

Questionnaire de survol pour l'évaluation des connaissances

Prénom & NOM : ORTALO Rodolphe Filière : Vacataire désigné

#	Questions [RAPPEL – le thème transverse de ce module est : "politiques de sécurité et évaluation de la sécurité"]	partie réservée à l'évaluation 0 1 2
1	<p>Donnez 4 exemples de malveillances, de fautes accidentelles ou de fautes intentionnelles mais non malveillantes (au moins 1 de chaque).</p> <p><i>Casser une vitre pour pénétrer dans un domicile : malveillant (sauf s'il y a le feu)</i></p> <p><i>Attaquer la porte d'entrée à la hache : intentionnel non malveillant (c'est un pompier à tous les coups - vous avez déjà vu un cambrioleur aussi débile ? de toute façon, il vaut mieux faire comme si c'était un pompier, c'est lui qui tient la hache.)</i></p> <p><i>Ecraser les pieds de sa cavalière : accidentel (si si, juré)</i></p> <p><i>Oublier son portable chez lui : intentionnel non malveillant (elle le trouve craquant).</i></p> <p><i>Oublier son portable chez elle : accidentel (ils sont trop bêtes pour avoir l'idée)</i></p>	
2	<p>Quelles sont les difficultés de mise en œuvre des politiques de sécurité obligatoires (MAC) par exemple dans les systèmes comme SELinux ?</p> <p><i>Depuis que Snowden a ouvert sa gueule, comme c'est la NSA qui l'a écrit et financé, plus personne n'a confiance dans l'implémentation. En plus, toutes les règles ont été produites expérimentalement alors...</i></p>	
3	<p>Quelles sont les informations fournies quotidiennement par un CERT dans le domaine technique ? Quel est leur avantage ?</p> <p><i>Ils rappellent au patron que le sous-traitant qui a bricolé le site Web devait faire un audit de sécurité sur la version en question du middleware. L'avantage avec eux, c'est que le patron croit pas le patron du sous-traitant quand il dit qu'on est nuls et qu'on raconte que des conneries (c'est le CERT quand même !).</i></p>	
4	<p>Donnez des exemples de vulnérabilités résiduelles associées à un tunnel réseau chiffré.</p> <p><i>On perd en général le papier sur lequel on note le mot de passe avant l'expiration des clefs d'authentification. Comme il fait 7 ou 8 caractères, on met ensuite parfois plusieurs jours à le craquer. Après, on retrouve le papier.</i></p>	
5	<p>Donnez 2 exemples de règles de sécurité dans une organisation.</p> <p><i>L'important c'est d'avoir tous les droits d'accès déployés rapidement.</i></p> <p><i>Pour des raisons de sécurité, on ne peut pas vous montrer le code source des applications. (NdE : Il y a les mots de passe dedans...)</i></p>	
6	<p>Pourquoi le nombre de scénarios d'attaque (ou de vulnérabilités) dans un syst d'information n'est pas une mesure intéressante pour suivre la sécurité ?</p> <p><i>Parce qu'il est toujours à 0 à la fin dans le rapport final validé ?</i></p>	
7	<p>Comment gérer la prise en compte de la sécurité dans le cadre d'un marché passé avec un sous-traitant ?</p> <p><i>On demande à la cellule juridique de s'en occuper. Une fois la réponse arrivée, même le marché public renouvelable le plus long est obsolète (sauf peut-être dans le cas des concessions autoroutières – mais il y a la ceinture et la barrière de sécurité – on sait bien que les autoroutes sont plus sûres).</i></p>	