SAÉ304 Découvrir le pentesting

Mario NGANGA

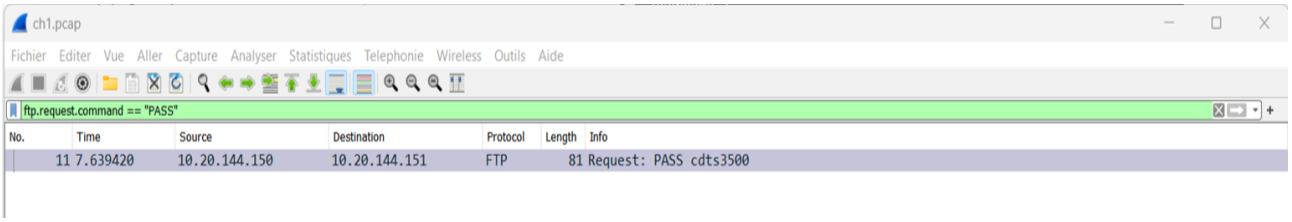
1- FTP Authentification

FTP est un protocole de communication utilisé pour transfert de fichiers entre un client et un serveur sur un réseaux.

J'ai commence d'abord pour télécharger le fichier pcap de ce challenge e après j'ai ouvrir pour faire analyse .

Pour résoudre cette challenge j'ai utilise le commande suivant dans le fritte du wireshark

ftp.request.command == "pass"



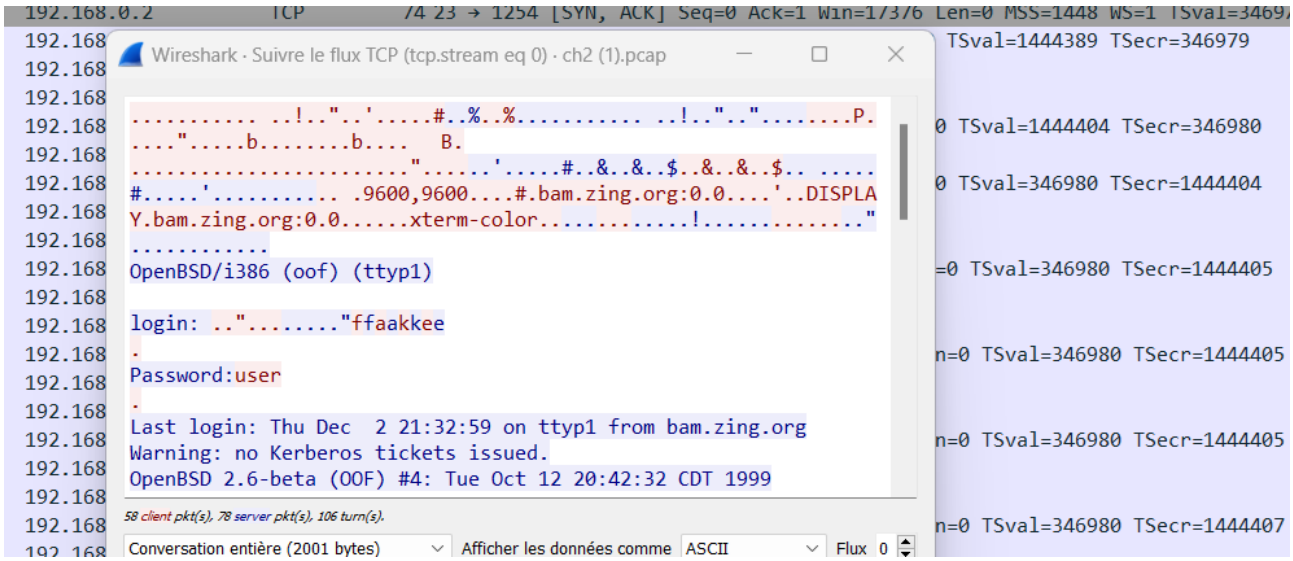
J'ai utilise le commande suivante car me permettre de filtrer tous les informations de wiresharh plus précieusement les informations concernent le mot de pass.

