Sécurité des Réseaux - TP5

Nmap

Monroe Samuel

30 décembre 2015

1 Préambule

J'ai réalisé ce tp dans un LAN domestique, ma machine sur laquelle j'utilise Nmap est un OSX 10.11 avec Nmap 6.49BETA5, je fais également tourner un VM CentOS Security, et d'autres appareils appartenant à ma famille fonctionnent dans ce LAN.

2 Utilisation de Nmap

Un Scan **nmap -Sp** du réseau me renvoie ma propre machine et l'ip du routeur.

Un Scan **nmap -Pn** du réseau me renvoie également une machine windows dont je sais que l'adresse IP est 192.168.1.3.

Je me trouve dans un réseau domestique **192.168.1.0/24**, pour commencer je vais lançer la commande **nmap -A** qui est censée selon la man page, me ramener la version des OS et logiciels utilisés sur les machines du réseau.

— Je commence avec l'adresse 192.168.1.1, j'apprend de celui-ci que le port 23 Telnet est ouvert mais également le port 80 HTTP (plate-forme web d'administration) et a pour titre Proximus, ainsi que le port 443 HTTPS.

  L'appareil est un router de marque **Sagem**.

  Un scan de version d'OS m'informera également sur les informations suivantes :

  — MAC Address : 6C :2E :85 :09 :89 :8D (Sagemcom)
  — Device type : WAP **Confirmation que c'est un router wi-fi**
  — Running : Linux 2.6.X
  — OS CPE : cpe :/o :linux :linux_kernel :2.6.13
  — OS details : Linux 2.6.13 (embedded)
  — Uptime guess : 2.271 days (since Sat Nov 7 12 :21 :12 2015)

— Un PC Windows 10 tourne à l'adresse 192.168.1.3 mais n'a pas été découvert lors du mappage par ping.

  La version de l'OS est obtenable via la commande **nmap -O -v ip**, en la tentant sur cet appareil, nmap me renvoie que la plus grande probabilité est que l'os soit un Windows Phone, ce qui est plus ou moins probant, Windows 10 étant conçu pour être un OS commun au parc des appareils Windows.

  Au niveau des services qui tournent sur celui-ci, j'obtiens via -A -T4 :

  — 135/tcp open msrpc
  — 139/tcp open netbios-ssn
  — 445/tcp open microsoft-ds
  — 1801/tcp open msmq
  — 2103/tcp open zephyr-clt
  — 2105/tcp open eklogin
  — 2107/tcp open msmq-mgmt
  — 5357/tcp open wsdapi