INSI

Syllabus de la Formation Cyber Attaque et Administration Réseaux et Systèmes

Aucune description

Niveau : Avancée

Prix : à partir de 0,00 Ar HT

Durée : jours | heures

Place : personnes

Sessions

Objectifs de cette formation

- Comprendre les bases des cyberattaques et les méthodes de sécurisation des réseaux et systèmes.
- Appliquer les meilleures pratiques pour sécuriser les infrastructures réseau et système.
- Identifier et répondre efficacement aux incidents de sécurité.
- Utiliser des outils de pentesting pour évaluer la sécurité des systèmes.
- Développer des stratégies de défense pour protéger les actifs informatiques de l’entreprise.

Programmes de cette formation

- - Introduction aux Cyberattaques et Sécurité Réseau Matinée

    1. **Accueil et présentation**
    2. Objectifs de la formation
    3. Tour de table des participants
    4. **Panorama des cyberattaques**
    5. Historique des cyberattaques célèbres
    6. Typologie des cyberattaques (phishing, malware, ransomware, DDoS, etc.)
    7. **Concepts fondamentaux de la cybersécurité**
    8. Principes de base de la cybersécurité (confidentialité, intégrité, disponibilité)
    9. Modèle CIA (Confidentiality, Integrity, Availability)
    10. **Rappels sur l’administration des réseaux**
    11. Modèle OSI et TCP/IP
    12. Configuration de base des routeurs et des commutateurs
    13. Protocoles de routage (RIP, OSPF, BGP)
    14. **Sécurisation des réseaux**
    15. Pare-feu et systèmes de détection d’intrusion (IDS/IPS)
    16. VPN et réseaux privés virtuels
    17. Segmentation réseau et VLAN

- - Administration des Systèmes et Sécurité Matinée

    1. **Rappels sur l’administration des systèmes**
    2. Introduction aux systèmes d’exploitation (Windows, Linux)
    3. Gestion des utilisateurs et des permissions
    4. Surveillance et gestion des ressources système
    5. **Sécurité des systèmes d’exploitation**
    6. Mise à jour et gestion des correctifs
    7. Antivirus et antimalware

8. Configuration sécurisée des systèmes
9. **Meilleures pratiques de sécurisation**
10. Hardening des systèmes (Linux, Windows)
11. Configuration sécurisée des serveurs web (Apache, Nginx)
12. Sécurisation des bases de données (MySQL, PostgreSQL)
13. **Gestion des incidents de sécurité**
14. Identification et analyse des incidents
15. Réponse aux incidents et plan de reprise
16. Analyse post-incident et amélioration continue

- - Pratiques Avancées et Études

1. **Techniques de cyberattaque avancées**
2. Exploitation des vulnérabilités (buffer overflow, injection SQL)
3. Attaques sur les réseaux sans fil (Wi-Fi hacking)
4. Ingénierie sociale et manipulation psychologique
5. **Évaluation des vulnérabilités**
6. Utilisation des outils de scan de vulnérabilités (Nessus, OpenVAS)
7. Introduction au pentesting (Metasploit, Kali Linux)
8. **Études de cas pratiques**
9. Analyse de cyberattaques réelles
10. Discussion des leçons apprises et des stratégies de défense
11. **Simulation de cyberattaque**
12. Mise en place d’un environnement de test
13. Exécution et analyse d’une cyberattaque simulée
14. Développement de stratégies de mitigation