Sécurité des systèmes d'information

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

Syllabus du cours sur le thème Sécurité des systèmes d'information dispensé en seconde année de Master (M2) de la filière Systèmes de Télécommunications et Réseaux Informatiques (STRI) à l'Université Toulouse 3 - Paul Sabatier.

Table des matières

1. Copyright et Licence 1
    1.1. Méta-information 1
2. Volume horaire, méthode pédagogique et projet 1
3. Scénario d'entreprise type : Candide S.A. 2
4. Architecture du système d'information 3
5. Echéancier des séances 4
6. Évaluation 5

1. Copyright et Licence

```
Copyright (c) 2000,2024 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the
terms of the GNU Free Documentation License, Version 1.3 or any later version
published by the Free Software Foundation; with no Invariant Sections, no
Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included
in the section entitled "GNU Free Documentation License".
```

```
Copyright (c) 2000,2024 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon
les termes de la Licence de Documentation Libre GNU (GNU Free Documentation
License), version 1.3 ou toute version ultérieure publiée par la Free Software
Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture,
et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est
incluse dans la section intitulée « Licence de Documentation Libre GNU ».
```

1.1. Méta-information

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `security.pdf`.

2. Volume horaire, méthode pédagogique et projet

Il est possible d'aborder l'enseignement sur la sécurité des systèmes d'information suivant plusieurs axes pédagogiques. Dans le cas présent, l'objectif général est de faire «découvrir» l'importance des processus de sécurité à partir d'illustrations pratiques.

Il est bien entendu que ce choix ne prétend nullement être «la bonne méthode» pédagogique. Il est cependant complètement ridicule d'enfermer les choix pédagogiques dans une opposition artificielle entre un enseignement académique qui introduit le vocabulaire et les méthodologies sans aucune application et un enseignement cantonné dans la technique qui ne propose aucune prise de recul.

Ce cours est un module construit sur 10 séances de 3 heures et une séance d'évaluation de 3 heures. Les 7 séances sont réparties de la façon suivante :

- 3 séances de cours avec la promotion complète.
- 7 séances de travaux pratiques en groupe.

À la suite de la première séance de présentation, les étudiants sont répartis en 3 groupes pour travailler sur un projet. Ce projet consiste à étudier et déployer une maquette d'infrastructure d'entreprise suivant un scénario type.

Les objectifs pédagogiques sont multiples :

- créer une émulation entre les groupes d'étudiants en «opposant» les rôles de chaque groupe,
- évaluer l'importance des relations humaines, de la coordination et même de l'ingénierie sociale dans la sécurité des systèmes d'information en imposant une taille de groupe importante,
- illustrer les problématiques des «métiers» de la sécurité des systèmes d'information à partir du scénario d'entreprise type.

Les groupes sont définis comme suit :

Groupe «défense»

> Ce groupe est chargé de mettre en place l'infrastructure des services du scénario d'entreprise. Il doit rechercher les moyens les plus simples possibles pour se défendre contre les tentatives d'intrusion et de compromission entreprises par le groupe «attaque».
>
> Du point de vue métier, les membres de ce groupe jouent le rôle d'exploitants des services. Comme les services peuvent être externalisés ou non, les membres peuvent être employés aussi bien chez un prestataire assurant l'externalisation qu'au sein même de l'entreprise où l'exploitation est directement assurée.

Groupe «analyse»

> Ce groupe est chargé de collecter un maximum d'informations et de les analyser pour identifier les actions entreprises aussi bien en défense qu'en attaque.
>
> Du point de vue métier, les membres de ce groupe jouent le rôle de consultants sécurité chargés de réaliser des audits. Au début du projet, ils sont étranger à la structure de l'entreprise. Par la suite, ils ne disposent que des informations et/ou des accès que leur fournissent les membres du groupe «défense».

Groupe «attaque»

> Ce groupe est chargé de rechercher toutes les possibilités d'intrusion et de compromission les plus efficaces et les plus faciles à mettre en œuvre.
>
> Du point de vue métier, les membres de ce groupe jouent le rôle de consultants sécurité chargés d'évaluer la solidité du système d'information défendu. Ils sont totalement étranger à la structure de l'entreprise. Les 2 autres groupes ne sont pas sensés leur communiquer la moindre information. Bien entendu, les membres du groupe «attaque» ne doivent pas se limiter aux moyens techniques pour collecter leurs informations.

