Questionnaire de survol pour l'évaluation des connaissances

Prénom & NOM : __ORTALO Rodolphe _____ *Filière :* _ Vacataire désigné _____

#	Questions *[RAPPEL – le thème transverse de ce module est : "poltiques de sécurité et évaluation de la sécurité"]*	partie réservé à l'évaluation 0 1 2
1	**Donnez 4 exemples de malveillances, de fautes accidentelles ou de fautes intentionnelles mais non malveillantes (au moins 1 de chaque).** *Un bug dans un programme : faute intentionnelle mais non malveillante* *L'installation d'un keylogger matériel : malveillance* *Un « collage à 1 » dans une RAM de satellite : accidentel (rayonnement solaire)* *Un atterrissage de tête dans un disque dur : accidentel*	
2	**Quelles sont les difficultés de mise en œuvre des politiques de sécurité obligatoires (MAC) par exemple dans les systèmes comme SELinux ?** *Les règles de paramétrage des contrôles obligatoires sont très complexes à écrire pour chaque application.* *Si elles sont générées à partir de situations expérimentales, celles-ci ne font alors que valider le comportement usuel dans ces situations (qui peut être non protégé).*	
3	**Quelles sont les informations fournies quotidiennement par un CERT dans le domaine technique ? Quel est leur avantage ?** *Le CERT diffuse des avis de vulnérabilités concernant les principaux logiciels. L'avantage des avis des CERT est notamment d'être indépendant des constructeurs et vérifiés.*	
4	**Donnez des exemples de vulnérabilités résiduelles associées à un tunnel réseau chiffré.** *Les clefs de chiffrement utilisées sont de longueur finies.* *La distribution préalable ou le renouvellement des clefs d'authentification est faite hors ligne souvent de manière peu protégée.*	
5	**Donnez 2 exemples de règles de sécurité dans une organisation.** *Un utilisateur ne peut demander seul des droits d'accès pour lui-même.* *Les accès réseaux doivent transiter par un parefeu. Les accès http doivent transiter par un proxy géré à « telendroit ».* *L'authentification pour un accès distant au réseau d'entreprise doit faire appel à un dispositif cryptographique portable (type carte à puce).*	
6	**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 ?** *Parce qu'il varie beaucoup trop facilement, même face à des évolutions mineures des vulnérabilités du système.*	
7	**Comment gérer la prise en compte de la sécurité dans le cadre d'un marché passé avec un sous-traitant ?** *La prise en compte passe essentiellement par l'intégration d'une clause contractuelle avec le sous-traitant. (Celui-ci est ensuite autonome – et responsable – pour l'atteinte des objectifs de sécurité qui lui ont été fixés avec les moyens accordés.)*	