|  |  |  |  |
| --- | --- | --- | --- |
|  | **Nmap** | | |
| **DESC** | | Scanner réseau | |
| **FILES** | |  | |
| **CLI** | | | |
| **Nmap [Opts] @IP** | |  | Attaque vanilla facilement repérable.  Appel à la fonction connect() sur tous les ports.  Syn – Syn/ack - ack |
|  | | -sS | Syn scan  Syn – Syn/ack |
|  | | -sF | Fin scan  Envoie de requêtes avec flag FIN |
|  | | -sN | Null Scan  Uniquement flag NULL |
|  | | -sX | Xmas scan  Flags FIN/URG/PUSH |
|  | | -O | Détermination du type d’OS  Un OS construit ses paquets d’une façon qui lui est propre |
| **Comments :**  Peut générer du traffic. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Nessus** | | | |
| **DESC** | | |  | |
| **FILES** | | |  | |
| **CLI** | | | | |
|  | | |  | |
|  | | |  | |
|  | | |  | |
| **Comments :** | | | | |
|  | **Netcat** | | | |
| **DESC** | | Etablissement TCP/UDP sur un port et envoie/réception de données | | |
| **FILES** | |  | | |
| **OPTS** | | | | |
| **Nc @IP Port** | |  | |  |
|  | |  | |  |
|  | |  | |  |
| **Comments :** | | | | |

|  |  |  |
| --- | --- | --- |
|  | **Metasploit** | |
| **DESC** | |  |
| **FILES** | |  |
| **OPTS** | | |
|  | |  |
|  | |  |
|  | |  |
| **Comments :** | | |

|  |  |  |
| --- | --- | --- |
|  | **OpenVAS** | |
| **DESC** | | Audit de vulnérabilité |
| **FILES** | |  |
| **OPTS** | | |
|  | |  |
|  | |  |
|  | |  |
| **Comments :** | | |