PROCÉDURE TECHNIQUE · BTS SIO SISR

Installer Kali Linux dans une VM Proxmox VE

Déployer une machine d'audit Kali Linux, opérationnelle et vérifiée, dans le laboratoire isolé du Plot 1.

Auteur	Plot 1
Contexte	TP réalisé en équipe — Plot 1, domaine ngrange.local
Version	2.0 — novembre 2026
Environnement	Proxmox VE (VM QEMU/KVM) / Kali Linux Installer amd64
Durée estimée	30 à 45 min (selon la bande passante)

Identifiants d'accès — Plot 1

Machine / service	Adresse	Identifiant	Mot de passe
VM-KALI	192.168.21.9	`sio`	`Azerty13.`
Proxmox VE	https://100.101.0.13:8006	`root@pam`	`non fourni`

Sommaire

1. Objectif et cadre légal
2. Architecture et prérequis
3. Installation pas à pas
4. Vérification
5. Dépannage
6. Sécurité et bonnes pratiques
7. Aide-mémoire : utiliser Kali au quotidien

Captures

Les captures proviennent du TP réalisé en équipe : les adresses et noms visibles peuvent différer ; les valeurs à utiliser sont celles du texte (Plot 1).

1. Objectif et cadre légal

Cette procédure installe Kali Linux dans une machine virtuelle Proxmox VE du laboratoire Plot 1 (Proxmox VE, `https://100.101.0.13:8006/`). Elle couvre le démarrage sur l'ISO, la localisation, le partitionnement du disque virtuel, le choix des logiciels, l'installation de GRUB puis les contrôles réseau de fin d'installation. Elle s'arrête à un système à jour, prêt à servir de poste d'audit en laboratoire.

> **Cadre légal – usage en laboratoire isolé uniquement**
>
> Kali embarque des outils d'intrusion. Leur emploi contre un système qui n'est pas explicitement autorisé est une infraction pénale (art. 323-1 et suivants du Code pénal en France). N'utiliser cette VM que dans le réseau pédagogique isolé, sur des cibles désignées par l'établissement, et ne jamais la connecter à un réseau de production ou à un réseau tiers.

2. Architecture et prérequis

Élément	Valeur
Hyperviseur	Proxmox VE, `https://100.101.0.13:8006/`
VM	Au moins 2 vCPU, 4 Gio de RAM, 40 Gio de disque virtuel (le TP utilise un disque QEMU de 96,6 Go)
Image d'installation	Kali Linux « Installer » amd64 (image complète), montée dans le lecteur CD/DVD virtuel
Mode de démarrage	BIOS (le menu de l'installateur affiche « BIOS mode »)
Réseau	VLAN 21 du Plot 1 : `192.168.21.9/24`, passerelle `192.168.21.254`, DNS `192.168.21.1` puis `192.168.21.2`
Nom de machine	`VM-KALI` (VMID 209 sur Proxmox)
Paramètres retenus	Graphical install · langue/pays/clavier Français · partitionnement assisté, disque entier, tout dans une seule partition · GRUB sur `/dev/sda`

> **À savoir**
>
> Vérifier l'intégrité de l'ISO avant de la monter : comparer son empreinte avec celle publiée sur kali.org (`sha256sum kali-linux-*-installer-amd64.iso`). Une ISO corrompue provoque des erreurs aléatoires en cours d'installation.

3. Installation pas à pas

1 Démarrer l'installateur graphique

Démarrer la VM sur le lecteur CD/DVD, sélectionner **Graphical install** avec les flèches du clavier et valider par Entrée. Sans touche pressée, l'installateur lance la synthèse vocale au bout de quelques secondes : agir rapidement.



Figure 1 – Menu de démarrage de l'installateur Kali (mode BIOS)

> **Le menu n'apparaît pas ?**
> Dans Proxmox, onglet *Options* > *Boot Order* de la VM, placer le lecteur CD/DVD avant le disque.

2 Choisir la langue et la localisation

Sélectionner **Français** comme langue, puis **France** comme pays (sauf consigne contraire de l'enseignant). Ces choix déterminent les paramètres régionaux et le fuseau horaire du système.

