PROJET - 2ème année - RSA Réseaux
2017-2018

MyNmap

Modalités

— Le PROJET sera réalisé en binôme. Il est à rendre pour le **vendredi 11 mai 2018**.
— Le rapport (format pdf) ainsi que les sources devront être déposés sous arche (format tar.gz). Aux sources devront être ajoutés un README et un makefile.
— Les soutenances seront organisées **la semaine du 14 au 18 mai 2018**.

Vous devez utiliser la plate-forme GitLab de l'école pour héberger une version de votre programme. Il sera privé et son identifiant sera de la forme Projet_RSA_Nom1_Nom2 (où Nom1 et Nom2 correspondent aux noms des membres du binôme). Donnez également les droits d'accès à Rémi Badonnel et à moi-même.

Tout projet non rendu pour le 11‡rt mai 2018 implique que le groupe est considéré comme démissionnaire du module et en conséquence ne pourra pas valider l'UE correspondant pour l'année universitaire 2017-2018.

Toute personne ne se présentant pas à la soutenance sera considérée comme démissionnaire du module et en conséquence ne pourra pas valider l'UE correspondant pour l'année universitaire 2017-2018.

Sujet

L'objectif de ce TP est de réaliser un "scanner simplifié" de ports à l'instar du logiciel nmap `https://nmap.org/`. Cet outil permet de connaître les ports qui sont ouverts sur les machines d'un réseau, de déterminer les services associés et éventuellement les systèmes d'exploitation hébergeant ces services. Une description plus complète des techniques de scan, est donnée dans [1].

Vous aurez à votre disposition un réseau de tests sur lequel sont connectées des machines avec des systèmes d'exploitation et des services différents. Les conditions d'accès à ce réseau vous seront communiquées ultérieurement. Attention, n'oubliez pas que les outils de scan réseaux peuvent être considérés comme des outils d'attaque. Il vous est donc demandé de ne pas utiliser de tels logiciels dans des environnements opérationnels.

Pour information, lors de la soutenance, le réseau de test sera re-configuré et ne sera donc pas identique à celui utilisé lors de vos différents tests. L'idée est d'évaluer l'adaptabilité de votre outil.

Le travail devra être organisé en plusieurs étapes qui apparaîtront dans des sous-répertoires différents. Le rapport soumis présentera et analysera ces étapes. Une version graphique pour votre logiciel MyNmap sera un plus.

1. Il s'agira dans un premier temps de déterminer les adresses IP des machines actives se trouvant sur le réseau local de test. Pour cela vous devrez envoyer des messages ICMP (echo request) en utilisant des sockets raw. Vous afficherez quelles sont les machines actives sur le réseau.

2. Pour chacune de ces machines actives, vous devrez déterminer et afficher les ports ouverts en TCP. Vous implanterez les quatre techniques suivantes :
   (a) **TCP scan.** C'est une méthode classique pour identifier les ports ouverts et/ou fermés sans terminer

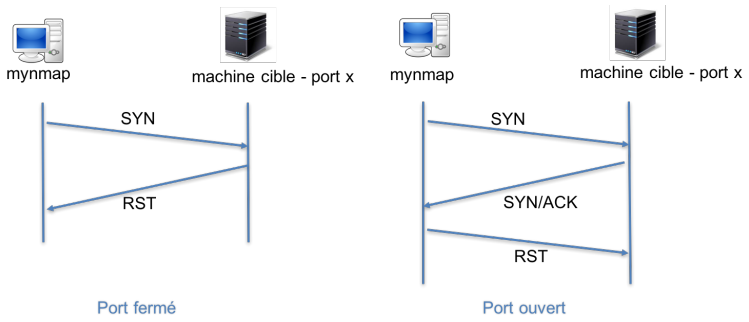

FIGURE 1 – TCP SYN scan

complètement le three-way handshake de TCP. Comme l'indique la Figure 1, quand le port x est fermé la machine cible envoie un segment TCP avec le flag RST positionné et lorsque le port est ouvert, un SYN-ACK est retourné.

(b) **TCP SYN/ACK scan.** Une méthode plus discrète et moins détectable par les systèmes de détection d'intrusion peut aussi être utilisée. Dans ce cas, l'envoi d'un segment TCP avec les flags SYN et ACK positionnés génère de la part de la machine cible un segment RST si le port est fermé et aucune réponse si le port est ouvert (cf. Figure 2).

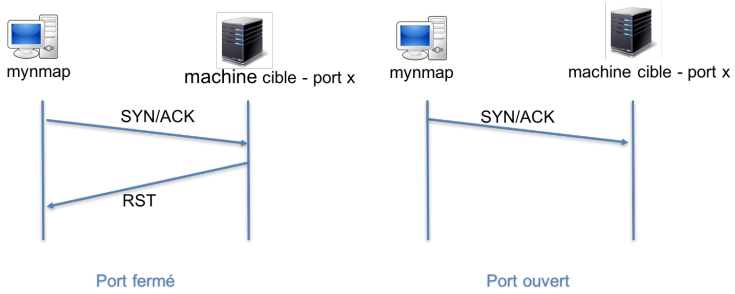

FIGURE 2 – TCP SYN/ACK scan

(c) **TCP IDLE scan.** Une autre méthode encore plus discrète mais plus complexe est d'utiliser une machine (zombie) qui fera le scan pour vous.

