

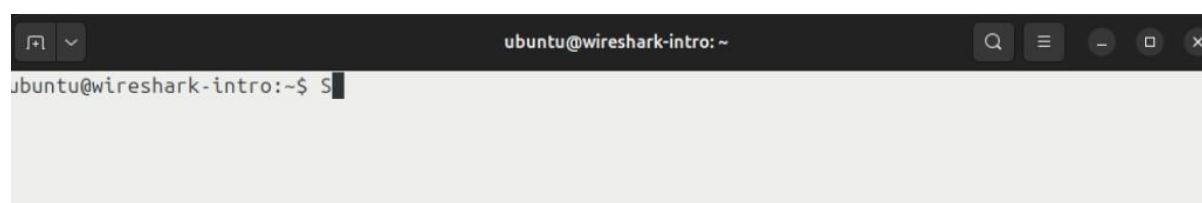
TP WireShark

Pour commencer notre Tp nous allons tout d'abord ouvrir notre Lab en exécutant la commande :

Labtainer wireshark-intro

```
student@LabtainerVMware:~/labtainer/labtainer-student$ labtainer wireshark-intro
```

Cela va ouvrir un terminal qui nous permettra d'exécuter les commandes demandées



Nous allons ensuite pour afficher le contenu du répertoire utilisez la commande : **ls-l**.

```
ubuntu@wireshark-intro:~$ ls -l
```

Un fichier s'affiche, nous allons afin de percevoir les détails du fichier utilisez la commande : **file telnet-pcap**

```
ubuntu@wireshark-intro:~$ file telnet.pcap
```

On va ensuite utilisez la commande : **wireshark** afin de lancer wireshark et d'exécuter une analyse PCAP du fichier.

```
ubuntu@wireshark-intro:~$ wireshark
```

Nous allons ensuite ouvrir le fichier telnet.pcap

Puis taper la commande telnet.data afin de filtrer et d'afficher seulement les paquets de données Telnet.



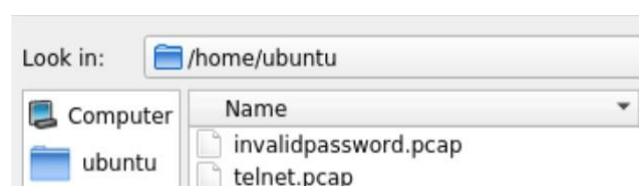
Nous allons ensuite localiser le paquet qui contient le Mdp fourni lorsque l'utilisateur John a tenté d'utiliser telnet.

No.	Time	Source	Destination	Protocol	Length	Info
145	51.159917	172.20.0.3	172.20.0.2	TELNET	86	Telnet Data ...
147	51.199906	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
149	54.245675	172.20.0.2	172.20.0.3	TELNET	72	Telnet Data ...
150	54.246744	172.20.0.3	172.20.0.2	TELNET	73	Telnet Data ...
152	54.249295	172.20.0.3	172.20.0.2	TELNET	76	Telnet Data ...
154	59.970096	172.20.0.2	172.20.0.3	TELNET	81	Telnet Data ...
155	59.970901	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
157	62.827197	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
159	62.827399	172.20.0.3	172.20.0.2	TELNET	83	Telnet Data ...
161	62.828708	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
163	64.914707	172.20.0.2	172.20.0.3	TELNET	71	Telnet Data ...

▶ Frame 159: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
 ▶ Ethernet II, Src: 02:42:ac:14:00:03 (02:42:ac:14:00:03), Dst: 02:42:ac:14:00:02 (02:42:ac:14:00:02)
 ▶ Internet Protocol Version 4, Src: 172.20.0.3, Dst: 172.20.0.2
 ▶ Transmission Control Protocol, Src Port: 23, Dst Port: 35544, Seq: 107, Ack: 98, Len: 17
 ▶ Telnet

0000	02 42 ac 14 00 02 02 42 ac 14 00 03 08 00 45 10	.B....B.....E.
0010	00 45 de 68 40 00 40 06 04 0d ac 14 00 03 ac 14	E.h@.@.....E.
0020	00 02 00 17 8a d8 22 e7 a1 72 39 65 48 c2 80 18r9eh....
0030	00 e3 58 65 00 00 01 01 08 0a 04 15 8a bf 04 15	..Xe.....
0040	8a bf 4c 6f 67 69 6e 20 69 6e 63 6f 72 72 65 63	..Login incorrec
0050	74 0d 0a	t..

Nous allons ensuite enregistrer le packet unique en utilisant : **File =>Export specified packets** sous le nom de **invalidpassword.pcap**.



Nous pouvons ensuite suivre l'exploration en observant d'autre paquets et en expérimentant des filtres.

Puis arrêter le Lab en tapant la commande : **stoplab**