CNAM Bretagne, Cybersécurité SEC101, eduf@ction
Notes de cours éditées le 25 janvier 2020

Les fiches techniques : vos travaux à rendre

Eric DUPUIS[1,2*]

Résumé
Ce document fournit les instructions pour la réalisation des travaux personnels du chapitre sécurité opérationnelle du cours SEC101.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Travaux pratiques, études, travaux personnels

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

1. Travaux personnels

1.1 généralités

Dans le cadre de ce cours, un seul travail est demandé. C'est un travail personnel, dont l'objectif est de vous faire travailler sur un sujet que vous souhaiter étudier dans le but de le présenter aux autres. Vous pouvez donc choisir un sujet que vous maitrisez ou un sujet que vous ferez découvrir avec un regard de béotien.

En résumé votre travail devra être :

- 1 document de moins de 20 pages
- Sur un produit du monde de la Sécurité Opérationnelle
- Un travail de votre expérience, ou simplement sur une recherche sur internet pour un produit à choisir ...

Votre analyse sera étayée et critique sur un élément de la sécurité opérationnelle. La notion d'élément SECOPS regroupe de nombreuses thématiques :

- Méthodologique ;
- Technologique ou technique ;
- Conceptuel ;
- Juridique...

Sur ces thématiques, il est important que votre sujet de FICHE TECHNO reste dans le domaine de la sécurité opérationnelle :

- **VEILLE/AUDIT** : Des produits/services de veille et de scan de vulnérabilités informatiques (Qualys, nessus, nmap, checkmarx, appscan . . . et bien d'autres . . .)
- **SURVEILLE/ALERTE** Des produits/services de gestion d'événement, de supervision et d'alerte (Log, SIEM : Qradar, ArcSight, LogPoint, splunk . . . et bien d'autres . . .)
- **ANALYSE/REPONSE** : Des produits/services d'analyse post-mortem, et de forensique (Forensic Toolkit, encase . . . et bien d'autres . . .)

Votre travail est à rendre en fin de session, sous forme informatique (OpenDoc, Formats Microsoft, PDF, Latex...)

1.2 méthode de notation

Votre travail est noter sur différents critères ci dessous.

Chaque critère est évalué suivant les valeurs suivantes

- Qualité du positionnement du problème ou du sujet
- Qualité de la conclusion, dont l'ouverture vers d'autres points
- Présence et affichage de votre point de vue : Apports personnels : apports liés à sa propre expérience

Les valeurs d'évaluation de ces critères sont :

- 0 - Travaux trop simpliste et sans valeur d'apport personnel ;
- 1 - Travaux simple ou sans apport personnel ;
- 2 - Apport étayé et présentation claire ;
- 4 - Apport didactique ;
- 5 - Apport personnel étayé.

1.3 Format

Si le format n'est pas imposé, il est demandé toutefois de suivre un plan permettant de suivre votre démarche et permettant d'être le plus pédagogique possible. Vous pouvez utiliser le modèle de document mis à votre disposition.

- WORD : SEC101-Part3-Modele-Fiche-Techno-VxRy
- Latex : MemModel sur GITHUB (Cyberdef101)

2. Sujets

2.1 Sélection des sujets

Avant de vous lancer dans vos travaux, il est demander de faire valider votre sujet par l'enseignant. Pour cela simplement envoyer un mail avec votre sujet et vos justificatif de choix.

Vous trouverez ci après quelques différentes thématiques avec des idées de sujet. Chaque sujet est constitué d'un thème, et d'un descriptif optionnel. Ces sujets sont donnés à titre indicatif. Il vous revient d'en proposer un si aucun de ceux présentés vous intéressent.

Votre travail est **à rendre** en fin de session

2.2 Sujets : Vulnerability Management

2.2.1 Exemples étayés de vulnérabilités

2.2.2 BugBounty

2.2.3 Outils au service des tests d'intrusion

2.3 Sujets : Threat Management

2.3.1 Description d'une attaque virale

2.3.2 Architecture d'un BOTNET

2.3.3 Description attaque DDOS

2.4 Sujets : Incident Management

2.4.1 Description attaque DDOS

2.5 Sujets : Crisis Management

2.5.1 ISO22301

2.5.2 Annuaire de crise

Table des matières

Table des figures