
Système & Réseau TD
INSA
INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN
3
Avez-vous ?
• NMAP
Wifi à utiliser :
TdReseauGm3
www.wooclap.com/XONDAT

Les TD : à voir aujourd'hui

- Différence LAN et hors LAN
- Tracer sa route
- Analyse des hôtes du réseau local
- Analyse des services proposés par un hôte
- Recherche longue sur un ensemble de protocoles

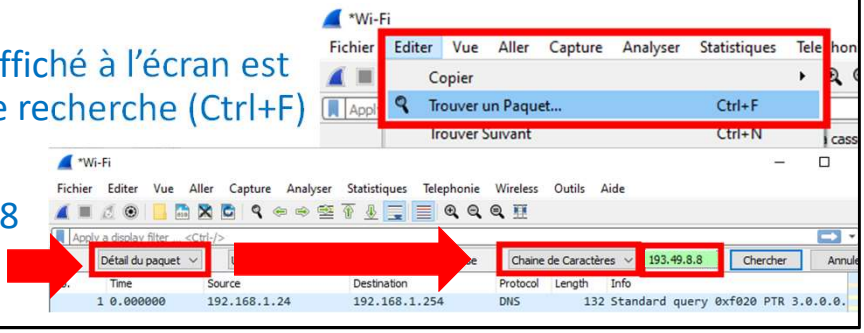
Différences de fonctionnement entre réseau local et hors réseau local

Test 1 : Sortir du réseau local

- Faire une nouvelle capture Wireshark
- Lancer un seul ping sur l'adresse IP 193.49.8.8 (IP publique de l'INSA)
  `ping 193.49.8.8 -c 1`
- Stopper et analyser la capture
  (Qui répond [IP/MAC] ? Avec quel protocole ?)

Si le nombre de trames affiché à l'écran est élevé, afficher la zone de recherche (Ctrl+F)

Rechercher l'IP 193.49.8.8



La recherche doit vous amener sur une série de requêtes ICMP infructueuses.
L'adresse IP n'appartenant pas à votre réseau, la communication est transmise à la couche IP
Note : les résultats seraient identiques avec une adresse ip qui répondrait. Le nombre de lignes serait juste moindre et moins visible pour le TD.
Note 2 : Si un ping est fait vers une IP non existante du réseau local, alors ICMP n'est pas activé car ARP est infructueux.

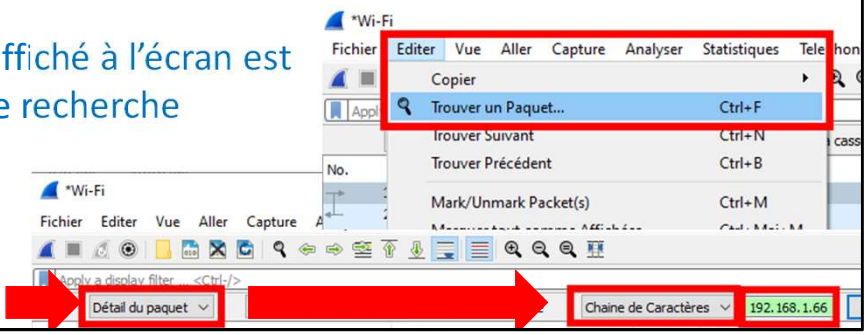
Test 2 : Comparaison avec le réseau local

- Faire une nouvelle capture Wireshark
- Faire un ping sur une adresse IP non utilisée dans votre réseau (privé)
- Stopper puis analyser la capture (192.168.4.166)
  (Qui répond (IP/MAC) ? Avec quel protocole ?)

Si le nombre de trames affiché à l'écran est élevé, afficher la zone de recherche

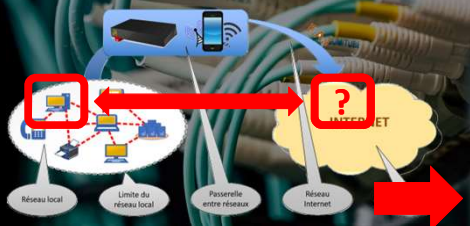
Rechercher l'IP choisie.