2-TELNET – authentification

Le but est de ce challege est de trouver le mot passe avec le protocole telnet.

Telnet est un protocole réseau qui permet la communication avec un autre périphérique sur Internet ou sur un réseau local en utilisant le protocole Telnet. Il est généralement utilisé pour accéder à distance à des périphériques tels que des serveurs, des routeurs ou d'autres systèmes qui prennent en charge Telnet

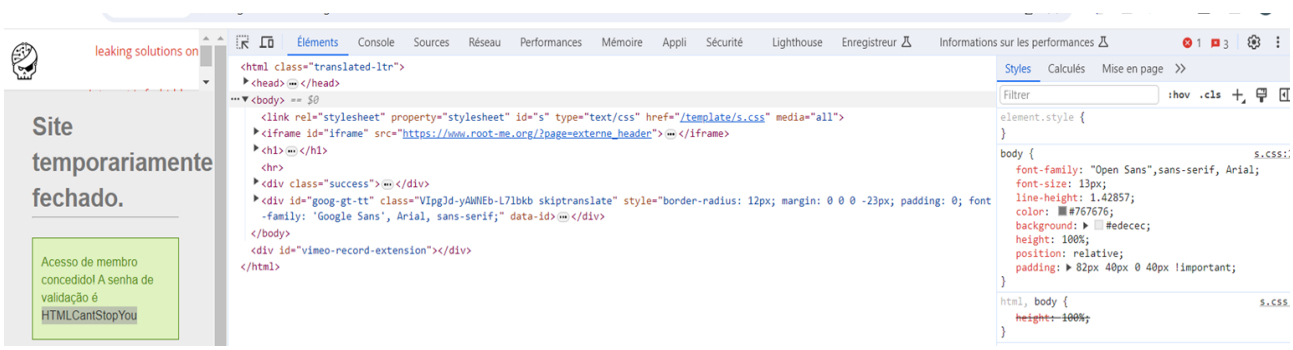
Pour résoudre ce challenge j'ai télécharge le fichier pcap e ensuite j'ai l'ouvrit. J'ai cliqué sur le premier paquet, autrement cliqué droit et ensuite j'ai cliqué dans le suivre et j'ai réussi à regarder le mot de passe.



3-HTML - boutons désactivés

Pour résoudre ce challenge j'ai ouvert l'outil du développer do navigator j'ai édite le code source dans l' input que appartient la partie submit, j'ai simplement remplace la partie disable pour enable de façon activer le bouton.

La capture de écran après faire désactiver le bouton

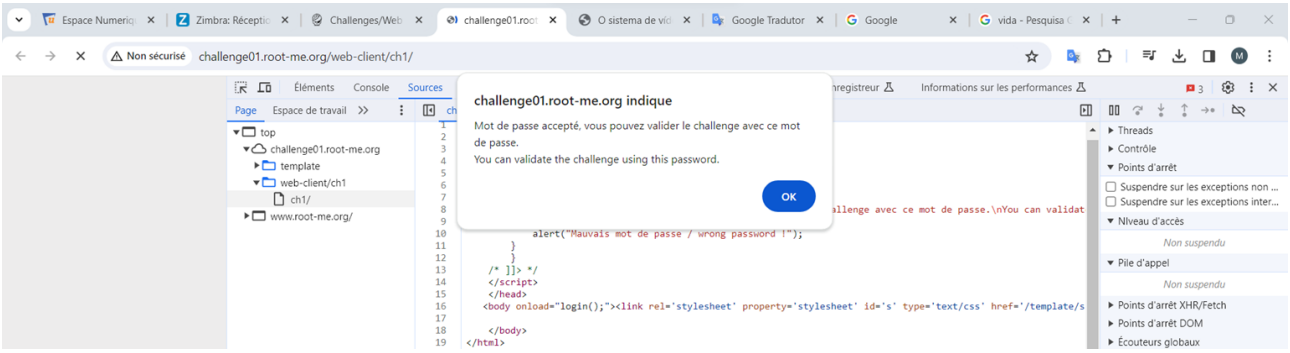


4-HTML - Code source

J’ai inspection seulement le coude source pour résoudre ce challenge et j’ai me rendre compte que le développer de cette application à laisser de bandage le mot de pass

