SAE 4.01B-compétence 3 (réseaux)

Contexte et modalités

Cette partie de la SAE 4.01B vise à évaluer votre maîtrise de la compétence 3. Elle est entièrement indépendante de la SAE 4.01A.

Le travail préconisé sera réalisé dans les mêmes groupes que le reste de la SAE 4.01A ; toutefois, le responsable de projet sera différent.

Ce projet modifie et étend le travail attendu pour la SAE 3.01B – toutefois, les notes sont indépendantes. Même avec une SAE 3.01B partiellement correcte, vous pouvez (avec un travail conséquent), réussir une SAE 4.01B complète ! Comme en S3, cette SAÉ se centrera autour de l'environnement du CHU précisé dans la S3.01B, et le travail sera réalisé toujours en Kathará.

Attention : **Votre objectif ne sera pas d'implémenter les applications et services de la S3.01B ou de la S4.01B, seulement d'assurer un filtrage mettant en place une zone démilitarisée !!**

Attention : **Vous ne serez pas toujours dans la même salle tout au long de cette SAÉ ! Il faudrait donc gérer cet aspect de « portabilité » au niveau du projet.**

Apprentissages critiques évalués

Cette SAE évaluera les apprentissages critiques suivants :

- AC1 : Concevoir et développer des applications communicantes
- AC2 : Utiliser des serveurs et des services réseaux virtualisés
- AC3 : Sécuriser un système

Ceci se fera :

- En sécurisant le système d'information
- En appliquant les normes en vigueur et les bonnes pratiques architecturales et de sécurité
- En offrant une qualité de service optimale
- En assurant la continuité d'activité

Description détaillée du sujet

Dans la SAÉ 3.01B vous avez réalisé un filtrage d'accès pour permettre la de l'infrastructure du CHU décrite dans le sujet, qui est partagée par des utilisateurs avec des privilèges d'accès différents. En plus de ces utilisateurs, un nombre de machines « sensibles » hébergent différents services nécessaires. Ces machines sont : S, MAIL, AUX, BDD.

Pour rappel, le réseau du CHU est divisé dans les sous-réseaux différents :

- Réseau patients : une sousplage de classe C
- Réseau visiteurs : une sousplage en /26
- Réseau enseignants, chercheurs et enseignants-chercheurs : une sousplage en /22
- Réseau étudiants : une sousplage en /22
- Réseau comptabilité : une sousplage en /24
- Réseau personnel soignant : une sousplage en /22
- Réseau serveur S : une sousplage en /28 qui ne contient que les machines S et DNS. L'adresse IP de S est fixée à 172.16.3.28.
- Réseau DSI : une sousplage en /24. L'adresse dédiée du responsable RSSI est la première adresse machine de cette plage.

Dans cette SAÉ vous allez devoir reprendre le scénario décrit dans la SAE 3.01B (qui est mis à la fin de ce sujet, pour rappel), et rajouter les contraintes suivantes pour le filtrage :

- Séparation du routage : dans la S3.01B, tout accès Internet se fait via un seul routeur, R0. Cela introduit potentiellement une faille, si jamais ce routeur tombe en panne. La DSI choisit de départager l'accès à Internet par 3 routeurs :
    - Un routeur pour l'infrastructure critique et de haute priorité
    - Un routeur pour l'accès éducatif/universitaire (priorité moyenne)
    - Un routeur pour l'accès à basse priorité

  Une fois les routeurs mis en place, la DSI fait en sorte de passer tout accès considéré critique par le premier routeur, l'accès éducatif pour le deuxième routeur, et finalement les accès non-prioritaire par le troisième. Ces 3 routeurs sont chacun connectés à Internet.

- Toutes les machines des étudiants et des enseignants, ainsi que le réseau du personnel soignant, la compta, le réseau du serveur S, toutes les machines sensibles (listées ci-dessous) et tous les routeurs doivent être configurables à distance de façon sécurisée par le personnel DSI (à partir de leurs machines fixes, présentes dans le réseau DSI).

Pour sa sécurité, la RSSI décide d'imposer une **politique de filtrage qui ne permet que les accès strictement nécessaires** dans le réseau. De plus, la DSI veut mettre en place **des tests automatisés** (en utilisant des scripts) qui vont tester que les conditions de filtrage sécurisé ont été mises en place.

Travail à réaliser

Vous allez reprendre le travail que vous avez effectué pour la SAÉ 3.01B.

Pour la SAÉ 4.01B vous aurez 4 tâches principales :

- Analysez la topologie de réseau de la S3.01B pour classifier les différents sous-réseaux selon la priorité d'accès. Mettez à jour la configuration de votre réseau.
- A partir de la nouvelle topologie, veuillez dans un premier temps analyser les accès strictement nécessaires dans l'architecture réseau de l'entreprise (par rapport au sujet de la SAÉ 3.01B et aux additions présentées dans ce sujet).
- À partir de ce travail d'analyse, veuillez implémenter des règles de filtrage sur les machines concernées par l'architecture réseau modélisée en Kathará
- À partir de votre analyse, veuillez trouver un sous-ensemble de cas de test pour pouvoir tester correctement la mise en place de votre filtrage
- Enfin, veuillez implémenter des tests automatisés pour votre filtrage sur une machine employé, une machine de la zone d'administration, le serveur S et le routeur qui donne accès Internet aux machines de votre architecture Kathará.

