Devoir Administration des réseaux

Durée 1h30

Contexte : L'entreprise *SUP-STUDENT-SULUTIONS*, spécialisée dans le développement de logiciels, a récemment décidé d'optimiser son infrastructure réseau et sa politique de sécurité. Le département informatique vous a confié plusieurs tâches pour répondre à leurs besoins dans divers domaines. Vous travaillerez en tant qu'administrateur réseau et vous avez les missions suivantes :

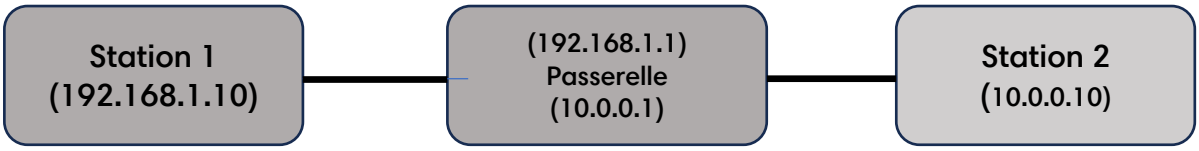
Exercice 1 : Configuration réseau sous Linux (7,5pts)

Vous êtes chargé de diagnostiquer un problème de connexion réseau sur une station sous Linux (Ubuntu 2024).

1. Quelle commande vous permet de visualiser la configuration réseau actuelle de la station ?
2. Expliquer la différence entre une configuration manuelle (ou statique) et une configuration dynamique de l'adresse IP de la machine.
3. Configurez cette station pour utiliser une adresse IP statique à l'aide d'un fichier YAML sous Ubuntu 2024. Donner manuellement à cette station l'adresse IP 192.168.1.10/24 avec une passerelle par défaut 192.168.1.1.
4. Expliquer le rôle des fichiers /etc/hosts et /etc/resolv.conf.
5. Donnez un exemple d'utilisation de /etc/hosts et /etc/resolv.conf

Exercice 2 : Routage statique (3pts)

Un problème d'interconnexion réseau a été signalé sur l'architecture suivante :



1. Ajoutez une route sur la **Station 1** pour permettre la communication avec la **Station 2** via la passerelle.
2. Ajoutez une route sur Station 2 pour accéder au réseau 172.16.0.0/16 via la passerelle (adresse de passerelle : 10.0.0.1).
3. Expliquez la différence entre une route par défaut et une route statique spécifique.

Exercice 3 : Firewall et règles de filtrage (7,5pts)

Vous devez mettre en place un firewall (iptables) pour sécuriser un serveur interne.

1. Donnez la commande permettant de nettoyer toutes les règles existantes dans un firewall basé sur **iptables.**
2. Appliquez une politique par défaut refusant tous les paquets (entrant et sortant).
3. Configurez les règles nécessaires pour autoriser uniquement le trafic FTP et SSH entrant.
4. Ajoutez une règle permettant de bloquer tout accès depuis (provenant de) une adresse IP spécifique 192.168.100.20.
5. Analysez le tableau suivant de règles firewall et répondez aux questions :

Règle	Direction	Source	Destination	Port	Action
1	Entrant	Externe	Interne	22	Permettre
2	Sortant	Interne	Externe	443	Permettre
3	Entrant	Externe	Interne	21	Refuser
4	Toutes	Toutes	Toutes	Tous	Refuser

   a) Le trafic FTP (port 21) est-il autorisé ?
   b) Le trafic SSH entrant est-il autorisé ?
   c) Le trafic HTTPS sortant est-il autorisé ?

Exercice 4 : Analyse réseau avec tcpdump (2pts)

Vous devez analyser le trafic réseau pour diagnostiquer un problème de lenteur.

1. Capturez tous les paquets transitant par l'interface eth0.
2. Filtrez uniquement les paquets provenant de l'adresse 172.16.1.10 et ayant une destination au port tcp 80.