# Cours Sécurité et cryptographie

## Chapitre 6:

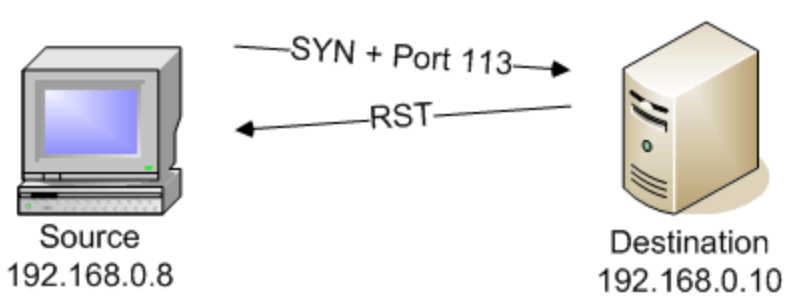
## Outils de sécurité

# Plan

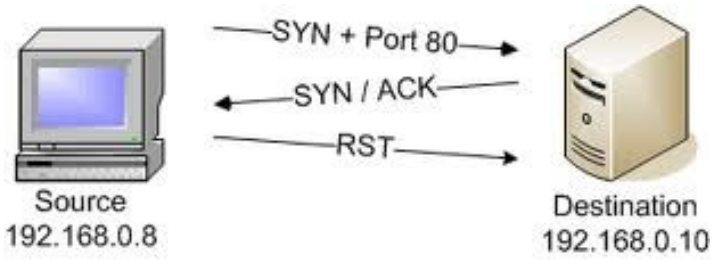
- Partie 1:
  - Définitions et principales caractéristiques
  - Exemples

# TCP SYN scan ou half open scan

- La source envoi un SYN
  - Si réception d'un SYN-ACK ➔ port en écoute
    - Un RST est envoyé pour arrêter la connexion
  - Si réception d'un RST ➔ port n'est pas en écoute



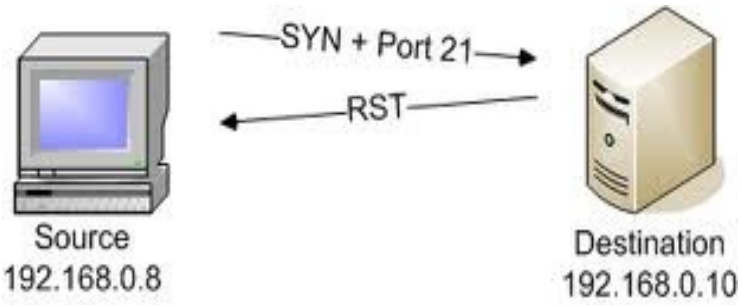

Port fermé



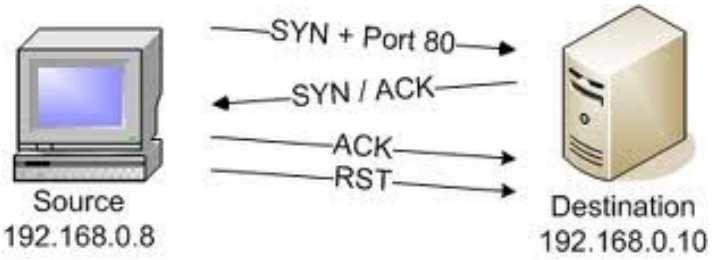

Port ouvert

# TCP connect scan

- Utilise l'appel système connect()
  - Succès de l'appel ➔ port ouvert
  - Echec de l'appel ➔ port fermé



