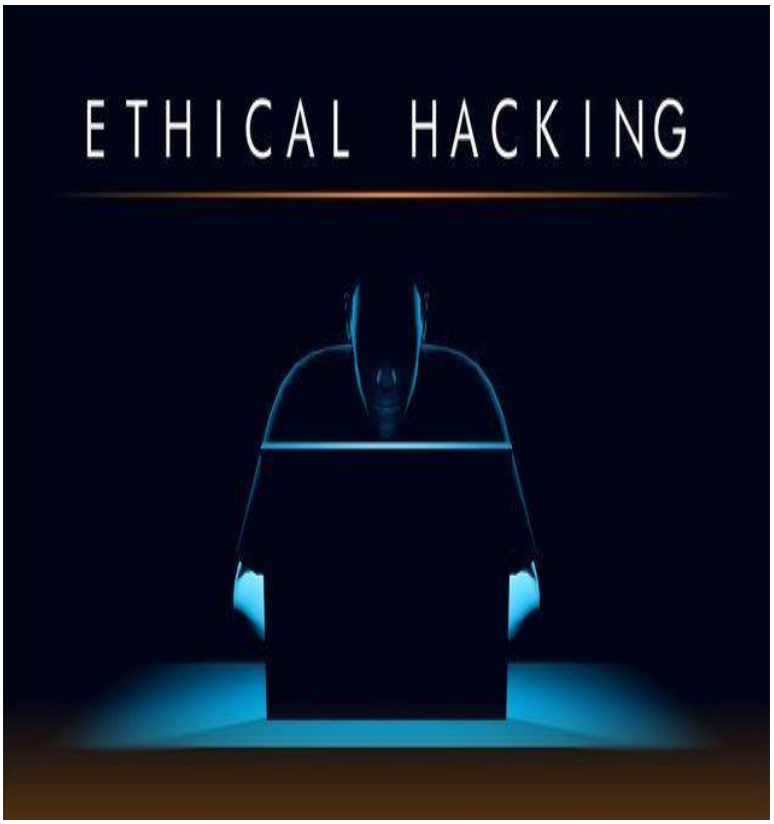
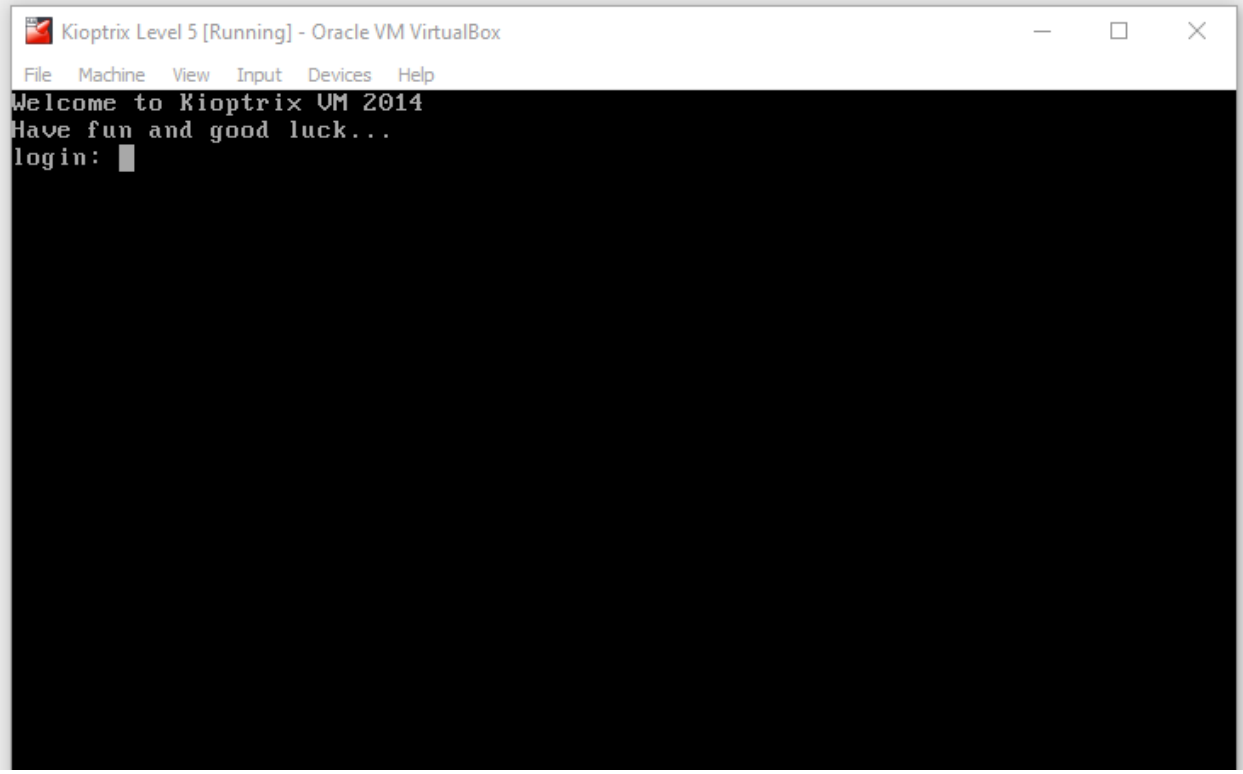


