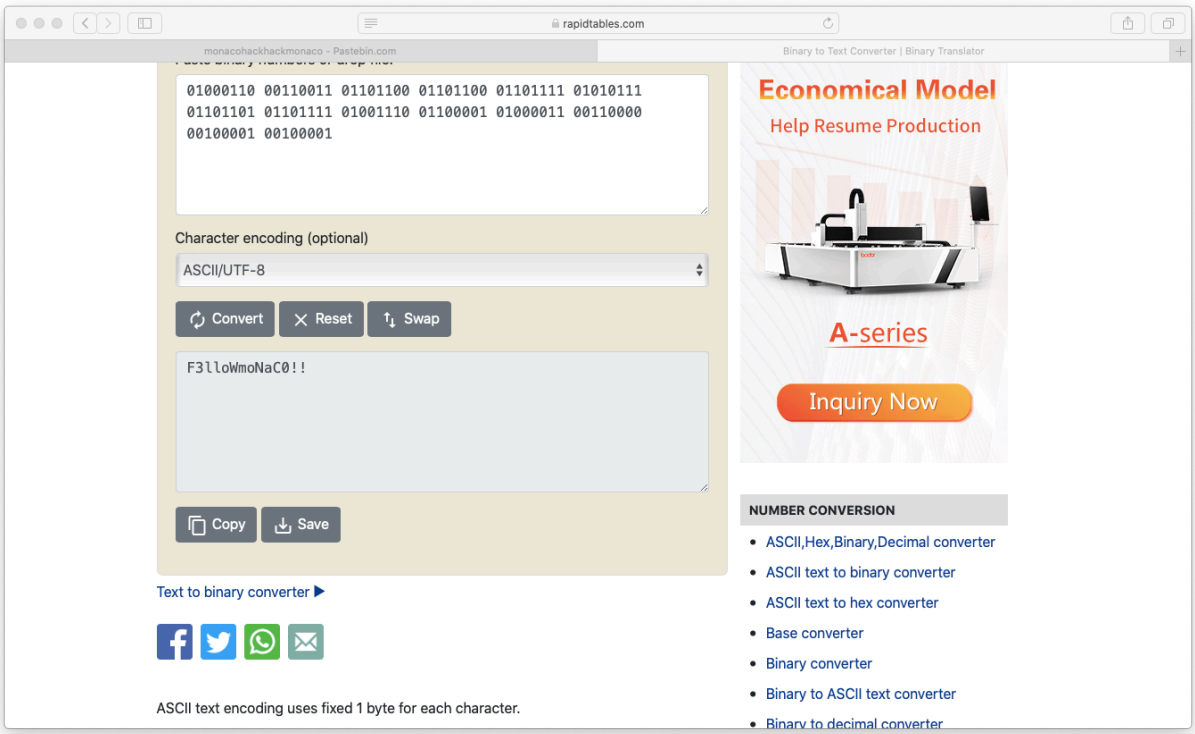


ROT

I might be hidden deep, You need to find me ASAP.

5. We got one email/username monacohackhackmonaco@gmail.com and some binary.
6. Putting them through binary to text convertor, we got IP and a Pass.

