EPHEC

Louvain-la-neuve

Sécurité des réseaux informatiques

Travail de recherche

Enoncé destiné aux 3T

Virginie Van den Schrieck

5 octobre 2015

1 Objectifs du travail

Dans le cadre du cours de Sécurité des réseaux informatiques, il vous est demandé de mener, individuellement, une recherche documentaire sur un sujet au choix lié bien sûr au domaine de la sécurité.

Pour rappel, les acquis d'apprentissage du cours sont :
- Etre capable d'expliquer les différentes méthodes d'attaques
- Pouvoir, sur base d'une situation d'un système informatique, évaluer les risques liés à la sécurité
- Proposer des contre-mesures techniques ou autres pour pallier ces riques
- Lister les risques résiduels en fonction de la stratégie de sécurité appliquée

Ce travail de recherche doit permettre à l'étudiant de démontrer qu'il est capable d'appliquer cette démarche stratégique de manière approfondie dans le cadre d'un sujet précis qu'il aura décrit avec précision du point de vue technique. Ce travail compte pour 25% de la note finale du cours théorique.

2 Description du travail

2.1 Choix du sujet

Les étudiants sont libres de la thématique à aborder dans le cadre de ce travail. Néanmoins, cette thématique doit s'inscrire dans la grille d'analyse vue au cours, et doit donc s'insérer dans une situation concrète.

Le thème peut donc être :
- une situation de départ (ex : sécurisation d'une PME, hardening d'un serveur),
- une attaque qui sera alors présentée dans un cas concret (ex : injection SQL sur le site web d'une ASBL organisant des stages sportifs, infestation d'un réseau d'entreprise par un worm),
- ou une contre-mesure qui sera utilisée (parmi d'autres mesures qui seront mentionnées mais moins détaillées) dans un cas concret (ex : déploiement d'une application Web nécessitant entre autres la configuration d'un firewall).

Le choix du sujet est à faire valider par le professeur.

2.2 Eléments du rapport

Le rapport de recherche documentaire devra comporter les éléments suivants :
- Une introduction expliquant les grandes lignes du sujet choisi et le contexte dans lequel il s'insère
- Une description de la situation concrète
- La présentation technique du sujet choisi
- L'analyse de sécurité structurée tel que vu au cours
- Une conclusion reprenant les principales contributions du travail effectué.
- Une bibliographie correctement mise en forme, contenant des références pertinentes (articles sérieux) et utilisées dans le texte

A titre indicatif, le rapport attendu devrait comporter entre 4 et 8 pages.

2.3 Correction croisée

Avant la remise finale du rapport, les étudiants auront l'opportunité de faire relire leur travail par un de leurs condisciples. L'objectif est de pouvoir recevoir un premier feedback (évaluation formative) permettant d'améliorer la production avant l'évaluation finale, qui, elle, sera sommative.

Après avoir remis son travail, chaque étudiant recevra un rapport à corriger. Il est invité à lire attentivement ce rapport conformément à la grille d'évaluation fournie plus bas, et à proposer un feedback **constructif** permettant à l'auteur d'améliorer sa production.

3 Calendrier du travail

Le travail de recherche comporte quatre échéances :

1. **Dépot du sujet** : Un document PDF d'une page sera remis au professeur via le Campus Virtuel pour **le mardi 13/10 13h**, comportant un descriptif du sujet choisi et une brève description du cas illustratif. Le sujet sera validé ou non endéans la semaine suivant cette remise.
2. **Remise de la première version** : Une première version finale du travail sera déposée sur le Campus Virtuel pour **le vendredi 30/10 à 13h**, et envoyée par email à l'étudiant correcteur (information communiquée ultérieurement).
3. **Remise du feedback de la correction croisée** : La grille d'évaluation remplie et les commentaires annexes seront transmis à l'étudiant concerné directement par email, et seront également soumis sur le Campus Virtuel pour le **vendredi 13 novembre à 18h**
4. **Remise de la version modifiée** : La version finale du rapport sera déposée sur le Campus Virtuel pour **le vendredi 20 novembre à 13h**.

4 Charge de travail demandée

Le cours théorique est crédité de 3 ECTS. En terme d'heures de travail, cela correspond à $25 \times 3 = 75$ heures de travail, qui se répartissent plus ou moins comme suit :

- $12 \times 2h30 = 30h$ en séance encadrée
- $15h$ de relecture hebdomadaire des notes
- $10h$ de préparation à l'examen
- $20h$ pour le travail de recherche

Dans le cadre du travail de recherche, les $20h$ prévues se répartissent comme suit :

- $2h$ pour la recherche du sujet et la rédaction du premier délivrable,
- $5h$ pour la recherche documentaire,
- $8h$ pour la rédaction du rapport,
- $3h$ pour la correction croisée,
- $2h$ pour l'amélioration du rapport sur base du feedback reçu.

5 Evaluation

5.1 Grille d'évaluation

La répartition des points pour ce travail s'effectue de la manière suivante :

Elément	**Pondération**
Respect des échéances	1
Qualité du feedback donné	4
Intégration du feedback reçu à la version finale	2
Forme du rapport final	2
Intro/conclusion	1
Descriptif technique	5
Cas illustratif et analyse	5
Total	**20**

5.2 Critères d'évaluation pour le rapport final

Les critères listés ci-dessous seront utilisés pour l'évaluation du rapport final. Les étudiants peuvent bien entendu s'en inspirer pour la correction croisée.

- Le rapport contient une page de garde claire reprenant les éléments principaux (auteur, classe, cours, titre, ...)
- Le texte du rapport est agréable à lire (style, orthographe)
- La structure du rapport est claire et pertinente (découpage en sections et paragraphes)
- L'introduction présente bien le sujet choisi et le contexte dans lequel il s'insère, ainsi que le cas illustratif qui sera présenté
- Au niveau technique, le sujet est décrit de manière précise, complète et compréhensible.
- La description technique est renforcée par des références sérieuses
- Si le sujet est une menace (description d'une attaque réelle ou d'un dispositif d'attaque), les contre-mesures possibles sont présentées
- Le cas illustratif choisi est réaliste
- Le sujet s'intègre bien dans le cadre du cas illustratif
- Le cas illustratif est décrit de manière complète
- L'analyse stratégique est correctement appliquée au cas illustratif
  - Les avoirs à protéger sont bien identifiés et classifiés en fonction de leurs valeurs
  - Les vulnérabilités sont listées de manière complète
  - Les attaques correspondant à ces vulnérabilités sont identifiées
  - Les risques liés à ces attaques sont évalués
  - Des contre-mesures sont proposées pour pallier à ces risques, et des choix sont effectués en fonction des coûts impliqués
  - Les risques résiduels sont bien documentés
- La conclusion reprend les éléments principaux du rapport
- La bibliographie est complète et bien présentée