Chaque groupe met en place une démarche de planification et de coordination des activités suivant les axes définis avec l'enseignant. Chaque groupe est libre de choisir les outils de gestion des activités. Tous les comptes rendus de tests ou les synthèses hebdomadaires doivent être centralisés et accessibles avant les séances encadrées. L'objectif pédagogique est de modéliser le fonctionnement d'un travail d'équipe dont les membres ne sont pas forcément sur le même lieu. Compte tenu de la taille de chaque groupe, la qualité de la coordination est primordiale pour l'avancement du projet.

3. Scénario d'entreprise type : Candide S.A.

L'activité des groupes définis ci-avant gravite autour du système d'information d'une entreprise totalement fictive mais dont les besoins sont représentatifs de ceux que l'on rencontre habituellement.

Supposons donc que les groupes vont travailler pour ou contre une agence baptisée Candide S.A.. Cette agence vient d'obtenir un gros contrat de services pour un très grand groupe industriel aéronautique. Ce grand groupe industriel est un acteur majeur dans un contexte de concurrence mondiale exacerbée.

Il fait donc l'objet d'actions d'intelligence économique tous azimuts. La chaîne des sous-traitants de ce grand groupe industriel constitue un axe de travail intéressant en matière d'intelligence économique pour collecter des informations à forte valeur ajoutée.

Notre agence Candide S.A., venant d'entrer dans cette chaîne de sous-traitance avec un contrat important, fait l'objet de beaucoup d'attention. Sa crédibilité, voire même sa survie économique, dépend de la qualité de la sécurité de son système d'information. Le rôle du groupe d'étudiants «défense» est de garantir cette crédibilité.

Compte tenu des enjeux, notre grand groupe industriel aéronautique, ne peut se contenter des engagements contractuels pris avec Candide S.A.. Aussi, il demande à quelques consultants indépendants (le groupe «analyse») d'observer au plus près les flux du système d'information du sous-traitant. Il s'agit de s'assurer que l'équipe en charge du système d'information est à même de remplir les engagements pris.

Un groupe industriel concurrent a appris par voie de presse qu'un contrat de services significatif avait été conclu entre Candide S.A. et son concurrent. À priori, Candide S.A. présente une opportunité intéressante de collecte d'informations sensibles en toute discrétion. Cette opportunité conduit notre groupe concurrent à faire appel à quelques consultants spécialisés dans ce genre de travail (le groupe «attaque»).

4. Architecture du système d'information

Pour illustrer le scénario, il faut modéliser le système d'information de l'agence de sous-traitance à l'aide d'une architecture type. La principale limitation de ce genre de maquette est l'absence d'une population suffisante d'acteurs sur le système d'information. En effet, plus la population d'utilisateurs est importante, plus l'ingénierie sociale est pertinente et efficace.

Pour rendre cette maquette de système d'information «réaliste», il est nécessaire d'introduire quelques biais :

La population des utilisateurs est limitée

> La maquette est une réduction minimaliste de système d'information. Il lui manque une population d'utilisateurs suffisante pour générer un trafic aléatoire permanent. Ce sont ces flux réseaux qui servent de «bruit de fond» pour camoufler les tentatives d'intrusion dans le système. Toute la difficulté, dans l'analyse des flux d'un véritable système d'information, est de distinguer un trafic réseau «normal» d'un trafic intrusif. A ce «bruit de fond» il faut ajouter toutes les tentatives d'intrusion leurres qui génèrent de fausses alertes : virus, vers, etc.
>
> Pour les travaux de groupes, le seul moyen d'analyse comparative envisagé consiste à confronter les données recueillies par plusieurs outils sur des postes raccordés au réseau public. De cette façon, après quelques semaines de collecte, on dispose d'un volume conséquent de «bruit de fond» et de leurres que l'on peut étudier en vis à vis des informations collectées sur la maquette.