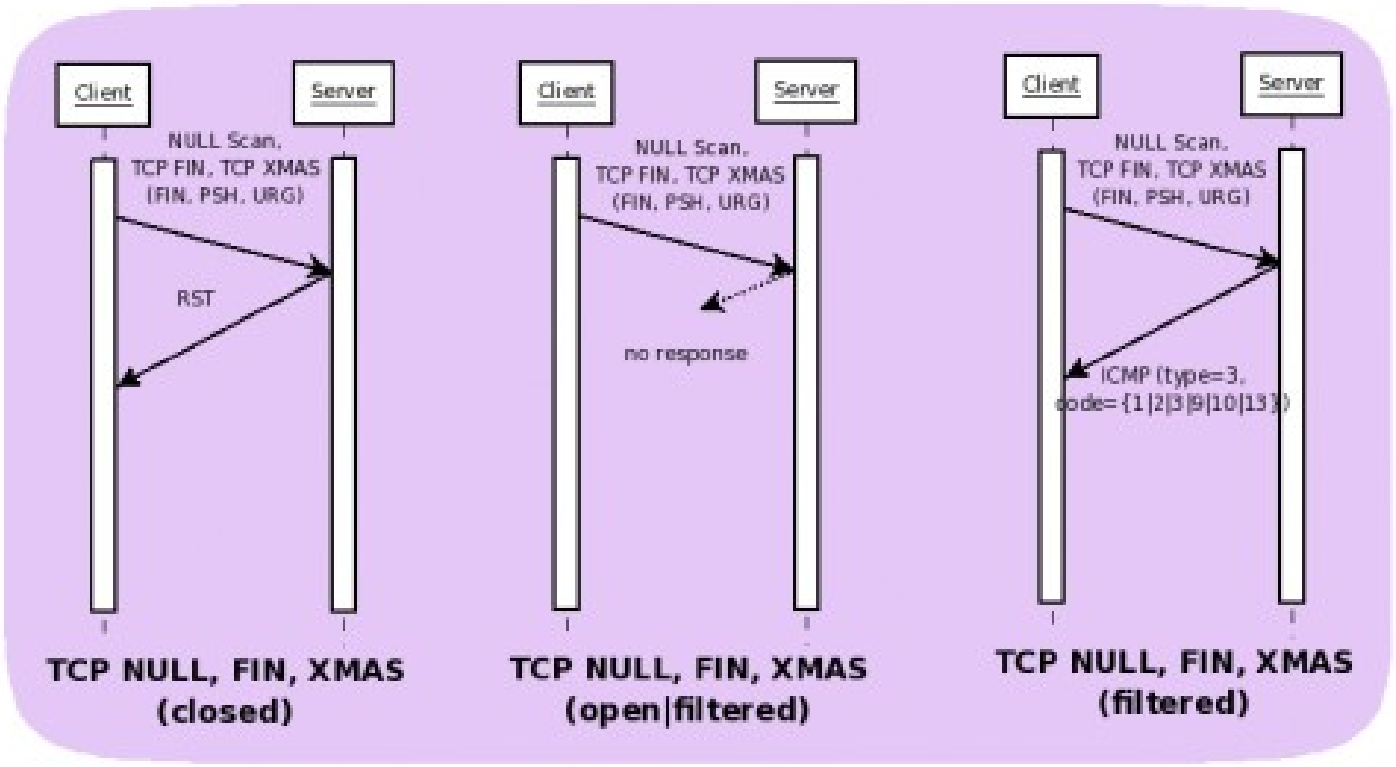

Port fermé




Port ouvert

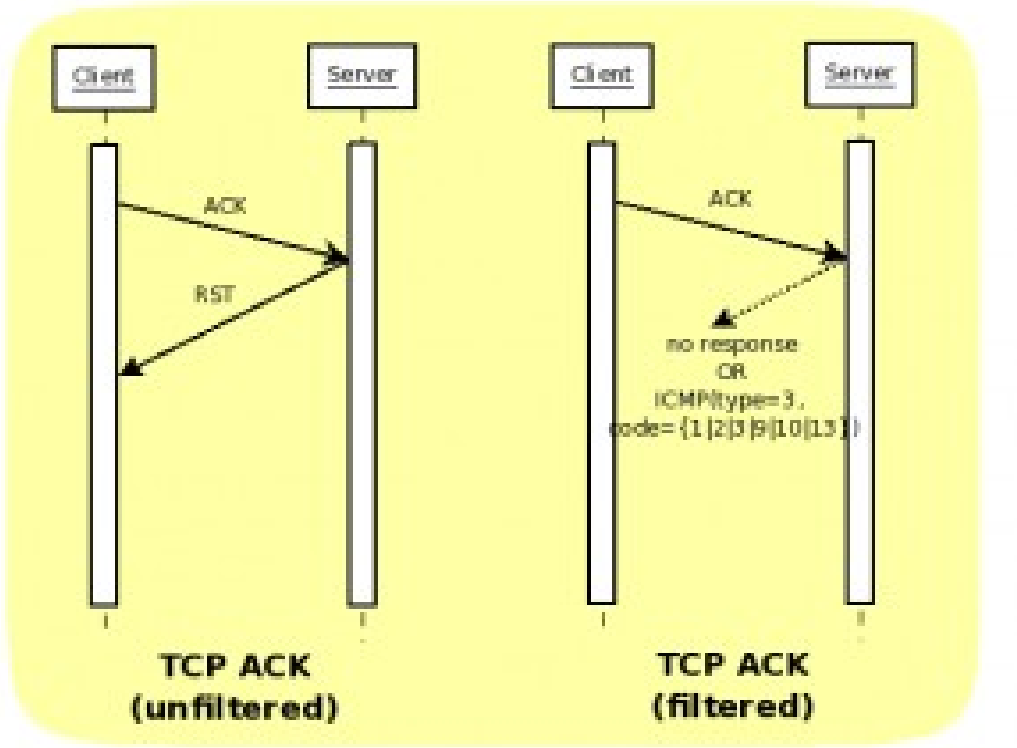
# TCP stealth FIN, Xmas Tree et NULL scan

