Petit vol en TP (INTRO)

Auteur(s) :

`Senkei`

Catégorie :

`Forensic`

Description :

Un élève mal intentionné a capturé le trafic réseau de son poste pendant que son professeur se connectait pour y récupérer un fichier.

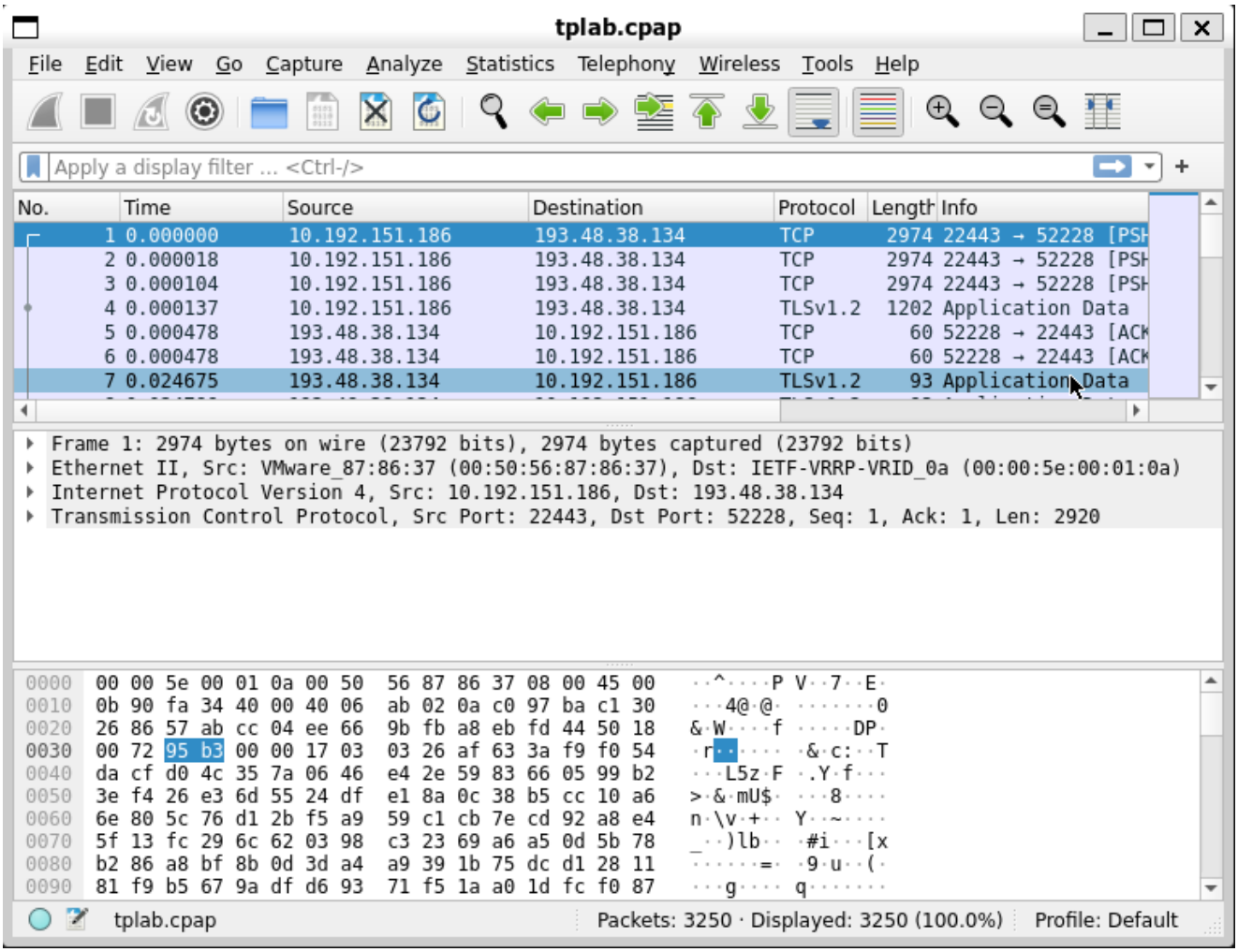
Quels sont le nom d'utilisateur et le mot de passe qu'a utilisé le professeur.