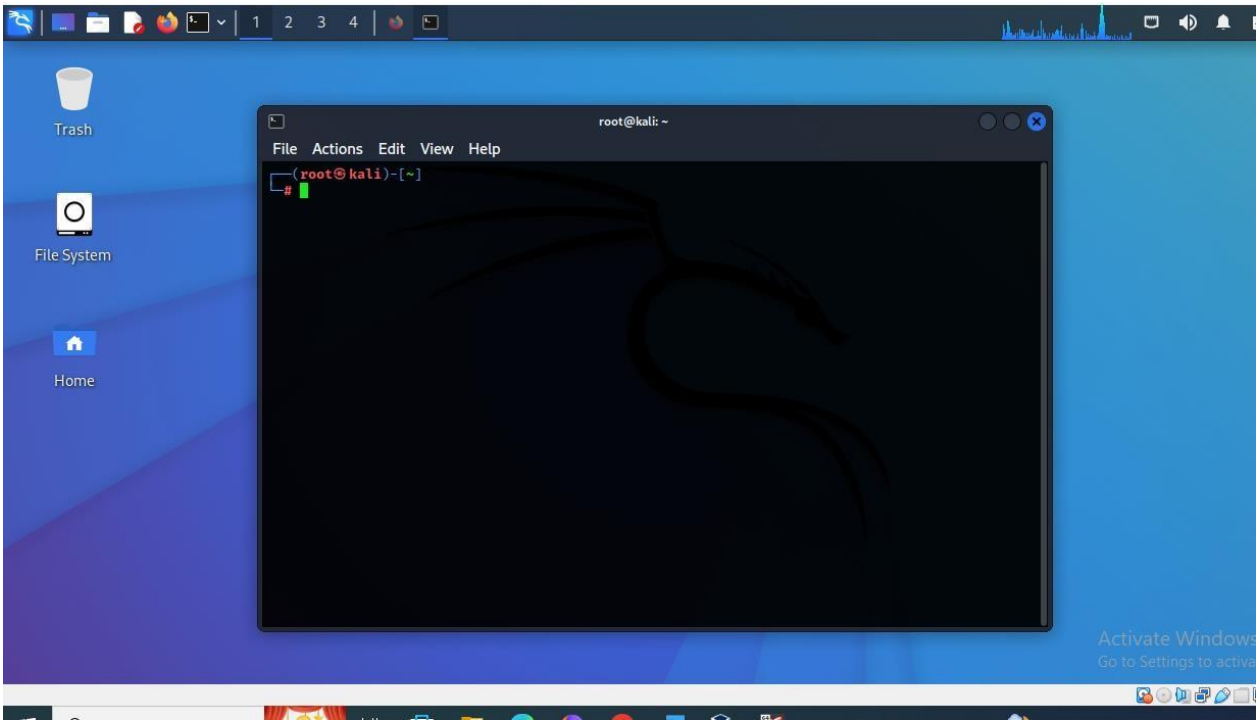
PENETRATION TESTING

KIOPTRIX LEVEL 5

BY

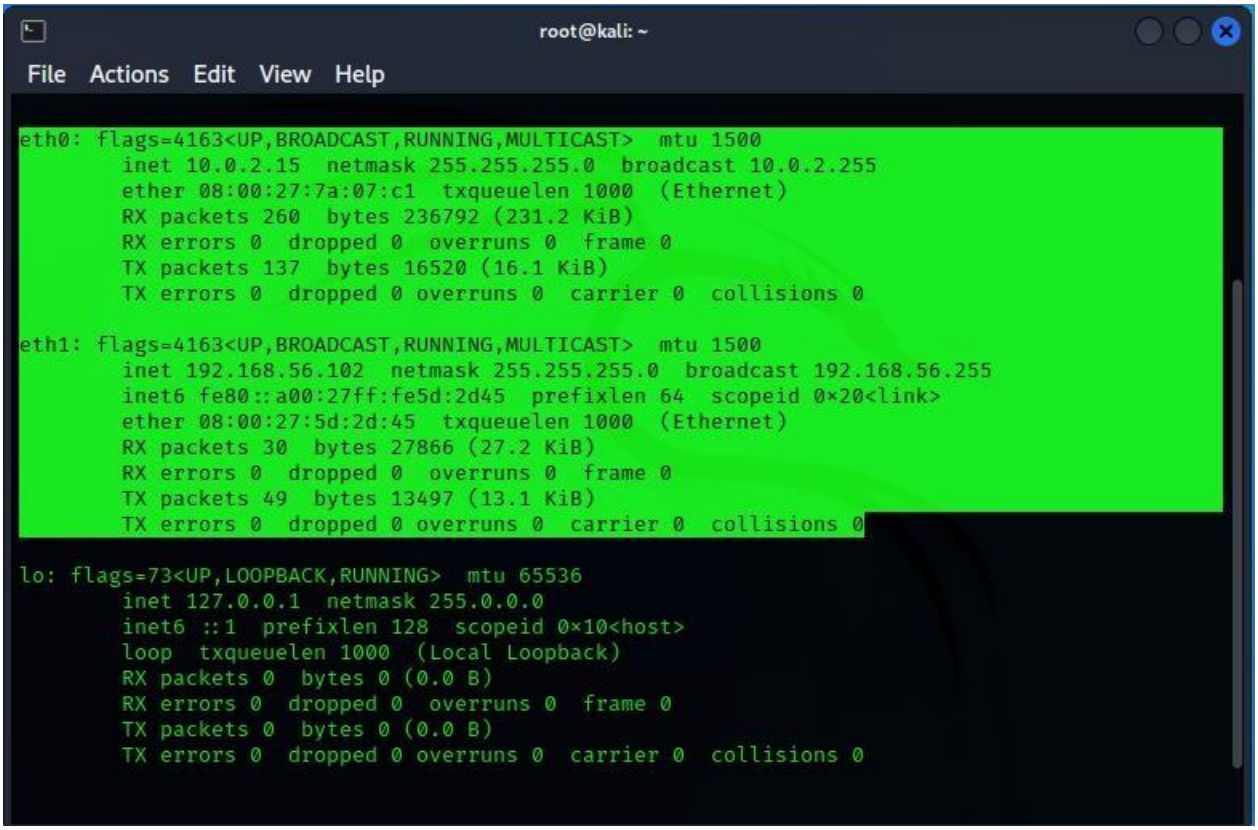
DEWTON KIPROP





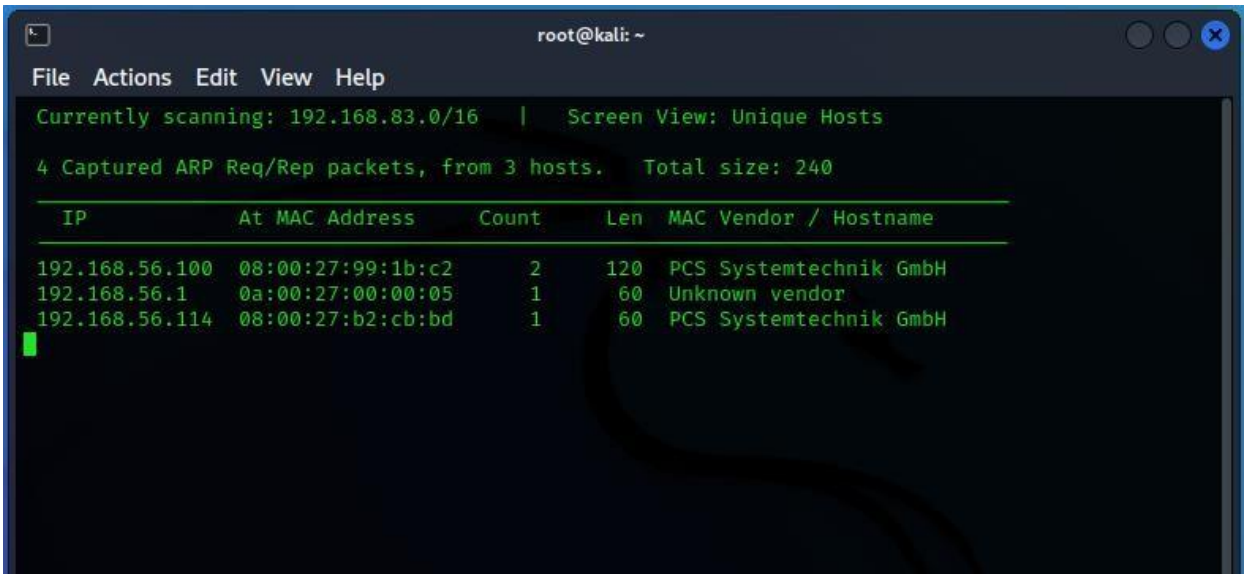
- Make sure your kioptrix and kali machines are up and running as shown on the screenshots above.

NOTE: under settings → network, make sure the kioptrix machine is under "host only " in adapter 1 and kali machine under "host only" in adapter 2 and NAT in adapter 1.

