



Discipline(s) : Informatique et télécommunications

SECURITY SUPERVISION

Semestre	Semestre 1
Nature	UE

RESPONSABLES

Valérie Viet Triem Tong

OBJECTIFS

DESCRIPTION

Dans ce module, nous étudions les principes de sécurité d'un système : machine, réseau et système distribué. Ce module débute par la présentation des politiques de sécurité classiques: contrôle d'accès discrétionnaire, obligatoire, contrôle de flux d'information (modèles de Biba, Bell et La Padula), approches par rôles. Nous montrons ensuite comment surveiller un système pour le protéger lors d'attaques informatiques. Cela nous amène à étudier la structure d'un IDS et les principes de la corrélation d'alerte. Ensuite nous étudierons des approches moins classiques et plus expérimentales.

MOTS-CLÉS

Politiques de sécurité: spécification, mise en place. Détection d'intrusion, IDS, corrélation d'alertes, approches par suivi de flux d'information

PRÉREQUIS

Aucun

CONTENU

- Politique de sécurité Dac, Lbac Rbac, contrôle de flux et contrôle d'usage
- Détection d'intrusion Hids, Nids, Siem
- Flux d'information pour la détection d'intrusion
- Détection d'erreurs
- Corrélation et génération de règles de corrélation
- Détection d'intrusions dans les systèmes distribués

COMPÉTENCES ACQUISES

Comprendre les enjeux de supervision de sécurité, connaître les approches classiques en détection d'intrusion approches comportementales, approches par signature. Corrélation d'alertes. Savoir évaluer un IDS. Savoir proposer une infrastructure de sécurité.

APPARTIENT À

Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

CONTACT(S)

Département Informatique et télécommunications

École normale supérieure de Rennes Campus de Ker Lann Avenue Robert Schuman

35170 BRUZ

Tél. : 02 99 05 52 43

[E-mail](#)

[Site Internet](#)