tplab.pcap

Flag : `UHOCTF{user:passwd}`

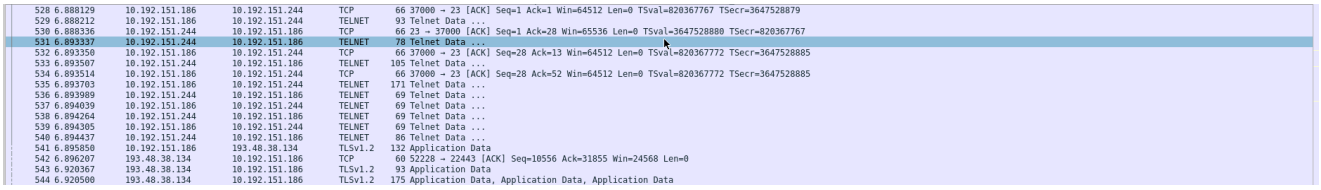
Solution

On a un fichier pcap, on l'ouvre avec wireshark et on cherche un peu.



!

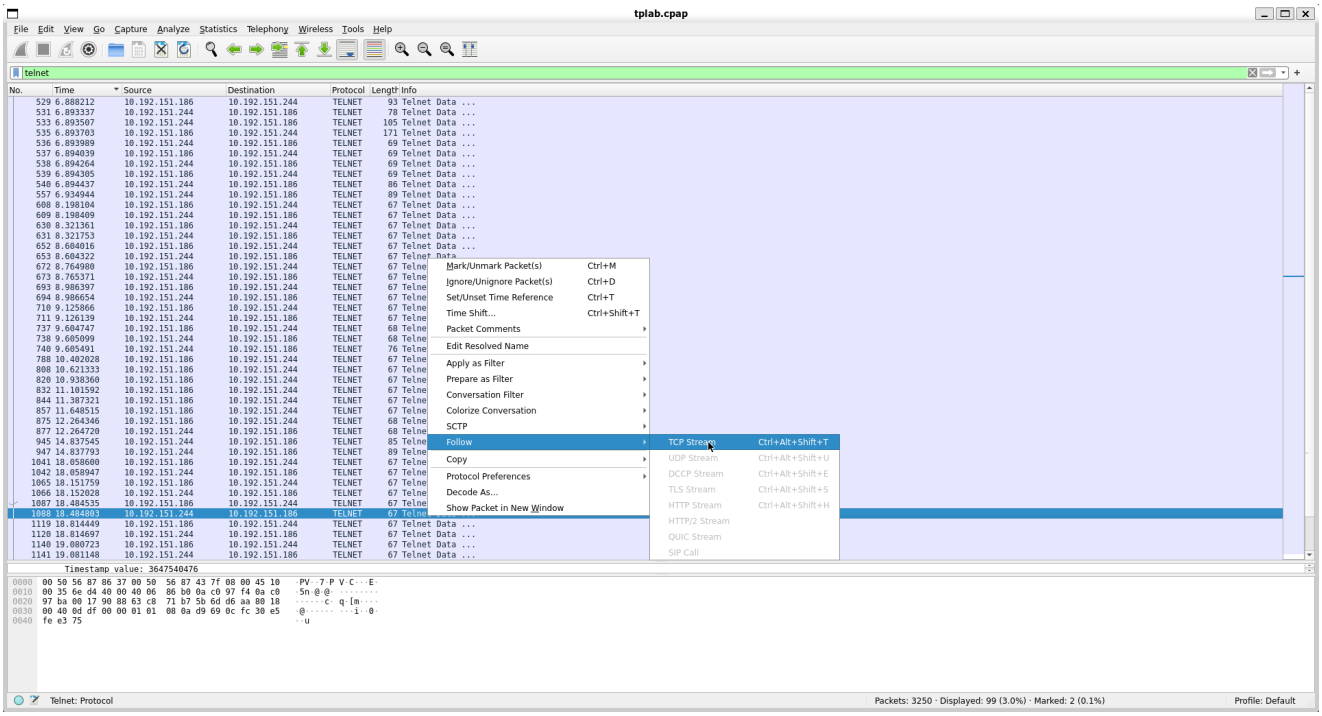
En examinant un peu les paquets, on voit que TELNET est utilisé, on peut donc utiliser le filtre `telnet` pour ne voir que les paquets telnet.



PROF

!

Il suffit de --> Follow --> TCP Stream pour voir le contenu des paquets telnet.



!

On peut maintenant filtrer les échanges entre le poste de l'élève et le poste du professeur et voir le username et le password.

!

Flag : UHOCTF{tpuser:T3lN3t_iS_n3t_Secure!!}

PROF