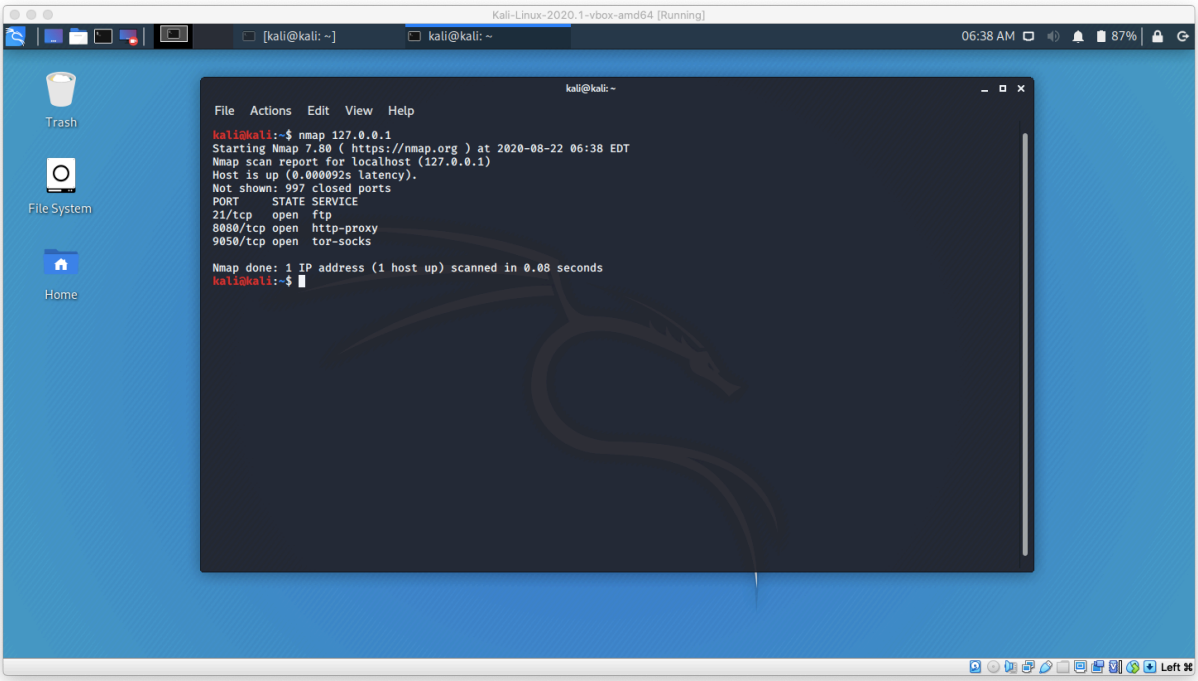




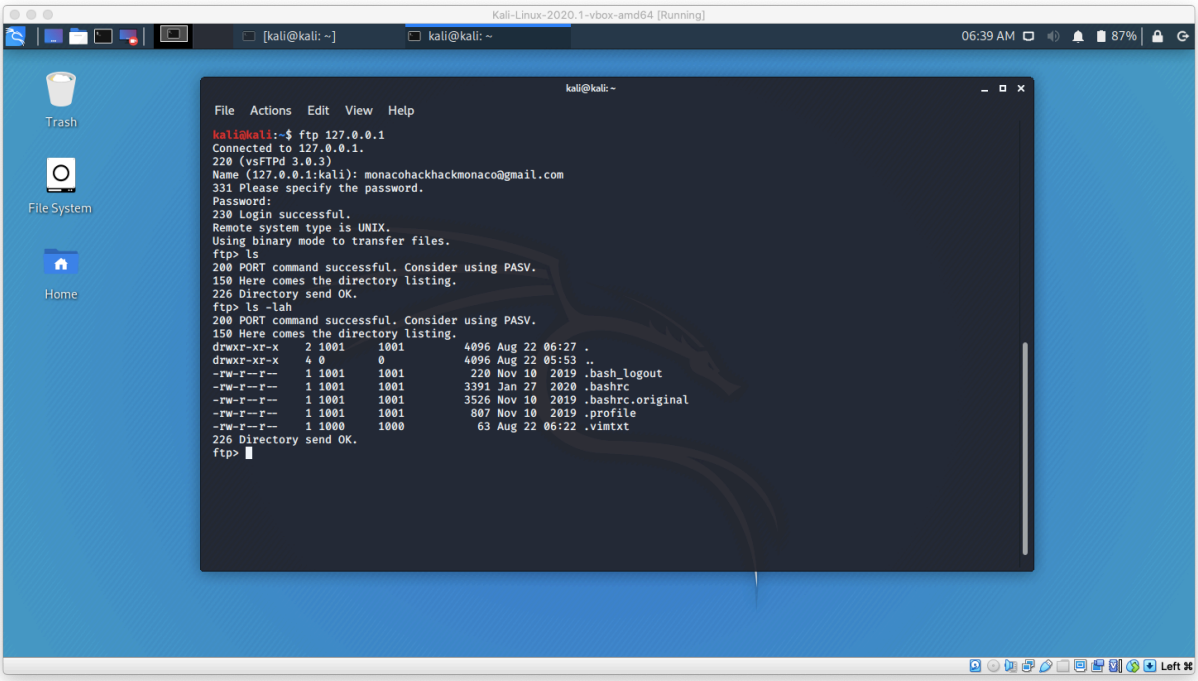
7. IP= 127.0.0.1 (local for now)
   Password= F3lloWmoNaC0!!

