FC9CS05 2 890 € 4 jour(s)

[Formation] Sécurité des réseaux

OBJECTIFS

- Acquérir une vision globale des problèmes de sécurité liés aux réseaux actuels
- Maîtriser les concepts sous-jacents aux solutions applicables
- Disposer des bases nécessaires pour sécuriser une connexion Internet
- Avoir une vue d'ensemble des aspects sécurité liés à la problématique d'interconnexion des réseaux

PROGRAMME

Introduction

Concepts fondamentaux et contexte de l'Internet

- Problèmes de sécurité sur l'Internet, origine des failles, risques
- Évolutions des menaces et modes d'attaques, écosystème
- Logiciels malveillants, malwares
- Sécurité des antivirus

Attaques réseaux

- Sécurité des réseaux LAN (Ethernet, VLAN, etc.)
- Attaques réseau classiques : usurpation, Man-in-the-Middle, déni de service, etc.
- Techniques de reconnaissance et de prise d'empreinte à distance
- Attaques par déni de service (DoS, DDoS) : taxonomie, moyens de protection

Audits de sécurité

- Social Engineering, sécurité par mot de passe
- Catégories, principes, outils d'audits (Nmap, Nessus, Arachni, Burp, etc.)
- Recherche de vulnérabilités non connues par « Fuzzing »

AVANCÉ

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Toute personne désirant acquérir une vision globale de la sécurité des réseaux, impliquée dans la sécurité des systèmes d'information (SI) ou du réseau de l'entreprise, ou en charge de projets avec des experts sécurité réseaux ou SI.

Une connaissance générale en réseaux IP est un prérequis. Une connaissance des bases de la sécurité sont souhaitables afin de tirer pleinement profit de la formation.

COORDINATEURS

Xavier AGHINA

Responsable de la Sécurité des Systèmes d'Information (RSSI) chez W-HA, avec l'objectif de garantir la sécurité, la disponibilité et l'intégrité du système d'information et des données. Il a développé une expertise en cybersécurité, par la conduite des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés.

Laurent BUTTI

Spécialiste sécurité depuis plus de 20 ans, au sein d'entités de recherche et développement chez un grand opérateur, puis

Supervision et gestion des événements de sécurité

- Logiciels de détection et de prévention d'intrusion (IDS/IPS)
- Security Event Information Management (SIEM)

Sécurité des réseaux sans-fil WiFi (802.11)

- Problématiques de sécurité et architectures WiFi sécurisées
- Principes de sécurisation
- Architectures WiFi sécurisées en contexte Hot-Spot, résidentiel et entreprise

Protocoles de sécurité réseau

- Contextes IPv4 et IPv6
- Protocoles cryptographiques, gestion des clés, certificats X509
- Protocole SSL/TLS
- IPsec
- Réseaux privés virtuels (VPN)
- Exemples et démonstrations

Architectures de sécurité

- Problématique et exemples d'architectures de sécurité
- Pare-feux réseaux (filtres de paquets, relais applicatifs, Stateful Inspection)
- Serveurs mandataires
- Zone démilitarisée DMZ.
- Place des VLAN pour la sécurité

Détection et gestion des événements de sécurité

- Évolution des attaques et des failles
- Organigramme typique d'une attaque
- Détection/prévention d'intrusion (IDS/IPS)
- Gestion des événements de sécurité (SIEM)
- Tendances et nouvelles menaces

Audits techniques de sécurité

- Social Engineering (techniques)
- Sécurité par mots de passe
- Recherche de vulnérabilités
- Analyse de risques

Synthèse et conclusion

de développement et d'hébergement d'applications Web dans un contexte à fortes contraintes opérationnelles.

MODALITES PEDAGOGIQUES

Des exemples illustrent les concepts théoriques.