TP : INTRODUCTION À LA SÉCURITÉ LINUX

Année scolaire 2022 - 2023 - Introduction à la sécurité informatique
Enseignant référent : Thibaud ROBIN (trobin@myges.fr)

CONSIGNES

Description

Pour réaliser ce TP, vous serez amenés à collecter 15 chaines de caractères (aussi appelées `flag`). Ces chaines sont obtenues à la suite de la validation de chaque challenge.

Vous vous connecterez à une machine distante avec les identifiants suivants :

- Nom d'utilisateur : `esgi`
- Mot de passe : `esgi`
- Protocole : `SSH`
- Port : `2222`

Le TP s'effectue de façon individuelle. Internet et le cours sont autorisés. Il n'est cependant pas autorisé de communiquer avec les autres étudiants (Discord, Messenger, etc). **L'utilisation de chat (ChatGPT, etc) n'est pas autorisé.**

Rendu

Le rendu s'effectue sur MyGes. Vous devez aussi déposer une copie sur le serveur de fichiers disponible en cours. La correction est automatique. Il est important de respecter les critères suivants :

- Votre rendu est un fichier unique nommé : `{NOM}-{Prénom}-2A{Groupe}.sh`
- La première ligne doit contenir la ligne : `#!/bin/bash`.
- La deuxième ligne doit contenir la ligne : `# {NOM} {Prénom} - 2A{Groupe}`
- Il doit être exécutable par `bash` présent sur la machine d'examen.
- Chaque ligne du script doit contenir une commande permettant de récupérer le flag de chaque challenge.

Vous pouvez vous connecter au serveur de fichier en collant l'ip dans votre explorateur de fichier :

Sous Windows avec l'explorateur

```
\\<IP AU TABLEAU>\TP
```

Sous Linux avec Nautilus

```
smb://<IP AU TABLEAU>/TP
```

Vous devez déposer le script dans le dossier correspondant à votre groupe ! Il est normal de ne pas pouvoir lire le contenu des dossiers.

Suivez l'exemple ci-dessous avec la résolution d'un challenge factice :

> *Challenge factice : vous devez récupérer la première ligne du fichier `robots.txt` du site web https://www.esgi.fr et l'afficher dans la console en une seule ligne.*

Contenu du fichier à rendre nommé `ROBIN-Thibaud-2AFIXME.sh`

```
#!/bin/bash
# ROBIN Thibaud - 2AGroupe-FIXME
curl -s https://www.esgi.fr/robots.txt | head -n 1
```

Ici le robot obtiendra le résultat suivant lorsqu'il testera votre travail.

```
root@20b349c24fc5:~# bash ROBIN-Thibaud-2AFIXME.sh
User-agent: *
```

Pour vérifier que votre script final est correct, vous pouvez le tester de la manière suivante sur la machine d'examen. Il doit avoir un rendu proche de celui ci-dessous :

```
esgi@20b349c24fc5:~# bash ROBIN-Thibaud-2AFIXME.sh
FLAG-1{FIXME}
FLAG-2{FIXME}
FLAG-3{FIXME}
FLAG-4{FIXME}
FLAG-5{FIXME}
FLAG-6{FIXME}
FLAG-7{FIXME}
FLAG-8{FIXME}
FLAG-9{FIXME}
FLAG-10{FIXME}
FLAG-11{FIXME}
FLAG-12{FIXME}
FLAG-13{FIXME}
FLAG-14{FIXME}
FLAG-15{FIXME}
```

Attention à bien respecter les consignes au risque de perdre inutilement des points !

Barème

Sauf indication inverse, chaque challenge vaut 1 point. La note est ensuite convertie sur 20.