- Utilisé si les scan SYN sont filtré (par des firewall)
  - NULL scan : n'active aucun des drapeaux de l'en-tête TCP (tous à 0).
  - FIN scan: n'active que le bit FIN
  - Xmas scan: active les drapeaux FIN, PSH et URG



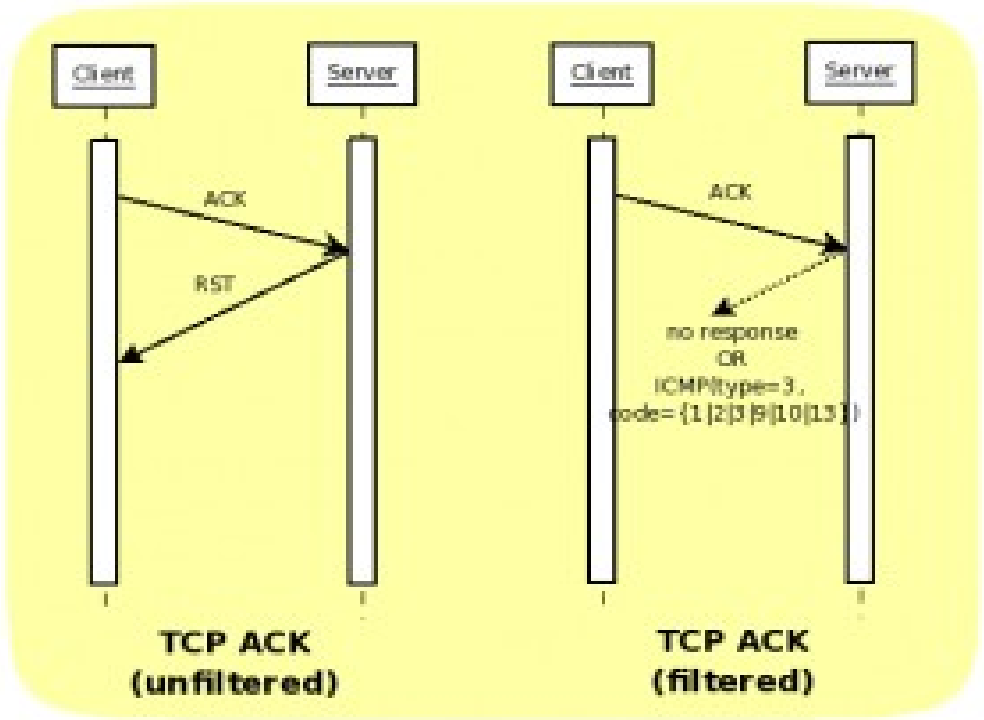
# TCP ACK scan et TCP Window scan

- ACK scan
  - **Ne détermine pas l'état des ports (ouvert, fermé)** mais est utilisé afin de déterminer si un firewall est stateful ou stateless.
  - N'active que le drapeau ACK des paquets



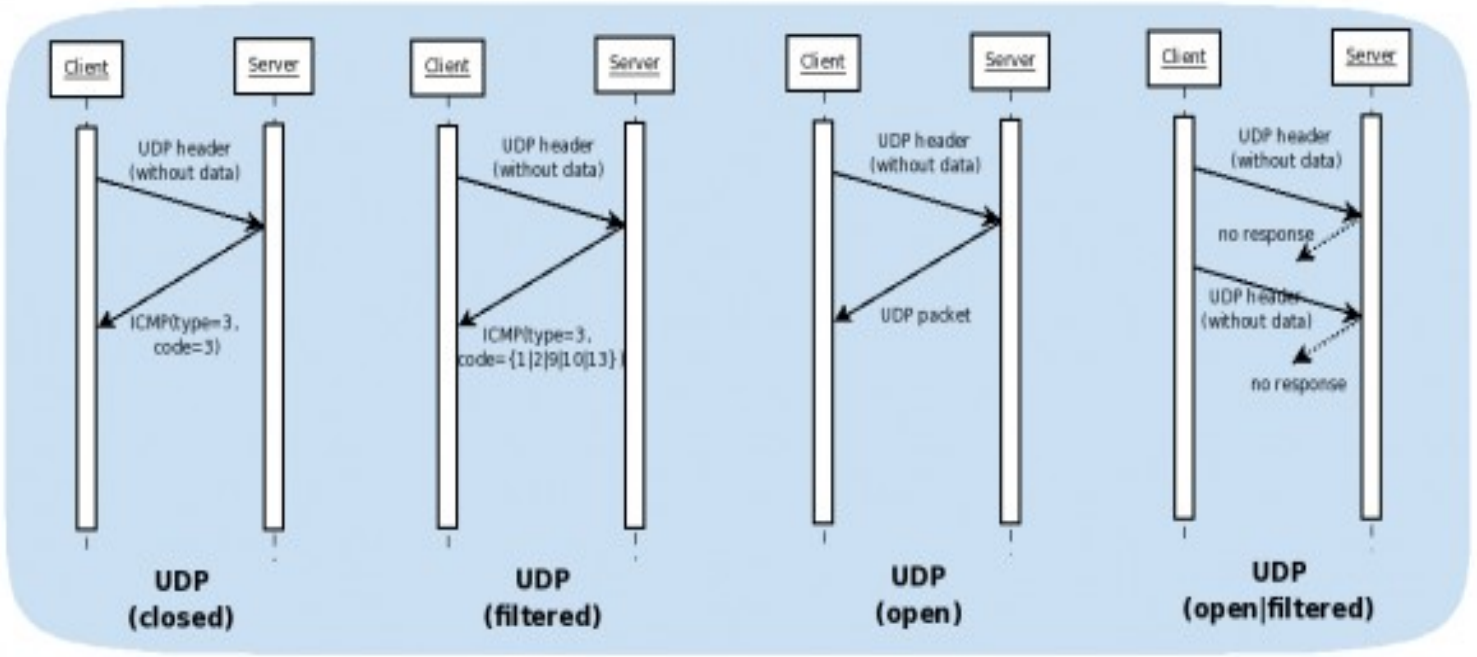
# TCP ACK scan et TCP Window scan

- Window scan
  - Même scan que le scan ACK, en plus
  - exploite un détail de l'implémentation de certains systèmes pour identifier les ports fermés des autres, au lieu de toujours afficher non filtré lorsqu'un RST est renvoyé.



# UDP scan

- Technique: envoyer  un paquet UDP vide (pas de données)
  - Réception d'un « ICMP port unreachable » ( type 3)➔ port fermé
  - Réception d'une réponse UDP ➔ port ouvert
  - Pas de réponse ➔ le port peut être « open/filtered »: port ouvert ou des filtres de paquets bloquent la communication



# UDP scan

- Technique: envoyer  un paquet UDP vide (pas de données)
  - Réception d'un « ICMP port unreachable » ( type 3)➔ port fermé
  - Réception d'une réponse UDP ➔ port ouvert
  - Pas de réponse ➔ le port peut être « open/filtered »: port ouvert ou des filtres de paquets bloquent la communication