Nmap, scanneur de ports

Soumis par VieuxProf
01-01-1999
Dernière mise à jour : 03-02-2008

- Nmap est un logiciel de scan des ports sur une machine ou un réseau distant.

- Il permet d'obtenir de nombreuses informations concernant la configuration TCP/IP de la machine-cible ou du réseau-cible et est très utile pour déceler des failles éventuelles de sécurité.

- Pour des informations complémentaires : http://www.insecure.org/nmap

{mospagebreak title=Utiles}

nmap [options] [hostname|ip|network]
scan des ports de la machine hostname ou du réseau network

/etc/services
description générale des services et des numéros de ports

/etc/inetd.conf, /etc/xinetd.conf
paramétrage général des ouvertures et fermetures de ports (suivi de # kill -HUP inetd)

nmap [-sS] -v -p 80 '127-222.*.2.3-5'
scan du port 80 pour les machines dont les IP se terminent en 2.3, 2.4, 2.5 sur les réseaux de 127.* à 222.* (réseaux IMHO)

host -l mondomaine.com | cut '-d ' -f 4 | ./nmap -v -i -
détermine l'ensemble des hôtes et leurs IP sur mondomaine.com en simulant un transfert de zone DNS (à tester)

{mospagebreak title=Quelques options}

-sS
scan SYN en half-open (scan sans trace)

-sF
idem -sS pour une machine-cible Linux

(par comparaison avec -sS, on sait si une machine est de type Windows ou Unix)

-v
mode verbose

-O
scan avec recherche du système d'exploitation

-p 80
scan sur le port 80