Présentation des TPs

TP 1 : Introduction aux réseaux d'entreprise et services de base

- **Objectif :** Familiariser les étudiants avec la configuration de services réseau de base.
- **Outils :** DNSMasq (DHCP/DNS), Linux (Ubuntu ou CentOS)
- **Contenu :**
  - Configuration de **DNSMasq** pour gérer le DHCP et le DNS local.
  - Tester la résolution de noms et l'attribution d'adresses IP dynamiques sur des hôtes virtuels.
- **Compétences :** Gestion des services réseau basiques, IP dynamique.

TP 2 : Virtualisation des réseaux avec KVM

- **Objectif :** Créer un environnement virtualisé pour simuler des réseaux d'entreprise.
- **Outils :** KVM (Kernel-based Virtual Machine), libvirt
- **Contenu :**
  - Installation et configuration de **KVM** et de **libvirt** pour créer des machines virtuelles.
  - Configuration de réseaux internes pour simuler des sous-réseaux et un routeur virtuel.
- **Compétences :** Création de machines virtuelles et configuration de réseaux virtuels.

TP 3 : Sécurisation des réseaux avec un firewall simple

- **Objectif :** Appliquer les concepts de pare-feu dans un réseau d'entreprise.
- **Outils :** Iptables ou UFW (Uncomplicated Firewall)
- **Contenu :**
  - Création de règles simples avec **Iptables** ou **UFW** pour filtrer le trafic.
  - Bloquer/autoriser des flux spécifiques entre machines virtuelles.
  - Tests de connectivité et analyse des logs.
- **Compétences :** Gestion de la sécurité réseau, filtrage de paquets.

TP 4 : Supervision avec Nagios

- **Objectif :** Mettre en place une supervision basique pour surveiller les services critiques du réseau.
- **Outils :** Nagios

- **Contenu :**
  - Installation de **Nagios** sur une machine virtuelle.
  - Supervision des services DNS, DHCP et des hôtes dans le réseau.
  - Configuration d'alertes et d'un tableau de bord.
- **Compétences :** Supervision réseau, gestion des alertes, configuration de Nagios.

TP 5 : Introduction à la gestion automatisée avec Ansible

- **Objectif :** Automatiser la configuration des machines dans l'infrastructure virtuelle.
- **Outils :** Ansible, KVM (VMs)
- **Contenu :**
  - Installation et configuration de **Ansible**.
  - Automatisation de la configuration de plusieurs machines virtuelles (installation de packages, configuration réseau).
  - Rédaction de playbooks simples pour automatiser les tâches de configuration.
- **Compétences :** Automatisation de tâches réseau, écriture de playbooks Ansible.

TP 6 : Mise en place d'un VPN sécurisé avec WireGuard

- **Objectif :** Sécuriser les communications inter-sites avec WireGuard.
- **Outils :** WireGuard
- **Contenu :**
  - Installation de **WireGuard** et création de tunnels VPN entre machines virtuelles.
  - Configuration des règles de routage pour permettre la communication sécurisée entre différents sous-réseaux.
  - Tests de connectivité et vérification de la sécurité.
- **Compétences :** VPN sécurisé, configuration WireGuard.

TP 7 : Mise en œuvre de VXLAN pour la virtualisation réseau

- **Objectif :** Comprendre et configurer un réseau virtualisé avec VXLAN.
- **Outils :** Linux (avec support VXLAN), KVM
- **Contenu :**
  - Configuration de **VXLAN** pour permettre la communication entre différentes machines virtuelles sur des hôtes distincts.
  - Utilisation de **bridge** et **tunnels** pour interconnecter les sous-réseaux.
- **Compétences :** Virtualisation réseau, VXLAN, segmentation de réseau.

TP 8 : Supervision avancée avec Nagios (supervision de services critiques)

- **Objectif :** Étendre la supervision pour inclure des services critiques comme VPN et VXLAN.
- **Outils :** Nagios
- **Contenu :**
  - Ajout de la supervision des tunnels **WireGuard** et **VXLAN**.
  - Analyse des états des services avec Nagios et gestion proactive des incidents.
- **Compétences :** Supervision avancée, intégration de nouveaux services dans Nagios.

