**Solutions**

## *CTF RESEAU MOYEN*

**Défi 1 : Le Serveur Web Sécurisé**

- Trouvez le flag caché dans le certificat SSL du serveur web.

**Solution :**

1. Exécutez la commande suivante pour afficher les détails du certificat SSL du serveur :

   openssl s_client -connect @ip:443 -servername localhost | openssl x509 -noout -text

   Cette commande établit une connexion SSL au serveur web et affiche les détails du certificat SSL.

2. Dans les informations du certificat, recherchez le champ "Common Name" (CN). C'est là que le flag est caché.

3. Notez le flag qui est contenu dans le champ "Common Name" du certificat.

4. Vous avez trouvé le flag caché dans le certificat SSL !

**Défi 2 : L'Énigme DNS**

- Explorez les enregistrements DNS pour résoudre l'énigme.

- Localisez le flag caché dans les enregistrements DNS.

**Solution :**

1. Utilisez la commande suivante pour effectuer une zone de transfert de zone (AXFR) sur le domaine example.com :

   dig @ip -p 5353 axfr example.com

2. Une fois que vous avez obtenu la liste des enregistrements DNS, examinez-les attentivement.

3. Recherchez des enregistrements TXT ou d'autres données inhabituelles qui pourraient contenir des indices ou le flag.

4. Combinez les informations obtenues des enregistrements DNS pour résoudre l'énigme et localiser le flag.

**Défi 3 : La Capture Wireshark Secrète dans le Serveur SMB**

- Extrayez la capture Wireshark du serveur de partage SMB "hidden".

- Analysez la capture pour localiser le flag transmis avec ncat.

Solution :

1. Utilisez la commande suivante pour accéder au partage SMB "hidden" avec smbclient :

   smbclient //localhost/hidden

2. Une fois connecté au partage SMB, utilisez la commande `get` pour télécharger la capture Wireshark (par exemple, "capture.pcap") depuis le partage SMB vers votre système local :

   get capture.pcap

3. Une fois que vous avez extrait la capture, utilisez Wireshark pour l'ouvrir et l'analyser.

4. Recherchez les paquets dans la capture Wireshark pour trouver le flag qui a été transmis avec ncat.