TLS-SEC

Questions et exercices d'examen

22 janvier 2016

Gouvernance de la sécurité des systèmes d'information

Consignes aux élèves et aux surveillants : *idem* première partie.

Répondez sur le document.

Partie I

Questions à choix unique (Une seule bonne réponse possible.)

Attention :

Réponse exacte : 1 point en plus
Réponse fausse : 0,25 point en moins
Pas de réponse : 0 point

Q1 Les documents stockés dans un répertoire « Privé et personnel » sur un PC professionnel :

- ☐ Ne peuvent être accédés que par un officier de police judiciaire dûment porteur d'une commission rogatoire d'un juge d'instruction.
- ☐ N'importe quel administrateur peut y accéder et transmettre le contenu à la hiérarchie du salarié pour le faire virer.
- ☐ Peuvent être ouverts en l'absence du salarié par son employeur disposant d'un motif légitime, en présence d'un représentant du personnel.
- ☐ Peuvent être chiffrés et leur propriétaire légitime peut refuser de les révéler à un enquêteur parce qu'ils sont personnels.

Q2 Un bon exemple d'expression de besoin en terme de sécurité :

- ☐ Tous les postes de travail doivent être équipés d'un antivirus.
- ☐ Tous les projets doivent faire l'objet d'une analyse de risques permettant d'identifier les besoins de sécurité.
- ☐ Tous les utilisateurs doivent faire l'objet d'une identification valide par rapport au répertoire GROMIAM et d'une authentification s'appuyant sur une information connue seulement de ces utilisateurs.
- ☐ Un nom d'utilisateur et un mot de passe seront suffisant pour accéder à l'application.

Q3 Quel est l'avantage principal du rattachement d'un RSSI à la direction audit, finances et comptabilité ?

- ☐ Il disposera de budgets plus importants pour financer la sécurité.
- ☐ Il sera indépendant de la direction informatique.
- ☐ Il n'aura pas besoin d'avoir de compétences techniques en informatique.
- ☐ Il pourra tranquillement utiliser tous les logiciels de *hacking* qu'il voudra.

Q4 Vous découvrez un mot de passe codé en dur dans le *firmware* d'un calculateur embarqué, récupéré par hasard chez un revendeur de pièces détachées informatique. Que faire de cette découverte ?

- ☐ Chercher des acheteurs potentiels sur les forums d'Internet pour en tirer le meilleur profit.
- ☐ Demander à Google s'ils seraient prêt à payer pour avoir cette information dans le cadre de leur programme de rachat des vulnérabilités (*Google Vulnerability Reward Program*).
- ☐ Contacter un CERT accrédité et suivre leurs instructions.
- ☐ Contacter le service technique du fabricant concerné pour leur transmettre l'information concernant la vulnérabilité technique.

Q5 Quelle est la catégorie de *mécanisme* de sécurité qui est nécessaire pour les niveaux de sécurité élevés dans les critères d'évaluation :

- ☐ Une politique de sécurité obligatoire.
- ☐ Un cheminement sûr.
- ☐ Une politique de sécurité discrétionnaire.
- ☐ Des scripts *suid*.

Q6 Quel est l'inconvénient le plus important d'une politique de sécurité obligatoire de type Bell-LaPadula ?

- ☐ L'existence de canaux cachés nécessitant une évaluation de vulnérabilité.
- ☐ Une surclassification progressive de l'information au fil du temps (et l'existence fréquentes de processus « de confiance » pour déclassifier).
- ☐ La difficulté à contourner les règles de sécurité obligatoires.
- ☐ La rigidité de l'utilisation qui empêche les utilisateurs privilégiés d'accéder aux informations courantes.

Q7 Quel est l'organisme qui est chargé de la sécurité informatique au niveau européen :

- ☐ L'ENISA
- ☐ L'ENIRIPSA
- ☐ Le NIST
- ☐ L'ITSEC

Q8 Après l'examen, le relevés de notes ne peut être accédé que par les professeurs et l'administration de l'N7. C'est une règle :

- ☐ de confidentialité
- ☐ d'intégrité
- ☐ de disponibilité
- ☐ de *survivability*

Q9 Sur un système d'exploitation mettant en œuvre une politique multi-niveaux de Bell La Padula, peut-il y avoir des droits d'accès et un propriétaire associés aux fichiers ?

