SÉCURISER VOTRE ARCHITECTURE VOIP

OBJECTIFS
Ce stage très pratique et technique vous montrera comment sécuriser des réseaux Voix sur IP. À l'issue de cette formation, vous saurez vous prémunir efficacement contre les différents risques encourus, les participants sauront définir une stratégie de sécurité, sécuriser les réseaux de transport de la voix et maintenir un niveau de sécurité optimum.

PARTICIPANTS
Toute personne soucieuse de connaître les risques et les parades liées aux attaques des architectures VOIP

PRÉ-REQUIS
Les participants doivent avoir de bonnes bases sur TCP/IP et des notions de Téléphonie et de VOIP

TRAVAUX PRATIQUES
- Parades aux écoutes de communications, de codes DTMF
- Parades au FLOODING (déni de service), aux usurpations d'identité

RÉF
SAV

DURÉE
2 Jours

PRIX
900€ HT

CONTENU :

INTRODUCTION VOIP ET SÉCURITÉ
- Qu'est ce que la convergence ?
- Impact de la VOIP sur la sécurité de l'entreprise
- Le modèle DICT *(Disponibilité, Intégrité, Confidentialité et Traçabilité)*

RAPPELS TECHNIQUES SUR LA VOIP
- Protocoles et faiblesses :
  - Les flux de signalisation (SIP, H.323)
  - Les flux médias RTP, RTCP
  - Les flux de provisionning : 802.1x, DHCP, DNS, TFTP
- Les éléments d'une architecture et ses vulnérabilités :
  - Les téléphones : Hardphones, Softphones
  - Les passerelles : Proxy SIP, Registrar, Gateway

LES ATTAQUES ET LEUR PARADES
- L'atteinte à la confidentialité : Ecoute de communication, récupération de code secret …
- L'atteinte à l'intégrité : modification des données transmises sur le réseau
- L'atteinte à la disponibilité et le déni de service.
- L'usurpation d'identité
- La fraude : surfacturation, détournement d'identité…
- Le SPAM

LA SÉCURITÉ DES ACCES
- Les concepts :
  - Le filtrage réseau, DMZ, liste noire, liste blanche,
  - Le principe des Firewalls *(Rôle, mode statefull/stateless)*
  - Le SBC : Session Border Controller
  - Exemples d'architectures sécurisées
- Le filtrage réseau
  - Les différents critères de filtrage
  - La translation d'adresse NAT : STUN, TURN, ICE
- Le filtrage applicatif
  - Les Firewalls, Proxy, SBC
  - Les critères de filtrage VOIP
  - Le Logging, aspect technique et juridique

LA SÉCURITÉ DES ECHANGES
- Les fonctions de cryptographie
- Les algorithmes fondamentaux
  - Les algorithmes symétriques
  - Les algorithmes asymétriques
  - Le Hashing
- Les combinaisons d'algorithmes
  - Le HMAC
  - Les certificats
  - La signature électronique

SÉCURISER VOTRE ARCHITECTURE VOIP *(SUITE)*

CONTENU :

- L'identification / Authentification
  - Le concept
  - Les protocoles PAP, SPAP, CHAP
  - L'identification / Authentification dans SIP
- Les protocoles de chiffrement
  - TLS, IPSEC*(AH, ESP, SA, IKE)*
  - SRTP
  - Le protocole MICKEY ou la gestion des clés en environnement multimédia

► **RECOMMANDATION D'ARCHITECTURE VOIP**

- Les postes téléphoniques
- Les équipements réseaux : Switch, serveurs,
- L'IPBX
- Les Gateway

► **CONCLUSION**