IUT de Béziers	Travaux dirigés	R1.11
Réseaux et Télécoms		
Université de Montpellier	Technologies de découverte des hôtes partie 2	Cybersécurité

La découverte des hôtes peut utiliser diverses technologies depuis les couches basses (partie 1 du TD) jusqu'aux couches de transport.

1. Utilisation d'un scanner de port TCP

Lorsqu'une machine est serveur TCP elle répond forcément aux demandes de connexions pour les services qu'elle propose.

a) Rappeler les trames échangées lors d'une connexion TCP
b) Comment faire pour découvrir les serveurs web d'un réseau ?
c) En général, une fois la connexion TCP établie le serveur commence à logger les éléments de la connexion. En quoi cela est-il utile ?
d) La trame TCP portant le flag RST demande au destinataire de réinitialiser la connexion TCP en cours. De même, avec le flag FIN cela demande de mettre fin à une connexion. Comment utiliser ces trames pour optimiser la découverte TCP tout en limitant les traces.
e) Pourquoi cela rend la détection plus difficile ?
f) Comment se protéger de ces technologies de découverte ?

2. Utilisation d'un scanner de port UDP

Lorsqu'une machine est serveur UDP, DNS par exemple, elle répond forcément aux demandes de connexions pour les services qu'elle propose.

a) Rappeler les trames échangées lors d'une connexion UDP
b) Comment utiliser des trames UDP pour découvrir des machines ?
c) Comment se protéger ?

3. Usurpation d'adresse MAC et IP

Lors de la phase de découverte on ne souhaite pas forcément être soi-même découvert. Dans ce cas on peut utiliser une adresse IP source qui n'est pas la notre.

a) Quelle conséquence cela va-t-il avoir pour la trame réponse de l'équipement scanné ?
b) Comment faire alors exploiter pleinement cette méthode
c) Il est également possible de falsifier l'adresse MAC de l'émetteur. Quel intérêt cela peut-il avoir et dans quelle situation ?