Sécurité VPN sans-fil et mobilité

DURÉE
4 jours (28h)

RÉFÉRENCE
RST47

CATÉGORIE
Sécurité Du Réseau

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Connaitre les problématiques de sécurité liées aux réseaux sans-fil
- Evaluer les vulnérabilités des protocoles de communication sans fil
- Comprendre la solution VPN
- Etre capable de sécuriser les réseaux sans-fil

POUR QUI ?

- Administrateurs systèmes et réseaux
- Experts en sécurité

Programme détaillé

1/ Les principes et concepts fondamentaux de la sécurité informatique

- Vue d’ensemble de la sécurité du Système d’Information
- Les composants de la cybersécurité
- Principales méthodes et normes pour l’analyse des risques
- Evaluation des risques dans un contexte de mobilité

2/ Appréhender les attaques sur l'utilisateur

- Les techniques d'attaques orientées utilisateur
- Les techniques de Social engineering
- Codes malveillants et réseaux sociaux
- Les dangers spécifiques du Web 2.0
- Attaque sur les mots de passe
- Attaque "Man in the Middle"

3/ Appréhender les attaques sur les postes clients

- Présentation des risques des postes clients
- Le navigateur le plus sûr
- Rootkit navigateur et poste utilisateur
- Les logiciels antivirus sont-ils efficaces ?
- Les risques associés aux périphériques amovibles
- Rôle du firewall personnel
- Sécurité des clés USB
- Les postes clients et la virtualisation

4/ Sécurité des réseaux sans-fil

- Les technologies WiFi : Rappels
- Le WiFi et ses vulnérabilités
- Vue d'ensemble des modes de chiffrement
- Le matériel offensif
- Présentation des risques inhérents aux réseaux sans fil
- Moyens pour protéger un réseau WiFi
- Configurer un routeur dans les différents modes
- Attaques dans les différents cas de figure (dont injections avec une carte Alpha)
- Durcissement de la configuration
- WiFi Pineapple

5/ Sécurité des réseaux privés virtuels (VPN)

- Différentes technologies et protocoles
- Sécuriser le transport des données
- Présentation des limites et exemples d’attaques
- Mise en place d’un tunnel IPSEC
- Sniffing
- Illustrer une attaque : le mode agressif

6/ SDR, HackRF One et Gnu Radio Companion

- Technologies radio : Introduction
- Les principes SDR
- Les principaux types de modulation
- Décoder un signal et présentation des principaux outils libres
- HackRF One et Yard Stick One
- GnuRadio
- Étude d’un carillon sans-fil
- Attaque par rejeu
- Décodage du signal et modulation avec le Yard Stick One

7/ Technologie Bluetooth

- Principes de fonctionnement du Bluetooth (BR, EDR et Low Energy)
- Les principaux risques
- Le paradoxe de la difficulté de détection (attaque et défense)
- Présentation de l'Urbertooth One
- Prise en main de l'Ubertooth
- Sniffing du trafic BLE

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 10 Juil. 2026	Casablanca - Maroc
01 au 04 Sep. 2026	Casablanca - Maroc
27 au 30 Oct. 2026	Casablanca - Maroc

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Scannez pour accéder à la fiche en ligne