



Sécurité Avancée WiFi

numéro de cours: TL-220

Durée: 2 jours

NET2S
INSTITUTE

Ce cours constitue une approche pratique de la sécurisation des réseaux locaux sans fil en entreprise et forme les stagiaires sur les risques réels en terme d'intrusions, d'écoutes ou de dénis de service. Des solutions types de sécurisation seront détaillées dans ce cours.

A qui s'adresse la formation:

Ce cours est destiné à des administrateurs réseaux, des chefs de projets, des consultants et des responsables sécurité amenés à travailler dans un environnement WiFi sécurisé.

Les stagiaires apprendront à:

- ▶ Comprendre et analyser la problématique de sécurité des réseaux locaux sans fil : confidentialité, intégrité des données, authenticité et disponibilité
- ▶ Sécuriser les réseaux sans fil afin de se défendre contre les attaques extérieures
- ▶ Chiffrer le trafic pour garantir la confidentialité et l'intégrité des données
- ▶ Protéger un réseau sans fil grâce aux dernières technologies WPA, WPA 2 (802.11i)
- ▶ Réaliser une authentification des clients par certificats avec les protocoles EAP-TLS, PEAP
- ▶ Mettre en place une infrastructure par Vlan

Tous les thèmes abordés font l'objet d'exercices pratiques spécifiquement conçus pour favoriser l'apprentissage. Les équipements utilisés dans ce cours reposent sur une solution CISCO AIRONET 1200. Cependant, pour des besoins spécifiques, il est possible de former les stagiaires sur d'autres produits (nous contacter).

Sujets abordés:

- ▶ Les risques émanant d'un réseau sans fil
- ▶ Les moyens techniques permettant d'assurer la confidentialité et l'intégrité des données grâce aux normes WEP, WPA, WPA 2 (802.11i)
- ▶ L'authentification des utilisateurs (LEAP, EAP-TLS, PEAP...)
- ▶ Problématique de la disponibilité des réseaux sans fil introduite par le déni de service
- ▶ Les principales architectures possibles pour interconnecter des équipements sans fil aux réseaux LAN de l'entreprise
- ▶ L'ensemble des failles des réseaux WiFi et les attaques engendrées par celles-ci
- ▶ Les solutions propriétaires Firewall, VPN (Virtual Private Network), Commutateurs et sondes IDS (Intrusion Detection System)

Pré-requis:

- ▶ Cours TL-210 (Administration des réseaux sans fil) sont nécessaires.

PREMIER JOUR

La technologie WiFi:

- ▶ Réseaux sans fil et standard IEEE 802.11
- ▶ Transmissions radio-électriques
- ▶ Réglementation française et internationale
- ▶ Équipements WiFi
- ▶ Topologie des réseaux 802.11
- ▶ Sécurité des réseaux locaux sans fil : disponibilité, confidentialité, intégrité des données et authenticité

Confidentialité et intégrité 802.11:

- ▶ Utilité du broadcast SSID
- ▶ Le WEP a-t'il un intérêt ?
- ▶ **New!** Exercice pratique : identifier les faiblesses du protocole WEP.
- ▶ WPA première réponse aux problèmes de sécurité WiFi
- ▶ **New!** Exercice pratique : mise en évidence des failles du protocole WPA-PSK au travers d'attaques par force brute ou par dictionnaire
- ▶ L'état de l'art actuel: WPA 2 / 802.11i

DEUXIEME JOUR

Méthodes d'authentification 802.11:

- ▶ Rappels : Radius, EAP
- ▶ L'apport du mécanismes 802.1x
- ▶ Authentification http, https
- ▶ Authentification par adresses MAC
- ▶ **New!** Exercice pratique : inefficacité du filtrage MAC
- ▶ Solutions propriétaires : LEAP, EAP-FAST
- ▶ **New!** Exercice pratique : analyser les défauts du protocole LEAP
- ▶ EAP-TLS, EAP-TTLS : authentification de haut niveau par certificat
- ▶ PEAP : sécurité et simplicité de déploiement
- ▶ Exercice pratique : mise en place et configuration d'une authentification et d'un chiffrement sécurisée WPA/PEAP

Disponibilité des réseaux WLAN:

- ▶ Peut on garantir un accès au service sans perturbation ?
- ▶ Déni de service
- ▶ Brouillage fréquence
- ▶ Attaques de type Flood
- ▶ Hijacking du client

Architectures sécurisées des WLAN:

- ▶ Firewall
- ▶ NAT
- ▶ VPN
- ▶ VLAN
- ▶ **New!** Exercice pratique : sécurisation d'un réseau par cloisonnement des utilisateurs WiFi dans des VLAN

Supervision et gestion centralisée de la sécurité:

- ▶ Les outils de supervision
- ▶ Commutateurs WiFi
- ▶ Sondes IDS