

Programme Séminaire Sécurité des systèmes d'information

Jour 1

Matin : la sécurité des SI

A : Introduction : généralités sur la sécurité des SI

- Quels sont les risques et les conséquences (pertes de données / destruction de données / indisponibilité / vol de données)
- Les formes d'atteintes numériques (intrusion / logiciels malicieux : virus – spyware adwares)
- Les formes d'atteintes extérieures et non numériques

Discussion

B : Ingénierie sociale vs Attaques numériques

- Deux grandes familles d'attaques par failles « humaines » ou « numériques »
- Principe de la vulnérabilité « humaine »
- Principe de la vulnérabilité logicielle
- Principe de la vulnérabilité matérielle

Discussion

C : Conséquences économiques et juridiques de la sécurité des SI

Discussion

Après midi : Vulnérabilité du réseau

A : La sécurité d'un réseau

- Vulnérabilités matérielles
- Vulnérabilités systèmes et logicielles (IP/ applications/mots de passe)
- Problématique particulière du sans fil

Discussion

B : Expériences pratiques sur réseau (2h) (TP)

Attaques :

Démonstration d'attaque par force brute (Brutus)
Analyse de trafic réseau (Pcap)
Atteintes à un réseau wi-fi
Scanning et recherche de failles (Analyser)
Défenses :
Détection d'intrusion et protection (Firewall / anti spywares et malwares)
Protection des accès (notions de complexité des clés – génération de mots de passe)
Prévention des failles (mises à jour logicielles)
Protection du réseau sans fil (bonne configuration)

Jour 2

Matin : Planifier la sécurité des SI

A : La sécurité physique du poste fixe
Prévention de l'intrusion (protections par mots de passe / Bios / Sessions / données)
Sauvegarde et configuration (en vue d'un PRA)

B : La sécurité physique des SI et les événements extérieurs non numériques
Catastrophes naturelles
Pannes matérielles
Incendies
Pannes électriques
Etc ...

C : Plan de sauvegarde et de retour à l'activité
Prévenir les pertes de données
Prévoir le retour à l'activité
Les normes de plans de sécurité (PSI / PRA / etc)

Discussion

Après midi : La sécurité des informations et contenus

A : Intrusion et sécurité des données

Vol d'information
Bonnes utilisation des protections
Principes des tunnels sécurisés
Théorie du cryptage
Vulnérabilité des plateformes web et de leurs document

Cryptage et décryptage : bonnes pratiques
Possibilité de sécurisation de contenus et de documents
Possibilités de décryptage de documents

B : Utilisation des outils de cryptage-décryptage (2h) (TP)