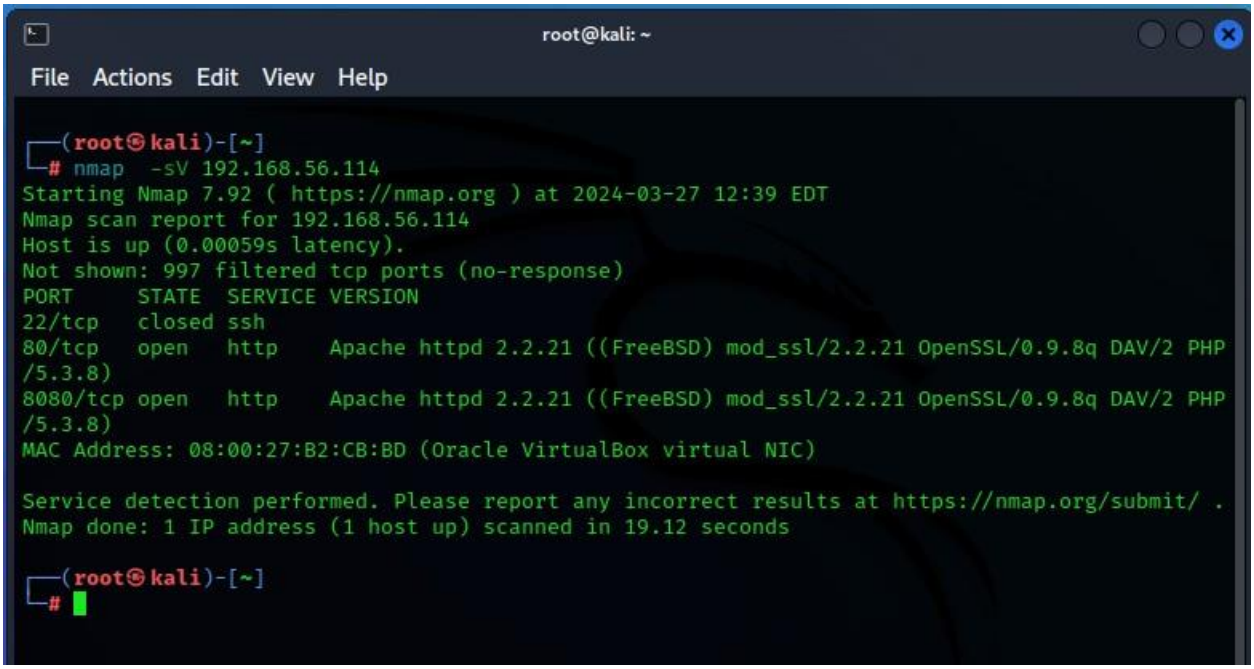


- When you run ifconfig, you should be able to see eth0 and eth1 assigned to IPs 10.0.2.15 and 192.168.56.102 . These are the two adapters of the kali machine. ***NOTE: your results for ip addresses might not be the same as those of the screenshot above.***

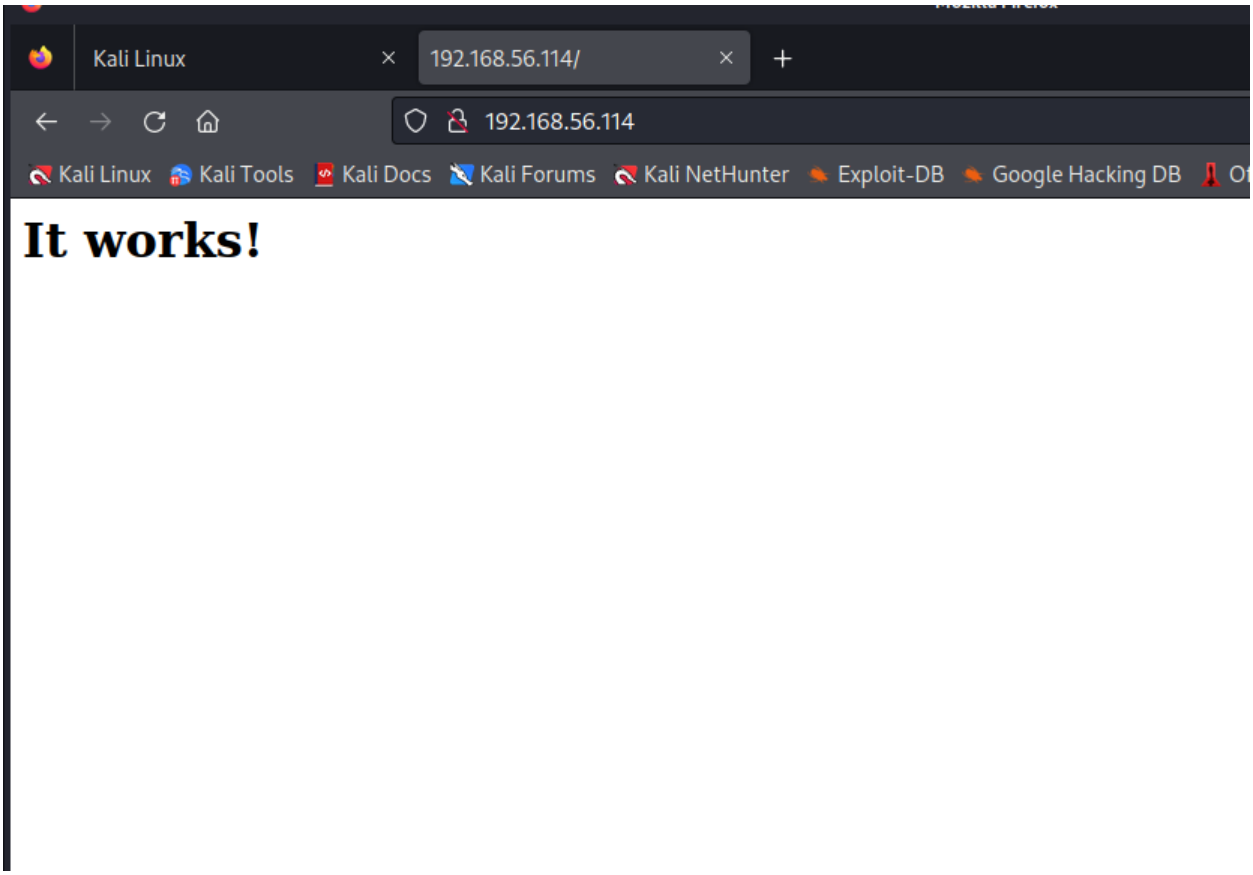
- Now you can proceed and do a netdiscover on eth1.



- Once the scan is complete, the output is three ip addresses as shown above. Usually, the third ip address from the scan is the ip address of the kioptrix machine. To confirm this, shutdown the kioptrix and run the netdiscover command and see if the third ip address is displayed.



