🔍 Analyse de paquets réseau avec tcpdump et Wireshark

🎯 Objectif :

Capturer les paquets réseau sur un serveur distant (Debian), les transférer sur une machine Kali Linux avec interface graphique, puis les analyser via Wireshark.

🧰 Pré-requis :

• tcpdump installé sur le serveur : sudo apt install tcpdump

• Accès SSH entre le serveur et la machine Kali

• Wireshark installé sur Kali

💡 Astuce : Utiliser Wireshark à distance via X11 forwarding

• Activez le X11 Forwarding pour lancer Wireshark depuis le serveur distant sur votre Kali (avec interface graphique).

Commande : ssh -X user@ip_serveur

Puis : wireshark & (le & permet de continuer à utiliser le terminal)

🛠 Étapes :

1️⃣ Déterminer l'interface réseau utilisée

Commande : ip a

Recherchez l'interface connectée au réseau (ex. : ens18).

```
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether bc:24:11:b5:0e:9e brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.27.10/24 brd 192.168.27.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:feb5:e9e/64 scope link
       valid_lft forever preferred_lft forever
```

2️⃣ Capturer les paquets

• Tout le trafic : sudo tcpdump -i ens18 -w /tmp/capture.pcap

• Trafic sur un port spécifique : sudo tcpdump -i ens18 port 50271 -w /tmp/capture.pcap

Arrêtez avec CTRL+C après quelques secondes.

```
aftec@debian:/etc/nginx/sites-available$ sudo tcpdump -i ens18 -w /tmp/capture.pcap
[sudo] Mot de passe de aftec :
tcpdump: listening on ens18, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C362 packets captured
364 packets received by filter
0 packets dropped by kernel
aftec@debian:/etc/nginx/sites-available$
```

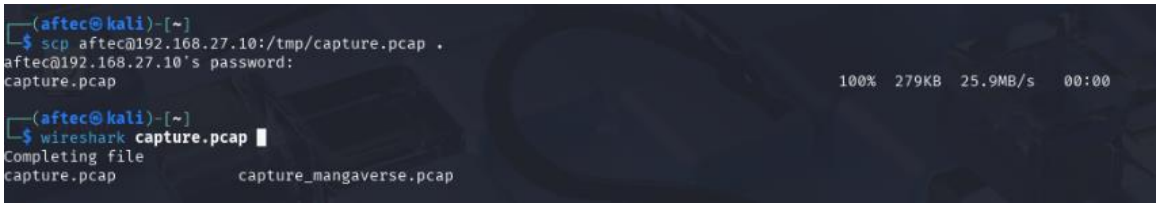
3️⃣ Transférer la capture sur Kali

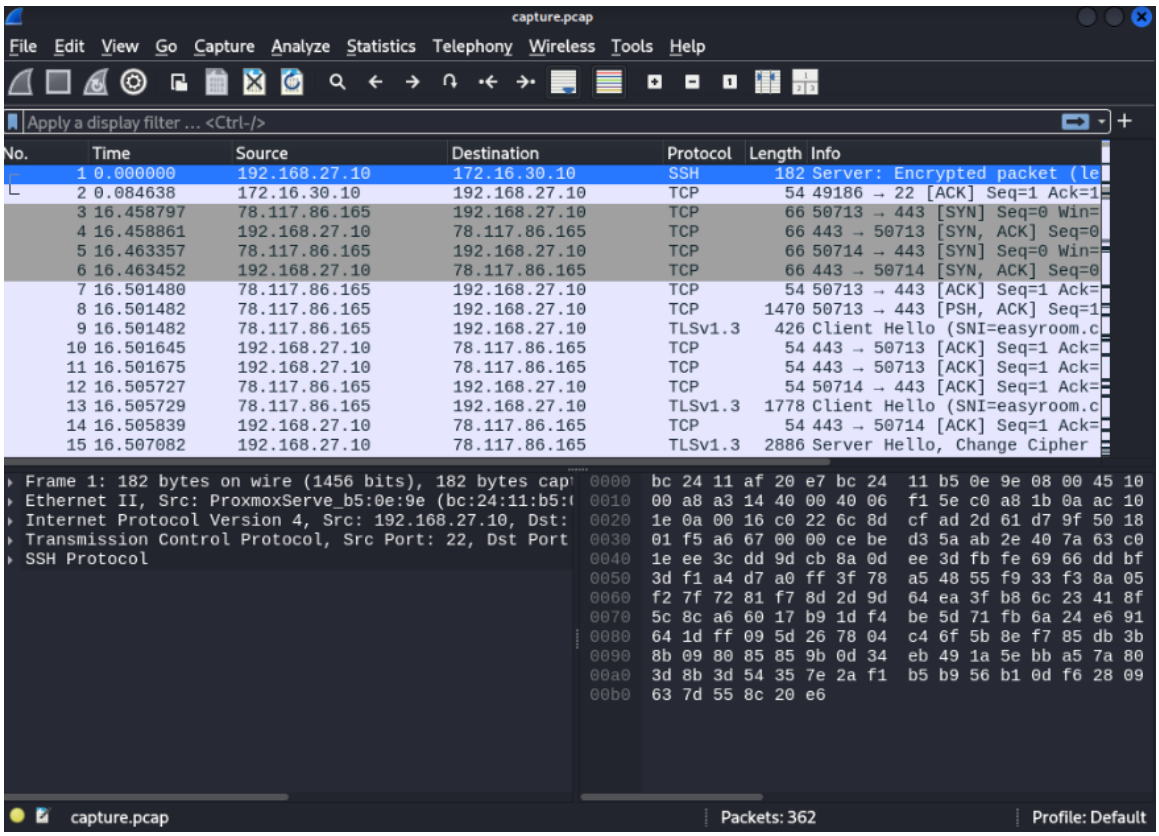
Commande sur Kali :