Évaluation

Vous travaillerez dans les mêmes groupes que pour la SAE générique, mais en utilisant un autre chef de projet (changement impératif).

Vous aurez à fournir (sur Moodle) une archive contenant vos fichiers Kathará (et éventuellement des fichiers séparés de scripts), ainsi qu'un rapport détaillant votre démarche, sur maximum 5 pages + 2 pages réservées à des figures à haute résolution détaillant (1) votre infrastructure), (2) les accès strictement nécessaires que votre filtrage doit permettre.

Vous serez évalués principalement pour :

- Votre travail d'analyse
- La corrélation entre l'analyse et le filtrage, et l'analyse et les cas de test trouvés
- Les tests automatisés (qui vont devoir marcher le jour de la soutenance !)

Pensez à inclure des exemples de code (pour le filtrage et les scripts).

De plus, votre rapport devra inclure une section qui devra comparer le filtrage réalisé pour la SAÉ 4.01B par rapport au filtrage de la SAÉ 3.01B (en mettant en évidence toute modification et ses répercussions par rapport à la sécurité de la totalité de l'architecture.

En dehors du rapport, chaque étudiant de chaque groupe aura une épreuve orale individuelle, pendant laquelle il/elle doit faire une démonstration du lab Kathará et des scripts de tests automatisés, en mettant en évidence les solutions choisies, les cas de test, ainsi que la sécurité que ce filtrage fournit.

Annexe (SAE 3.01B)

Contexte et modalités

Cette partie de la SAE 3.01B vise à évaluer votre maîtrise de la compétence 3. Elle est entièrement indépendante du reste de la SAE 3.01A.

Le travail préconisé sera réalisé dans les mêmes groupes que le reste de la SAE 3.01A ; toutefois, le responsable de projet sera différent.

Le projet décrit ci-dessous comporte deux parties : une partie analytique et une partie pratique. Cette dernière sera mise en place dans l'émulateur Kathará (dans la VM Ubuntu). Le sujet suppose l'existence *a priori* de plusieurs services et d'applications sur 5 machines différentes : une machine S, une machine BDD, une machine MAIL, une machine DNS et une machine AUX.

Attention : **Votre objectif ne sera pas d'implémenter ces applications et services, seulement d'assurer un filtrage mettant en place une zone démilitarisée !!**

Attention : **Vous ne serez pas toujours dans la même salle tout au long de cette SAÉ ! Il faudrait donc gérer cet aspect de « portabilité » au niveau du projet.**

Apprentissages critiques évalués

Cette SAE évaluera les apprentissages critiques suivants :

- AC1 : Développer des applications communicantes
- AC2 : Utiliser des serveurs et des services réseaux virtualisés

Ceci se fera :

- En sécurisant le système d'information
- En appliquant les normes en vigueur et les bonnes pratiques architecturales et de sécurité
- En offrant une qualité de service optimale
- En assurant la continuité d'activité

Description détaillée du sujet

Contexte

L'infrastructure de réseau du centre hospitalier universitaire (CHU) d'une certaine ville héberge plusieurs types de personnes simultanément : des patients, des visiteurs, du personnel administratif, du personnel de santé (médecins, infirmières, etc.), des étudiants en médecine, ainsi que des chercheurs. La direction des services d'information, et surtout le responsable de la sécurité des systèmes d'information (RSSI) doivent assurer la disponibilité de certains services qui sont nécessaires au bon fonctionnement du CHU, tout en limitant l'accès aux données à caractère sensible (l'accès doit être toujours réduit au stricte nécessaire).

Une double authentification

L'agence du numérique en santé (ANS) demande à ce que l'accès à des données à caractère sensible concernant la santé ne puisse être garanti que par une double authentification. Le RSSI du CHU en question décide de mettre en place une double authentification avec un mot de passe et un code reçu par mail à l'adresse mail CHU de chaque membre du personnel autorisé.

Services et serveurs

Chaque membre du personnel a une adresse mail CHU. Le serveur mail est hébergé sur une machine MAIL.

Pour gérer la gestion des noms de domaines, le CHU a mis en place un serveur DNS qui fonctionne sur UDP avec le port standard. Ce serveur est hébergé sur une machine DNS.

En plus, le CHU dispose d'une machine S, qui héberge à la fois le site web public du CHU (disponible en https) et à la fois un accès Intranet (toujours par https). La résolution de noms pour ce domaine se fait par la machine DNS. Pour les étudiants l'accès Intranet leur permet de visualiser l'emploi de temps, les notes. Pour les enseignants et médecins cela leur permet de visualiser leurs emplois de temps, mais également d'accéder à des ressources pédagogiques et de recherche. Le personnel administratif peut modifier le site web et avoir un accès Intranet pour la gestion des salles, des étudiants, etc.