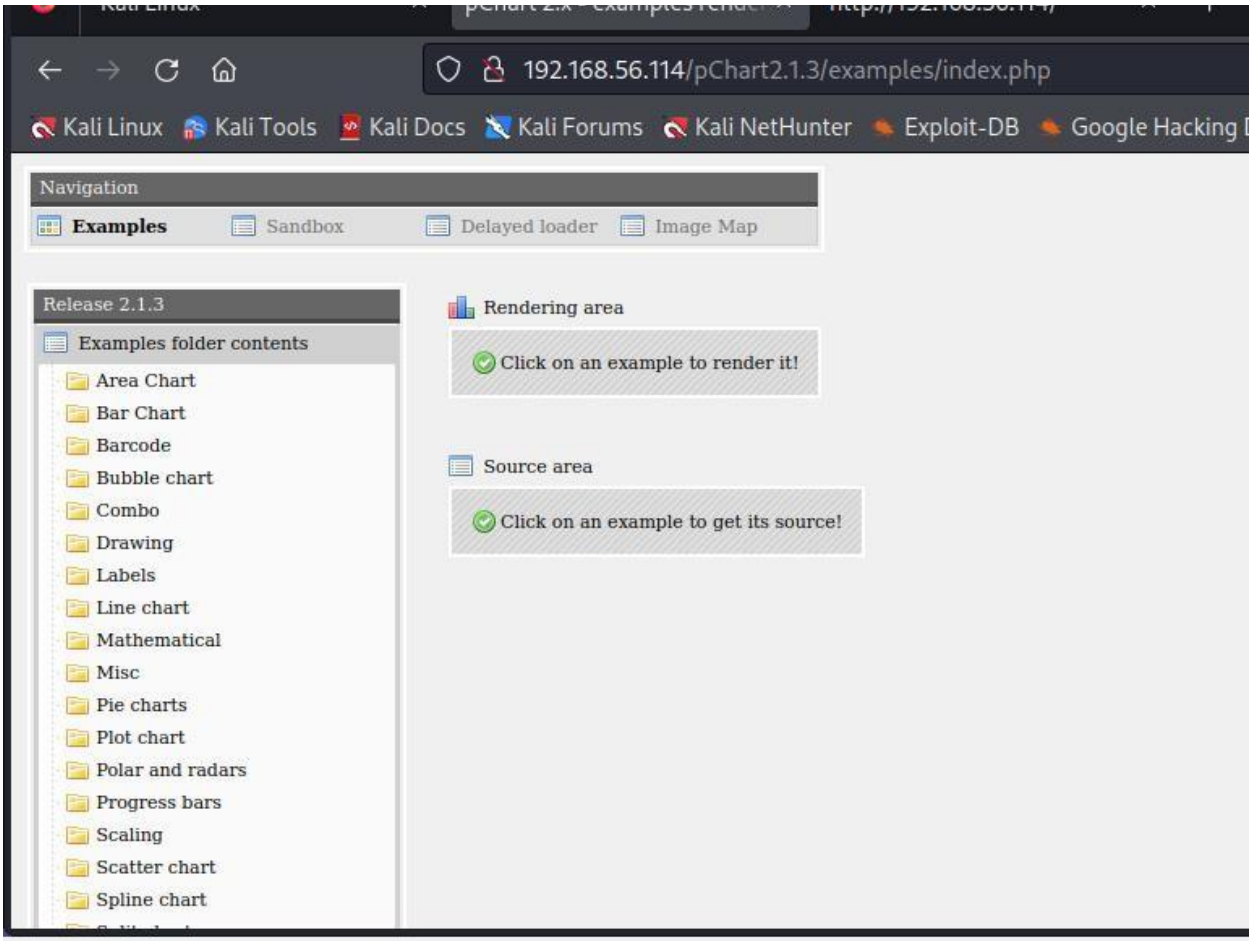
- We do an nmap scan on the kioptrix ip address as shown on the screenshot with the -sV flag for version detection. From the output we deduce that port 22 is closed, port 80 and 8080 are open. The ports 80 and 8080 are running web server.



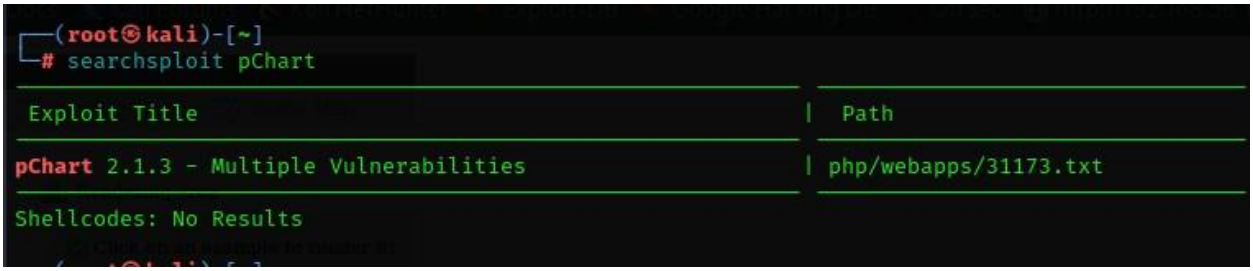
- We take the ip address paste it on the browser and a page is rendered with the message “It works!”. Nothing much!

```
1 <html>
2  <head>
3   <!--
4   <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
5   -->
6  </head>
7
8  <body>
9   <h1>It works!</h1>
10 </body>
11 </html>
12
```

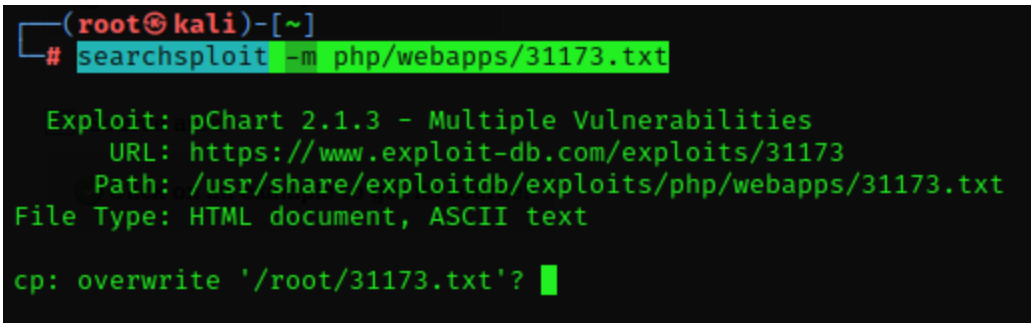
- We then right click on the page and view the source code. We found something nice, a url pChart2.1.3/index.php.



- We hit on */pChart2.1.3/index.php.* the above is displayed.

