|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NMAP** | | | | | |
| **DESC** | | | Exploration réseau + scanner | | |
| **CLI** | | | | | |
| **GENERALE** | | | | | |
| **Nmap [opts] <cible> [<cible2>]** | | Scan CIDR possible ex 192.168.0.0/24  Les bornes sont incluses  Intervalles possibles : 192.168.12.1-40  192.168.1.1,2,3 possible aussi  IPv6 possible mais pas d’intervalles pour IPv6 | | | |
|  | | --reason | | Verbeux | |
|  | | -n | | Pas de résolution DNS | |
|  | | -R | | Toujours faire la résolution DNS | |
|  | | --dns-servers <serveur>, … | |  | |
| **SELECTION CIBLES** | | | | | |
| **nmap** | -iL <file> | | Fichiers de cibles à utiliser  \n ou espace ou tab pour séparer les hôtes | | |
|  | -iR <#hosts> | | Scan aléatoire de #Hosts (@privées et multicast non scannées)  0 = scan sans fin | | |
|  | --exclude <host> [,<host2…] | | Exclusion d’hosts à scanner | | |
|  | --excludefile <file> | | Fichier d’exclusion | | |
| **PING** | | | | | |
| **nmap** | -PN  -P0 | | Ne pas utiliser de scan ping  Pas de découverte d’hôtes donc  Pzero et non PO  De base, NMAP fait un scan approfondi s’il trouve une machine active ; ici, scan approfondi sur toutes les machines du réseau | | |
|  | -PS[<port>, <port2>…] | | **TCP SYN** sur le port  Par défaut port 80   * RST en retour si port fermé * SYN SYN/ACK RST (RST envoyé par kernel et non NMAP) | | |
|  | -PA[<port>, <port2>…] | | **TCP ACK** sur le port  Mieux que TCP SYN, puisque les pares-feux bloquent généralement TCP SYN sur les services qui ne doivent pas se trouver sur internet.  Mais si pare-feu statefull track une connexion, TCP ACK ne marchera pas des masses. | | |
|  | -PU[<port>, <port2>…] | | Envoie **paquet UDP vide**  Par défaut 31338  Permet de contourner les pares-feux qui ne filtrent que TCP | | |
|  | -PE | | echo | | Ping **ICMP custom** |
|  | -PP | | Timestamp | |
|  | -PM | | Masque d’adresse | |
|  | -PR | | Ping **ARP** | | |
|  | -PO<protocole> | | Envoie **paquet IP** avec champs protocole custom | | |
| **SCAN** | | | | | |
| **nmap** | -sL | | Listing des hôtes du réseau  N’envoie aucun paquet aux hôtes, utilise reverse DNS sur les cibles  Ne signifie pas que ces hôtes sont actifs  **Reverse DNS** | | |
|  | -sP | | Scan PING  Liste donc les hôtes actifs (ayant répondus au ping)  Plus fiable qu’un ping sur le multicast, certain hôte ne répondant pas au ping multicast  Permet de faire un listing des machines pour les admins.  **TCP ACK sur port 80 + ICMP echo**  **Scan ARP si réseau local** | | |
|  | -sT | | **Scan TCP complet**  SYN - SYN/ACK – ACK | | |
|  | -sS | | **Scan SYN**  SYN - SYN/ACK - RST | | |
|  |  | |  | | |
|  | -sU | | **Scan UDP** | | |
|  | -sN | | **Scan Null**  Flags TCP == 0 | | |
|  | -sF | | **Scan Fin**  Flag TCP FIN | | |
|  | -sX | | **Scan Xmas**  Flags SYN PSH URG | | |
|  |  | |  | | |
|  | -A | | Détection OS + version des services | | |
|  | -s0 | | Scan protocole IP | | |
|  | -T4 | | Scan plus rapide | | |
|  |  | |  | | |
|  |  | |  | | |
|  |  | |  | | |
|  |  | |  | | |
| **Comments :**  Prendre en compte que les pares-feux bloquent souvent les pings  Découverte d’hôtes de NMAP va au-delà du simple ping | | | | | |