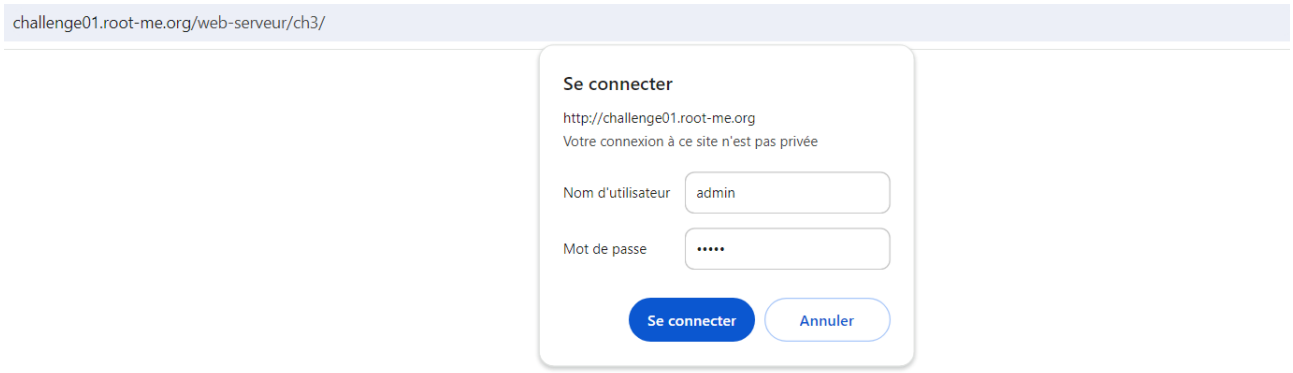
```
-->
<h1> ... </h1>
<form> ... </form> == $0
<!--

Je crois que c'est vraiment trop simple là !

It's really too easy !

password : nZ^&@q5&sjJHev0

-->
```

Capture de écran après mettre le mot de passe dans le page d’accueil.



5-Mot de passe faible

Pour résoudre ce challenge j’ai essaye de mettre le mot de passe admin e aussi login de utilisateur.



Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

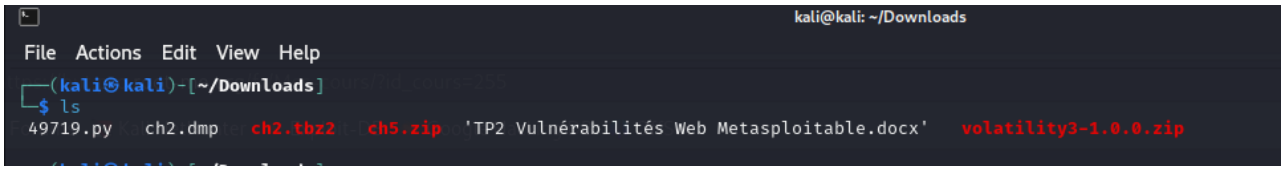
Well done, you can use this password to validate the challenge