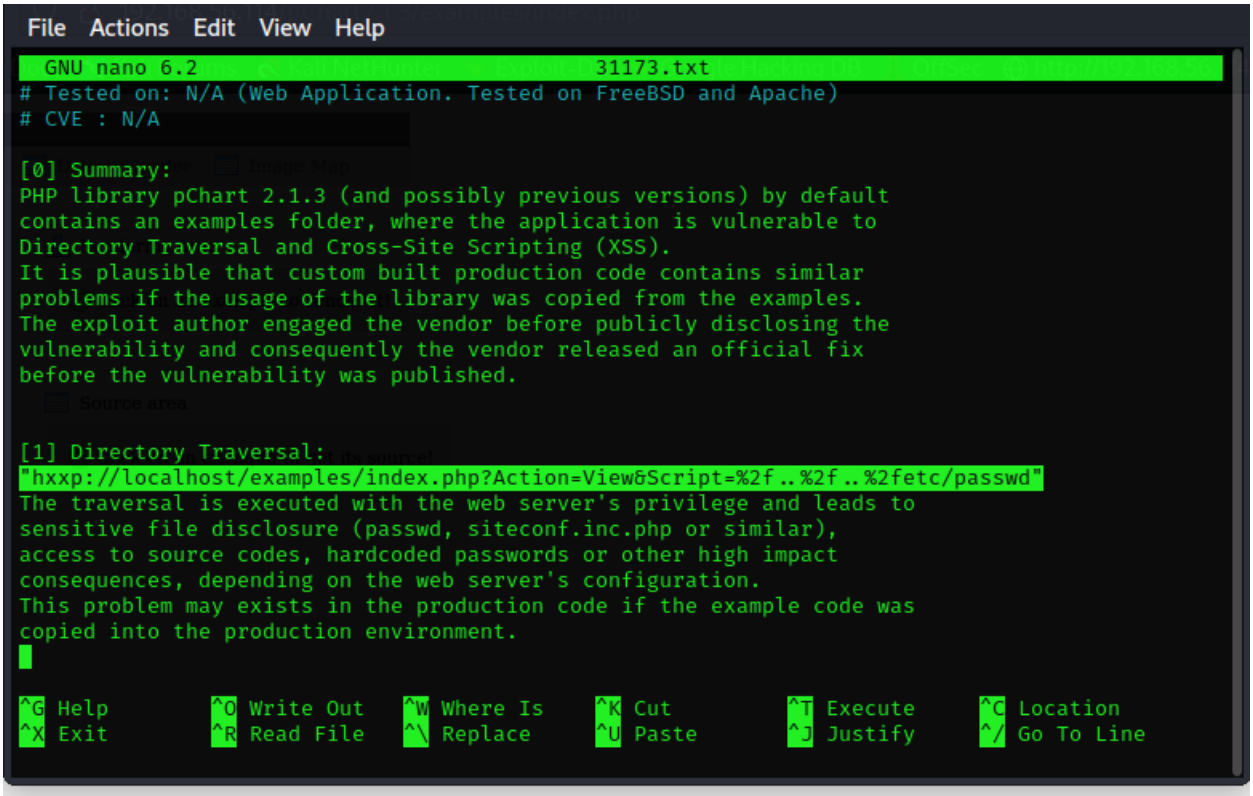


- We do a searchsploit on the tool's name as above and the results is as shown above.

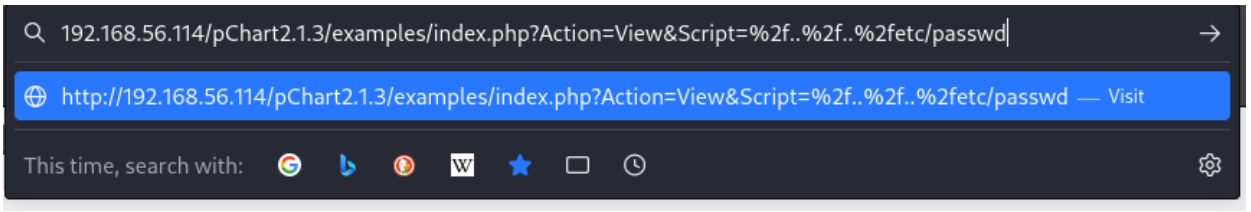


- We Copy the exploit to your current working directory by issuing the highlighted command on the screenshot above, we already copied in advance.

- We do a nano on the file on the screenshot above to see its content.



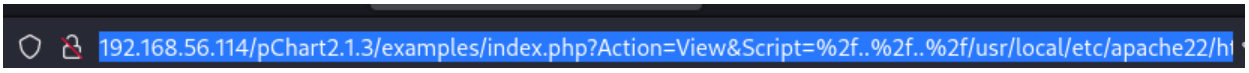
- We navigate to directory traversal and copy the highlighted and edit it.



- After the edit, the url should look as shown in the screenshot above.

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecr:*:1003:1001:User &:/usr/local/ossec-hids:/sbin/nologin
```

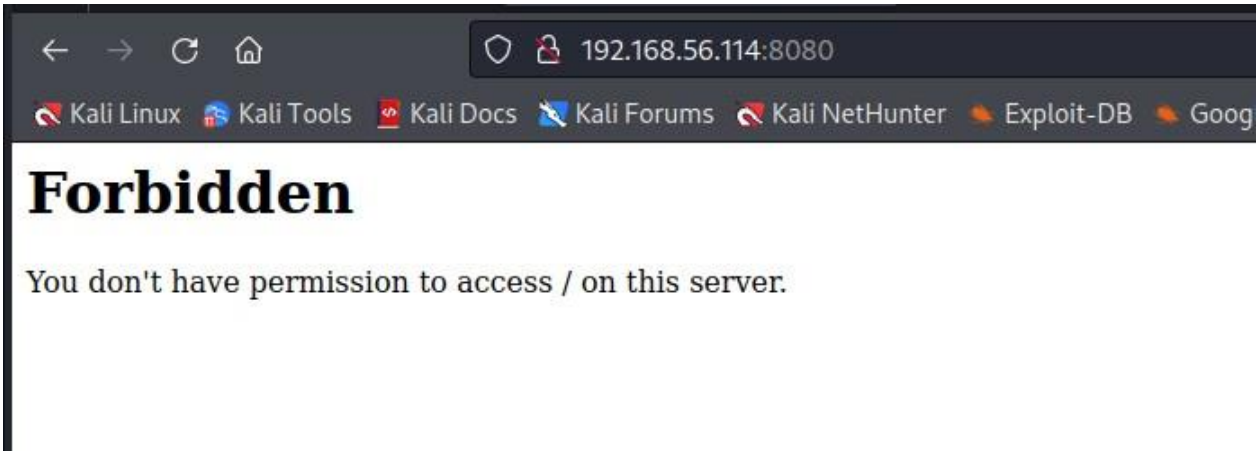
- From the results displayed, we see that the victim runs FreeBSD.



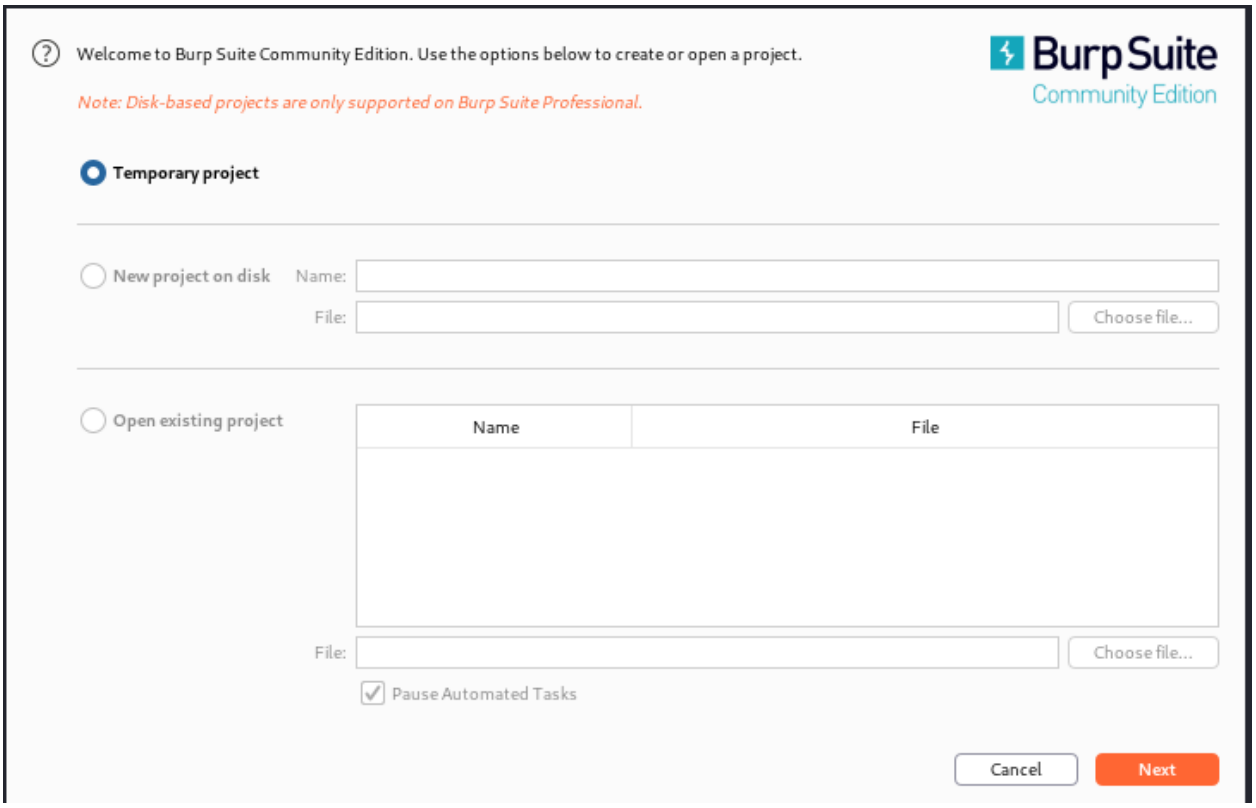
- Since we know the server is running Apache, we search for Apache config file path for FreeBSD and edit the url as above.

