Sécurité de la téléphonie IP (Partie 1)

Durée:
2 jours

Niveau:
Avancé,
Expert

Sécurité de la téléphonie sur IP (Partie 1)

Cette formation présente la sécurité de la téléphonie sur IP sous un angle théorique et indépendant des offres constructeurs.

Une place importante est donnée à l'état de l'art du domaine ainsi qu'aux aspects méthodologiques. Néanmoins, l'approche reste pragmatique avec notamment la présentation synthétique des meilleures pratiques et recommandations à suivre.

Objectifs:
Savoir identifier les objectifs de sécurité d'une solution ToIP.
Comprendre les menaces et les vulnérabilités.
Connaître les outils et mécanismes de sécurisation de la ToIP.
Prendre en compte les recommandations et meilleures pratiques en vigueur.

Pré-requis :
Avoir suivi les formations Convergence voix-données ou avoir les connaissances équivalentes.

Cours magistraux illustrés par des études de cas, des exercices et des démonstrations pratiques.

Public :
Ce cours est destiné à des profils techniques (consultants, ingénieurs avant-vente, ingénieurs et administrateurs de solutions ToIP) mais peut tout à fait convenir à des décideurs et des responsables de services informatiques (DSI, RSSI, etc.).

JOUR 1

A - Menaces et principales attaques

1 - Introduction à la sécurité de la ToIP
VoIP: avantages et inconvénients
Quelques mythes...
Analyse de risques
Définitions et terminologie
Méthodologie générale des attaques
Démonstration: énumération avec l'outil nmap.

2 - Attaques en déni de service
Attaques basées sur la charge (*flooding*)
- attaques génériques
- attaques spécifiques

Démonstration: attaque DoS avec l'outil sipsak.
Attaques basées sur des paquets ou messages malicieux (*fuzzing*)
Démonstration: utilisation des outils PROTOS.
Attaques DoS propres à la VoIP
- détournements (*hijacking*)
- falsification (*spoofing*)

3 - Écoute et analyse de trafic
Accès aux infrastructures
Attaques préparatoire
Reniflement et écoutes téléphoniques
Démonstration: écoute d'une conversation téléphonique

4 - Fraudes et accès non autorisés
Facteurs favorisants
Typologie des fraudes
Méthodes d'attaques
Démonstration: crack d'un compte SIP (login / mot de passe)

5 - Menaces sociales
SPIT, SPIM et SPP
Voice Pishing (*vishing*)
Autres nuisances ou menaces sociales

B - Vulnérabilités

Analyse des vulnérabilités

1 - Divulgation des informations
Ingénierie sociale
Vol d'informations

2 - Architecture, Design
Vérification insuffisante des données
Manques de ressources
Gestion de mots de passe
Qualité de l'infrastructure réseau
etc.

3 - Mise en oeuvre
Défauts à l'exécution
Erreurs de manipulation des variables de développement
Gestion des erreurs
etc.

4 - Configuration
Gestion
Permissions et privilèges

Sécurité de la téléphonie IP (Partie 1)

JOUR 2

C - Protections: outils et mécanismes

1 - Protection de la signalisation
- Authentification SIP: *HTTP Digest Authentication*
- Transport Layer Security
- Secure SIP (SIPS)
- S/MIME
- SIP et S/MIME
- IPsec
- Protections applicables à MGCP
- Protections H.323 (H.235)
- Protections de protocoles propriétaires

2 - Protection des flux média
- Secure RTP (SRTP)
- Dérivation des clés de session
- Secure RTCP

3 - Gestion des clés de chiffrement
- Protocole MIKEY
- SDescription (SDES)
- ZRTP
- DTLS-SRTP

4 - Contrôle d'accès
- AAA
- DIAMETER pour SIP
- VoIP-aware Firewall
- Considérations spécifiques au NAT
  - STUN
  - TURN
  - ICE
- Session Border Controler (SBC)
- Détection d'intrusions

D - Cadre de sécurité pour la ToIP

1 - VoIP & Référentiels de sécurité
- NIST SP800-58
- ISO 27001

2 - Prise en compte ISO27001
- Politique de sécurité VoIP
- Tiers
- Gestion des biens
- Sécurité physique et environnementale
- Sécurité des équipements
- Gestion des opérations
- Contrôle d'accès
- Gestion des incidents
- Continuité opérationnelle

E - Synthèse des meilleures pratiques

1 - Infrastructure
- Sécurité des réseaux convergents
- Sécurité physique
- Réseaux de campus
- Spécificités Wi-Fi
- Divers

2 - Systèmes terminaux
- Téléphones matériels (*hardphone*)
- Téléphones logiciels (*softphone*)
- Passerelles VoIP

3 - IPBX, Serveurs ToIP
- Serveurs ToIP
- Proxy SIP

4 - Applications VoIP/ToIP
- Service TFTP
- Service DNS
- Service DHCP

5 - Architecture sécurisée
- Coupe-feu (*firewall*)
- Contrôle d'accès
- Sondes IDS