Segmentation - Marius TAUDON

Exercice 1 : Rechercher trois méthodes pour segmenter une infrastructure réseau de façon sécurisée.Quels sont les avantages et inconvénients de chaque méthode?

Segmenter son réseau, c'est le séparer en plus petites entités, il existe plusieurs façon de faire cela :

Utiliser le réseau VLAN

Pour segmenter leur réseau, les entreprises ont longtemps créé plusieurs segments de réseau plus petits avec des réseaux locaux virtuels (VLAN) ou des sous-réseaux, où tous les hôtes sont connectés virtuellement les uns aux autres, comme s'ils se trouvaient dans le même réseau local. Quant aux sous-réseaux, ils utilisent les adresses IP pour diviser un réseau en sous-réseaux plus petits reliés par des périphériques réseau.
Ces deux approches permettent à la fois d'améliorer les performances du réseau, et surtout d'empêcher les menaces qui peuvent se propager au-delà de votre système VLAN ou d'un sous-réseau particulier. Cependant, elles présentent deux défis majeurs. D'une part, votre équipe informatique doit réviser l'architecture réseau pour répondre aux besoins de la segmentation. D'autre part, il est souvent difficile de programmer la gestion des milliers de règles de liste de contrôle d'accès (ACL) se trouvant sur les périphériques réseau et qui permettent de créer des sous-réseaux.

Segmenter le pare-feu

Il est possible d'utiliser le réseau pour appliquer la segmentation, mais les pare-feu constituent également une autre option. Les pare-feu peuvent être déployés à l'intérieur d'un centre de données ou d'un réseau afin de créer des zones internes, ce qui permet de segmenter les domaines fonctionnels les uns des autres et de limiter les surfaces d'attaque. De cette manière, vous pouvez empêcher les menaces de se propager au-delà d'une zone de sécurité. Vous pouvez par exemple séparer les applications d'ingénierie des finances ou protéger les zones sensibles où résident les données PCI.
Les administrateurs réseau et de sécurité ont une bonne connaissance sur les pare-feu qui sont déployés sur le périmètre, mais ils ont souvent tendance à introduire une grande complexité lorsque ces mêmes pare-feu sont utilisés pour effectuer une segmentation interne. La raison est que des milliers de règles de pare-feu doivent être appliquées pour segmenter les réseaux internes et qu'il faut aussi tenir compte du fait qu'une mauvaise configuration du pare-feu pourrait casser une application et nuire à votre entreprise. L'autre inconvénient d'utiliser des pare-feu pour la segmentation réseau est le coût énorme que les pare-feu pourraient

imposer, car ils sont généralement achetés par paire pour plusieurs sites, ce qui peut représenter des millions d'euros.

Utiliser le réseau défini par logiciel (SDN)

En utilisant le SDN, votre organisation pourra mettre en œuvre la microsegmentation, également appelée segmentation de sécurité ou segmentation basée sur l'hôte. Grâce à cette approche, vous allez pouvoir augmenter la granularité de la segmentation puisque vous allez isoler les charges de travail individuelles les unes des autres. En d'autres termes, vous ne serez plus contraint de travailler à l'échelle de plusieurs points d'extrémité, tel qu'on faisait avec la segmentation réseau dans sa forme traditionnelle.
Cette granularité supplémentaire augmente les avantages de la segmentation, car elle offre un niveau plus élevé de visibilité et de contrôle du réseau. Cette approche tend également à utiliser des modèles de liste blanche qui permettent de bloquer tous les trafics réseau, sauf ceux qui sont autorisés.
Le problème avec la segmentation basée sur l'hôte est que les professionnels ont souvent besoin d'une certaine période d'adaptation. De plus, la plupart des nouveaux utilisateurs doivent être formés à une nouvelle façon de créer des règles et d'appliquer la segmentation en utilisant le SDN, même s'ils sont familiers avec les pare-feu et les concepts de mise en réseau.

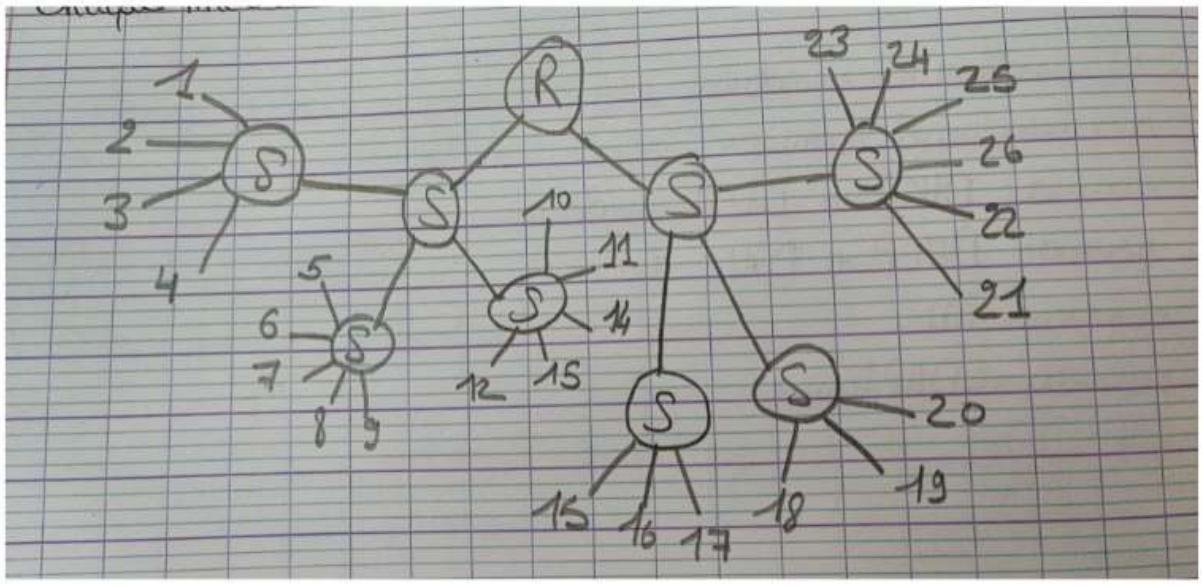
Exercice 2 : Sur le schéma ci-dessous.

