

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 : UH0CTF{user:passwd}

Solution

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

The screenshot shows the tplab.ccap interface. The top menu includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows "Apply a display filter ... <Ctrl-/>". The main packet list shows several entries, with packet 7 selected. The detailed view of packet 7 shows the following information:

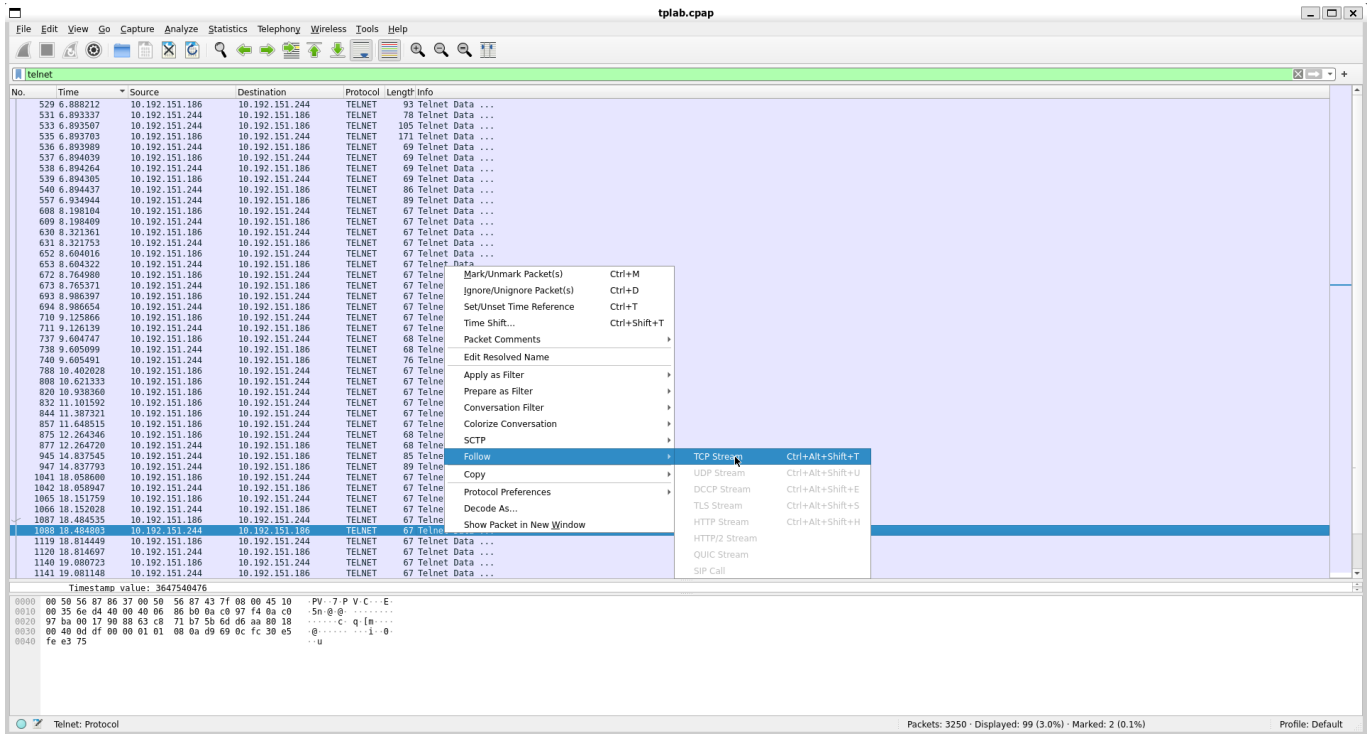
- Frame 1: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits)
- Ethernet II, Src: VMware_87:86:37 (00:50:56:87:86:37), Dst: IETF-VRRP-VRID_0a (00:00:5e:00:01:0a)
- Internet Protocol Version 4, Src: 10.192.151.186, Dst: 193.48.38.134
- Transmission Control Protocol, Src Port: 22443, Dst Port: 52228, Seq: 1, Ack: 1, Len: 2920

The packet data is displayed in hexadecimal and ASCII format at the bottom.

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.

528	6.888129	10.192.151.186	10.192.151.244	TCP	66	37000 → 23 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=820367767 TSecr=3647528879
529	6.888212	10.192.151.186	10.192.151.244	TELNET	93	Telnet Data ...
530	6.888336	10.192.151.244	10.192.151.186	TCP	66	23 → 37000 [ACK] Seq=1 Ack=28 Win=65536 Len=0 TSval=3647528880 TSecr=820367767
531	6.893337	10.192.151.244	10.192.151.186	TELNET	78	Telnet Data ...
532	6.893350	10.192.151.186	10.192.151.244	TCP	66	37000 → 23 [ACK] Seq=28 Ack=13 Win=64512 Len=0 TSval=820367772 TSecr=3647528885
533	6.893507	10.192.151.244	10.192.151.186	TELNET	165	Telnet Data ...
534	6.893514	10.192.151.186	10.192.151.244	TCP	66	37000 → 23 [ACK] Seq=28 Ack=52 Win=64512 Len=0 TSval=820367772 TSecr=3647528885
535	6.893703	10.192.151.186	10.192.151.244	TELNET	171	Telnet Data ...
536	6.893989	10.192.151.244	10.192.151.186	TELNET	69	Telnet Data ...
537	6.894039	10.192.151.186	10.192.151.244	TELNET	69	Telnet Data ...
538	6.894264	10.192.151.244	10.192.151.186	TELNET	69	Telnet Data ...
539	6.894305	10.192.151.186	10.192.151.244	TELNET	69	Telnet Data ...
540	6.894437	10.192.151.244	10.192.151.186	TELNET	86	Telnet Data ...
541	6.895850	10.192.151.186	193.48.38.134	TLSv1.2	132	Application Data
542	6.896207	193.48.38.134	10.192.151.186	TCP	60	52228 → 22443 [ACK] Seq=18556 Ack=31855 Win=24568 Len=0
543	6.920367	193.48.38.134	10.192.151.186	TLSv1.2	93	Application Data
544	6.920500	193.48.38.134	10.192.151.186	TLSv1.2	175	Application Data, Application Data, Application Data

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 : UH0CTF{tpuser:T3lN3t_iS_n3t_Secure!!}