Sécurité avancée

[CO14]

Ce cours vous permet d'évaluer le niveau de risque de vos réseaux à travers les différents solutions et outils actuellement déployés. Il vous permet également d'acquérir les connaissances théoriques nécessaires pour comprendre les principales solutions avancées de sécurité.

OBJECTIFS

Cette formation vous permet de :

- Maîtriser une architecture de sécurité
- Maîtriser les solutions de sécurité
- Maîtriser la mise en œuvre d'attaques
- Contrer les attaques les plus courantes

PARTICIPANTS

Responsables réseau, responsables sécurité des systèmes d'information (RSSI), administrateurs, architectes réseaux souhaitant comprendre et mettre en œuvre les cyber attaques afin de protéger leurs réseaux.

PRÉ-REQUIS

Connaissances générales sur les réseaux Ethernet/IP : infrastructure, protocoles, applications. Notions sur la sécurité des réseaux.

TRAVAUX DIRIGÉS

Des travaux pratiques (50% de la formation) permettent de valider les acquis.

DURÉE

5 jours

INTRODUCTION ET RAPPELS

- Rappels sur TCP/IP
- L'architecture des réseaux
- Equipements et fonctions : Firewall, proxy, IDS
- Architecture et services de sécurité
- Manipulation du trafic avec Scapy

PROTOCOLES DE SÉCURITÉ

- Principes et algorithmes cryptographiques symétriques et asymétriques.
- Certificats X509
- Protocole IPsec
- Réseaux privés virtuels (VPN)
- Protocoles SSL/TLS
- Travaux pratiques
  - Génération de certificats X509
  - Serveur web sécurisé
  - Tunnel VPN-IPSEC

ATTAQUES RÉSEAUX

- Taxonomie des attaques
- Déni de service distribué
- ARP et DNS spoofing
- Attaques par flooding
- Attaques de type Smurf
- Mise en place d'attaques

LES SYSTÈMES DE DÉTECTION D'INTRUSIONS

- Méthodes de détection d'intrusions
- IDS Snort
  - Installation et configuration
  - Création des règles
  - Interprétation des alertes
- IDS Suricata
  - Installation et configuration
  - Création des règles
  - Interprétation des alertes
- Travaux pratiques Mise en œuvre d'un scénario réel : firewalls, DMZ, proxy, serveurs, IDS, etc.

SÉCURITÉ DES RÉSEAUX WI-FI

- Contexte (acteurs, réglementation, standards)
- Architectures, protocoles WEP, WPA, WPA-2
- Faiblesses, attaques et solutions
- Travaux pratiques : attaques sur les réseaux WiFi

SÉCURITÉ DE LA TÉLÉPHONIE SUR IP

- Architecture d'un système VoIP
- Protocoles SIP, RTP, RTCP
- Attaques sur SIP et RTP
- Travaux pratiques sur Asterisk