Avertissement

Le contenu de cet enseignement est à visée strictement pédagogique. Toute personne (étudiante ou non) exploitant son contenu hors du cadre qu'il définit s'expose à rendre des comptes devant des instances universitaires voire juridiques ! ! !

M4101C - Administration Systèmes et Réseaux (ex-Sécurité)

Focus sur Matériels, Données, Systèmes, Réseaux, (et moins sur les applications et les personnes)

Nicolas Hernandez

Cours de DUT informatique – 2ème année
IUT de Nantes – Département Informatique
https://sites.google.com/site/nicolashernandez

21 janvier 2021

Organisation du module

- **Volume horaire**
  - 4 CM d'1H20 et 7 * 2 * 1H20 TD/TP sur 7 semaines
- **Modalité de validation du module** : à préciser type, date et durée
  - 1 note de TD coeff. 1
  - 1 note de DS coeff. 1
- **Equipe pédagogique**
  - CM : Nicolas Hernandez
  - TD : Erwann Helleu*2, Johann Scourzic, et moi-même

Objectifs du module

- **Sensibilisation aux problèmes de sécurité**
- **Outils et techniques pour sécuriser (attaquer) un système d'information**
- **Mise en place d'une architecture réseau sécurisée pour une petite entreprise**

Contexte du module

- Philippe Rannou (1ère et 2ème année) : Mathématique pour la cryptographie
- S. Cazalas et D. Kueviakoe (2ème année) : Informatique et société (aspects juridiques)
- N. Hernandez (1ère année) : Interconnexion des réseaux
- J-F Remm (2ème année) : Services applicatifs des réseaux

Quelles ressources sécuriser ?

Les ressources sensibles / critiques d'une entreprise

- **Matériels** (serveur de calcul, disques, équipements d'interconnexion, imprimantes, etc.)
- **Données** (savoir-faire/carnet de clients de l'entreprise, bases de données, sauvegardes, etc.)
- **Systèmes** (l'exploitation des matériels)
- **Réseaux** (l'échange des données)
- **Applications** (sources des programmes, services démons (DNS, FTP,...), applications web, etc.)
- **Personnes** (salariés, personnel en régie (chez le client), etc.)

Quelles garanties assurer ?

Principalement

- **Disponibilité** garantie l'accès et l'utilisation à des ressources (services, bande passante, données) de manière continue et non altérée (test de montée en charge, sauvegarde)
- **Intégrité** garantie qu'une ressource (données, applications, materiels...) n'a pas été modifiée, altérée ou détruite (transfert sécurisé)
- **Confidentialité** permet de garder privée des (échanges de) données (contrôle d'accès, chiffrement)

Quelles garanties assurer ?

En lien avec la confidentialité et le chiffrement

- **Authentification** valide l'identité prétendue (password)
- **Non-répudiation** garantie qu'un message a bien été envoyé par un émetteur authentifié
- **Traçabilité** permet de retrouver les opérations réalisées sur les ressources (journaux/logs)

Organisme et réglementation

Pour aider à élaborer une politique de sécurité :

- **ANSSI** (Agence nationale de la sécurité des systèmes d'information) Prévention, protection, réaction, formation et labellisation de solutions et de services pour la sécurité numérique de la Nation (créée en 2009) `www.ssi.gouv.fr`
- CNIL (Commission nationale de l'informatique et des libertés) cadre le traitement informatique des données à caractère personnel Missions d'informer, réguler, protéger, contrôler, sanctionner et anticiper avec des droits d'information, d'accès, de rectification/radiation, d'opposition pour les personnes
- La RGPD (Règlement général sur la protection des données personnelles) est le règlement no 2016/679 de l'Union européenne

Dispositions légales nationales

Le chapitre III du Code pénal traite des atteintes aux Systèmes de Traitement Automatisé de Données (STAD)

