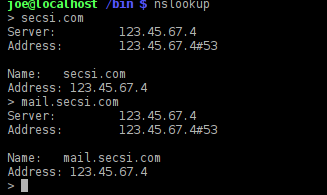
# Question 2

1. **À** **quelle adresse IP correspondent le domaine secsi.com et le serveur mail mail.secsi.com**

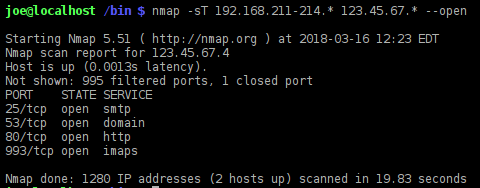
L’adresse IP de correspondant au domaine secsi.com est le même que le celui du serveur mail mail.secsi.com soit 123.45.67.4.



1. **Lancez** **la** **commande « nmap –sT 192.168.211-214.\* 123.45.67.\* --open » en tant qu’utilisateur joe. Que fait cette commande? Expliquez le résultat.**

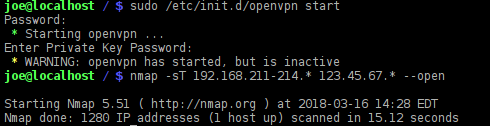
La commande est utilisée afin de déterminer quels ports sont ouvert sur un réseau. Cette commande nous informe de plusieurs choses sur ces ports comme par exemple les services disponibles sur ces ports ainsi que le système d’exploitation de l’hôte offrant ce service. L’option « sT » de nMap spécifie de faire un scan en essayant d’ouvrir une connexion TCP sur les ports. Les deux adresses suivant le paramètre « sT » spécifie à nMap sur quelle plage d’adresse la tentative de connexion TCP devrait se faire. Dans le cas de la première adresse spécifier, on scan les ports sur toutes les adresses IP entre 192.168.211.0 et 192.168.214.255. Le tiret dans le 3ième octet veut donc simplement dire que l’on veut faire le scan entre les deux valeurs spécifier. L’étoile à la fin des deux adresses IP signifie que toutes les possibilités doivent être tester entre 0 et 255. Finalement, l’option « --open » permet de filtrer les résultats que nMap donne afin d’afficher seulement les ports qui sont ouvert auquel il est possible de se connecter.

Le résultat nous montre que les ports ouverts et disponibles depuis le réseau du Poste\_internet sont tous disponibles depuis l’adresse 123.45.67.4. Tous les ports ouverts et disponibles sont ceux que le service NAT du pare-feu externe redirige.



1. **Que fait un** **service VPN? Expliquez le nouveau résultat.**

Un VPN permet de créer un réseau virtuel privé qui redirige en quelque sorte le trafic. Maintenant, si le Poste\_internet veut faire une requête, il doit passer par le VPN en premier lieu. C’est pour cela que maintenant que tout passe par le VPN que le Poste\_internet n’est plus capable de voir les ports ouverts de l’adresse IP 123.45.67.4.



1. **Comparez les informations obtenues à l’aide de nmap à votre schéma du réseau. Expliquez les différences.**

La différence entre les deux nMap est que la première fois, le Poste\_internet ainsi que le pare-feu externe étaient tout deux dans le même réseau soit 123.45.67.0/24 tandis qu’une fois le VPN ouvert, les deux ordinateurs n’étaient plus dans le même réseau local à cause du niveau d’abstraction que le VPN apporte. Donc la première fois que la commande nMap fut lancer, le Poste\_internet à pus voire les ports d’ouvert tandis que la deuxième fois il n’a pas eu cette occasion.

1. **Quel** **est l’avantage du NAT contre un balayage de ports?**

Le NAT peut appliquer des restrictions qui font en sorte qu’il présente certains ports selon la provenance de la requête. Ainsi un balayage des ports provenant de l’extérieur du réseau peut être prévenue.

1. **Pour les deux utilisations de nmap, dîtes à quel endroit du réseau il aurait fallu placer un IDS (Intrusion Detection System) pour détecter le balayage de ports.**

Ajouter un IDS à mon pare-feu externe aurait permis de détecter le balayage de ports.