IUC-Prépa Exam

ETUDE DU CONTEXTE

1- Quels sont les critères traditionnels de la sécurité ? La DSI souhaite ajouter le critère de traçabilité dans le périmètre de son étude. Proposer une définition de ce critère
2- Définir les notions : Risque, Menace, Vulnérabilité. Donnez une équation du risque.
3- Dans notre contexte, à quoi sert la matrice des risques informatiques.
4- Quelles sont les bonnes pratiques pour réduire ces risques informatiques.
5- Vous avez croisé votre Directeur Général dans le couloir qui en substance disait au DSI« Il faut que l'on se fasse certifier 27001, c'est primordial ! Il faut gérer l'incertitude, maintenir une inquiétude raisonnée et entretenir une véritable vigilance en mettant en place une politique de défense en profondeur»
   a) Définir le concept de défense en profondeur.
   b) Qu'est-ce qu'un SMSI, donnez un exemple d'outil pouvant faire référence.
   c) Cette norme est fondée sur le PDCA. Donnez son principe et décrivez les différentes étapes.
   d) Pour une garantie majeure de sécuriser les infrastructures, l'entreprise mise sur les outils de type SIEM. De quoi s'agit-il et donnez deux exemples.

Exercice1.

Dans le cadre de sa mission de fournisseur d'énergie, SITRAELEC doit prendre en compte la sécurité de ses réseaux de distribution et de gestion. M. CHANGA, l'adjoint à la DSI, a la responsabilité de la sécurité des systèmes d'information (RSSI).

Abonné aux alertes du site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), l'avis du 14 mai 2019 concernant notamment trois vulnérabilités (exécuter des commandes système arbitraires avec les privilèges du serveur de base de données local : élévation de privilège) publiquement connues (CVE) a attiré son attention. Ces vulnérabilités décrivent plusieurs failles de sécurité découvertes dans le logiciel utilisé dans le réseau de distribution d'électricité (ICS) de SITRAELEC, à savoir le logiciel SIMATIC WinCC.

1. CVE, qu'est-ce que c'est?
2. En quoi va consister la vulnérabilité liée à « Une élévation de privilèges »

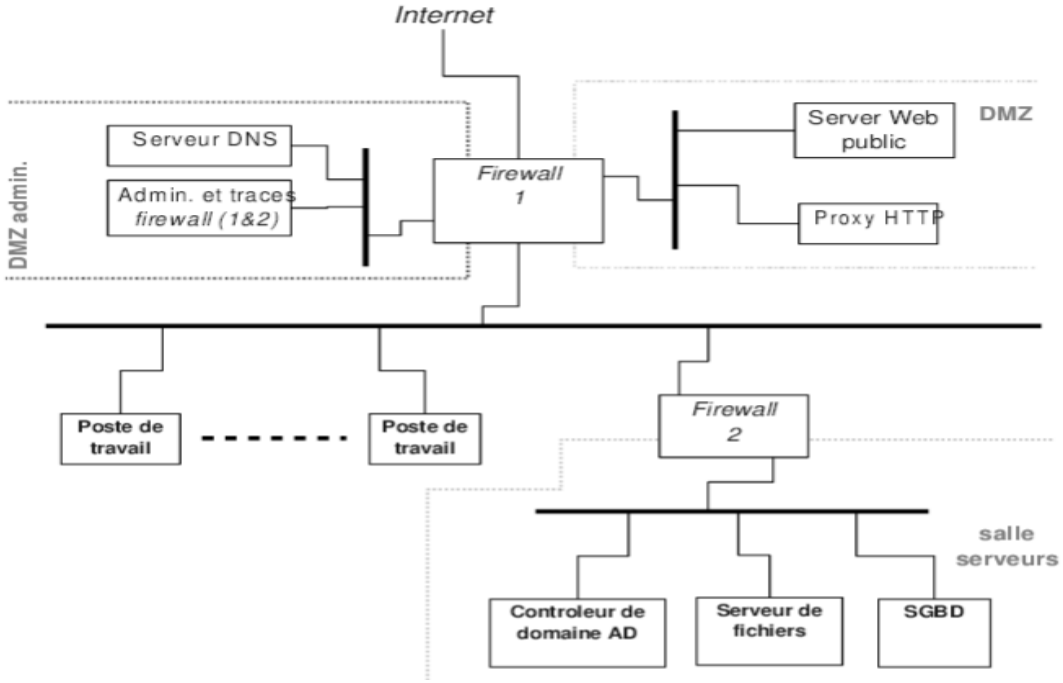
Pour mieux appréhender la situation, il organise un appel d'offre pour faire auditer la sécurité de son réseau. Deux offres sont proposées :