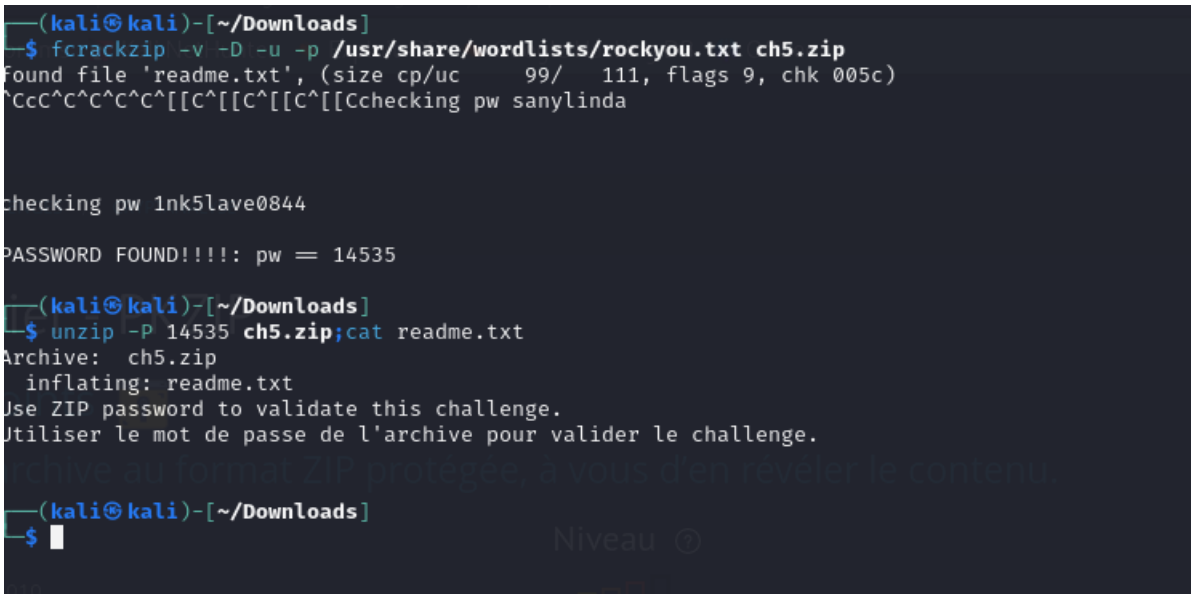
6- Fichier - PKZIP

Pour ce challage j'ai décide de utiliser le fcrackzip.

Fcrackzip est un outil de ligne de commande utilisé pour les attaques par force brute contre les fichiers zip protégés par mot de passe.Le but est de tenter de deviner le mot de passe protégeant le fichier ZIP en essayant plusieurs combinaisons possibles.

J'ai commence pour telechager zip du challenge et ensuite j'ai utilise dezipei le **usr/share/wordlists/rochoux.tzr** de façon être dans format **txt** pout utiliser avec **Fcrackzip .**





-v: Option pour activer le mode verbose (verbeux) qui affiche plus d'informations lors de l'exécution de la commande.

-D: Indique que l'entrée fournie est une liste de mots de passe (un dictionnaire) au lieu d'un jeu de caractères pour la force brute.

-u: Mode unzip. Cela indique que fcrackzip essaiera de décompresser le fichier ZIP avec le mot de passe trouvé pour vérifier si le mot de passe est correct.

-p **usr/share/wordlists/rochoux.txt**: Spécifie le chemin d'accès du fichier contenant la liste des mots de passe à tester.