La population des utilisateurs est singulière

> Comme les rôles des groupes d'étudiants sont biens définis au départ, il reste peu de place pour les surprises. Le comportement de chacun vis à vis du système d'information est facile à prédire. On imagine mal que le rédacteur de la politique de sécurité sur le courrier électronique se mette à l'enfreindre en quelques minutes. Il est donc très difficile d'introduire un utilisateur véritablement étranger à l'architecture du système d'information et, en plus, de lui laisser le temps de prendre des initiatives originales.

La dérive des usages

> Comme la durée du cours est limitée à quelques semaines, il est difficile d'imaginer une dérive des usages et de la configuration du système d'information par rapport aux politiques de sécurité définies. C'est pourtant une des principales pistes d'exploitation pour les tests d'intrusion.
>
> Lors des tests pratiques, il faut disposer d'au moins un serveur et un poste de travail sur lesquels la dérive est simulée en n'installant pas tous les correctifs nécessaires et conformes aux définitions des politiques de sécurité. De la même façon, on simule les prestations de services «bancales» des opérateurs en programmant des «temps d'absence» sur le pare-feu de la maquette.

5. Echéancier des séances

Séance 1Introduction et présentation du projet

Introduction à la sécurité des systèmes d'information à partir d'un jeu de questions ouvertes.

- Qu'est-ce que la sécurité d'un système d'information ?
- Quelles sont les problématiques spécifiques aux métiers de la sécurité ?
- Qu'est-ce que l'intelligence économique ?
- Quel avenir pour le marché de la sécurité informatique ?
- Qu'est-ce que la veille sécurité ?

Exemple des 4 principes de base et leurs modalités d'application.

- la connaissance de son propre système d'information,
- le principe du moindre privilège,
- la défense en profondeur,
- la prévention c'est l'idéal, la détection c'est une nécessité.

Présentation du projet et des travaux de groupes. Organisation et conditions d'accès à la maquette du système d'information.

Pour aboutir à une synthèse correcte sur la collecte d'informations, il est nécessaire de pouvoir comparer les informations issues de la maquette avec celles issues d'un réseau public courant.

Séance 2Les politiques de sécuritéL'architecture sécurisée des périmètres de services

Présentation thématique sur les politiques de sécurité. Cette présentation doit servir prioritairement au groupe «défense» dans le but de définir les modalités d'utilisation du système d'information de Candide S.A.. Le groupe «analyse» doit rechercher des exemples de politiques de sécurité relatives aux audits. Enfin, le groupe «attaque» doit faire de même pour les tests d'intrusion internes et externes.

Présentation thématique sur la conception de périmètres de services sécurisés.

Pour la partie travaux de groupes, cette séance marque la finalisation des «plans de bataille». Chacun doit avoir un rôle et des missions définies à l'issue de cette séance.

Séance 3L'importance de la journalisationLe filtrage et ses fonctionnalités aux différents niveaux de la modélisation OSI

Présentation thématique sur la journalisation système et réseau, ses modalités d'exploitation et ses limites. L'objectif pédagogique est de montrer que sans exploitation correcte de la journalisation, aucune mesure du niveau de sécurité n'est envisageable.

Présentation thématique sur le filtrage et les «possibilités» des couches liaison, réseau, transport et application. L'objectif pédagogique est de montrer que si certains exploits sont très complexes à mettre en œuvre, d'autres sont utilisables très|trop facilement.

Pour la partie travaux de groupes, le choix des outils de chaque groupe doit être arrêté et la maquette du système partiellement en place.

Séance 4

Début d'exploitation d'une version minimale du système d'information de l'agence Candide S.A.. Les rôles de chaque membre de chaque groupe sont définis ainsi qu'un planning prévisionnel. Chaque groupe désigne une cellule de communication avec les autres groupes. La première tâche importante de ces cellules de communication est de définir les dates de confrontation planifiées.

