Tableau synthèse comparatif des outils de découvertes ports et réseaux de Kali Linux.

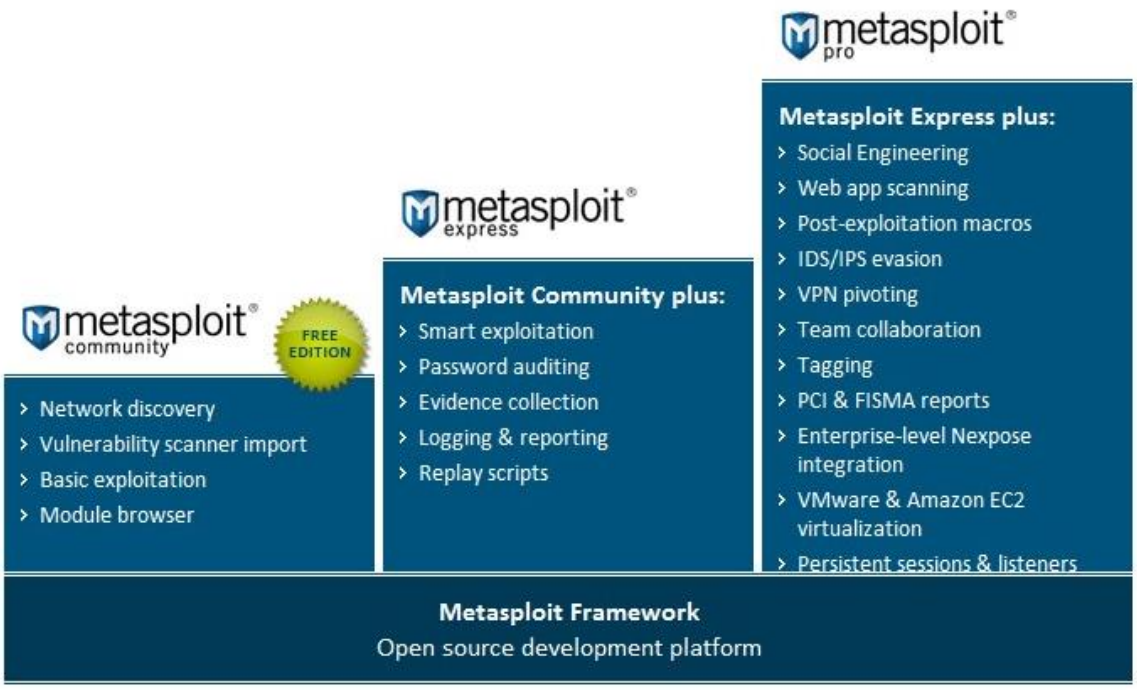
Vous trouverez dans ce document un tableau synthèse comparatif des outils Kali Linux concernant le hacking ethnique et permettant des pénétrations ou encore la découverte de ports et réseaux.

	Nmap :	AdvancedPortScanner :	Metasploit :
Présentation	Nmap est un scanner de ports. Il permet de détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur ou un réseau distant.	Advanced Port Scanner est un analyseur de réseau il permet de déterminer la version des programmes utilisant les ports détectés. L'interface du programme est à la fois riche et intuitive.	Metasploit est un outil pour l'exécution d'exploits contre une machine distante, il permet de tester des vulnérabilités et des failles des systèmes informatiques afin de les rectifier et les protéger, il peut être aussi utiliser par des pirates.
Avantages	- Libre et gratuit	- Gratuit - Permet de trouver rapidement les ports ouverts sur les ordinateurs d'un réseau	- Versions Framework et Community gratuites. – Protection du matériel – Protection des données – Détection de virus et vulnérabilités – Authentification – Alertes – Plugins avec alertes personnalisées – Actions : bloquer les intrusions, bloquer l'IP… – Analyse des données – Accessibilité 24-7
Désavantages	- Uniquement en Anglais		- Versions Pro et Express payantes. - Peut devenir ou service d'outil malicieux.
Caractéristiques			- Metasploit Pro est adapté aux besoins des entreprises : Logiciels

			Grand Compte, Logiciels PME, Logiciels Startup … - Cette application est conseillée pour les métiers : Logiciels Informatique – DSI … - Ce progiciel cloud est utilisé dans les secteurs : Logiciels Généraliste …
Fonctionnalités	- Permet la récupération d'un scan des ports ouverts sur une machine. - S'informer sur le système d'exploitation utilisé sur la machine distante scanné. - Scanner une adresse IP. - Affiche un rapport avec la liste des protocoles et ports ouverts, comme tcp, http, https, ect… - Différentes options de commande pour obtenir un affichage personnalisé	- Analyse de ports multithread. - Accès à distance. - Obtention d'information sur les périphériques réseau. - Accès facile aux ressources trouvées. - Wake-On-LAN et arrêt à distance de l'ordinateur. - Exécution de commandes sur un ordinateur à distance. - Identification des programmes utilisant les ports détectés. - Enregistrer la liste / charger la liste. - Bouton de la barre d'outils Sous-réseau Classe "C" / bouton de la barre d'outil de sous-réseau Ordinateur actuel. - Outils Ping / Tracert / Telnet / SSH.	<u>Collecte :</u> - Importation - Découverte réseau - Exploitation basique <u>Automatisation :</u> - Interface ligne de commande - Exploitation intelligente - Brut-forcing sur identifiants <u>Divers :</u> - Hameçonnage et pushing - Ligne de commande et interface web avec choix avancée.

		- Options Performances / Ressources / Divers - Connexion http / HTTPS / FTP / Radmin / Remote Desktop Protocol.	

(Annexe) - Un simple comparatif des fonctionnalités disponible sur Metasploit en fonction des versions :



(Annexe) – Explication rapide d'un balayage de ports :