



CONTENU DU COURS « SECURITE - ETAT DE L'ART »

Chapitre 1 : Présentation générale de la sécurité informatique

- Pourquoi un cours sur la sécurité ?
- Le problème de la confiance
- Quels sont les risques ?
- Que faut-il protéger ?
- Les risques de l'interconnexion
- Intrusion
- Vol d'information
- Les victimes

Chapitre 2 : Sécurité Humaine

- Qu'est ce qu'un hacker ?
- Qui sont les pirates informatiques
- Les Black Hat Hackers
- Ingénierie Sociale
- Présentation de MPack

Chapitre 3 : Sécurité Physique

- Contrôle d'accès physique en France
- Sécurité physique des équipements
- Statistique sur les vols d'ordinateur
- Les systèmes d'authentification (mot de passe, biométrie, carte d'accès)

Chapitre 4 : Sécurité système d'exploitation

- WindowsNT/2000
- Windows XP
- Windows 2003 Server et Windows 2008 Server
- Windows Vista et Windows 7
- Unix / Linux
- Macintosh
- Cas d'un réseau informatique hétérogène
- Virtualisation
- Sécurité des postes utilisateurs

Chapitre 5 : Sécurité réseaux

- Hubs/Switchs
- Routeurs
- Modems
- Serveurs d'accès
- Comparaison des techniques d'interconnexion

- Autres périphériques d'interconnexion

Chapitre 6 : Protocoles réseaux

- TCP/IP
- Problèmes liés à IP
- Problèmes liés à TCP
- NAT
- DNS
- DHCP
- IPv6

Chapitre 7 : Sécurisation des flux réseaux

- Pare-feu/Firewall
- Les UTMs
- Critères de sélection d'un firewall
- Les serveurs mandataires (proxy)
- IDS/IPS

Chapitre 8 : Wifi

- Risques liés aux réseaux sans fil
- Principes du WEP
- Principes du WPA et WPA2
- Sécurité WIMAX

Chapitre 9 : Chiffrement

- Cryptographie
- Cryptanalyse
- Algorithmes de chiffrement symétrique (DES, AES,...)
- Algorithmes de chiffrement asymétrique (RSA, DSA)
- Algorithme Diffie-Hellman
- Les fonctions de hachage (MD5, SHA1)
- PGP

Chapitre 10 : Certificats

- Protocole X.509
- Types de certificats
- Les Autorités de Certification
- Infrastructures de clés publiques (ICP/PKI)
- Les modèles des tiers de confiance

Chapitre 11 : VPN

- Présentation sur les Réseaux Privés virtuels (RPV ou VPN)
- PPP
- PPTP
- L2TP
- MPLS
- IPSec
- VPN SSL

- SSH

Chapitre 12 : Gestion des logs

- Présentation du protocole Syslog
- Le logiciel Syslogd
- Le logiciel Kiwi
- Les problématiques
- Présentation du SIEM et de Net Report

Chapitre 13 : Web

- Le protocole HTTP
- Le protocole SSL
- Filtrage des éléments actifs du Web
- Serveurs web du marché
- Sécurités des navigateurs Internet

Chapitre 14 : Messagerie

- Protocole SMTP
- Protocole POP3
- Protocole IMAP
- S/MIME
- Fonctionnalités de sécurité des serveurs de messagerie
- Les techniques d'Anti-Spam (Domainkeys, filtrage bayésien, honeypots,...)

Chapitre 15 : Anti-virus

- Virus/Vers
- Méthodes de Protection
- Cheval de Troie
- Spyware
- Produits anti-virus (personnel, réseau,..)

Chapitre 16 : SMSI

- ISO 27000
- Le modèle PDCA
- ISO27002 : guide des bonnes pratiques
- Norme MEHARI
- Comparaison entre MEHARI et les normes ISO

Chapitre 17 : Nmap

- Présentation de Nmap
- Quelques options disponibles de Nmap

Chapitre 18 : Nessus

- Présentation de Nessus
- Fonctionnement
- Installation, configuration de Nessus
- Génération des Rapports

Chapitre 19 : Exploitation des failles

- Exercices sur les pré-requis d'une attaque
- Détection des vulnérabilités sur le réseau
- Les attaques de mot de passe (John the ripper, RainbowCrack)

Chapitre 20 : Metasploit

- Mise en oeuvre d'une attaque
- Détection des vulnérabilités
- Exploitation d'une des failles de la machine
- Avoir un accès RDP sur la machine