- ☐ OUI
- ☐ NON

Question bonus ! (Pas de malus)

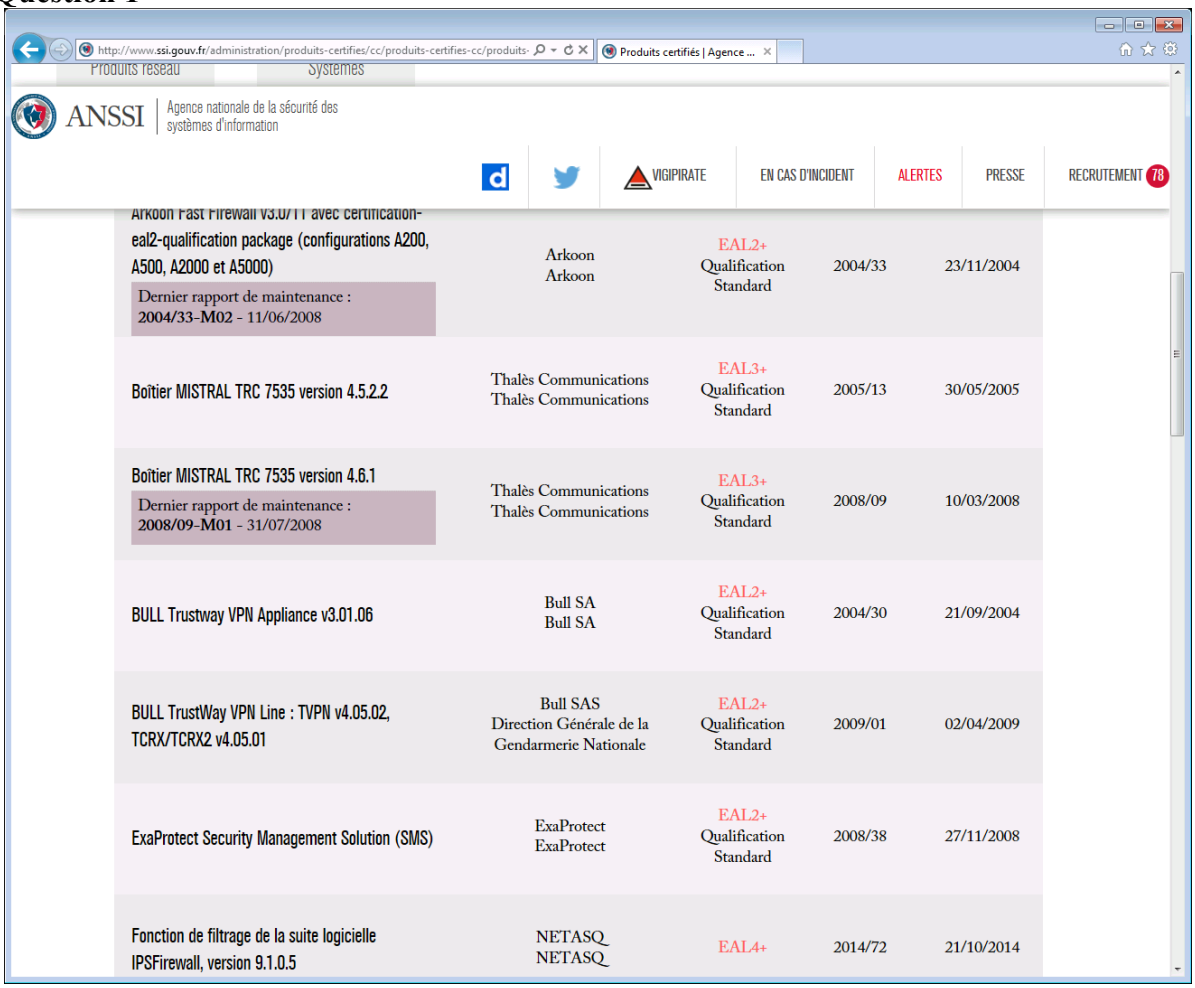
Quelles sont les raisons *vraisemblables* (*plusieurs réponses possibles*) pour lesquelles on refuse de vous laisser examiner le code source d'une application que vous souhaitez acheter ?