ROT
I might be hidden deep, You need to find me ASAP.

8. NMAP the IP.



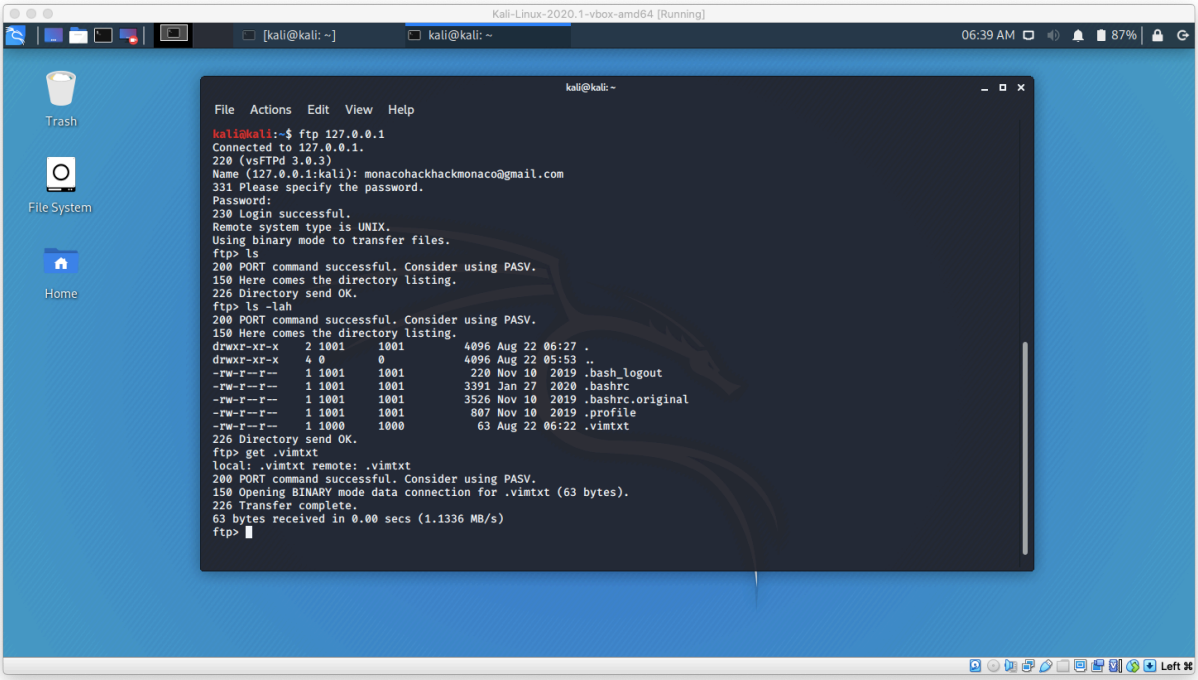
9. Got FTP open, Lets Try the Creds as monacohackhackmonaco@gmail.com: F3lloWmoNaC0!!

