Projet Sécurité: CTF

GROUPE	BACKDOOR	**SCENARIO 21/10**
PHASE 1	DEVELOPPEMENT CTF	***Réseaux***
NIVEAU	FACILE	

RESEAU INFILTRE : UNE ENQUETE UNIVERSITAIRE

L'université est confrontée à une situation d'infiltration potentielle de son réseau. L'administrateur réseau de l'université a réussi à intercepter une communication réseau suspecte entre des dispositifs inconnus sur le réseau de l'université. Les participant incarnent des étudiants en sécurité informatique qui ont été recrutés pour enquêter sur cette menace. Prêt à relever le défi de la sécurité du réseau de l'université XYZ ?

Les participants ont pour rôle l'identification de la menace potentielle, l'administrateur réseau leur fournira un fichier de capture Wireshark contenant des paquets chiffrés provenant de la communication suspecte sur le réseau de l'université. Les participants devront être capable d'effectuer l'analyse de paquets et le décryptage des chiffrements.

Temps estimé: 10 mins

Pour cela, ils devront utiliser Wireshark ainsi que d'autres outils de décryptage.

Défis :

Les participants identifient les messages spécifiques contenant des flags cachés dans les communications liées à chaque protocole. Chaque protocole a son propre flag à découvrir.

1. **Identification des Paquets Telnet**

Analysez le fichier de capture pour identifier les paquets associés au protocole Telnet.

Identifiez les messages spécifiques chiffrés dans les paquets Telnet qui contiennent le flag caché.

2. **Identification des Paquets Netcat**

Analysez le fichier de capture pour identifier les paquets associés au protocole Netcat.

Identifiez les messages spécifiques chiffrés dans les paquets Netcat qui contiennent le flag caché.

3. Identification des Paquets IRC

Analysez le fichier de capture pour identifier les paquets associés au protocole IRC.

Identifiez les messages spécifiques chiffrés dans les paquets IRC qui contiennent le flag caché.

4.**Déchiffrement des messages CHIFFRE DE CESAR**

Déchiffré les messages afin de retrouver les flags.