Chapitre 0 Introduction

R01 Administration distante

1 Enjeux

Besoin d'administrer des Serveurs, routeurs, switchs à distance.

Les protocoles d'accès distant permettent de :

- Lancer des commandes sur une machine sans être physiquement présent.
- Configurer et superviser les equipements

Enjeu majeur : la sécurité

- Les données échangées (identifiants, commandes) doivent être protégées.

2 Telnet TELecommunication NETwork

Arpanet 1969
Internet 1983

Créé en 1969 (avant internet) pour permettre à un utilisateur de se connecter à un ordinateur distant et d'y exécuter des commandes.

Utilisations :

- Très populaire dans les années 70-90
- Administration de serveurs et équipements réseaux
- Outil simple pour tester la connectivité et les ports ouverts

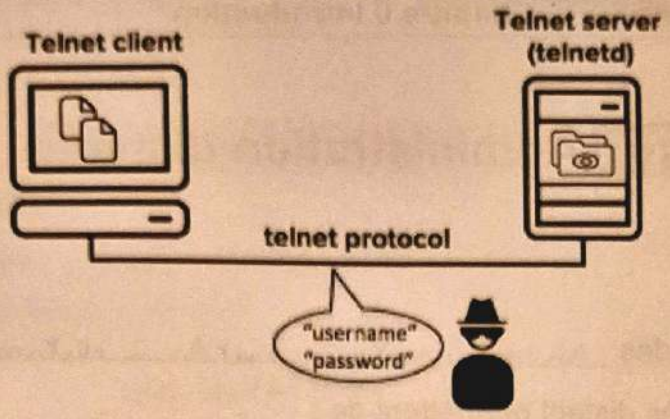
Problème majeur : toutes les communications sont en clair → vulnérable aux attaques.

2.1 Fonctionnement

Protocole de communication TCP/IP

Connexion via port 23/TCP

Les commandes tapées côté client sont exécutées à distance.



Pas de sécurité : tout circule en clair (login, mot de passe, données)

Quel type de logiciel utilise-il ?

Un sniffer (ex : Wireshark)

2.2 Avantages

Protocole simple, léger, rapide.

Encore présent sur certains équipements anciens.

Exemple de commande : telnet towel.blinkenlights.nl

3 SSH Secure Shell

Créé en 1995 (par Tatu Ylönen, chercheur finlandais), SSH a pour objectif de remplacer Telnet en garantissant confidentialité et sécurité des connexions distantes.

Dans les années 90, les attaques par interception de mots de passe Telnet se multiplient. SSH apporte une couche de chiffrement forte et une authentification améliorée.

SSH est rapidement devenu la norme dans les environnements Unix/Linux. Aujourd'hui, incontournable dans des métiers réseau et système.

3.1 Fonctionnement

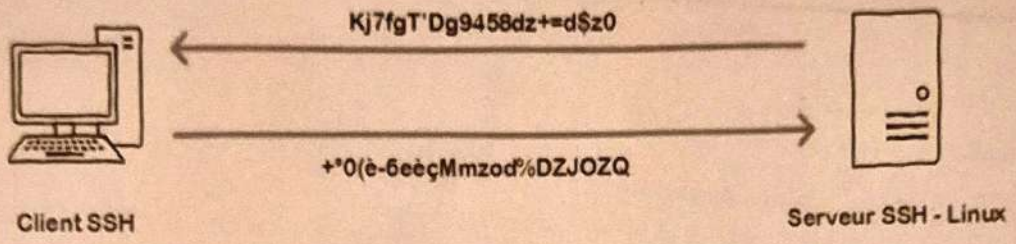
Protocole sécurisé de communication à distance.

Connexion via le port 22/TCP

Etablir un canal chiffré :
- Authentification (mot de passe ou clé publique).
- Echanges cryptés pour garantir confidentialité et intégrité.

Fonctionnalité additionnelle :

- Transfert de fichiers (SCP secure copy, SFTP secure file transfert protocole.)



3.2 Avantages

Communication sécurisée (protection contre oreilles et attaques)

Authentification forte avec clés asymétriques. (RSA) Rivest Shamir Adleman

Standard actuel dans les environnements professionnels.

Compatible Linux, macOS et Windows (OpenSSH, PUTTY, PowerShell)

Exemple de commandes :

ssh user@192.168.1.10

scp fichier.txt user@192.168.1.10:/home/user/

4 Telnet vs SSH

Critère	Telnet	SSH
Port par défaut	23 /TCP	22 /TCP
Sécurité	Aucune (tout en clair)	chiffrement complet
Authentification	Login/mot de passe simple	Mot de passe ou clé publique
Utilisation	Rare, obsolète	Standard de l'industrie
Cas d'usage	Tests rapides, anciens équipements	Administration distante, transfert sécurisés