Voici un tableau avec les principales commandes Linux utilisées dans le terminal (CMD)

| **Commande** | **Description** |
| --- | --- |
| ls | Liste les fichiers et dossiers du répertoire actuel |
| cd [chemin] | Change de répertoire |
| pwd | Affiche le chemin du répertoire actuel |
| mkdir [nom] | Crée un nouveau dossier |
| rmdir [dossier] | Supprime un dossier vide |
| rm [fichier] | Supprime un fichier |
| rm -r [dossier] | Supprime un dossier et son contenu |
| cp [source] [destination] | Copie un fichier ou un dossier |
| mv [source] [destination] | Déplace ou renomme un fichier ou dossier |
| touch [nom\_fichier] | Crée un fichier vide |
| cat [fichier] | Affiche le contenu d'un fichier |
| nano [fichier] | Édite un fichier avec l’éditeur Nano |
| vim [fichier] | Édite un fichier avec l’éditeur Vim |
| echo "texte" | Affiche un texte dans le terminal |
| echo "texte" > fichier.txt | Écrit du texte dans un fichier (écrase le contenu) |
| echo "texte" >> fichier.txt | Ajoute du texte à un fichier |
| chmod [mode] [fichier] | Change les permissions d’un fichier |
| chown [utilisateur] [fichier] | Change le propriétaire d’un fichier |
| find / -name [fichier] | Recherche un fichier par son nom |
| grep "mot" [fichier] | Recherche un mot dans un fichier |
| df -h | Affiche l’espace disque disponible |
| du -sh [dossier] | Affiche la taille d’un dossier |
| ps aux | Affiche les processus en cours |
| kill [PID] | Termine un processus par son ID |
| top | Affiche les processus en temps réel |
| htop | Version améliorée de top (si installé) |
| free -m | Affiche l’utilisation de la mémoire RAM |
| uname -a | Affiche les informations du système |
| uptime | Affiche le temps de fonctionnement du système |
| whoami | Affiche l’utilisateur connecté |
| id | Affiche l’ID de l’utilisateur actuel |
| history | Affiche l’historique des commandes |
| clear | Efface le terminal |
| reboot | Redémarre le système |
| shutdown -h now | Éteint le système immédiatement |
| man [commande] | Affiche le manuel d’une commande |
| **Archivage et compression** |  |
| tar -cvf archive.tar [dossier] | Crée une archive .tar |
| tar -xvf archive.tar | Décompresse une archive .tar |
| zip -r archive.zip [dossier] | Crée une archive .zip |
| unzip archive.zip | Décompresse une archive .zip |
| **Téléchargement de fichiers** |  |
| wget [url] | Télécharge un fichier depuis une URL |
| curl [url] | Récupère le contenu d’une URL |
| **Mise à jour du système** |  |
| sudo apt update | Met à jour la liste des paquets (Debian/Ubuntu) |
| sudo apt upgrade | Installe les mises à jour des paquets (Debian/Ubuntu) |
| sudo dnf update | Met à jour les paquets (Fedora) |
| sudo yum update | Met à jour les paquets (RedHat/CentOS) |
| **Réseau et diagnostic** |  |
| ping [adresse] | Teste la connectivité avec une adresse IP ou un domaine |
| ifconfig | Affiche les interfaces réseau (obsolète, remplacé par ip a) |
| ip a | Affiche les interfaces réseau et leurs adresses IP |
| ip r | Affiche la table de routage |
| netstat -tulnp | Affiche les connexions réseau actives et les ports ouverts |
| ss -tulnp | Alternative moderne à netstat pour afficher les connexions réseau |
| nslookup [domaine] | Résout un nom de domaine en adresse IP |
| dig [domaine] | Donne des informations DNS détaillées sur un domaine |
| traceroute [adresse] | Montre le chemin emprunté par les paquets pour atteindre une adresse |
| mtr [adresse] | Version améliorée de traceroute, avec des mises à jour dynamiques |
| nc -zv [hôte] [port] | Vérifie si un port est ouvert sur une machine distante |
| scp [fichier] user@hote:[chemin] | Copie un fichier via SSH |
| ssh user@hote | Se connecte à un serveur distant en SSH |

Ressources en lignes :

