

Sécurité VPN, sans-fil et mobilité

Référence : **SECSVSM**

Durée : **3 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- Maîtrise de l'administration système et réseau.
- Maîtrise des technologies de virtualisation (Virtualbox).
- Notions de Scripting (Shell, Python).
- Utilisation autonome de l'invite de commande Linux.

PROFIL DES STAGIAIRES

- Administrateurs systèmes et réseau.
- Experts en sécurité.

OBJECTIFS

- Former et sensibiliser des équipes techniques aux problématiques de sécurité liées aux réseaux sans-fil, dans le contexte actuel de forte mobilité des outils technologiques.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

- Rappels sur les technologies WiFi
- Revue des modes de chiffrement
- Présentation du matériel offensif
- Description des différentes techniques d'attaque
- Présentation des moyens de protection

WiFi

- Le WiFi et ses vulnérabilités
- Comment protéger un réseau WiFi

TP Wifi

- Configuration d'un routeur dans les différents modes
- Attaques dans les différents cas de figure (dont injections avec une carte Alpha)
- Durcissement de la configuration
- Présentation du WiFi Pineapple

VPN

- Présentation des différentes technologies et protocoles
- Sécurisation du transport des données
- Limites et exemples d'attaques

TP VPN

- Mise en place d'un tunnel IPSEC
- Sniffing
- Illustration d'une attaque : le mode agressif

JOUR 2

SDR, hackRF One et Gnu Radio Companion

- Introduction basique aux technologies radio
- Explications sur les principes SDR
- Reconnaître les principaux types de modulation

- Méthodes pour décoder un signal et présentation des principaux outils libres
- Présentation du HackRF One et du Yard Stick One

TP SDR

- Prise en main du HackRF One, GnuRadio, etc.
- Étude d'un carillon sans-fil
- Attaque par rejeu
- Décodage du signal et modulation avec le Yard Stick One

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

TP Bluetooth

- Prise en main de l'Ubertooth
- Sniffing du trafic BLE