

La découverte des hôtes sur un réseau permet d'obtenir la liste des adresses IP des machines présentes sur le réseau. A quoi peut bien servir cette liste ?

1. Réseaux locaux

Dans cette partie on recherche les hôtes présents sur un réseau local (LAN) auquel on a accès.

- Comment faire pour obtenir la plage des adresses IP potentielles ?
- Est-il possible de passer à côté de certaines machines ?
- Quelle sécurité est apportée par l'utilisation de VLAN ?
- Supposons que l'on pingue (ICMP Echo Request) une adresse du LAN. Quels sont les échanges sur le réseau ?
- Proposer une solution qui ne nécessite pas l'envoi d'un ping.
- Proposer une solution qui permette d'interdire ou de limiter la découverte de réseau

2. ICMP

Une méthode simple de découverte de réseau est le ping classique (ICMP Echo Request).

- Hors du réseau local, comment faire pour identifier les plages d'adresses IP potentielles ?
- Montrer les trames échangées à travers l'internet lorsqu'on utilise cette méthode.
- Comment bloquer cette méthode.
- Le protocole ICMP permet d'envoyer d'autres types de message que Echo Request. TimeStamp Request demande au destinataire un horodatage, par exemple, pour mesurer le temps de transit d'un paquet. Montrer que ce type de message permet d'identifier les hôtes.
- Comment se protéger de ce type de technologie de découverte ?