3. Un scan de vulnérabilités: à l'aide de sondes spécialisées placées à différents endroits du réseau, l'expert découvrira automatiquement les vulnérabilités des équipements ;
4. Un test d'intrusion: sans aucune information préalable, l'expert tentera de pénétrer le réseau de l'entreprise depuis Internet et de s'approprier des informations confidentielles.

Chaque audit est utile à sa manière. Pour chacun, décrire une situation qui en ferait l'usage approprié

Exercice2

On étudie l'architecture de protection réseau suivante:



Question1: Compte tenu du mode de fonctionnement suggéré par le schéma, présentez les différentes zones de sécurité associées à l'architecture de protection réseau et leurs niveaux de sécurité respectifs

Question2: On a ici une architecture de protection faisant appel à deux équipements distincts, l'un tourné vers Internet et l'autre vers les systèmes serveurs.
Que pensez-vous de ce choix d'architecture en termes de protection, de configuration? Quelles seront à votre avis les contraintes de fonctionnement respectives de chacun des deux équipements, en particulier du point de vue des flux réseaux à traiter (nature, débit, etc.).(Mettez notamment en évidence les différences.)

Question3: On suppose que les deux firewall sont de technologie identique et que le serveur d'administration et de gestion des traces est unique pour les deux. Commentez cet aspect vis
A vis de l'administration et du positionnement de la DMZ d'administration

Exercice 3

Une société, soucieuse d'améliorer sa notoriété, décide de mettre en ligne un serveur HTTP et FTP accessible au public. Ce serveur, installé dans les locaux de l'entreprise, sera placé dans une zone démilitarisée (DMZ) comme l'indique l'annexe 1. L'équipement pare-feu (firewall) contrôle les accès qui arrivent sur ses différentes interfaces. Il est programmé de telle façon que seul le trafic réseau respectant les règles indiquées dans l'annexe 2 est accepté. Ces règles peuvent faire référence à des adresses IP d'ordinateurs, des adresses de réseau et des protocoles réseau. Un serveur mandataire (proxy) est également installé entre le routeur R1 et

le pare-feu : il est le point de passage obligatoire de tous les accès du réseau local vers l'internet.

a) Expliquer en quoi la mise en œuvre d'une zone démilitarisée permet d'améliorer la sécurité du réseau local. **1pt**

Un anti-virus a révélé la présence d'un programme « cheval de Troie » sur le serveur situé dans la DMZ.L'étude révèle que le "troyen" n'a pas été placé par les protocoles HTTP ou FTP.

b)

a. ces incidents de nature malveillante peuvent survenir sur les équipements informatiques: poste et/ou serveur bloqué par un «cryptovirus» . Quelles recommandations préconisez vous d'appliquer en premier lieu ?

b. En analysant les règles de l'annexe 2, indiquez quelle règle a pu permettre l'installation de ce programme. Proposer, pour réduire les risques liés à ce type de problème, une ou plusieurs règles en remplacement de la règle concernée.**2pts**

c) Définissez ce que sont un Virus et un cheval de Troie. Quelles sont les différences entre ces menaces ? Comment se protéger d'un cheval de Troie ?**3pts**

Ce « cheval de Troie » est destiné à perturber le fonctionnement du réseau local, en s'exécutant automatiquement périodiquement.

d) En analysant les règles de l'annexe 2, indiquez si les postes du réseau local sont susceptibles d'être atteints par le « cheval de Troie ». **1pt**

Annexe : Architecture avec pare-feu (*firewall*) et serveur mandataire (*proxy*)