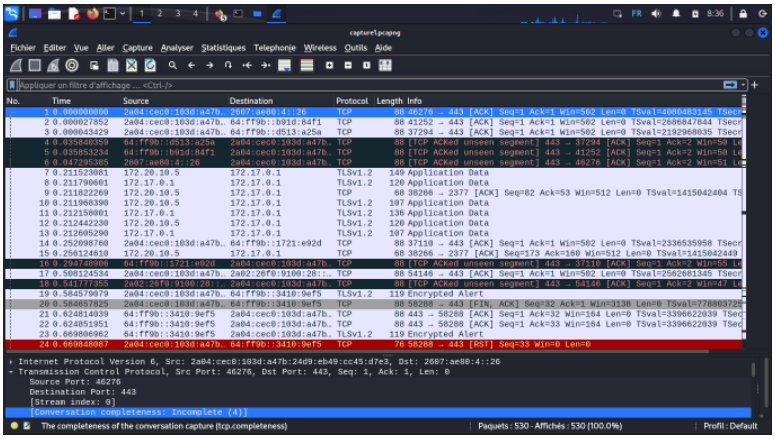
Projet Sécurité: CTF

GROUPE	BACKDOOR	**Solution**
PHASE 1	DEVELOPPEMENT CTF	***RESEAU***
NIVEAU	FACILE	

Flag 1:

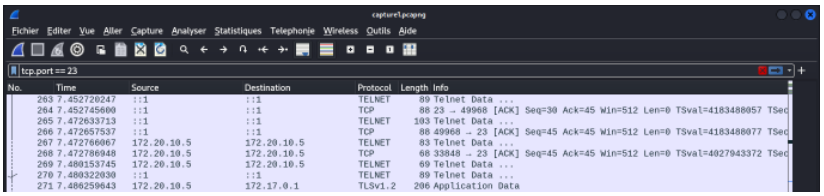
Analyser la capture Wireshark :

- Ouvrez la capture Wireshark fournie.
- Appliquez un filtre pour afficher uniquement les paquets TELNET en utilisant la commande : tcp.port==23.



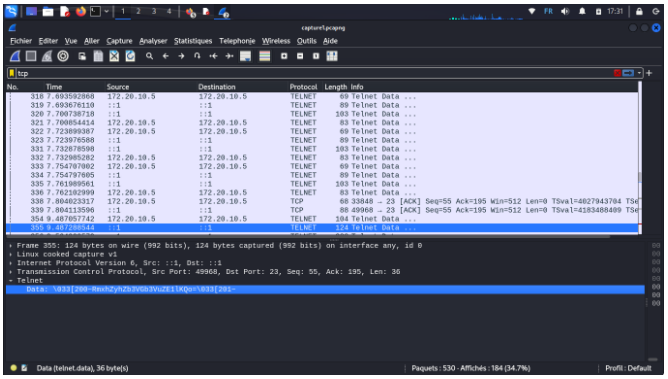
Repérer le paquet contenant le flag :

- Parcourez les paquets TELNET et recherchez des données inhabituelles ou potentiellement codées.
- Identifiez le paquet qui semble contenir le flag. Cela peut être indiqué par une longueur de données suspecte, ou d'autres signes distinctifs.

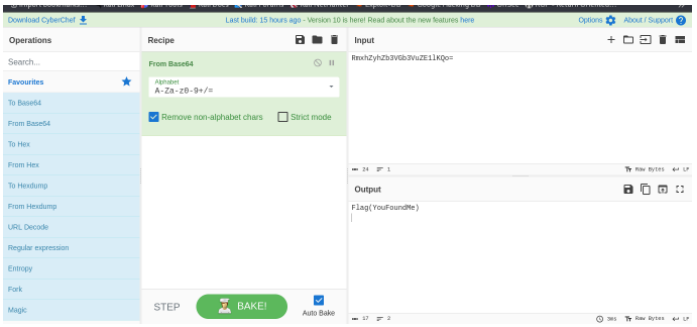


Extraire le paquet avec le flag :

- Identifiez le numéro de séquence du paquet contenant le flag.
- Utilisez les fonctionnalités de filtrage de Wireshark pour extraire uniquement ce paquet.



Déchiffrer les données

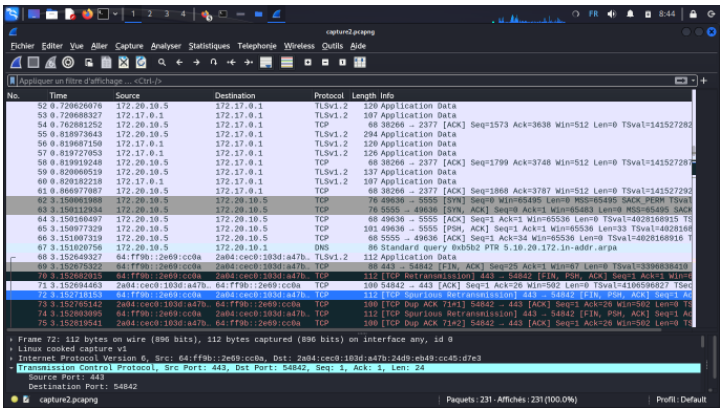


Flag(YouFoundMe)

Flag 1:

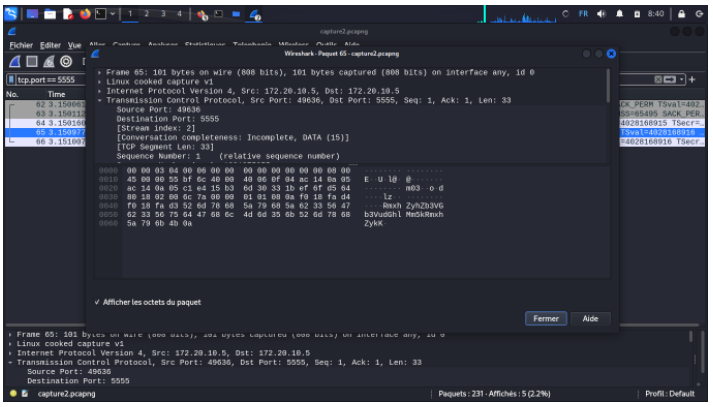
Analyser la capture Wireshark :

- Ouvrez la capture Wireshark fournie et examinez les connexions entrantes et sortantes.
- Identifiez des schémas de trafic suspects ou des ports qui pourraient être associés à Netcat.



Identifier le paquet contenant le flag :

- Une fois que vous avez repéré des paquets Netcat, examinez le contenu des données pour rechercher le flag. Recherchez des motifs spécifiques ou des chaînes qui pourraient indiquer la présence du flag.



Déchiffrer les données :

- Copiez le contenu du champ de données du paquet extrait.
- Si le trafic Netcat est chiffré, identifiez le type de chiffrement utilisé (s'il est spécifié) et utilisez des outils appropriés pour déchiffrer le contenu.