```
SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>


</VirtualHost>
```

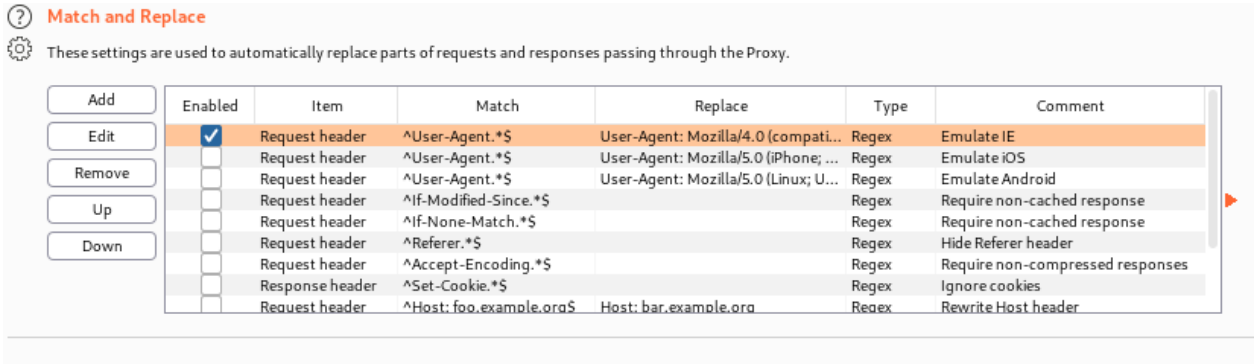
- From the results we see a virtual host running on port 8080. And also not that user agent is set to Mozilla 4.0.



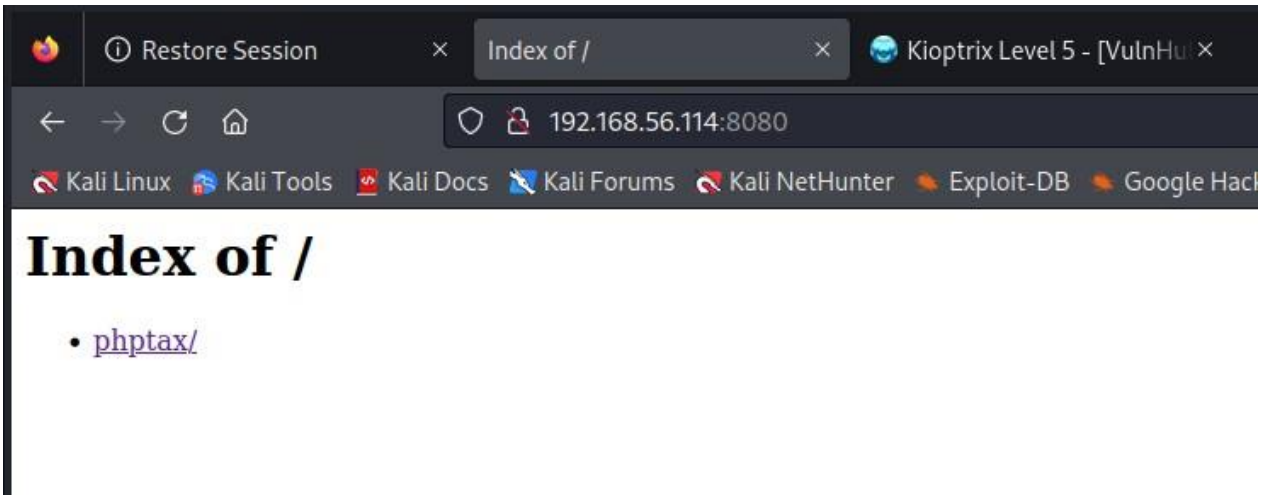
- We try accessing port 8080. No success! Forbidden.



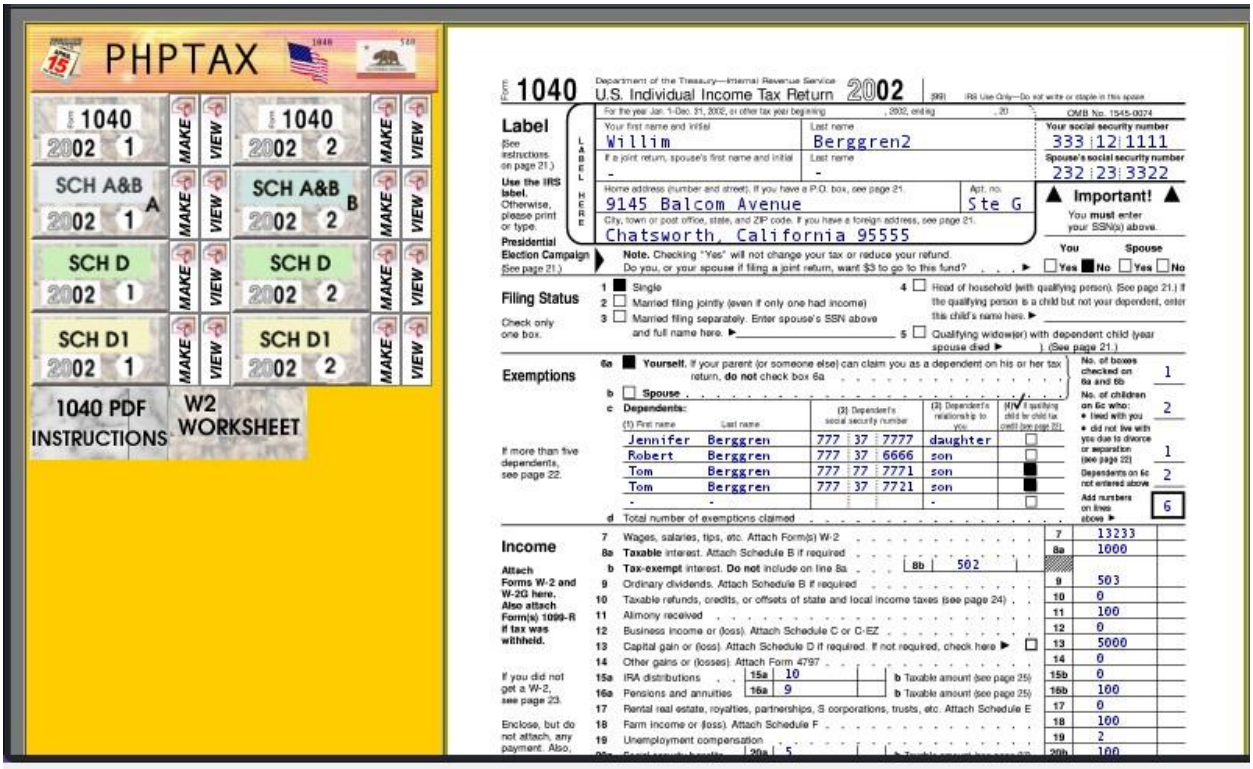
- We power on our burpsuite as above. Since we know the SetEnvIf user agent is set to Mozilla/4.0. We will go ahead and change the user agent via burpsuite.



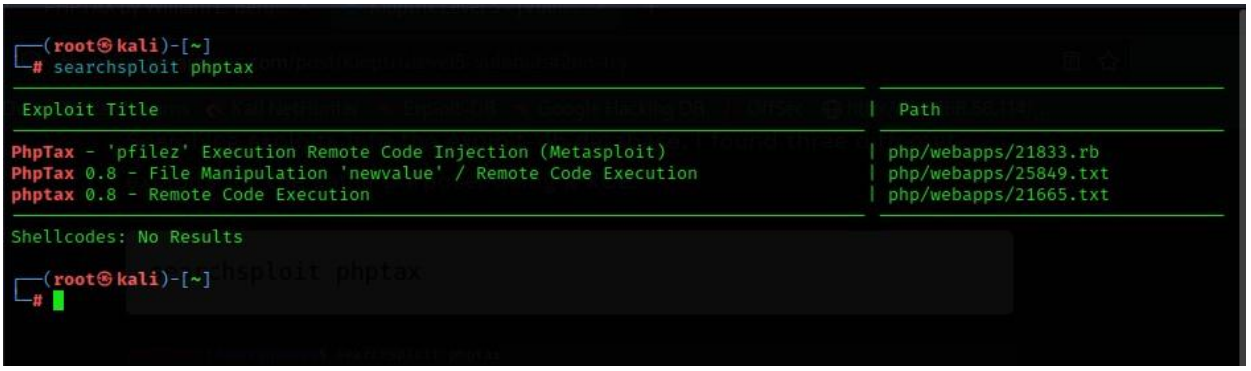
- To change the user agent in burpsuite we navigate to proxy ->options-> then scroll down to match and replace and check the box for user agent Mozilla/4.0 as shown above.



