



## FORMATION EXPERTISE : DÉTECTER ET BLOQUER LES FRAUDES VoIP

### OBJECTIFS

Cette formation technique vous donnera les clefs de compréhension technologique pour lutter contre la Fraude VoIP. Une bonne connaissance de l'architecture et des réseaux NGN/VoIP est indispensable.

Cette formation vous permettra de :

- identifier les différents cas de Fraude VoIP.
- décrire les différentes méthodes utilisées par les hackers / fraudeur pour identifier des réseaux VoIP et détecter des équipements mal sécurisés.
- décrire les méthodes d'exploitation de ces failles de sécurité.
- décrire les méthodes de détection des fraudes VoIP et les moyens de protéger son réseau.

### MÉTHODE

Les exposés théoriques sont illustrés d'exemples concrets, de représentations schématiques. De nombreux exercices pratiques sur machines permettent l'apprentissage pratique des parades. Tout au long de la formation, du temps sera consacré aux exercices et aux questions permettra d'intégrer les notions de base et de les manipuler en groupe.

L'atteinte des objectifs est contrôlée au fur et à mesure du stage.

### PERSONNES CONCERNÉES, PRÉREQUIS

Cette formation technique expert s'adresse à une population technique : responsables des SI en charge de la téléphonie, administrateurs, techniciens et ingénieurs en charge de plateforme PABX / IPBX, SSII, opérateur télécom, FAI proposant des services de VoIP. Ce module de spécialisation constitue la continuité du module Approfondissement VoIP.

### DUREE

Cette formation d'une journée est dispensée en langue française en intra entreprise pour 3 à 10 participants.

### Introduction

- les différents types d'atteinte à la sécurité d'un réseau VoIP
  - interruption de service / nuisances
  - capture de trafic / écoutes
  - falsification d'identité
  - accès non autorisé
  - fraude avec bénéfice financier

### Cas de fraude VoIP

- comprendre pour bloquer les appels gratuits ou à moindre coût vers l'international
- comprendre pour bloquer les appels en masse vers des numéros 08xx à haut revenue
- comprendre pour bloquer la revente à moindre coût de trafic VoIP

### Méthodes d'identification de cible

- présentation des différentes méthodes d'identification de cibles
- recherches d'équipements de constructeurs spécifiques
- recherches de réseaux VoIP mal sécurisés
- recherches des postes fixes VoIP mal sécurisés

### Contre l'exploitation / configuration de la fraude VoIP

- corriger l'exploitation de mauvaises configurations des équipements
- corriger l'exploitation de failles logicielles connues
- corriger l'exploitation d'accès au réseau VoIP faiblement configuré

### Méthodes de détection des fraudes et protections d'un réseau VoIP

- méthodes de détections des fraudes
- révision de la configuration des équipements VoIP
- pallier aux failles logicielles
- durcir l'accès aux équipements VoIP

### Exercices pratiques

- solutions pour contre la prise en main d'un IPBX mal configuré
- comment contre l'utilisation d'un IPBX pour mettre en place une fraude
- détecter une fraude dans l'IPBX et vérifier/corriger la configuration de l'IPBX
- vérifier après durcissement de configuration que l'IPBX est mieux protégé