Autres Séances

Le contenu des autres séances est fonction des différents paliers de progression prévus par chaque groupe. Généralement, il est possible de réaliser trois confrontations au cours des séances en groupe. Suite à chacune de ces confrontations, des préconisations sont émises par le groupe «analyse». Ces préconisations, ainsi que les observations faites par les deux autres groupes doivent guider les évolutions et les corrections à apporter.

On peut assimiler cette démarche à trois tours de roue décrivant le cycle : Plan, Do, Check, Act.

6. Évaluation

Chaque groupe doit remettre un rapport écrit et faire une présentation orale lors de la dernière séance.

Le ***rapport écrit*** doit avoir la forme d'un compte rendu d'audit détaillant les missions confiées à chacun des membres du groupe, les résultats obtenus et faire une synthèse critique sur l'ensemble de la réalisation. Il comprend donc obligatoirement les éléments suivants :

Une introduction avec :

Une présentation des objectifs que le groupe s'est fixé relativement aux «contraintes» fixées par le présent document. Une présentation du plan retenu et des buts à atteindre pour la synthèse finale.

Une partie «distribution des (tâches|rôles)» avec :

Une distribution des tâches en fonctions des objectifs définis dans l'introduction. Dans cette distribution doivent apparaître : les affectations des membres du groupe, le volume horaire consacré, le positionnement des tâches dans le planning ainsi que des précisions sur les tâches qui ont donné lieu à une exploitation (ou non).

Un tableau de synthèse des échéanciers avec :

Une mise en évidence des différences entre l'échéancier prévisionnel et l'échéancier effectivement suivi. Pour chaque (différence|décalage) on trouvera un (renvoi|lien) vers l'explication correspondante dans les parties suivantes.

Une partie (Politique de sécurité|Audit) avec :

Une présentation des principales observations réalisées et des préconisations correspondantes. Le Groupe «défense» présente dans cette partie les politiques de sécurité relatives au déploiement des équipements et des services de la «maquette» du système d'information. Le Groupe «analyse» présente dans cette partie le rapport d'audit sur les observations des échanges entre les réseaux de la «maquette». Enfin, le Groupe «attaque» présente le rapport d'audit sur les tests de pénétration et d'intrusion du système d'information. Chaque groupe doit faire apparaître ses préconisations pour un fonctionnement plus sûr et plus sécurisé du système d'information étudié.

Une partie «tâches et réalisations» avec :

Une présentation détaillée des tâches réalisées par les différents membres du groupe. Pour chacune des tâches réalisées on précisera :

- Quels sont les objectifs particuliers à cette tâche ?
- Qui à participé ?
- Comment cette tâche se positionne dans l'échéancier ?
- Quels sont les (outils|moyens) utilisés ?
- Quels sont les résultats obtenus ?

Dans le cas où un travail n'a pas donné lieu à une exploitation sur la maquette, on précisera pourquoi et surtout quelles sont les préconisations pour qu'une exploitation puisse avoir lieu.

Une partie bilan avec :

Une synthèse sur l'ensemble du projet présentant les points positifs et négatifs ainsi que des préconisations pour l'améliorer. Toutes les propositions sont les bienvenues !

La ***présentation orale*** doit permettre aux membres des autres groupes de comprendre le cheminement suivi pour les différentes actions entreprises. Elle doit aussi faire la synthèse sur les difficultés rencontrées et les pistes d'améliorations possibles pour le projet. Les modalités d'organisation sont les suivantes :

Une présentation par groupe de 1 heure 20 minutes maximum

Il ne s'agit pas de reprendre le rapport écrit mais d'extraire les faits marquants du déroulement du projet. Il ne faut retenir que les points techniques représentatifs de la démarche suivie. Il faut aussi insister sur les aspects métier et prendre position en argumentant sur les choix et les préconisations faites par le groupe.

Ordre de passage

L'ordre de passage pour les présentations est : «Défense», «Analyse» et «Attaque».

Un débat entre les trois groupes

Chaque groupe doit pouvoir répondre aux questions des deux autres sur les choix effectués et leurs justifications. Chaque groupe doit aussi proposer des pistes d'améliorations pour les sessions à venir.

Les documents doivent être rendus au format PDF aussi bien pour le rapport écrit que pour les vues de la soutenance orale.