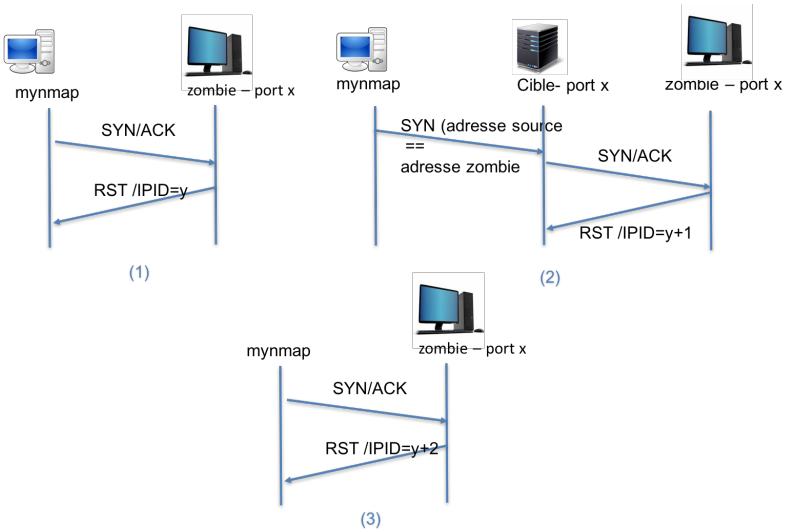

FIGURE 3 – TCP IDLE scan (spoofing)

Cette technique utilise l'identification des paquets IP ainsi que le *spoofing* (usurpation) d'adresse IP comme illustré dans la Figure 3.

L'idée est la suivante. Votre logiciel de scan envoie tout d'abord un segment TCP avec les flags SYN/ACK à la machine zombie qui retourne un RST (port fermé) avec un ID de paquet y. Il envoie ensuite une demande de connexion TCP (segment SYN) à la machine cible en se faisant passer pour la machine zombie. La machine cible, si le port est ouvert, retourne alors un segment TCP SYN/ACK à la machine zombie qui génère un RST avec un ID de paquet de $y + 1$. Votre logiciel de scan émet de nouveau un segment TCP avec les flags SYN/ACK à la machine zombie qui retourne un RST avec un ID de paquet $y + 2$ si le port était ouvert sur la machine cible.

Pour que le mécanisme fonctionne, il faut que la machine dite *zombie* ne gère aucune autre session TCP durant le scan (état IDLE de l'automate TCP). Le mieux est donc de choisir une machine TCP sur laquelle ne tourne aucun service. Il faut également vérifier, avant de réaliser le scan, que les numéros d'identification des paquets IP sont gérés de manière cohérente et prédictible.

(d) Lorsque vous aurez déterminer l'adresse d'une machine avec un serveur ftp, vous utiliserez ce serveur ftp comme proxy entre votre logiciel de scan et la machine cible. L'idée est de profiter du fait que le protocole FTP gère des connexions TCP différentes pour la partie contrôle et pour la partie données.

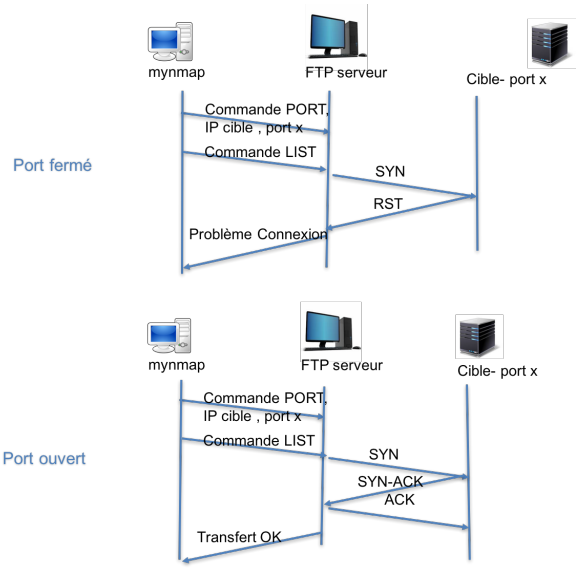

FIGURE 4 – FTP proxy

Comme l'indique la Figure 4, il faut activer tout d'abord le serveur FTP en mode actif en lui envoyant une commande PORT avec l'adresse IP de la machine cible et le port souhaité. Il s'agira ensuite d'émettre une commande FTP qui génère des données (exemple LIST). Ainsi, le serveur ftp essaiera de se connecter sur la machine cible. Si le port est fermé, un segment TCP avec le flag RST sera retourné au serveur qui enverra sur la connexion de contrôle un message d'erreur. Si le port est ouvert, un message confirmant le transfert effectué sera émis.

3. Pour chacune de ces machines, vous devrez déterminer et afficher les ports ouverts en UDP. Comme il n'y a pas de connexion en UDP, l'indication du port fermé est signalée par la réception d'un message ICMP (cf. Figure 5).

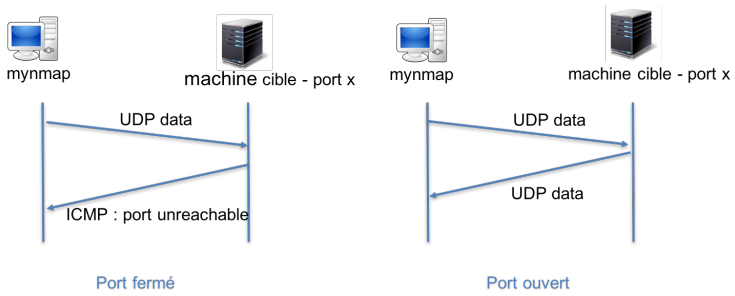

FIGURE 5 – UDP scan

4. Pour l'ensemble des ports ouverts sur les différentes machines, vous essaierez, dans la mesure du possible, de déterminer la version du service et éventuellement de déterminer le système d'exploitaion (windows ou linux).

Références

[1] Bou-Harb, E., Debbabi, M., & Assi, C. (2014). Cyber scanning : a comprehensive survey. IEEE Communications Surveys & Tutorials, 16(3), 1496-1519.