3 Configurer le clavier et le nom de la machine

Choisir la disposition **Français**. Saisir ensuite le nom de machine prévu par le plan de nommage (`VM-KALI`) : un nom conforme évite les conflits DNS et facilite l'inventaire. Renseigner le domaine DNS `ngrange.local` (domaine AD du Plot 1).

4 Créer le compte utilisateur

Renseigner le nom complet, l'identifiant et le mot de passe (identifiant `sio`, mot de passe `Azerty13.`). Ce compte non privilégié utilisera `sudo` : ne pas travailler en `root`. Ne jamais laisser le mot de passe visible dans une capture d'écran partagée.

5 Choisir le partitionnement et le disque

Choisir **Assisté – utiliser un disque entier**. Ne pas retenir iSCSI, RAID, LVM ni volumes chiffrés, sauf demande explicite du sujet. L'installateur affiche la liste des disques : sélectionner uniquement le disque de la VM Kali (ici *SCSI1 (0,0,0) (sda) – 96,6 GB QEMU HARDDISK*), puis le schéma **Tout dans une seule partition**.

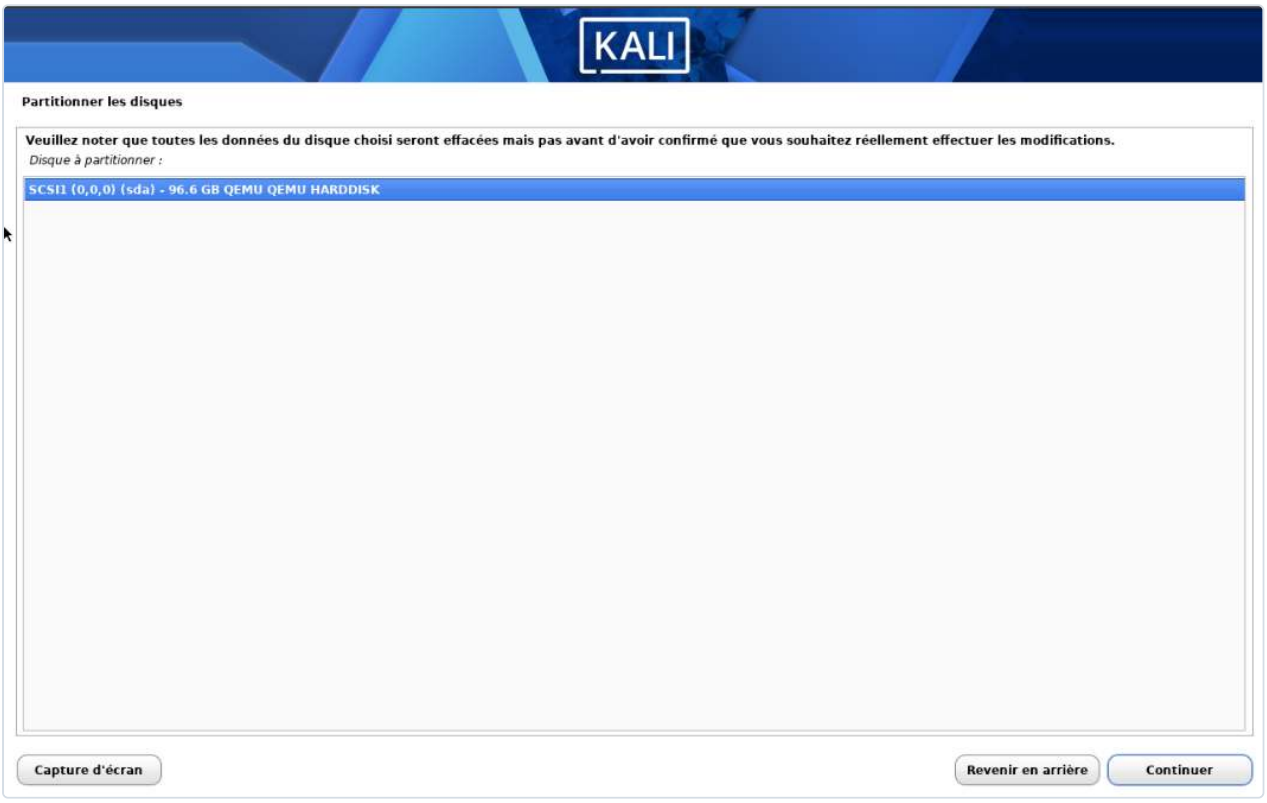

Figure 2 – Sélection du disque virtuel à partitionner (sda)

> **Attention**
> Le partitionnement assisté efface toutes les données du disque choisi. Vérifier que le disque appartient bien à la VM Kali.