Note : Ici je cherche l'IP 192.168.1.66



La recherche doit vous amener sur une série de requêtes ARP infructueuses.
L'adresse IP appartenant a votre réseau, la communication est directe et doit utiliser l'adresse physique du destinataire.
C'est que ce cherche à obtenir ARP

« La route vers l'Internet »



Application + Présentation + Session

Transport

Réseau

Liaison de données

Physique

Le chemin vers le destinataire

Chacun sa route, chacun son chemin

Cherchons le chemin utilisé pour aller vers un hôte distant

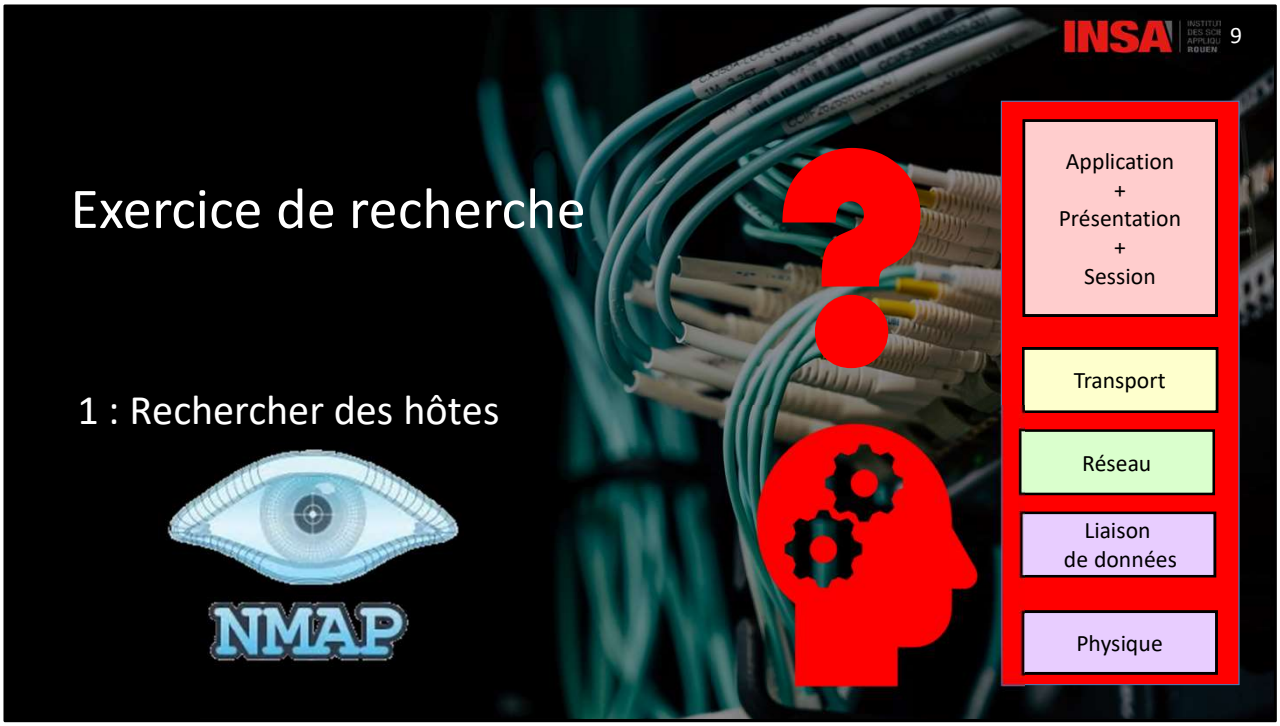
- Saisir :
  `tracert -4 -d 193.49.10.217` (windows)
  `tracepath -4 193.49.10.217` (linux)
- Saisir :
  `tracepath -4 -n google.fr` (linux)
  `tracert -4 -d google.fr` (windows)

  D'où est géographiquement la dernière IP visible ?
  Aidez-vous du site : https://ip-info.org/fr

- Quel élément est-il possible de reconnaitre ?

tracepath / tracert sont des commandes qui permettent de connaitre les routeurs traversés, notre route, pour atteindre un destinataire.
Il est possible de reconnaitre l'IP de notre passerelle lors de la capture.
A ce jour, les informations obtenues avec un Linux peuvent être différentes de celles d'un Windows du fait d'un fonctionnement différent des deux commandes (test UDP sous Linux et ICMP sous Windows, sous Linux, l'option –I = ICMP)
L'option -4 force l'utilisation d'IPv4
Sous Windows, l'option –d empêche la récupération d'un éventuel nom associé à l'adresse IP (+ rapide)

