Coding CLUB

Crypt1ge des Inf0rmat10ns

Coding CLUB 0
Installation des programmes 2
Installation de Python 2
Installation de Nmap 2
Installation de VSCode 2
Contexte 3
Decrypt Course 3
Decrypt Course – Explications 3
Testez votre programme 4
Avancée majeure 4
Executez « nmap » 4

Installation des programmes

Installation de Python

1. Allez sur https://www.python.org/
2. Appuyez sur « Downloads » puis « Download Python »
3. Exécutez le fichier téléchargé
4. Cochez « Add python.exe to PATH »
5. Appuyez sur « Customize Installation »
6. Décochez tout sauf « PIP » et « For all users (Requires admin privileges) »
7. Appuyer sur « Next »
8. Décochez tout
9. Cochez « Add python.exe to environment variables »
10. Terminez l'installation !

Installation de Nmap

1. Allez sur https://nmap.org/dist/nmap-7.95-setup.exe
2. Décochez tout sauf « Nmap Core »
3. Terminez l'installation !

Installation de VSCode

1. Allez sur https://code.visualstudio.com/docs/?dv=win64user
2. Ouvrez l'exécutable d'installation et suivez les instructions d'installation classiques
3. Terminez l'installation !

Contexte

Vous incarnez l'un des agents de la cybersécurité de la « Santa Corp. », votre mission est de récupérer les données volées de la compagnie après que des hackers de la « Fouettard Inc. » se soient introduits dans le réseau et chiffrées les données.

Vous serez équipé de vos ordinateurs, du langage de programmation Python, ainsi que des **Cobras, une force d'élite pouvant vous aider en cas de tout pépin**.

Decrypt Course

// RECEPTION DE MESSAGE //

Je sais pour qui vous travaillez. Je vous ai envoyé un fichier zip, il contient des données en rapport avec la fuite « Santa Corp ». Il contient un fichier avec un message, crypté semble-il. J'ai essayé de faire un script en python permettant de le décrypter, mais je n'ai plus assez de temps. Il est lié avec le fichier texte, peut-être arriverez-vous a en examiner les contenus.

A vous de trouver l'algorithme et le décalage. Bonne chance.

Après avoir reçu ce message mystérieux, il semble judicieux de maintenant ouvrir le fichier en question.

« fuite.zip »

Le fichier contient :

- Du code a trou pouvant être complété à partir de ressources trouvées internet.

Decrypt Course – Explications

Après avoir ouvert le fichier, il semble être fait uniquement de lettres et de chiffres, leur composition semble illogique, mais le fichier semble être composé de mots, et semble former une phrase, même si elle est dénuée de sens. **Tout s'apparente à un « Chiffrage César ».**

Le « Chiffrage César », existant depuis l'Antiquité, consiste à décaler chaque lettre d'un cran positif ou négatif dans l'Alphabet.

- Un décalage de **+1** sur le mot **« Mot »** donnera **« Npu »**
- Un décalage de **-1** sur le mot **« Mot »** donnera **« Lns »**
- Un décalage de **+1** sur la phrase **« Cinq 5 cinq »** donnera **« Djor 5 djor »**
- Un décalage de **-1** sur la phrase **« Cinq 5 cinq »** donnera **« Bhmp 5 bhmp »**

L'objectif ici serait de compléter le script python, à partir des ressources disponibles sur Internet et de l'aide donnée par les Cobras, afin de décrypter le fichier.

Il faut :

- Ouvrir le fichier dans le programme
- Demander le décalage à l'utilisateur
- Déchiffrer le fichier à partir des données obtenues et d'un algorithme de déchiffrage du code césar
- Afficher les données déchiffrées

Testez votre programme

- Ouvrez une invite de commande / terminal (En faisant la touche Windows plus la touche 'R' (Win + 'R'))
- Entrez la commande « python decrypt.py »

Si la commande « python » n'existe pas, vérifiez votre installation et essayez avec « python.exe » ou « python3 » ou « python3.exe »

Avancée majeure

Félicitations ! Vous avez réussi à décrypter le fichier, et vous avez obtenu la clé pour décrypter les fichiers du Serveur A, mais celles du Serveur B sont toujours bloquées. Mais la mission n'est pas encore finie, agent. Vous savez maintenant ou les données sont stockées, mais vous ne savez pas encore comment les extraire.

La piste semble rediriger vers un serveur avec une **« adresse IP ».**
Une **adresse IP** est un identifiant numérique attitré a un ordinateur connecté à un réseau et/ou à Internet. Il est composé de quatre chiffres allant de 0 à 255. (Ex : 192.168.0.1). L'adresse IP ici semble rediriger vers un serveur local. Cependant, quand on essaye d'accéder au serveur via une page internet, l'on n'obtient rien.
Etrange.

Peut-être que le serveur semble nous cacher quelque-chose.

Ici, le logiciel **« NMap »** va nous aider.
NMap est un programme permettant de scanner les ordinateurs ainsi que leur **« ports »**. Les ports sont comme des portes que les programmes utilisent pour communiquer avec les réseaux auxquels ils sont connectés. Par exemple, la majeure partie des sites web tournent sur le port 80, 443, 8000 ou 8443. NMap identifie les ports de trois manières, ouverts (« open »), filtrés (« filtered »), et fermés.

- Si le port est ouvert, tout le monde connecté au réseau peut y accéder.
- Si le port est filtré, seuls les utilisateurs configurés dans l'ordinateur peuvent y accéder.
- Si le port est fermé, personne ne peut entrer.

NMap nous aidera ici à voir quels ports le serveur semble ouvrir, et par conséquent par quelle interface pourrions-nous interagir avec. Cela nous permettra de l'examiner plus en profondeur et de potentiellement récupérer la clé de déchiffrage du second serveur.

Executez « nmap »

- Ouvrez une invite de commande / terminal (En faisant la touche Windows plus la touche 'R' (Win + 'R'))
- Entrez la commande « nmap <adresse ip> »

Si la commande « nmap » n'existe pas, vérifiez votre installation et essayez avec « nmap.exe ».