Mission

Club*Nix

ESIEE Paris

December 9, 2024

Contents

IMPORTANT: Il n'y a pas d'ordre pour les missions bonus, amusez-vous à faire ce qui vous tente !

1 Mission principale

1.1 Description de votre mission

Bonjour à tous, nous sommes du Nix, une organisation rivale aux anonymous œuvrant pour le libre et l'open source !
Nous sommes ici pour recruter nos prochains membres de l'organisation qui seront sous les ordres du célébrissime Isnubi, chef de la division d'attaque. Sous ses ordres ? Nos meilleurs éléments, Mewone, DD, Wida, Enderend et ZEN responsables de la chute des systèmes informatiques Russes et Américains pendant près de 9h. Pour se faire, chaque binôme doit récupérer un fichier d'une importance extrême, mais... là est le hic, il se trouve sur le pc de vos adversaires. Pour rappel, tout bon hackeur n'utilise pas Windows mais Linux ! Une liste de commande avec des explications vous sera donnée. Chacun d'entre vous s'est illustré en infiltrant nos locaux. Maintenant ? C'est à nous de vous tester pour déceler les perles rares qui se trouvent parmis vous. La ligne d'arrivée ? Déchiffrer le fichier récupéré sur le PC de vos adversaires.

1.2 Vos objectifs

- Vérifier la connexion du PC de vos adversaires
- Scanner les ports de la machine adverse
- Vous connecter sur le PC de vos adversaires et récupérer le fichier
- Déchiffrer le fichier pour obtenir des informations confidentiels

Chères recrues nous comptons sur vous pour œuvrer dans le bien. Le premier binôme qui réussit à récupérer et déchi le fichier remporte le jeu. Préparez-vous à relever le défi et à montrer vos compétences en matière de hack !

1.3 Hints

1.3.1 Vérifier la connexion du PC de vos adversaires

Commandes possibles:

- ping
- nmap
- ip a

1.3.2 Scanner les ports de la machine adverse

Commandes possibles:

- nmap
- ping
- sudo

1.3.3 Vous connecter sur le PC de vos adversaires et récupérer le fichier

Commandes possibles:

- ssh
- scp
- ls
- cd
- hostname

1.3.4 Déchiffrer

Commandes possibles:

- Exection de code
- Execution de code python
- Rappels programmation et Python

2 Missions Bonus

2.1 Programmation

2.1.1 Minimum et Maximum

Réaliser un programme permettant de trouver la valeur minimale et/ou maximale d'une liste d'entiers.

```
liste = [5, 8, 9, 4, -3, -5, 2, 11]

"""
Trouver le minimum et le maximum (et on vous voit les ptits malins qui savent qu'il y a des
fonctions qui le font automatiquement !)
"""
```

2.1.2 Afficher l'inverse

Affichez une chaîne de caractères (dont la taille est supérieure à 3) à l'envers.

2.1.3 Palindrome

Vérifiez si une chaîne de caractères est un palindrome ou non !

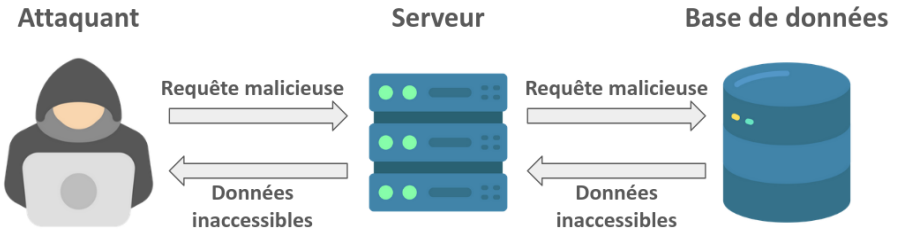
2.1.4 Fibonacci

Ecrivez une **fonction** qui affiche la suite de fibonacci pour **n** entiers donné.

2.2 Vous reprendrez bien un peu de hacking ?

2.2.1 Injection SQL

Qu'est ce qu'une Injection SQL ? Une injection SQL est une attaque visant à créer des demandes spécifiques dans le but de manipuler illégalement une base de données.
Pour ce faire on utilise un langage nommé le **SQL** (Structured Languague Query) qui est le langage permettant de manipuler la plupart des bases de données.
Dans le cas d'exemple ci-dessous, nous allons intégrer des informations un peu spéciales aux champs "username" et "password" dans la requête pour pouvoir passer au travers de la vérification et ainsi obtenir. Les informations même si nous ne connaissons pas le mot de passe administrateur.



Pour cette mission:

- Aller sur le site sqliteonline.
- Exécuter le script n°1 en copiant collant le contenu et en appuyant sur ”run”, la flèche verte en haut. En cas de problème avec le contenu de la Base de données, n'hésitez pas à l'exécuter à nouveau pour réinitialiser.
- Vérifiez le résultat du script avec les commandes SELECT * FROM Admin; et SELECT * FROM Secrets;
- Ouvrez un éditeur de code, collez-y le script n°2 et modifiez les valeurs de **username** et **password** présents au début du script.
- Exécutez le script et tentez d'exécuter la requête obtenue sur le site web. Si vous obtenez en dessous de l'éditeur de texte l'affichage du ”supersecretpassword”, **C'est Gagné !**

Script n°1 : Il permet de créer une simple base de données contenant des infos ”Secrètes” et des infos sur les ”Admin”. Ne vous attardez pas sur le code:

```
DROP TABLE IF EXISTS Demo;
DROP TABLE IF EXISTS Admin;
DROP TABLE IF EXISTS Secrets;

CREATE TABLE IF NOT EXISTS Secrets (
    id INT PRYMARY KEY,
    supersecretpassword VARCHAR(25) NOT NULL
);

CREATE TABLE IF NOT EXISTS Admin (
    id INT PRYMARY KEY,
    username VARCHAR(25),
    password VARCHAR(25)
);

INSERT INTO Secrets VALUES(1, "nixforever");
INSERT INTO Admin VALUES(1, "enderend", "azertyuiop");
```

Script n°2 (script python):

```
username = ""
password = ""

r = f"SELECT s.supersecretpassword FROM Secrets s, Admin a WHERE a.username = '{username}'
AND a.password = '{password}';"

print(r)
```

Que faut-il savoir?

- Si on trouve un ”OR” dans une condition, il suffit qu'une seule condition soit ”Vraie” pour passer.
- La chaîne ” est égale à la chaîne ”.
- La requête qui sélectionne le secret si le nom et le pseudo et le mot de passe correspondent entoure ces derniers de simple guillemets pour pouvoir obtenir du **texte** et le comparer avec les valeurs de la base de données.
- **Indice** : La méthode la plus simple consiste ‘a laisser vide le champ username et à mettre votre injection dans le champ password.
- **Indice** : Essayez d'éxécuter le script sans mettre d'informations dans les champs pour voir à quoi ressemble la condition.

2.2.2 Découvrir un peu plus

Intéressé par la cybersécurité ? Essayez les cours de **TryHackMe**, très complets et intéressants qui permettent une bonne introduction à ce vaste univers !