

Réseaux

On va s'échauffer avec quelques petits challenges qui vont nous permettre de mettre en pratique nos connaissances. Ca va se jouer sur root-me.

Question 6. Résolvez le challenge FTP en ouvrant le fichier .pcap dans Wireshark

Question 7. Lisez rapidement la RFC 959: de quand date le protocole FTP ? Que fait la commande USER ? Que fait la commande PASS ?

Question 8. Que peut-on imaginer concernant les conditions de la capture ?

Question 9. Qu'aurait-il fallu faire pour que les informations ne soient pas passées "en clair" ?

Cas réels : voici à gauche une connexion de mon ordinateur sur mon serveur FTP personnel chez OVH. À droite une connexion sur le FTP de votre serveur du lycée (192.168.70.102) via le VPN.

The image displays two side-by-side screenshots of the Wireshark network protocol analyzer, specifically the 'Follow TCP Stream' window for an FTP connection (tcp.stream eq 0).

Left Screenshot (Wi-Fi): Shows the initial part of the connection. The status bar indicates 'Wi-Fi'. The stream content shows a '220- Welcome to OVH' message, followed by '220 This is a private system - No anonymous login'. The user 'lessicuo' is prompted for a password. The stream ends with '226 13 matches total'.

Right Screenshot (Conexion au réseau lo...): Shows a more complex stream content, likely from a school server. It displays a list of supported algorithms for the 'AUTH TLS' and 'AUTH SSL' commands, including various encryption and integrity algorithms like 'aes128-ctr', 'aes256-ctr', 'chacha20-poly1305', etc. The stream ends with '226 13 matches total'.

Question 10. Que peut-on dire de ces deux connexions ? De quels types sont-elles ?

Question 11. Concluez sur les bonnes pratiques concernant une connexion FTP.

Question 12. Résolvez le challenge TELNET

Question 13. Lisez rapidement la RFC854. Quelle est la principale faiblesse de telnet ?

Question 14. Par quoi a-t-il été progressivement remplacé ? Concluez sur les bonnes pratiques

Question 15. Pourquoi les caractères sont-ils "doublés" ?

Question 16. Quelles commandes a effectué le client ?

Question 17. Réalisez le challenge Ethernet.

Question 18. Qu'est-ce que l'encodage base64 ? Est-ce considéré comme un mécanisme de chiffrement ? de hachage ?

Question 19. Faire le challenge "authentification Twitter"

Question 20. Selon vous, dans quelles conditions a été réalisée la capture ?

Question 21. Quelle contre-mesure peut empêcher des interceptions de ce type ?

L'échauffement est désormais terminé. Il est temps de mettre en pratique ce que l'on a appris jusque lors et ...

Question 22. Faire le challenge "CISCO-mot de passe"

Question 23. Evaluation 3 p 131