TP 9 : Sécurisation réseau avec une DMZ

- **Objectif :** Mettre en place une DMZ pour sécuriser un réseau d'entreprise.
- **Outils :** Iptables/UFW, KVM
- **Contenu :**
  - Configuration d'une **DMZ** pour isoler des services publics (serveur web, etc.) des ressources internes.
  - Définition de règles de pare-feu pour limiter l'accès entre la DMZ et les sous-réseaux internes.
- **Compétences :** Isolation des services, création d'une DMZ, filtrage réseau.

TP 10 : Mise en place d'un reverse proxy avec NGINX

- **Objectif :** Utiliser un reverse proxy pour gérer les requêtes web et sécuriser les services internes.
- **Outils :** NGINX
- **Contenu :**
  - Installation de **NGINX** en tant que reverse proxy pour rediriger les requêtes vers des services internes (Web, API).
  - Configuration de règles SSL pour sécuriser les communications.
- **Compétences :** Reverse proxy, gestion SSL, NGINX.

TP 11 : Mise en place d'un load balancer avec HAProxy

- **Objectif :** Garantir la haute disponibilité des services avec un équilibrage de charge.

- **Outils :** HAProxy
- **Contenu :**
  - Installation et configuration de **HAProxy** pour distribuer la charge entre plusieurs serveurs web.
  - Configuration de tests de résilience pour assurer la haute disponibilité.
- **Compétences :** Équilibrage de charge, HAProxy.

TP 12 : Automatisation complète du réseau avec Ansible et Terraform

- **Objectif :** Automatiser le déploiement et la configuration complète d'une infrastructure réseau.
- **Outils :** Ansible, Terraform
- **Contenu :**
  - Utilisation de **Terraform** pour automatiser la création d'infrastructures (VMs, réseaux).
  - Configuration automatisée des machines avec **Ansible** pour installer et configurer les services.
  - Automatisation de la création de VPN WireGuard, services DNS, et configuration de VXLAN.
- **Compétences :** Automatisation complète, intégration de Terraform et Ansible.

TP 13 : Surveillance et tests de performance du réseau

- **Objectif :** Mesurer et surveiller les performances d'un réseau virtuel.
- **Outils :** Iperf, Nagios
- **Contenu :**
  - Utilisation d'**Iperf** pour tester la bande passante et les performances des tunnels VPN et des réseaux VXLAN.
  - Configuration des tests de performance dans Nagios pour générer des alertes en cas de baisse de performance.
- **Compétences :** Test de performance réseau, intégration des résultats dans Nagios.

TP 14 : Test de résilience et de sécurité (DMZ, VPN, Load Balancer)

- **Objectif :** Tester la sécurité et la résilience des configurations mises en place (DMZ, VPN, Load Balancer).
- **Outils :** NGINX, HAProxy, WireGuard
- **Contenu :**

  - Simulation d'incidents (défaillance de serveurs, coupure de réseau) pour tester la résilience du load balancer et des tunnels VPN.
  - Vérification des mesures de sécurité mises en place dans la DMZ.
- **Compétences :** Résilience réseau, sécurité, gestion des pannes.

TP 15 : Projet final – Conception et déploiement d'une infrastructure réseau complète

- **Objectif :** Appliquer toutes les compétences acquises pour concevoir une infrastructure réseau évolutive et sécurisée.
- **Outils :** Ansible, Terraform, KVM, NGINX, WireGuard, HAProxy, Nagios
- **Contenu :**
  - Déploiement complet d'une infrastructure réseau intégrant DMZ, VPN, VXLAN, load balancer, reverse proxy et supervision.
  - Tests de performance et sécurité.
- **Compétences :** Conception d'architecture réseau, automatisation, supervision, sécurité.