6 Valider la table des partitions

Contrôler le résumé : une partition primaire **ext4 montée sur** `/` (91,7 Go dans le TP) et une partition logique **swap** (5,0 Go). Choisir **Terminer le partitionnement et appliquer les changements**, puis confirmer l'écriture sur le disque (*Oui*, *Continuer*).

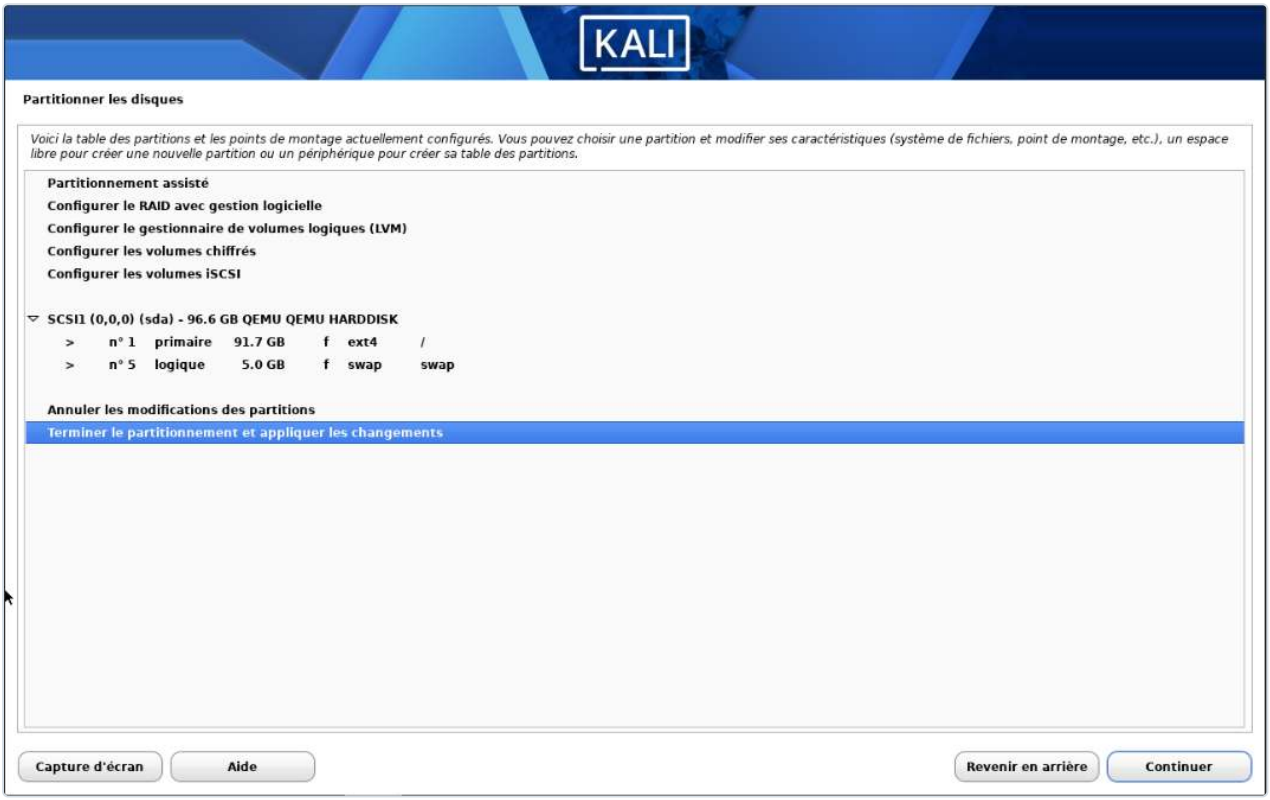

Figure 3 – Résumé des partitions : ext4 sur « / » et swap

7 Installer le système de base

Attendre la fin de la copie du système de base sans éteindre ni redémarrer la VM, sous peine d'un disque inutilisable.