- ☐ Pour protéger le patrimoine intellectuel de l'éditeur commercialisant le logiciel, on ne peut pas vous laisser examiner les algorithmes originaux contenus dans le code source.
- ☐ Pour pouvoir breveter le logiciel, il est absolument nécessaire de le garder confidentiel pendant la phase de dépôt du brevet.
- ☐ L'éditeur n'est en fait pas propriétaire du code source et n'en dispose pas.
- ☐ Le code source de l'application est bien trop gros pour être audité vis à vis de la sécurité et il faut des compétences tout à fait particulière en développement pour le faire.
- ☐ L'application contient un mot de passe, légèrement dissimulé par une méthode naïve, un ou-exclusif avec le nom de la société.

Partie II

Cette partie est constituée de quatre questions ouvertes. Répondez sur la feuille.

Question 1



Arkoon Fast Firewall v3.0/11 avec certification-eal2-qualification package (configurations A200, A500, A2000 et A5000) Dernier rapport de maintenance : **2004/33-M02** - 11/06/2008	Arkoon Arkoon	EAL2+ Qualification Standard	2004/33	23/11/2004
Boîtier MISTRAL TRC 7535 version 4.5.2.2	Thalès Communications Thalès Communications	EAL3+ Qualification Standard	2005/13	30/05/2005
Boîtier MISTRAL TRC 7535 version 4.6.1 Dernier rapport de maintenance : **2008/09-M01** - 31/07/2008	Thalès Communications Thalès Communications	EAL3+ Qualification Standard	2008/09	10/03/2008
BULL Trustway VPN Appliance v3.01.06	Bull SA Bull SA	EAL2+ Qualification Standard	2004/30	21/09/2004
BULL TrustWay VPN Line : TVPN v4.05.02, TCRX/TCRX2 v4.05.01	Bull SAS Direction Générale de la Gendarmerie Nationale	EAL2+ Qualification Standard	2009/01	02/04/2009
ExaProtect Security Management Solution (SMS)	ExaProtect ExaProtect	EAL2+ Qualification Standard	2008/38	27/11/2008
Fonction de filtrage de la suite logicielle IPSFirewall, version 9.1.0.5	NETASQ NETASQ	EAL4+	2014/72	21/10/2014

A quoi correspond la liste des équipements identifiée (partiellement) sur cette page ?

Indiquez les informations les plus intéressantes concernant la sécurité des quelques produits (pris au hasard) figurant sur cette liste.

Question 2

Présentez les avantages et les inconvénients associés à l'utilisation d'une analyse de risques.

Question 3

Expliquez pourquoi le *nombre de chemins* d'attaques existant entre un ensemble de privilèges de départ (ceux de l'attaquant) et un ensemble de privilèges cibles dans le modèle du graphe des privilèges n'est pas une très bonne mesure de la sécurité.

Question 4

Dans le chapitre « Intégration de la SSI dans le cyle de vie des systèmes d'information », le PSSIE contient une section relative à la « Gestion des risques et l'homologation de sécurité » où l'on trouve l'objectif suivant et sa déclinaison (p.18 de la v.1.0) :

Objectif 5 : risques. Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information. Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée), le cas échéant après avis de la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

Quelles sont les entités de l'organisation qui sont rendues nécessaires par cet objectif ?

Quelles sont les activités qui sont rendues nécessaires ici ?

Sachant que la PSSIE couvre l'ensemble des services de l'état français, quelles difficultés pouvez-vous envisager pour la mise en application de cette régle ?