INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

INSA Campus LyonTech - 6 avenue des arts
Batiment Claude Chappe - 69621 VILLEURBANNE

Ingénierie de la sécurité des systèmes d'information

Sécurité des infrastructures et protection périmètrique

IDENTIFICATION

CODE : MS-CYNU-SINF
ECTS : 2.0

HORAIRES

Cours :	7.0 h
TD :	8.0 h
TP :	6.0 h
Projet :	0.0 h
Face à face pédagogique :	21.0 h
Travail personnel :	15.0 h
Total :	36.0 h

ÉVALUATION

Examen. Etude de cas. Participation

SUPPORTS PÉDAGOGIQUES

LANGUE D'ENSEIGNEMENT

Français

CONTACT

M. IDRISSI BELKASMI Mohammed
khalid.idrissi@insa-lyon.fr
M. ROBERT Christophe
christophe.robert@insa-lyon.fr

OBJECTIFS RECHERCHÉS PAR CET ENSEIGNEMENT

Comprendre les mécanismes pour mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux.
Après avoir défini quelques concepts de sécurité et étudié quelques menaces pesant sur le système d'information, nous apprendrons le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en œuvre.
Le cours fera aussi l¿objet de la présentation des évolutions des concepts sur l¿architecture de sécurité notamment en présentant la protection en profondeur ainsi les concepts de prévention d¿intrusion, contrôle d¿accès, d¿analyse de comportement, filtrage applicatif, authentification ...

PROGRAMME

Introduction et Définition des concepts
Notions Risques et Menaces :
Architectures de sécurité :
o Plan d'adressage sécurisé, le RFC 1918
o Des firewalls simples vers les Appliances
Sécurité des données :
o Authentification
o Cryptographie symétrique/asymétrique
Logiciels malveillants :
o Virus/backdoor/ransomware/
o Méthodes de propagation
Sécurité des échanges : VPN et Protocoles chiffrés
Prévention et Détection des intrusions
Problématiques d¿authentification : password, SSO, OTP, ¿
Hardening
Travaux Pratiques :
o Découvrir quelques commandes Linux/Windows
o Découvrir un analyseur de trafic réseau (Wireshark),
o Analyser le fonctionnement de SSH,
o Cracker un mot de passe sous Windows,
o Collision MD5,
o Mettre en place un tunnel VPN IPSec (Windows 2016),
o Hardening: configuration des paramètres de comptes, protection de protocole faibles à travers un tunnel IPSec sous Windows, paramétrage des paramètres d¿audit système, ¿
o Tester l¿application PSI Secunia (Windows)
o Tester l¿application Open Scap (Linux)
o Tester l¿outil Nmap,
o Usurper une adresse IP avec hping3,
o Filtrer un flux avec IPTables,
o Mettre en place du NAT avec IPTables,
o Installer un serveur Proxy (Squid)