8 Sélectionner les logiciels

Laisser Xfce comme bureau, décocher **KDE Plasma** pour ne pas installer deux environnements graphiques concurrents, et conserver la collection **par défaut – outils recommandés**. Le lot *top10* est facultatif. Valider par **Continuer** et attendre la fin de l'installation des paquets.

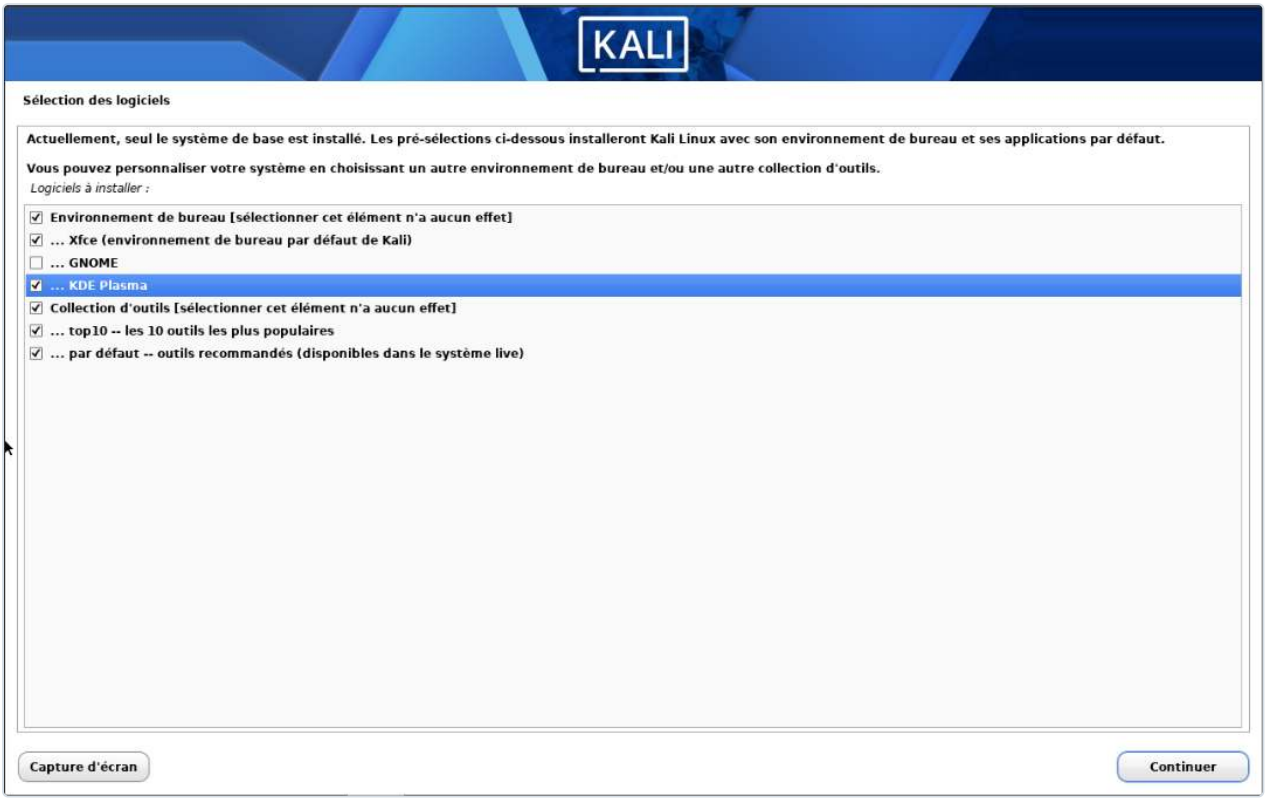

Figure 4 – Écran de sélection des logiciels tel qu'il apparaît au TP (Xfce et KDE Plasma cochés)

> **Écart avec la capture**
>
> La capture montre Xfce et KDE Plasma cochés, et le bureau final de la figure 6 est d'ailleurs de type Plasma. Pour une installation propre, ne conserver que Xfce (plus léger pour une VM) et décocher KDE Plasma.

9 Installer le programme de démarrage GRUB

Répondre **Oui** à « Installer GRUB sur le disque principal », puis choisir le **disque entier** `/dev/sda`, jamais une partition comme `/dev/sda1` : le chargeur doit résider dans le secteur d'amorçage du disque.