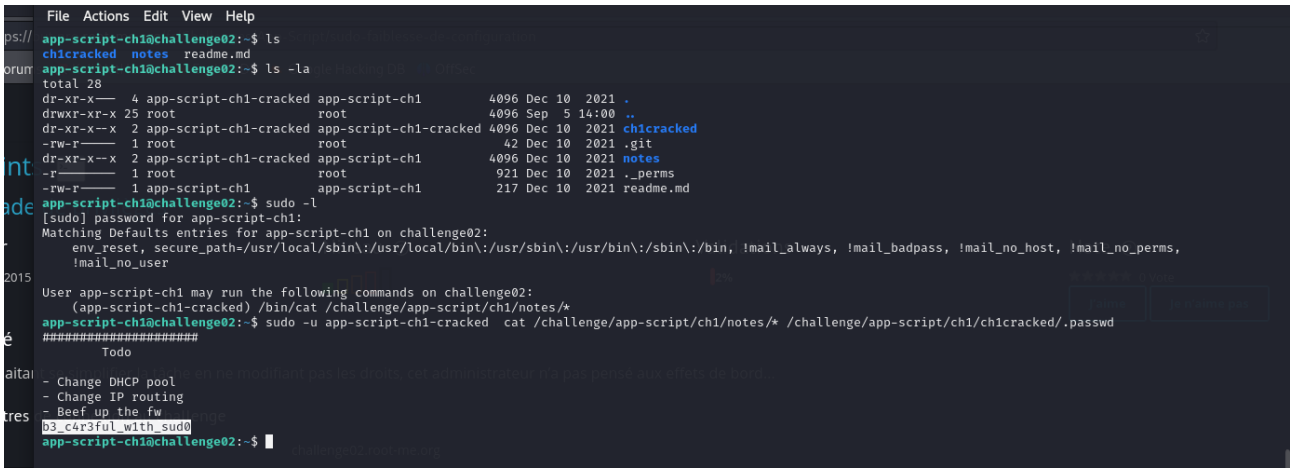
unzip -P 14535 ch5.zip: Cette commande décompresse le fichier ZIP appelé **ch5.zip** en utilisant le mot de passe **-P 14535**. Le paramètre -p est utilisé pour spécifier le mot de passe nécessaire pour décompresser le fichier protégé par mot de passe.

7-sudo - faiblesse de configuration

sudo -l: *Cette commande est utilisée pour lister les privilèges de l'utilisateur pour exécuter des commandes en tant que super utilisateur et aussi permettre de vérifier quelles commandes j'ai peux exécuter avec sudo sans fournir de mot de passe.*

sudo -u app-script-ch1-cracked /bin/ cat /challenge/app-script/ch1/ch1cracked/.passwd*: Basé sur la sortie de* ***sudo -l,*** *Je suis autorisé à exécuter la commande* ***/bin/cat*** *en tant qu'utilisateur* ***app-script-ch1-cracked.***

L'objectif est de lire le contenu du fichier ***.passwd*** *situé dans* ***/challenge/app-script/ch1/ch1cracked/***



8-Python – input()

La fonction input() en Python est utilisée pour recevoir l'entrée de l'utilisateur par le clavier. Il pour l'exécution du programme et attend de l'utilisateur de fournir du texte.

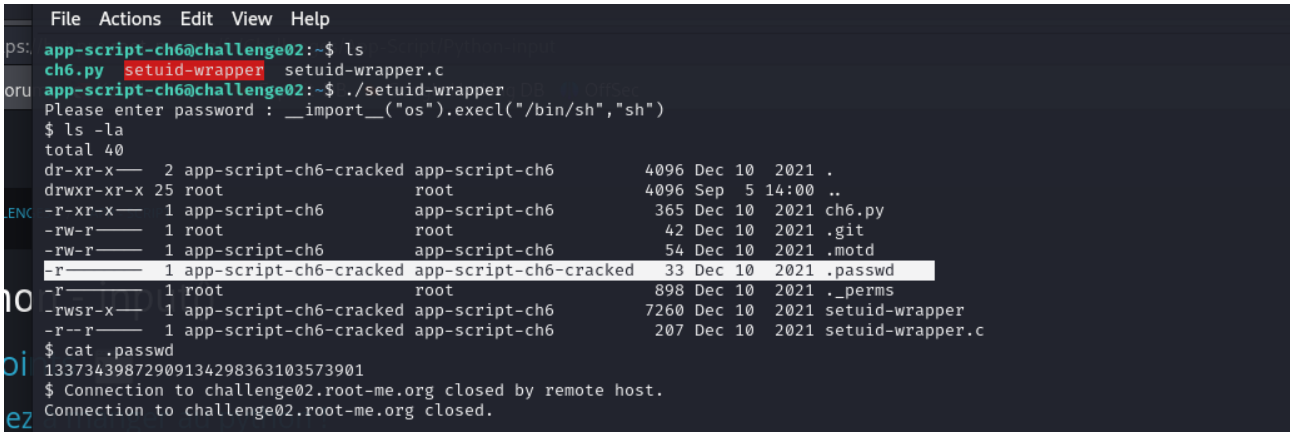
Ce qui se passe ici est une configuration setuid dans un programme appelé setuid-wrapper, qui permet l'exécution de commandes avec les privilèges du propriétaire du programme.

