Semaine 8 : Réseau et nmap
IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

14 novembre 2022

Pour cette séance d'exercice, nous utiliserons l'outil en ligne de commande *nmap* pour effectuer plusieurs scans d'hôtes et réseaux autant locaux que distant.

L'essentiel des exercices se fera dans un réseau de test mit en place à l'école pour la durée de ce labo. Afin d'atteindre ce réseau, vous devrez vous connectez au jumphost *ssh* suivant :

ipl@172.17.50.1

par exemple en utilisant le logiciel *Putty*. Le mot de passe de cette utilisateur est *ipl*

Quelques points important :

- Considérez le scan de port comme illégal, ne scannez que des adresses et réseaux que vous êtes autorisé à scanner et pensez aux réseaux intermédiaire qui vont être traversé et subir le trafic que vous allez générer.
- Le scan de port, comme le réseau de manière général, n'est pas une science exacte. IP est « best effort ». Un « coup de lag » soudain sur le réseau ou de la machine ciblé peut altérer vos résultats tout comme la version de *nmap* que vous utilisez.
- Vous êtes plusieurs à effectuer les mêmes exercices au même moment. Cela va générer un trafic important et beaucoup de bruit sur les cibles. Essayez de faire preuve de bon sens et de toujours utiliser la méthode la moins nuisible/bruyante pour résoudre les exercices.
- Le premier exemple dans le *man* de *nmap* : *nmap -A -T4* n'est pas un si bon exemple que ça. Si vous lisez un peu plus loin dans le man :
  - *-A (Aggressive scan options)*
  - *-T (Set a timing template) (...) aggressive (4).*

  Maintenant, relisez le point précédent ;-).

Exercices

1. Dans un premier temps, nous allons nous intéresser aux réseaux 10.40.0.0/29 et 172.22.22.0/27 :
   - Que veulent dire ces réseaux :
     - À quoi correspond la première partie ? 10.40.0.0 et 172.22.22.0 Ce sont les addresses du réseau
     - À quoi correspond la deuxième partie ? /29 et /27 Masque de sous-réseau
     - Quels sont les adresses IP contenues dans ces réseaux ? /29 /27
     - Quels sont les hôtes potentiellement contenu dans ce réseau ? 6 ip 30 ip
     - Comment pouvons-nous calculer ces valeurs ? Avec le masque et l'ip de base
   - Procédez à un ping scan, combien d'hôtes sont visible sur ce réseau, à quelles IP ? nmap -sn 10.40.0.0/29
   - Une fois les hôtes trouvés, effectuez un scan rapide des ports les plus courant sur ces hôtes pour tenter d'identifier leur fonction dans le réseau. nmap -sV 10.40.0.2
   - Dans le 1er réseau (10.40.0.0/29), un des hôtes semble ne pas avoir de port « courant » ouvert. Et si vous effectuiez un scan de tous les ports de cet hôte ? Vous semble-t-il à sa place ? nmap -p- 10.40.0.1
2. Le réseau 172.22.22.128/25 dispose d'un hôte qui a choisi d'exposer son serveur SSH sur un port différent du 22. Commencez par trouver cet hôte puis son port SSH. Comment pouvez-vous vous assurer que ce port est bien celui pour SSH ? (Avec nmap, bien sûr !) nmap 172.22.22.128/25 et nmap -p- 172.22.22.250
3. Le réseau 10.10.0.0/24 dispose, en plus de votre jumphost, de 3 autres hôtes. Scannez les ! Quels sont les services exposés ? Les connaissez-vous ? Que fait chacun de ces services ? nmap 10.10.0.0/24
4. Le projet nmap dispose de plusieurs hôtes mises à la disposition des apprentis scanner, s'il vous reste du temps, pourquoi ne pas en profiter pour les scanner également ?
   - scanme.nmap.org
   - 45.33.49.119
5. Bonus : Avec les différents informations collectés lors des exercices 1 à 3 et éventuellement quelques scans/traceroute supplémentaires, essayez de retracer le schéma du réseau que vous avez exploré.