Exercice de recherche



1 : Rechercher des hôtes

Recherche d'hôtes sur le réseau local

Dans un terminal, ou avec l'interface graphique Zenmap :

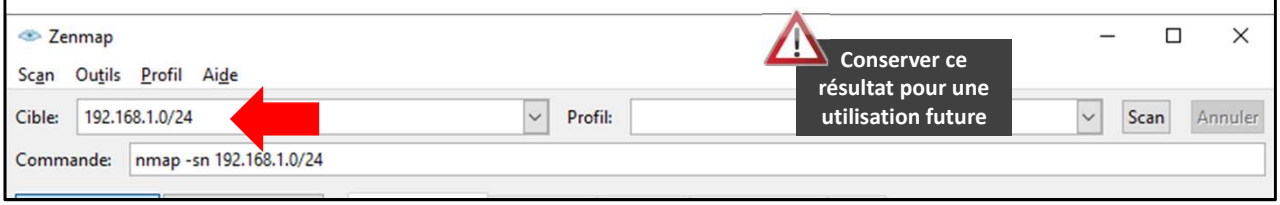
Sous Windows, nmap est dans le dossier C:\Program Files (x86)\Nmap

- Saisir nmap –sn 'Adresse IP réseau/masque réseau CIDR'

  Exemple, si votre IP est 10.1.2.3 sur un réseau en /8 alors il faut saisir

  `nmap -sn 10.0.0.0/8`

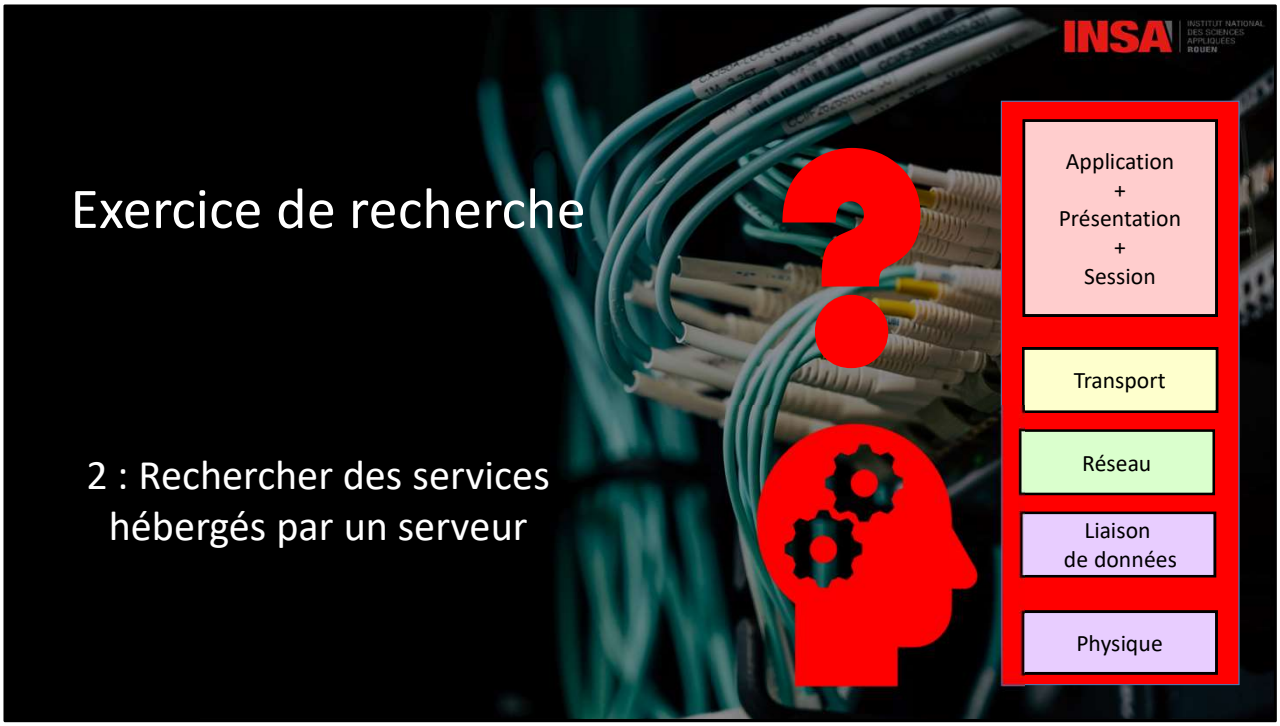
  L'option –sn teste seulement la présence d'hôte sur le réseau indiqué



NMAP permet de rechercher les hôtes dans un réseau.
Ici, il va tester la présence de tous les hôtes possible (/8) du réseau (10.0.0.0) ce qui risque d'être assez long ☺
Ici, l'option –sn ne teste que la présence d'hôtes sur le réseau en sautant la longue phase 'test de service' abordée plus tard

Exercice de recherche

2 : Rechercher des services hébergés par un serveur



Analyse : recherche de services sur un hôte du réseau

Dans un terminal, ou avec l'interface graphique Zenmap :
Sous Windows, nmap est dans le dossier C:\Program Files (x86)\Nmap

Ici nous ne scannons pas un réseau mais une seule adresse IP.
La recherche inclus les services hébergés par l'hôte scanné.

- **`nmap -T4 -F 'adresse de votre passerelle'`**

  Exemple, si votre passerelle possède l'IP 192.168.1.254 alors il faut saisir
  `nmap -T4 -F 192.168.1.254`

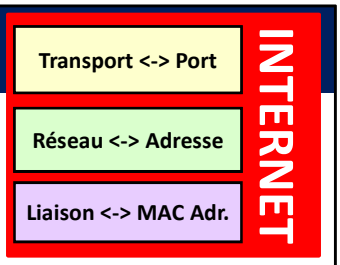
Note : les options –T4 et –F servent à accélérer le test.

L'option –T4 contrôle la vitesse du scan
-F , pour fast, scanne moins de ports que le scan par défaut
-A cherche l'OS de destination et sa version
- v rend nmap plus verbeux

Astuce pour connaitre les informations du dhcp sans faire une demande d'adresse :
nmap -sU -p 67 --script=dhcp-discover 'Adresse IP du serveur DHCP'
-sU = scan UDP –p67 = sur le port 67 –script = lance un script d'analyse, ici le dhcp-discover
Liste des scripts ici : https://nmap.org/nsedoc/scripts/

Les ports : source d'identification

15



Connus : 0 à 1023 sont utilisés par les OS

Enregistrés : 1024 à 49151 (par l'IANA)

Dynamique : 49152 ($2^{15}+2^{14}$) à 65535 (non enregistrable)

Pour donner une indication sur les services disponibles, nmap se base sur une carte de services visibles dans le fichier **services**. (/etc/services Linux, c:\windows\system32\drivers\etc\services Windows)

Port	Utilisation	Port	Utilisation
20,21	FTP (File Transfert Protocol)	22	SSH (Secure Shell = terminal distant sécurisé)
23	Telnet (Terminal distant non sécurisé)	25	SMTP (Simple Mail Transfert Protocol)
53	DNS (Domaine Name System)	68	DHCP (Dynamic Host Control Protocol)
80	HTTP (Hyper Text Transfert Protocol)	110	POP3 (Post Office Protocole)
137-139	Netbios Windows	143	IMAP (Internet Message Access Protocol)
443	HTTPs (HTTP sécurisé par certificats)	993	IMAPs
995	POP3s (Post Office Protocol)	389	Annuaire LDAP (Lightweight Directory Access P.)
3389	RDP (Remote Desktop : bureau distant)	5900	VNC (contrôle distant)

Les 1024 premiers ports sont difficilement utilisable si vous n'êtes pas administrateur du poste.
Les ports dynamiques sont utilisés aléatoirement par le système d'exploitation lors d'une connexion à un service, qui lui sera fixe, exemple, la connexion a du HTTP va utiliser un port entre 49152 et 65535 (client) mais va directement aller sur le port 80 (serveur).
49152 = 2^16 – 2^14. On utilise les 2^14 (16384) derniers ports pour la partie dynamique

Démo

L’interface de notre box

Affichage lors du TD de l’interface Web d’administration de notre petit boitier.

FIN DU TD 3