La machine S héberge également un logiciel de gestion de patients et de RDVs, lié à un service comptable. Le logiciel de gestion de patients est une application web qui peut être utilisée à partir des machines fixes (ordinateurs dans les bureaux du personnel de santé) mais aussi à partir de tablettes utilisées localement pour la gestion des RDVs et des dossiers des patients. L'application fonctionne en mode client-serveur. La machine S héberge le serveur de cette application, tandis que les machines qui s'y connectent jouent le

rôle de clients. Une authentification à double facteur est obligatoire dans ce cas-ci. Le RSSI a reconfiguré l'application pour que le serveur écoute sur le port TCP 1224.

Cette application doit également être joignable par le service de comptabilité, qui fait le suivi financier des RDVs.

L'application de gestion de patients/RDVs qui est hébergée sur le serveur S doit pouvoir accéder à une base de données sécurisée, hébergée sur une machine qu'on appelle BDD. L'accès à la base de données se fait en MySQL via son port standard 3306. Un service d'anonymisation mis en place sur cette machine permet également de produire, à partir des données de la BDD, des extraits massifs de données anonymisées, auxquels ont accès seulement les chercheurs du CHU. Ces extraits sont retrouvables via SFTP et suivant une double authentification.

Ayant déjà été victime d'une cyberattaque de type rançongiciel, le CHU a mis en place un système de sauvegarde récurrent, qui permet le stockage d'un état complet des services mentionnés ci-dessus à la fin de chaque jour sur une machine (dont on change le dispositif de stockage régulièrement), qui s'appelle AUX.

Infrastructure

L'infrastructure ci-dessus utilisera seulement des adresses privées, dont les valeurs sont de votre choix mais qui doivent garantir les tailles de réseaux demandées ci-dessous. L'infrastructure contient plusieurs plages contiguës d'adresses, correspondant aux « zones » suivantes :

- Réseau patients : une sousplage de classe C
- Réseau visiteurs : une sousplage en /26
- Réseau enseignants, chercheurs et enseignants-chercheurs : une sousplage en /22
- Réseau étudiants : une sousplage en /22
- Réseau comptabilité : une sousplage en /24
- Réseau personnel soignant : une sousplage en /22
- Réseau serveur S : une sousplage en /28 qui ne contient que les machines S et DNS. L'adresse IP de S est fixée à 172.16.3.28.
- Réseau DSI : une sousplage en /24. L'adresse dédiée du responsable RSSI est la première adresse machine de cette plage.

La DSI héberge, au sein de son sous-réseau, les machines sensibles : le serveur MAIL, la machine BDD et la machine AUX.

Le serveur S se retrouve derrière son propre routeur, dans sa propre plage.

Chaque sous-plage accède au réseau par le biais de son propre routeur. Il n'y a pas de routeur partagé par deux sous-réseaux. Finalement, un routeur spécial noté R0 est l'intermédiaire entre chacun des routeurs

des sous-plages et Internet. Il n'y a pas d'accès vers ou à partir d'Internet qui passe autrement que par R0.

Accès

Le RSSI veut s'assurer que toute partie de son infrastructure soit seulement accessible selon besoin. Les accès suivants doivent être garantis :

- Résolution DNS : toute gestion de résolution de noms se fait en utilisant le serveur DNS du CHU.
- Accès Internet : on suppose que tous les accès Internet se font exclusivement par nom de domaine et non par adresse IP.
- Accès ping : La DSI doit pouvoir faire des pings envers toutes les machines présentes dans l'infrastructure.
- Patients + visiteurs : les patients et les visiteurs doivent pouvoir accéder à S pour visualiser seulement le site web public. Ils ne doivent pas avoir accès à d'autres parties de l'infrastructure. Tout patient et/ou visiteur doit pouvoir accéder à Internet.
- Étudiants et enseignants : accès à la boîte mail CHU, accès à S (site public et Intranet), accès Internet.
- Chercheurs et enseignants-chercheurs : même accès que les étudiants et les enseignants, et en plus accès à la machine BDD en SFTP (accès aux données anonymisées).
- Personnel soignant : accès au service de messagerie sur MAIL et au service de gestion de patients et de RDVs présent sur S. Accès Internet et accès au site public hébergé sur S.
- Comptabilité et administration : accès service messagerie, accès à S pour le suivi financier des RDVs, accès Internet et au site public hébergé sur S.
- DSI : la DSI en général doit pouvoir accéder à tous les services et machines ci-dessus sauf BDD (même si tout le personnel DSI n'aura pas nécessairement les droits d'accès en double authentification pour les services), ainsi qu'à Internet. Le RSSI doit pouvoir accéder à toute machine, y compris à BDD.

Astuces : Le sujet ne précise pas la liste exhaustive des accès nécessaires (et ne détaille pas tous les besoins justement pour vous permettre de réfléchir là-dessus). Vous pourriez par exemple réfléchir à la différence, en termes d'accès ou des flux de messages, entre un accès à la partie publique du site web et l'accès en Intranet. Vous pouvez également penser à la problématique d'accès, depuis l'extérieur du CHU, pour les étudiants, profs, personnel soignant, etc. N'oubliez pas de détailler ce type de questions et votre analyse, dans le rapport !