Année: 2024-2025
Promotion: 3IRC
Semestre: 5

STN - CyberSécurité

Cryptographie et protocoles pour la sécurité informatique (32 heures)

24_25_3IRC_05_UE4_SECU_042_C

ACQUIS

· Analyser les différents algorithmes de cryptographie et identifier leur rôle dans la sécurisation des communications et des informations
· Appliquer des techniques et algorithmes cryptographiques pour sécuriser efficacement les informations et les communications numériques
· Évaluer les risques de sécurité liés aux vulnérabilités des systèmes informatiques avec un focus sur les aspects cryptographiques et proposer des solutions adaptées pour atténuer ces risques.
· Intégrer les bonnes pratiques pour développer et intégrer des applications sécurisées
· Implémenter et configurer des protocoles sécurisés tels que SSL/TLS et SSH, essentiels pour la sécurisation des communications réseaux
· Assurer la gestion des clés Cryptographiques : génération, partage, stockage, et révocation
· Identifier les vulnérabilités cryptographiques et réaliser des audits de sécurité ciblés
· Appliquer une politique de sécurité adaptée face aux risques et menace cyber.

CONTENU

· Enjeux de la sécurité informatique
- Importance de la sécurité de l'information
- Risques et conséquences des cyberattaques
- Analyse de différents types de cyberattaques
- Déni de service et déni de service distribué (DoS ou DDoS)
- Rançongiciel (Ransomware)
- Hameçonnage (Phishing)
- Password Spraying
- Dépassement de tampon (buffer overflow)
- Attaque par force brute, dictionnaire
- Malware
- Les méthodes et les outils d'attaque
· La cryptologie et ses applications dans le domaine de la sécurité informatique
- Cryptographie, présentation des outils de cryptographie
- Chiffrements symétriques et asymétriques
- Introduction au hachage et à la sécurité des mots de passe
- Principes du hachage cryptographique
- Hachage de mot de passe avec salting
- Méthodes pour renforcer la sécurité des mots de passe

- Chiffrement et signature numérique
- Infrastructure à clé publique (PKI)
- Présentation des PKI (Public Key Infrastructure) et HTTPS
- Certificate Authority Based
- Utilisation de certificats (X509)
- Web of Trust (PGP)
- TOFU (SSH, Signal Protocol)
· Travaux pratiques : Exercices pratiques et outils pour l'audit de sécurité des mots de passe
- Utilisation d'outils de "cracking" de mot de passe (John the Ripper, Hashcat)
- Techniques d'audit pour évaluer la robustesse des mots de passe
· Travaux pratiques : Création et configuration de certificats pour HTTPS
- Générer une paire de clés (publique et privée)
- Création de demandes de signature de certificat (CSR)
- Signature et gestion de certificats avec une autorité de certification (CA) ou en auto-signé
- Configuration de serveurs web (par exemple, Apache, Nginx) pour utiliser HTTPS

PRÉREQUIS

· Principes de base de l'algèbre et des mathématiques discrètes
· Notions de base des probabilités et des statistiques
· Fondamentaux de la programmation en langages tels que Python ou Java
· Structures de données (listes, files, piles, tables de hachage)
· Principes de base des systèmes d'exploitation
· Notions de base sur le fonctionnement des réseaux TCP/IP et des architectures réseau.

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE