NIMBUS TRAINING
La formation NTIC • Tél : 02-40-85-19-32 • cedric.tron@nimbus-training.fr

La sécurité Wireless

Déscription :

Ce séminaire vous apprendra le fonctionnement des différents protocoles de sécurité proposés par les bornes sans fils classiques afin de choisir de manière optimale ceux qui conviendront pour assurer une utilisation sécurisée des technologies réseaux sans fils.

Des laboratoires permettront de se rendre compte de la faiblesse de certaine solution de sécurité et de la pérennité des autres

Objectifs

- Introduction
- Sécuriser l'administration des équipements réseaux sans fils
- Administration en mode caractère
- Sécuriser les accès clients
- Outils de hacking et faiblesse de la clé WEP
- Méthodes 802.1X
- Standards de sécurité pour les réseaux sans fils
- Gestion de la sécurité d'un réseau sans fils d'entreprise
- Sécurité supplémentaire par administration centralisée

Publics

A tous les administrateurs réseaux et tous les responsables sécurités en charge d'une architecture possédant des points d'accès sans fil ou des PC équipés de cartes sans-fil.

Durée

2 jours

Pré-requis

Avoir une bonne connaissance des principes de fonctionnement des réseaux sans fils. La connaissance du protocole TCP/IP.

Programme de cette formation

Introduction

- Rappels sur les réseaux sans fils
- Le SSID
- Les Vlans

Sécuriser l'administration des équipements réseaux sans fils

- Administration par SNMP
- Le protocole SNMP
- SNMP V1 et V2
- SNMP V3
- Administration par page Web
- http
- https

Administration en mode caractère

- telnet
- SSH

Sécuriser les accès clients

- Introduction
- Authentification
- Association

Problématique de la sécurité des réseaux sans fils

- Méthodes par défaut
- SSID
- Authentification ouverte
- Authentification partagée
- Clé WEP

Outils de hacking et faiblesse de la clé WEP

- Airsnort
- John the ripper, etc…
- Technique de hacking
- Attaque passive et active
- Attaque weak IV
- Attaque par dictionnaire
- Attaque type bit flip
- Attaque type IV replay

Méthodes 802.1X

- EAP Fast
- PEAP
- EAP TLS
- Quelle méthodes 802.1X choisir

Standards de sécurité pour les réseaux sans fils

- VPN IPSEC
- 802.11i
- WPA
- WPA 2
- TKIP et MIC
- Encryption AES

Gestion de la sécurité d'un réseau sans fils d'entreprise

- Problématique du vol d'équipement ou du départ d'un employé
- La gestion centralisée de la sécurité
- Intégration dans un domaine active directory
- Utilisation des comptes utilisateurs windows
- Utilisation de one time password (OTP)

- Le serveur AAA
- Gestion de la sécurité des bornes type Box
- Live box
- Free box
- Conseils de configuration

Sécurité supplémentaire par administration centralisée

- L’administration sans fils centralisée avec bornes légères
- L’administration centralisée avec bornes intelligentes
- Détection des bornes ennemies
- Détection d’une tentative de pénétration
- Centralisation des politiques de sécurité