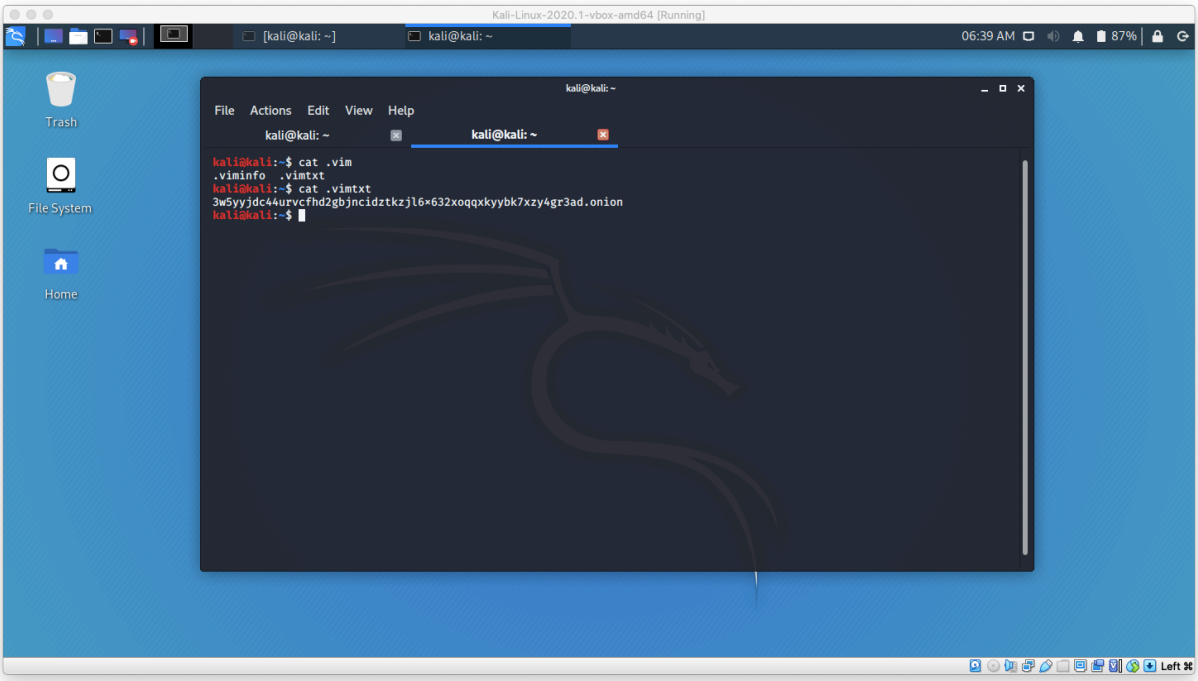


ROT

I might be hidden deep, You need to find me ASAP.