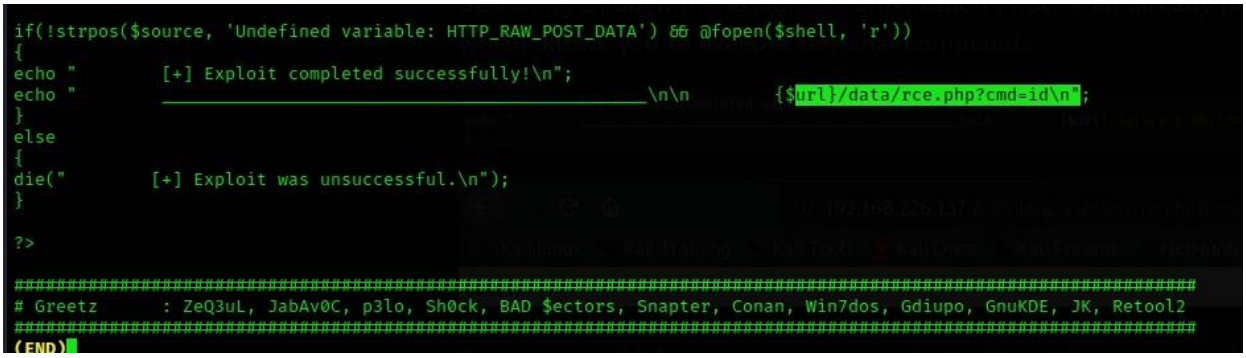
- After changing the user agent, we are now able to access port 8080 as shown above.



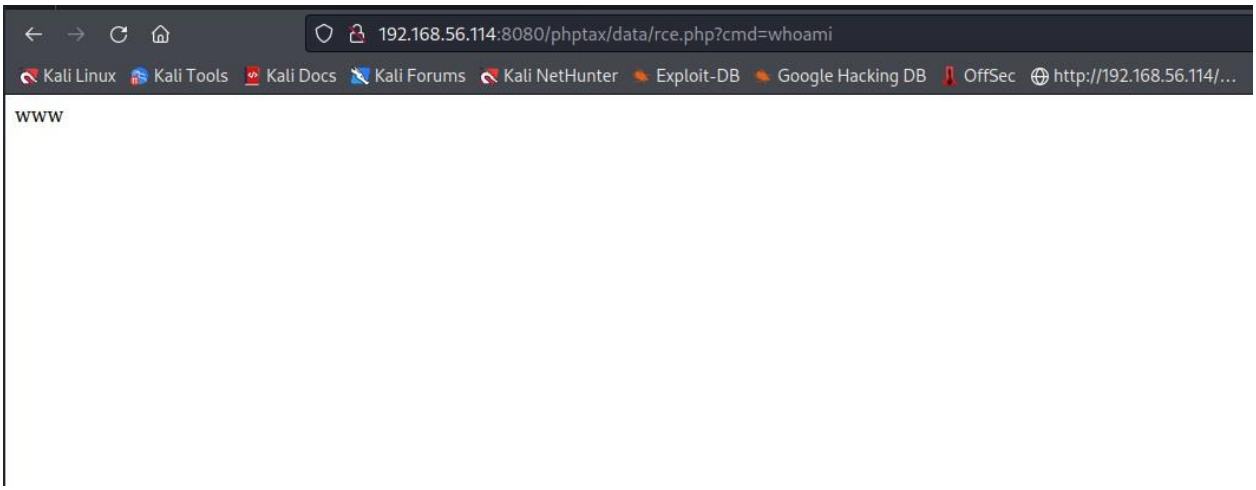
- We click on phptax/ and the above is displayed.



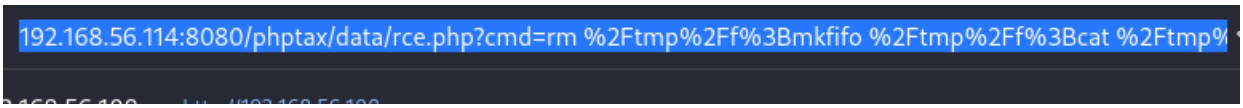
- We do a searchsploit phptax to search for phptax exploits and the results are as displayed in the screenshot above.

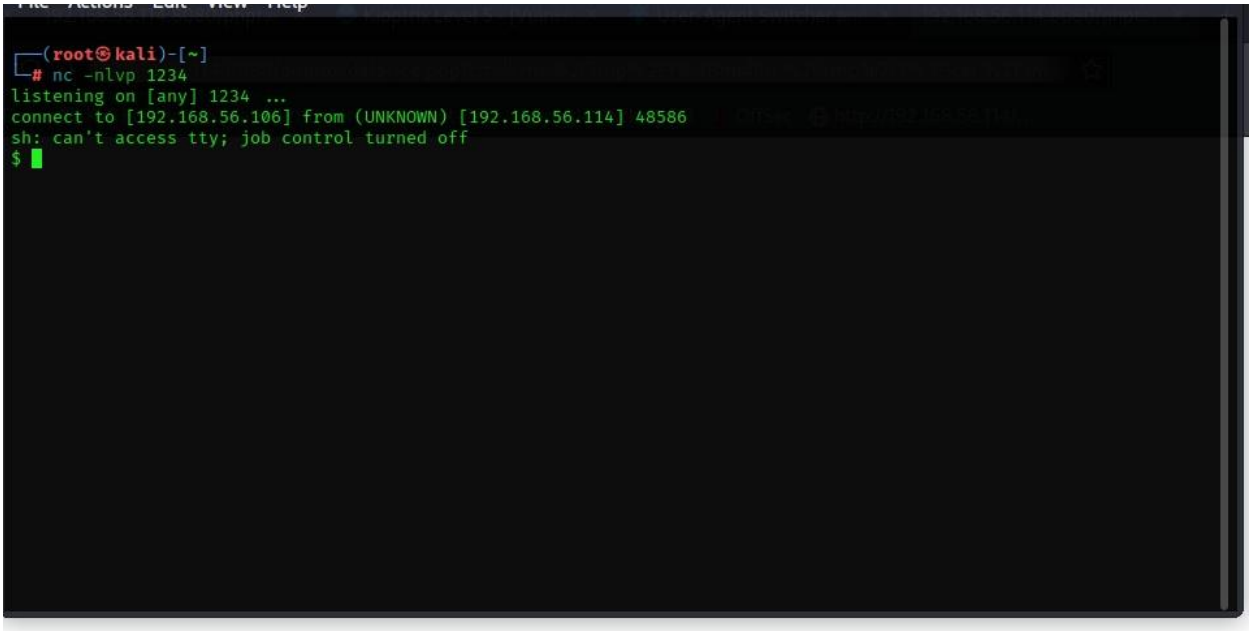


- After going through the documentation of php/webapps/25849.txt, we notice a php file that allow execution of terminal commands.

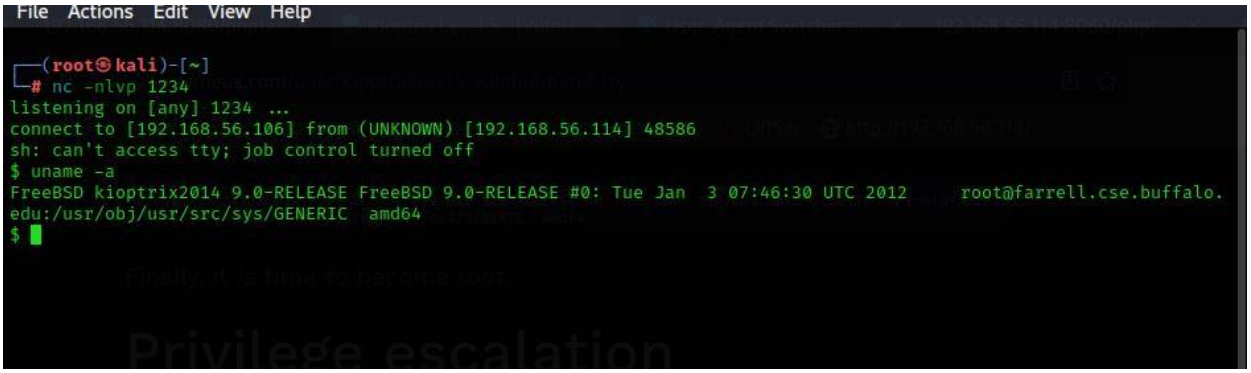


- We try executing whoami command as shown above.



