Nmap 3.84ALPHA1, un appel aux testeurs

Cette nouvelle mouture de 'nmap' ne compte pas moins de 34 changements et nouvelles fonctionnalités significatives dont nous décrivons les plus importantes ici.

Quelques changements mineurs sont également consignés dans l'annonce que Fyodor permet de consulter à cette adresse: https://seclists.org/lists/nmap-dev/2005/Jul-Sep/0041.html. **Raw Ethernet vs Raw Socket** 'Nmap' possède désormais la capacité d'envoyer et router proprement des paquets 'Raw Ethernet' contenant des datagrammes IP. Avant cette nouvelle fonctionnalité, 'Nmap' acheminait les paquets en utilisant les 'Raw Socket'. Cette nouveauté vient contrecarrer l'action de Microsoft qui avait désactivé le support 'Raw Socket' au sein de Windows XP SP2. Au démarrage d'un scan, 'Nmap' choisit donc la méthode la mieux appropriée. **ARP Ping** 'Nmap' peut désormais envoyer des requêtes ARP afin de déterminer si une machine est active sur le LAN. Auparavant, 'Nmap' reposait sur des résultats provenant des couches IP plus élevées, limitant ainsi le champ d'action du logiciel à un réseau local sans router. **Toujours plus d'empreintes et de services** Environ 350 nouvelles empreintes de systèmes d'exploitations ont été rajoutées au moteur de détection d'OS (OS fingerprinting). Les plus remarquables sont celles de Mac IS 10.4 (Tiger), OpenBSD 3.7, FreeBSD 5.4, Windows Server 2003 SP1, Sony AIBO? Les derniers noyaux linux n'ont pas été épargnés ainsi que l'IOS Cisco 12.4, les nouveaux 'firewalls' Fortinet (pare-feu), et divers systèmes de VoIP. De plus, la base de détection de services distants a également été enrichie. À travers cette récente annonce, Fyodor compte sur la communauté pour tester cette dernière version et recueillir le plus d'informations possible de la part des utilisateurs du logiciel Nmap. **Olivier Devaux** pour **Vulnerabilite.com**