Auteur: Nicolas C. - Campus Fenelon Notre Dame - La Rochelle, 2023 - 2024

3. TP Brute Force maison

TP Brute Force maison

v 0.2

Mise en place

- Un serveur SSH basé sur Docker est mis à disposition des étudiants.
- Le serveur SSH doit disposer d'un utilisateur **userfaible**

Pré requis

- Notion de l’attaque Force brute
- Dictionnaire
- SSH

Activité 1 - Exécuter le code

Exécuter le code suivant.

```
import paramiko
# https://www.paramiko.org/

# Infos
host="127.0.0.1"
username="user1"
password="user1"
port=2222

pirate=False

try:
    # Connexion
    client = paramiko.client.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    client.connect(host, username=username, password=password, port=port)
    pirate=True

except:
    pirate=False
    client.close()

if pirate:
    command = "tail /etc/passwd" # On peut voir la liste des utilisateurs sur la machine
    _stdin, _stdout, _stderr = client.exec_command(command)
```

```
    print ("Sortie")
    print( _stdout.read().decode() )

client.close()
```

(les 3 valeurs pour **host**, **username**, **password** seront fournies).

Activité 2 - Modifier le code

Il y a l'utilisateur **userfaible** sur la machine **172.16.XX.XX**.

Proposer une solution pour que l'*utilisateur/pirate* saisisse la valeur **password** pour tenter de pirater le compte **userfaible**.

Le programme doit dire si le mot de passe est correct ou incorrect.

Activité 3 - Lire un fichier externe

- Créer le fichier texte **file.txt** dont le contenu est:

```
Bonjour
Hello
Azerty
password
```

- Exécuter le code Python suivant:

```
# Ouvrir le fichier en lecture seule
file = open("file.txt", "r")

# Utiliser readlines pour lire les lignes du fichier
```

```
# La variable "lignes" est une liste contenant toutes les lignes du fichier
lines = file.readlines()

# Fermer le fichier après avoir lu les lignes
file.close()

# Itérer sur les lignes
for line in lines:
    print (line.strip())    # Juste pour le test # Stip pour enlever le saut de ligne
```

> Que fait ce code ?

Activité 4 - Rassembler les fonctionnalités

> Préparer un fichier texte avec des mots de passe populaires.

> Faire un programme Python afin de faire une attaque sur le mot de passe de l'utilisateur *userfaible*, en utilisant ce fichier.