- L'article 323-1 condamne le fait d'accéder et se maintenir frauduleusement, c'est-à-dire sans droits, dans un système. Les peines vont jusqu'à 3 ans de prison et 45 000 E d'amende
- L'article 323-2 sanctionne le fait d'entraver ou de fausser le fonctionnement d'un STAD de 5 ans de prison et de 75 000 E d'amende
- L'article 323-3 condamne le fait d'introduire frauduleusement des données ou supprimer ou modifier frauduleusement des données. Le délit est puni de 5 ans de prison et 75 000 E d'amende.
- L'article 323-3-1 condamne le fait de détenir ou d'offrir des moyens permettant les délits cités dans les articles 323-1 à 323-3 et sanctionne de la même manière que les délits
- Les articles 323-4 à 323-7 sanctionnent la préparation des délits, l'intention, prévoient des peines complémentaires telles qu'interdiction des droits civiques, civils, de famille, d'exercer dans la fonction publique, la fermeture des établissements ayant servi à commettre les faits, des sanctions pour les personnes morales.

Sources d'information

Pour l'administrateur comme le pirate...

- **cyberedu** matériel pédagogique de l'ANSSI pour les formations en SSI `https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/`
- **CERT** (Computer Emergency Response Team) centres d'alerte et de réaction aux attaques informatiques `www.certa.ssi.gouv.fr`
- **OSSIR** (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux) `www.ossir.org`
- **Outils** (pass crackers, sniffers, vuln. scanners, vuln. exploitation, web scanners, wireless, packet crafting, etc.) `sectools.org`
- **Mailing lists** `seclists.org`
- **Bugtraq** (mailing list de failles, d'exploits) `www.securityfocus.com/archive`, `insecure.org/sploits.html`

Ouvrages réseaux

C. Servin,
Réseaux et Télécoms, Dunod, 2003 et 2009
CDI ; une référence ; exercices avec corrigés

G. Pujolle
Initiation aux réseaux, Eyrolles, 2002 et Edition 2011
CDI ; une référence mais parfois trop technique

A. Tannenbaum,
Réseaux - Architectures, protocoles, applications, InterEditions, 1996 (3ieme édition)et 2004 (4eme ed.)
CDI ; une référence ; exercices avec corrigés dans le 2004

J. Dordoigne,
Les réseaux : entraînez-vous à l'administration d'un réseau,
Contenu très pratique accessible à un étudiant DUT Eni, 2008

Ouvrages en sécurité

C. Llorrens et al.,
Tableaux de bord de la sécurité réseau, 2ème édition, Eyrolles, 2006
CDI ; bonne couverture ; attaques, contrôles/protections ; orienté pratique

B. Schneier
Debian GNU-Linux : sécurité du système, sécurité des données, pare-feu, chiffrement, authentification.., ENI 2008
CDI ; Contenu très pratique accessible à un étudiant DUT

G. Avoine, P. Junod, P. Oechslin, R. Longeon
Sécurité informatique : Exercices corrigés, Vuibert 2004 et 2009
Cours en ligne de *Christian Bulfone* `http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/IC2A-DCISS/`
Et de Abdou Guermouche
`http://dept-info.labri.u-bordeaux.fr/~guermouc/SR/`


S. Ghernaouti-Hélie,
Sécurité informatique et réseaux, Cours et exercices corrigés, Licence 3e année, master, écoles d'ingénieurs,
Dunod, 2006
CDI ; général ; 50% aspect managériale et 50% technologique ; théorique


B. Schneier
Cryptographie appliquée, Algorithme, Protocole et Code source en C,
Vuibert, 2ème édition, 2001
CDI


McClure et al.,
Hacking Exposed 5th Edition, Network Security Secrets & Solutions,
Mc Graw Hill/Osborne, 2005
comment hacker ; listes de vulnérabilités et de leurs contre-mesures des systèmes (unix, windows), des réseaux et des logiciels ; orienté pratique
MISC www.miscmag.com