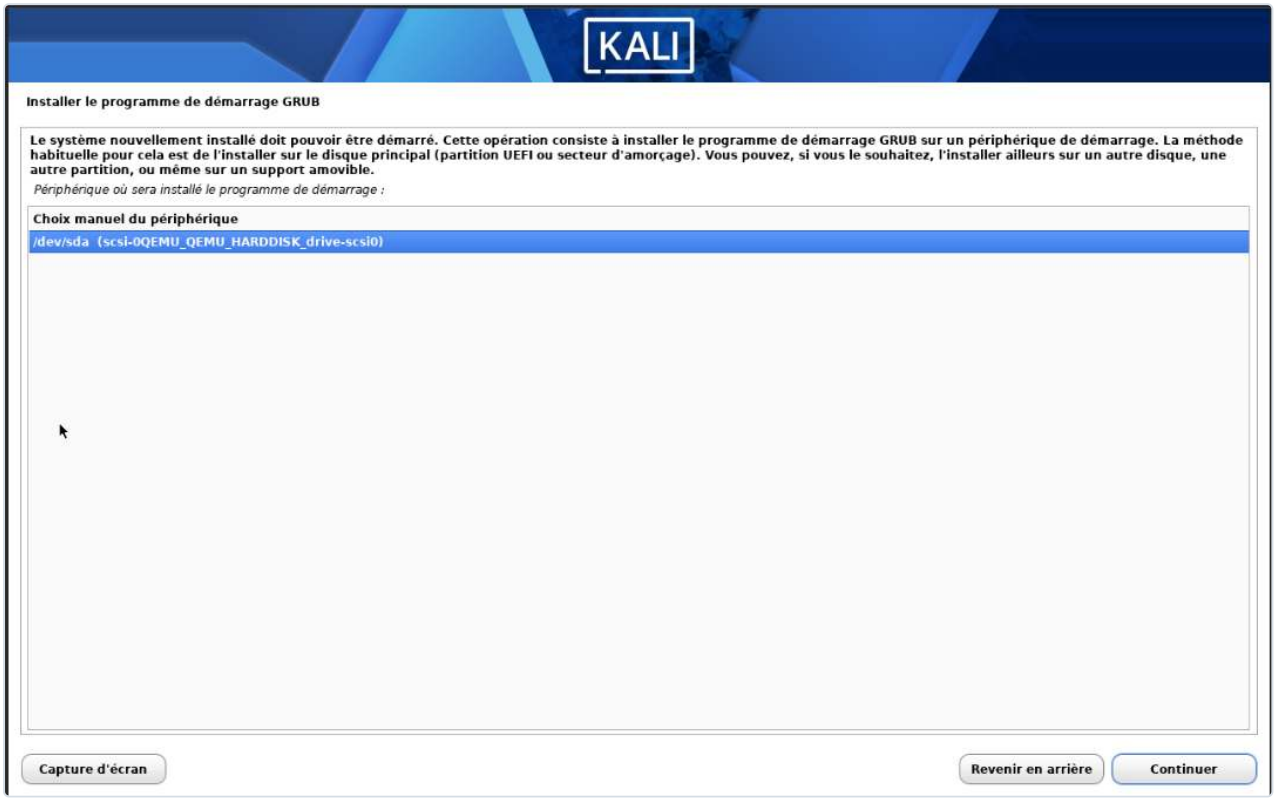

Figure 5 – Choix du périphérique d'amorçage /dev/sda

10 Terminer et redémarrer

À l'affichage de « Installation terminée », éjecter l'ISO dans Proxmox (*Hardware* > *CD/DVD Drive* > *Do not use any media*) et vérifier que le disque précède le lecteur dans l'ordre de démarrage. Cliquer enfin sur **Continuer** pour redémarrer.

> **Important**
> Si l'ISO reste montée et prioritaire, la VM relance l'installateur au redémarrage.

