IPT009
SÉCURITÉ EN TOIP

Informations

- **Réf :** IPT009
- **Durée :** 2 jours
- **Prix :** 1 090 € HT
- **Dates :**
  - 27 au 28 novembre 2014
  - 09 au 10 mars 2015
- **Horaires :**

9h15 - 12h30 / 13h30 - 17h30

Participants

Les ingénieurs, chefs de projet ToIP, techniciens et responsables techniques chargés de la gestion opérationnelle des réseaux de l'entreprise

Pré-requis

- Expérience télécoms & réseaux

Travaux Pratiques (Exercices et Ateliers)

La mise à disposition de notre réseau de données et de serveurs de mail, web, DHCP, DNS, LDAP pendant toute la formation (Switch, RouterSwitch, Router Adsl, Router RNIS, Firewall, Router VPN).

Elle permet à travers différents cas d'intégration de simuler des cas concrets clients sur une infrastructure Cisco.

Echantillon d'équipements présents sur la maquette de travaux pratiques :

- Aastra
- Alcatel-Lucent
- Asterisk
- Avaya
- Cisco
- HP
- LG Ericsson
- PowerDsine

OBJECTIFS

- **Comprendre les différentes problématiques de la sécurité en téléphonie sur IP : les risques propres aux protocoles de la ToIP, les risques générés par l'intégration de la ToIP au SI**
- **Appréhender les solutions en terme de protocoles, de matériels et d'éléments de configuration sur des architectures de type entreprise et opérateur**
- **La démonstration s'appuiera sur une architecture de type entreprise multi-sites**

PROGRAMME

LA PROBLÉMATIQUE

- **Rappels sur la sécurité :**
  - Authentification, contrôle d'accès, intégrité, confidentialité, non répudiation, disponibilité
- **Risques issus du système d'information :**
  - Flooding, Spoofing, déni de service, virus
- **Nouveaux risques :**
  - Usurpation d'identité, appels illicites, écoute clandestine, interruption d'appel
- **Identification des faiblesses des protocoles de signalisation et de média**
- **Moyens mis à disposition pour tester la sécurité de son système (scanner, snier, cracker, spoofer) :**

LES SOLUTIONS : LA THÉORIE

- **Différentes normes de sécurisation :**
  - Normes ToIP (SIP, H235, SRTP)
  - Normes réseau (TLS, IPSec) SSC
- **Elément de sécurisation d'un système d'information :**
  - Firewall, VPN, IDS / IPS, NAT, VLAN, DHCP
- **Elément de qualification des performances d'une infrastructure ToIP sécurisée :**
  - Sécurité vs. Performance : Qualité, Délai,Gigue …
  - Outils de tests

LES SOLUTIONS : LA PRATIQUE

- **Solution entreprise vs solution Centrex :**
  - Présentation des deux architectures
  - Accès à l'infrastructure de communication (attachement au réseau, enregistrement, authentification)
  - Coeur de l'infrastructure (authentification mutuelle des équipements de routage et de traitement, domaine de conance)
  - Services associés (mobilité des abonnés, messagerie unifiée)
- **Eléments de sécurisation mis en place par les constructeurs :**
  - Protocoles propriétaires (authentification et signalisation)
  - Modules de chiffrement externe

ILLUSTRATIONS & DÉMONSTRATIONS

- **Présentation de l'architecture de tests : entreprise multi-sites**
- **Attaques ToIP s'appuyant sur des attaques SI déjà connues (écoute clandestine, interruption d'appel, dégradation d'une communication, usurpation d'identité)**
- **Présentation d'un IPBX Open source, Asterisk ou SER, avec mise en oeuvre des normes ToIP Sécurisées**
- **A partir de la démonstration faite en première partie, reprendre les éléments qui composent - la PFS et définir la stratégie de défense à adopter pour contrer les principales attaques**