<https://doc.ubuntu-fr.org/tutoriel/console_commandes_de_base>  
<https://www.hackingloops.com/command-cheat-sheet-for-linux/>

| **Catégorie** | **Commande** | **Description** |
| --- | --- | --- |
| **Raccourcis Clavier** | Ctrl + C | Termine la commande en cours |
|  | Ctrl + R | Recherche dans l'historique des commandes |
|  | Ctrl + A | Aller au début de la ligne |
|  | Ctrl + E | Aller à la fin de la ligne |
|  | Ctrl + Z | Met en pause un programme |
|  | !! | Réexécute la dernière commande |
|  | ![commande] (ex: !ping) | Réexécute la dernière commande commençant par ce mot |
|  | Flèche ↑ | Parcourt l'historique des commandes |
|  | Flèche ↓ | Parcourt l'historique en sens inverse |
|  | Tab | Auto-complétion des fichiers/dossiers |
| **Commandes de base** | mount | Affiche les systèmes de fichiers montés |
|  | uptime | Affiche la durée d'activité du système |
|  | clear | Efface l'écran du terminal |
|  | date | Affiche la date et l'heure |
|  | whoami | Affiche l'utilisateur actuel |
|  | su root | Passe en mode super-utilisateur |
|  | pwd | Affiche le répertoire courant |
|  | ls | Liste les fichiers et dossiers |
|  | ls -l | Liste détaillée des fichiers/dossiers |
|  | ls -la | Liste détaillée, y compris les fichiers cachés |
|  | cd [dossier] | Change de répertoire |
|  | cd ../ | Remonte d'un niveau dans l'arborescence |
|  | `[commande] | grep [mot-clé]` |
|  | ps aux | Affiche les processus en cours |
|  | kill [PID] | Tue un processus spécifique |
| **Commandes réseau** | ifconfig | Affiche les interfaces réseau |
|  | ifconfig [interface] down | Désactive une interface réseau |
|  | ifconfig [interface] up | Active une interface réseau |
|  | route | Affiche la table de routage |
| **Ports et services** | netstat -l | Affiche les ports en écoute |
|  | netstat -a | Affiche tous les ports ouverts |
|  | netstat -u | Affiche les connexions UDP ouvertes |
|  | netstat -t | Affiche les connexions TCP ouvertes |
|  | `netstat -a | grep [protocole]` |
| **Commandes NMAP** | nmap [IP] | Scan d’un hôte spécifique |
|  | nmap [nom de domaine] | Scan un site internet |
|  | nmap [plage IP] | Scan une plage d’adresses IP |
|  | nmap [sous-réseau] | Scan un sous-réseau entier |
|  | nmap -p [port] [IP] | Scan un port spécifique |
|  | nmap -p [port1-port2] [IP] | Scan une plage de ports |
|  | nmap -F [IP] | Scan rapide des ports courants |
|  | nmap -p- [IP] | Scan tous les ports (lent) |
|  | nmap -sT [IP] | Scan TCP |
|  | nmap -sU [IP] | Scan UDP |
|  | nmap -Pn [IP] | Scan sans découverte d’hôte |
|  | nmap -sS [IP] | Scan SYN |
|  | nmap -sV [IP] | Détecte les versions des services |
|  | nmap -O [IP] | Détecte le système d’exploitation |
|  | nmap -oX fichier.xml [IP] | Sauvegarde en XML |
|  | nmap -oG fichier.txt [IP] | Sauvegarde en format grep |
| **Commandes Metasploit** | msfupdate | Mise à jour de Metasploit |
|  | msfconsole | Lance Metasploit |
|  | show exploits | Liste les exploits disponibles |
|  | show payloads | Liste les payloads |
|  | show auxiliary | Liste les modules auxiliaires |
|  | search [nom] | Recherche un exploit/module |
|  | use [nom] | Charge un exploit/module |
|  | lhost [IP] | Définit l’IP locale |
|  | rhost [IP] | Définit l’IP cible |
|  | show options | Affiche les options d’un module |
|  | show targets | Liste les cibles possibles |
|  | check | Vérifie si une cible est vulnérable |
| **Commandes Metasploit (DB)** | db\_nmap [commande Nmap] | Exécute Nmap depuis Metasploit |
|  | db\_export [fichier] | Exporte la base de données |
|  | db\_import [fichier] | Importe une base de données |
|  | db\_status | Vérifie le statut de la base de données |
|  | hosts | Affiche les hôtes découverts |
|  | hosts -a [IP] | Ajoute une IP à la base |
|  | hosts -d [IP] | Supprime une IP de la base |
|  | hosts -u | Affiche les hôtes actifs |

Ce tableau te servira de **cheat sheet** pour tes commandes Linux, Nmap et Metasploit.