PIRATAGE ET INTRUSION DES SI, APPROCHE ÉTHIQUE

OBJECTIFS
L'ouverture du système d'information, la guerre économique, expose les entreprises au piratage avec des failles de plus en plus techniques.

Vous étudierez la démarche de ces pirates, leur méthodologie ainsi que les outils qu'ils utilisent. Ainsi vous serez sensibilisé aux faiblesses de votre Système d'information et vous serez à même de mettre en place les parades pour en réduire les vulnérabilités.

PARTICIPANTS
Ingénieurs/Techniciens/ Administrateurs système et réseau.

PRE-REQUIS
Connaissance des réseaux, des bases du chiffrement et du filtrage pour les personnes impliquées dans la SSI : RSSI

RÉF
VEP

DURÉE
4 Jours

PRIX
1800€ HT

CONTENU :

- **INTRODUCTION**
  - Les objectifs du cours
  - Le système d'information et ses menaces
  - La démarche sécurité
  - L'aspect « politique »
    - Méthodologie, organisation, procédure, suivi
  - L'aspect « technique »
    - La sécurité physique, la sécurité logique
  - L'aspect juridique
    - Les lois du monde numérique, exemples de jurisprudence
  - Le monde du piratage
    - Le profil des attaquants, le profil des victimes
- **LA METHODOLOGIE D'ATTAQUE**
  - Les étapes d'une intrusion
    - Le repérage, la recherche des attaques réalisables
    - La planification, la réalisation, l'effacement des traces
- **L'EXPLOITATION D'ATTAQUE**
  - La collecte d'informations sur la cible
    - Le facteur humain et l'obtention d'informations
    - La recherche d'information sur Internet
    - L'utilisation de moteurs de recherche
    - L'analyse de mail, les bases whois
- **LE NIVEAU RESEAU**
  - Les accès aux composants du réseau
  - Telnet, le vol de mot de passe, injection de commandes
  - ssh (scp sftp)
    - Attaque de mot de passe et de type « homme du milieu »
  - Les switch
    - Atteinte à la disponibilité (découverte, SNMP)
  - L'écoute du trafic par attaque du switch
    - L'attaque de la table mac
    - L'écoute du trafic par empoisonnement des caches arp
    - Les « sauts » de vlan
  - Les routeurs
    - Atteinte à la disponibilité
    - L'empoisonnement de la table de routage
  - Le point d'accès wifi
    - L'atteinte à la disponibilité : Attaque du serveur DHCP Brouillage de fréquences
    - La cartographie de point d'accès
    - Le crack de clés WEP selon plusieurs méthodes
  - Le PABX et la VOIP / TOIP
    - Les risques liés aux autocommutateurs non sécurisés
    - L'écoute téléphonique :

PIRATAGE ET INTRUSION DES SI, APPROCHE ÉTHIQUE *(SUITE)*

CONTENU :

- **LE NIVEAU DU SYSTEME ET DES APPLICATIONS**

Le piratage du système d'exploitation :

- Le BIOS
  - Accès à la machine, avec mot de passe
  - Les particularités des systèmes d'exploitation
  - Microsoft Windows / Unix / Linux
  - La casse de mot de passe
  - Les attaques non connectées
- Les attaques par capture du trafic réseau
- L'exécution d'applications à distance :
- Les méthodes utilisées
- Le vol d'information
- La récupération de fichiers effacés
- L'élévation de privilège
- Les « rootkit »
- Les supports externes : clés usb, pda, …
- Récupération d'informations par la saisie automatique

Les chevaux de Troie et les portes dérobées

- Cas pratiques et exemples
- L'introduction d'un cheval de Troie dans le SI
- L'atteinte à la confidentialité, la disponibilité et l'intégrité

Les atteintes à la disponibilité

- Les classiques
- Saturations par requêtes « get », par « seg-syn »
- L'utilisation des bugs
- Envois de paquet provocant des disfonctionnements

Les vulnérabilités des applications web

- Les vulnérabilités côté serveurs
- Serveur apache, serveur IIS
- L'utilisation de l'unicode
- Les attaques côté serveur
- Les attaques par injection de code :
- SQL, PHP
- Les attaques côté client
- Mot de passe de comptes utilisateur sur les sites web
- Exécution de script, contrôle activeX, applet java nuisibles
- Le hameçonnage
- L'usurpation de session web

Les vulnérabilités de la messagerie

- Les atteintes à la disponibilité
- Réception de message mail administrateur
- Les vols via le réseau
- Les comptes de messagerie, les pièces jointes
- Exécution de code malveillant, les virus et les vers
- L'introduction d'un vers et/ou d'un virus dans le SI
- Atteinte à la confidentialité, disponibilité, intégrité

- **LE CONTOURNEMENT D'OUTILS DE SECURITE**
  - Coupe-feu, système d'IDS, pot de miel
  - Contournement d'antivirus, L'effacement des logs
- **SYNTHESE**
  - La gestion des mises à jour
  - La veille technologique
  - Les liens web utiles pour la sécurité :
    - Les nouveaux outils
    - Les nouvelles failles
- **GLOSSAIRE**