République Algérienne Démocratique Et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
ECOLE NATIONALE POLYTECHNIQUE D'ORAN MAURICE AUDIN

Département Mathématiques et Informatique
Filière IMSI : 4ème année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

kablifatima47@gmail.com

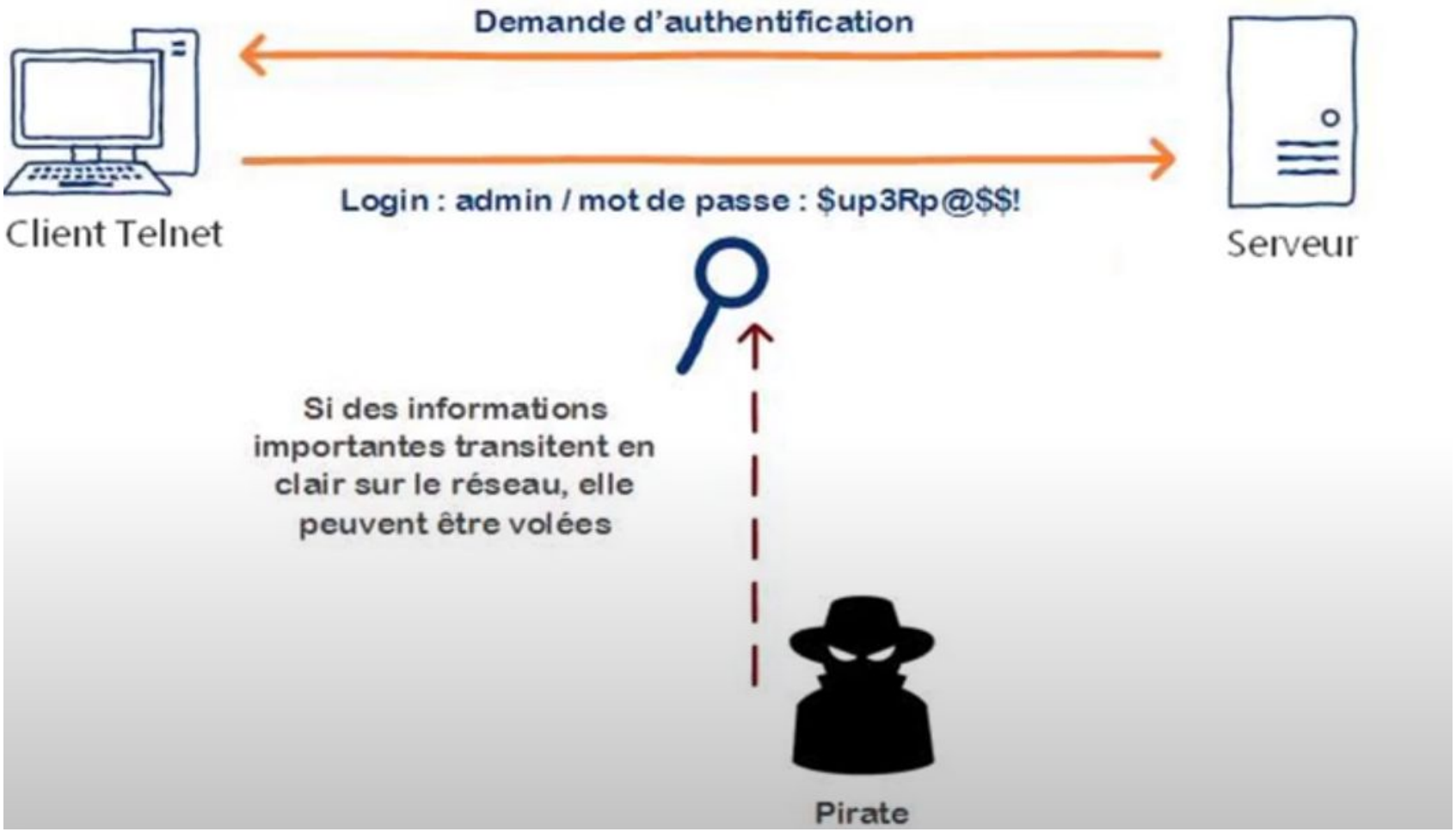
Protocole SSH

Définition Telnet

- Telnet est un protocole de communication de réseau qui permet à un utilisateur de se connecter à distance à un ordinateur ou un serveur distant pour accéder à une console ou un shell système.
- Le protocole Telnet est basé sur une communication client-serveur, dans laquelle le client se connecte au serveur via le port 23 en utilisant une connexion TCP/IP.
- Généralement utilisé pour l'administration à distance des serveurs et des réseaux
- Il peut également être utilisé pour accéder à distance à des systèmes et à des services de manière interactive.
- Telnet est considérée comme peu sécurisée car toutes les informations échangées entre le client et le serveur sont transmises en clair, y compris les noms d'utilisateur et les mots de passe.