Utilisation des pas :

Direction : 1,26,16 def de projet : 13,14 RH : 2,3,4,15

Devs : 10,11,21,22,23,24 compta : 7,8,9,18,19

Admin Réseau : 5,6,12,17,20,25



Pourquoi cette disposition n'est-elle pas sécurisée ?

- Cette disposition n’est pas sécurisée car tous les pc peuvent communiquer entre eux sans distinction, en plus de ne pas être très organisé, cela peut être embêtant si un seul système est infecté, sans segmentation, un virus pourrait se répandre sur toutes les machines.

Proposer une solution de segmentation sans changer l’information réseau pour chacune des méthodes de l’exercice 1.

- Vlan : Pour segmenter en Vlan, il faut séparer chaque service les uns des autres avec un plan IP différent. Ainsi, on prendra un net-id similaire mais un subnet-id différents. Je conseille l’utilisation d’une adresse de classe A avec un masque en /24.
- Pare-Feu : Même si ce n’est pas conseiller, la segmentation par Pare-feu peut être faite de la même manière que la segmentation par VLAN à la différence que chaque équipement pourra être isolé des autres, c’est assez compliqué à mettre en place, mais au niveau de la sécurité c’est ce qu’il y a de mieux, puisque même si un système est infecté, il sera difficile pour le virus de se diffuser sur tout le réseau. Cela fonctionne un peu comme les ACL de chez Cisco.
- SDN : La segmentation logicielle est assez simple à mettre en place, pour ce faire, il va falloir créer des règles, des rôles et des droits. Cela fonctionne un peu comme les GPO de Windows Server, un groupe de personnes sera segmenté ensemble et un autre ensemble et ainsi de suite. Les machines ne sont pas forcément isolées, c’est ici les droits des utilisateurs sur les machines qui sont différents selon les groupes, donc le risque qu’un employé fasse une bourde dans un service qui ne le concerne pas est normalement réduit.

Exercice 3 : La direction veut mettre en place un BYOD,la disposition de base est-elle adaptée pour que tous les employés puissent l’utiliser ? Si oui pourquoi ? Sinon proposer des modifications.

- La disposition actuelle n’est pas adaptée au BYOD, puisque la sécurité ne serait pas géniale voire inexistante. Le BYOD, ou Bring Your Own Device est une manière de travailler qui consiste à ce que chaque employé vienne travailler avec son propre matériel. C’est une démarche qui facilite l’organisation et qui est très économique, mais au niveau de la sécurité des infrastructures de l’entreprise c’est vraiment problématique, dans le sens où si un système d’un utilisateurs est infecté, il pourrait diffuser ce virus sur tous les systèmes de l’entreprise. Et c’est le cas dans notre dispositif actuel. Le fait

qu’il n’y ait pas de segmentation entre les systèmes, et que tout soit relié les uns aux autres, y compris les systèmes personnels des utilisateurs, est un gros défaut. Pour adapter cette disposition au BYOD, je préconiserai de segmenter tous les services déjà, et que dans chaque service ou un utilisateur apporte son matériel, il y ai une Box internet non relié à notre réseau, les échanges avec les systèmes de l’entreprise pourrait se faire par le biais de serveurs WEB par exemple. Il est évidemment nécessaire que les équipements de l'entreprise soient séparés des autres. Dans l’idéal, il faudrait que les employés n'utilisent leurs ordinateurs que pour travailler et non pour le reste chez eux, comme télécharger des films en peer to peer avec Utorrent par exemple.

Exercice 4 : Pensez-vous que l’on puisse segmenter l'accès à une application ? Comment ?

- Il est possible de restreindre et de segmenter l’accès à une application par connexion d’utilisateurs autorisés. Si ce sont les administrateurs qui crées les comptes des applications, personne d’autres ne pourra en créer, ou se connecter. De ce fait, l’accès à une application sera segmenté. Avec un serveur LDAP et les bonnes restrictions, il est aussi possible de segmenter l’accès à une application à des services, des postes ou même à des utilisateurs.