CHALLENGES

Challenge 1

Vous devez récupérer le contenu du fichier `/home/esgi/challenge-1/flag-1.txt`.

cat /home/esgi/challenge-1/flag-1.txt

Challenge 2

Vous devez récupérer la valeur du flag dans le répertoire `/home/esgi/challenge-2/`.

for i in {0..9}; do echo "fichier0$i"; echo \n; done

Challenge 3

Vous devez récupérer la valeur du flag dans le répertoire `/home/esgi/challenge-3/`.

for i in {0..10}; do echo "fichier$i"; echo \n; done

Challenge 4

Parmi toutes ces images, une image n'en est pas une. Déduisez-en le flag.

for i in {0..10}; do type "fichier$i"; echo \n; done

Challenge 5

Le flag est morcelé dans le fichier `/home/esgi/challenge-5/file.txt`. Vous devez retrouver tous les morceaux pour reconstituer la chaine finale.

head, tail, grep

- La première partie est située à la ligne **après** la chaine `javvmvtsbeywjasvzbbaqmwccnmtzmaw`.
- La deuxième partie est située à la ligne **avant** la chaine `urosygmimlmoichpyezbfziaiarubuyt`.
- La troisième partie est située 3 lignes **après** la chaine `eakprodnurhzqtlvsogprkzvdgfszlww`.
- La quatrième partie est située 3 lignes **avant** la chaine `azmewuwszxnsbklpeqgcuzfzaokcpbgf`.
- La cinquième partie est située ligne `9928`.

Votre script doit afficher le flag sur une seule ligne (ex : `FLAG-5{2f9a944db9fcd3d87b85e7c36a0330b11665fd7353941dea6f18d83cbeada70d}`)

```
grep "javvmvtsbeywjasvzbbaqmwccnmtzmaw" test.txt && grep -B0 urosygmimlmoichpyezbfziaiarubuyt test.txt && grep -A 3 "eakprodnurhzqtlvsogprkzvdgfszlww" test.txt | tail -1 && grep -B 3 "azmewuwszxnsbklpeqgcuzfzaokcpbgf" test.txt | head -1 && sed -n 20p test.txt
```

Challenge 6

Vous devez trouver le flag dans le fichier `/home/esgi/challenge-6/file.txt`.

grep file.txt

Challenge 7

Vous devez trouver un moyen de décoder le fichier `/home/esgi/challenge-7/file.txt`.

base64 -d file.txt

Challenge 8

Vous devez trouver un moyen de déchiffrer le flag présent dans `/home/esgi/challenge-8/file.txt`.

cat file.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

Challenge 9

Le répertoire `/home/esgi/challenge-9/` contient 500 fichiers. Le fichier contenant le flag est d'une taille de 86 octets et possède 6 lettres a.

find -c 86 *aaaaaa*

Challenge 10

Le flag du challenge 10 est situé quelque part sur la machine. Son nom de fichier est `flag-10.txt`.

find / flag-10.txt

Challenge 11

Le fichier `/home/esgi/challenge-11/archive.zip` a été compressé une dizaine de fois avec des mécanismes de compression différents. Décompressez le tout et retrouvez le flag.

file archive.zip = gz
mv archive.zip archive.gz
gunzip archive.gz

file archive
mv archive archive.tar
tar -xf archive.tar

xxd -r = ASCII

bz2 -d = .bz2

Challenge 12

Vous devez lire le contenu du fichier `/home/flag-12/flag-12.txt`. Or il n'est accessible qu'à travers l'utilisateur `flag-12`.

Des informations sont à votre disposition dans le dossier `/home/esgi/challenge-12/`.

cat /home/esgi/challenge-12 | nt localhost

Challenge 13

Du code source est disponible dans le répertoire `/home/esgi/challenge-13/`. Retrouvez les changements dans le code pour déceler le flag.

diff passwords.txt

Challenge 14

Un service est à votre disposition sur le port `1444` de l'hôte local de la machine d'examen. Le mot de passe pour s'y connecter est `5rf3L0pmd3k5md2`.

Il manque cependant la dernière lettre du mot de passe pour obtenir le flag. Retrouvez la pour valider ce challenge.

```
echo "5rf3L0pmd3k5md2?" | nc localhost 1444
```

Challenge 15

Un service est à votre disposition sur le port `1555` de l'hôte local de la machine d'examen.

Le jeu est simple : vous devez retrouver un chiffre aléatoire entre 0 et 1000. Vous n'êtes pas limité sur le temps et les requêtes à effectuer.

Attention ! Le nombre à deviner change à chaque nouvelle connexion au service. Assurez-vous de ne pas vous déconnecter.

Testez votre script avant de le déposer sur MyGes et sur le serveur de fichier ! Merci et bon courage ! 😊

```
for i in {0..1000}; do echo "$i" | openssl s_client -quiet \ -connect localhost:1555 2> /dev/null; done
```