FICHE GRATUITE
CyberSafe

10 commandes essentielles pour débuter avec Kali Linux

Avant de commencer

Utilise ces commandes uniquement sur des systèmes que tu possèdes, ou pour lesquels tu as une autorisation explicite. Scanner ou analyser un système sans autorisation peut être illégal, même dans un but d'apprentissage.

01 `$ nmap -sV -T4 exemple.com`

Détecte les ports ouverts d'une cible et tente d'identifier les services qui y répondent. Ce n'est pas un scanner de vulnérabilités à lui seul — juste une photo de ce qui est exposé.

02 `$ whois exemple.com`

Affiche les informations d'enregistrement d'un nom de domaine (registrar, dates). De plus en plus de données sont masquées par défaut pour protéger la vie privée du propriétaire.

03 `$ dig exemple.com TXT`

Interroge directement les enregistrements DNS d'un domaine. Utile pour vérifier soi-même la présence d'un SPF (remplace TXT par CAA ou NS pour d'autres types d'enregistrements).

04 `$ curl -I https://exemple.com`

Récupère uniquement les en-têtes HTTP renvoyés par un site, sans le contenu de la page — la manière la plus rapide de vérifier soi-même la présence des headers de sécurité.

05 `$ openssl s_client -connect exemple.com:443 -servername exemple.com </dev/null`

Inspecte le certificat TLS présenté par un serveur : validité, date d'expiration, chaîne de certification.

06 `$ traceroute exemple.com`

Affiche le chemin réseau (les routeurs traversés) jusqu'à une cible — utile pour diagnostiquer une latence ou repérer où un trafic est bloqué.

07 `$ sudo ss -tulnp`

Liste les ports en écoute sur ta propre machine (TCP et UDP) et les processus associés — pratique pour repérer un service exposé sans le vouloir.

08 `$ sudo tcpdump -i eth0 -n`

Capture le trafic réseau en direct sur une interface. Réservé à un réseau que tu administres ou es autorisé à analyser — remplace eth0 par ton interface réelle.

09 `$ ssh-keygen -t ed25519 -C "ton_email@exemple.com"`

Génère une paire de clés SSH modernes (ed25519, recommandé aujourd'hui plutôt que RSA) pour se connecter à un serveur sans mot de passe, de façon plus sûre.

10 `$ sudo apt update && sudo apt list --upgradable`

Sur Kali ou toute base Debian, liste les paquets pour lesquels une mise à jour est disponible — le réflexe de base à prendre régulièrement.