10. We are in and got .vimtext as a file in ftp transfer it over to the local machine and cat it.

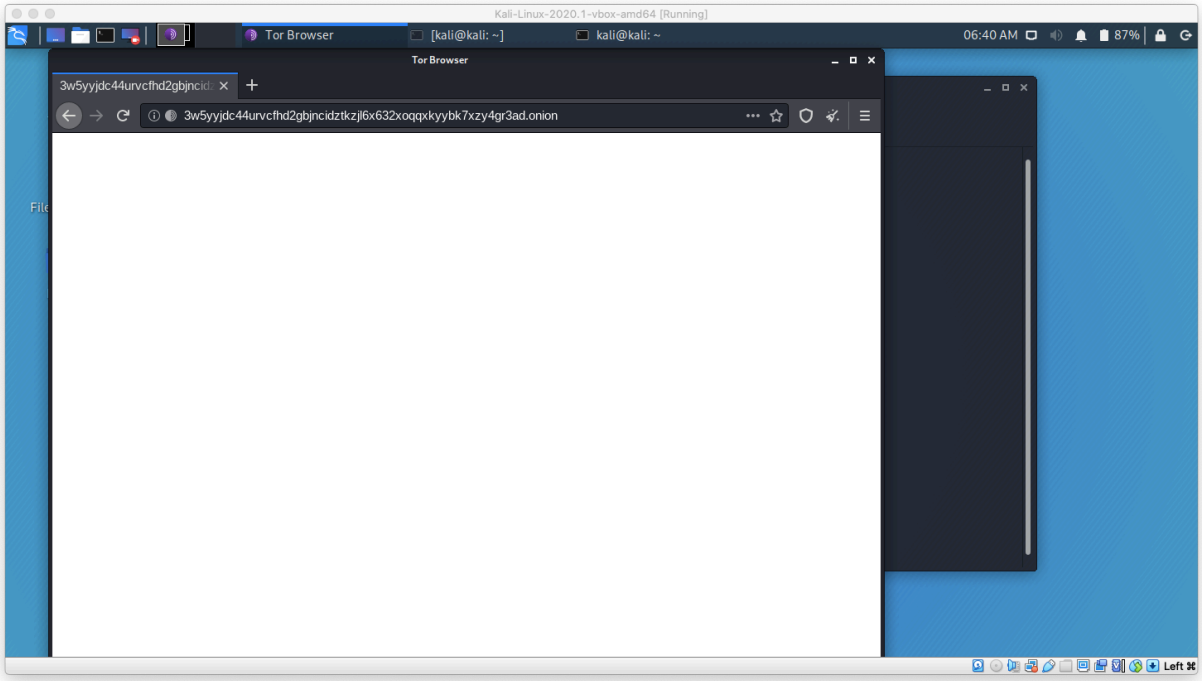




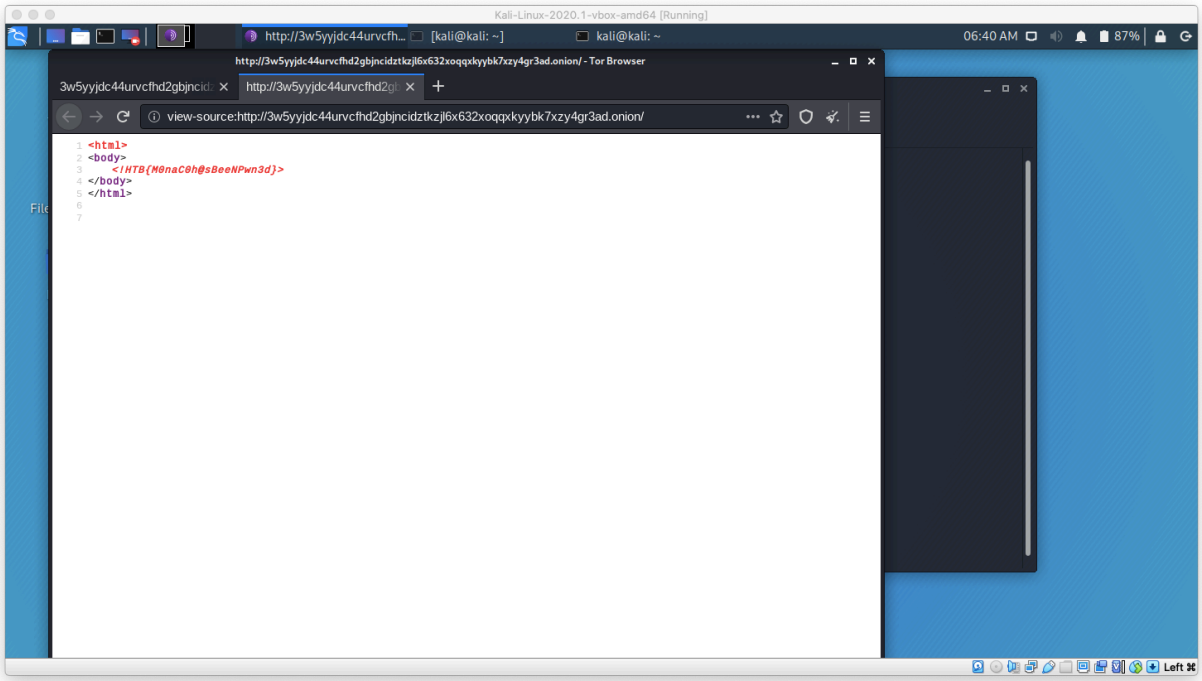
ROT

I might be hidden deep, You need to find me ASAP.

11. We got an ONION url,
http://3w5yyjdc44urvcfhd2gbjncidztkzjl6x632xoqqxkyybk7xzy4gr3ad.onion/
Lets bootup the torbrowser and see if we got anything.



12. View Source and we got the flag.



Sources Used for Setup of TOR :- https://null-byte.wonderhowto.com/how-to/host-your-own-tor-hidden-service-with-custom-onion-address-0180159/