

CyberSécurité

Sécurité des systèmes (36 heures)

26_27_4IRC_07_CYBER_UE2_021_MAJ

ACQUIS

- Comprendre les bases de la sécurité des systèmes Windows et Linux.
- Mettre en oeuvre des configurations sécurisées sur les systèmes d'exploitation.
- Gérer les utilisateurs, les permissions et les processus critiques.
- Effectuer une surveillance de base à l'aide des journaux et détecter des anomalies simples.

CONTENU

- Introduction aux systèmes d'exploitation et à la sécurité
 - Architecture de base de Windows et Linux.
 - Différences clés entre les deux systèmes.
 - Introduction aux commandes de base : PowerShell pour Windows, Bash pour Linux.
 - Gestion des utilisateurs et des permissions.
 - Gestion des comptes utilisateurs et groupes (Windows et Linux).
 - Permissions de fichiers : NTFS et ACLs (Windows), chmod et sudo (Linux).
 - Mise en oeuvre du principe du moindre privilège.
 - Durcissement des systèmes d'exploitation
 - Désactivation des services inutiles.
 - Configuration de sécurité réseau : Pare-feu Windows Defender, SSH sécurisé sur Linux.
 - Gestion des mises à jour et réduction des vulnérabilités.
 - Introduction à la journalisation.
 - Concepts et importance de la journalisation.
 - Journaux système : Event Viewer (Windows), Syslog et journaux SSH (Linux).
 - Analyse simplifiée pour détecter des anomalies.
 - Exercices pratiques et études de cas.
 - Gestion des permissions et utilisateurs.
 - Configuration sécurisée de SSH et des politiques locales.
- Analyse de journaux pour détecter des comportements suspects.

PRÉREQUIS

- Connaissance de base des systèmes d'exploitation (concepts de fichiers, processus, et réseaux).
- Familiarité avec les commandes de base de la ligne de commande (Windows CMD/PowerShell, Bash).

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE