Exploitation

Ecoute du trafic sur un réseau local

Attaque de type « Man In The Middle »

- Objectifs généraux
  - Récupérer les objets sensibles (logins,mots de passe…)
  - Détourner des flux réseaux et les modifier
  - Profiter des liens de confiance entre machines
- Vulnérabilités
  - Réseaux non segmentés
  - Protocoles non chiffrés ou vulnérables
- Remarque

  Le chiffrement n’est plus une protection si les clés sont compromises…

Exploitation

Ecoute du trafic sur un réseau local

Attaque de type « Man In The Middle »

- Prérequis
  - Corrompre le cache ARP d'une ou plusieurs machines
  - Activer le « forwarding » :
    - Linux : `%echo 1 > /proc/sys/net/ipv4/ip_forward`
    - Windows : `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, clé « IPEnableRouter », valeur = 1`