

FICHE TECHNIQUE DE FORMATION

Cryptographie

Objectifs de la Formation:

Comprendre les concepts et les techniques de la cryptographie.

Développer des compétences pour sécuriser les données avec des méthodes cryptographiques.

Maîtriser les outils et les pratiques pour implémenter la cryptographie dans les systèmes d'information.

Public Cible:

Ingénieurs en sécurité, développeurs, administrateurs réseau, toute personne impliquée dans la sécurisation des données.

Prérequis:

Connaissances de base en cybersécurité et en mathématiques.

Méthodologie Pédagogique:

Exposés théoriques, démonstrations pratiques, ateliers interactifs, études de cas.

Programme de la Formation:

1. Introduction à la Cryptographie

Concepts de Base : Comprendre les principes de la cryptographie.

Historique de la Cryptographie : Exploration de l'évolution et des applications de la cryptographie.

2. Chiffrement Symétrique

Algorithmes Symétriques : Présentation des algorithmes de chiffrement symétrique (AES, DES).

Techniques de Chiffrement : Techniques pour implémenter le chiffrement symétrique.

3. Chiffrement Asymétrique

Algorithmes Asymétriques : Exploration des algorithmes de chiffrement asymétrique (RSA, ECC).

Techniques de Chiffrement : Méthodes pour implémenter le chiffrement asymétrique.

4. Hachage et Intégrité des Données

Algorithmes de Hachage : Présentation des algorithmes de hachage (SHA-256, MD5).

Techniques d'Intégrité : Techniques pour assurer l'intégrité des données.

5. Signature Numérique et PKI

Signatures Numériques : Utilisation des signatures numériques pour authentifier les données.

Infrastructure à Clé Publique (PKI) : Concepts et mise en œuvre de la PKI.

6. Protocoles de Sécurité

Protocoles SSL/TLS : Exploration des protocoles SSL/TLS pour sécuriser les communications.

Protocoles de Sécurité des E-mails : Présentation des protocoles pour sécuriser les e-mails (PGP, S/MIME).

7. Cryptographie Quantique et Post-quantique

Concepts de Cryptographie Quantique : Introduction aux principes de la cryptographie quantique.

Algorithmes Post-quantiques : Exploration des algorithmes de cryptographie post-quantique.

8. Applications Pratiques

Ateliers de Chiffrement et Hachage : Exercices pratiques pour implémenter des techniques de chiffrement et de hachage.

Simulations de Sécurisation des Communications : Jeux de rôle pour pratiquer la sécurisation des communications.

9. Outils de Cryptographie

Outils Logiciels : Introduction aux outils logiciels pour la cryptographie (OpenSSL, GnuPG).

Automatisation des Tâches de Cryptographie : Techniques pour automatiser les tâches de cryptographie.

10. Évaluation Finale