

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.

tplab.cpap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.192.151.186	193.48.38.134	TCP	2974	22443 → 52228 [PSH]
2	0.000018	10.192.151.186	193.48.38.134	TCP	2974	22443 → 52228 [PSH]
3	0.000104	10.192.151.186	193.48.38.134	TCP	2974	22443 → 52228 [PSH]
4	0.000137	10.192.151.186	193.48.38.134	TLSv1.2	1202	Application Data
5	0.000478	193.48.38.134	10.192.151.186	TCP	60	52228 → 22443 [ACK]
6	0.000478	193.48.38.134	10.192.151.186	TCP	60	52228 → 22443 [ACK]
7	0.024675	193.48.38.134	10.192.151.186	TLSv1.2	93	Application Data

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

```

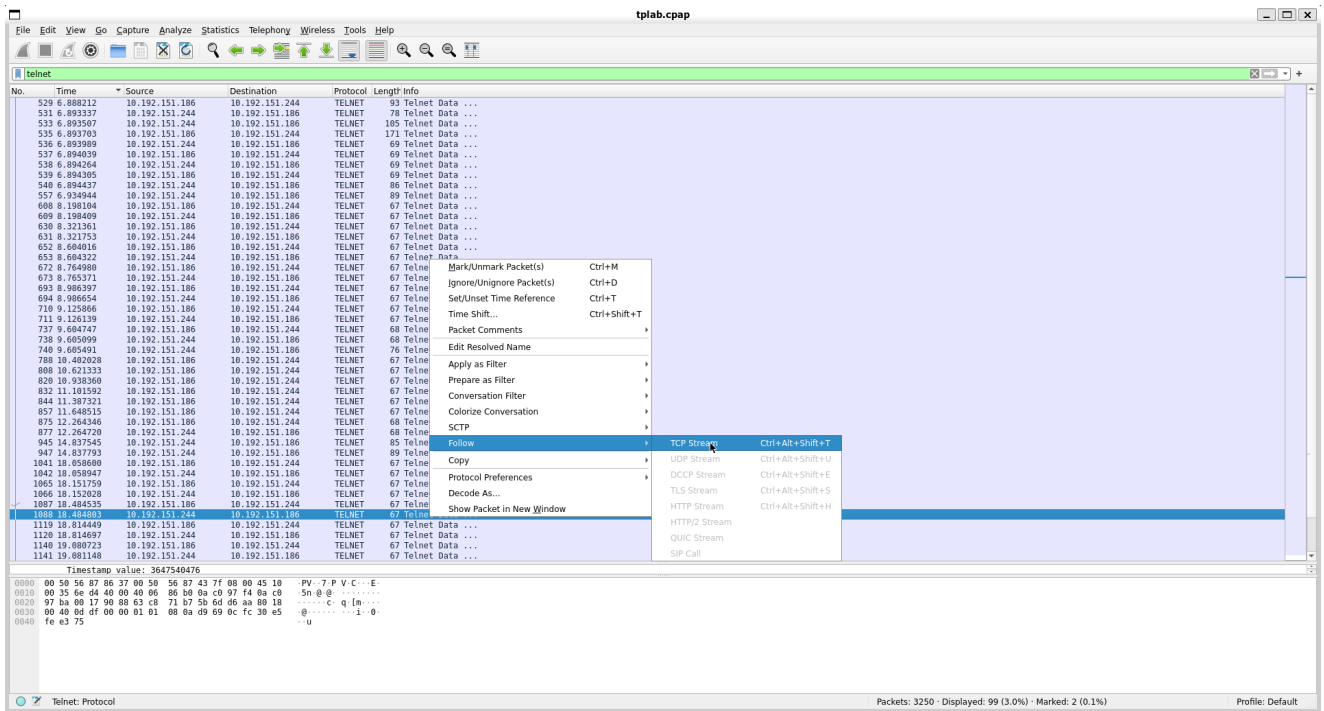
0000  00 00 5e 00 01 0a 00 50 56 87 86 37 08 00 45 00  ..^...P V..7..E.
0010  0b 90 fa 34 40 00 40 06 ab 02 0a c0 97 ba c1 30  ...4@.@.....0
0020  26 86 57 ab cc 04 ee 66 9b fb a8 eb fd 44 50 18  &W...f....DP.
0030  00 72 95 b3 00 00 17 03 03 26 af 63 3a f9 f0 54  .r...&c:T
0040  da cf d0 4c 35 7a 06 4e e4 2e 59 83 66 05 99 b2  ...L5z.F..Y.f...
0050  3e f4 26 e3 6d 55 24 df e1 8a 0c 38 b5 cc 10 a6  >.&mU$...8...
0060  6e 80 5c 76 d1 2b f5 a9 59 c1 cb 7e cd 92 a8 e4  n.v.+...Y~...
0070  5f 13 fc 29 6c 62 03 98 c3 23 69 a6 a5 0d 5b 78  _.)lb...#i...[x
0080  b2 86 a8 bf 8d 3d a4 a9 39 1b 75 dc d1 28 11  ...==.9.u.(
0090  81 f9 b5 67 9a df d6 93 71 f5 1a a0 1d fc f0 87  ...g....q.....
  
```

tplab.cpap Packets: 3250 · Displayed: 3250 (100.0%) Profile: Default

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=20 Ack=13 Win=64512 Len=0 TSval=820367772 TSecr=3647528885
533	6.893507	10.192.151.244	10.192.151.186	TELNET	105	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	88	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=10556 Ack=31855 Win=24568 Len=0
543	6.920567	193.48.38.134	10.192.151.186	TLSv1.2	93	Application Data
544	6.920580	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 : UHOCTF{tpuser:T3lN3t_is_n3t_Secure!!}**

