Nom : .....

Exercice 1 *6 points*

1. **Expliquer la différence entre un switch et un routeur.**
   Un switch est un équipement qui permet de distribuer les paquets à l'intérieur d'un sous-réseau. Il distribue les paquets grâce à l'adresse MAC qui est associée à la carte réseau de chaque ordinateur. Un routeur permet quant à lui de relier deux sous-réseaux entre eux. Il distribue les paquets grâce à l'adresse IP attribuée à chaque ordinateur.
2. **Donner une différence fondamentale entre l'adresse MAC et l'adresse IP d'une machine.**
   L'adresse MAC d'une machine est configurée lors de la fabrication en usine de la carte réseau de l'ordinateur. Elle est donc définitive.
   L'adresse IP d'un ordinateur est déterminée à chaque connexion à un réseau. Elle est souvent attribuée par le routeur lui-même (DHCP). Une adresse IP est donc changeante, alors qu'une adresse MAC est définitive.
3. **On considère deux ordinateurs ayant pour adresses IP respectives `192.168.0.1` et `192.168.1.156`, associées au masque de sous-réseau `255.255.255.0`. Ces deux ordinateurs peuvent-ils communiquer ensemble ? Pourquoi ?**
   Le masque de sous-réseau `255.255.255.0` indique que la machine d'IP `192.168.0.1` ne pourra communiquer qu'avec des machines d'adresse `192.168.0.X`, où `X` est un nombre entre 1 et 254.
   Il sera donc impossible de communiquer avec la machine d'adresse `192.168.1.156`.
4. **Décrire un moment où, dans l'acheminement d'un paquet entre ma machine et une machine située sur un autre réseau (ex : les serveurs de Google), les données sont partiellement décapsulées avant d'être ré-encapsulées.**
   Un décapsulage partiel des données a lieu lors du passage à travers un routeur : celui-ci ouvre la trame pour aller consulter l'adresse IP de destination du paquet, avant de ré-encapsuler avec le paquet.

Exercice 2 *2 points*

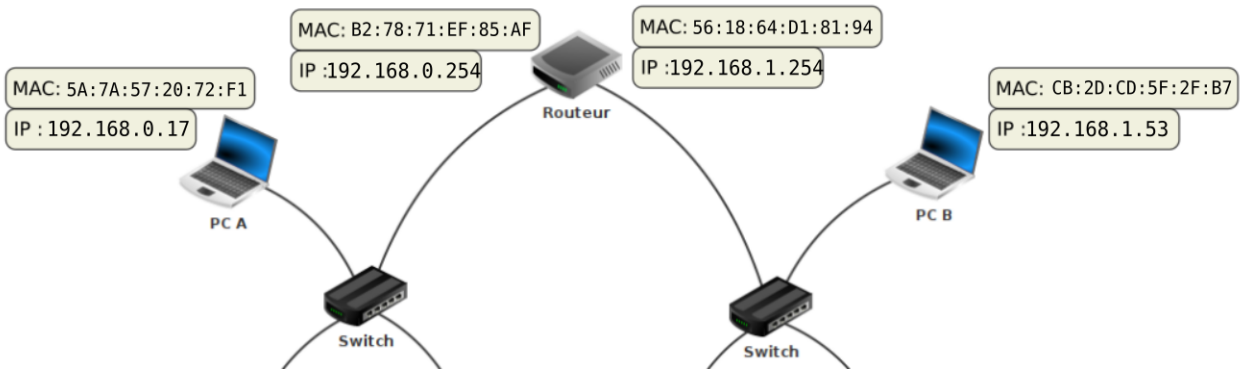
On considère l'extrait de Terminal suivant, sur mon ordinateur de bureau. L'adresse de passerelle de ma Freebox (qui me permet d'accéder à internet) est la plus grande adresse IP possible de mon sous-réseau.

```
gilles@gilles-bureau:~$ arp -a
? (192.168.0.13) à b8:27:eb:6c:7c:80 [ether] sur enp2s0
_gateway (192.168.0.254) à f4:ca:e5:56:fa:29 [ether] sur enp2s0
? (192.168.0.25) à e4:b3:18:73:a1:86 [ether] sur enp2s0
```

Quelle est l'adresse MAC de la Freebox ?

Ma Freebox est la passerelle (gateway en anglais), qu'on peut reconnaître aussi à son IP en `.254`. On peut donc lire que son adresse MAC est `f4:ca:e5:56:fa:29`.

Exercice 3 *4 points*



Exercice 4 *2 points*

Compléter les lignes ci-dessous :

1. Nom du langage à balises permettant l'écriture de pages web : HTML
2. Nom du langage permettant la création de feuilles de style pour les pages web : CSS
3. Nom d'un langage permettant des actions de l'utilisateur sur sa page, côté client : JavaScript
4. Nom d'un langage permettant de fabriquer sur le serveur une page spécifique pour le client, avant de lui distribuer cette page : PHP

Exercice 5 *3 points*

1. **Expliquer une différence entre les requêtes GET et POST.**
   Une donnée envoyée à un serveur via un requête GET sera apparente dans l'url de la page consultée, ce qui n'est pas le cas lors d'une requête POST.
2. **Un mot de passe transmis via une requête POST est-il interceptable ?**
   Si le transfert des données se fait en `http` et non `https`, oui, un mot de passe transmis par une requête POST pourra être intercepté. Si le transfert se fait en `https`, les données restent interceptables mais illisibles grâce au chiffrage.

Exercice 6 *3 points*

Expliquer (sans rentrer dans les détails techniques) comment fonctionne une attaque de mot de passe par force brute.

Le principe de la force brute est «d'essayer toutes les combinaisons possibles». Toutefois, dans le cas d'une attaque de mot de passe, il faudrait essayer un nombre immense de combinaisons improbables, comme `fd45ùfc27` (qui est peut être le bon mot de passe, ou peut être pas).

Pour aller beaucoup plus vite tout en gardant de bonnes chances de trouver le mot de passe, connaissant la propension des utilisateurs à utiliser des mots de passe simples à retenir, on peut se baser sur des dictionnaires de mots de passe ayant réellement été utilisés. Ces dictionnaires sont librement téléchargeables (notamment pour vérifier que son mot de passe personnel n'y est pas, sinon il faut le changer !).

La technique consiste alors à essayer tous les mots possibles de ce dictionnaire, jusqu'à trouver le bon. Cette technique est toutefois empêchée par de nombreuses contre-mesures (compte bloqué après 3 erreurs, délai de temps très long entre les tentatives...)