|  |  |  |  |
| --- | --- | --- | --- |
| **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 | |
| **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 |
| **DECOUVERTE D’HOTES** | | | |
| **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 |
|  | -PN | |  |
|  |  | |  |
|  | -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 | | | |