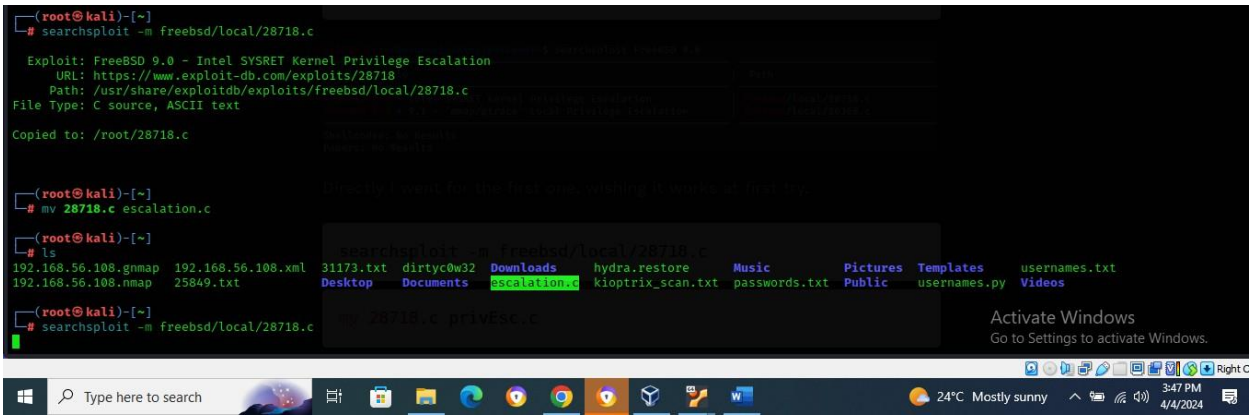


- We got a reverse shell and did and nc to establish connection with the target machine.

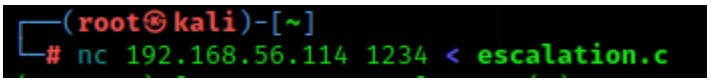


- By issuing a uname -a command, we see that the target machine uses FreeBSD.

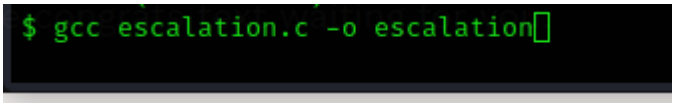
- We search for an exploit for FreeBSD so as to perform privilege escalation.



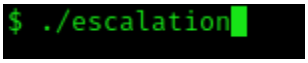
- We copy the file to root and rename the file to escalation.c as shown in the screenshot above.



- We issue the command to send the escalation.c to our target machine.



- We compile the file using the command shown in the screenshot above.



- After that execute.