./Setuid-wrapper : J'ai exécuté le programme **setuid-wrapper** et ensuite il me demande le mot passé.

Veuillez entrer votre mot de passe : _____**("os"). Execl("/bin/sh","sh")** : Le programme demande mot passé, mais je suis entré une commande Python déguisée en mot de passe. Cette commande Python utilise la fonction execl pour remplacer le processus courant par un **/bin/sh(/bin/sh)**, lui donnant ainsi accès au shell.

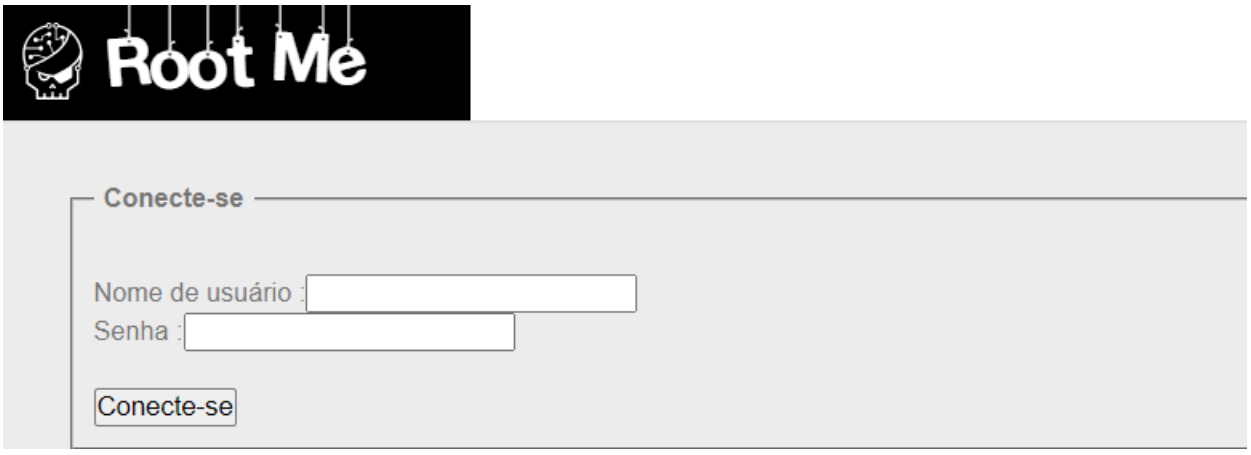
Pour finir, j'ai tapé ls -la pour lister les dossiers et le fichier et voir leurs droits et j'ai remarqué

que le fichier passwd pour le droit de lecture, pour voir le drapeau, j'ai simplement tapé cat . passwd, la capture d'écran montre toutes les étapes que j'ai faites



9- **Javascript – Authentification**

Pour ce défi l'application m'a demandé le login et aussi le mot de passe comme le montre l'image ci-dessous



Pour résoudre j'ai ouvert l'outil de développement et suis allé à l'option qui me permet de voir le code source puis de lire le code j'ai réalisé que dans la condition qui permet à longin il est possible de voir le login et le mot de passe

C'est ainsi que j'ai résolu ce problème.

```
function Login(){
    var pseudo=document.login.pseudo.value;
    var username=pseudo.toLowerCase();
    var password=document.login.password.value;
    password=password.toLowerCase();
    if (pseudo=="4dm1n" && password=="sh.org") {
        alert("Password accepté, vous pouvez valider le challenge avec ce mot de pas
    } else {
        alert("Mauvais mot de passe / wrong password");
    }
}
/* ]]> */
```

10-Encodage – ASCII

Pour résoudre ce défi, j'ai utilisé uniquement le site **https://www.dcode.fr/ascii-code** car un site web me permet de déchiffrer le hachage.