Sécurité des réseaux informatique TP : Utilisation de Nmap.

Gil DE GROVE

12 novembre 2012

1 Utilisation de Nmap

Lors du début du TP, nous avons du installer NMap. Nmap comme beacoup de commande utilisé dans un TTY linux, peut est facilement changée et adapté á ses besoins grâce á l'utilisation des options. Comme première prise en main, j'ai pu utilisé la commande :

nmap -sP 10.4.35.*

Cette commande permet de lister les hotes disponnible sur le réseau et en ligne (ping scan).

Ceci n'est qu'une commande utlisé pour une prise en main. Il sera expliqué plus longuement lors de la suite de ce document.

2 Analyse du fonctionnement de Nmap

Pour utiliser une option plus spécifique lors de l'utilisation de Nmap, il suffit de la connaitre et de la mettre derrière un "-"

- ***-sS (Scan TCP SYN)***
  Le scan SYN est celui par défaut et le plus populaire pour de bonnes raisons. Il peut être exécuté rapidement et scanner des milliers de ports par seconde sur un réseau rapide lorsqu'il n'est pas entravé par des pare-feux. Le scan SYN est relativement discret et furtif, vu qu'il ne termine jamais les connexions TCP. Il marche également contre toute pile respectant TCP, au lieu de dépendre des particularités environnementales spécifiques comme les scans Fin/Null/Xmas, Maimon ou Idle le sont. Il permet de plus une différentiation fiable entre les états ouvert, fermé et filtré. option permet [1]

1. pour plus d'information consulté le site http ://nmap.org/man/fr/man-port-scanning-techniques.html

– ***-sT(Scan TCP connect())***
Le scan TCP connect() est le type de scan par défaut quand le SYN n'est pas utilisable. Tel est le cas lorsque l'utilisateur n'a pas les privilèges pour les paquets bruts (raw packets) ou lors d'un scan de réseaux IPv6. Plutôt que d'écrire des paquets bruts comme le font la plupart des autres types de scan, Nmap demande au système d'exploitation qui l'exécute d'établir une connexion au port de la machine cible grâce à l'appel système connect(). C'est le même appel système haut-niveau qui est appelé par les navigateurs Web, les clients P2P et la plupart des applications réseaux qui veulent établir une connexion. Cet appel fait partie de l'interface d'application connue sous le nom de « Berkeley Sockets API ». Au lieu de lire les réponses brutes sur le support physique, Nmap utilise cette application API pour obtenir l'état de chaque tentative de connexion.
– ***-sU(Scan UDP)***
Même si les services les plus connus d'Internet son basés sur le protocole TCP, les services UDP sont aussi largement utilisés. DNS, SNMP ou DHCP (ports 53, 161/162 et 67/68) sont les trois exemples les plus courants. Comme le scan UDP est généralement plus lent et plus difficile que TCP, certains auditeurs de sécurité les ignorent. C'est une erreur, car les services UDP exploitables sont courants et les attaquants eux ne les ignoreront pas. Par chance, Nmap peut aider à répertorier les ports UDP.
Le scan UDP est activé avec l'option-sU. Il peut être combiné avec un scan TCP, comme le scan SYN (-sS), pour vérifier les deux protocoles lors de la même exécution de Nmap.
– ***-sN ; -sF ; -sX (Scans TCP Null, FIN et Xmas)***
Ces trois types de scans (d'autres sont possibles en utilisant l'option –scanflags décrite dans la section suivante) exploitent une subtile faille de la RFC TCP pour différencier les ports entre ouverts et fermés. La page 65 indique que "si le port [de destination] est dans l'état fermé... un segment ne contenant pas le drapeau RST provoque l'émission d'un paquet RST comme réponse.". La page suivante indique que pour les paquets envoyés à des ports sans aucun des drapeaux SYN, RST ou ACK activés : "il est peut vraisemblable que cela arrive, mais si cela est le cas, il faut rejeter le segment."
Pour les systèmes respectant ce texte de la RFC, chaque paquet ne contenant ni SYN, ni RST, ni ACK se voit renvoyé un RST si le port est fermé et aucune réponse si le port est ouvert. Tant qu'aucun de ces drapeaux n'est utilisé, toute combinaison des trois autres (FIN, PSH et URG) son valides. Nmap exploite cela avec les trois types de scans :
  – Scan Null (-sN)
  N'active aucun des bits (les drapeaux de l'en-tête TCP vaut 0).
  – Scan FIN (-sF)

N'active que le bit FIN.

– Scan Xmas (-sX)
  Active les drapeaux FIN, PSH et URG, illuminant le paquet comme un arbre de Noël .

Ces trois types de scan ont exactement le même comportement, sauf pour les drapeaux TCP utilisés dans des paquets de tests (probes packets). Si un RST est reçu, le port est considéré comme étant fermé, tandis qu'une absence de réponse signifiera qu'il est dans l'état ouvert|filtré. Le port est marqué comme filtré si un message d'erreur ICMP « unreachable (type 3, code 1, 2, 3, 9, 10 ou 13) » est reçu.

– ***-sO(Scan du protocole IP)***
  Le scan du protocole IP permet de déterminer quels protocoles IP (TCP, ICMP, IGMP, etc.) sont supportés par les cibles. Ce n'est donc pas techniquement un scan de ports, car Nmap essaie les différents numéros de protocoles IP à la place des numéros de ports TCP ou UDP. Ce scan permet néanmoins d'utiliser l'option -p pour sélectionner les numéros de protocoles à scanner – le rapport de Nmap étant toujours dans le style habituel des tables de ports – et utilise le même moteur de scan utilisé pour le scan de ports. Ainsi, cette technique est suffisamment proche du scan de port pour être présenté ici [2].

2. pour plus d'information consulté le site http ://nmap.org/man/fr/man-port-scanning-techniques.html