11 Ouvrir une session et mettre à jour

Se connecter avec le compte créé, ouvrir un terminal puis, lorsque l'accès Internet du laboratoire est autorisé, mettre le système à jour pour corriger les failles connues avant tout usage :

```
sudo apt update
sudo apt full-upgrade -y
sudo reboot
```



Figure 6 – Bureau Kali après le premier démarrage

4. Vérification

Dans un terminal de la VM, contrôler l'identité, le réseau et le disque :

```
hostnamectl                     # nom de machine et OS
ip -br address                  # IP attendue sur l'interface
ip route                        # route par défaut vers la passerelle du réseau
pédagogique
cat /etc/resolv.conf            # serveurs DNS
ping -c 3 192.168.21.254          # passerelle pfSense du Plot 1
getent hosts debian.org         # résolution DNS (si Internet autorisé)
lsblk -f                        # sda1 en ext4 sur /, swap actif
cat /etc/os-release | head -n 3  # version de Kali
```

Résultat attendu

- La VM démarre sur le disque sans relancer l'installateur ; le bureau s'affiche et le compte fonctionne.
- `hostnamectl` affiche le nom `VM-KALI`.
- L'interface porte l'adresse `192.168.21.9/24` ; la route par défaut pointe vers `192.168.21.254` et le DNS vers `192.168.21.1` / `192.168.21.2`.
- `lsblk -f` montre une partition ext4 montée sur `/` et une partition swap.
- Une preuve de validation (capture ou sortie des commandes) est conservée si le sujet l'exige.

5. Dépannage

Symptôme	Cause probable	Solution
Erreur de lecture ou de copie depuis le support	ISO incomplète ou corrompue	Re-télécharger l'ISO, comparer le SHA-256, la rattacher au lecteur CD/DVD de la VM.
Retour au menu d'installation après redémarrage	ISO encore montée et prioritaire	Éjecter l'ISO et placer le disque virtuel en premier dans l'ordre de démarrage.
Aucune adresse IP	Bridge, VLAN ou DHCP incorrect	Vérifier le bridge Proxmox et l'étiquette VLAN de la carte réseau de la VM, le DHCP ou l'adresse statique du plan réseau.
Pas de résolution DNS	DNS ou domaine mal renseigné	Contrôler `/etc/resolv.conf` et les serveurs DNS fournis par le réseau pédagogique.
GRUB ne démarre pas	GRUB sur une partition, ou BIOS différent de celui de l'installation	Vérifier l'installation sur `/dev/sda` et que le mode BIOS de la VM (SeaBIOS) est identique à celui utilisé à l'installation.

6. Sécurité et bonnes pratiques

- Isoler la VM dans un VLAN de laboratoire, sans route vers la production ni vers Internet non autorisé.
- Utiliser un compte standard avec `sudo` et un mot de passe robuste et unique ; ne pas conserver le mot de passe par défaut des outils.
- Prendre un instantané Proxmox (snapshot) juste après la mise à jour initiale pour pouvoir revenir à un état sain.
- Mettre à jour régulièrement (`apt update && apt full-upgrade`) ; n'installer des outils que depuis les dépôts Kali officiels.
- Journaliser les opérations d'audit et ne cibler que les machines listées dans le périmètre autorisé.

7. Aide-mémoire : utiliser Kali au quotidien

> **Rappel légal**
> Tout ce qui suit s'exécute uniquement dans le laboratoire isolé, contre des machines désignées par l'établissement. Scanner ou capturer le trafic d'un réseau sans autorisation écrite est une infraction (art. 323-1 et suivants du Code pénal).

Mettre à jour le système et installer des outils

1 **Mises à jour et paquets**

```
sudo apt update && sudo apt full-upgrade -y      # mise à jour complète
apt search nom_outil                               # rechercher un outil
sudo apt install -y nom_outil                      # installer
sudo apt install -y kali-linux-headless            # métapaquet d'outils sans
interface (exemple)
apt list --installed | grep -i nom_outil           # vérifier
sudo apt autoremove --purge -y                     # nettoyer
```

Menu graphique : *Menu des applications* (Kali Linux) classe les outils par catégorie (collecte d'informations, analyse de vulnérabilités, sniffing, etc.). Les métapaquets disponibles se listent avec `apt search kali-linux-`.

