Comprendre l’attaque pour se défendre

Objectifs de la formation

- Comprendre le rôle des différents matériels et logiciels dans un réseau local.
- Acquérir les techniques d’installation et de configuration des composants d’un réseau local.
- Analyser les paquets réseau et interpréter les modèles de trafic réseau à l'aide de Wireshark.
- Identifier et diagnostiquer les problèmes de performance du réseau et les menaces de sécurité.
- Acquérir une connaissance des concepts fondamentaux de la cybersécurité et des considérations éthiques.
- Comprendre le monde de la cybersécurité et sa gouvernance, les risques et menaces, le cadre technique, normatif, légal et réglementaire.
- Explorer les cyberattaques avec des scénarios prédéfinis, identifier les menaces et les vulnérabilités, et comprendre l’architecture nécessaire à une sécurité solide.
- Se concentrer sur les aspects pratiques de la mise en œuvre des mécanismes de sécurité en mettant l’accent sur les compétences pratiques et les meilleures pratiques.

Volume horaire de la formation : 10 jours (50 heures)

Dates et créneaux horaires seront fixés ultérieurement

Contenu de la formation

1- **Fondements des Réseaux**

- Expliquer le rôle et la fonction des composants réseau
- Décrire les caractéristiques des architectures et topologies réseau
- Modèle OSI et TCP/IP
- Configurer et vérifier l'adressage et le sous-réseautage (subnetting) IPv4
- Configurer et vérifier l'adressage et les préfixes IPv6
- Décrire les principes des réseaux sans-fil
- Expliquer les fondamentaux de la virtualisation

2- Analyser le réseau avec Wireshark

- Introduction à Wireshark et aux réseaux de données
- Supports de transmission et normes
- Format d'une trame Ethernet
- Adresses réseau et encapsulation IP
- Protocoles :
  - ✓ ARP
  - ✓ ICMP
  - ✓ DHCP
  - ✓ DNS
  - ✓ HTTP / HTTPS
- Installation de Wireshark
- Fonctionnalités Wireshark
- Diagnostic des performances du réseau
- Les tâches d'analyse

3- Concepts fondamentaux de la sécurité

- Enjeux et impact de la cybersécurité
- Objectifs de la sécurité de l'information
- Menaces, vulnérabilités et risques
- Gestion des risques et conformité
- Gouvernance de la cybersécurité
- Continuité des activités et reprise après sinistre
- Attributs et processus des attaques
- Méthodologie de la chaîne de destruction cybernétique
- Indicateur de compromis
- Phases de Cyberattaque
- Analyse des vulnérabilités

4- Concept de Cyberattaque avec des scénarios prédéfinis

- Scanning du réseau
- Enumération
- Attaque serveur web
- Attaque d’application web
- Attaque par injection SQL
- Denial of Service

5- Concept de Cyberdéfense

- Outils et technologies de défenses
- Chiffrement
- Installation et administration d'outils de filtrage
- Détection d'intrusions
- Collecte et analyse d'informations