TELNET - Authentification

1. Présentation du challenge

- **Objectif** : Retrouver le mot de passe de l'utilisateur dans une capture réseau de session TELNET1.
- **Fichier fourni** : `ch2.pcap` 2.

2. Analyse du protocole

Le protocole **Telnet** présente une vulnérabilité critique car il a été conçu à une époque où la sécurité n'était pas une priorité3.

- **Transmission en clair** : Toutes les données échangées (y compris les identifiants) ne sont pas chiffrées4.
- **Risque de sécurité** : Une interception du trafic permet à une personne malveillante de récupérer facilement le nom d'utilisateur et le mot de passe5.
- **Usage actuel** : À bannir sur Internet ; acceptable uniquement sur un réseau local fermé en l'absence d'alternative6.

3. Méthodologie de résolution

Étape 1 : Analyse avec Wireshark

L'ouverture du fichier `.pcap` dans Wireshark permet d'observer les échanges entre deux machines7.

- **Observation initiale** : Les trois premiers segments TCP montrent une ouverture de connexion (**SYN, SYN/ACK, ACK**)8.
- **Localisation des données** : Les informations de connexion se trouvent dans les segments suivant l'établissement de la session9.

Étape 2 : Utilisation de "Follow TCP Stream"

Pour faciliter l'analyse, la fonction **Follow TCP Stream** de Wireshark permet de reconstituer l'échange complet10.

- **Procédure** : Clic droit sur une trame → **Follow** → **TCP Stream**11.

4. Résultats et Solution

En analysant le flux reconstitué, on voit apparaître les bannières du système ainsi que les invites de connexion12121212.

- **Identifiant observé** : `fake` (note : il apparaît sous la forme `ffaakkee` à cause de l'écho du terminal).
- **Mot de passe observé** : Le mot de passe apparaît en clair après le prompt `Password`.

> 🔑 Mot de passe trouvé : user

---

5. Conclusion et Recommandations

Ce challenge illustre la vulnérabilité majeure du protocole Telnet due à l'absence de chiffrement16.

- **Recommandation** : Il est fortement recommandé d'utiliser des protocoles sécurisés comme **SSH (Secure Shell)**17.
- **Avantage de SSH** : SSH chiffre l'intégralité des échanges, incluant les identifiants de connexion18.

Challenge réalisé sur la plateforme Root-me