Protocole SSH

Définition Telnet (port 23)



Protocole SSH

Définition SSH :

- Le protocole SSH (Secure Shell) est un protocole de communication sécurisé qui permet d'établir une connexion réseau cryptée entre deux ordinateurs, généralement un client et un serveur.

- Permettre à un utilisateur de se connecter de manière sécurisée à un serveur distant et d'y exécuter des commandes à distance, tout en protégeant les communications contre l'interception et l'espionnage.

- Le protocole SSH est une méthode sûre pour accéder à un ordinateur distant et d'y effectuer des opérations à distance.

Protocole SSH

SSH-Serveur :

Les systèmes d'exploitation peuvent inclure un serveur SSH, mais il est généralement désactivé par défaut pour des raisons de sécurité. Les administrateurs système doivent activer et configurer le serveur SSH avant de pouvoir l'utiliser pour permettre des connexions SSH entrantes.

SSH client :

Nombreux systèmes d'exploitation modernes comme:

Linux
Unix
macOS
Windows 10

Prennent en charge SSH et offrent des clients SSH natifs qui peuvent être utilisés pour se connecter à des serveurs SSH distants.

Protocole SSH

Communication Client–Serveur SSH

1. Demande de connexion envoyée par le client : Le client initie une demande de connexion vers le serveur SSH. Cela se produit généralement sur le port 22, le port par défaut pour SSH.

2. Le serveur répond avec une chaîne d'identification : À la réception de la demande de connexion, le serveur répond avec sa chaîne d'identification, qui inclut des informations sur la version et l'implémentation SSH du serveur.

3. Échange de clés : Le client et le serveur s'engagent dans un processus d'échange de clés pour établir une connexion sécurisée. Cela implique la génération de clés de chiffrement pour la session. L'algorithmes couramment utilisé pour l'échange de clés est Diffie-Hellman.

Protocole SSH

Communication Client–Serveur SSH

4. Authentification du client : Le client s'authentifie auprès du serveur en utilisant un nom d'utilisateur et, éventuellement, un mot de passe. Alternativement, le client peut utiliser une authentification par clé publique, où la clé publique du client est stockée sur le serveur et utilisée pour l'authentification.

5. Authentification du serveur : Le serveur s'authentifie auprès du client en présentant sa clé publique. Le client vérifie l'identité du serveur en vérifiant la clé publique du serveur par rapport à une liste d'hôtes connus stockée dans le fichier known_hosts.

6. Établissement de la connexion chiffrée : Une fois que le client et le serveur se sont mutuellement authentifiés, ils commencent le processus de chiffrement du canal de communication. Cela garantit que toutes les données transmises entre le client et le serveur sont sécurisées et ne peuvent pas être interceptées par des attaquants.

Protocole SSH

Communication Client–Serveur SSH

7. Session interactive : Si les processus d'authentification et de chiffrement sont réussis, une session interactive est établie, permettant au client d'exécuter des commandes sur le serveur et d'interagir avec ses ressources.

8. Échange de données : Pendant la session, le client et le serveur peuvent échanger des données de manière sécurisée. Cela inclut l'exécution de commandes à distance, le transfert de fichiers et l'exécution d'autres opérations réseau.

9. Fin de session : Lorsque la session est terminée, soit le client, soit le serveur peut mettre fin à la connexion. Le protocole SSH inclut des mécanismes pour fermer la connexion et libérer toutes les ressources associées.

Protocole SSH

L’authentification par clé publique

- Le client envoie sa clé publique au serveur SSH pour l'authentification. La clé publique est généralement stockée dans le fichier authorized_keys sur le serveur.
- Le serveur SSH stocke la clé publique du client pour une utilisation ultérieure. Le serveur utilise cette clé publique pour vérifier la signature numérique du client lors de connexions futures.
- Lorsque le client se connecte au serveur SSH, le serveur envoie une demande de signature numérique. Cette demande inclut un message aléatoire généré par le serveur, appelé le "challenge".
- Le client utilise sa clé privée pour générer la signature. La signature est basée sur le challenge et la clé privée du client.
- Le serveur vérifie la signature en utilisant la clé publique stockée du client et autorise l'accès si la signature est validée. Si la signature est incorrecte, la connexion est refusée.

Protocole SSH

SSH et Telnet

Les protocoles SSH et Telnet sont similaires dans leur fonctionnement et leur capacité à fournir une communication interactive entre un client et un serveur, SSH offre une sécurité supplémentaire grâce au **cryptage** des données et à **l'authentification forte**. C'est pourquoi il est généralement préféré pour les connexions réseau sécurisées.