Poser un snapshot Proxmox avant tout test

2 **Snapshot et retour arrière**

Interface Proxmox : sélectionner la VM, onglet *Snapshots* > *Take Snapshot*, donner un nom (ex. `avant-tests`), décocher *Include RAM* pour aller vite. Retour arrière : choisir le snapshot > *Rollback*. Équivalent en ligne de commande, sur l'hôte Proxmox (`209` = VMID de VM-KALI) :

```
qm snapshot 209 avant-tests --description "Avant audit lab"
qm listsnapshot 209
qm rollback 209 avant-tests
qm delsnapshot 209 avant-tests
```

Gérer le réseau (ip, nmcli)

3 Adresse, route, DNS

```
ip -br address                  # interfaces et IP
ip route                        # route par défaut
nmcli device status             # état des interfaces (NetworkManager)
nmcli connection show           # connexions enregistrées
# IP statique Plot 1 (adapter le nom de connexion)
sudo nmcli connection modify "Wired connection 1" ipv4.method manual ipv4.addresses
192.168.21.9/24 ipv4.gateway 192.168.21.254 ipv4.dns "192.168.21.1 192.168.21.2"
sudo nmcli connection up "Wired connection 1"
# Retour en DHCP
sudo nmcli connection modify "Wired connection 1" ipv4.method auto ipv4.addresses ""
ipv4.gateway ""
sudo nmcli connection up "Wired connection 1"
```

> **Exemple**
>
> Valeurs du Plot 1 : Kali `192.168.21.9` , passerelle `192.168.21.254` , DNS AD `192.168.21.1` / `192.168.21.2` .

Découvrir les machines du lab : netdiscover et nmap

4 Découverte et scans en lab

```
sudo netdiscover -r 192.168.21.0/24    # découverte ARP active (LAN du Plot 1)
sudo netdiscover -p -i eth0            # mode passif : écoute seulement

nmap -sn 192.168.21.0/24                # hôtes actifs, sans scan de ports
nmap 192.168.21.10                     # (ex. PC-CLIENT) 1000 ports TCP les plus
courants
nmap -p- <IP_CIBLE>                    # tous les ports TCP
nmap -sV -O <IP_CIBLE>                 # versions de services et système (-O : root
requis)
nmap -sC -sV -oN scan.txt <IP_CIBLE>   # scripts par défaut, résultat enregistré
nmap -sU --top-ports 50 <IP_CIBLE>     # UDP, ports courants (lent)
```

Cibles d'exemple : machines du Plot 1 (`192.168.21.1` à `.10`). À utiliser uniquement sur son propre lab. Toujours viser une cible du périmètre. Conserver les fichiers de résultats (`-oN` , `-oX`) comme preuves du TP.

Capturer et filtrer avec Wireshark

5 Capture et filtres courants

Menu *Applications* > *Sniffing & Spoofing* > *Wireshark* (ou `sudo wireshark`), double-clic sur l'interface à écouter pour démarrer ; carré rouge pour arrêter ; *Fichier* > *Enregistrer* pour conserver. Filtres d'affichage (barre verte) :

Objectif	Filtre
Une machine	`ip.addr == <IP>`
Source / destination	`ip.src == <IP>` / `ip.dst == <IP>`
Un protocole	`dns`, `http`, `icmp`, `arp`, `dhcp`
Un port TCP	`tcp.port == 443`
Établissement de connexion TCP	`tcp.flags.syn == 1 && tcp.flags.ack == 0`
Erreurs TCP	`tcp.analysis.flags`
Requêtes HTTP	`http.request`
Suivre une conversation	clic droit sur un paquet > *Suivre* > *Flux TCP*

Capture en ligne de commande, rapide à scripter : `sudo tshark -i eth0 -f "host <IP>" -w capture.pcap` puis `tshark -r capture.pcap -Y "dns"`.

Raccourcis et emplacements utiles

Besoin	Emplacement / commande
Terminal	Icône de la barre des tâches ou `Ctrl+Alt+T` selon le bureau
Version de Kali	`cat /etc/os-release`
Dépôts APT	`/etc/apt/sources.list`
Configuration DNS	`/etc/resolv.conf`
Journaux système	`journalctl -xe`
Snapshot / console VM	Interface Proxmox : VM > Snapshots ; VM > Console
Résultats d'audit	Dossier de travail personnel (ex. `~/audit/`), fichiers `-oN` / `.pcap`

Sources : documentation officielle Kali Linux (kali.org/docs/installation) · Proxmox VE Administration Guide (pve.proxmox.com) · Procédure rédigée à partir d'un TP réalisé en équipe.