scp user@ip_serveur:/tmp/capture.pcap .

4️⃣ Ouvrir et analyser la capture

Commande : wireshark capture.pcap

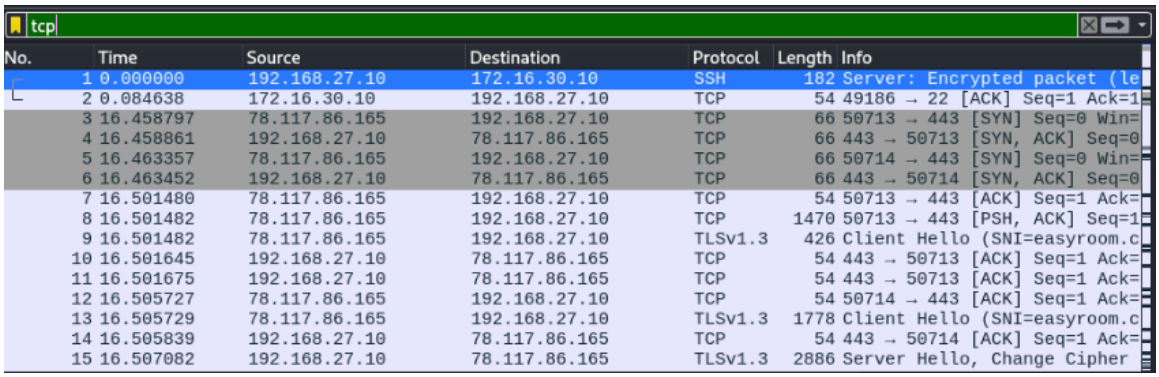




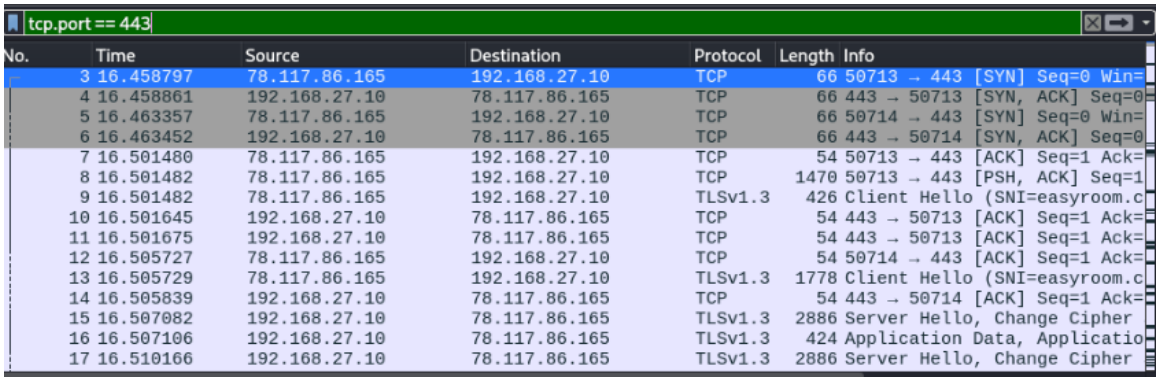
5️⃣ Utiliser les filtres dans Wireshark

Exemples de filtres utiles :

• tcp → pour ne voir que les paquets TCP



- tcp.port == 443→ pour cibler un port précis



• ip.addr == 192.168.27.10 → pour filtrer une IP spécifique